関係各部署　御中

To departments concerned

Confidentiality classification	PROTECTED 関係者外秘	原紙保管 Storage of original	M/Y /
		コピー保管 Storage of copy	M/Y /

侵入検知 セキュリティ機能向け 復旧 要求仕様書
Requirements Specification of Recovery System for Security

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
System Network & Architecture Development Dept. 4G
E/E Architecture Development Div.

No. SEC-ePF-IDS-REC-REQ-SPEC-a00-03-b

承認 Approved by	調査 Checked by	作成 Created by	2022/05/20
河井	松井	竹山	Omission of signature (approved electronically)

適用先 Target	リプロ機能を有するエントリーポイント ECU/VM に適用する。 Applies to entry point ECU/VM with reprogramming function.
変更概要 Change	SEC-ePF-IDS-REC-REQ-SPEC-a00-03-a ⇒ SEC-ePF-IDS-REC-REQ-SPEC-a00-03-b ・誤記修正 Editorial errors corrected
特記 Special note	【展開規則　Distribution rule】 必要に応じて、関係会社・関係部署（海外事業体、ボデーメーカ、ECU サプライヤ）への展開をお願いします。 Please distribute this document to affiliated companies, or departments (e.g. overseas business entities, car body manufacturers, or ECU suppliers) if necessary. 【問合せ先　Contact information】 制御電子プラットフォーム開発部　制御ネットワーク・アーキ開発室 セキュリティ仕様問合せ窓口 System Network & Architecture Development Dept. E/E Architecture Development Div. Contact for Security Inquiries email: epf-sec-sp@mega.tec.toyota.co.jp

変更履歴

Version	変更内容	日付	変更者
a00-00-a	新規作成	2020/06/23	46F 4G 稲垣
a00-01-a	誤記修正（ヘッダ仕様書英名） 適用範囲を「防御機能を有する ECU」から「エントリーポイント ECU/VM」に変更 1.1 本書の目的を詳細化、2.1 システム構成を簡略化 適用範囲変更に伴い、前提条件を「エントリーポイント ECU/VM の防御機能」に変更 状態通知機能（IDSRER_02100 - 2300）を削除 要求一覧を追加、ハードウェア関連要件を記載	2021/04/05	46F 4G 稲垣
a00-01-b	英訳の追加 上位文書名を「車両サイバーセキュリティコンセプト定義書」に変更	2021/05/14	46F 4G 稲垣
a00-02-a	適用範囲を修正 構成、項目名変更 IDSRER_01100 と IDSRER_01200 を集約して IDSRER_01300 を定義	2021/12/03	46F 4G 竹山
a00-03-a	IDSRER_03100 証明書失効リスト（CRL）の要求を追加	2022/02/03	46F 4G 竹山
a00-03-b	要求事項対応表の誤記訂正	2022/05/20	46F 4G 竹山

目次

変更履歴 2

1. はじめに 4

1.1. 本書の目的 4
1.2. 適用範囲 4
1.3. 前提条件 4
1.4. 要求事項の記載 4
1.5. 関連文書 4
1.5.1. 上位文書 4
1.5.2. 参照文書 4

2. 要求概要 5

2.1. システム構成 5
2.2. システム構成 5
2.3. 要求一覧 6

3. 機能要求詳細 7

3.1. 脆弱性の修正 7
3.1.1. プログラムの更新 7
3.1.2. 証明書失効リスト（CRL）の更新 7

1. はじめに

1.1. 本書の目的

本書の目的は、米国国立標準研究所（NIST）が作成したサイバーセキュリティ対策に関するフレームワークにおける「復旧」機能を車載で実現するためのシステムであるセキュリティ機能向け復旧の要求を定義することである。セキュリティ機能向け復旧は、L/O 後の新たな脆弱性を修正するための機能である。

1.2. 適用範囲

本書はリプロ機能を有するエントリーポイント ECU/VM に適用される。

1.3. 前提条件

本書はエントリーポイント ECU/VM の防御機能に関する脆弱性の修正を前提とする。

1.4. 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。

1.5. 関連文書

上位仕様書、参照文書を示す。なお、関連文書のバージョンは ECU の要求仕様書に従うこと。

1.5.1. 上位文書

表 1-1 上位文書

No.	文書名	Ver.
1	車両サイバーセキュリティコンセプト定義書	-

1.5.2. 参照文書

表 1-2 参照文書

No.	文書名	Ver.
1	Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology, April 16, 2018, https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11	1.1
2	標準リプログラミングセキュリティ要求仕様書	-
3	センター通信セキュリティ要求仕様書	-

2. 要求概要

2.1. システム構成

復旧システム（以下、本システム）のシステムコンテキストをデータフローダイアグラムで示す（図 2-1）。円は本システムを、四角は本システムと情報やサービスのやり取りを行う主体を表す。本システムは、サイバーセキュリティ防御機能の脆弱性をリプログラミングツールや OTA リプログラミングアプリから修正する。

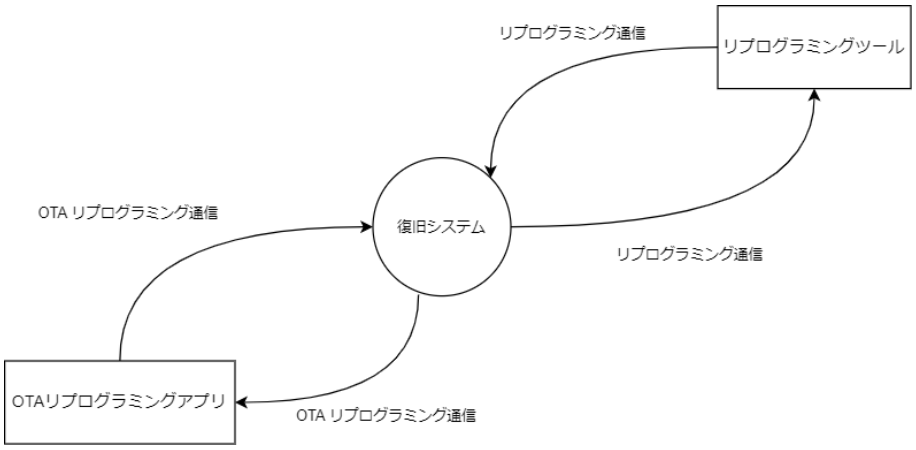

図 2-1 システムコンテキスト図

2.2. システム動作概要

本システムは、図 2-2 で示す通りの動作をする。

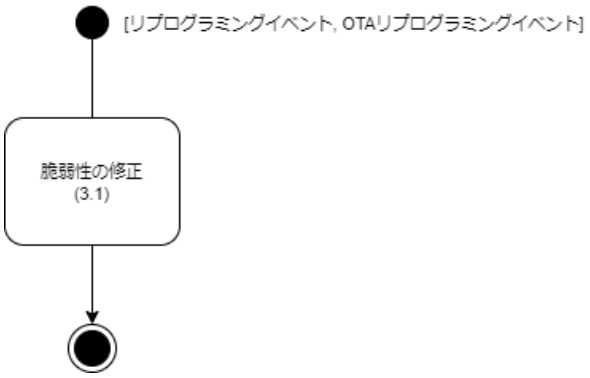

図 2-2 UML アクティビティ図

2.3. 要求一覧

本仕様書を実装する場合、対応すべき要求事項の一覧を表 2-1 に示す。

表 2-1 要求事項対応表

要求分類	分類	要求事項	ハードウェア関連要件
機能要求	脆弱性の修正	IDSRER_01300	-
		IDSRER_03100	-

3. 機能要求詳細

以下に復旧の機能要求を定義する。

3.1. 脆弱性の修正

本節ではサイバーセキュリティ防御機能の脆弱性を修正するための機能要求を定義する。

3.1.1. プログラムの更新

【要求事項：IDSRER_01300】

サイバーセキュリティ防御機能は参照文書[2]に従い有線リプログラミングもしくは OTA リプログラミングにて書き換え可能である必要がある。

3.1.2. 証明書失効リスト（CRL）の更新

【要求事項：IDSRER_03100】

本要求は、参照文書[3]の証明書失効リスト(CRL)を持つ ECU/VM に適用される。参照文書[3]で用いる証明書失効リスト(CRL)は参照文書[2]に従い有線リプログラミングもしくは OTA リプログラミングにて書き換え可能である必要がある。

Revision Record

Version	Change	Date	Reviser
a00-00-a	First version issued	2020/06/23	46F 4G Inagaki
a00-01-a	Error corrected (English name in the header of this doc.) Target modified from "ECUs with defenses" to "entry point ECU/VMs". Prerequisites changed to in accordance with the change of the target. Status notification function (IDSRER_02100-2300) deleted. List of requirements and column of hardware-related requirements added.	2021/04/05	46F 4G Inagaki
a00-01-b	English translation added Input document name changed to "Vehicle Cyber Security Concept Definition Specification ” .	2021/05/14	46F 4G Inagaki
a00-02-a	Target of this document changed. Document structure and name of sections changed IDSRER_01100 and IDSRER_01200 merged to DSRER_01300.	2021/12/03	46F 4G Takeyama
a00-03-a	Certificate Revocation List (CRL) request (IDSRER_03100) added.	2022/02/03	46F 4G Takeyama
a00-03-b	Error corrected (List of requirements)	2022/05/20	46F 4G Takeyama

Table of Contents

1. Introduction 3

1.1. Purpose of this document 3
1.2. Target 3
1.3. Prerequisites 3
1.4. Description of requirements 3
1.5. Related documents 3
1.5.1. Input documents 3
1.5.2. References 3

2. Requirements overview 4

2.1. System context 4
2.2. System operation overview 4
2.3. List of requrements 5

3. Functional requirements 6

3.1. Fixing vulnerabilities 6
3.1.1. Updating the program 6
3.1.2. Updating Certificate Revocation List (CRL) 6

1. Introduction

1.1. Purpose of this document

The purpose of this document is to define requirements of Recovery System for Security, which realizes the *Recovery* function in the framework for cybersecurity ([1]) defined by National Institute of Standards and Technology (hereinafter referred to as *NIST*). Recovery for security functions fix new vulnerabilities turned out after line off.

1.2. Target

This document is allocated to entry point ECUs/VMs that have reprogramming functions.

1.3. Prerequisites

We assume that this system recoveries vulnabilities of defense functions in entry point ECU/VMs.

1.4. Description of requirements

We describe requirements as [Requirement: **] in this document where <Note> means just a supplementary note.

1.5. Related documents

Inputs documents, and references are shown in this section. If the specification of the ECU specifies the version of the reference, follow it.

1.5.1. INPUT DOCUMENTS

Table 1-1 Superordinate documents

No.	Document name	Ver.
1	Vehicle Cyber Security Concept Definition Specification	-

1.5.2. REFERENCES

Table 1-2 Referenced documents

No.	Document name	Ver.
1	Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology, April 16, 2018, https://www.nist.gov/publications/framework-improving-Critical-infrastructure-cybersecurity-version-11	1.1
2	Requirements Specification of Standard Reprogramming Security	-
3	Requirements Specification of Center Communication Security	-

2. Requirements overview

2.1. System context

We show the system context with DFD (Figure 2-1). The circle means this system, and the rectangles mean subjects transmitting or receiving information or services. This system fixes vulnerabilities in cyber security defense functions with reprogramming tools and OTA reprogramming applications.

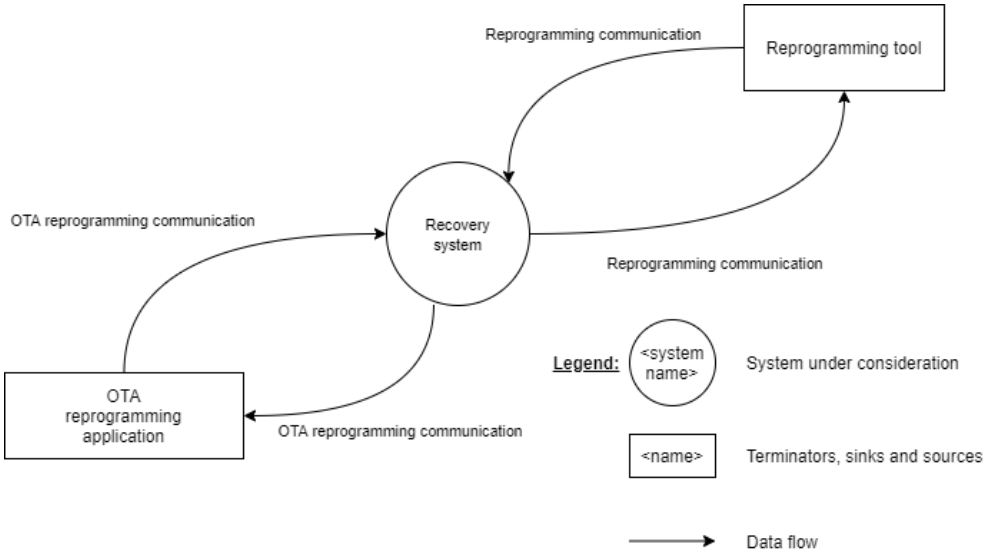

Figure 2-1 System context

2.2. System operation overview

This system operates as shown in Figure 2-2.

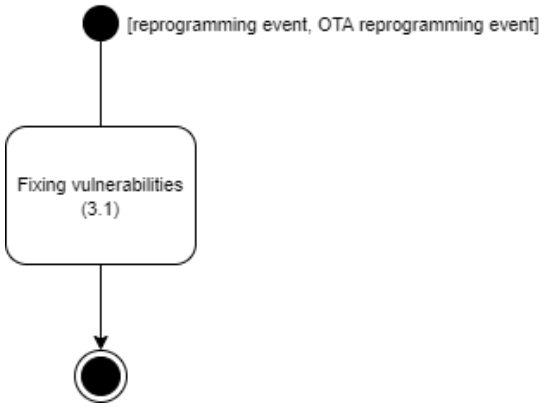

Figure 2-2 System operation

2.3. List of requrements

Table 2-1 lists the requirements to be addressed when implementing this specification.

Table 2-1 List of requirements

Category		Requirements	Hardware-related requirements
Functional requirements	Fixing vulnerabilities	IDSRER_01300	No
		IDSRER_03100	No

3. Functional requirements

We define functional requirements in this chapter.

3.1. Fixing vulnerabilities

We define functional requirements of fixing vulnerabilities in cyber security defense functions in this section.

3.1.1. UPDATING THE PROGRAM

[Requirement: IDSRER_01300]

This system shall be capable to rewrire cyber security defense functions by wired or OTA reprogramming in accordance with [2].

3.1.2. UPDATING CERTIFICATE REVOCATION LIST (CRL)

[Requirement: IDSRER_03100]

This requirement shall be allocated to ECUs/VMs that have Certificate Revocation List (CRL) in accordance with [3]. This system shall be capable to rewrite the Certificate Revocation List (CRL) used in [3] by wired or OTA reprogramming in accordance with [2].