

ECU	Test specification of Penetration Testing for ECU	1/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

<b>関係各部署 御中</b> <b>To departments concerned</b>	Confidential level	<div>PROTECTED</div> <div>関係者外秘</div>	原紙保管 Storage of original	M/Y /
			コピー保管 Storage of copy	M/Y /

<b>ECU 侵入テスト仕様書</b> <b>Test Specification of Penetration Testing for ECU</b>	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-EPN-TST-SPEC-a00-04-a			
	承認 Approved 河井	調査 Checked 松井	作成 Created 玉樹	2021/05/31
適用 Scope	19PF Ver.2 以降のエントリーポイントを有する ECU に適用する。 Applies to ECUs that have an entry point in 19PF Ver2 and later.			
変更内容 Revision Record	<b>【主な変更点 Main changes】</b> (SEC-ePF-VUL-EPN-TST-SPEC-a00-03-a ⇒ SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a) ・要件変更 Change requirements			
特記 Special note	<b>【入手先 Source】</b> 本文書は iSpirit からダウンロードしてください。 This document can be downloaded from iSpirit. [Folder]/Repository/Electronics_Spec/Cybersecurity[サイバーセキュリティ]/Standard [標準]/SPEC[仕様書]/VUL[脆弱性]/仕様書 ALL 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.			
	<b>【問合せ先 Contact Information】</b> 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			

ECU	Test specification of Penetration Testing for ECU	2/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## 変更履歴<sup>Δ1</sup>

記号	Version	日付	変更者	項目	変更内容
	a00-00-a	2018/6/30	51F 尾崎	全項目	
Δ1	a00-01-a	2018/11/6	51F 尾崎	変更履歴	変更履歴の表を追加
↑	↑	↑	↑	3. 用語の定義	“エントリポイント”の定義を上位文書の記載に統一
↑	↑	↑	↑	6. 侵入テスト要件	<ul style="list-style-type: none"> <li>・実施者についての備考「外部組織へテストを委託してもよい」を要件に変更</li> <li>・テスト内容の要件を変更</li> </ul>
↑	↑	↑	↑	参考資料 1	<ul style="list-style-type: none"> <li>・テストケースの名称を内容が分かりやすいように更新</li> <li>・重複していたテストケースの削除（「ダイアグ機能の OSS 脆弱性によるコマンドインジェクション」「ネットワーク経路による攻撃：ARP ポイズニング」）</li> </ul>
↑	↑	↑	↑	全項目	その他の誤記修正
Δ2	a00-02-a	2019/4/26	46F 尾崎	1.1. 本書の目的	開発プロセスの手順に沿うように修正
↑	↑	↑	↑	1.2. 適用範囲	<ul style="list-style-type: none"> <li>・表 1 を追加して対象 ECU の条件を設定</li> <li>・設計変更における考え方を変更</li> </ul>
↑	↑	↑	↑	1.3. 関連文書	<ul style="list-style-type: none"> <li>・関連文書一覧の表を追加</li> <li>・公的関連文書一覧の表に『SP 800-115』『WP29』『個人情報保護法』を追加</li> </ul>
↑	↑	↑	↑	1.4. 用語の定義	<ul style="list-style-type: none"> <li>・“エントリポイント”の定義を上位文書の記載に統一</li> <li>・“エントリポイント”以外の用語を追加</li> </ul>
↑	↑	↑	↑	1.5. 関係者の定義	新規追加
↑	↑	↑	↑	2. 侵入テスト要件	<ul style="list-style-type: none"> <li>・テスト全体の進め方の見直しに沿って表 5 の内容を修正</li> <li>・表 6 を追加</li> </ul>
↑	↑	↑	↑	Appendix 1	章と表の名前を変更
↑	↑	↑	↑	Appendix 2, 3	新規追加
↑	↑	↑	↑	全項目	<ul style="list-style-type: none"> <li>・章立てを変更</li> <li>・その他の軽微な修正</li> </ul>

ECU	Test specification of Penetration Testing for ECU		3/24
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

Δ 3	a00-03-a	2020/6/23	46F 松井	1.1. 目的	<ul style="list-style-type: none"> <li>・ “リスク許容のできない” 脆弱性が存在しないことを確認するという表現へ目的を変更</li> </ul>
↑	↑	↑	↑	1.2. 適用範囲	<ul style="list-style-type: none"> <li>・ 1.2.2.項に “Post19PF 以降の適用範囲” を追加</li> <li>・ 1.2.3.項に “設計変更における再実施” を追加</li> </ul>
↑	↑	↑	↑	1.3. 関連文書	関連文書に以下を追加 <ul style="list-style-type: none"> <li>・ 19 電子 PF LAN 情報セキュリティ対策要件書</li> <li>・ ISO/SAE 21434</li> </ul>
↑	↑	↑	↑	1.4. 用語の定義	用語の定義を全体的に更新
↑	↑	↑	↑	1.5. 関係者の定義	<ul style="list-style-type: none"> <li>・ 評価者に「修正の必要な脆弱性が発見された場合」の役割を追加</li> </ul>
↑	↑	↑	↑	1.6. 前提条件	<ul style="list-style-type: none"> <li>・ 前提条件の節を追加</li> </ul>
↑	↑	↑	↑	2. 要件	<ul style="list-style-type: none"> <li>・ 要件番号を追記</li> <li>・ 侵入テストの要件に「事前合意・許可」の項目を追加</li> <li>・ エビデンスに記載する項目を更新</li> <li>・ 2.2.節に “脆弱性対策の要件” を追加</li> </ul>
↑	↑	↑	↑	表紙	<ul style="list-style-type: none"> <li>・ 【入手先】を追加</li> </ul>
Δ 4	a00-04-a	2021/5/31	46F 菅野	1.2. 適用範囲	1.2.2.項 “Post19PF 以降の適用範囲” を更新
↑	↑	↑	↑	1.3. 関連文書	<ul style="list-style-type: none"> <li>・ リスク指標定義書の Specification No.を追加</li> </ul>
↑	↑	↑	↑	2.1. 侵入テスト要件	<ul style="list-style-type: none"> <li>・ 参照先の変更に合わせて表 7 の No.3 内の要求 ID を修正</li> <li>・ 表 7 の No.8 のネットワークとサーバに関する要件を修正</li> </ul>
↑	↑	↑	↑	全て	英訳追加

ECU	Test specification of Penetration Testing for ECU		4/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a	

## 目次

<b>1. はじめに</b>	<b>5</b>
1.1. 目的	5
1.2. 適用範囲	6
1.2.1. 19PF における適用範囲	6
1.2.2. Post19PF 以降における適用範囲 <sup>Δ3Δ4</sup>	6
1.2.3. 設計変更における再実施（19PF／Post19PF 以降で共通） <sup>Δ3</sup>	7
1.3. 関連文書	8
1.4. 用語の定義	9
1.5. 関係者の定義 <sup>Δ2</sup>	11
1.6. 前提条件 <sup>Δ3</sup>	12
<b>2. 要件</b>	<b>13</b>
2.1. 侵入テストの要件	13
2.2. 脆弱性対策の要件 <sup>Δ3</sup>	18
<b>Appendix 1. テストケースの例 <sup>Δ2</sup></b>	<b>19</b>
<b>Appendix 2. 情報及び機材の例 <sup>Δ2</sup></b>	<b>22</b>
<b>Appendix 3. テスト内容立案の考え方 <sup>Δ2</sup></b>	<b>23</b>

ECU	Test specification of Penetration Testing for ECU		5/24
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## 1. はじめに

お客様に安全・安心なクルマを提供するため、車載部品の脆弱性を低減するための活動が必要である。車載部品に潜在する脆弱性を発見するには、侵入テストを実施することが有効である。本書では、ECUを対象とする侵入テストの要件を示す。<sup>Δ2</sup>

なお、適用範囲になるかの判断や要件を満たせるかの判断が難しい場合は、トヨタのセキュリティ主管部署、トヨタの ECU 設計部署及び ECU 開発者で協議することとする。<sup>Δ2</sup>

### 1.1. 目的

ECU 開発チーム以外のメンバーでありサイバーセキュリティに関する高度な能力を有する評価者が、市場での攻撃を模擬することで、ECU にリスク許容のできない脆弱性が存在しないことを確認する

<sup>Δ2Δ3</sup>

ECU	Test specification of Penetration Testing for ECU		6/24
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## 1.2. 適用範囲

19PF における本書の適用範囲は 1.2.1 項に従うこと。一方で、Post19PF 以降は 1.2.2 項に従うこと。  
 なお、1.2.3 項で定義する、設計変更における再実施については、19PF にも Post19PF 以降にもどちらにも適用してよい。<sup>Δ3</sup>

### 1.2.1. 19PF における適用範囲

19PF Ver.2 以降のエントリポイントを有する ECU のうち、表 1 の条件のいずれかを満たすものに適用する。<sup>Δ2</sup>

表 1. エントリポイントを有する ECU のうち侵入テストの対象となるものの条件 (19PF) <sup>Δ2</sup>

No.	条件	条件に該当する ECU の例	備考
1	セキュリティレベル L3 に該当するもの	AVN、DCM、ITS	<ul style="list-style-type: none"> <li>攻撃への遭遇確率が高いため</li> <li>セキュリティレベル L3 の定義は『19 電子 PF LAN 情報セキュリティ対策要件書』<sup>Δ3</sup>を参照</li> </ul>
2	グローバルバスに接続されており且つ通信のなりすましによりリスクランク 7 以上の事象となるもの	本書発行時点ではなし	<ul style="list-style-type: none"> <li>攻撃が成功した際の影響度が大きいため</li> <li>本書発行時点では、19PF のエントリポイントを有する ECU は、この条件に該当することが許可されていない。</li> </ul>
3	エントリポイントを持つシステムと持たないシステムをつなぐ 2 層目に該当するもの	CGW、ESW	<ul style="list-style-type: none"> <li>攻撃が成功した際の影響度が大きいため</li> </ul>

### 1.2.2. Post19PF 以降における適用範囲<sup>Δ3Δ4</sup>

Post19PF のエントリポイントを有する ECU のうち、表 2 の条件のいずれかを満たすものに適用する。

表 2. 侵入テストの対象となるものの条件 (Post19PF 以降)

No.	条件	条件に該当する ECU の例	備考
1	AP20 に該当するもの	AVN、DCM	<ul style="list-style-type: none"> <li>攻撃への遭遇確率が高いため</li> <li>AP の定義は『ECU 脆弱性対策要求仕様書』を参照</li> </ul>

ECU	Test specification of Penetration Testing for ECU		7/24
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

2	エントリポイントを持つシステムと持たないシステムをつなぐ2層目に該当するもの	Central ECU	・ 攻撃が成功した際の影響度が大きい
---	--	-------------	--------------------

### 1.2.3. 設計変更における再実施（19PF／Post19PF 以降で共通）<sup>Δ3</sup>

ECU の設計変更において以下の①～③をすべて満たす場合は、脆弱性の混入につながらないと判断できるため、侵入テストを実施しなくてよい。<sup>Δ2</sup>

- ① その設計変更より前の版数（※1）の ECU に対して本書に従って侵入テストを実施し、そのエビデンスが存在すること<sup>Δ3</sup>  
（※1） ECU ノード名及びサプライヤが同一であれば、前の版数と見なしてよい。
- ② 自 ECU に新たなエントリポイントが追加されないこと
- ③ 自 ECU のエントリポイントを制御するハードウェア及びソフトウェアに、サイバーセキュリティに係る変更をしないこと

ただし、以下の例はサイバーセキュリティに係る変更該当するため、③を満たさない。

1. エントリポイントを制御するマイコンの変更（ただし、マイコンのメモリ容量変更や、マイコン内蔵ペリフェラルの削除は、サイバーセキュリティに係らない変更である。）
2. エントリポイントを制御するマイコンに、設計変更前まで未実装の通信規格を用いるインタフェースを追加（例：エントリポイントではない Ethernet や USB の追加）
3. エントリポイントを制御するマイコンにおける、OS、BSW 又はサイバーセキュリティに係るソフトウェアモジュール（SELinux、TOMOYO Linux 等）の置き換え

ECU	Test specification of Penetration Testing for ECU	8/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

### 1.3. 関連文書

表 3. トヨタ発行関連文書一覧<sup>Δ2</sup>

仕様書番号	名称
SEC-24PF-VCL- RIC-INST-DOC <sup>Δ4</sup>	Post19 電子 PF サイバーセキュリティリスク指標定義書(未発行) Post19ePF Cyber Security Risk Criteria Definitions(Unissued) <sup>Δ4</sup>
SEC-ePF-VUL- ECU-REQ-SPEC	ECU 脆弱性対策要求仕様書 Requirements specification of vulnerability countermeasure for ECU
SEC-ePF-VUL- ECU-TET-SPEC	ECU 脆弱性対策評価仕様書 Test specification of vulnerability countermeasure for ECU
SEC-ePF-VUL- CMN-REQ-SPEC	共通脆弱性対策要求仕様書 Requirements Specification of Common Vulnerability Countermeasure
SEC-ePF-TRM- GUD-PROC	制御電子 PF サイバーセキュリティ及びプライバシー用語定義書 Terms and Definitions related to Cybersecurity and Privacy in E/E Architecture

表 4. 公的関連文書一覧

本書における略称	名称/外部リンク
SP 800-115 <sup>Δ2</sup>	National Institute of Standards and Technology (NIST) , U.S. Department of Commerce, “Technical Guide to Information Security Testing and Assessment,” (Sep. 2008), <a href="https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf">https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf</a>
NHTSA-BP	National Highway Traffic Safety Administration (NHTSA) , U.S. Department of Transportation, “Cybersecurity Best Practices for Modern Vehicles,” (Oct. 2016), <a href="https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf">https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf</a>
ISO18045 <sup>Δ2</sup>	ISO/IEC 18045:2008, “Information technology — Security techniques — Methodology for IT security evaluation,” (Aug. 2008)
個人情報保護法 <sup>Δ2</sup>	個人情報の保護に関する法律（平成 15 年法律第 57 号） <a href="https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf">https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf</a> Act on the Protection of Personal Information (Act No. 57 of 2003) <a href="http://www.japaneselawtranslation.go.jp/law/detail/?id=2781&amp;vm=04&amp;re=01&amp;new=1">http://www.japaneselawtranslation.go.jp/law/detail/?id=2781&amp;vm=04&amp;re=01&amp;new=1</a>
ISO/SAE 21434 <sup>Δ2Δ3</sup>	ISO/SAE DIS 21434:2020, “Road Vehicles — Cybersecurity engineering,” (Feb. 2020)



ECU	Test specification of Penetration Testing for ECU	9/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

#### 1.4. 用語の定義

この節では、本書において特に詳細に定義すべき用語を解説する。なお、この節に解説のない用語は、『制御電子 PF サイバーセキュリティ及びプライバシー用語定義書』の解説の通りとする。<sup>Δ3</sup>

#### 侵入テスト<sup>Δ2</sup>

アプリケーション、システム又はネットワークのセキュリティ機能を回避する方法を特定するために、評価者が実際の攻撃を模擬するセキュリティテスト。

侵入テストは3つのフェーズ（計画フェーズ、実行フェーズ及び報告フェーズ）からなる。侵入テストの実施とは、3つのフェーズをいずれもすべて実施することである。

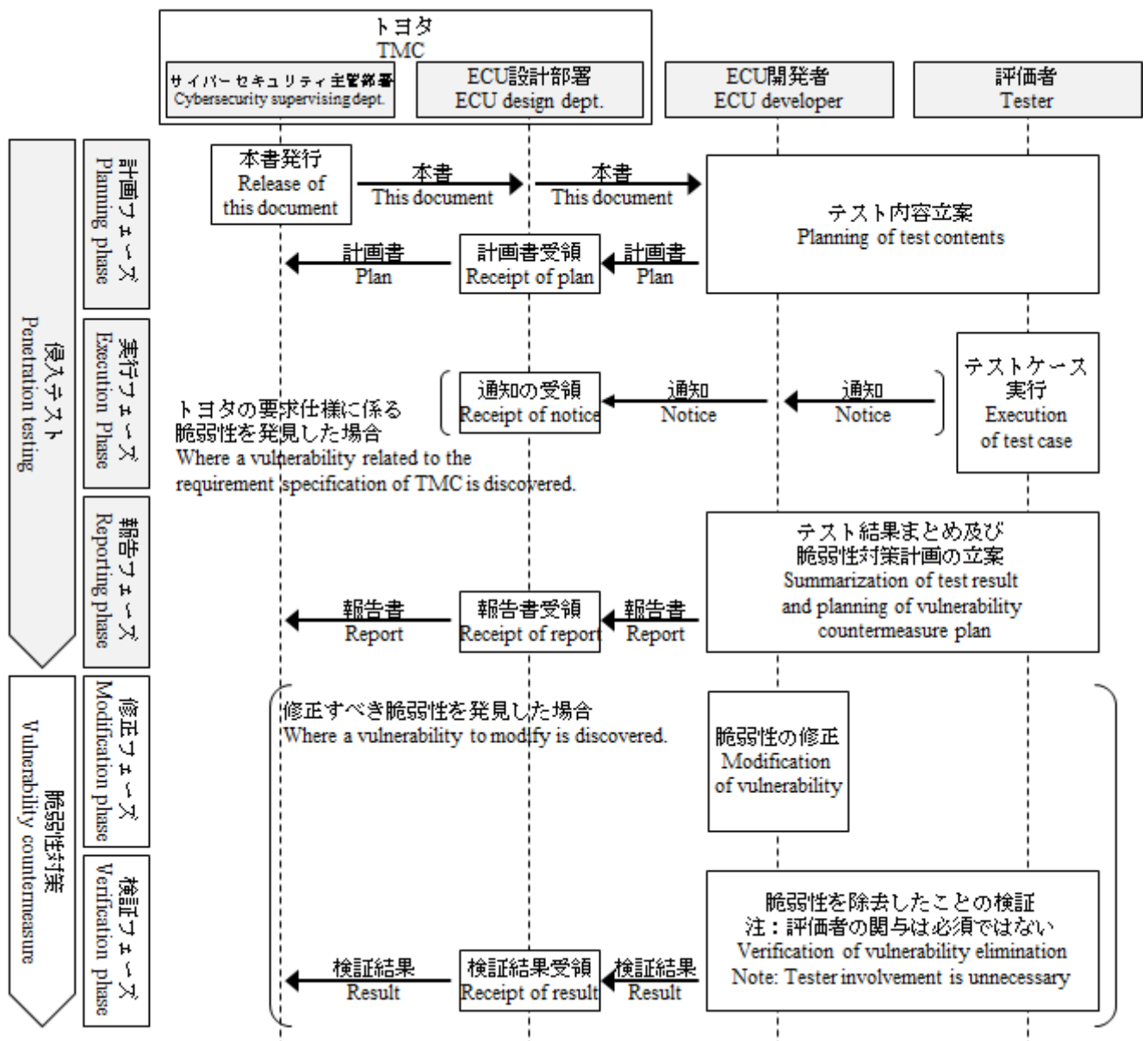


図1. 侵入テストと脆弱性対策の進め方のイメージ<sup>Δ3</sup>

ECU	Test specification of Penetration Testing for ECU	10/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

### 脆弱性対策<sup>Δ3</sup>

脆弱性対策は、2つのフェーズ（修正フェーズ及び検証フェーズ）からなる。侵入テストを実施した後に、実施する。脆弱性対策の実施とは、2つのフェーズをどちらも実施することである。侵入テストによって、修正の必要な脆弱性が発見されなかった場合は、脆弱性対策を省略できる。

### テストケース<sup>Δ2</sup>

脅威が生じる恐れのあるシナリオを実現するために、どのようなテストをするかを洗い出してまとめたもの。下図のイメージを参照。

1件のテストケースを実行することによって、少なくとも1個以上の脆弱性の有無が明らかにできるような粒度で設計される。

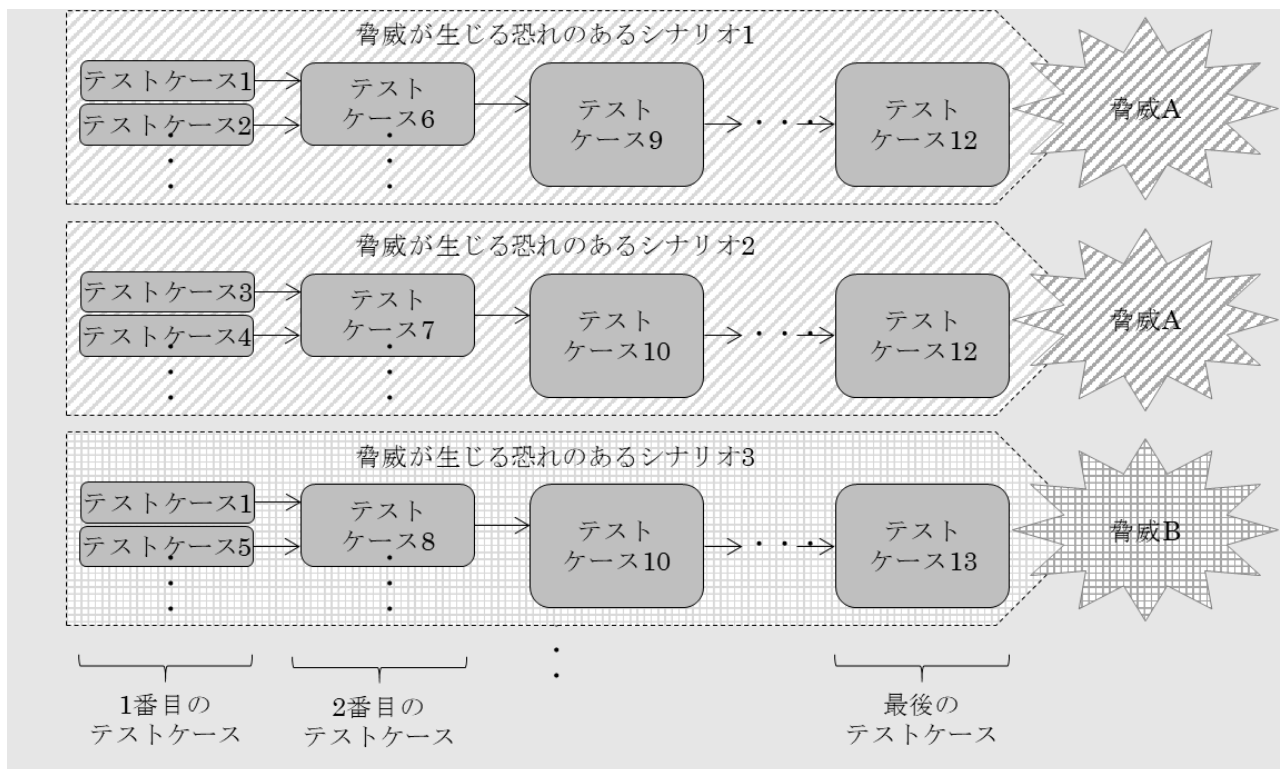


図2．脅威とテストケースの関係性のイメージ<sup>Δ2</sup>

ECU	Test specification of Penetration Testing for ECU	11/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

### 1.5. 関係者の定義 <sup>Δ2</sup>

ECU に対する侵入テストにおける関係者の一覧とその役割を示す。

表 5. 関係者の一覧とその役割

関係者	役割
トヨタのサイバーセキュリティ 主管部署 (46F3G)	トヨタにおいて、車両のサイバーセキュリティを担保するため、 電子 PF のセキュリティ対策を開発する。以下の活動をする。 ➤ 本書の引き当て条件の定義 ➤ 本書の発行
トヨタの ECU 設計部署	トヨタにおいて、電子 PF のセキュリティ機能を搭載した ECU の設計を行う。以下の活動をする。 ➤ ECU に対する本書の引き当て ➤ 計画書、報告書及び検証結果を開発文書の一部として保管
ECU 開発者	ECU 開発チームのメンバーであり、評価者とともに侵入テスト 及び脆弱性対策を実施する。以下の活動をする。 ➤ 計画フェーズ及び報告フェーズの実施（実行フェーズの実施 は不可） ➤ 修正の必要な脆弱性が発見された場合に、修正フェーズ及び 検証フェーズの実施 <sup>Δ3</sup> ➤ トヨタの ECU 設計部署へ、計画書、報告書及び検証結果を 提出
評価者	ECU 開発者とともに侵入テスト及び脆弱性対策を実施する。以 下の活動をする。 ➤ 計画フェーズ、実行フェーズ及び報告フェーズをすべて実施 ➤ 修正の必要な脆弱性が発見された場合に、検証フェーズを実 施（任意） <sup>Δ3</sup>

ECU	Test specification of Penetration Testing for ECU		12/24
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

#### 1.6. 前提条件<sup>△3</sup>

本書では、ECU 開発者及び評価者が、表 6 の各項目について適切に対応することを前提としている。

表 6．前提条件

No.	分類	前提条件	背景
1	ツール	所属組織におけるツールに係る規程に従って、使用したツールを管理する。	ISO21434 5.4.7 項 Tool Management
2	脆弱性	所属組織における脆弱性に係る規程に従って、発見された脆弱性を管理する。	ISO21434 7.6 節 Vulnerability Management
3	エビデンス	所属組織における情報セキュリティ管理規程に従って、各エビデンスを管理する	ISO21434 5.4.8 項 5.4.8 Information Security Management, ISO21434 10.5 節 Work Products の[WP-10-06]

ECU	Test specification of Penetration Testing for ECU	13/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## 2. 要件

### 2.1. 侵入テストの要件

【要件番号：VULEPN\_00001】<sup>Δ3</sup>

侵入テストの適用対象となった ECU は、表 7 の要件に従い、侵入テストを実施すること。

表 7. 侵入テストの要件

No.	分類	要件	備考
1	実施時期	次の条件をもとに実施時期を選定すること。 1. (必須条件①) CV 品の納入までに侵入テストの実施を完了できること <sup>Δ2</sup> 2. (必須条件②) 号試移行までに脆弱性対策の実施を完了できること 3. (推奨条件) 号口品に可能な限り近い仕様をもとに実装した ECU をテストできること	シス検品以降の ECU を対象に実施することを想定
2	進め方 <sup>Δ2</sup>	ECU 開発者及び評価者は、次のフェーズを実施すること。 ➤ 計画フェーズ：ECU 開発者及び評価者は、本書に従ってテスト内容を立案し、計画書を作成する。 実行フェーズの前に、テスト環境を構築するための準備を行う ➤ 実行フェーズ：評価者は、計画に従ってテスト環境を構築し、テストケースを実行する ➤ 報告フェーズ：ECU 開発者及び評価者は、テスト結果のまとめ及び脆弱性対策計画の立案を行い、報告書を作成する	計画フェーズ及び報告フェーズは『SP 800-115』における同じ用語に対応している。 実行フェーズは『SP 800-115』における発見フェーズと攻撃フェーズのふたつを包含したものである。
3	対象 ECU <sup>Δ2</sup>	号口品と同等の仕様をもとに実装した ECU にテストをすること。やむを得ず同等にできない場合は、号口品との仕様の差分とその理由をエビデンスに記すこと。	特権機能（テストアクセスポート等）に対しても、号口品と同等のセキュリティ対策を有効にすること。 『共通脆弱性対策要求仕様書』の要件 VULCMN_00400 <sup>A4</sup> 及び VULCMN_02500 <sup>A4</sup> を参照。
4	対象機能	1. 脅威分析で明らかになった脅威が生じる恐れのある機能をテストすること。 <sup>Δ2</sup> 2. (設計変更時に侵入テストを実施する場合、) 設計変更より前の版数(※1)で侵入テストが実施されて	—

ECU	Test specification of Penetration Testing for ECU	14/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

No.	分類	要件	備考
		<p>いるならば、設計変更により影響を受ける機能のみをテストすることとしてよい。<sup>Δ2</sup></p> <p>(※1) ECU ノード名及びサブライヤが同一であれば、前の版数と見なしてよい。</p>	
5	実施体制 <sup>Δ2</sup>	<p>1. 評価者は、ECU 開発チームのメンバーではないこと<sup>Δ2</sup></p> <p>2. 評価者には、サイバーセキュリティテストに関する十分な能力(※2)を有している者を少なくとも一人以上含むこと<sup>Δ2</sup></p> <p>3. 外部組織へテストを委託してもよい<sup>Δ1</sup></p> <p>(※2) サイバーセキュリティについて5年以上のプロフェッショナルとしての業務経験(大卒者は4年間の経験で可(1年分の経験免除))且つ過去3年間に類似のテスト(※3)を実施した経験があること。</p> <p>(※3) 類似のテストとは、対象 ECU に使用されている技術に係る組込みシステムに対する侵入テストとする。<sup>Δ2</sup></p>	<p>・『NHTSA-BP』6.6.2 節に“テストを行うにあたり、開発チーム以外のメンバーであり、十分な能力を有しているテスターや、脆弱性の特定に対して高いインセンティブが与えられているメンバーを含むべきである”と記載されているため</p> <p>・業務経験年数の条件は、サイバーセキュリティの国際資格である CISSP の認定条件を引用</p>
6	提供情報・提供機材 <sup>Δ2</sup>	<p>ECU 開発者は、開発チームによる脆弱性分析結果を評価者に提供すること。また、次の条件に当たる情報及び機材を評価者に提供すること。</p> <p>I. 対象 ECU を正常に動作させるために必要なもの</p> <p>II. 製品出荷後に市場で入手可能なもの</p> <p>III. テスト時間の短縮に有効であり且つ現実的な時間内に攻撃者が入手可能であるとの証拠を評価者が示したもの</p>	<p>・『Appendix 2. 情報及び機材の例』を参考にしてもよい。</p> <p>・現実的な時間とは、『ISO18045』の攻撃能力の計算方法から、おおよそ半年間と想定。</p> <p>・評価者は ECU 開発者に用途を説明すること。</p>
7	テスト内容	<p>ECU 開発者及び評価者は、計画フェーズにおいて、以下の順にテスト内容を立案すること。<sup>Δ2</sup></p> <p>I. 開発チームによる脆弱性分析結果の提供：対象 ECU の開発において行った脆弱性分析の結果を、ECU 開発者から評価者に提供する。<sup>Δ2</sup></p> <p>II. 脅威分析：評価者は、ECU 開発者から提供された対象 ECU の情報をもとに、攻撃者目線で脅威分析を行う。<sup>Δ2</sup></p> <p>III. シナリオ検討：II.の脅威分析で明らかになった</p>	<p>・外部組織への委託の必要性の検討に、『Appendix 1. テストケースの例』を参考にしてもよい。</p> <p>・テスト内容立案の手順には、『Appendix 3. テスト内容立案の考え方』の解説を参考にしてもよい。<sup>Δ2</sup></p>

ECU	Test specification of Penetration Testing for ECU	15/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

No.	分類	要件	備考
		脅威が生じる恐れのある攻撃シナリオを、評価者の能力で実行できる範囲で検討する。 <sup>Δ2</sup> IV. テストケース作成：検討した攻撃シナリオをすべて実行できるように、テストケースを作成する。 <sup>Δ2</sup>	
8	事前合意・許可 <sup>Δ3</sup>	ECU 開発者は、少なくとも次の条件に当たる行為を実行する場合は、事前にトヨタの ECU 設計部署へ問合せし、許可を得ること。 1. トヨタの許可が必要な情報及び機材を評価者へ提供 2. トヨタの所有する機材の不可逆な操作や破壊 3. ECU 開発者または評価者が所有していないネットワークやサーバへの接続 <sup>Δ4</sup>	同様に、ECU 開発者評価者の間でも、提供機材の取り扱い等について事前に合意することが望ましい。
9	エビデンス <sup>Δ2</sup>	1. ECU 開発者及び評価者は、計画フェーズにおいて、計画書を作成すること。計画書は、実行フェーズの開始の前にトヨタの ECU 設計部署へ提出すること <sup>Δ2</sup> 2. ECU 開発者及び評価者は、報告フェーズにおいて、報告書を作成すること。報告書は、CV 品の納品までにトヨタの ECU 設計部署へ提出すること <sup>Δ2</sup> 3. 計画書及び報告書には、少なくとも表 8 の各項目を記載すること <sup>Δ2Δ3</sup> ただし、表 8 の各項目のうち、No.6「テスト内容」及び No.7「発見した脆弱性」の内容は、評価者が作成すること。ECU 開発者は、評価者の合意なく内容を変更しないこと <sup>Δ3</sup> 4. エビデンスに記載する情報が、『個人情報保護法』における“個人情報”に該当しないよう配慮すること	『NHTSA-BP』6.6.2 節に“侵入テスト報告書は、サイバーセキュリティアプローチに関連する内部文書の一部として保管すべきである。文書化する際は評価者、評価者の能力、評価者の長所について明記すべきである。報告書には、検知したサイバーセキュリティの脆弱性への対策に係る内容、及び、対策方法の詳細を文書化すべきである。”と記載されているため。
10	その他	1. トヨタからのテストに関する問合せに回答できること。テスト内容や作業ログ（例：ターミナルログ等）は、報告書の提出から半年間は保存すること。 2. トヨタの要求仕様に係る脆弱性を発見した場合は、発見した時点で速やかにトヨタの ECU 設計部署へ通知すること。 3. 発見した脆弱性の再現手順を、ECU 開発者が再現可能な粒度で示すこと。 <sup>Δ2</sup> 4. 発見した脆弱性の深刻度を評価すること。深刻度の評価基準には、CVSS v3 を用いること。CVSS v3 のほかに、別の評価基準も併せて用いる場合は、その評	1.について、脆弱性の改修方針を決定するまでに、最大で半年かかると想定。

ECU	Test specification of Penetration Testing for ECU	16/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

No.	分類	要件	備考
		価基準の仕様を示すこと。 <sup>Δ2</sup>	

【要件番号：VULEPN\_00002】 <sup>Δ3</sup>

ECU に対する侵入テストを実施する際には、表 8 の項目をエビデンスへ記載すること。

表 8. エビデンスに記載する項目 <sup>Δ2</sup>

No.	項目	記載内容	計画書での 記載の要否	報告書での 記載の要否
1	実施時期	➤ 計画フェーズ、実行フェーズ及び報告フェーズのスケジュール	要	要
2	対象 ECU	➤ 対象 ECU のハードウェア及びソフトウェアの版数を特定できる情報（例：名称、品番、ソフト品番） ➤ 対象 ECU と号口品との差分の有無及び差分がある場合にはその一覧	要	要
3	対象機能	➤ 侵入テスト対象となる機能を限定する場合には、除外する機能の一覧と除外理由 ➤ 設計変更時のテストにおいて、対象機能を限定する場合にはその機能の一覧	要	要
4	実施体制	➤ ECU 開発者及び評価者の体制（例：人数、役割分担） ➤ ECU 開発者の責任者及び業務窓口担当者 ➤ 評価者の所属組織及び選定理由 ➤ 評価者の専門性を示す情報（例：業務経験、保有する能力）	要	要
5	提供情報・提供機材	➤ ECU 開発者から評価者への提供情報の一覧 ➤ ECU 開発者から評価者への提供機材の一覧	要	要
6	テスト内容	➤ 脅威の一覧 <sup>Δ3</sup> ➤ テストケースの一覧 ・テストケースの名称 ➤ テストケースの詳細 ・テストケースによって実現したい脅威 ・脅威により損なわれる資産とそのサイバーセキュリティ特性 <sup>Δ3</sup> ・テストケースにおいて標的とする攻撃の入口	要 (※4)	要 (※4)



ECU	Test specification of Penetration Testing for ECU	17/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

No.	項目	記載内容	計画書での記載の要否	報告書での記載の要否
		<ul style="list-style-type: none"> <li>・テストケースを実行するために使用するツールの情報 (例：名称、版数、再現のための設定) <sup>Δ3</sup></li> <li>➤ テストケースを実行するためのテスト環境の構成</li> <li>➤ テスト環境と実環境との差分 (※5) <sup>Δ3</sup>の有無及び差分がある場合にはその一覧</li> <li>(※5) 実環境とは、対象 ECU が車両に組み付いた状態のことである。 <sup>Δ3</sup></li> </ul>		
		<ul style="list-style-type: none"> <li>➤ テストケースの一覧 <ul style="list-style-type: none"> <li>・実行フェーズにおいて実行したか否か</li> <li>・脆弱性を発見したか否か</li> </ul> </li> <li>➤ 実行フェーズで実行しなかったテストケースがある場合はその理由</li> </ul>	-	要 (※4)
7	発見した脆弱性	<ul style="list-style-type: none"> <li>➤ 発見した脆弱性の一覧</li> <li>➤ 発見した脆弱性の詳細 <ul style="list-style-type: none"> <li>・脆弱性により損なわれる資産とそのサイバーセキュリティ特性 <sup>Δ3</sup></li> <li>・脆弱性の深刻度とその導出過程</li> <li>・脆弱性の再現手順</li> </ul> </li> </ul>	-	要 (※4)
8	脆弱性対策計画	<ul style="list-style-type: none"> <li>➤ 発見した脆弱性の対策計画 <ul style="list-style-type: none"> <li>・修正する脆弱性の修正方法とそのスケジュール</li> <li>・修正しない脆弱性を修正しないと判断した理由</li> </ul> </li> </ul>	-	要

(※4) 評価者が作成すること。ECU 開発者は、評価者の合意なく内容を変更しないこと。

ECU	Test specification of Penetration Testing for ECU		18/24
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## 2.2. 脆弱性対策の要件<sup>Δ3</sup>

【要件番号：VULEPN\_00003】

ECU に対する侵入テストによって、修正が必要な脆弱性が発見された場合、表 9 の要件に従い、脆弱性対策を行うこと。

表 9. 脆弱性対策の要件

No.	分類	要件	備考
1	進め方	<p>ECU 開発者及び評価者は、次の 2 つのフェーズを実施すること。</p> <ol style="list-style-type: none"> <li>修正フェーズ：ECU 開発者は、報告書に記載した脆弱性対策計画に沿って、修正する。</li> <li>検証フェーズ：ECU 開発者及び評価者は、脆弱性が修正できていることを検証する。ただし、評価者の関与は任意とする。</li> </ol>	<ul style="list-style-type: none"> <li>検証フェーズは、実行フェーズ及び報告フェーズを再実施することで、代替してもよい。</li> <li>検証の手段は、脆弱性が修正できたことが示せばよい。ため、テストは必須ではない。</li> </ul>
2	エビデンス	<ol style="list-style-type: none"> <li>ECU 開発者及び評価者は、検証フェーズにおいて、検証結果を作成すること。検証結果は、脆弱性の修正ができた試作品の納品までにトヨタの ECU 設計部署へ提出すること。</li> <li>検証結果には、脆弱性が修正できたことを示す根拠を記載すること。</li> </ol>	—

ECU	Test specification of Penetration Testing for ECU		19/24
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## Appendix 1. テストケースの例<sup>Δ2</sup>

外部組織への委託の必要性を検討するための参考資料として、侵入テストのテストケースの例を提示する。<sup>Δ2</sup>

下表は、あるセキュリティ会社が、ある ECU に対する侵入テストを計画した際の、テストケースの抜粋である。ECU によっては、プロトコルを実装していない等の理由で、実行しなくてよいテストケースが含まれている。<sup>Δ2</sup>

表 10. テストケースの例<sup>Δ1Δ2</sup>

分類	No.	テストケースの名称
Remote Access & Persistence	1	ダイアグ機能による ECU のバックドアの検出
	2	ダイアグ機能による不揮発性メモリへのアクセス
	3	ダイアグ機能による不揮発性メモリへの鍵のアクセス
	4	ダイアグ機能によるテストモードの検出、有効化
	5	ダイアグ機能によるデモモードの検出、有効化
	6	リバースエンジニアリングによるテストモードの検出、有効化
	7	リバースエンジニアリングによるデモモードの検出、有効化
	8	OSS 脆弱性によるファームウェアの変更
	9	ダイアグ機能による不揮発性メモリへのキー書き込み
	10	ダイアグ機能による不揮発性メモリへの書き込み
	11	ダイアグ機能によるファームウェアの変更
	12	ダイアグ機能による不揮発性メモリのバーンアウト
	13	ダイアグ機能によるファームウェアのダウングレード
	14	リバースエンジニアリングによる ECU のバックドアの検出
Execution	15	ダイアグ機能によるコマンドインジェクション
	16	CAN メッセージによるコマンドインジェクション
	17	OSS 脆弱性によるコマンドインジェクション
	18	ファームウェアイメージのセキュリティ対策の分析
	19	CAN リプレイ
	20	CAN メッセージのフラッディングによる侵入検知の妨害
	21	エラーメッセージの大量送信によるサービス妨害
	22	不正なダイアグメッセージ

ECU	Test specification of Penetration Testing for ECU	20/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

分類	No.	テストケースの名称
Execution	23	運転手に成りすまして偽装したコマンドでシステムを攪乱
	24	ダイアグメッセージのフラッディング
	25	ダイアグメッセージのフラッディングによる侵入検知の妨害
	26	ダイアグ機能の権限昇格
	27	SYN フラッディング
	28	CAN メッセージによるバッファオーバーフロー
	29	ダイアグメッセージによるバッファオーバーフロー
	30	OSS 脆弱性によるバッファオーバーフローインジェクション
	31	優先度の高いダイアグメッセージを許容される状態以外で送信
	32	ECU を中間者攻撃のために使用する
	33	ECU をリレーとして使用する
	34	ブートローダーのセキュリティ機能の回避
Delivery	35	物理ポートのセキュリティ機能の分析（プラグアンドプレイ機能の設定）
	36	物理ポートの侵入検知機能の分析
	37	クエリ文字列における機密情報
	38	HTTP GET における機密情報
	39	ネットワークの適切なセグメント化
	40	取り外し可能な記憶媒体からファームウェアを抽出する
	41	取り外し可能な記憶媒体を変更する
Development	42	デバイス間で鍵が共有されないようにする
	43	Web サービスの不正なアクティブ化
	44	ARP ポイズニング
	45	サービス妨害フラッディング
	46	キャプチャしたダイアグメッセージのリプレイ
	47	リスクの低いダイアグ機能によるデータの引き出し
	48	TCP ハイジャック
	49	TCPKill によるサービス妨害

ECU	Test specification of Penetration Testing for ECU	21/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

分類	No.	テストケースの名称
Development	50	通信のフレームパディングにおけるメモリ情報の漏えい
	51	CAN メッセージのフィルタリング
	52	ブートローダーがファームウェアを適切に認証しない
Discovery	53	無防備なネットワークやサービスの受動的発見（通信キャプチャ）
	54	脆弱性スキャンツールによるスキャン
	55	ネットワークストレステスト
	56	telnet、TFTP、SSH、ダイアグ機能のデータファジング
	57	telnet、TFTP、SSH、ダイアグ機能プロトコルファジング
	58	通信フレームの処理時間の計測による応答性能の分析
	59	バックアップによって機密情報を保存する
	60	無防備なネットワークやサービスの能動的発見（ポートスキャン）
	61	期限切れのカーネル
	62	期限切れのライブラリおよびアプリケーション
	63	取り外し可能な記憶媒体
	64	ハードウェアデバッグポート
	65	SSH、TFTP、FTP、telnet 共通認証情報の利用
	66	アクセス制御のエラーメッセージの分析
	67	デフォルト認証を使用するファクトリーリセット
	68	ダイアグ機能によって予期せぬ状態をアクティブ化する
	69	通信によって予期せぬ状態をアクティブ化する
	70	リバースエンジニアリングによる予期せぬ状態の発見

ECU	Test specification of Penetration Testing for ECU		22/24
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## Appendix 2. 情報及び機材の例<sup>A2</sup>

ECU に対する侵入テストを実施するために用いる情報及び機材の例を表 11 に示す。

開発中の ECU に関する情報及び機材は、市場ではまだ入手ができない。このため、評価者が市場での攻撃を模擬できるように、ECU 開発者から評価者へ表 11 の情報及び機材を提供する。

なおこの表は参考資料であるため、やむを得ない事情があれば提供しなくてよい。また、表に記載していないものの提供を妨げるものではない。

表 11. 情報及び機材の例

No.	説明	情報の例	機材の例
1	対象 ECU を正常に動作させるために必要なもの	<ul style="list-style-type: none"> <li>➤ コネクタのピンアサイン</li> <li>➤ ECU の起動手順、リセット手順</li> </ul>	<ul style="list-style-type: none"> <li>➤ ECU 試作品</li> <li>➤ ワイヤハーネス</li> <li>➤ 外付け部品 (例：アンテナ)</li> </ul>
2	製品出荷後に市場で入手可能なもの	<ul style="list-style-type: none"> <li>➤ オーナーズマニュアルに記載する情報</li> <li>➤ サービスマニュアルに記載する情報</li> <li>➤ 車載ネットワークにおける対象 ECU の接続構成</li> <li>➤ 対象 ECU の有する入出力インタフェースと、その規格（例：CAN、USB、100BASE-TX）及び設定値（例：MAC アドレス、IP アドレス、VLAN ID）</li> <li>➤ 対象 ECU が搭載する半導体パッケージ（例：マイコン、マイコン外付けメモリ）の型番、製造者、データシート及びマニュアル。 ただし、例えば HSM（Hardware Security Module）のマニュアルのように、入手に制限がなされている情報はこれに含まれない。</li> </ul>	<ul style="list-style-type: none"> <li>➤ 診断ツール</li> </ul>
3	テスト時間の短縮に有効であり且つ現実的な時間内に攻撃者が入手可能であるとの証拠を評価者が示したもの	<p>【現実的な時間内に攻撃者が入手可能である証拠を評価者が示した場合のみ】</p> <ul style="list-style-type: none"> <li>➤ 車載ネットワーク上で対象 ECU が送受信する信号の一覧</li> <li>➤ 使用しているオープンソースソフトウェアとそのバージョン</li> <li>➤ 暗号化済みリプロ用ファームウェア</li> <li>➤ 実行コード（バイナリ）</li> </ul>	<p>【現実的な時間内に攻撃者が入手可能である証拠を評価者が示した場合のみ】</p> <ul style="list-style-type: none"> <li>➤ リプロ用ツール</li> </ul>

ECU	Test specification of Penetration Testing for ECU	23/24
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

### Appendix 3. テスト内容立案の考え方<sup>△2</sup>

この参考資料では、テスト内容立案の手順について解説する。

テスト内容立案の手順は、『ISO21434』にもとづいたトヨタのサイバーセキュリティ開発プロセスと関係づけることを基本方針として作成している。イメージを下図に示した上で、重要なポイントについて解説する。<sup>△3</sup>

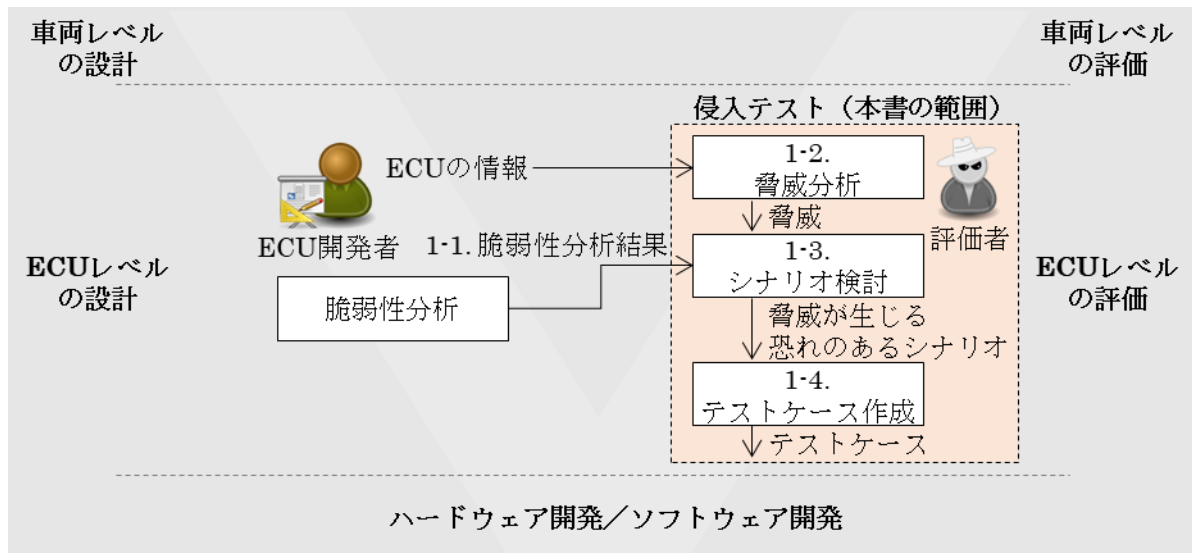


図3. テスト内容立案の考え方のイメージ

#### 1-1. 開発チームによる脆弱性分析結果の提供

➤ 侵入テストは、サイバーセキュリティ開発プロセスにおける“ECU レベルの評価”の工程に含まれる。このためV字モデル上では、“ECU レベルでの設計”の工程で実施する“脆弱性分析”と対の関係に位置づけることができる。この関係をもとに、開発チームによる脆弱性分析の結果をテスト内容立案において利用することとする。これには次の狙いがある。

- 脆弱性分析において対処すると判断した脆弱性のうち、実機で対処できていることを確認すべきと判断したものを、侵入テストで確認する。
- 評価者が実行する必要性の低いテストケースを作成することを避ける。なお、実行する必要性の低いテストケースとは、次の例のようなもののことである。

例1：ECU 開発者にとって既知の脆弱性に対するテストケース

例2：リスクが低いため ECU 開発者が許容した脆弱性に対するテストケース

➤ 脆弱性分析の手法については本書の範囲外であるが、例として、次のいずれかの結果を脆弱性分析結果として利用してもよい。

- 『ECU 脆弱性対策要求仕様書』に従った脆弱性分析
- 有識者による脆弱性分析の実施

➤ 本書の要件を満たすためだけに、開発チームが新たに脆弱性分析をすることは想定していない。

ECU	Test specification of Penetration Testing for ECU		24/24
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## 1-2. 脅威分析

- 侵入テストでは、ECU 開発チームとは独立した立場から、攻撃者の目線で行った分析結果を含めるべきである。これは、ECU 開発チームには気づけなかった脅威を、侵入テストによって発見することを狙うものである。
- 脅威分析の詳細手順は、本書では指定しない。なお、評価者は過去の侵入テストの経験を活かし、作業量の削減を図ることが望ましい。

## 1-3. シナリオ検討

- シナリオ検討の詳細手順は本書では指定しない。
- 「評価者の能力で実行できる範囲で検討」としているのは、侵入テストにおけるテスト内容の妥当性の裏付けは、突き詰めると評価者の能力に拠るものと考えているためである。
- 表 7 のエビデンスに記載する項目には、シナリオ検討の結果を含めていないが、これはシナリオを文書化する作業量の削減を狙ったものである。

## 1-4. テストケース作成

- テストケース作成の詳細手順は本書では指定しない。
- 本書では、評価者が必ず計画を立てるようにするため、実行フェーズの前に、計画書を作成することになっている。計画を立てることには、次の狙いがある。
  - 限られた期間に有効なテストを行うため、ECU の重要な部位に対して重点的にテストケース作成したり、テストケースの優先順位をつけたりする。
  - 侵入テストのエビデンスは、開発文書の一部として保管する。このため、脆弱性を発見したテストケースのほかに、“実行したが脆弱性が発見されなかったテストケース” 及び “実行しなかったテストケース” もエビデンスに記録する。
- 評価者に比べ、その他の関係者のサイバーセキュリティに関する能力は低いことが一般に想定されるため、評価者が作成したテストケースが、十分なものとなっているかの確認は難しい。一方で、標的とする攻撃の入口が十分に洗い出されているかは、ECU の特徴に詳しい ECU 開発者であれば比較的容易と考えられる。この様に、ECU 開発者は、評価者からテストケースを作成した背景をヒヤリングすることで、テストケースに不足がないかを確認することを推奨する。



ECU	Test specification of Penetration Testing for ECU	1/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## Revision Records<sup>Δ1</sup>

Mark	Version	Date	Revised	Item	Revision contents
	a00-00-a	Jun,30, 2018	51F Ozaki	All item	
Δ1	a00-01-a	Nov,06, 2018	51F Ozaki	Revision Records	Added the revision record table
↑	↑	↑	↑	3. Terms and Definitions	Unified the definition of entry point into that in upper-level documents
↑	↑	↑	↑	6. Requirements for Penetrating Testing	<ul style="list-style-type: none"> <li>• “Testing may be outsourced to an external organization.” has been changed from a remark to the requirement for the tester.</li> <li>• Revised the requirements on the test contents.</li> </ul>
↑	↑	↑	↑	Reference Material 1	<ul style="list-style-type: none"> <li>• Updated the names of the test cases to names that are easy to understand</li> <li>• Deleted the redundant test cases (“Command injection via OSS vulnerabilities of diagnostic function” and “Attack via network path: ARP poisoning”)</li> </ul>
↑	↑	↑	↑	All items	Error correction of the others
Δ2	a00-02-a	Apr,26, 2019	46F Ozaki	1.1. Purpose	Corrected the contents so as to be in accordance with the procedure of the development process
↑	↑	↑	↑	1.2. Scope	<ul style="list-style-type: none"> <li>• Added Table 1 to set the conditions of the target ECU</li> <li>• Changed the principle in engineering change</li> </ul>
↑	↑	↑	↑	1.3. Related Documents	<ul style="list-style-type: none"> <li>• Added a table of a list of related documents</li> <li>• Added SP 800-115, WP29, and Personal Information Protection Act to the list of official related documents</li> </ul>
↑	↑	↑	↑	1.4. Terms and Definitions	<ul style="list-style-type: none"> <li>• Unified the definition of “entry point” into that in upper-level documents</li> <li>• Added terms other than “entry point”</li> </ul>
↑	↑	↑	↑	1.5. Definitions of Persons Concerned	Added newly
↑	↑	↑	↑	2. Requirements for Penetrating	<ul style="list-style-type: none"> <li>• Corrected the contents in Table 5 in accordance with the ways to proceed with the whole test</li> </ul>

ECU	Test specification of Penetration Testing for ECU	2/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

				Testing	• Added Table 6
↑	↑	↑	↑	Appendix 1	Changed the names of the chapters and table
↑	↑	↑	↑	Appendices 2 and 3	Added newly
↑	↑	↑	↑	All items	<ul style="list-style-type: none"> <li>• Changed the chapter structure</li> <li>• Other minor correction</li> </ul>
Δ 3	a00-03-a	Jun,23, 2020	46F Matsui	1.1. Purpose	• Changed the expression in the purpose to confirm that there is no vulnerability “with unacceptable risks”.
↑	↑	↑	↑	1.2. Scope	<ul style="list-style-type: none"> <li>• Added “Scope of Post19PF and later” in subsection 1.2.2.</li> <li>• Added “Re-Testing due to design changes” in subsection 1.2.3.</li> </ul>
↑	↑	↑	↑	1.3. Related Documents	<ul style="list-style-type: none"> <li>Added following documents in the list of Related Documents</li> <li>• Cyber Security Countermeasure Requirements for 19PF</li> <li>• ISO/SAE 21434</li> </ul>
↑	↑	↑	↑	1.4. Terms and Definitions	Modified terms and definitions
↑	↑	↑	↑	1.5. Definitions of Persons Concerned	Added the role of “if the vulnerabilities which should be corrected is found” for tester
↑	↑	↑	↑	1.6. Preconditions	Added the section of Preconditions
↑	↑	↑	↑	2. Requirements	<ul style="list-style-type: none"> <li>• Added the Requirement ID</li> <li>• Added the items of “Prior agreement and permission” in the requirements of penetrating testing</li> <li>• Updated the items of evidence</li> <li>• Added “Requirements of vulnerability countermeasure” in section 2.2</li> </ul>
↑	↑	↑	↑	Cover	Added “Source”
Δ 4	a00-04-a	May,31, 2021	46F Sugano	1.2. Scope	Updated “Scope of Post19PF and later” in subsection 1.2.2

ECU	Test specification of Penetration Testing for ECU		3/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

↑	↑	↑	↑	1.3. Related Documents	Added the specification No. of Post19ePF Cyber Security Risk Criteria Definitions
↑	↑	↑	↑	2.1. Requirements of Penetrating Testing	<ul style="list-style-type: none"> <li>• Corrected the requirement ID in No.3 of Table7 in accordance with the modification of reference document.</li> <li>• Modified the requirement related to “network and server” described in No.8 of Table7.</li> </ul>
↑	↑	↑	↑	All	Add English translation

ECU	Test specification of Penetration Testing for ECU		4/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## Table of Contents

<b>1. Introduction.....</b>	<b>5</b>
1.1. PURPOSE.....	5
1.2. SCOPE .....	6
1.2.1. Scope of 19PF.....	6
1.2.2. Scope of Post19PF and later <sup>Δ3Δ4</sup> .....	6
1.2.3. Re-Testing due to a design changes (Common for 19PF and Post19PF and later) <sup>Δ3</sup> .....	7
1.3. RELATED DOCUMENTS.....	9
1.4. TERMS AND DEFINITIONS .....	10
1.5. DEFINITIONS OF PERSONS CONCERNED <sup>Δ2</sup> .....	13
1.6. PRECONDITIONS <sup>Δ3</sup> .....	14
<b>2. Requirements.....</b>	<b>15</b>
2.1. REQUIREMENTS FOR PENETRATION TESTING.....	15
2.2. REQUIREMENTS OF VULNERABILITY COUNTERMEASURE <sup>Δ3</sup> .....	23
<b>Appendix 1. Examples of Test Cases<sup>Δ2</sup> .....</b>	<b>24</b>
<b>Appendix 2. Examples of Information and Equipment<sup>Δ2</sup>.....</b>	<b>27</b>
<b>Appendix 3. Concept of Test Contents Planning<sup>Δ2</sup>.....</b>	<b>29</b>

ECU	Test specification of Penetration Testing for ECU		5/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## 1. Introduction

It is necessary to conduct activities for reducing vulnerabilities of an in-vehicle part in order to provide a safe and secure automobile to a customer. Implementation of penetrating testing is effective for discovering potential vulnerabilities in an in-vehicle part. This document indicates the requirements of penetration testing for an ECU<sup>Δ2</sup>.

If it is difficult to judge whether the scope is applicable or whether a requirement is satisfied, TMC security supervising dept., TMC ECU design dept. and the ECU developer shall discuss it<sup>Δ2</sup>.

### 1.1. Purpose

The purpose is to confirm that there is no vulnerability with unacceptable risks in an ECU via mimicking of attacks in the market by a tester who does not belong to the ECU development team and has a high level of cybersecurity related ability. <sup>Δ2Δ3</sup>

ECU	Test specification of Penetration Testing for ECU		6/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a	

## 1.2. Scope

The scope of this document for 19PF is accordance with subsection 1.2.1. On the other hand, the scope for Post19PF and later is accordance with subsection 1.2.2. In addition, Re-testing due to design changes may be applied to 19PF and Post19PF and later. <sup>Δ3</sup>

### 1.2.1. Scope of 19PF

This document shall apply to an ECU which has an entry point in 19PF Ver.2 and later and satisfies any of the conditions in Table 1. <sup>Δ2</sup>

Table1. Conditions to Be an ECU with an Entry Point Subject to Penetration Testing(19PF) <sup>Δ2</sup>

No.	Condition	Example of ECU satisfying the condition	Remarks
1	An ECU which security level is L3	AVN、DCM、ITS	<ul style="list-style-type: none"> <li>• Because of high probability of being attacked</li> <li>• Refer “Cyber Security Countermeasure Requirements for 19PF” for the definition of security level.</li> </ul>
2	An ECU which is connected to a global bus and to which communication spoofing brings about an event of Risk rank 7 or higher	n/a as of the release date of this document	<ul style="list-style-type: none"> <li>• Because of a great impact when an attack succeeds</li> <li>• As of the release date of this document, an ECU with an 19PF entry point is not allowed to fall under this condition.</li> </ul>
3	An ECU which serves as the Layer 2 connecting a system with an entry point and a system without an entry point	CGW、ESW	<ul style="list-style-type: none"> <li>• Because of a great impact when an attack succeeds</li> </ul>

### 1.2.2. Scope of Post19PF and later<sup>Δ3Δ4</sup>

This document shall apply to an ECU which has an entry point in Post19PF and satisfies either

ECU	Test specification of Penetration Testing for ECU		7/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

of the conditions in Table 2.

Table2. Conditions to Be an ECU to Penetration Testing (Post19 and later)

No.	Condition	Example of an ECU satisfying the condition	Remarks
1	An ECU which AP is 20	AVN, DCM	<ul style="list-style-type: none"> <li>• Because of a high probability of being attacked</li> <li>• Refer “Requirements Specification of Vulnerability Countermeasure of ECU” for the definition of AP</li> </ul>
2	An ECU which serves as the Layer 2 connecting a system with an entry point and a system without an entry point	Central ECU	<ul style="list-style-type: none"> <li>• Because of a great impact when an attack succeeds</li> </ul>

### 1.2.3. Re-Testing due to a design changes (Common for 19PF and Post19PF and later)<sup>Δ3</sup>

If all of the following ① to ③ are satisfy at an engineering change, penetration testing does not have to be implemented since it could be judged that vulnerability will not occur. <sup>Δ2</sup>

① Penetration testing was occurred on an ECU of a previous version(\*1) before the relevant engineering change.

(\*1) An ECU whose node name and supplier are the same may be considered an ECU of the previous version.

② No entry point is to be added.

③ No cybersecurity related change is to be made on hardware and software controlling entry points. Provide, however, that the following examples do not meet ③ since they fall under a cybersecurity related change.

1. Change of a microcontroller controlling entry points (Provided, however, that change of a memory capacity of the microcontroller and deletion of a peripheral embedded in the microcontroller are changes that are not related to cybersecurity.)
2. Additional of an interface using a communication standard which has not been implemented

ECU	Test specification of Penetration Testing for ECU		8/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

before the engineering change to a microcontroller controlling entry points (e.g. addition of Ethernet or USB which will not be an entry point.)

3. Replacement of OS, BSW or cybersecurity related software module (SELinux, TOMOYO Linux, etc.) for a microcontroller controlling entry points



ECU	Test specification of Penetration Testing for ECU	9/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

### 1.3. Related Documents

Table3. List of Related Documents issued by TMC<sup>Δ2</sup>

Specification No.	Name
SEC-24PF-VCL- RIC-INST-DOC <sup>Δ4</sup>	Post19 電子 PF サイバーセキュリティリスク指標定義書(未発行) Post19ePF Cyber Security Risk Criteria Definitions(Unissued) <sup>Δ4</sup>
SEC-ePF-VUL- ECU-REQ-SPEC	ECU 脆弱性対策要求仕様書 Requirements specification of vulnerability countermeasure for ECU
SEC-ePF-VUL- ECU-TET-SPEC	ECU 脆弱性対策評価仕様書 Test specification of vulnerability countermeasure for ECU
SEC-ePF-VUL- CMN-REQ-SPEC	共通脆弱性対策要求仕様書 Requirements Specification of Common Vulnerability Countermeasure
SEC-ePF-TRM- GUD-PROC	制御電子 PF サイバーセキュリティ及びプライバシー用語定義書 Terms and Definitions related to Cybersecurity and Privacy in E/E Architecture

Table4. List of Related Official Documents

Abbreviation in this document	Name/external link
SP 800-115 <sup>Δ2</sup>	National Institute of Standards and Technology (NIST) , U.S. Department of Commerce, “Technical Guide to Information Security Testing and Assessment,” (Sep. 2008), <a href="https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf">https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf</a>
NHTSA-BP	National Highway Traffic Safety Administration (NHTSA) , U.S. Department of Transportation, “Cybersecurity Best Practices for Modern Vehicles,” (Oct. 2016), <a href="https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf">https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf</a>
ISO18045 <sup>Δ2</sup>	ISO/IEC 18045:2008, “Information technology — Security techniques — Methodology for IT security evaluation,” (Aug. 2008)
PIP Act <sup>Δ2</sup>	Act on the Protection of Personal Information (Act No. 57 of 2003) <a href="http://www.japaneselawtranslation.go.jp/law/detail/?id=2781&amp;vm=04&amp;re=01&amp;new=1">http://www.japaneselawtranslation.go.jp/law/detail/?id=2781&amp;vm=04&amp;re=01&amp;new=1</a>
ISO/SAE 21434 <sup>Δ2Δ3</sup>	ISO/SAE DIS 21434:2020, “Road Vehicles — Cybersecurity engineering,” (Feb. 2020)

ECU	Test specification of Penetration Testing for ECU		10/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

#### 1.4. Terms and Definitions

This section explains the terms which have to be defined in detail especially in this document. Note that the terms and definitions which are not defined in this section are according to “Terms and Definitions related to Cybersecurity and Privacy in E/E Architecture” <sup>Δ3</sup>

##### **Penetration Testing** <sup>Δ2</sup>

Security testing in which testers mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network.

Penetration testing is made up of 3 phases (planning phase, execution phase, and reporting phase). Implementation of penetration testing refers to implementation of all of the 3 phases.

ECU	Test specification of Penetration Testing for ECU	11/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

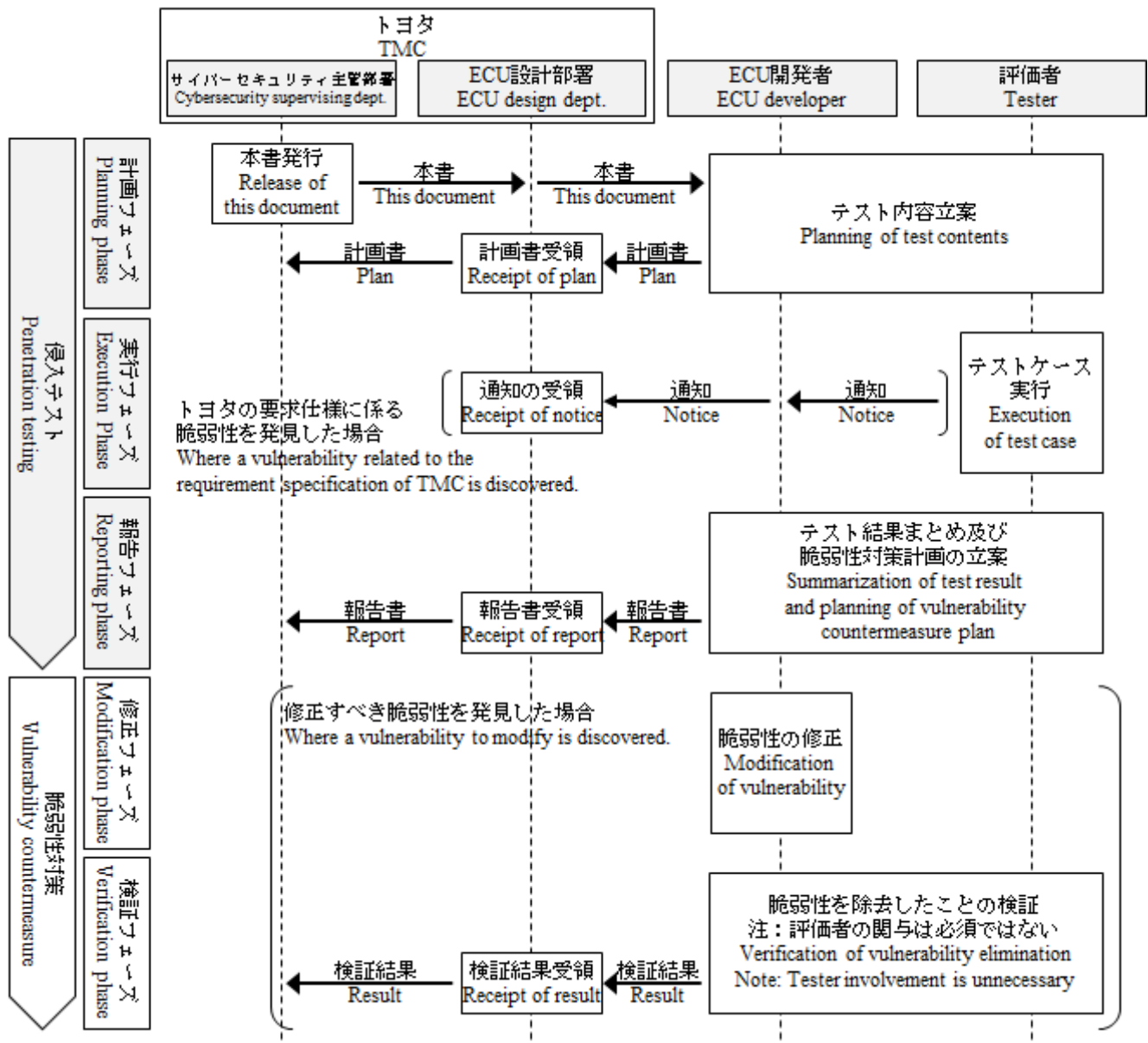


Fig.1. Process image of penetration testing and vulnerability countermeasure<sup>△3</sup>

### Vulnerability Countermeasure<sup>△3</sup>

Vulnerability countermeasure is made up of 2 phases (modification phase and verification phase). It is implemented after penetration testing. Implementation of vulnerability countermeasure means to implement both of the 2 phases. If any vulnerabilities to be modified is not discovered by penetration testing, a vulnerability countermeasure does not have to be implemented.

### Test case<sup>△2</sup>

ECU	Test specification of Penetration Testing for ECU	12/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

A set of tests to be implemented which have been identified and compiled in order to realize a scenario where a threat might be generated. See the image figure below.

A test case is designed at a granularity where implementation of 1 test case can clarify presence/absence of at least one vulnerability.

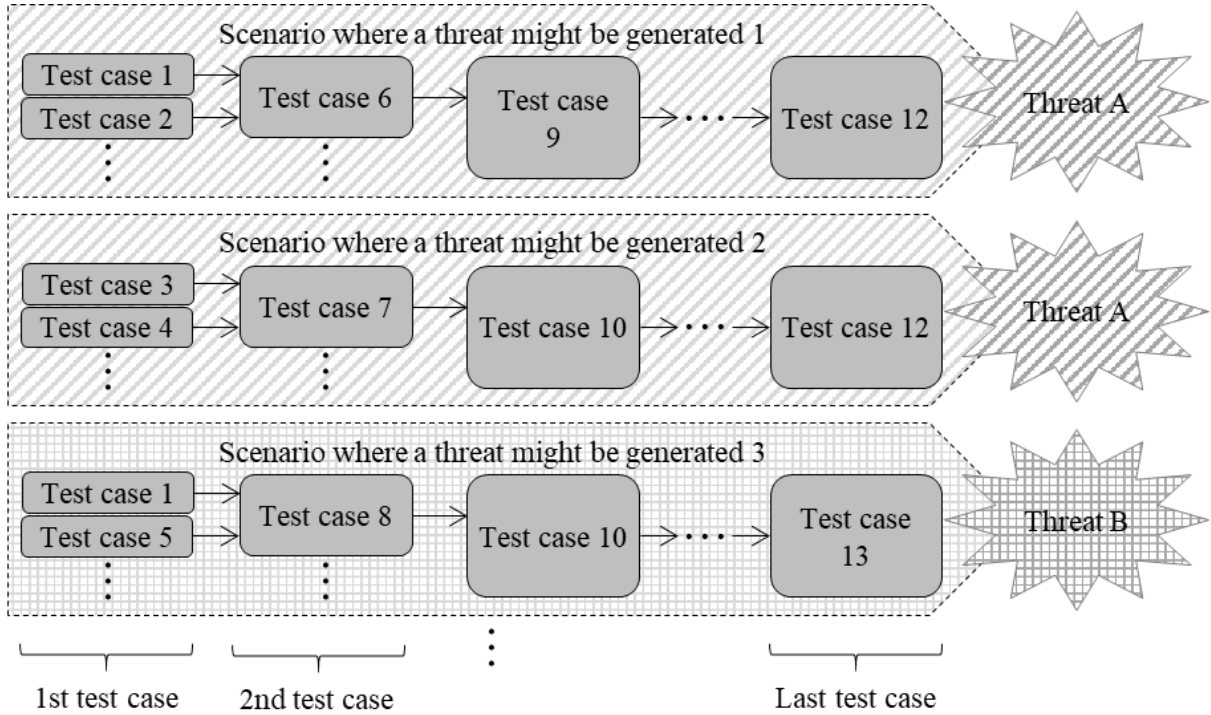


Fig.2. Image of Relationship between Threats and Test cases<sup>Δ2</sup>

ECU	Test specification of Penetration Testing for ECU	13/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## 1.5. Definitions of Persons Concerned<sup>Δ2</sup>

The list of persons concerned and their roles in penetration testing for ECU are indicated below.

Table 5 List of Persons Concerned and their Roles

Persons concerned	Role
TMC security supervising dept. (46F4G)	<p>Develops security measures for electronics PF to secure cybersecurity of a road vehicle at TMC. Conducts the following activities.</p> <ul style="list-style-type: none"> <li>➤ Defines the allocation condition of this document</li> <li>➤ Releases this document</li> </ul>
TMC ECU design dept.	<p>Designs an ECU installing the security features for electronics PF at TMC. Conducts the following activities.</p> <ul style="list-style-type: none"> <li>➤ Allocates this document to an ECU</li> <li>➤ Stores the plan and the report as a part of development documents</li> </ul>
ECU developer	<p>Is a member of an ECU development team and implements penetration testing in cooperation with the tester. Conducts the following activities.</p> <ul style="list-style-type: none"> <li>➤ Implements the planning and reporting phases (Is not allowed to implement the execution phase)</li> <li>➤ Submits the plan and the report to TMC ECU design dept.</li> </ul>
Tester	<p>Implements penetration testing in cooperation with the ECU developer. Conducts the following activities.</p> <ul style="list-style-type: none"> <li>➤ Implements all of the planning, execution, and reporting phases</li> </ul>

ECU	Test specification of Penetration Testing for ECU		14/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

### 1.6. Preconditions<sup>Δ3</sup>

It is preconditions in this document that ECU developers and testers perform the items of table 6 properly.

Table 6. Preconditions

No.	Classification	Preconditions	Remarks
1	Tool	The tools which is used are managed according to the rule related to tool provided by the affiliated department.	ISO21434 subsection 5.4.7 Tool Management
2	Vulnerability	The discovered vulnerabilities are managed according to the rule related to vulnerability provided by the affiliated department.	ISO2143 subsection 4 7.6 Vulnerability Management
3	Evidence	The evidences are managed according to the rule related to information security management provided by the affiliated department.	ISO2143 subsection 4 5.4.8, 5.4.8 Information Security Management, ISO21434 subsection 10.5[WP-10-06] in Work Products

ECU	Test specification of Penetration Testing for ECU		15/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## 2. Requirements

### 2.1. Requirements for Penetration Testing

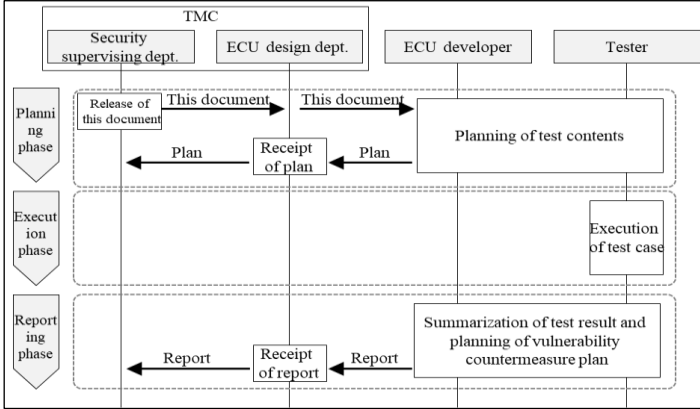
【要件番号 : VULEPN\_00001】<sup>Δ3</sup>

An ECU which satisfies the application conditions of penetration testing shall be implemented the penetration testing according to the requirements in Table 7.

Table 7. Requirements for Penetration Testing

No.	Classification	Requirements	Remarks
1	Implementation timing	<p>The implementation timing shall be decided based on the following conditions.</p> <ol style="list-style-type: none"> <li>1. (Required (1)) Penetration testing shall be completed before delivery of a CV production.<sup>Δ2</sup></li> <li>2. (Required (2)) A vulnerability discovered in penetration testing shall be able to be corrected before transfer to pilot production<sup>Δ2</sup>.</li> <li>3. (Recommended) An ECU configured based on a specification as close as possible to a mass-produced production shall be able to be tested.</li> </ol>	The assumed testing targets are an ECU for the system study and subsequent ECUs.

ECU	Test specification of Penetration Testing for ECU	16/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

2	Ways to proceed with <sup>Δ2</sup>	<p>The ECU developer and the tester shall implement the following 3 phases.</p> <ul style="list-style-type: none"> <li>➤ Planning phase: The ECU developer and the tester shall plan the test contents in accordance with this document and prepare a plan. Before the execution phase, they shall prepare for constructing a test environment.</li> <li>➤ Execution phase: The testers shall construct the test environment and implement test cases in accordance with the plan.</li> <li>➤ Reporting phase: The ECU developer and the tester shall summarize the test result, develop a vulnerability countermeasure plan, and prepare a report.</li> </ul>  <p>The flowchart illustrates the process of penetration testing across three phases: Planning, Execution, and Reporting. It involves four main entities: TMC (Security supervising dept. and ECU design dept.), ECU developer, and Tester. In the Planning phase, TMC releases the document, which is then passed to the ECU developer and Tester for planning. In the Execution phase, the Tester executes test cases. In the Reporting phase, the Tester reports results, which are then summarized and used to plan countermeasures by the ECU developer, who then reports back to TMC.</p>	<p>The planning and reporting phases correspond to the same terms in SP 800-11, respectively. The execution phase includes the detection and attack phases in SP 800-115.</p>
3	Target ECU <sup>Δ2</sup>	<p>An ECU implemented based on a specification equivalent to that of a mass-produced production shall be tested. If it is not possible to achieve equal implementation due to a compelling reason, the specification difference from that of the mass-produced production and the reason for difference shall be described in the evidence.</p>	<p>Security measures equal to those for a mass-produced production shall be enabled also for a privileged function (test access port, etc.) See the countermeasure requirements VULCMN_00400 and VULCMN_02500 <sup>Δ4</sup>in Requirements Specification of Common Vulnerability Countermeasure.</p>
4	Target	1. A function for which a threat identified in threat analysis	



ECU	Test specification of Penetration Testing for ECU	17/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

	functions	<p>shall be tested.<sup>Δ2</sup></p> <p>2. (In the case where penetration testing is to be implemented at the time of engineering change), testing may be limited to the functions to be affected by the engineering change as long as penetration testing was conducted for an ECU of a previous version (*1) before the engineering change.<sup>Δ2</sup></p> <p>(*1) An ECU whose node name and supplier are the same may be considered an ECU of the previous version.</p>	
5	Implementation organization <sup>Δ2</sup>	<p>1. The tester shall not be a member of the ECU development team.<sup>Δ2</sup></p> <p>2. The testers shall include at least one person who has adequate capability on cybersecurity testing (*2).<sup>Δ2</sup></p> <p>3. Testing may be outsourced to an external organization<sup>Δ1</sup></p> <p>(*2) The tester shall have work experience as cybersecurity professional for at least 5 years (university graduate requires 4-year experience (exempted from 1-year experience)) and have carried out similar testing in the past 3 years (*3).</p> <p>(*3) A similar test means penetration testing for an embedded system related to a technology used in the target ECU.<sup>Δ2</sup></p>	<p>This is because Section 6.6.2 of NHTSA-BP specifies as follows: “The automotive industry should consider extensive product cybersecurity testing to include using penetration tests. These tests should include stages that deploy qualified testers who have not been part of the development team, and who are highly incentivized to identify vulnerabilities.”</p> <p>The condition on the years of work experience is quoted from the CISSP certification condition.</p>
6	Information and equipment to be provided <sup>Δ2</sup>	<p>The ECU developer shall provide the information and equipment that falls under the following conditions to the testers. Note that if TMC’s permission is required for provision of the tester, permission shall be obtained before provision.</p> <p>1. Information/equipment needed for operating the target normally</p> <p>2. Information/equipment which can be obtained in the</p>	<p>· Appendix 2. Examples of Information and Equipment may be referred to.</p> <p>• A realistic period of time is estimated to be approx. a half year based on the calculation method of the</p>

ECU	Test specification of Penetration Testing for ECU	18/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

		<p>market after shipment of the production</p> <p>3. Information/equipment for which the tester proved the evidence that the information/equipment is effective for reducing testing time and the information/equipment can be obtained by an attacker within a realistic time period.</p>	<p>attacking ability.</p> <ul style="list-style-type: none"> <li>• The tester shall explain the usage to the ECU developer.</li> </ul>
7	Test contents	<p>Test contents shall be planned according to the following order in the planning phase.<sup>Δ2</sup></p> <ol style="list-style-type: none"> <li>1. Provision of vulnerability analysis result by the development team: The ECU developer shall provide the result of vulnerability analysis conducted in development of the target ECU to the tester.<sup>Δ2</sup></li> <li>2. Threat analysis: The tester shall conduct threat analysis from the attacker's viewpoint based on the information on the target ECU provided by the ECU developer.<sup>Δ2</sup></li> <li>3. Scenario study: The tester shall examine a scenario in which the threat identified in threat analysis in 2. could occur within the feasible range in terms of the tester's capability.<sup>Δ2</sup></li> <li>4. Preparation of test cases: The tester shall prepare test cases so that all the examined scenarios can be implemented.<sup>Δ2</sup></li> </ol>	<ul style="list-style-type: none"> <li>• Appendix 1. Example of Test Cases may be referred to for examining the necessity of outsourcing to an external organization.</li> <li>• The explanation in Appendix 3. Principle of Planning of Test Contents regarding the procedure may be referred to for planning test contents.<sup>Δ2</sup></li> </ul>
8	Prior agreement/permission <sup>Δ3</sup>	<p>If ECU developers execute behaviors which satisfy at least one of the following criteria, ECU developers shall ask the ECU design department in Toyota about it and then get the permission.</p> <ol style="list-style-type: none"> <li>1. Provide the information and tools which need the permission from Toyota to testers in advance.</li> <li>2. Irreversible operation or destruction of the tools owned by Toyota.</li> <li>3. Connect to network or server which ECU developer or tester don't possess<sup>Δ4</sup></li> </ol>	<p>As in the left, it is recommended that ECU developers and testers agree with handling of a provided tool and etc. in advance.</p>
9	Evidence <sup>Δ2</sup>	<ol style="list-style-type: none"> <li>1. A (documented) plan shall be prepared in the planning phase. The plan shall be submitted to the TMC ECU design dept. before start of the execution phase.<sup>Δ2</sup></li> <li>2. A report shall be prepared in the reporting phase. The report shall be submitted to the TMC ECU design dept. before delivery of a CV product.<sup>Δ2</sup></li> <li>3. At least, all items in Table 8 shall be described in the plan</li> </ol>	<p>This is because Section 6.6.2 of NHTSA-BP stipulates "All reports which result from these penetration tests should be maintained as part of the body of internal</p>

ECU	Test specification of Penetration Testing for ECU	19/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

		<p>and the report.<sup>Δ2Δ3</sup></p> <p>However, the testers shall create the contents of No.6 "test contents" and No.7 "discovered vulnerabilities" in items of Table 8. ECU developers shall not modify the contents without the permission of testers. <sup>Δ3</sup></p> <p>4. Care shall be taken so that the information to be described in the evidence does not correspond to "personal information" in PIP Act.</p>	<p>documentation associated with the cybersecurity approach. Documentation should identify the testers, their qualifications, and their recommendations. These penetration testing reports should also document the disposition of detected cybersecurity vulnerabilities. If vulnerability is fixed, the details of the fix need to be documented."</p>
10	Other	<p>1. Be ready to reply to an inquiry on the testing from TMC. The test contents and the operation log (e.g., terminal log) shall be stored for at least 6 months after submission of the report.</p> <p>2. In the event where a vulnerability related to the requirement specification of TMC is discovered, the TMC ECU design dept. shall be informed of the vulnerability as soon as possible after the discovery.</p> <p>3. The procedure for reproducing the discovered vulnerability shall be indicated at a granularity with which the ECU developer can reproduce.<sup>Δ2</sup></p> <p>4. Severity of the discovered vulnerability shall be assessed. CVSS v3 shall be used as severity assessment criteria. If other assessment criteria is to be used together with CVSS v3, the specification of the assessment criteria shall be indicated.<sup>Δ2</sup></p>	<p>Regarding (1), it is assumed that it will take at most half a year to determine the vulnerability modification policies.</p>

【要件番号 : VULEPN\_00002】 <sup>Δ3</sup>

The items in table 8 shall be described in the evidence when testers perform penetration testing for an ECU.

ECU	Test specification of Penetration Testing for ECU		20/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

Table 8 Items to Be Described in Evidence<sup>Δ2</sup>

No.	Item	Description contents	Necessity for description in Plan	Necessity for description in Report
1	Implementation timing	➤ The schedule of the planning, execution, and reporting phases	Required	Required
2	Target ECU	<ul style="list-style-type: none"> <li>➤ The information with which the hardware and the version No. of software of the target ECU can be identified (e.g., name, part No., software part No.)</li> <li>➤ Presence/absence of a difference between the target ECU and the mass-produced product and the list of the differences if there are any.</li> </ul>	Required	Required
3	Target function	➤ If the functions subject to testing at engineering change are to be limited, a list of these functions shall be described.	Required	Required
4	Implementation organization	<ul style="list-style-type: none"> <li>➤ The organization of the ECU developers and the testers (e.g., the number of persons, division of roles)</li> <li>➤ The person responsible and the contact person in ECU development</li> <li>➤ The organization the testers belong to and the reason for their selection</li> <li>➤ The information indicating expertise of the testers (e.g., work experience, capability they possess)</li> </ul>	Required	Required
5	Information/equipment to be provided	<ul style="list-style-type: none"> <li>➤ A list of the information provided from the ECU developer to the tester</li> <li>➤ A list of the equipment provided from the ECU developer to the tester</li> </ul>	Required	Required
6	Test contents	<ul style="list-style-type: none"> <li>➤ A list of the threats<sup>Δ3</sup></li> <li>➤ A list of the test cases <ul style="list-style-type: none"> <li>• Name of the test case</li> </ul> </li> </ul>	Required (※ 4)	Required (※ 4)

ECU	Test specification of Penetration Testing for ECU	21/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

No.	Item	Description contents	Necessity for description in Plan	Necessity for description in Report
		<ul style="list-style-type: none"> <li>➤ Details of the test case <ul style="list-style-type: none"> <li>• The threat you want to realize via the test case</li> <li>• The assets damaged by threats and its cybersecurity characteristics<sup>Δ3</sup></li> <li>• The target entrance of attack in the test case</li> <li>• The information of tools to be used for executing the test case (e.g Name, Version, Configuration to reproduce the test case) <sup>Δ3</sup></li> </ul> </li> <li>➤ Configuration of the test environment for excuting the test case</li> <li>➤ Presence/absence of a difference between the test environment and the actual environment (※ 5) <sup>Δ3</sup>, and then the list of the differences if there are any (※ 5) The actual environment indicates the state that the target ECU is assembled into a vehicle. <sup>Δ3</sup></li> </ul>		
		<ul style="list-style-type: none"> <li>➤ List of the test cases <ul style="list-style-type: none"> <li>• Whether or not each test case was executed in the execution phase shall be described.</li> <li>• Whether or not a vulnerability was discovered shall be described.</li> </ul> </li> <li>➤ If there is a test case which was not executed in the execution phase, the reason for not executing it shall be described.</li> </ul>	-	Required (※ 4)
7	Discovered vulnerabilities	<ul style="list-style-type: none"> <li>➤ List of the discovered vulnerabilities</li> <li>➤ Details of the discovered vulnerabilities <ul style="list-style-type: none"> <li>• The assets damaged by threats and the cybersecurity characteristics<sup>Δ3</sup></li> <li>• Severity of the vulnerability and its</li> </ul> </li> </ul>	-	Required (※ 4)

ECU	Test specification of Penetration Testing for ECU		22/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

No.	Item	Description contents	Necessity for description in Plan	Necessity for description in Report
		derivation process • Procedure for reproducing the vulnerability		
8	Vulnerability countermeasure plan	➤ Countermeasure plan against the discovered vulnerability • The method for modifying the vulnerability to be modified and its schedule • The reason that a vulnerability was judged not to be modified	-	Required (※ 4)

(※ 4) Testers shall create. ECU developers shall not change the contents without consent of testers.

ECU	Test specification of Penetration Testing for ECU		23/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## 2.2. Requirements of Vulnerability countermeasure<sup>Δ3</sup>

【要件番号 : VULEPN\_00003】

The Vulnerability countermeasure shall be implemented in accordance with the requirements of table 9 if the vulnerabilities which need to be fixed have discovered by penetration testing for an ECU.

Table 9. Requirements of vulnerability countermeasure

No.	Classification	Requirement	Remarks
1	Process	<p>ECU developers and testers shall implement the following 2 phases.</p> <ol style="list-style-type: none"> <li>1. Modification phase: ECU developers shall modify in accordance with the vulnerability countermeasure plan in the report.</li> <li>2. Verification phase: ECU developers and testers shall verify that the vulnerabilities are fixed. The involvement of testers is voluntary</li> </ol>	<ul style="list-style-type: none"> <li>• Verification phase may be substituted by reproducing an execution phase and a report phase.</li> <li>• Testing is not required as a means of verification because it is necessary to be shown that the vulnerabilities are fixed.</li> </ul>
2	Evidence	<ol style="list-style-type: none"> <li>1. ECU developers and testers shall create verification results in the verification phase. The verification results shall be submitted to ECU design department in Toyota by the delivery of prototype which the vulnerabilities are fixed.</li> <li>2. The evidence which vulnerabilities have been corrected shall be described in the verification results.</li> </ol>	—

ECU	Test specification of Penetration Testing for ECU		24/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## Appendix 1. Examples of Test Cases<sup>Δ2</sup>

As a reference material for studying the necessity for outsourcing to an external organization, examples of penetration test cases are presented.<sup>Δ2</sup>

The following table is an extraction of a part of the penetration test cases for an ECU planned by a security firm. This table includes test cases that do not have to be executed for some ECUs because a protocol is not implemented in those ECUs.<sup>Δ2</sup>

Table 8. Examples of Test Cases<sup>Δ1Δ2</sup>

Classification	No.	Name of test case
Remote Access & Persistence	1	Detect ECU backdoor via diagnostic function
	2	Non-volatile memory access via diagnostic function
	3	Non-volatile memory access of key via diagnostic function
	4	Detect and enable test mode via diagnostic function
	5	Detect and enable demo mode via diagnostic function
	6	Detect and enable test mode via reverse engineering
	7	Detect and enable demo mode via reverse engineering
	8	Firmware modification via OSS vulnerabilities
	9	Non-volatile memory key writing via diagnostic function
	10	Non-volatile memory writing via diagnostic function
	11	Firmware modification via diagnostic function
	12	Non-volatile memory burnout via diagnostic function
	13	Downgrade firmware via diagnostic function
	14	Detect ECU backdoor by reverse engineering
Execution	15	Command injection via diagnostic function
	16	Command injection via CAN messages
	17	Command injection via OSS vulnerabilities
	18	Security measure analysis under firmware image
	19	CAN replay
	20	Interference of intrusion detection via CAN message flooding
	21	DoS via bulk transmission of error messages
	22	Illegal diagnostic messages



ECU	Test specification of Penetration Testing for ECU		25/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

Classification	No.	Name of test case
Execution	23	System disruption via a command disguised as being from the driver
	24	Diagnostic messages flood
	25	Interference of intrusion detection via diagnostic message flooding
	26	Diagnostic privilege escalation
	27	SYN flooding
	28	Buffer overflow via CAN messages
	29	Buffer overflow via diagnostic messages
	30	Buffer overflow injection via OSS vulnerabilities
	31	Tigger high priority diagnostic messages outside of allowed conditions
	32	Using the ECU a mITM
	33	Using the ECU as a relay
	34	Boot bypass
Delivery	35	Security feature analysis of intrusion port (Setting of plug-and-play function)
	36	Lack of data intrusion port monitoring
	37	Sensitive information in query
	38	HTTP GET with sensitive information
	39	Proper network segmentation
	40	Extract firmware from removable storage medium
	41	Modify removable storage medium
Development	42	Keys should not be shared between devices
	43	Unauthorized activation of web services
	44	ARP poisoning
	45	DoS flooding
	46	Replay captured diagnostic messages
	47	Data exfiltration via low risk diagnostic function
	48	TCP hijacking
	49	DoS via TCPKill

ECU	Test specification of Penetration Testing for ECU	26/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

Classification	No.	Name of test case
Development	50	Memory information leakage via padding of communication frame
	51	CAN Message filtering
	52	Boot loader not validating the firmware properly
Discovery	53	Passive discovery of exposed network and services (communication capture)
	54	Scan via vulnerability scanner
	55	Network stress test
	56	Data fuzzing of telnet, TFTP, SSH, and diagnostic function
	57	Protocol fuzzing of telnet, TFTP, SSH, and diagnostic function
	58	Analysis of response performance via measurement of communication frame processing time
	59	Backup stores sensitive data
	60	Active discovery of exposed network and services (port scan)
	61	Outdated kernel
	62	Outdated libraries and applications
	63	Removable storage medium
	64	Hardware debugging port
	65	Common credential usage of SSH, TFTP, FTP, and telnet
	66	Analysis of access control error messages
	67	Factory reset uses default credentials
	68	Activate unexpected state via diagnostic function
	69	Activate unexpected State via communication
	70	Discover unexpected State via reverse engineering

ECU	Test specification of Penetration Testing for ECU		27/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

## Appendix 2. Examples of Information and Equipment<sup>A2</sup>

Examples of the information and the equipment used for implementing penetration testing for an ECU are indicated in Table 9.

Information and equipment related to an ECU under development cannot be obtained in the field yet. Therefore, the ECU developer provides the tester with the information and equipment in Table 9 so that the tester can mimic attacks in the field.

Note that this table is a reference material and information or equipment does not have to be provided if there is a compelling reason for not doing so. In addition, this table does not prevent information/equipment not listed in the table from being provided.

Table 9 Examples of Information and Equipment

No.	Description	Example of information	Example of equipment
1	Information/equipment needed for operating the target ECU normally	<ul style="list-style-type: none"> <li>➤ Pin assignment of a connector</li> <li>➤ Procedures for starting up and resetting the ECU</li> </ul>	<ul style="list-style-type: none"> <li>➤ Prototype ECU</li> <li>➤ Wiring harness</li> <li>➤ External part (e.g., antenna)</li> </ul>
2	Information/equipment available in the field after the product is shipped	<ul style="list-style-type: none"> <li>➤ Information described in the owner's manual</li> <li>➤ Information described in the service manual</li> <li>➤ Topology of the target ECU in the in-vehicle network</li> <li>➤ Input/output interfaces the target ECU has, their standards (e.g., CAN, USB, 100BASE-TX), and the set values (e.g., MAC address, IP address, VLAN ID)</li> <li>➤ The model No., manufacturer, data sheet, and manual of the semiconductor package installed in the target ECU (e.g., microcontroller, external memory for the microcontroller)</li> </ul> <p>Provided, however, that information whose obtainment is restricted such as the manual for Hardware Security Module (HSM) is excluded.</p>	<ul style="list-style-type: none"> <li>➤ Diagnostics tool</li> </ul>
3	Information/equipment for which the tester proved the evidence	[Only in the case where the tester proved the evidence that information/equipment can be obtained by an attacker within a realistic time]	[Only in the case where the tester proved the evidence that information/equipment can be

ECU	Test specification of Penetration Testing for ECU		28/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

	that the information/equipment is effective for reducing testing time and the information/equipment can be obtained by an attacker within a realistic time period	period] <ul style="list-style-type: none"> <li>➤ List of signals transmitted and received by the ECU on the in-vehicle network</li> <li>➤ Open source being used and its version</li> <li>➤ Encrypted reprogramming firmware</li> <li>➤ Execution code (binary)</li> </ul>	obtained by an attacker within a realistic time period] <ul style="list-style-type: none"> <li>➤ Reprogramming tool</li> </ul>
--	---	---	---

ECU	Test specification of Penetration Testing for ECU	29/30
Application: ECU of In-Vehicle Network	No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

### Appendix 3. Concept of Test Contents Planning<sup>A2</sup>

This reference material will explain the procedure for planning test contents.

This procedure for planning test contents has been prepared referring to a draft of ISO21434 which is being developed at the time of release of this document based on the policy that the procedure is associated with the information security development process. The image is indicated in the figure below and the critical points will be explained.

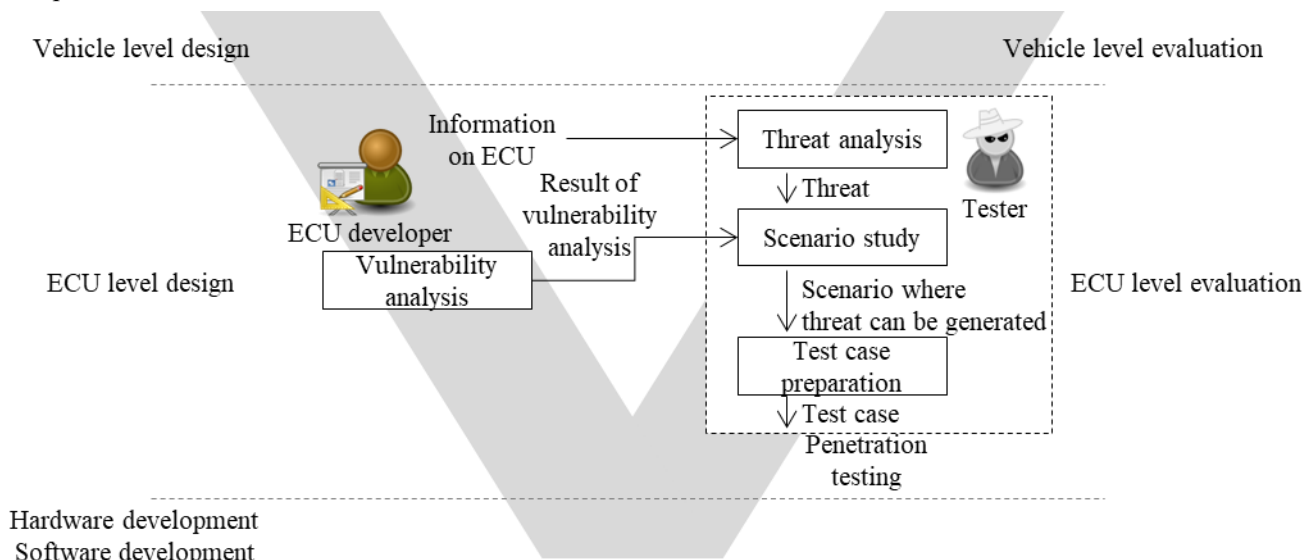


Fig. 3 Image of Concept of Test Contents Planning

#### 1. Provision of vulnerability analysis result by the development team

➤ Penetration testing is included in the “ECC level evaluation” process in the information security development process of a vehicle. Accordingly, this testing can be positioned on the V-shaped model in the relationship of being paired with “vulnerability analysis” in the “ECU level design” process. On the basis of this relationship, the result of vulnerability analysis by the development team shall be used for planning the test contents, which aims at the following.

- Of the vulnerabilities judged to be responded in vulnerability analysis, the vulnerabilities judged to be confirmed on the actual machine that a response has been made shall be confirmed in penetration testing.
- Preparation of a test case which there is not much need for a tester to implement shall be avoided. Note that test cases of which there is not much need for implementation include the following examples.

Example 1: A test case for a vulnerability known to the ECU developer

Example 2: A test case for a vulnerability accepted by the ECU developer because of its low risk

➤ Methodology of vulnerability analysis is not within the scope of this document. Yet, the result of either of the following example methodologies may be used as a vulnerability analysis result.

- Vulnerability check according to “Requirements Specification of Vulnerability Countermeasure of In-vehicle Information Security”
- Implementation of vulnerability analysis by an expert

ECU	Test specification of Penetration Testing for ECU		30/30
Application: ECU of In-Vehicle Network		No.	SEC-ePF-VUL-EPN-TST-SPEC-a00-04-a

- It is not anticipated that the development team conducts a new vulnerability analysis in order only to meet the requirements of this document.

## 2. Threat analysis

- Penetration testing should include the result of analysis conducted from the attacker's viewpoint that is the independent standpoint that is not the ECU development team. This aims at discovering, with penetration testing, a threat the ECU development team failed to notice.
- This document does not specify the detailed procedure of threat analysis. It is preferable that the tester try to reduce their work amount using the experience in the previous penetration testing.

## 3. Scenario study

- This document does not specify the detailed procedure of scenario study.
- "Within the feasible range in terms of the tester's capability" because TMC security supervising dept. believe that the validity of the test contents in penetration testing is based on the tester's capability.
- The items to be described in the evidence in Table 7 do not include the result of scenario study, which is for the purpose of reducing the work amount of documentation of the scenario.

## 4. Preparation of test case

- This document does not specify the detailed procedure of preparation of a test case.
- This document stipulates that a (documented) plan be prepared before the execution phase so that the tester does not fail to develop a plan. Developing a plan aims at the following.
  - Prepare a test case intensively for a critical portion of the ECU and prioritize the test cases in order to conduct effective testing in the limited time.
  - Store the evidence of penetration testing as a part of the development documents. Therefore, on top of a test case where a vulnerability was discovered, a test case which was implemented but in which no vulnerability was discovered shall also be recorded in the evidence.
- Compared to a tester, it is generally assumed that a person concerned other than the tester has a lower cybersecurity related capability. So, it is difficult to confirm that the test case prepared by a tester is sufficient. On the other hand, it would be easy for an ECU developer familiar with the ECU features to confirm that the target entrances of attack have been fully identified. Accordingly, it is recommended that the ECU developer should confirm that there is no shortage in test cases by interviewing the tester about the background of preparation of test cases.