関係各部署御中

| 表示 | PROTECTED 関係者外秘 | 原紙保管 | M/Y: / |
|---|---|---|---|
| | | コピー保管 | M/Y: / |

| 車両サイバーセキュリティコンセプト定義書<br>Vehicle Cybersecurity Concept Difinition | 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-24PF-VCL-CPT-INST-DOC-a00-01-a | | | |
| | 承認 Approved<br>河井 | 調査 Checked<br>松井 | 作成 Created<br>玉樹 | 2021/09/17<br>Omission of signature (approved electronically) |

| | |
|---|---|
| **適用**<br>**Scope** | Post19 電子 PF の ECU に適用する。<br>Applies to Post19ePF ECUs. |
| **変更内容**<br>**Revision Record** | 【主な変更点 Main changes】<br>(SEC-24PF-VCL-CPT-INST-DOC-a00-00-a ⇒ SEC-24PF-VCL-CPT-INST-DOC-a00-01-a)<br>要件変更(Change requirements) |
| **特記**<br>**Special note** | 【入手先 Source】<br>本文書は iSpirit からダウンロードしてください。<br>This document can be downloaded from iSpirit.<br>[Folder]/Repository/Electronics_Spec/Cybersecurity[ サイバーセキュリティ]/Standard[ 標準]/Concept[コンセプト]/24PF[24 電子プラットフォーム]/CPT[コンセプト]/仕様書 ALL<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>E/E Architecture Development Div System network & architecture development dept<br>Contact for security inquiries<br>Mail:epf-sec-sp@mega.tec.toyota.co.jp<br><br>本書はトヨタ内限定<br>委託先／サプライヤへの展開・提供を禁止する。 |

# 1. 変更履歴

| Version | 変更内容 | 日付 | 変更者 |
|---|---|---|---|
| a00-00-a | 新規作成 | 2020/9/8 | 46F 玉樹 |
| a00-01-a | 2.3 暫定 LAN 構成の修正、暫定セントラル ECU 構成の追加、エントリポイント一覧の修正 | 2021/09/17 | 46F 玉樹 |
| | 2.5 関連文書の修正 | | |
| | 4.1 引き当てに関する要求の明確化 | | |
| | 4.2 Zone 分類の修正 | | |
| | 4.4 アタックポテンシャルの達成条件の関する要求の追加 | | |
| | 別紙 1　法規対応による CSR の追加、CSR とサイバーセキュリティゴールの対応関係明確化等 | | |

# 目次


1. 変更履歴 ..... 2

2. はじめに ..... 4

2.1. 本書の位置付け ..... 4
2.2. 適用範囲 ..... 4
2.3. 前提条件 ..... 4
2.4. 要求事項の記載 ..... 6
2.5. 関連文書 ..... 6
2.6. 参考文書 ..... 6

3. 要求概要 ..... 7

3.1. 要求一覧 ..... 7

4. 車両サイバーセキュリティコンセプト ..... 8

4.1. 引当て仕様書 ..... 8
4.2. POST19 電子 PF LAN の制約条件 ..... 8
4.3. エントリポイントの制約条件 ..... 10
4.4. アタックポテンシャルの達成条件 ..... 10

5. Appendix ..... 11

# 2. はじめに

## 2.1. 本書の位置付け

本書では、Post19 電子 PF における車両サイバーセキュリティコンセプトを定義する。

## 2.2. 適用範囲

本書の適用範囲は、Post19 電子 PF に搭載する ECU とする。

## 2.3. 前提条件

本書においては 2021/7/27 時点での暫定 LAN 構成、2021/8/3 時点での暫定セントラル ECU 構成を前提とし、”図 2-1 暫定 LAN 構成”、”図 2 暫定セントラル ECU 構成” に示す。

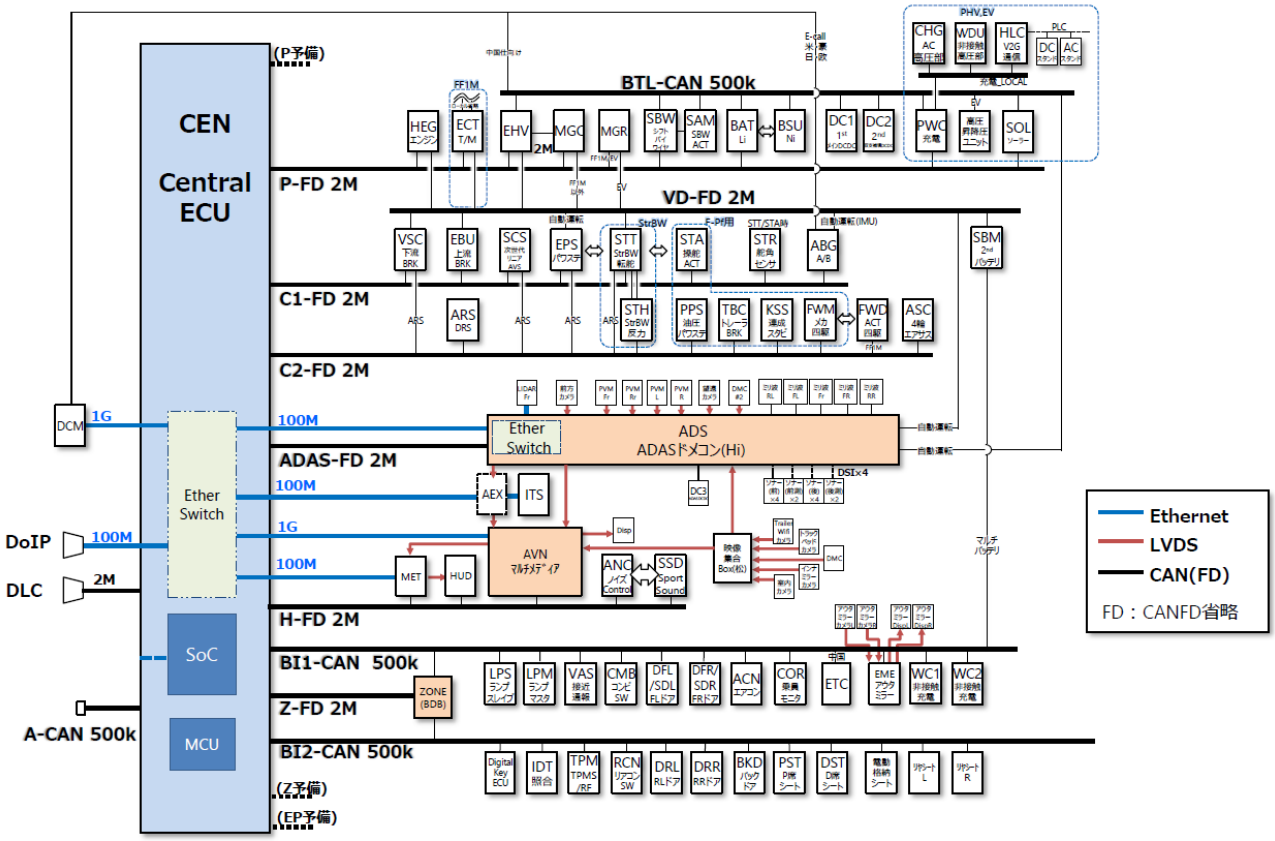


図 2-1 暫定 LAN 構成

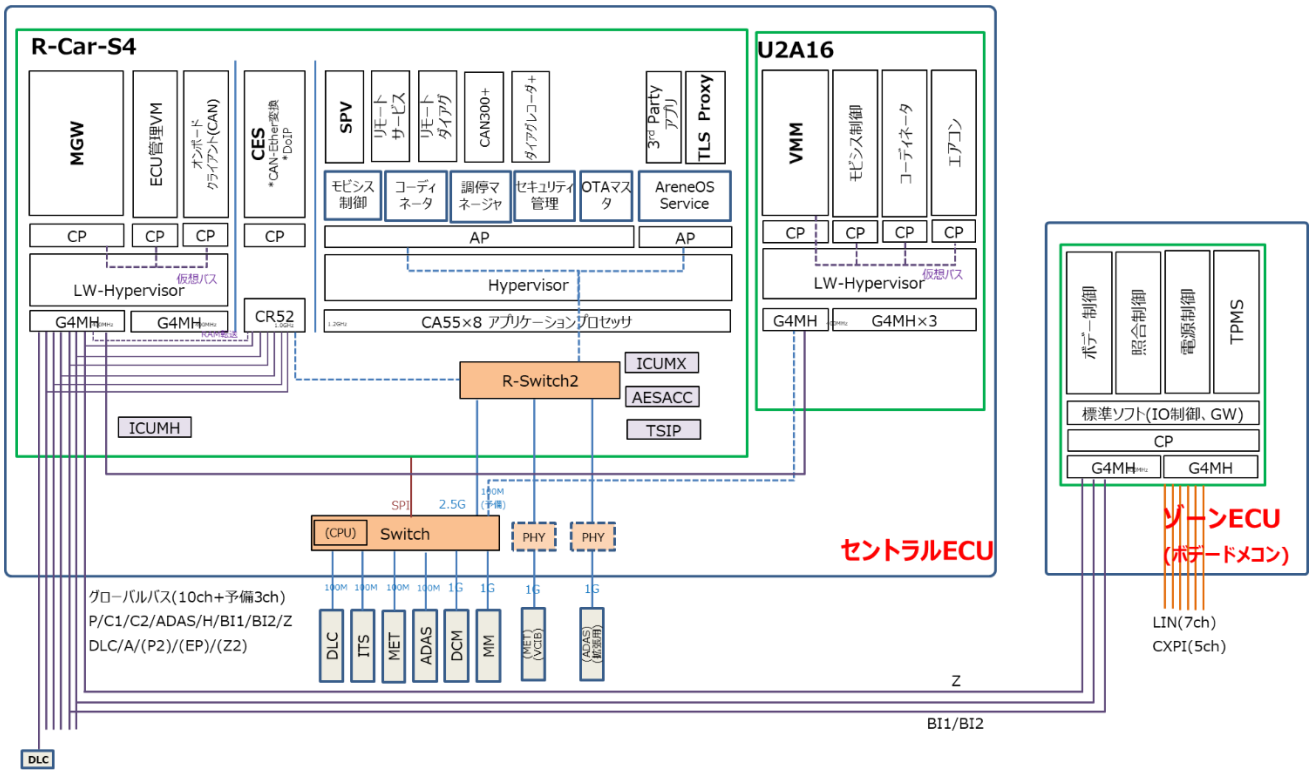


**図 2 暫定セントラル ECU 構成**

本書において前提とするエントリポイント、及びそのユースケースを”表 2-1 エントリポイント一覧”に示す。

**表 2-1 エントリポイント一覧**

| ECU | エントリポイント | ユースケース |
|---|---|---|
| セントラル ECU | DLC | ダイアグ(DoIP, DoCAN) |
| | | リプログラミング |
| | | データロガー |
| | TLS 終端 | リモートサービス |
| | 3rd party アプリケーション | T.B.D. |
| マルチメディア ECU | Wi-Fi | 持ち込み機器接続 |
| | Bluetooth | |
| | USB | リプログラミング |
| | DSRC | ETC |
| DCM | 移動通信(3G, 4G, 5G) | センタ通信 |
| ITS | DSRC | 路車間通信 |
| IDT | RF 通信 | スマートキー |
| | BLE | スマートフォンキー |

| | | |
|---|---|---|
| RKE | RF 通信 | キーレスキー |
| TPM | RF 通信 | 空気圧センサ |
| HLC | PLC | 充電設備通信(充電制御、PnC) |
| | CAN | 充電設備通信(充電制御) |
| | Wi-Fi | 非接触スタンド通信(充電制御) |
| MaaS ECU | MaaS 通信機 | センタ通信 |
| 映像集合 Box | Wi-Fi | Trailer Camera(ADAS ドメコン) |
| ETC | DSRC | ETC |
| Qi | NFC | スマートフォン接続 |
| GDO | IEEE 802.15.4 | ガレージドアオープナー |

## 2.4. 要求事項の記載

【要求事項：**】と記載されている部分が本書で要求する仕様とする。ただし、（補足）と記載されているものは補足事項のため要求仕様ではない。

## 2.5. 関連文書

| 文書名 | Ver. | 発行元 |
|---|---|---|
| [1] Post19 電子 PF 脅威分析とリスクアセスメント結果報告書 | SEC-24PF-VCL-TARA-INST-DOC-***-**-* | 46F |
| [2] 車両サイバーセキュリティ及びプライバシー用語定義書 | SEC-ePF-TRM-GUD-PROC-***-**-* | 46F |
| [3] 共通脆弱性対策要求仕様書 | SEC-ePF-VUL-CMN-REQ-SPEC-***-**-* | 46F |
| [4] ECU 脆弱性対策要求仕様書 | SEC-ePF-VUL-ECU-REQ-SPEC-***-**-* | 46F |
| [5] ECU 脆弱性対策評価仕様書 | SEC-ePF-VUL-ECU-TST-SPEC-***-**-* | 46F |
| [6] ECU 侵入テスト仕様書 | SEC-ePF-VUL-EPN-TST-SPEC-***-**-* | 46F |

関連文書のバージョンは ECU の要求仕様書に従うこと。

## 2.6. 参考文書

| 文書名 | Ver. | 発行元 |
|---|---|---|
| T.B.D. | | |
| | | |
| | | |

# 3. 要求概要

## 3.1. 要求一覧

ECU が対応すべき要求事項の一覧を”表 3-1 要求事項対応表”に記す。要求事項の詳細については、4 章以降を参照。

**表 3-1 要求事項対応表**

| 要求事項 | ECU |
|---|---|
| VCLCPT_00001 | ○ |
| VCLCPT_00002 | ○ |
| VCLCPT_00003 | ○ |
| VCLCPT_00004 | ○ |
| VCLCPT_00005 | ○ |

# 4. 車両サイバーセキュリティコンセプト

本章では、車両サイバーセキュリティコンセプトを示す。

## 4.1. 引当て仕様書

【要求事項：VCLCPT_00001】

各 ECU、及びシステム設計者は、別紙 1 を参照し、引当たるサイバーセキュリティ要求を決定すること。

## 4.2. Post19 電子 PF LAN の制約条件

【要求事項：VCLCPT_00002】

Trusted Zone にエントリポイントを追加してはいけない。やむをえず Trusted Zone にエントリポイントを追加する場合は、追加されるエントリポイントに多層分離要求仕様書を引当てるなどの対応が必要となるため、サイバーセキュリティ標準設計に連絡し許可を得ること。

“図 2-1 暫定 LAN 構成”において、Untrusted Zone 及び Trusted Zone に所属する CAN バス、Ethernet を”表 4-1 Zone 分類一覧”に示す。

セントラル ECU 内、及びローカルバスの Zone 分類については T.B.D.

**表 4-1 Zone 分類一覧**

| 分類 | 通信プロトコル | バス/ポート |
|---|---|---|
| Untrusted Zone | Ethernet | DCM 接続ポート |
| | | ITS 接続ポート |
| | | MaaS 通信機接続ポート |
| | | ADAS ドメコン接続ポート |
| | | VCIB 接続ポート |
| | | MM 接続ポート |
| | | セントラル ECU 内仮想 Ethernet |
| | CAN | P バス |
| | | C1 バス |
| | | C2 バス |
| | | H バス |
| | | BI1 バス |
| | | BI2 バス |
| | | Z バス |
| | | スタンドローカルバス |

| | | |
|---|---|---|
| | | 充電ローカルバス |
| | | A バス |
| | | セントラル ECU 内仮想 CAN |
| Trusted Zone | CAN | BT ローカルバス |
| | | VD バス |
| | | RH85－U2A16⇔Zone ECU ローカルバス |
| | | RH85－U2A16⇔F1KM ローカルバス |
| | その他 Untrusted zone 以外で RR7 制御通信を行う通信線※1 | |

※１：電子 PF アーキ決定後に具体名を記載予定

## 4.3. エントリポイントの制約条件

【要求事項：VCLCPT_00003】

”表 2-1 エントリポイント一覧”に記載のないエントリポイントを追加する場合は、サイバーセキュリティ標準設計に連絡すること。

【要求事項：VCLCPT_00004】

エントリポイントを持つ ECU のエントリポイント領域において、リスクランク 7 以上の制御、及びリスクランク 7 以上のコマンド送信を行ってはいけない。加えてエントリポイントを持つ ECU は、遠隔からのリスクランク 7 以上のコマンド中継を行ってはいけない。

## 4.4. アタックポテンシャルの達成条件

【要求事項：VCLCPT_00005】

各 ECU、及びシステム設計者は、サイバーセキュリティ要求に対する目標 AP を達成するために、関連文書[3]-[6]に従い脆弱性対策を実施すること。

表 2-1 エントリポイント一覧でエントリポイントを持つ ECU は、別紙 1 の「エントリポイントを持つ ECU の目標 AP」の列を確認すること。エントリポイントを持たない ECU は、別紙 1 の「エントリポイントを持たない ECU の目標 AP」の列を確認すること。
ただし、多層分離を VM で実現する ECU（セントラル ECU）に関して、エントリポイント領域（1 層目）に配置される VM は「エントリポイントを持つ ECU の目標 AP」の列を確認し、内部領域の Untrusted Zone（2 層目）に配置される VM は「エントリポイントを持たない ECU の目標 AP」の列を確認すること。

# 5. Appendix

T.B.D.