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 評価仕様書
Test 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-TST-SPEC-a00-02-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-TST-SPEC -a00-02-a ⇒ SEC-ePF-IDS-REC-TST-SPEC -a00-02-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 「セキュリティ機能向け 復旧 要求仕様書」を上位文書とし、本書の目的を上位文書の為の評価要件に変更 状態通知機能（IDSRET_02100 - 2300）を削除 要求仕様書の機能要求修正に伴い、評価要求を修正	2021/04/05	46F 4G 稲垣
a00-01-b	英訳の追加	2021/05/14	46F 4G 稲垣
a00-02-a	適用範囲を修正 構成、項目名変更 IDSRET_01100 と IDSRET_01200 を集約して IDSRET_01300 を定義 IDSRET_03100 証明書失効リスト（CRL）の要求追加 評価内容を全体的に具体化	2022/02/17	46F 4G 竹山
a00-02-b	参照文書を修正（センター通信セキュリティ評価仕様書を追加） IDSRET_03100 の試験手順 (8), 測定項目 (C), 合否判定の参照文書番号を修正	2022/05/20	46F 4G 竹山

目次

1. はじめに

1.1. 本書の目的

本書では、侵入検知 セキュリティ機能向け 復旧 要求仕様書（上位文書[1]）によって定義された要求を評価する為の評価仕様を定義する。

1.2. 適用範囲

本書の適用範囲は、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。

1.3. 前提条件

なし。

1.4. 要求事項の記載

【IDSRET_**】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

上位文書、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	侵入検知 セキュリティ機能向け 復旧 要求仕様書	-

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	-
4	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	-
5	無線通信セキュリティ要求仕様書	-

6	メッセージフィルタリング要求仕様書	-
7	センター接続機器認証要求仕様書	-
8	標準リプログラミング要求仕様書	-
9	センター通信セキュリティ評価仕様書	-

1.6. 用語定義

本書で用いる用語については、参照文書[4] を参照のこと。

2. 評価概要

評価項目一覧を表 2-1 に示す。評価項目の合否判定を全て満たす場合、合格と判定すること。

表 2-1：評価項目一覧

上位文書[1]が定義する要求項目			評価項目	生産時機能
分類		要求 ID	評価 ID	
機能要求	脆弱性の修正	IDSRER_01300	IDSRET_01300	-
		IDSRER_03100	IDSRET_03100	-

3. 評価環境

本仕様書で想定する評価環境を図 3-1 に示す。

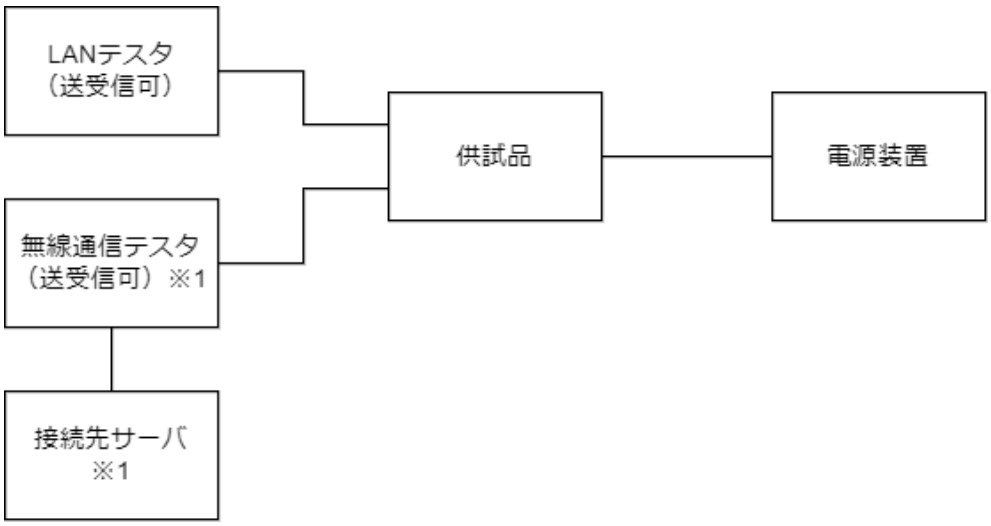

図 3-1：評価環境

※1 必要に応じて評価に用いること。

4. 評価詳細

復旧システムの要求の実装を確認するための評価要求を定義する。

4.1. 機能要求評価

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評価要求を定義する。

4.1.1. プログラムの更新

【IDSRET_01300】	
試験内容	サイバーセキュリティ防御機能が参照文書[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できることを確認する。
事前条件	● 供試品は、古いバージョンの防御機能※1 を含むプログラム（以下、プログラム A）が書き込まれている。 ● プログラム A より新しいバージョンの防御機能※1 を含むプログラム（以下、プログラム B）が用意できている。
試験手順	(1) 供試品の電源を ON にする。 (2) LAN テスタから供試品に対し、プログラム B を書き込む。 (3) 供試品を再起動する。 (4) LAN テスタから供試品に対し、参照文書[8] 8.1.11.4 の書換えデータチェック要求を送信する。 (5) LAN テスタが供試品から書換えデータチェック応答を受信する。 (6) LAN テスタから供試品に対し、参照文書[8] 8.1.8.1 のソフトウェア品番読み出し要求を送信する。 (7) LAN テスタが供試品からソフトウェア品番読み出し応答を受信する。
測定項目	(A) 試験手順(5)における LAN テスタの受信メッセージ (B) 試験手順(7)における LAN テスタの受信メッセージ
合否判定	● 測定項目(A)に書換えデータチェックのネガティブレスポンスを示すメッセージが含まれないこと。 ● 測定項目(B)にプログラム B のバージョンを示すメッセージが含まれること。
備考	※1 ここでの防御機能は、無線通信セキュリティ要求仕様書（参照文書[5]）、メッセージフィルタリング要求仕様書（参照文書[6]）、センター接続機器認証要求仕様書（参照文書[7]）の内、供試品に適用される要求仕様書にて定義される防御機能を想定する。

4.1.2. 証明書失効リスト(CRL)の更新

【IDSRET_03100】	
試験内容	参照文書[3]で用いる証明書失効リスト(CRL)が参照文書[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できることを確認する。
事前条件	● 供試品は、古いバージョンの CRL を含むプログラム（以下、プログラム A）が書き込まれている。 ● プログラム A より新しいバージョンの CRL を含むプログラム（以下、プログラム B）が用意できている。
試験手順	(1) 供試品の電源を ON にする。 (2) LAN テスタから供試品に対し、プログラム B を書き込む。 (3) 供試品を再起動する。 (4) LAN テスタから供試品に対し、参照文書[8] 8.1.11.4 の書換えデータチェック要求を送信する。 (5) LAN テスタが供試品から書換えデータチェック応答を受信する。 (6) LAN テスタから供試品に対し、参照文書[8] 8.1.8.1 のソフトウェア品番読み出し要求を送信する。 (7) LAN テスタが供試品からソフトウェア品番読み出し応答を受信する。 (8) 参照文書[9]の 5.1.1. および 5.1.2. (CCSTST_00012, CCSTST_00041, CCSTST_00042, CCSTST_00043）で要求される試験手順に従って試験する。
測定項目	(A) 試験手順(5)における LAN テスタの受信メッセージ (B) 試験手順(7)における LAN テスタの受信メッセージ (C) 試験手順(8) における参照文書[9]の 5.1.1. および 5.1.2. (CCSTST_00012, CCSTST_00041, CCSTST_00042, CCSTST_00043）で要求される測定項目
合否判定	● 測定項目(A)に書換えデータチェックのネガティブレスポンスを示すメッセージが含まれないこと。 ● 測定項目(B)にプログラム B のバージョンを示すメッセージが含まれること。 ● 測定項目(C) が参照文書[9]の 5.1.1. および 5.1.2. (CCSTST_00012, CCSTST_00041, CCSTST_00042, CCSTST_00043）で要求される合否判定を満たすこと。
備考	なし。

Revision Record

Version	Change	Date	Changer
a00-00-a	The first version issued.	2020/06/23	46F 4G Inagaki
a00-01-a	Error corrected (header specification English name). The scope of application changed from "ECUs with defenses" to "entry point ECU/VM". "Requirements Specification of Recovery System for Security" added to the input document, and the purpose of this document changed to defining tests for it. The status notification function (IDSRET_02100-2300) deleted. The tests modified in accordance with the modification of the functional requirements of the requirements specification.	2021/04/05	46F 4G Inagaki
a00-01-b	English translation added.	2021/05/14	46F 4G Inagaki
a00-02-a	The target of this document added. The structure of this document modified. IDSRET_01100 and IDSRET_01200 merged into IDSRET_01300. Certificate Revocation List (CRL) requirement (IDSRER_03100) added. Tests fleshed.	2022/02/17	46F 4G Takeyama
a00-02-b	References modified (Test Specification of Center Communication Security added). Test Procedure (8), Measurement item (C) and Pass criteria in IDSRET_03100 modified.	2022/05/20	46F 4G Takeyama

Table of Contents

1. Introduction

1.1. Purpose of this Document

This document defines the test specification for testing the requirements defined by "Requirements Specification of Recovery System for Security" (Input document [1]).

1.2. Target of this Document

This document shall be allocated to entry-point ECU/VM.

1.3. Prerequisites

None.

1.4. Description of requirements

We describe tests as [IDSRET_**] 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: Input Documents

No	Document name	Ver
1	Requirements Specification of Recovery System for Security	-

1.5.2. REFERENCES

Table 1-2: References

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	-
4	Terms and Definitions related to Vehicle Cybersecurity and Privacy	-

5	Requirements Specification of Wireless Communication Security	-
6	Requirements Specification of Message Filtering	-
7	Requirements Specification of Center Communication Security	-
8	Standard Reprogramming Specifications	-
9	Test Specification of Center Communication Security	-

1.6. Glossary

See Reference [4] for terms used in this document.

2. Tests Overview

We show the table of all tests defined in this document (Table 2-1). The Device Under Test (hereinafter referred to as DUT) shall pass all tests.

Table 2-1: Table of all tests

Requirements defined in the input document [1]			Tests	Production -time function
Category		Requirement ID	Test ID	
Functional Requirements	Fixing Vulnerabilities	IDSRER_01300	IDSRET_01300	-
		IDSRER_03100	IDSRET_03100	-

3. Test Environment

In this document, we assume the test environment shown in Figure 3-1.

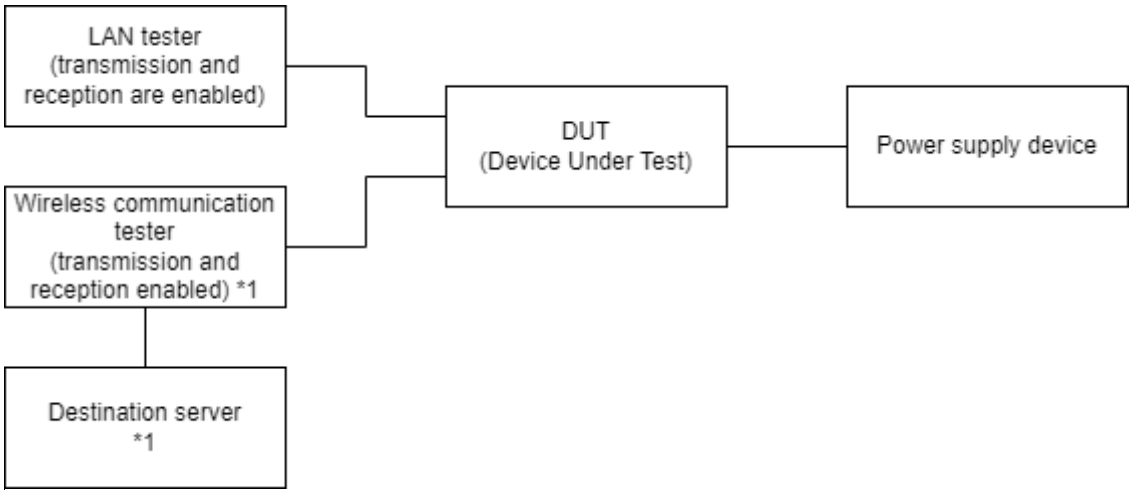

Figure 3-1: Test environment

*1 Use it if necessary.

4. Tests

Tests are defined to ensure that all the requirements of the recovery system are satisfied.

4.1. Functional requirement tests

This section defines the test requirements to fix vulnerabilities in cyber security defenses.

4.1.1. UPDATING PROGRAM

[IDSRET_01300]	
Test	Test whether this system is capable to rewrite cyber security defense functions by wired or OTA reprogramming in accordance with [2].
Pre-condition	● A program that contains an older version of cyber security defense functions *1 (hereinafter referred to as Program A) shall be written to the DUT. ● A program that contains the newer version of the cyber security defense functions than that of Program A *1 (hereinafter called Program B) is prepared.
Test Procedure	(1) Turn on the power of the DUT. (2) Write Program B from the LAN tester to the DUT. (3) Reboot the DUT. (4) Send the reprogramming-data-check request defined in 8.1.11.4 in the reference document [8] from the LAN tester to the DUT. (5) Receive the reprogramming-data-check response from DUT using LAN tester. (6) Send the ApplicationSoftwareIdentificationDataIdentifier request defined in 8.1.8.1 in the reference document [8] from the LAN tester to the DUT. (7) Receive the ApplicationSoftwareIdentificationDataIdentifier response from DUT using LAN tester.
Measurement item	(A) The messages received by the LAN tester during the test procedure (5). (B) The messages received by the LAN tester during the test procedure (7).
Pass criteria	● Measurement item (A) shall not include a message indicating negative response of ApplicationSoftwareIdentificationDataIdentifier. ● Measurement item (B) shall include a message indicating the version of Program B.
Note	*1 We assume that the DUT has the cyber security defense functions defined in the references allocated to the DUT from [5], [6] and [7].

4.1.2. UPDATING CERTIFICATE REVOCATION LIST (CRL)

[IDSRET_03100]	
Test	Test whether this system is capable to rewrite the Certificate Revocation List (CRL) used in the reference [3] by wired or OTA reprogramming in accordance with the reference [2].
Pre-conditions	● A program that contains an older version of the CRL (hereinafter referred to as Program A) shall be written to the DUT. ● A program that contains the newer version of the CRL than that of Program A *1 (hereinafter called Program B) is prepared.
Test Procedure	(1) Turn on the power of the DUT. (2) Write Program B from the LAN tester to the DUT. (3) Reboot the DUT. (4) Send the reprogramming-data-check request defined in 8.1.11.4 in the reference document [8] from the LAN tester to the DUT. (5) Receive the reprogramming-data-check response from DUT using LAN tester. (6) Send the ApplicationSoftwareIdentificationDataIdentifier request defined in 8.1.8.1 in the reference document [8] from the LAN tester to the DUT. (7) Receive the ApplicationSoftwareIdentificationDataIdentifier response from DUT using LAN tester. (8) Test according to the test procedures required in 5.1.1. and 5.1.2. (CCSTST_00012, CCSTST_00041, CCSTST_00042, CCSTST_00043) in the reference [9].
Measurement item	(A) The messages received by the LAN tester at the test procedure (5). (B) The messages received by the LAN tester at the test procedure (7). (C) Measurement items required in 5.1.1. and 5.1.2. (CCSTST_00012, CCSTST_00041, CCSTST_00042, CCSTST_00043) in the reference [9] at the test procedure (8).
Pass criteria	● Measurement item (A) shall not include any message indicating negative response of ApplicationSoftwareIdentificationDataIdentifier. ● Measurement item (B) shall include any message indicating the version of Program B. ● Measurement item (C) shall pass the pass criteria required in 5.1.1. and 5.1.2. (CCSTST_00012, CCSTST_00041, CCSTST_00042, CCSTST_00043) in the reference [9].
Note	None.