



In-Vehicle Network	Reprogramming Security Operation Regulations	1/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

関係各部署 御中	<div style="border: 1px solid black; padding: 5px; text-align: center;"> PROTECTED 関係者外秘 </div>	原紙保管	M/Y: /
		コピー保管	M/Y: /
リプログラミングセキュリティ 運用規定		No. SEC-ePF-RPR-OPE-STD- S00-03-a	
		情報セキュリティ推進部	
		承認 	調査 
		tel:050-3192-2763	
適用	標準リプログラミングセキュリティ要求仕様書を適用する ECU 及びリプログラミングツール		
変更内容	(1) 新規 (2) <u>変更</u> ベース仕様書は No. <u>SEC-ePF-RPR-OPE-STD-S00-01-a</u> とする。		
特記事項	<p>【入手先】 本文書及び関連帳票は iSpirit からダウンロードしてください。 iSpirit : /リプログラミングセキュリティ 必要に応じて、関係会社・関係部署（海外事業体、ボデーメーカー、ECU サプライヤ）への展開をお願いします。</p> <p>【問合せ先】 運用 QA メーリス名称: <u>リプロセキュリティ関連ツール運用窓口</u> Mail: in-repro-secsvr-help@mail.toyota.co.jp</p>		

In-Vehicle Network	Reprogramming Security Operation Regulations	2/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

目次

1. はじめに	4
1.1. 本書の目的	4
1.2. 用語解説	4
1.3. 関連文書	5
1.4. 関連帳票	5
2. リプログラミングセキュリティ運用概要	6
3. 鍵(システムキー、ツール認証キー、署名検証キー)の変更条件	7
4. リプログラミングセキュリティ関連ツール利用申請	8
4.1. リプログラミングセキュリティ関連ツール概要	11
4.1.1. リプログラミングセキュリティ関連ツールのネットワーク要件	12
4.2. TMC 社内 ECU 設計部署実施事項	12
4.2.1. リプログラミングセキュリティ関連ツール社外提供契約締結フロー	12
4.2.2. リプログラミングセキュリティ関連ツール利用申請(TMC 社内設計部署)	13
4.2.3. リプログラミングセキュリティ関連ツール利用申請(TMC 社外設計部署)の承認	13
4.2.4. リプログラミングセキュリティ関連ツール利用申請(ECU ソフト開発部署)の承認	14
4.2.5. 鍵情報管理宣誓書の承認	14
4.2.6. リプログラミングセキュリティ関連ツールアカウント取得	14
4.3. TMC 社外 ECU 設計部署実施事項	14
4.3.1. リプログラミングセキュリティ関連ツール利用申請(TMC 社外設計部署)	14
4.3.2. リプログラミングセキュリティ関連ツールアカウント取得	14
4.4. ECU ソフト開発部署実施事項	14
4.4.1. リプログラミングセキュリティ関連ツール利用申請(ECU ソフト開発部署)	15
4.4.2. 鍵情報管理宣誓書	15
4.4.3. リプログラミングセキュリティ関連ツールアカウント取得	15
4.5. リプログラミングセキュリティ関連ツール申請/利用における要求事項	15
5. サービスキーの発行について	17
5.1. サービスキーの発行対象部署	17
5.2. サービスキーの発行手順	17
6. プログラム暗号化の運用手順	18

In-Vehicle Network	Reprogramming Security Operation Regulations		3/20
Application:	ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

6.1.	ECU 設計部署実施事項.....	19
6.1.1.	鍵生成機能の利用	19
6.1.2.	外部パラメータ生成機能の利用	19
6.1.3.	ECU 情報テキスト依頼書・鍵 ID の送付	19
6.2.	ECU ソフト開発部署実施事項.....	19
6.2.1.	鍵参照機能の利用	19
6.2.2.	プログラム暗号化	20
6.3.	試作時パラメータ指示書利用時の運用	20

変更履歴

仕様書 NO	変更箇所	日付	作成者
SEC-ePF-RPR-OPE-STD-S00-00-a	新規発行	2018/10/15	後藤
SEC-ePF-RPR-OPE-STD-S00-01-a	要求仕様書の機密区分変更に伴う仕様書開示依頼の削除 新システム移行に伴う運用変更	2019/9/17	橋爪
SEC-ePF-RPR-OPE-STD-S00-02-a	ツール利用申請方法の変更 ネットワークに関する案内の追加 鍵の変更条件に注記を追加	2021/3/22	永原
SEC-ePF-RPR-OPE-STD-S00-03-a	関連文書一覧、関連帳簿一覧に格納先を追加 鍵の変更条件を変更 ツール申請/利用における要求事項を変更	2022/10/10	永原

In-Vehicle Network	Reprogramming Security Operation Regulations	4/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

1. はじめに

1.1. 本書の目的

本書は標準リプログラミングセキュリティ要求仕様書を適用し、リプログラミングを実施する場合に必要な手続きについて、情報セキュリティに関わる部分のみ記載する。

1.2. 用語解説

本書で用いる略語を解説する。

表 1-1 用語一覧

用語	解説
リプログラミング	マイコンに搭載されているフラッシュメモリ内のデータを書換えること。
リプロ	リプログラミングの略語。
書き込みプログラム	リプロを行う為のソフトウェア。
平文	暗号化していない書き込みプログラム。
暗号文	暗号化した書き込みプログラム。
認証子	書き込みプログラムが不正に変更されたことを検知する為に、あらかじめ決められた方式(共通鍵暗号)で演算されたデータのこと。
MAC	認証子(Message Authentication Code)の略称。
鍵	暗号鍵とも呼ばれる。暗号化/復号を実施する時に必要なセキュリティ上最も機密性の高い秘密情報のこと。
共通鍵暗号	暗号化と復号で必要な鍵が、共通の暗号方式。対称鍵暗号とも呼ばれる。
署名	書き込みプログラムが不正に変更されたことを検知する為に、あらかじめ決められた方式(公開鍵暗号)で演算されたデータのこと。
公開鍵暗号	暗号化と復号で必要な鍵が、異なる暗号方式。非対称鍵暗号とも呼ばれる。
外部パラメータ	標準リプログラミングで使用するパラメータのこと。 本書では、セキュリティ関連の外部パラメータのことを指す。
標準リプログラミングセキュリティ要求仕様書	リプログラミングを実施する ECU が適用するセキュリティ要件を記載した仕様書。 本書では「標準リプログラミングセキュリティ要求仕様書」と「標準リプログラミングセキュリティ要求仕様書(デジタル署名版)」の両方の仕様書を指す。
ECU テキスト情報作成依頼書	標準リプログラミングで使用されるパラメータを定義するファイル。

In-Vehicle Network	Reprogramming Security Operation Regulations	5/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

1.3. 関連文書

本書の運用に関わる文書を記載する。

表 1-2 関連文書一覧

ドキュメント名	ドキュメント No.	入手先
標準リプログラミングセキュリティ要求仕様書	SEC-ePF-RPR-REQ-SPEC-a00-**	iSpirit *1
試作時パラメータ指示書	SFWSP-I00-01	iSpirit *2
試作時パラメータ指示書	SFWSP-I01-01	
リプロ鍵管理・暗号化システム 操作ガイド	v1.7	iSpirit *3

*1 Repository > Electronics_Spec > Cybersecurity > Standard > SPEC > RPR

*2 Repository > Electronics_Spec > Reprogramming Security > Standard > 30_OPER > 30_PARM

*3 Repository > Electronics_Spec > Reprogramming Security > Standard > 30_OPER > 20_Manual

1.4. 関連帳票

本書で規定する運用で使用する帳票を記載する。

表 1-3 関連帳票一覧

ドキュメント名	ドキュメント No.	送付先	入手先
セキュリティ関連ツール利用申請書(TMC 社外設計部署)	SEC-ePF-RPR-APP-DOC-S05-00-a	情報セキュリティ推進部	iSpirit *1
セキュリティ関連ツール利用申請書(ECU ソフト開発部署)	SEC-ePF-RPR-APP-DOC-S03-01-a	情報セキュリティ推進部	
鍵情報管理宣誓書	SEC-ePF-RPR-NDA-DOC-S00-01-a	情報セキュリティ推進部	
鍵発行依頼書	SEC-ePF-RPR-APP-DOC-S04-00-a	ECU 設計	
ツール提供契約締結済みリスト	—	—	
システム社外提供検討依頼書	—	情報セキュリティ推進部	T-Click *2
セキュリティ関連ツール利用申請書	—	情報セキュリティ推進部	
サービスキー指示書	GWC-CGWRPKEY-XALL-010-A	—	46F (5 章参照)

*1 Repository > Electronics_Spec > Reprogramming Security > Standard > 30_OPER > 10_SPEC

*2 全社公開 > 生産・技術 > リプログラミングセキュリティ

In-Vehicle Network	Reprogramming Security Operation Regulations	6/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

2. リプログラミングセキュリティ運用概要

本章ではリプログラミングセキュリティ運用の概要と各エンティティの役割を記載する。

ECU 設計部署・ECU ソフト開発部署・リプログラミングツール開発部署は、本書の運用規定に則り、ECU をリプロする為の暗号文作成に必要なリプロセキュリティ関連ツールの利用が必要となる。詳細な運用手順は 3 章以降を確認のこと。運用規定に則っていない申請や管理については、申請棄却・利用停止等の対応を実施する。

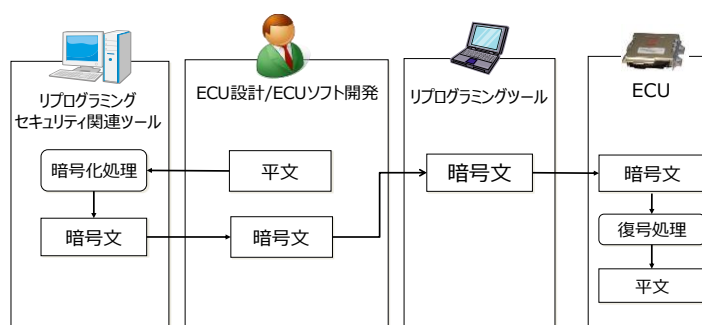


図 2-1 リプロセキュリティ運用の概要

表 2-1 各エンティティの役割

エンティティ名	役割
リプログラミングセキュリティ関連ツール	書き込みプログラムの暗号化及び、暗号化に必要なパラメータの生成をするサーバ。
ECU 設計	リプロをする ECU の開発を実施する担当。
ECU ソフト開発	書き込みプログラムを開発する担当。
リプログラミングツール	ECU をリプロする為に必要なツール。 GTS・TS-Writer を想定。

In-Vehicle Network	Reprogramming Security Operation Regulations	7/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

3. 鍵(システムキー、ツール認証キー、署名検証キー)の変更条件

本章ではリプログラミングセキュリティ関連ツールにて使用する鍵(システムキー、ツール認証キー、署名検証キー)の変更条件を記載する。

ソフトの変更があり、それにより影響範囲が増える場合、下記の表 3-1 に基づき、鍵の変更を行う。

表 3-1 鍵の変更条件

#	想定ケース	ソフト	マイコン	サプライヤ	ECUノード	車両	鍵変更	備考
0	【ベース条件】	○	○	○	○	○	－	【ベース条件】
1	マイコン変更 (バックアップ対応等)	●	●	－	－	－	推奨	・ソフト変更あり ・マイコン違いの複数ECUに影響範囲拡大
2	サプライヤ変更 (車種展開のすみわけ等)	●	－	●	－	－	推奨	・ソフト変更あり ・サプライヤ違いの複数ECUに影響範囲拡大
3	ECU変更 (別ECUにソフト転用等)	●	－	－	●	－	推奨	・ソフト変更あり ・複数ECUに影響範囲拡大
4	車両変更 新規開発 (別車両で新規ECU開発)	●	－	－	－	●	推奨	・ソフト変更あり ・複数車両に影響範囲拡大
5	車両変更 ECU流用 (別車両にECU流用)	○	○	○	○	●	任意	・ソフト変更なし ・複数車両に影響範囲拡大
6	ソフト品番変更 (巻き替え/リプロソフト等)	●	○	○	○	○	任意	・ソフト変更あり ・ソフトの巻き替えであり、影響範囲は変化なし

●：変更あり ○：変更なし

※注意事項

- ・ソフト変更とは、ロジック変更がある場合を指す。定数変更のみの場合はソフト変更なしと解釈可能。
- ・車両変更とは、車種(車両コード)に変更がある場合を指す。
- ・鍵変更推奨のケースで鍵変更が困難な場合は、鍵漏洩時のリスクを考慮の上、設計部署で変更可否を判断すること。

In-Vehicle Network	Reprogramming Security Operation Regulations	8/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

4. リプログラミングセキュリティ関連ツール利用申請

本章では、暗号文生成時に必要なパラメータの取得、及び平文の暗号化をするリプログラミングセキュリティ関連ツールの利用申請手順を記載する。

ECU 及びリプログラミングツール開発日程や評価日程を考慮し、リプログラミングセキュリティ関連ツール利用申請を行うこと。原則、標準日程での対応以外実施しない。申請から利用可能となるまで 2 ～ 3 週間を要する。

また、社外者が本ツールを利用する為には、利用契約を締結する必要があるので、4.2.1 を必ず確認し、事前に契約締結を完了させること。契約締結には 3～6 か月必要となる。

図 4-1 にリプログラミングセキュリティ関連ツール利用申請(TMC 社内設計部署)の手順、図 4-2 にリプログラミングセキュリティ関連ツール利用申請(TMC 社外設計部署/ECU ソフト開発部署)の手順、図 4-3 に鍵情報管理宣誓書の運用手順を記載する。

図 4-3 の鍵情報管理宣誓書は、鍵管理要件を記載した宣誓書である。4.1 リプログラミングセキュリティ関連ツール概要で記載する鍵参照の機能を利用する場合には必ず起票すること。

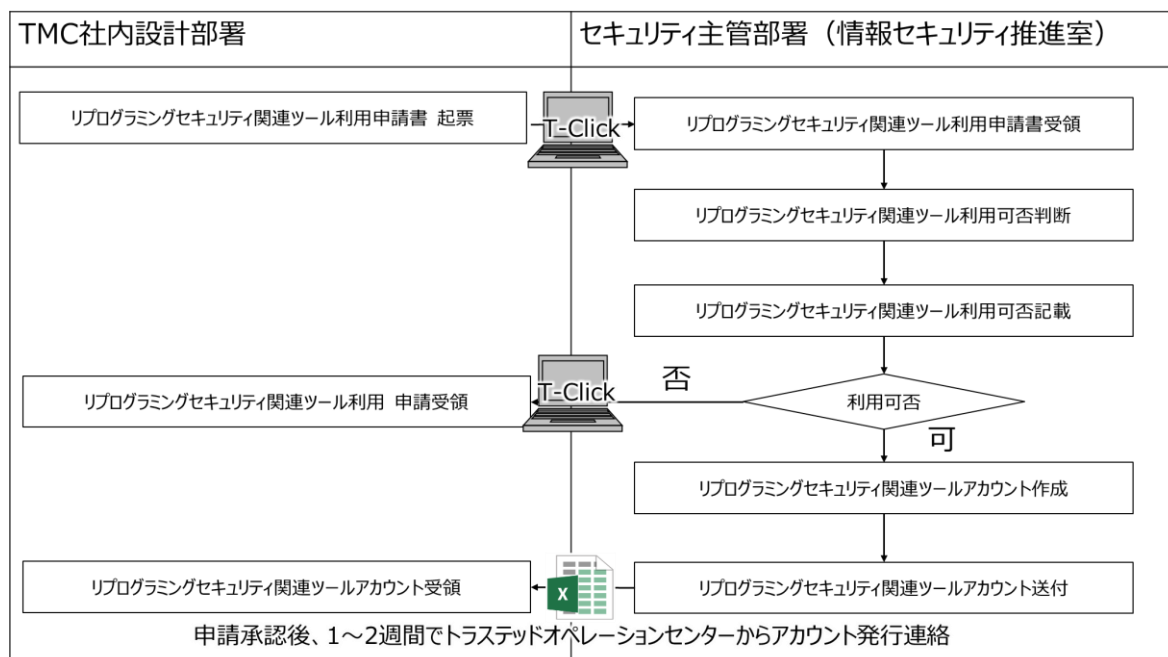


図 4-1 リプログラミングセキュリティ関連ツール利用申請(TMC 社内設計部署) 運用手順

In-Vehicle Network	Reprogramming Security Operation Regulations	9/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

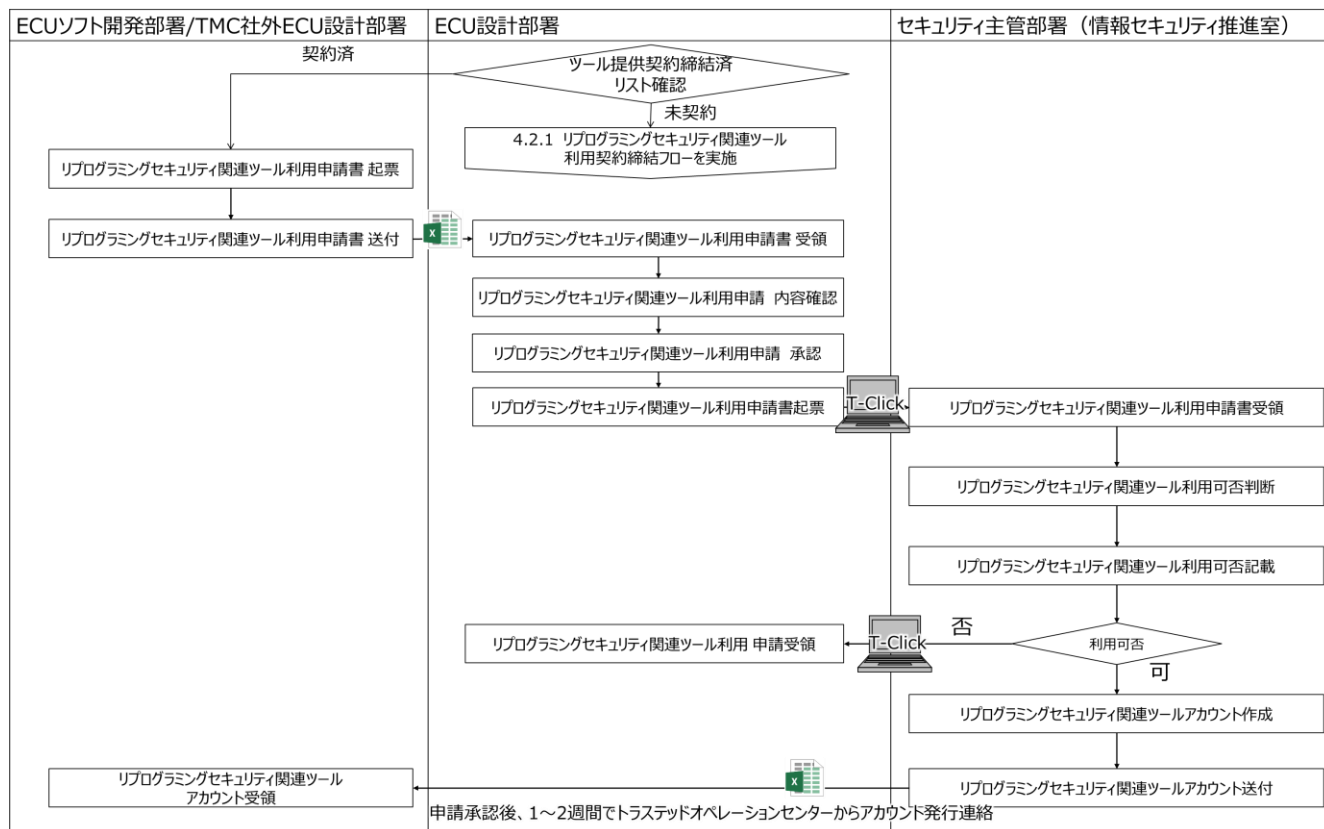


図 4-2 リプログラミングセキュリティ関連ツール利用申請(TMC 社外設計部署/ECU ソフト開発部署) 運用手順

In-Vehicle Network	Reprogramming Security Operation Regulations	10/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

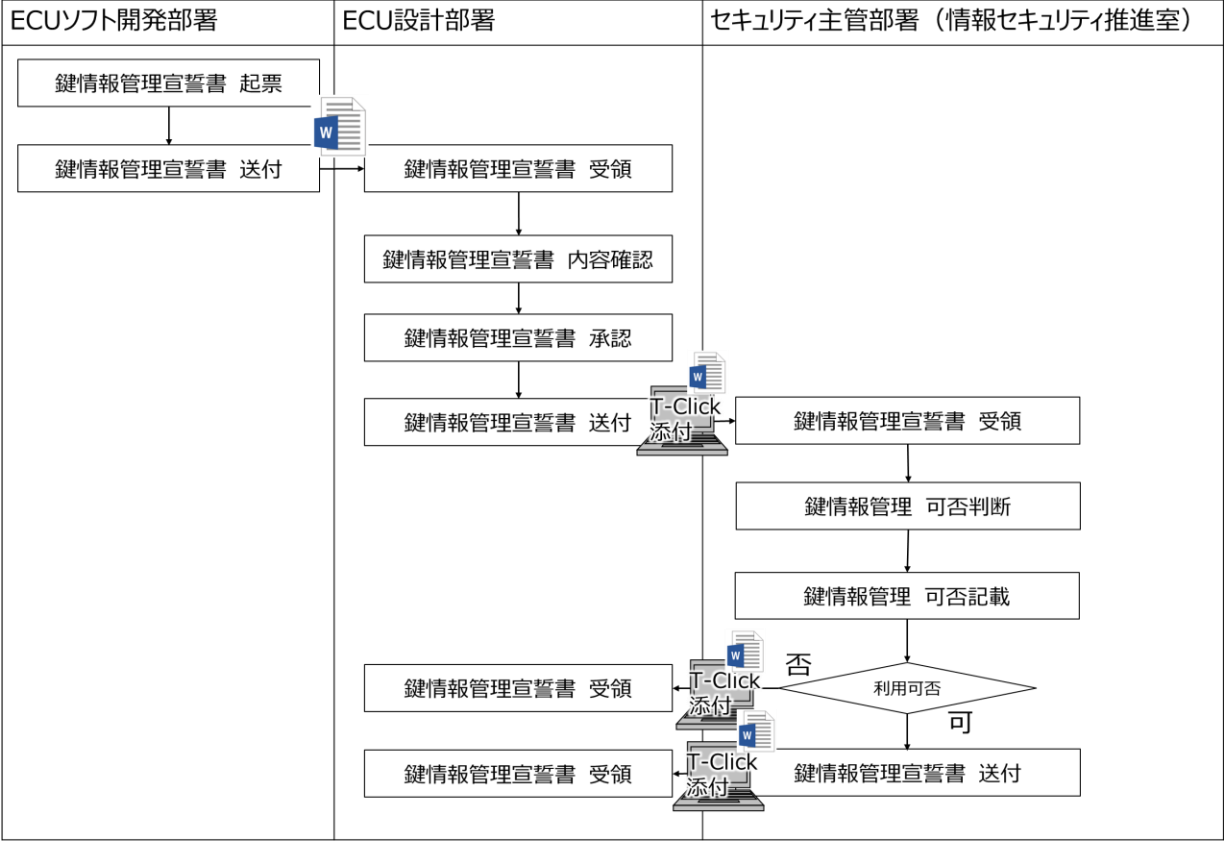


図 4-3 鍵情報管理宣誓書 運用手順

In-Vehicle Network	Reprogramming Security Operation Regulations	11/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

4.1.リプログラミングセキュリティ関連ツール概要

本節では、リプログラミングセキュリティ関連ツールの概要を記載する。図 4-4 にリプログラミングセキュリティ関連ツールの機能及び運用概要を記載する。また、表 4-1 にリプログラミングセキュリティ関連ツールの機能詳細を記載する。
鍵 ID は、標準リプログラミングセキュリティ要求仕様書で定義する鍵の種類毎に存在するので、該当仕様書とリプロ用セキュリティ関連ツール操作マニュアルを確認し、正しく発行及び入力を実施すること。

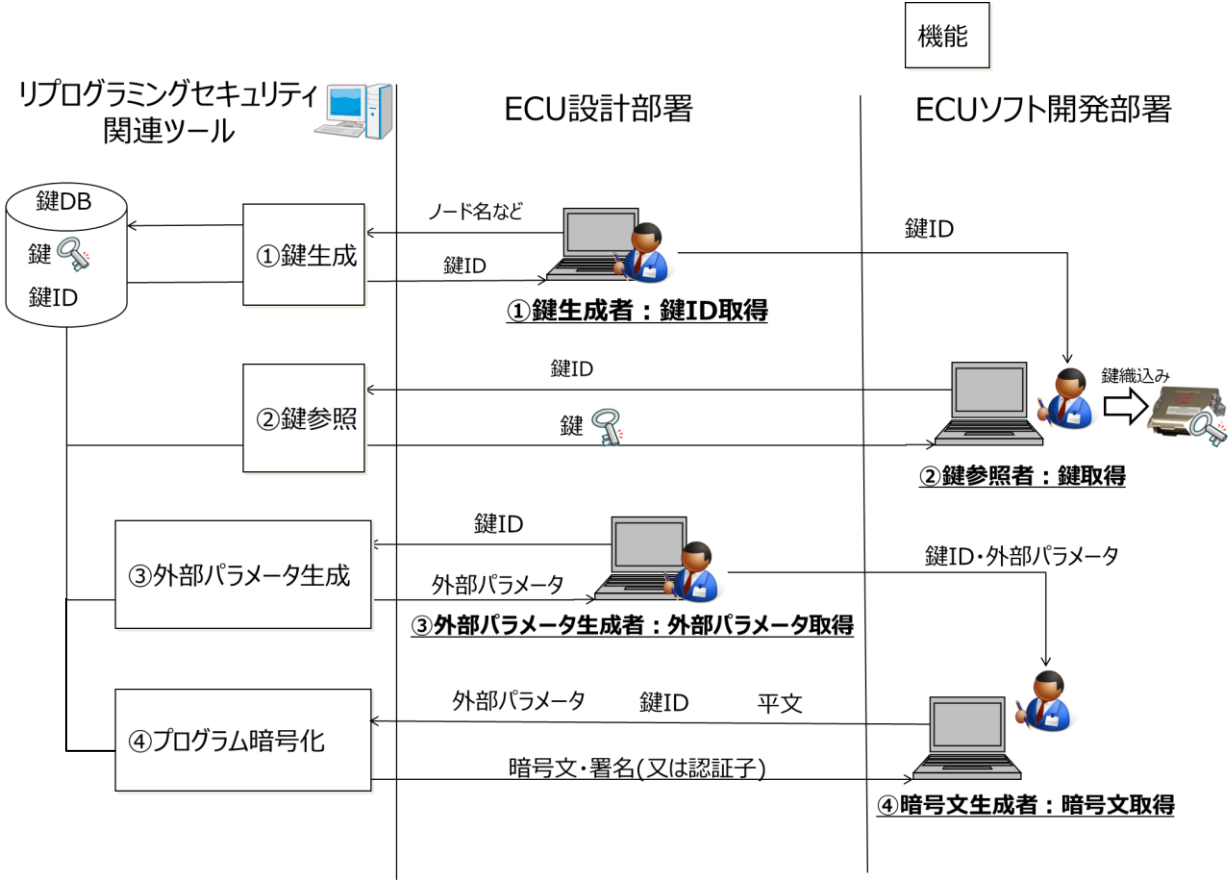


図 4-4 リプログラミングセキュリティ関連ツールの機能及び運用概要

表 4-1 リプログラミングセキュリティ関連ツールの機能詳細

機能	役割
鍵生成	暗号文作成に必要な鍵を生成する機能。本機能利用者は鍵に紐付いた鍵 ID を取得する。
鍵参照	鍵値を取得する機能。本機能利用者は、鍵生成者が発行した鍵 ID を利用して鍵を取得する。
外部パラメータ生成	リプロするのに必要な外部パラメータを生成する機能。 鍵生成時に発行した鍵 ID を利用すること。
プログラム暗号化	鍵生成・外部パラメータ生成で発行したパラメータを利用して、暗号文を作成する機能。 鍵 ID・外部パラメータ・平文を入力することで暗号文の生成・取得を行う。

In-Vehicle Network	Reprogramming Security Operation Regulations		12/20
Application:	ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

4.1.1. リプログラミングセキュリティ関連ツールのネットワーク要件

社外から本ツールを使用する場合には、リプログラミングセキュリティ関連ツールは社内イントラネットに接続できる環境、具体的には De-net、TGN、JNX、TGEMS いずれかのネットワークが配備されている必要がある。事前に左記のネットワークが配備されていることを確認すること。

ネットワークが配備されていない場合は、別途ネットワークサービスの契約が必要になるため、リプロセキュリティ関連ツール運用窓口（表紙記載）に相談すること。

4.2.TMC 社内 ECU 設計部署実施事項

本節では TMC 社内 ECU 設計部署で実施する内容を記載する。

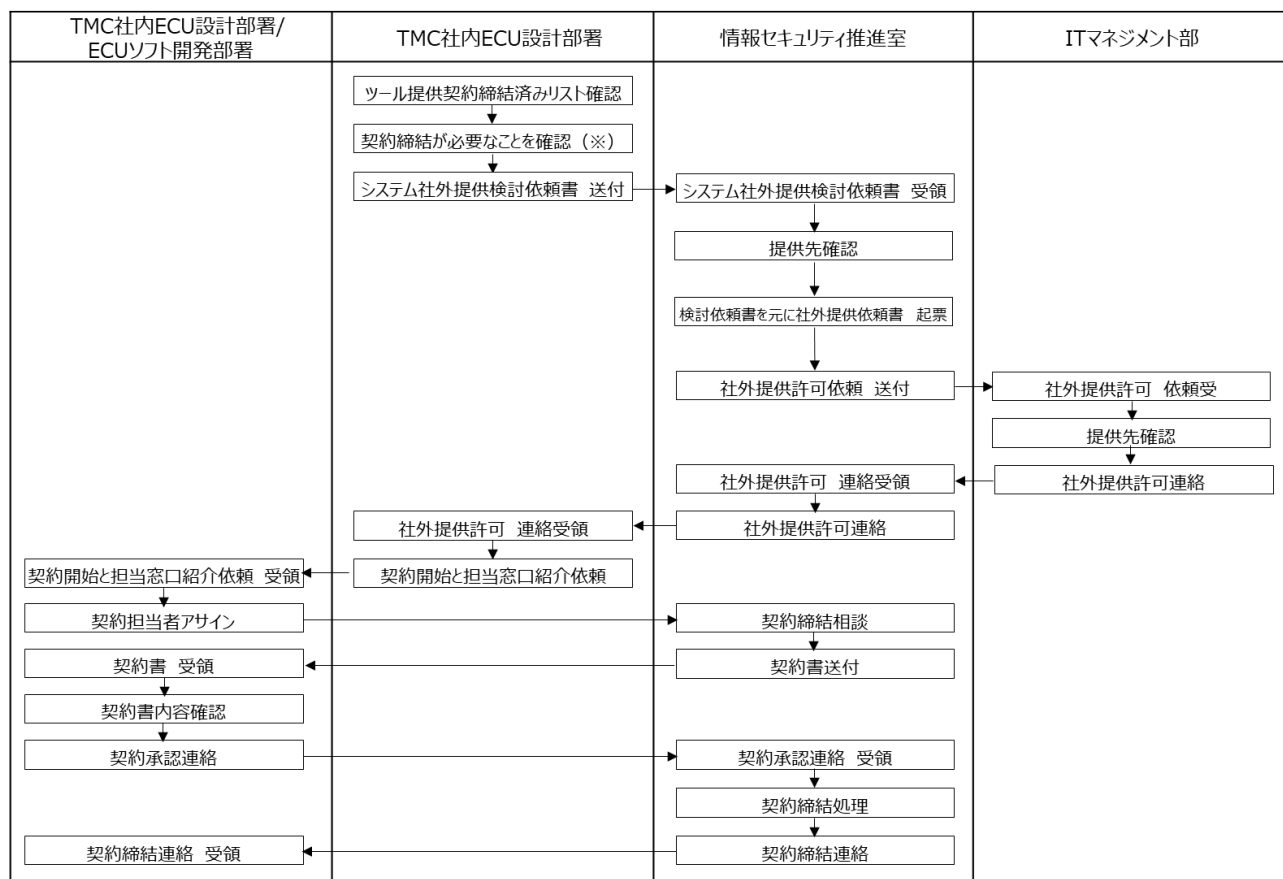
4.2.1. リプログラミングセキュリティ関連ツール社外提供契約締結フロー

図 4-5 にリプログラミングセキュリティ関連ツール社外提供契約締結フローを記載する。

TMC 社内 ECU 設計部署は、TMC 社外 ECU 設計部署/ECU ソフト開発部署が、「ツール提供契約締結済みリスト」に登録されているか確認する。登録されていない場合は、リプロセキュリティ関連ツール運用窓口（表紙記載）に連絡し提供先と契約を締結すること。

契約締結後は、4.2.2 以降の運用手順を実施する。

In-Vehicle Network	Reprogramming Security Operation Regulations	13/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a



(※)ツール提供先契約締結済みリストを確認し、契約締結済の会社である場合は本フロー対象外

図 4-5 リプログラミングセキュリティ関連ツール社外提供契約締結フロー

4.2.2. リプログラミングセキュリティ関連ツール利用申請(TMC 社内設計部署)

TMC 社内 ECU 設計部署は「リプロ鍵管理・暗号化システム利用申請書」(T-Click)に必要事項を記入後、セキュリティ主管部署に回送し、鍵生成と外部パラメータ生成機能の利用申請をする。「4.5 リプログラミングセキュリティ関連ツール申請/利用における要求事項」に記載の要求事項に同意の上でセキュリティ主管部署に回送すること。

4.2.3. リプログラミングセキュリティ関連ツール利用申請(TMC 社外設計部署)の承認

TMC 社内 ECU 設計部署は、TMC 社外 ECU 設計部署が起票した「リプログラミングセキュリティ関連ツール利用申請書(TMC 社外設計部署)」を TMC 社外 ECU 設計部署から受領した時に、「4.5 リプログラミングセキュリティ関連ツール申請/利用における要求事項」に記載の要求事項に同意の上で、「リプロ鍵管理・暗号化システム利用申請書」(T-Click)に必要事項を記入後、セキュリティ主管部署に回送すること。

In-Vehicle Network	Reprogramming Security Operation Regulations		14/20
Application:	ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

4.2.4. リプログラミングセキュリティ関連ツール利用申請(ECU ソフト開発部署)の承認

TMC 社内 ECU 設計部署は、ECU ソフト開発部署が起票した「リプログラミングセキュリティ関連ツール利用申請書 (ECU ソフト開発部署)」を ECU 開発部署から受領した時に、「4.5 リプログラミングセキュリティ関連ツール申請/利用における要求事項」に記載の要求事項に同意の上で、「リプロ鍵管理・暗号化システム利用申請書」(T-Click) に必要事項を記入後、セキュリティ主管部署に回送すること。

4.2.5. 鍵情報管理宣誓書の承認

TMC 社内 ECU 設計部署は「鍵情報管理宣誓書」を ECU ソフト開発部署から受領した時、鍵情報管理宣誓書に記載された宣誓者が鍵情報管理宣誓書の同意事項を守れることの確認と、「鍵情報管理宣誓書」に記載された鍵情報を扱う上での要求に同意の上で、承認を行い、リプログラミングセキュリティ関連ツール利用申請時に添付し、セキュリティ主管部署に回送すること。

4.2.6. リプログラミングセキュリティ関連ツールアカウント取得

セキュリティ主管部署から TMC 社内 ECU 設計部署にリプログラミングセキュリティ関連ツールの利用許可連絡、及び URL・ユーザ ID・初期パスワードが送付される。URL・ユーザ ID・初期パスワードはリプログラミングセキュリティ関連ツールの利用に必要なので、必ず取扱いに注意し、大切に保管すること。

4.3.TMC 社外 ECU 設計部署実施事項

本節では TMC 社外 ECU 設計部署で実施する内容を記載する。

4.3.1. リプログラミングセキュリティ関連ツール利用申請(TMC 社外設計部署)

TMC 社外 ECU 設計部署は「リプログラミングセキュリティ関連ツール利用申請書(TMC 社外設計部署)」に必要事項を記入後、TMC 社内 ECU 設計部署に送付し、鍵生成と外部パラメータ生成機能の利用申請をする。ECU 設計部署は「4.5 リプログラミングセキュリティ関連ツール申請/利用における要求事項」に同意の上で、「リプロ鍵管理・暗号化システム利用申請書」(T-Click)に必要事項を記入後、セキュリティ主管部署に回送すること。

4.3.2. リプログラミングセキュリティ関連ツールアカウント取得

セキュリティ主管部署から TMC 社外 ECU 設計部署にリプログラミングセキュリティ関連ツールの利用許可連絡、および URL・ユーザ ID・初期パスワードが送付される。URL・ユーザ ID・初期パスワードはリプログラミングセキュリティ関連ツールの利用に必要なので、必ず取扱いに注意し、大切に保管すること。

4.4.ECU ソフト開発部署実施事項

In-Vehicle Network	Reprogramming Security Operation Regulations	15/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

本節では ECU ソフト開発部署で実施する内容を記載する。

4.4.1. リプログラミングセキュリティ関連ツール利用申請(ECU ソフト開発部署)

ECU ソフト開発部署は「リプログラミングセキュリティ関連ツール利用申請書(ECU ソフト開発部署)」に必要事項を記入後、TMC 社内 ECU 設計部署に送付し、鍵参照とプログラム暗号化機能の利用申請をする。ただし、鍵参照機能の利用申請は鍵情報管理宣誓書の申請後とする。TMC 社内 ECU 設計部署は「4.5 リプログラミングセキュリティ関連ツール申請/利用における要求事項」に同意の上で、「リプロ鍵管理・暗号化システム利用申請書」(T-Click)に必要事項を記入後、セキュリティ主管部署に回送すること。

4.4.2. 鍵情報管理宣誓書

ECU ソフト開発部署は「鍵情報管理宣誓書」に必要事項を記入後、TMC 社内 ECU 設計部署 に送付する。

4.4.3. リプログラミングセキュリティ関連ツールアカウント取得

セキュリティ主管部署から ECU ソフト開発部署にリプログラミングセキュリティ関連ツールの利用許可連絡、および URL・ユーザ ID・初期パスワードが送付される。URL・ユーザ ID・初期パスワードはリプログラミングセキュリティ関連ツールの利用に必要なので、必ず取扱いに注意し、大切に保管すること。

4.5. リプログラミングセキュリティ関連ツール申請/利用における要求事項

リプログラミングセキュリティ管理ツールを申請/利用するにあたって、TMC 社内 ECU 設計部署は以下の要求事項を遵守すること。

TMC 社外 ECU 設計部署/ECU ソフト開発部署がツールを利用する場合には、TMC 社内 ECU 設計部署が以下の要求事項を周知し、遵守を徹底させること。

● 共通

- ・運用規定を確認済みであること
- ・本ツールのアカウントを申請者以外の第 3 者に開示しないこと
- ・本ツールの利用目的は設計担当 ECU のリプロセキュリティ開発に限ること
- ・上記以外の利用目的については主管部署に問い合わせ、主管部署承認を得た上で特記事項に記載すること
- ・本ツールを利用して拾得した個人情報・秘密情報の運用・管理の責任は担当者及び設計担当部署が担い、情報が漏えいしないように注力すること
- ・本ツールの申請者を変更（担当者の変更）する際は、以下の表に従って手続きを実施すること

変更内容	変更方法
利用申請者の変更	T-Click
利用機能の変更	T-Click
メールアドレスのみ変更	リプロセキュリティ関連ツール運用窓口（表紙記載）にメールで申請

In-Vehicle Network	Reprogramming Security Operation Regulations	16/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

会社名変更	変更先の会社がツール提供契約締結済みリストに記載があることを確認後、 <u>リプロセキュリティ関連ツール運用窓口（表紙記載）</u> にメールで申請
-------	--

●個人情報の取得および利用について

利用申請書に記載された個人情報（氏名、連絡先）に関しては以下のように取り決める。

利用申請書が申請された時点で利用者の同意を得たものとみなす。

1)以下の利用目的で利用される。

- ・システム利用に関する連絡に氏名・連絡先を利用する
- ・生成した鍵の公開先の指定に氏名を利用する

2)鍵管理センタおよびツール運用窓口において管理責任者を定め、紛失・漏洩がないよう管理を行う。

3)鍵検索機能を利用する場合、本システムの鍵生成画面において鍵の公開先の選択肢として会社名および氏名を公開する。

4)利用申請にて削除申請があった場合には、取得した個人情報を破棄する。

問い合わせ先：リプロセキュリティ関連ツール運用窓口（表紙記載）

●利用者が TMC 社外の場合

- ・本ツールの利用者が所属する会社は TMC とツール提供契約を締結していること

●鍵参照機能を申請する場合

- ・鍵参照機能の利用者は鍵情報管理宣誓書を添付して申請すること。また、セキュリティ上の理由から

鍵参照機能の利用者は 1 名または 2 名に限定すること。3 名以上で利用する場合は

リプロセキュリティ関連ツール運用窓口（表紙記載）に相談すること

●GM 承認で申請する場合

- ・承認者(GM)に室長権限が委譲されていること

In-Vehicle Network	Reprogramming Security Operation Regulations	17/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

5. サービスキーの発行について

本章では、リプログラミングツールの開発に必要な鍵であるサービスキーの開示について記載する。サービスキーは ECU 設計部署（TMC 社内/TMC 社外）及び、ECU ソフト開発部署では不必要な鍵である。

5.1. サービスキーの発行対象部署

サービスキーはリプログラミングを実施するツールへの適用する暗号鍵であり、原則 TMC 標準のリプログラミングツールへの配布以外認めないものとする。配布が必要な上記以外の部署はセキュリティ主管部署に連絡すること。

5.2. サービスキーの発行手順

5.1 でサービスキーの配布許可を得た部署は鍵情報管理宣誓書の運用手順と同等の手順を実施し、宣誓者をセキュリティ主管部署へ申請する。

セキュリティ主管部署で問題ないと判断された場合は、サービスキー開示許可連絡とサービスキー指示書の送付が行われる。

In-Vehicle Network	Reprogramming Security Operation Regulations	18/20
Application: ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

6. プログラム暗号化の運用手順

本章は、プログラム暗号化までの各パラメータの運用手順を記載する。5 章までの運用手順が終了後に本章の運用手順を実施すること。また、プログラム暗号化に必要なリプログラミングセキュリティ関連ツールの機能については、4.1 リプログラミングセキュリティ関連ツール概要を確認すること。また、図 6-1 にプログラム暗号化の手順を記載する。差分・圧縮プログラムの暗号化の際にも同じ手順を実施する。

鍵 ID は、標準リプログラミングセキュリティ要求仕様書で定義する鍵の種類毎に存在するので、該当仕様書とリプロ用セキュリティ関連ツールの操作マニュアルを確認し、正しく発行及び入力を実施すること。

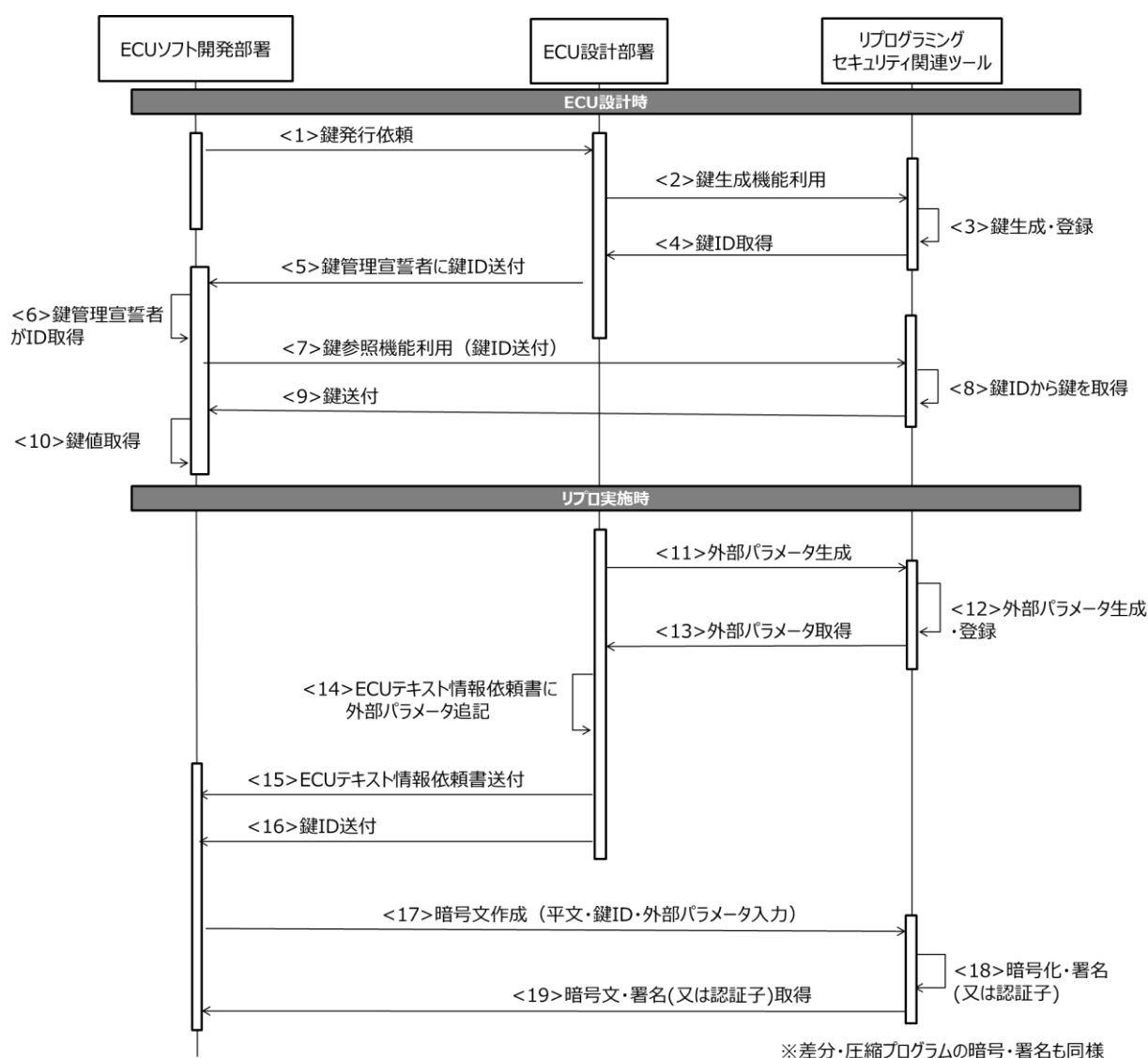


図 6-1 プログラム暗号化運用手順

In-Vehicle Network	Reprogramming Security Operation Regulations		19/20
Application:	ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

6.1.ECU 設計部署実施事項

本節では ECU 設計部署（TMC 社内/TMC 社外）で実施する内容を記載する。

6.1.1. 鍵生成機能の利用

ECU ソフト開発部署から鍵の発行依頼を受領した時に、リプログラミングセキュリティ関連ツールの鍵生成機能を利用して、鍵の生成を実施する。鍵生成機能の利用により、リプログラミングセキュリティ関連ツールに鍵の登録と ID の発行がされる。発行された鍵の ID を取得し、ECU ソフト開発部署に送付する。

送付先は下記 2 担当者とする。

<1>鍵情報管理宣誓者

ECU 開発時に暗号鍵の織込みが必要となるので、鍵情報管理宣誓書で承諾された担当者に鍵 ID を送付し、鍵参照機能が利用できるようにする。

<2>プログラム暗号化担当者

平文の暗号化に鍵 ID が必要となるので、「リプログラミングセキュリティ関連ツール利用申請（TMC 社外設計部署）」で承諾された担当者に鍵 ID を送付する。

6.1.2. 外部パラメータ生成機能の利用

ECU 設計部署（TMC 社内/TMC 社外）は、平文の暗号化に必要な外部パラメータを、リプログラミングセキュリティ関連ツールの外部パラメータ生成機能を利用して生成する。生成した外部パラメータは ECU テキスト情報作成依頼書に記載する。ECU テキスト情報作成依頼書は、セキュリティで使用する外部パラメータ以外にも、リプロをする為に記載する外部パラメータがあるので、必ず全て記載すること。

6.1.3. ECU 情報テキスト依頼書・鍵 ID の送付

ECU ソフト開発部署で平文を暗号化するために、リプロに必要な外部パラメータを記載した ECU テキスト情報作成依頼書と鍵 ID をプログラム暗号化の担当者に送付する。

6.2.ECU ソフト開発部署実施事項

本節では ECU ソフト開発部署で実施する内容を記載する。

6.2.1. 鍵参照機能の利用

ECU ソフト開発部署の鍵情報管理宣誓者は、ECU 設計部署（TMC 社内/TMC 社外）から鍵 ID を受け取り、ECU 開発に必要な鍵をリプログラミングセキュリティ関連ツールの鍵参照機能を利用し、取得する。

In-Vehicle Network	Reprogramming Security Operation Regulations		20/20
Application:	ECU of In-Vehicle network	No.	SEC-ePF-RPR-OPE-STD-S00-03-a

6.2.2. プログラム暗号化

ECU ソフト開発部署は、ECU 設計部署（TMC 社内/TMC 社外）から ECU テキスト情報作成依頼書と鍵 ID を受け取り、平文と共にリプログラミングセキュリティ関連ツールのプログラム暗号化機能を利用して、平文の暗号化を行い、暗号文を取得する。

6.3. 試作時パラメータ指示書利用時の運用

試作時パラメータ指示書は、鍵の値及び、リプログラミングセキュリティに必要な外部パラメータの指示をしている。本指示書を利用する場合は、鍵値及び外部パラメータの取得が不要となるので、プログラム暗号化機能を利用して、平文の暗号化を実施する。