| 関係各部署　御中<br>**To departments concerned** | Confidentiality classification | PROTECTED<br>関係者外秘 | 原紙保管<br>Storage of original | M/Y　/ |
|---|---|---|---|---|
| | | | コピー保管<br>Storage of copy | M/Y　/ |

| **ECU 脆弱性対策要求仕様書**<br>**Requirements Specification of Vulnerability Countermeasure for ECU** | 制御電子プラットフォーム開発部<br>制御ネットワーク・アーキ開発室　4G<br>E/E Architecture Development Div.<br>System network & architecture development dept 4G. | | | |
|---|---|---|---|---|
| | No. SEC-ePF-VUL-ECU-REQ-SPEC-a00-07-a | | | |
| | 承認 Approved<br>平林 | 調査 Checked<br>松井 | 作成 Created<br>玉樹 | 2022/12/22 |

| | |
|---|---|
| **適用先**<br>**Target** | サイバーセキュリティ管理策を織り込む ECU<br>ECUs that cybersecurity controls are incorporated. |
| **特記**<br>**Special note** | 【展開規則 Distribution rule】<br>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。<br>Please distribute this document to affiliated companies, or departments (e.g., overseas business entities, car body manufacturers, or ECU suppliers) if necessary.<br><br>【問合せ先 Contact information】<br>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<br>セキュリティ仕様問合せ窓口<br>System Network & Architecture Development Dept. E/E Architecture Development Div. Contact for Security Inquiries<br>email: 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 | 全項目 | セキュリティレベルを目標 AP に変更<br>各要件の適用条件と適用レベルを、適用条件と目標 AP に変更 |
| ↑ | ↑ | ↑ | ↑ | 4 | 目標 AP の定義に変更 |
| ↑ | ↑ | ↑ | ↑ | 6 | 要件の実施者に関する記述を修正 |
| ↑ | ↑ | ↑ | ↑ | 6.1 | 位置の修正 |
| Δ2 | a00-01-b | 2021/05/20 | 46F<br>石川<br>菅野 | 全項目 | 英訳の追加 |
| Δ3 | a00-02-a | 2021/09/16 | 46F 玉樹 | 6.2.1<br>6.2.2<br>6.3.1 | 脆弱性分析要件の詳細化 |
| ↑ | ↑ | ↑ | ↑ | 6.2.3 | 対象 ECU 以外へのセキュリティ要求の定義（VULERQ_02003）の要件は削除 |
| ↑ | ↑ | ↑ | ↑ | 1.3<br>1.4<br>1.5 | CC の略語の誤記修正<br>CC,CEM の略語を追加<br>CC の用語を修正、CEM の用語を追加 |
| ↑ | ↑ | ↑ | ↑ | 4 | 目標 AP の定義を変更 |
| Δ4 | a00-03-a | 2021/9/30 | 46F 安江 | 5.3.2 | 要件(VULERQ_01006)を追加（既製品へのセキュリティガイド対応） |
| Δ5 | a00-04-a | 2021/10/20 | 46F 玉樹 | 5.2.2 | (別紙 1) 既製品の脆弱性分析ガイドを追加 |
| ↑ | ↑ | ↑ | ↑ | 6.3.1 | (別紙 2) 設計/実装の脆弱性分析ガイドを追加 |
| Δ6 | a00-05-a | 2021/10/25 | 46F 早川 | 5.3.3 | トヨタで過去に報告・対処された脆弱性の確認対象の修正 |
| ↑ | ↑ | ↑ | ↑ | 1.3<br>1.4 | 適用範囲、要件の記載の章構成変更と内容明確化 |
| ↑ | ↑ | 2021/10/27 | 46F 安江 | 1.5 | 関連文書を更新 |
| ↑ | ↑ | 2021/11/01 | ↑ | 1.6<br>1.7 | SEC-ePF-TRM-GUD-PROC-***-**-*に記載されている略語、用語の削除 |
| ↑ | ↑ | 2021/11/05 | 46F 玉樹 | 1.2 | 図 1 を削除 |
| ↑ | ↑ | ↑ | ↑ | 全項目 | エビデンス要求を削除 |
| Δ7 | a00-05-b | 2022/3/24 | 46F 石川 | 1.4<br>4.2.2. | 参照している章または項の誤記を修正 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 4.4.1.<br>5 | |
| Δ8 | a00-06-a | 2022/3/31 | 46F **玉樹** | 5.3.1 | アーキテクチャ設計に対する脆弱性分析に、実施者の要件を追加 |
| ↑ | ↑ | ↑ | ↑ | 5.3.2 | ECU 脆弱性テスト観点を利用した脆弱性分析の実施(VULERQ_02005)の要件を削除 |
| Δ9 | a00-07-a | 2022/11/10 | 46F **玉樹** | 4.3.1 | 既製品に対するセキュリティ評価項目の定義の要件(VULERQ_01003)を削除 |
| ↑ | ↑ | ↑ | ↑ | 全項目 | 参考要件を削除 |
| ↑ | ↑ | ↑ | ↑ | 2.2 | CIAD を CIA に変更 |
| ↑ | ↑ | ↑ | ↑ | 4.4 | SIRT 活動に対する引継ぎ事項の定義の要件(VULERQ_01004)を削除 |
| ↑ | ↑ | ↑ | ↑ | 4.2.1 | 既製品にハードウェアを追加 |
| ↑ | ↑ | 2022/12/22 | ↑ | 4.2.1 | 既製品に開発環境/ツールを追加 |

# 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するために、サプライヤが脆弱性分析／脆弱性対策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 Δ6

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（本書） | 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 | 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 Δ6

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 Δ6

脆弱性対策によってセキュリティリスクを許容可能なレベルまで低減するためには、目標とする Attack Potential(以下、目標 AP)に応じた脆弱性対策の適用が必要となる。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 3 章を参照）

## 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 | 文書名 |
|---|---|
| | リスク指標定義書(未発行) |
| SEC-ePF-VUL-ECU-TST-SPEC | ECU 脆弱性対策評価仕様書 |
| SEC-ePF-VUL-CMN-REQ-SPEC | 共通脆弱性対策要求仕様書 |
| SEC-ePF-TRM-GUD-PROC[Δ6] | 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<br>Road vehicles — Cybersecurity engineering<br>https://www.iso.org/standard/70918.html |
| ISO/IEC 15408 | ISO/IEC 15408<br>Evaluation criteria for IT Security<br>または、Common Criteria と呼ばれる [Δ3]<br>https://www.ipa.go.jp/security/jisec/about_cc.html |
| 調達ソフトウェア採用セキュリティガイド [Δ6] | 調達ソフトウェア採用セキュリティガイド Ver.1.0 文書番号:ST-CST-2<br>https://www.jaspar.jp/standard_documents/detail_disclosure/585 |
| ECU 脆弱性テスト要件書 [Δ6] | ECU 脆弱性テスト要件書 Ver.1.1<br>文書番号: ST-CST-1<br>https://www.jaspar.jp/standard_documents/detail_disclosure/494 |

## 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 Δ6

| 略語 | 解説 |
|---|---|
| CC Δ3 | Common Criteria |
| CEM Δ3 | Common Evaluation Methodology |
| CVE | Common Vulnerability and Exposures |
| EAL | Evaluation Assuarance Level |
| EDSA | Embedded Device Security Assurance |
| VAN | Vulnerability Analysis |

## 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 Δ6

| 用語 | 解説 |
|---|---|
| CC Δ3<br>（ISO/IEC 15408） | 情報技術セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格。 |
| CEM Δ3<br>（ISO/IEC 18045） | CC に基づいた評価が異なる制度や評価機関で行われた場合でも、その評価結果を均質にするための評価手法を定めた国際標準規格。 |
| CVE | 米国 MITRE 社の公開情報 DB 。個別製品中のプログラム上のセキュリティ脆弱性が一意に識別されている。<br>http://cve.mitre.org/cve/　参照 |
| 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。<br>・通信に関する堅牢性試験<br>・セキュリティ機能の実装評価<br>・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 |
| JVN iPedia | 国内外問わず日々公開される脆弱性対策情報を収集、蓄積することを目的とした脆弱性対策情報データベース(DB)。キーワードやベンダ名、製品名等により特定の脆弱性対策情報を効率的に検索できる。<br>http://jvndb.jvn.jp/　参照 |
| NVD | 米国の NIST(National Institute of Standards and Technology)が運営する脆弱性情報 DB。<br>ソフトウェアの脆弱性に関する情報が提供される。<br>https://nvd.nist.gov/　参照 |
| US-CERT | 米国国土安全保障省の公開情報 DB 。<br>ソフトウェアの脆弱性に関する情報が提供される。<br>http://www.kb.cert.org/vuls/　参照 |
| 既製品 | 仕様に従って新たに開発するものではなく、<br>製品として既に出来上がっているもの<br>例．QNX や AGL などの標準 OS、OpenSSL などの標準ライブラリ<br>（Open Sorce Software を含む ） |

# 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、ECU に脆弱性なく作りこむための要件を定義する。

## 2.1. 本書と各社のルール&プロセスの関係

サプライヤは、各社で整備したプロセス&ルールに従って、脆弱性分析／脆弱性対策を実施するものとする。そのため、本書には脆弱性分析／脆弱性対策の実施手段は定義せず、トヨタが分析結果の妥当性を確認するために必要な項目を要件として定義する。本書と各社のルール&プロセスの関係図を図 **2** に示す。

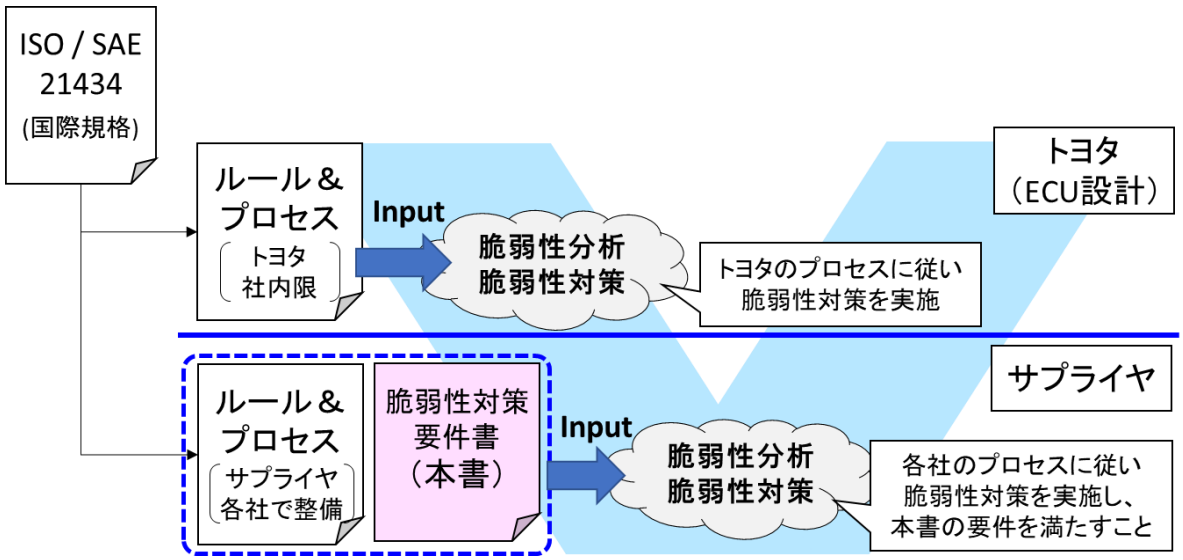


図 2　本書と各社のルール&プロセスの関係図

## 2.2. トヨタとサプライヤ間での CIA の締結 [Δ9]

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）[Δ9] を締結している。締結した CIA[Δ9] 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. 目標 AP の定義 Δ1Δ3

目標 AP は各 ECU に引当たるサイバーセキュリティ要求に付与され、「車両サイバーセキュリティコンセプト定義書」で確認することができる。Δ3

各 ECU、及びシステム設計者はサイバーセキュリティ要求の目標 AP を確認し、目標 AP ごとの脆弱性対策を確認すること。Δ3

表 6 目標 AP ごとの脆弱性対策 Δ3

| 目標 AP | 必要な脆弱性対策 | 脆弱性対策例 | （参考比較）<br>ISO15408 の基準 |
|---|---|---|---|
| 20 | 14~19＋<br>ハード解析による車外通信用の秘密鍵漏洩と改ざん防止 | 14~19＋耐タンパ（ハード解析に対応） | AVA-VAN.4 |
| 14~19 | 10~13＋<br>外部からの不正メッセージによる車内通信用の秘密鍵の漏洩、改ざん防止<br><br>最新の脆弱性をなくす（ゼロデイ攻撃対策） | 10~13＋セキュアメモリ<br>公知脆弱性 DB+文献調査(IT 汎用技術使用時) | AVA-VAN.3 |
| 10~13 | 一般的な脆弱性対策を実施する | セキュアコーディング、デバッグポート対策等 | AVA-VAN.2 |

# 4. 既製品の採用に関する脆弱性対策要件

ECU の構成部品／構成技術として、他社／他団体で開発済みのソフトウェア（既製品）を採用する場合は、既製品に対して脆弱性が報告されていないかを確認すること。もし、脆弱性が報告されている場合には脆弱性を塞ぐための対策を実施すること。

## 4.1. 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 | | VULERQ_01005 |
| 適用条件 Δ1Δ6 | 機能/部品 | - |
| | 目標 AP Δ1 | - |
| 要件 | | （欠番） |

## 4.2. 既製品のセキュリティ関連調査

### 4.2.1. 採用する既製品の特定

| 項目 | | 内容 |
|---|---|---|
| ID | | VULERQ_01001 |
| 適用条件 Δ1Δ6 | 機能/部品 | 全ての ECU |
| | 目標 APΔ1 | 全て |
| 要件 | | 号口品に含まれる既製品を特定し、セキュリティに関する情報を調査すること。<br><br><u>既製品に該当する条件</u><br>・ OSS（Open Source Software）<br>例. OS（Linux, AGL など）、ライブラリ（OpenSSL）など<br>・ 外部調達ソフトウェア<br>例. BSW、Hypervisor、OS（QNX）など<br>・ 外部調達ハードウェア Δ9<br>例. マイコン、SoC、HSM、メモリなど<br>・外部調達の開発環境/ツール Δ9<br>開発環境/ツールは、ソフトウェア実装に使用するものを対象とする。<br>例. コンパイラ、モデルベース開発のコード自動生成ツール<br>※製品のファームウェアに含まれる OSS／外部調達ソフトウェアも条件に該当<br><br><u>セキュリティに関する情報として調査する項目</u><br>・ ソフトウェア・ハードウェア Δ9 の種類、バージョン<br>・ セキュリティに関するエビデンス(※)の有無<br>※例：各種セキュリティ認証の証書（Common Criteria、EDSA 認証、など)、ソフトウェアベンダによる脆弱性分析／評価結果など。 |

| | |
|---|---|
| | **補足事項**<br>採用する製品が既製品に該当するか判断に迷う場合は、本書の発行部署と<br>別途協議を行い、対応を明確化すること。 |
| 理由 | 既製品に対して脆弱性が報告された際に、対策要否を速やかに確認するため。 |

### 4.2.2. 採用する既製品の脆弱性分析

| 項目 | | 内容 |
|---|---|---|
| ID | | VULERQ_01002 |
| 適用条件<br>Δ1Δ6 | 機能/部品 | 号口品に既製品を用いる ECU |
| | 目標 $AP^{\Delta 1}$ | 全て |
| 要件 | | ①号口品に用いる既製品に、公知の脆弱性がないかを脆弱性 DB を用いて確認すること。ただし、既製品にセキュリティに関するエビデンスが存在する場合は除く。<br>②既製品に脆弱性が確認された場合には、脆弱性をなくすための対応を実施すること。<br><br>**確認対象とする脆弱性 DB**<br>・ JVN iPedia（または NVD）<br>・ CVE<br>・ US-CERT<br><br>**脆弱性 DB が更新された場合**<br>脆弱性 DB には新しい脆弱性情報が日々追加されるため、脆弱性 DB は継続的な確認が必要である。継続的な監視は 4.4.1 項の要求に従い、実施すること。<br><br>**脆弱性がないことの確認方法** |

| | |
|---|---|
| | 脆弱性がないことの確認をする方法として、以下を利用することができる。<br>・(別紙 1) 既製品の脆弱性分析ガイド Δ5 |
| 理由 | 攻撃者に悪用される恐れがある公知の脆弱性が残存することを防ぐため。 |

## 4.3. 既製品のセキュリティ評価項目

### 4.3.1. （欠番）Δ9

| 項目 | | 内容 |
|---|---|---|
| ID | | VULERQ_01003 |
| 適用条件 Δ1Δ6 | 機能/部品 | - |
| | 目標 APΔ1 | - |
| 要件 | | （欠番） |
| 理由 | | - |

### 4.3.2. 既製品に対するセキュリティガイドの実施 Δ4

| 項目 | | 内容 |
|---|---|---|
| ID | | VULERQ_01006 |
| 適用条件 Δ6 | 機能/部品 | 号口品に既製品を用いる ECU |
| | 目標 AP | 全て |
| 要件 | | 既製品のソフトウェアの調達は、JASPAR「調達ソフトウェア採用セキュリティガイド」に従って採否を判断すること。 |
| 理由 | | 既製品に脆弱性が混入していないことが業界標準で担保されていることを確認するため |

## 4.4. （欠番）Δ9

### 4.4.1. （欠番）Δ9

| 項目 | | 内容 |
|---|---|---|
| ID | | VULERQ_01004 |
| 適用条件 Δ1Δ6 | 機能/部品 | - |
| | 目標 APΔ1 | - |
| 要件 | | （欠番） |
| 理由 | | - |

# 5. アーキテクチャ設計に対する脆弱性対策要件

ECU 開発におけるシステムアーキテクチャ設計、ハードウェアアーキテクチャ設計、および、ソフトウェアアーキテクチャ設計に関して[Δ1]、設計成果物に対する脆弱性分析を実施すること。分析により脆弱性が確認された場合には、その対策を実施すること。

**本章の脆弱性要件の位置づけ**

本章では、アーキテクチャ設計に対する脆弱性対策の要件として、脆弱性分析の Input に必要な設計情報（5.2 章）と、脆弱性分析の実施時に考慮する確認観点（5.3 章）を定義する。本章の脆弱性要件の位置づけを図 3 に示す。

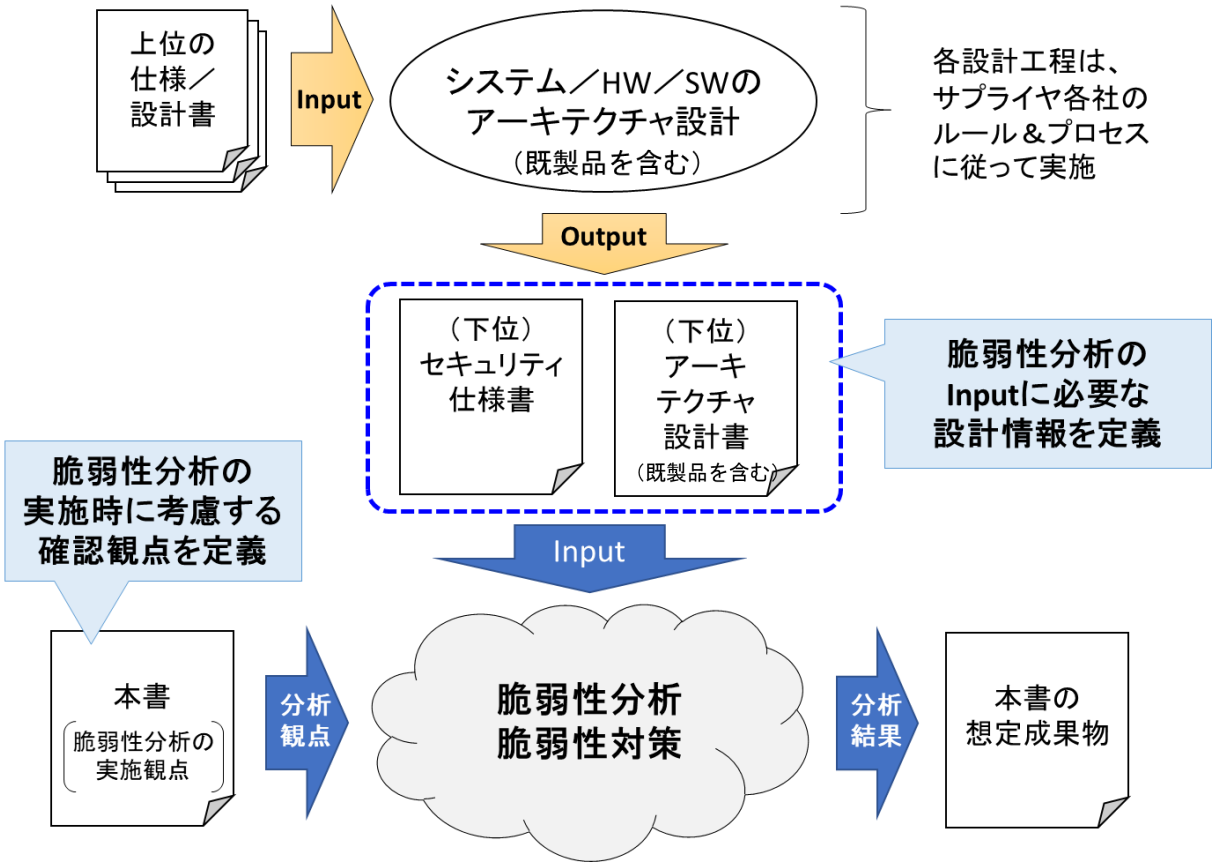


図 3　本章の脆弱性要件の位置づけ

## 5.1. 共通要件 Δ1

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 | | VULERQ_02007 |
| 適用条件 Δ1Δ6 | 機能/部品 | - |
| | 目標 AP Δ1 | - |
| 要件 | | （欠番） |

## 5.2. 脆弱性分析の Input 情報

### 5.2.1. セキュリティ機能の特定 Δ3

| 項目 | | 内容 |
|---|---|---|
| ID | | VULERQ_02001 |
| 適用条件 Δ1Δ6 | 機能/部品 | 全ての ECU |
| | 目標 AP Δ1 | 全て |
| 要件 | | 目標 AP が割り当てられたセキュリティ機能を特定すること。Δ3<br><br>セキュリティ機能の要求種別毎の例を下記に示す。Δ3<br>・セキュリティ主管部署が発行する仕様<br>　例：メッセージ認証、リプログラミングセキュリティ<br>・セキュリティ主管部署以外が発行する仕様<br>　例：独自リプロのセキュリティ<br>・脆弱性対策で適用するセキュリティ機能<br>　例：JTAG 認証、チップ間の通信の暗号化 |
| 理由 | | 脆弱性分析の Input 情報として利用するため。Δ3 |

### 5.2.2. インタフェースの特定

| 項目 | | 内容 |
|---|---|---|
| ID | | VULERQ_02002 |
| 適用条件 Δ1Δ6 | 機能/部品 | 全ての ECU |
| | 目標 AP Δ1 | 全て |
| 要件 | | ECU が有するインタフェースは攻撃の入口となりえるため、ECU が有するインタフェースと、そのインタフェースの用途やパラメータを識別すること。Δ3<br><br>**<u>インタフェースに関する情報として調査する項目</u>** Δ3<br>・ インタフェースの目的、用途<br>・ インタフェースの車両工場出荷後の使用有無<br>注　市場回収後にのみ使用するものであっても“有り”とすること<br>・ インタフェースのパラメータ<br>例　通信で用いるプロトコル、許可されるデータの範囲<br><br>**<u>注意事項</u>**<br>・ 製造時のみ有効で、製品出荷後は使用しないものも含めて、特定すること<br>・ 試作品でのみ有効で、号口品では使用しないものも含めて、特定すること<br><br>**<u>攻撃に悪用される恐れがあるインタフェースの例</u>**<br>・ 車両外の機器と接続する無線通信インタフェース<br>➢ 3G／LTE／5G Δ3、Wi-Fi、Bluetooth、ITS、ETC／DSRC、RF 通信 Δ3 など<br>・ 車両外の機器と接続する有線通信インタフェース<br>➢ CAN、Ethernet、USB、SD、CD、DVD、 |

| | |
|---|---|
| | Blu-ray、など<br>・ 車両の分解／改造を伴う物理解析に悪用されるインタフェース<br>➢ J-TAG、マイコン内部メモリ・外部メモリにアクセス可能な端子 Δ3 など |
| 理由 | 脆弱性分析の Input 情報として利用するため。 |

### 5.2.3. 対象 ECU 以外へのセキュリティ要求の定義 Δ3

| 項目 | | 内容 |
|---|---|---|
| ID | | VULERQ_02003 |
| 適用条件 Δ1Δ6 | 機能/部品 | - |
| | 目標 AP Δ1 | - |
| 要件 | | （欠番） |
| 理由 | | - |

## 5.3. 脆弱性分析の実施

### 5.3.1. アーキテクチャ設計に対する脆弱性分析の実施

| 項目 | | 内容 |
|---|---|---|
| ID | | VULERQ_02004 |
| 適用条件 Δ1Δ6 | 機能/部品 | 全ての ECU |
| | 目標 AP Δ1 | 全て |
| 要件 | | ①VULERQ_02001、VULERQ_02002 で特定した全てのセキュリティ機能とインタフェースの設計や実装に対して脆弱性分析すること。脆弱性分析の観点は、「アーキテクチャ設計に対する脆弱性の分析観点」を参考にすること。Δ3 脆弱性分析の実施者は、「実施者の要件」を満たすこと。Δ8<br>②脆弱性が確認された場合は、脆弱性に対策すること。対策しない場合には、対策不要である理由を示すこと。Δ3<br>・対策の例：CWE に記載のある緩和策(セキュリティ機能の追加配置など) |

・対策しない根拠の例：脆弱性を悪用するためのインタフェースが存在しない

<u>アーキテクチャ設計に対する脆弱性の分析観点</u> Δ3

脆弱性を分析するための観点として、下記を利用することができる。Δ3

・CC/CEM　附属書 B.2「脆弱性評定」

・CWE

CWE を用いた脆弱性分析方法を参考として下記に示す。Δ3

・(別紙 2) 設計/実装の脆弱性分析ガイド Δ5

<u>実施者の要件</u> Δ8

脆弱性分析には、目標 AP に応じたサイバーセキュリティの知識と経験を必要とするため、脆弱性分析の実施者は下記の要件を満たすこと。

| 目標 AP | 実施者の要件 |
|---|---|
| 20 | 新たな脆弱性や攻撃手法を考案する知識を有し、豊富な実務経験を有すること。具体的には、下記を全て満たすこと。<br>・ 5年以上のセキュリティ業務経験（※1）<br>・ 過去 3 年の脆弱性分析や侵入テストの実績（※2）<br><br>（※1）業務経験の年数は、サイバーセキュリティの国際資格である CISSP の認定条件から引用。<br>（※2）実績は、経済産業省が定める「情報セキュリティサー |

| | | | |
|---|---|---|---|
| | | | ビス基準」の脆弱性診断サービスの基準から引用。 |
| | | 14 | セキュリティの高度な知識として、有名な脆弱性や攻撃手法の知識を有すること。<br>（例：情報処理安全確保支援士相当、CWE Top25 を理解） |
| | | 10 | セキュリティの基礎的な知識を有すること。<br>（例：応用情報技術者試験相当、共通脆弱性対策要求仕様書を理解） |
| 理由 | ECU に混入する設計上の脆弱性を取り除くため。 | | |

### 5.3.2. ECU 脆弱性テスト観点を利用した脆弱性分析の実施 Δ8

| 項目 | | 内容 |
|---|---|---|
| ID | | VULERQ_02005 |
| 適用条件 Δ1Δ6 | 機能/部品 | - |
| | 目標 AP Δ1 | - |
| 要件 | | （欠番） |
| 理由 | | - |

### 5.3.3. 過去に対処した脆弱性の再発防止

| 項目 | | 内容 |
|---|---|---|
| ID | | VULERQ_02006 |
| 適用条件 Δ1Δ6 | 機能/部品 | 全ての ECU |
| | 目標 APΔ1 | 全て |
| 要件 | | トヨタで過去に報告・対処された内容と、同様の脆弱性が残っていないこと。<br><br>**トヨタで過去に報告・対処された脆弱性の確認方法**<br>トヨタでは、過去に報告・対処された脆弱性のうち、公的脆弱性 DB（JVN 等）に登録されていない内容を、トヨタ車載脆弱性 DBΔ6 として一覧化している。サプライヤ各社は ECU の開発を開始する際に、トヨタ車載脆弱性 DBΔ6 を確認し、過去に対処した脆弱性の再発防止を行うこと。なお、ECU の開発を開始した後に脆弱性が報告された場合は、車両 SIRT の仕組みに従って対処を行うこと。<br><br>トヨタ車載脆弱性 DBΔ6：<br>https://team-atsp.kitora.toyota.co.jp/sites/cybersecurity/SitePages/Sec_Home.aspx<br>(アクセス権限設定の制約上、社外関係者（サプライヤー様）のアクセス制限が有効になっております。社外関係者の方は TMC 設計部署から入手ください。) |
| 理由 | | 過去に対処した脆弱性の再発防止を徹底するため。 |

## Change History[Δ1]

| Mark | Version | Date | Revised by | Item | Description |
|---|---|---|---|---|---|
| | a00-00-a | 2020/06/23 | 46F Matsui | All items | First version issued. |
| Δ1 | a00-01-a | 2021/04/01 | 46F Ishikawa | All items | Changed security level to target AP. |
| ↑ | ↑ | ↑ | ↑ | 4 | Changed to the definition of target AP. |
| ↑ | ↑ | ↑ | ↑ | 6 | Modified a description about carrying on requirements. |
| ↑ | ↑ | ↑ | ↑ | 6.1 | Changed position. |
| | a00-01-b | 2021/05/20 | 46F Ishikawa Sugano | All items | Added English translation |
| Δ3 | a00-02-a | 2021/09/16 | 46F Tamaki | 6.2.1<br>6.2.2<br>6.3.1 | Updated detail of vulnerability analysis requirement |
| ↑ | ↑ | ↑ | ↑ | 6.2.3 | Deleted requirement VULERQ_02003 in “Definition of Security Requirements for Things except Target ECUs” |
| ↑ | ↑ | ↑ | ↑ | 1.3<br>1.4<br>1.5 | Changed a typo for abbreviation of CC<br>Add abbreviations for CC and CEM<br>Change term of CC, Add term of CEM |
| ↑ | ↑ | ↑ | ↑ | 4 | Changed Definition of Target AP. |
| Δ4 | a00-03-a | 2021/09/30 | 46F Yasue | 5.3.2 | Add requirement VULERQ_01006 (execution of security guideline to off-the-shelf component) |
| Δ5 | a00-04-a | 2021/10/20 | 46F Tamaki | 5.2.2 | Add (Annex 1) Off-The-Shelf Vulnerability Analysis Guide |
| ↑ | ↑ | ↑ | ↑ | 6.3.1 | Add (Annex 2) Guide of Vulnerability Analysis for Design / Implementation |
| Δ6 | a00-05-a | 2021/10/ | 46F Hayakawa | 5.3.3 | Modified the confirmation target of the vulnerabilities reported, handled in the past at Toyota |

| | | | | | |
|---|---|---|---|---|---|
| ↑ | ↑ | ↑ | ↑ | 1.3<br>1.4 | Change the chapter structure and clarify the content of scope and description of requirements |
| ↑ | ↑ | 2021/10/27 | 46F<br>Yasue | 1.5 | Update related documents |
| ↑ | ↑ | 2021/11/01 | ↑ | 1.6<br>1.7 | Delete abbreviations and terms which are described in SEC-ePF-TRM-GUD-PROC-***-**-* |
| ↑ | ↑ | 2021/11/5 | 46F<br>Tamaki | 1.2 | Delete Fig 1. |
| ↑ | ↑ | ↑ | ↑ | All items | Delete evidence requirements. |
| Δ7 | a00-05-b | 2022/3/24 | 46F<br>Ishikawa | 1.4<br>4.2.2<br>4.4.1<br>5 | Correct editorial errors in the referenced subsection or chapter |
| Δ8 | a00-06-a | 2022/3/31 | 46F<br>Tamaki | 5.3.1 | Add requirements related to a person who executes Vulnerability Analysis for Architectural Designs |
| ↑ | ↑ | ↑ | ↑ | 5.3.2 | Delete the requirement “Execution of Vulnerability Analysis using ECU Vulnerability Test Perspectives (VULERQ_02005)” |
| Δ9 | a00-07-a | 2022/11/10 | 46F<br>Tamaki | 4.3.1 | Delete the requirement “Definition of Security Evaluation Items of Off-the-Shelf component(VULERQ_01003)” |
| ↑ | ↑ | ↑ | ↑ | All items | Delete the “Reference requirements” |
| ↑ | ↑ | ↑ | ↑ | 2.2 | Change terms from CIAD to CIA |
| ↑ | ↑ | ↑ | ↑ | 4.4 | Delete the requirement “Definition of Transition Items to SIRT Activities (VULERQ_01004)” |
| ↑ | ↑ | ↑ | ↑ | 4.2.1 | Add the hardware to off-the-shelf components |
| ↑ | ↑ | 2022/12/22 | ↑ | 4.2.1 | Add development environment / tool to off-the-shelf components |

# Table of Contents

# 1. Introduction

## 1.1. Purpose of this Document

This document defines the requirements on Vulnerability analysis / Vulnerability countermeasures for ECU done by supplier to fulfill the requirements of ISO / SAE21434 and reduce ECU vulnerability to the appropriate level.

## 1.2. Position of this Document[Δ6]

Similar to this document, Table1 shows a list of countermeasure requirements / evaluation requirements and the position of each document in order to develop an ECU without vulnerabilities.

Table1 List of specifications to reduce vulnerabilities

| Title | Position |
|---|---|
| Requirements specification of vulnerability countermeasure for ECU (this document) | In each architecture design process in ECU development, Define requirements for vulnerability analysis and vulnerability countermeasures. |
| Test specification of vulnerability countermeasure for ECU | 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[Δ6]

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 security functions. (Hereinafter an ECU that is instructed to develop one of the security specifications are referred to as "security target ECU")

## 1.4. Description of Requirements[Δ6]

In order to reduce security risks to acceptable levels by vulnerability countermeasures, it is necessary to apply vulnerability countermeasures according to the Target Attack Potential (subsequently described as “Target AP”). 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. (See Chapter 3 for the definition of the Target AP)

## 1.5. Related Documents

The documents related to this document are as follows.

Table2 List of Related Documents

| Specification Number | Title |
|---|---|
| | Post19ePF Cyber Security Risk Criteria Definitions (Unissued) |
| SEC-ePF-VUL-ECU-TST-SPEC | Test specification of vulnerability countermeasure for ECU |
| SEC-ePF-VUL-CMN-REQ-SPEC | Requirements Specification of Common Vulnerability Countermeasure |
| SEC-ePF-TRM-GUD-PROC[Δ6] | Terms and Definitions related to Vehicle Cybersecurity and Privacy |

Table3 List of Public Related Documents

| Abbreviation in this document | Title and External links |
|---|---|
| ISO/SAE 21434 | ISO/SAE DIS 21434<br>Road vehicles — Cybersecurity engineering<br>https://www.iso.org/standard/70918.html |
| ISO/IEC 15408 | ISO/IEC 15408<br>Evaluation criteria for IT Security<br>or<br>Common Criteria<br>https://www.ipa.go.jp/security/jisec/about_cc.html |
| Third-party software, Open source software Procurement Security Guide[Δ6] | Third-party software, Open source software Procurement Security Guide Ver.1.0<br>Document No. : ST-CST-2<br>https://www.jaspar.jp/standard_documents/detail_disclosure/584 |
| ECU Vulnerability Test | ECU Vulnerability Test Requirements Ver.1.1 |

| | |
|---|---|
| Requirements[Δ6] | Document No. : ST-CST-1<br>https://www.jaspar.jp/standard_documents/detail_disclosure/495 |

## 1.6. Abbreviations and Definitions

The abbreviations to be used in this document are explained in Table4.

Table4　List of Abbreviations[Δ6]

| Abbreviation | Explanation |
|---|---|
| CC[Δ3] | Common Criteria |
| CEM[Δ3] | Common Evaluation Methodology |
| CVE | Common Vulnerability and Exposures |
| EAL | Evaluation Assurance Level |
| EDSA | Embedded Device Security Assurance |
| VAN | Vulnerability Analysis |

## 1.7. Terms and Definitions

The terms used in this document are explained in Table5.

Table5　List of Terms[Δ6]

| Term | Explanation |
|---|---|
| CC[Δ3]<br>（ISO/IEC 15408） | International standard to evaluate if designs and implementations of products or systems is appropriate with security aspects. |
| CEM[Δ3]<br>(ISO/IEC 18045) | International standard that establishes evaluation methods to homogenize the evaluation results, even if evaluations based on CC are conducted at different systems or evaluation organizations. |
| CVE | A public information DB operated by the MITRE Corporation (a US company). Security vulnerabilities of the programs of individual products are uniquely identified.<br>See http://cve.mitre.org/cve/ |
| EDSA | A Certification scheme for security assurance of control devices. Evaluation items are as below.<br>・Testing the robustness of communication<br>・Evaluating the implementations of security functions<br>・Evaluating the Security at each phase in software developments. |

| Term | Explanation |
|---|---|
| JVN iPedia | A vulnerability countermeasure information database (DB) aiming at collection and accumulation of the vulnerability countermeasure information disclosed on a daily basis domestically and internationally. A specific type of vulnerability countermeasure information can be searched efficiently by specifying a keyword, vendor name, and product name, etc.<br>See http://jvndb.jvn.jp/ |
| NVD | A vulnerability information DB operated by the National Institute of Standards and Technology (NIST) of the United States.<br>This DB provides information related to software vulnerability<br>See https://nvd.nist.gov/ |
| US-CERT | A public information DB operated by the United States Department of Homeland Security.<br>This DB provides information related to software vulnerability.<br>See http://www.kb.cert.org/vuls/ |
| off-the-shelf component | A component that has been already completed, it's not necessary to develop newly in accordance with the specifications.<br>Examples: standard OS such as QNX, AGL, standard library such as OpenSSL(including Open Source Software) |

# 2. The precondition of this document

In this document, it's precondition that ISO/SAE 21434 compliant processes & rules of suppliers are prepared. Based on this, this document defines the requirements for developing the cybersecurity control required by Toyota for the ECU without vulnerabilities.

## 2.1. The relation between this document and rules & processes of each supplier

Vulnerability analysis / vulnerability countermeasures shall be executed in accordance with rules and processes prepared by each supplier. Therefore, this document doesn't define the means of implementing vulnerability analysis / vulnerability countermeasures, but defines the items necessary for Toyota to confirm the validity of the analysis results as requirements. The relation between this document and rules & processes of each supplier is shown in Fig. 2.

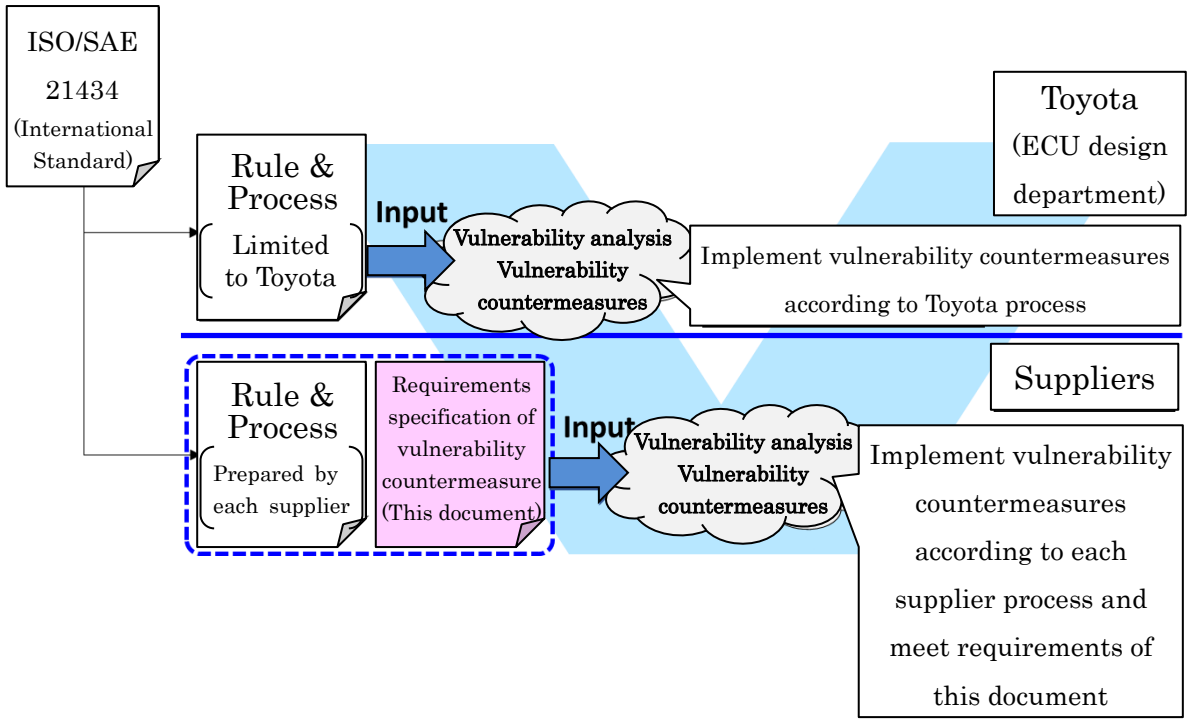


Fig. 2 Figure of the relation between rules & processes of each supplier

## 2.2. Conclusion CIA between Toyota and suppliers[Δ9]

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. [Δ6]

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)[Δ9] will be concluded. The CIA[Δ9] concluded is attached to the RDDP in addition to the security-related specifications.

## 3. Definition of Target AP[Δ1Δ3]

Target AP is given to the cybersecurity request that is assigned to each ECU, and can be confirmed in the "Vehicle Cyber Security Concept Definitions".[Δ3] Each ECU and system designer confirms the Target AP of cyber security requirements and vulnerability countermeasures for each Target AP. [Δ3]

**Table 6 Vulnerability Countermeasures for each Target AP[Δ3]**

| Target AP | Required vulnerabilities measure | Example of vulnerability measure | (Comparison for reference) ISO15408 standard |
|---|---|---|---|
| 20 | 14~19+<br>Prevention of leakage and tampering of a private key for vehicle external communication by hardware analysis | 14~19 + anti-tampering (counteracting hardware analysis) | AVA-VAN.4 |
| 14~19 | 10~13+<br>Prevention of leakage of a private key for in-vehicle communication and tampering by an unauthorized message from the outside<br><br>Elimination of the latest vulnerabilities (a measure against 0-day attack) | 10~13 + secure memory<br>Survey on known vulnerabilities DB + literatures (when using a general-purpose IT technology) | AVA-VAN.3 |
| 10~13 | Implementation of general vulnerability measures | Secure coding, measures against debug port, etc. | AVA-VAN.2 |

# 4. Requirements on Vulnerability Countermeasures in adoption of Off-the-Shelf Components

If adopting a software (off-the-shelf component) that has been already completed by other companies / other organizations as a component / technology for ECU, suppliers shall check whether vulnerability is reported in an individual component / technology. If vulnerabilities are found, suppliers shall execute countermeasures to mitigate the vulnerabilities.

## 4.1. Common Requirements

This section provides common requirements for the requirements described in this chapter.

**Requirements for evidence creation deadlines**

| Item | | Description |
|---|---|---|
| ID | | VULERQ_01005 |
| Application conditons[Δ1Δ6] | Functions/Parts | - |
| | Target AP[Δ1] | - |
| Requirements | | Deleted. |

## 4.2. Security Related Check of Off-the-Shelf Components

### 4.2.1. Identification of Off-the-Shelf Components to be adopted

| Item | | Description |
|---|---|---|
| ID | | VULERQ_01001 |
| Application Conditions[Δ1Δ6] | Functions/Parts | All ECUs |
| | Target AP[Δ1] | All |
| Requirements | | Suppliers shall identify off-the-self components to be adopted and check for information related to security.<br><br><u>Conditions That Apply to Off-the shelf components</u><br>・ OSS（Open Source Software）<br>e.g. OS（Linux, AGL etc.）、Library（OpenSSL）etc.<br>・ External procurement software<br>e.g. BSW、Hypervisor、OS（QNX）etc.<br>・ External procurement hardware[Δ9]<br>e.g. Microcontroller、SoC、HSM、Memory etc.<br>・ External procurement development environment / tools[Δ9]<br>The development environment / tools to be applied are those used in software implementations.<br>e.g. Compiler, automatic code generation tool for model-based development<br>※OSS / External procurement software embedded in firmware of product is also applied to this condition.<br><br><u>Items for Checking Information Related to Security</u><br>・ Type of the software and hardware[Δ9], version<br>・ Whether there is evidence(※) related to security<br>※ e.g. : Certificate of security certification(Common Criteria, EDSA Certification, etc.), Vulnerability analysis / evaluation result by software vendor etc.<br><br><u>Supplement</u><br>If it is hard to judge whether the component to be adopted is off-the-shelf component, the department in charge of security (the department issuing the present specifications), the department in charge of design, and suppliers shall make discussion separately and clarify the |

| | |
|---|---|
| | measures. |
| Reasons | To check the necessity of countermeasures when vulnerabilities of off-the-shelf components are reported |

### 4.2.2. Vulnerability Analysis of Off-the-Shelf Components to be Adopted

| Item | | Description |
|---|---|---|
| ID | | VULERQ_01002 |
| Application Conditions[Δ1Δ6] | Functions/Parts | ECUs that uses off-the-shelf components for the production |
| | Target AP[Δ1] | All |
| Requirements | | ①Suppliers shall check whether public vulnerabilities described in the vulnerability DB is present in off-the-shelf components to be used for the production. However, except that there are security related evidences of off-the-shelf components.<br>②If vulnerabilities are found, execute countermeasures mitigate the vulnerabilities.<br><br>**Vulnerability DB to be Checked**<br>・ JVN iPedia（or NVD）<br>・ CVE<br>・ US-CERT<br><br>**In the Case of Update in Vulnerability DB**<br>It is necessary to check vulnerability DB continuously since the information in vulnerability DB is updated every day. Continuous monitoring shall be executed in accordance with the subsection 4.4.1.<br>**Methods to Check the Nonexistence of Vulnerabilities**<br>The following is available to check the nonexistence of vulnerabilities.<br>・(Annex 1) Off-The-Shelf Vulnerability Analysis Guide[Δ5] |
| Reasons | | To prevent remaining public vulnerabilities that can be exploited by attackers. |

## 4.3. Security Evaluation Items of Off-the-Shelf components

### 4.3.1. Deleted [Δ9]

| Item | | Description |
|---|---|---|
| ID | | VULERQ_01003 |
| Application Conditions[Δ1Δ6] | Functions/Parts | - |
| | Target AP[Δ1] | - |
| Requirements | | Deleted. |
| Reasons | | - |

### 4.3.2. Execution of Security Guideline to Off-the-Shelf Component[Δ4]

| Item | | Description |
|---|---|---|
| ID | | VULERQ_01006 |
| Application Conditions[Δ6] | Functions/Parts | ECUs that use off-the-shelf components for the production |
| | Target AP | All |
| Requirements | | Suppliers shall judge whether to use the procurement software in accordance with JASPAR “Third-party software, Open source software Procurement Security Guide”. |
| Reasons | | To check that vulnerabilities are not incorporated into off-the-shelf components by industry standard. |

## 4.4. **Deleted**[Δ9]

### 4.4.1. Deleted[Δ9]

| Item | | Description |
|---|---|---|
| ID | | VULERQ_01004 |
| Application Conditions[Δ1Δ6] | Functions/Parts | - |
| | Target AP[Δ1] | - |
| Requirements | | Deleted. |
| Reasons | | - |

# 5. Vulnerability Countermeasure Requirements of Architecture Designs

Execute vulnerability analysis for design outputs of system architectural designs, hardware architectural designs, and software architectural designs in ECU developments. Δ1
If vulnerabilities are found by vulnerability analysis, execute vulnerability countermeasures.

## Positioning of Vulnerability Countermeasures in this Chapter

This chapter defines design information to be needed for inputs of vulnerability analysis (chapter 5.2) and perspectives to be taken into consideration for executing vulnerability analysis (chapter 5.3) as requirements of vulnerability analysis for architectural designs. Positioning of vulnerability countermeasures in this chapter is shown in Fig. 3.

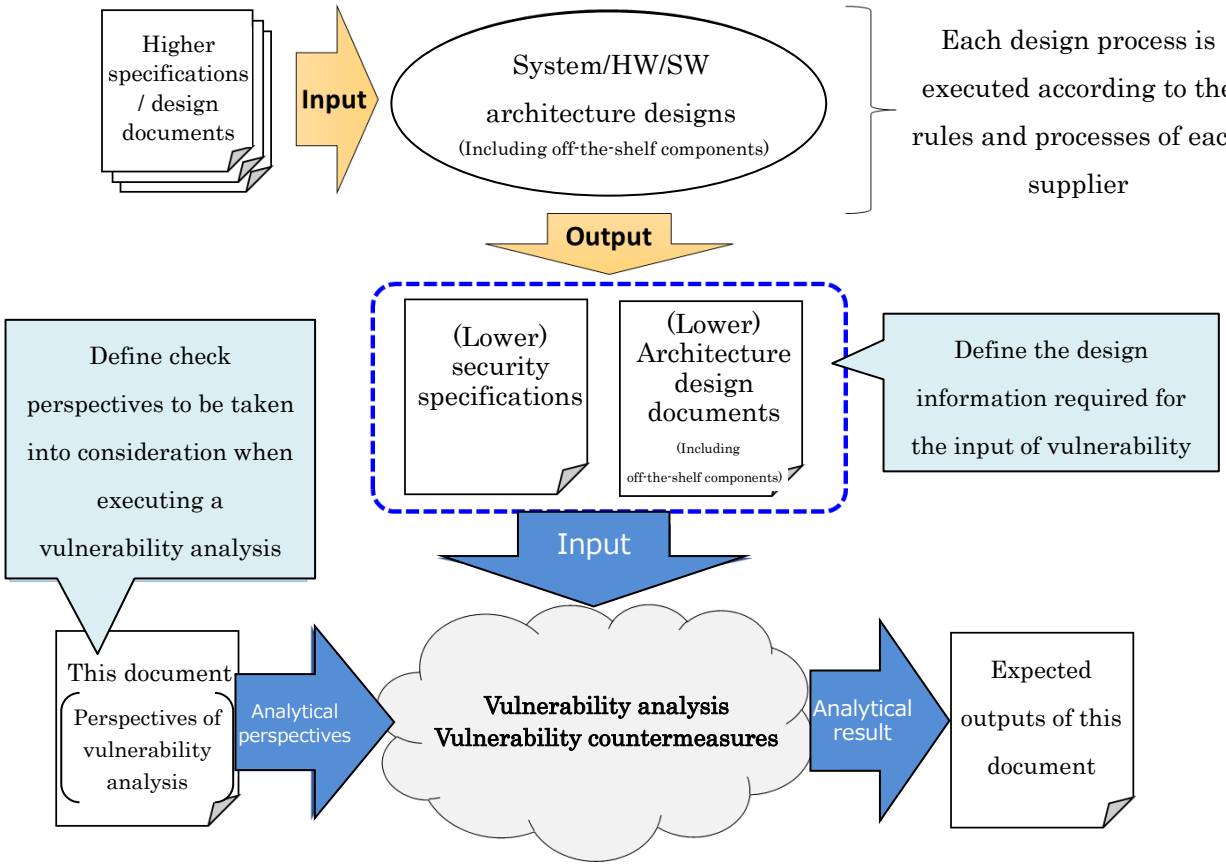


**Fig. 3** Positioning of Vulnerability Countermeasures in this Chapter

## 5.1. Common Requirements[Δ1]

This section defines common requirements for the requirements set out in this chapter.

**Requirements for evidence creation deadlines**

| Item | | Description |
|---|---|---|
| ID | | VULERQ_02007 |
| Application Conditions[Δ1Δ6] | Functions/Parts | - |
| | Target AP[Δ1] | - |
| Requirements | | Deleted. |

## 5.2. Input Information for Vulnerability Analysis

### 5.2.1. Identification of Security functions[Δ3]

| Item | | Description |
|---|---|---|
| ID | | VULERQ_02001 |
| Application Conditions[Δ1Δ6] | Functions/Parts | All ECUs |
| | Target AP[Δ1] | All |
| Requirements | | Suppliers shall identify security functions to which target AP is assigned. [Δ3]<br><br>Examples for each requirement kind of security functions are shown below. [Δ3]<br>- Security specifications issued by department in charge of cybersecurity<br>e.g. Message Authentication, Reprogramming Security<br>- Security specifications issued by other than the department in charge of cybersecurity<br>e.g. Security for proprietary-reprogramming<br>- Security functions applied as vulnerability countermeasure, etc.<br>e.g. JTAG authentication, encryption of communication between chips |
| Reasons | | To use as input information for vulnerability analysis. [Δ3] |

### 5.2.2. Identification of Interface

| Item | Description |
|---|---|

| | | |
|---|---|---|
| ID | | VULERQ_02002 |
| Application Conditions[Δ1Δ6] | Functions/Parts | All ECUs |
| | Target AP[Δ1] | All |
| Requirements | | Suppliers shall identify ECU's interfaces, usages and used parameters because ECU's interfaces could become attack entry point.[Δ3]<br><br>**Check Items as Interface Related Information**[Δ3]<br>・ Purposes and usage of interfaces<br>・ Whether interfaces are usable after shipment form vehicle assembly plants.<br>Note Regard interfaces as "existent", even if that interfaces are only used after recall from market.<br>・ Parameters of interfaces<br>e.g. protocols used on communications, ranges of data<br><br>**Notes**<br>・ Identify including interfaces that is usable only for production phase and nt usable after product shipment.<br>・ Identify including interfaces that is usable only for prototypes and not usable for productions.<br><br>**Examples of Interfaces that may be Exploitable**<br>・ Wireless communication interfaces that connect to devices which are outside the vehicles.<br>➢ 3G／LTE／5G[Δ3]、Wi-Fi、Bluetooth、ITS、ETC／DSRC、RF communication[Δ3]etc.<br>・ Wired communication interfaces that connect to devices which are outside the vehicles.<br>➢ CAN、Ethernet、USB、SD、CD、DVD、Blu-ray、etc.<br>・ Interfaces that are exploitable for physical analyses with disassembling vehicles / modifications.<br>➢ J-TAG, such as terminals which can access internal memory or external memory on microcontroller.[Δ3] |
| Reasons | | To use as input information for vulnerability analysis. |

### 5.2.3. Definition of Security Requirements for Things except Target ECUs[Δ3]

| Item | | Description |
|---|---|---|
| ID | | VULERQ_02003 |
| Application Conditions[Δ1Δ6] | Functions/Parts | - |
| | Target AP[Δ1] | - |
| Requirements | | Deleted. |
| Reasons | | - |

## 5.3. **Execution of Vulnerability Analysis**

### 5.3.1. Execution of Vulnerability Analysis for Architectural Designs

| Item | | Description |
|---|---|---|
| ID | | VULERQ_02004 |
| Application Conditions[Δ1Δ6] | Functions/Parts | All ECUs |
| | Target AP[Δ1] | All |
| Requirements | | ① Suppliers shall execute vulnerability analysis for design and implementation both of all security functions and interfaces which specified in VULERQ_02001, VULERQ_02002. Perspective of vulnerability analysis shall be referred to "Perspectives Analysis for Vulnerabilities of Architectural Designs" in below. [Δ3]<br>A person who executes vulnerability analysis shall meet "Requirement for a person who execute vulnerability analysis" in below. [Δ8]<br>② Suppliers shall execute vulnerability countermeasure if vulnerability has found. If suppliers do not take countermeasure, suppliers shall explain reason that countermeasure is not necessary. [Δ3]<br>- example of countermeasure: Mitigation described in CWE (such as additional deployment of security function)<br>- example of reason that countermeasure is not taken: There is no interface to exploit vulnerability<br><br>**Perspectives Analysis for Vulnerabilities of Architectural Designs**[Δ3]<br>As viewpoints for analyzing vulnerabilities, it can be used below. [Δ3] |

- CC/CEM Appendix B.2 “Vulnerability Assessment”
- CWE

As a reference, the methods of vulnerability analysis with CWE are shown below. [Δ3]

- (Annex 2) Guide of Vulnerability Analysis for Design / Implementation[Δ5]

**Requirement for a person who executes vulnerability analysis**[Δ8]

Vulnerability analysis requires cybersecurity knowledge and experience according to the Target AP. Therefore, the person who executes the vulnerability analysis shall meet the following requirements.

| Target AP | Requirements for a person who executes vulnerability analysis |
|---|---|
| 20 | Knowledge of devising new vulnerabilities and attack methods, extensive practical experience is required. Specifically, all of the followinga shall be met.<br>- More than 5 years of security work experience (*1)<br>- Past 3 years of vulnerability analysis and penetration testing results (*2)<br><br>(*1) “The number of years of work experience” is cited from the certification conditions of CISSP, an international cyber security qualification.<br>(*2) “Results” is cited from the vulnerability assessment service standards of the “Information Security Service Standards” stipulated by the Ministry of Economy, Trade and Industry in Japan. |
| 14 | Having advanced security knowledge of well-known vulnerabilities and attack methods. |

| | | | |
|---|---|---|---|
| | | | (e.g. Equivalent to Registered Information Security Specialist, understanding of CWE Top 25) |
| | | 10 | Having basic knowledge of security.<br>(e.g. Equivalent to Applied Information Technology Engineer Examination, understanding of "Requirements Specification of Common Vulnerability Countermeasure") |
| Reasons | To remove architectural vulnerabilities incorporated in ECUs. | | |

### 5.3.2. Execution of Vulnerability Analysis using ECU Vulnerability Test Perspectives [Δ8]

| Item | | Description |
|---|---|---|
| ID | | VULERQ_02005 |
| Application Conditions[Δ1Δ6] | Functions/Parts | - |
| | Target AP[Δ1] | - |
| Requirements | | (Deleted) |
| Reasons | | - |

### 5.3.3. Recurrence Prevention of Vulnerabilities that Handled in the Past

| Item | | Description |
|---|---|---|
| ID | | VULERQ_02006 |
| Application Conditions[Δ1Δ6] | Functions/Parts | All ECUs |
| | Target AP[Δ1] | All |
| Requirements | | Similar vulnerabilities handled in the past at Toyota shall be nonexistent.<br><br>**Methods to Check the Vulnerabilities Reported, Handled in the Past at Toyota.**<br>At Toyota, vulnerabilities reported, handled in the past and not registered in public vulnerability DBs (JVN etc.) are listed as Toyota in-vehicle Vulnerability Notes(TVN) [Δ6]. Suppliers shall check the TVN[Δ6] and prevent recurrence of vulnerabilities handled in the past in starting of ECU developments. And, if vulnerabilities are reported after starting of ECU developments, suppliers shall handle it in accordance with processes of vehicle SIRT.<br><br>TVN[Δ6]:<br>https://team-atsp.kitora.toyota.co.jp/sites/cybersecurity/SitePages/Sec_Home.aspx<br>(Access restriction of external affiliate(supplier) is activated according to the restriction of access permission setting. External affiliate could obtain the TVN from TMC design department.) |
| Reasons | | To prevent recurrence of vulnerabilities handled in the past thoroughly. |