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　/

車載個人・プライバシー情報 削除要求仕様書 Deletion Requirement Specifications of In-vehicle Personal and Privacy 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 4G System Network & Architecture Development Dept. 4G E/E Architecture Development Div			
	No. PPI-ePF-DLT-REQ-SPEC-a00-02-a			
	承認 Approved by 河井	調査 Checked by 平井 垣屋	作成 Created by 山川	2023/05/31

適用先 Target	個人情報・プライバシーに関わる情報を不揮発メモリ*1に保存する ECU *1 不揮発性メモリの定義については用語集を参照のこと ECUs that store personal and privacy information in non-volatile memory*1. *1 See Terminology for definition of non-volatile memory.
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 specification to affiliated companies, or departments (e.g., overseas business entities, car body manufacturers, or ECU suppliers) if necessary. 【問合せ先　Contact Information】 本仕様に関する社外からの問合せは TMC 設計部署にて対応をお願いします。 Inquiries about this specification from ECU suppliers should be handled by TMC design department. 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. http://team-adsp.kitora.toyota.co.jp/sites/cybersecurity/SitePages/Sec_Contact2.aspx

変更履歴

Marks	Version	変更内容	日付	変更者
–	a00-00-a	新規作成	2022/10/31	勝部
△1	a00-00-b	英訳追加 “図　2.2.2　ディーラ操作による PI 削除の動作シーケンス”の、対象 ECU の補足説明を追加	2022/12/8	垣屋 勝部
△2	a00-01-a	・削除処理のタイムアウト時間の規定 ・【要求事項：PPIDLR_02029】を追加 ・削除要求を通知する信号（CAN）を反映 ・物理消去の対象範囲の明確化 ・Phase6 ダイアグ通信仕様との乖離を訂正 ・走行中の安全措置を、要件から補足に変更【PPIDLR_01004】 ・不揮発性メモリの定義を明確化 ・誤記修正(状態遷移表、Phase5 ダイアグ通信)	2023/2/28	垣屋 勝部
△3	a00-02-a	1.2.適用範囲　更新 1.7.個人プライバシー情報と重要度の設定　追加 2.1.システム構成　更新 2.3.要求一覧　更新 3.1.2.本書の対象範囲　更新 3.1.3.対象機能の実装要否条件　更新 3.1.4.　PI 削除の対象情報について更新 3.3.3.　　対象 ECU の要件について更新	2023/5/31	山川

目次

1. はじめに

1.1. 本書の目的

本書は上位文書[1]に基づき、各 ECU において実施しなければならない要件を示す。

1.2. 適用範囲

本書の適用範囲は、19PF ver3[△3]で車載ネットワークに接続され、個人情報・プライバシーに関わる情報を不揮発メモリに保存する ECU とする。

1.3. 要求事項の記載

【要求事項：PPIDLR_*****】と記載されている部分が本書の要件とする。ただし、（補足）と記載されているものは補足事項のため要件ではない。

1.4. 上位文書

本書の上位文書を以下に示す。

表 1-1 上位文書[△2]

No	仕様書	Ver(最新版を適用ください)	主管
[1]	車両プライバシー要件	TPR-RVe0001	情トラ部 ※1-1

※1-1：情報セキュリティ・トラスト部　プライバシーガバナンス G

1.5. 関連文書

本書の関連文書を以下に示す。

表 1-2 関連文書一覧

No	文書名	Ver(最新版を適用ください)	主管
[A]	Diagnostic design specification UDS Protocol		46F7G
[B]	RoutineControl service 標準仕様書 (sid31-rd***)		46F7G
[C]	車載個人・プライバシー情報 共通対策要求仕様書	SEC-ePF-PCC-REQ-SPEC	46F

表 1-3　公的関連文書一覧

略称	名称/外部リンク
OECD8 原則	プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告(Sep. 2013) 第 2 部 国内適用における基本原則 Recommendation of the Council concerning Guidelines Governing the Protection of Personal Data PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION Microsoft Word - Modernising priv framework.docx (oecd.org)
ISO/IEC29100	ISO/IEC 29100:2011(Dec. 2011) 情報技術-セキュリティ-プライバシーの枠組み Information technology - Security techniques - Privacy framework
GDPR	REGULATION(EU) 2016/679 OF THE EUROPEAN AND OF THE COUNCIL of 27 April 2016 本文 EUR-Lex - 02016R0679-20160504 - EN - EUR-Lex (europa.eu) 仮日本語訳 https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/
GDPR ガイドライン	Guidelines 05/2020 on consent under Regulation 2016/679 仮日本語訳 https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/
日本法規	個人情報の保護に関する法律（令和 4 年時点） https://www.ppc.go.jp/personalinfo/legal/
日本法規ガイドライン	各種ガイドライン・QA https://www.ppc.go.jp/personalinfo/legal/
中国法規	・中華人民共和国個人情報保護法(2021.8.20) ・自動車データ安全管理の若干規定(試行)
中国 GBT	・情報安全技術　個人情報安全規範
CCPA (カリフォルニア消費者プライバシー法)	California Consumer Privacy Act of 2018 仮日本語訳 https://www.ppc.go.jp/enforcement/infoprovision/laws/CCPA/

1.6. 用語集

表 1-4 用語一覧△2

用語	説明
PI	“個人情報・プライバシーに関わる情報”の略称
ユーザ	車両を使用されるお客様
データ主体	識別された自然人又は識別可能な自然人（本人）
不揮発性メモリ	一般的には電源が供給されなくてもデータを保持できるメモリを指すが、本書では IG/ACC OFF 時に+B 電源でデータを保持するメモリも不揮発性として扱う

1.7. 個人情報・プライバシーに関わる情報と重要度の設定△3

個人情報・プライバシーに関わる情報とは関連文書[C]の Appendix.A に示すカテゴリー番号 1～10 番の情報である。重要度とはカテゴリーごとに付与される値であり、具体的な値は Appendix.A の「重要度」の列を参照されたい。△3

2. 要求概要

2.1. システム構成

本仕様書でプライバシー要求を定義するにあたり前提となる構成を図　2-1　本システムの構成に示す。また、構成要素の説明を表　2-1　構成要素の説明△3に示す。

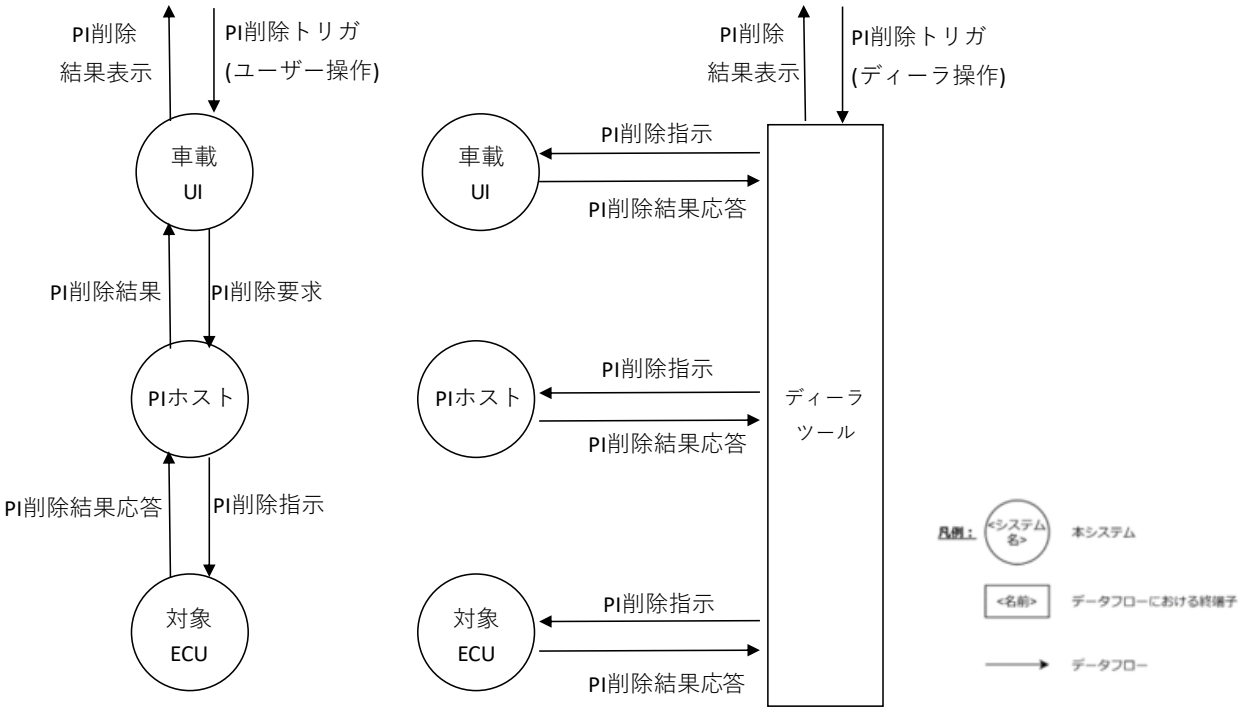

図　2-1　本システムの構成

表　2-1　構成要素の説明△3

構成要素	説明
車載 UI	ユーザ操作による PI 削除トリガを取得するための UI を持つ ECU。19PF ver3 ではマルチメディア
PI ホスト	PI 削除指示を、複数の対象 ECU に伝達するホスト
対象 ECU	削除対象の PI を保存しており、PI 削除指示を受けて PI の削除を実施する ECU
ディーラツール	ディーラ操作による PI 削除トリガを取得するための UI を提供する、 かつ、PI 削除指示を、複数の対象 ECU に伝達するツール

2.2. 動作シーケンス

本仕様の動作シーケンスを以下に示す。

2.2.1. ユーザ操作による PI 削除の動作シーケンス

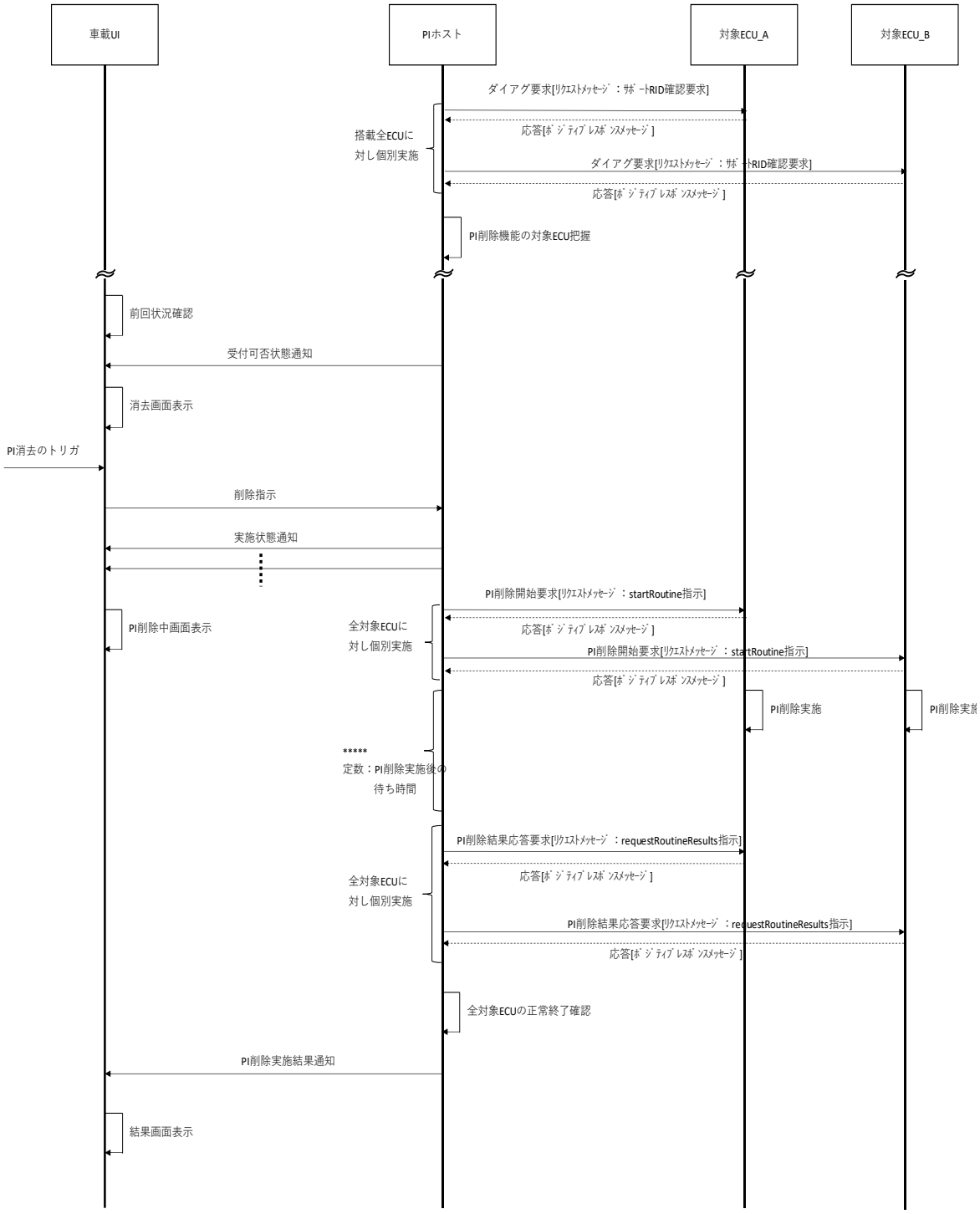

図　2.2.1　ユーザ操作による PI 削除の動作シーケンス△2

2.2.2. ディーラ操作による PI 削除の動作シーケンス

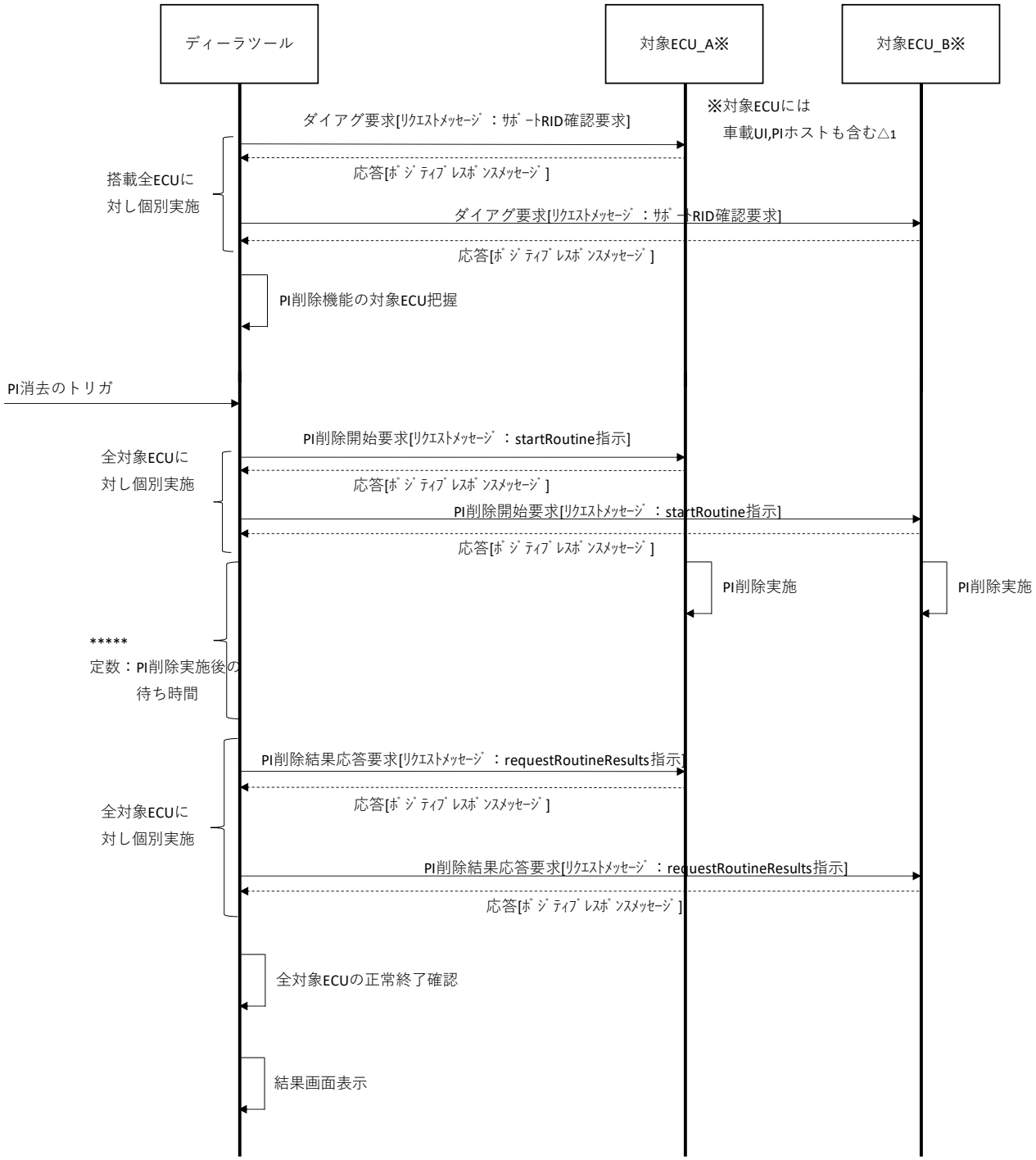

図　2.2.2　ディーラ操作による PI 削除の動作シーケンス△1△2

2.3. 要求一覧

各構成要素[△3]が対応すべき要求事項の一覧を表 2 に示す。(凡例 ○：適用 −:非適用)

要求事項の詳細については、3 章以降を参照。

表 2-2[△3] 要求事項対応表[△2]

要求事項番号	車載 UI	PI ホスト ※19PF ver3 では不在[△3]	対象 ECU
PPIDLR_01001	○	○	○
PPIDLR_01002	○	○	○
PPIDLR_01003	○	○	○
PPIDLR_01004	削除	削除	削除
PPIDLR_02001	−	○	−
PPIDLR_02002	−	−	○
PPIDLR_02003	−	○	−
PPIDLR_02004	−[△3]	−	−
PPIDLR_02005	−[△3]	−	−
PPIDLR_02006	−[△3]	−	−
PPIDLR_02007	−	○	−
PPIDLR_02008	−	○	−
PPIDLR_02009	−[△3]	−	−
PPIDLR_02010	−[△3]	−	−
PPIDLR_02011	−[△3]	−	−
PPIDLR_02012	−[△3]	−	−
PPIDLR_02013	−[△3]	−	−
PPIDLR_02014	−[△3]	−	−
PPIDLR_02015	−	○	−
PPIDLR_02016	○	○	○
PPIDLR_02017	○	○	○
PPIDLR_02029	○	○	○
PPIDLR_02018	○	○	○
PPIDLR_02019	○	○	○
PPIDLR_02020	○	○	○
PPIDLR_02021	○	○	○
PPIDLR_02022	○	○	○
PPIDLR_02023	○	○	○

PPIDLR_02024	○	○	○
PPIDLR_02025	○	○	○
PPIDLR_02026	○	○	○
PPIDLR_02027	○	○	○
PPIDLR_02028	○	○	○
PPIDLR_03001	○	○	○

3. 機能要求詳細

3.1. 個人・プライバシー情報の削除機能要件

3.1.1. 説明

個人・プライバシー情報の削除機能は、車両内で保存している PI を、ユーザの要望によって削除できる機能である。

3.1.2. 本書の対象範囲

本書は、車両内で実現される標準の PI 削除機能について記載する。

そのため、下記については本書の対象範囲外とする

・車両外で保存している PI（サーバーなど）の削除に関する機能

3.1.3. 対象機能の実装要否条件

【要求事項：PPIDLR_01001】

車載 UI は、自身が保存している PI を、自身の UI で取得されるユーザの要望に応じて、物理削除(※1)すること。さらに、車載 UI は、自身が保存している PI を、3.3 の機能(※2,※3)で物理削除(※1)すること。

車載 UI 以外の対象 ECU は、自身が保存している PI を、ディーラツールからの要望に応じて、3.3 の機能で物理削除(※1)すること。※4△3

ただし、重要度 B 以下の情報は、物理削除は必須ではなく、通常の消去（メモリ上のデータ本体は残っている状態）を許容する。△2

※1：物理削除とは、データが容易に復元できないよう全て”1 or 0”で上書きするなどの処理を指す。

※2：ディーラでの操作による削除を実装する場合、お客様に対し、ディーラで削除可能な旨をオーナーズマニュアル等で連絡すること。

※3：ダイアグコマンド指示に対応できない ECU については、特殊操作（例：物理ボタンの同時長押しなど）による削除機能に対応しても良いものとする。

※4：19PF ver3 では 3.2 の機能を用いた PI 物理削除を見送る。次期 e-PF では 3.2 の機能を用いた PI 物理削除を必須とする△3

3.1.4. PI 削除の対象情報について

【要求事項：PPIDLR_01002】

PI の削除対象情報とは関連文書[C]の Appendix.A に示す削除欄で「○」のカテゴリー（カテゴリー番号 1～7 番）の情報である。ただし関連文書[C]の Appendix.A の「表 A-1.削除対象外にできるデータ」は削除の対象外としてもよい。

3.1.5. PI 削除途中での中断について

【要求事項：PPIDLR_01003】

PI 削除処理の途中に ECU の起動電源（ACC/IG など）が OFF になった場合には、可能な限り処理を継続し完了させること。継続が不可能で、やむを得ず中断する場合には、処理中であったデータの保全を行うこと（インデックスの維持などを実施し、中断によるデータ破損を発生させないこと。）

3.1.6. 走行中の PI 削除動作について

（補足）△2PI 削除処理の途中に、車両が走行状態となった場合でも、PI 削除動作によって安全性を損なう動作に至らせないこと。

3.2. ユーザ操作による PI 削除機能

3.2.1. 説明

ユーザ操作による PI 削除機能は、19PFver3 では採用を見送る。19PFver3 において対象外とする要求事項の詳細は、2.3 章を参照。△3

ユーザ操作による PI 削除機能は、UI(マルチメディアなど)を提供することで、車両内でのユーザ操作による PI 削除を実現する機能である。

3.2.2. PI 削除指示画面処理

3.2.2.1. 対象 ECU の把握

【要求事項：PPIDLR_02001】

PI ホストは、搭載全 ECU に対し、
サポート RID 確認要求(RID$1000(Phase5)/RID$D1D9(Phase6))を送信することで
PI 削除機能の対象 ECU を事前に把握すること。△2

【要求事項：PPIDLR_02002】

PI 削除機能の対象 ECU は、
サポート RID 確認要求(RID$1000(Phase5)/RID$D1D9(Phase6))をサポートすること。△2

3.2.2.2. PI 削除要求の受付可否状態通知

【要求事項：PPIDLR_02003】

PI ホストは、車載 UI に対し下記データラベルにて PI 削除要求の受付可否状態を送信すること。

データラベル：PIDLT_ACEPT△2

（補足）：PI 削除要求の受付可否状態：1bit(0:受付不可能、1:受付可能)
Event&Periodic

3.2.2.3. PI 削除指示画面の表示

【要求事項：PPIDLR_02004】

車載 UI は、3.2.2.2.の信号の受信状態によって、PI 削除指示画面及び処理を切り替えること。

（補足）：PI ホストの存在有無、PI ホストの起動処理などに伴う処理受付可否状態を判断する。

3.2.2.4. PI 削除要求の再確認画面の表示

【要求事項：PPIDLR_02005】

車載 UI は、ユーザが PI 削除要求ボタンを押下した際に、ユーザに対し再確認画面を表示すること。

（補足）：記録データがリセットされ、一部の機能が初期状態に戻る場合があるため、ユーザに削除意思の再確認を実施する。

3.2.2.5. PI 削除要求の送信

【要求事項：PPIDLR_02006】

車載 UI は、PI ホストに対し下記データラベルにて PI 削除要求を送信すること。

データラベル：SYSRESET△2

（補足）：PI 削除要求：1bit(0:要求無し、1:要求有り)

Event　50ms 間隔で 3 回イベント送信すること

【要求事項：PPIDLR_02007】

PI ホストは、450ms 以内に 2 回以上 PI 削除要求(要求有り)を受信した場合 PI 削除処理を実施すること。

3.2.3. PI 削除実施中の画面処理

3.2.3.1. PI 削除の実施状態通知

【要求事項：PPIDLR_02008】

PI ホストは、車載 UI に対し下記データラベルにて PI 削除の実施状態を送信すること。

実施完了時は、全ての対象 ECU が正常終了となった場合のみ 2:実施完了_成功とし、

それ以外の場合は 3:実施完了_失敗とすること。

データラベル：PIDLT_PROG△2

（補足）：PI 削除の実施状態：2bit(0:実施無し、1:実施中、2:実施完了_成功、3:実施完了_失敗)

Event&Periodic

3.2.3.2. PI 削除実施の画面表示

【要求事項：PPIDLR_02009】

車載 UI は、3.2.3.1.の信号の受信状態によって、PI 削除実施の画面表示(成功、失敗など)を切り替えること。また、PI 削除実施中は、画面の一部を動作させ続け、画面処理が停止していないことを示

すこと

（補足）：処理進行バーをアニメーションさせるなどを想定している。

3.2.3.3. PI 削除のタイムアウト処理

【要求事項：PPIDLR_02010】

車載 UI は、3.2.2.5.の PI 削除要求送信後、PI ホストから 60sec(暫定値)応答がない場合は失敗を画面表示すること。△2

3.2.3.4. PI 削除の実施中断記録

【要求事項：PPIDLR_02011】

車載 UI は、3.2.2.5.の PI 削除要求送信後、実施完了及びタイムアウト前に供給電源が遮断された場合は中断として扱い、中断を記憶すること。

3.2.3.5. PI 削除の実施中断表示

【要求事項：PPIDLR_02012】

車載 UI は、中断を記憶している状態で電源 ON された場合、ユーザへ PI 削除が失敗したことを通知する。このとき、中断状態はリセットすること。

3.2.3.6. PI 削除失敗時のリトライ表示

【要求事項：PPIDLR_02013】

車載 UI は、PI 削除が失敗した場合、ユーザへリトライ要望の有無を通知し、

リトライ要望があった場合は、ユーザ操作による PI 削除機能を再度実施すること。

3.2.4. PI 削除の実施

3.2.4.1. 車載 UI_ECU の削除処理

【要求事項：PPIDLR_02014】

車載 UI の役割を担う ECU は、ユーザ操作による PI 削除機能において、

車載 UI_ECU 内で PI 削除機能を実現しても良い。

（補足）：マルチメディア操作によって、PI ホストの指示を受けず PI 削除機能を実現しても良い。

3.2.4.2. PI ホスト_ECU の削除処理

【要求事項：PPIDLR_02015】

PI ホストの役割を担う ECU は、ユーザ操作による PI 削除機能において、

PI ホスト_ECU 内で PI 削除機能を実現しても良い。

（補足）：PI ホストの DIAG コマンドを受けず PI 削除機能を実現しても良い。

3.2.4.3. 機能要件

【要求事項：PPIDLR_02016】

個人・プライバシー情報の削除機能を実装する ECU は、表 3.2.4-1 に示す機能を有すること。コマンドを受け付けるセッション、およびセキュリティアクセス解除の要否についても表 3.2.4-1 に従うこと。

表 3.2.4-1 個人・プライバシー情報削除機能△2

機能名	概要	ID	受付ｾｯｼｮﾝ			ｾｷｭﾘﾃｨ ｱｸｾｽ解除
			ﾃﾞﾌｫﾙﾄ	拡張	ﾘﾓｰﾄ	
個人・プライバシー情報削除機能	ツールからの要求に対し、保存する個人・プライバシー情報を削除する。	SID$31 RID$1016(Phase5) RID$D906(Phase6)	○	○	○	不要

【要求事項：PPIDLR_02017】

IG-ON 中に個人・プライバシー情報削除の subFunction - startRoutine リクエストを受信した場合、対象外とできる情報を除き、保存している個人・プライバシー情報を全て削除すること。

【要求事項：PPIDLR_02029】

対象 ECU は、個人・プライバシー情報削除の subFunction - startRoutine リクエストを受信してから、50sec(暫定値)以内に削除処理を完了すること。△2

※(補足)：3.2.3.3 PI 削除のタイムアウト処理を考慮して処理時間を規定する。

【要求事項：PPIDLR_02018】

個人・プライバシー情報削除中に、IG OFF となった場合、個人・プライバシー情報の削除を可能な限り継続すること。

【要求事項：PPIDLR_02019】

個人・プライバシー情報削除中に、個人・プライバシー情報削除の subFunction - startRoutine リクエストを受信した場合は、個人・プライバシー情報の削除処理を継続すること。

【要求事項：PPIDLR_02020】

subFunction - requestRoutineResults のリクエストを受信した場合は、表 3.2.4-2 個人・プライバシー情報削除の状態遷移表△3に示す状態遷移の制御ステータスを応答すること。

【要求事項：PPIDLR_02021】

subFunction - stopRoutine は非対応とする。stopRoutine のリクエストを受信した場合は、ネガティ

ブレスポンス(NRC 0x12)を応答すること。個人・プライバシー情報を削除中であれば、個人・プライバシー情報の削除処理を継続すること。

【要求事項：PPIDLR_02022】
セッション移行は処理継続とする。状態遷移は実施せず、個人・プライバシー情報を削除中であれば、個人・プライバシー情報の削除処理を継続すること。

3.2.4.4. 状態遷移

【要求事項：PPIDLR_02023】
個人・プライバシー情報削除機能の状態遷移は、図 3.2.4-1 および表 3.2.4-2 に従うこと。

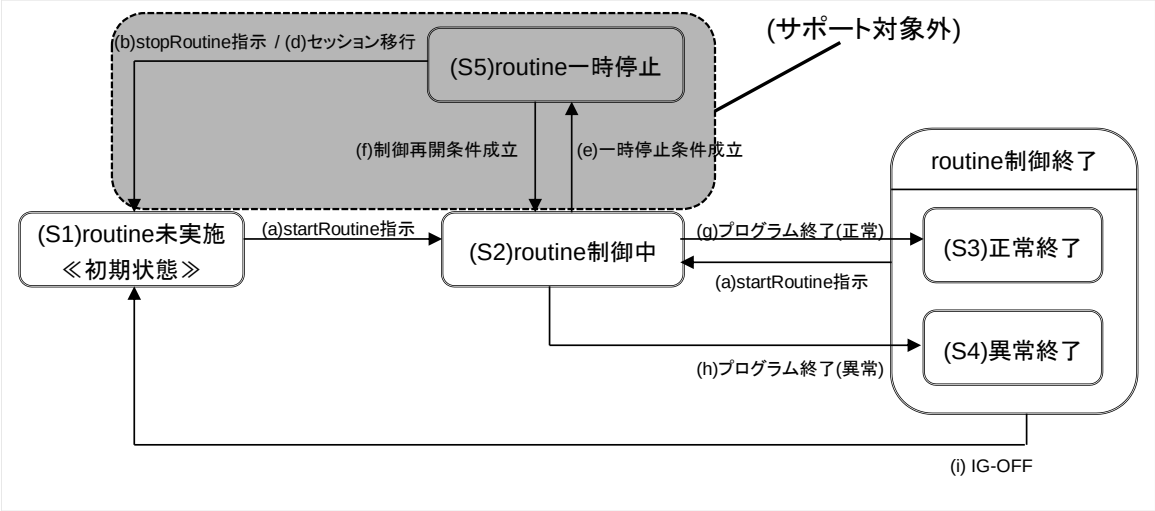

図 3.2.4-1　個人・プライバシー情報削除の状態遷移図△2

各ステータスの動作は以下の通り。

各ステータスでの動作

(S1)routine 未実施
　実施処理なし。
(S2)routine 制御中
　個人・プライバシー情報の削除を実施する。
(S3)正常終了
　実施処理なし。
(S4)異常終了
　実施処理なし。
(S5)routine 一時停止

本機能ではサポートしない。

表 3.2.4-2　個人・プライバシー情報削除の状態遷移表△2

				状態			
				S1	S2	S3	S4
				routine未実施(0x00)	routine制御中(0x01)	正常終了(0x02)	異常終了(0x03)
イベント	(a)	startRoutine指示	アクション	・ポジティブレスポンスを応答する ・個人・プライバシー情報消去を開始する	・ネガティブレスポンス(NRC24)を送信する ・個人・プライバシー情報消去を継続する	・ポジティブレスポンスを応答する ・個人・プライバシー情報消去を開始する	・ポジティブレスポンスを応答する ・個人・プライバシー情報消去を開始する
			遷移先	S2	S2	S2	S2
	(b)	stopRoutine指示 →サポート対象外	アクション	・ネガティブレスポンス(NRC12)を送信する	・ネガティブレスポンス(NRC12)を送信する ・個人・プライバシー情報消去を継続する	・ネガティブレスポンス(NRC12)を送信する	・ネガティブレスポンス(NRC12)を送信する
			遷移先	S1	S2	S3	S4
	(c)	強制終了条件成立 →サポート対象外	アクション	N/A(Not Applicable)	N/A	N/A	N/A
			遷移先				
	(d)	セッション移行	アクション	・何もしない ※1	・個人・プライバシー情報消去を継続する	・何もしない※1	・何もしない※1
			遷移先	S1	S2	S3	S4
	(e)	一時停止条件成立 →サポート対象外	アクション	N/A	N/A	N/A	N/A
			遷移先				
	(f)	制御再開条件成立 →サポート対象外	アクション	N/A	N/A	N/A	N/A
			遷移先				
	(g)	プログラム終了(正常)	アクション	N/A	・何もしない ※1	N/A	N/A
			遷移先		S3		
	(h)	プログラム終了(異常)	アクション	N/A	・何もしない ※1	N/A	N/A
			遷移先		S4		
	(i)	IG OFF	アクション	・何もしない ※1	・個人・プライバシー情報消去を継続する※2	・何もしない ※1	・何もしない ※1
			遷移先	S1	S2	S1	S1
	(x)	request Routine Results指示	アクション	・Phase5の場合、ポジティブレスポンス(routineStatus#1=0x00)を送信する ・Phase6の場合、ネガティブレスポンス(NRC24)を送信する	・Phase5の場合、ポジティブレスポンス(routineStatus#1=0x01)を送信する ・Phase6の場合、ネガティブレスポンス(NRC21)を送信する ・個人・プライバシー情報消去を継続する	・ポジティブレスポンス(routineStatus#1=0x02)を送信する	・ポジティブレスポンス(routineStatus#1=0x03)を送信する
			遷移先	S1	S2	S3	S4

※1　個人・プライバシー情報消去機能の処理に関わるもののみ記載している。
※2　処理を継続できない場合はS1に遷移する。

3.2.4.5. 通信コマンド

【要求事項：PPIDLR_02024】

個人・プライバシー情報削除機能は物理アドレスに対応すること。

(1) startRoutine 指示

【要求事項：PPIDLR_02025】

個人・プライバシー情報削除機能の startRoutine 指示は、表 3.2.4-3 に従うこと。

表 3.2.4-3 個人・プライバシー情報削除のリクエストメッセージフォーマット(startRoutine)

A_Data byte	Parameter	Byte Value		Scaling/Bit
		Phase5	Phase6	
#1	RoutineControl Request SID	0x31		hexadecimal
#2	subFunction = startRoutine, suppressPosRspMsgIndicationBit = FALSE/TRUE	0x01/0x81		hexadecimal
	routineIdentifier[] = 個人・プライバシー情報削除[			
#3	byte#1(MSB)	0x10	0xD9	hexadecimal
#4	byte#2]	0x16	0x06	hexadecimal

※routineControlOptionRecord はなし。

【要求事項：PPIDLR_02026】

個人・プライバシー情報削除機能の startRoutine のレスポンスは表 3.2.4-4 に従うこと。

表 3.2.4-4 個人・プライバシー情報削除のレスポンスメッセージフォーマット(startRoutine)

A_Data byte		Parameter	Byte Value		Scaling/Bit
Phase5	Phase6		Phase5	Phase6	
#1		RoutineControl Response SID	0x71		hexadecimal
#2		subFunction = startRoutine	0x01		hexadecimal
		routineIdentifier[] = 個人・プライバシー情報削除[			
#3		byte#1(MSB)	0x10	0xD9	hexadecimal
#4		byte#2]	0x16	0x06	hexadecimal
-	#5	routineInfo	NA	0x03	hexadecimal

※routineStatusRecord はなし。

ポジティブレスポンスおよびネガティブレスポンスの詳細はPhase6の場合は関連文書[A]のDiagnostic design specification UDS Protocol、Phase5 の場合は関連文書[B]の RoutineControl service 標準仕様書(sid31-rd***)に準拠する。

(2) stopRoutine 指示

未サポート

(3) requestRoutineResults

【要求事項：PPIDLR_02027】

個人・プライバシー情報削除機能の requestRoutineResults 指示は、表 3.2.4-5 に従うこと。

表 3.2.4-5 個人・プライバシー情報削除のリクエストメッセージフォーマット(requestRoutineResults)

A_Data byte	Parameter	Byte Value		Scaling/Bit
		Phase5	Phase6	
#1	RoutineControl Request SID	0x31		hexadecimal
#2	subFunction = requestRoutineResults, suppressPosRspMsgIndicationBit = FALSE/TRUE	0x03/0x83		hexadecimal
	routineIdentifier[] = 個人・プライバシー情報削除[			
#3	byte#1(MSB)	0x10	0xD9	hexadecimal
#4	byte#2]	0x16	0x06	hexadecimal

※routineControlOptionRecord はなし。

【要求事項：PPIDLR_02028】

個人・プライバシー情報削除機能の requestRoutineResults のレスポンスは、表 3.2.4-6 に従うこと。

表 3.2.4-6 個人・プライバシー情報削除のレスポンスメッセージフォーマット(requestRoutineResults)

A_Data byte		Parameter	Byte Value		Scaling/Bit
Phase5	Phase6		Phase5	Phase6	
#1		RoutineControl Response SID	0x71		hexadecimal
#2		subFunction = requestRoutineResults	0x03		hexadecimal
		routineIdentifier[] = 個人・プライバシー情報削除[			
#3		byte#1(MSB)	0x10	0xD9	hexadecimal
#4		byte#2]	0x16	0x06	hexadecimal
-	#5	routineInfo	NA	0x03	hexadecimal
		routineStatusRecord[] = [			
#5	#6	routineStatus#1]	0DLR		hexadecimal

※routineStatusRecord の応答値は以下の通り。

0x00 = routine 未実施(Phase5 の場合のみ対応する) △2

0x01 = routine 制御中(Phase5 の場合のみ対応する) △2

0x02 = 正常終了

0x03 = 異常終了

3.3. ディーラ操作による PI 削除機能

3.3.1. 説明

ディーラ操作による PI 削除機能は、ディーラ作業による PI 削除（ディーラツールでのダイアグコマンド指示など）を実現する機能である。

3.3.2. ディーラツールの詳細要件について

本書では、ディーラツールの詳細要件については記載しないこととする。

3.3.3. 対象 ECU の要件について

【要求事項：PPIDLR_03001】

ディーラツールから送信される PI 削除指示は、PI ホストから送信される PI 削除指示と同等となるため、3.2.2.1[△3],3.2.4.3, 3.2.4.4, 3.2.4.5【要求事項：PPIDLR_02002[△3],PPIDLR_02016～PPIDLR_2029】の要件を同様に満たすこと。[△2]

（補足）：車載 UI_ECU, PI ホスト_ECU も本項の対象となるため留意すること。

Revision Record

Marks	Version	Revision contents	Date	Revised
-	a00-00-a	Initial Release	Oct. 31,2022	Katsube
△1	a00-00-b	Add English translation. Add an explanation of target ECU in Fig. 2.2.2 Operation sequence for PI deletion based on dealer operation.	Dec. 8,2022	Kakiya Katsube
△2	a00-01-a	Update PI deletion timeout processing. Add Requirement：PPIDLR_02029. Update signal (CAN) for notification of deletion request. Clarify the scope of physically deletion. Correct the deviation from Phase6 diagnosis communication spec. Change from requirement to supplement in PPIDLR_01004. Add definition of non-volatile memory. Correct editorial errors (State transition diagram, Phase5 diagnosis communication)	Feb. 28,2023	Kakiya Katsube
△3	a00-02-a	Update 1.2. Scope Add 1.7. Personal information/ or privacy-related information, and assigning sensitivity Update 2.1. System configuration Update 2.3. Requirement List Update 3.1.2. Scope of this document Update 3.1.3. Conditions determining whether to implement the applicable function Update 3.1.4. Information subject to PI deletion Update 3.3.3. Requirements for target ECUs	May. 31,2023	Yamakawa

Table of contents

Introduction

1.1. Purpose of this document

This document indicates the requirements that shall be satisfied at the individual ECUs based on Upper-level Document [1].

1.2. Scope

The allocation targets are△3 ECUs in 19PF ver3 △3that are connected to In-vehicle network and store personal and privacy information in non-volatile memory.

1.3. Description of Requirements

The parts described 【Requirement：PPIDLR_*****】 are requirements in this document.
However, the parts described (Supplement) are supplementary items and are not requirements.

1.4. Upper-level Documents

Upper-level documents in this document are shown in Table1.

Table1 Upper-level Document List△2

No	Document name	Ver (Applied to the latest version)	Issued
1	In-vehicle Privacy Requirements	TPR-RVe0001	Information Security and Trust Management Div.

1.5. Related Documents

Related Documents in this document are shown in Table2.

Table2 Related Document List

No	Document name	Ver	Issued
[A]	Diagnostic design specification UDS Protocol	-	46F7G
[B]	RoutineControl service standard specification (sid31-rd***)	-	46F7G
[C]	Common Requirements Specifications of In-vehicle Personal and Privacy Information	SEC-ePF-PCC-REQ-SPEC	46F

Table 1-3: Publicly Available Related Documents

Abbreviation used in the text	Name/external link
The eight OECD principles	Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Sep. 2013) Part 2: Basic Principles of National Application Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
ISO/IEC29100	ISO/IEC 29100:2011(Dec. 2011) Information technology -- Security techniques -- Privacy framework Information technology -- Security techniques -- Privacy framework
GDPR	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 Main text: https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04 Provisional Japanese translation: https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/
GDPR Guidelines	Guidelines 05/2020 on consent under Regulation 2016/679 Provisional Japanese translation: https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/
Japanese regulations	Act on the Protection of Personal Information (as of 2022) https://www.ppc.go.jp/personalinfo/legal/
Guidelines for Japanese regulations	Various guidelines and Q & A https://www.ppc.go.jp/personalinfo/legal/
Chinese regulations	・Personal Information Protection Law of the People's Republic of China (issued August 20, 2021) ・Various regulations on automobile data safety management (trial)
Chinese GBT	・Specification on information security technology and personal information safety
CCPA (California Consumer Privacy Act)	California Consumer Privacy Act of 2018 Provisional Japanese translation: https://www.ppc.go.jp/enforcement/infoprovision/laws/CCPA/

1.6. Terminology

Table 1-4: List of terminology△2

Term	Description
PI	This is an abbreviation for “personal information” or “privacy-related information”.
User	The customer that uses the vehicle.
Data subject	This refers to an identified natural person or a natural person who can be identified (i.e., the user).
Non-volatile memory	In general, it refers to the memory that can retain data even when power is not supplied, but in this document, the memory that retains data with +B power when IG/ACC is turned off is also treated as non-volatile.

1.7. Personal information/privacy-related information, and assigning △3sensitivity

Personal information/privacy-related information means information from Category No. 1 to 10 in the Appendix A of the related document [c]. Sensitivity means value assigned up to the category. Refer to the column “sensitivity” in the Appendix A for the specific value. △3

2. Outline of requirements

2.1. System configuration

We show the structure assumed for the requirements defined in this specification in Fig. 2-1. In addition, we show the descriptions of the components in Table 2-1. △3

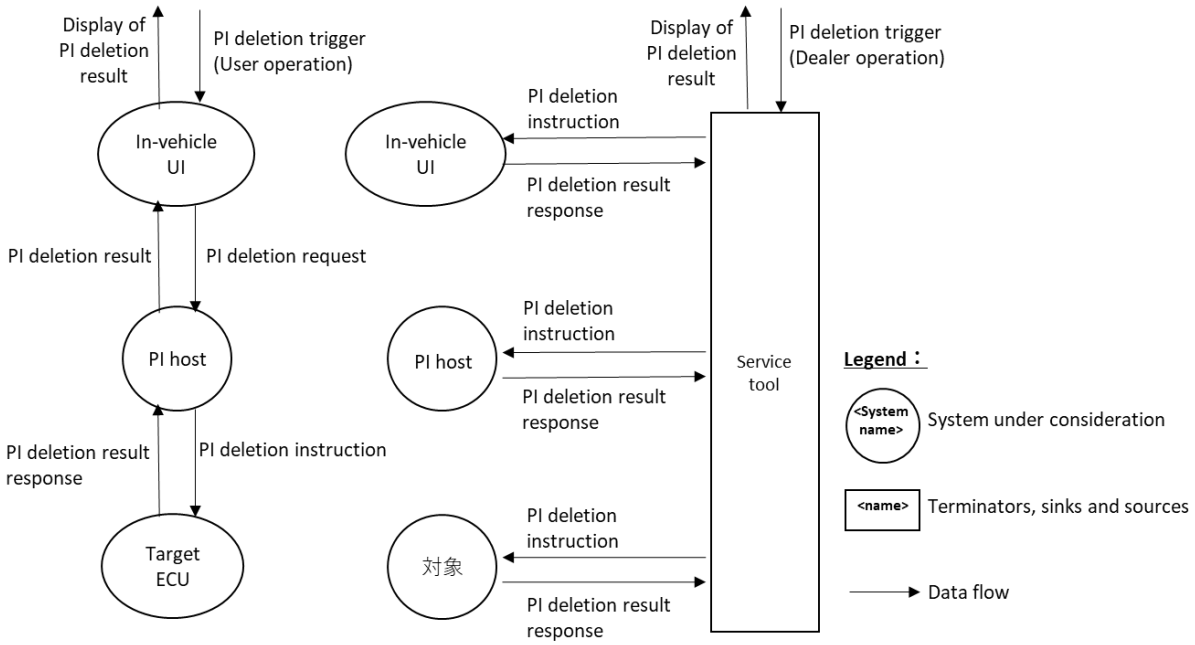

Fig. 2.1: System Configuration

Table 2-1: Definition of terms in Fig. 2-1△3

Component	Description
In-Vehicle UI	ECU that has UI that gets trigger for PI deletion by user operation. MM on 19PF ver3.
PI host	Host that transmits PI deletion instruction to target ECUs.
Target ECU	ECU that has PI to be deleted, and delete the PI according to the deletion instruction.
Dealer tool	Tool that offers UI to get trigger for PI deletion by dealer operation, and transmits PI deletion instruction to target ECUs.

2.2. Operation sequences

The operation sequences in this specification are presented below.

2.2.1. Operation sequence for PI deletion based on user operation

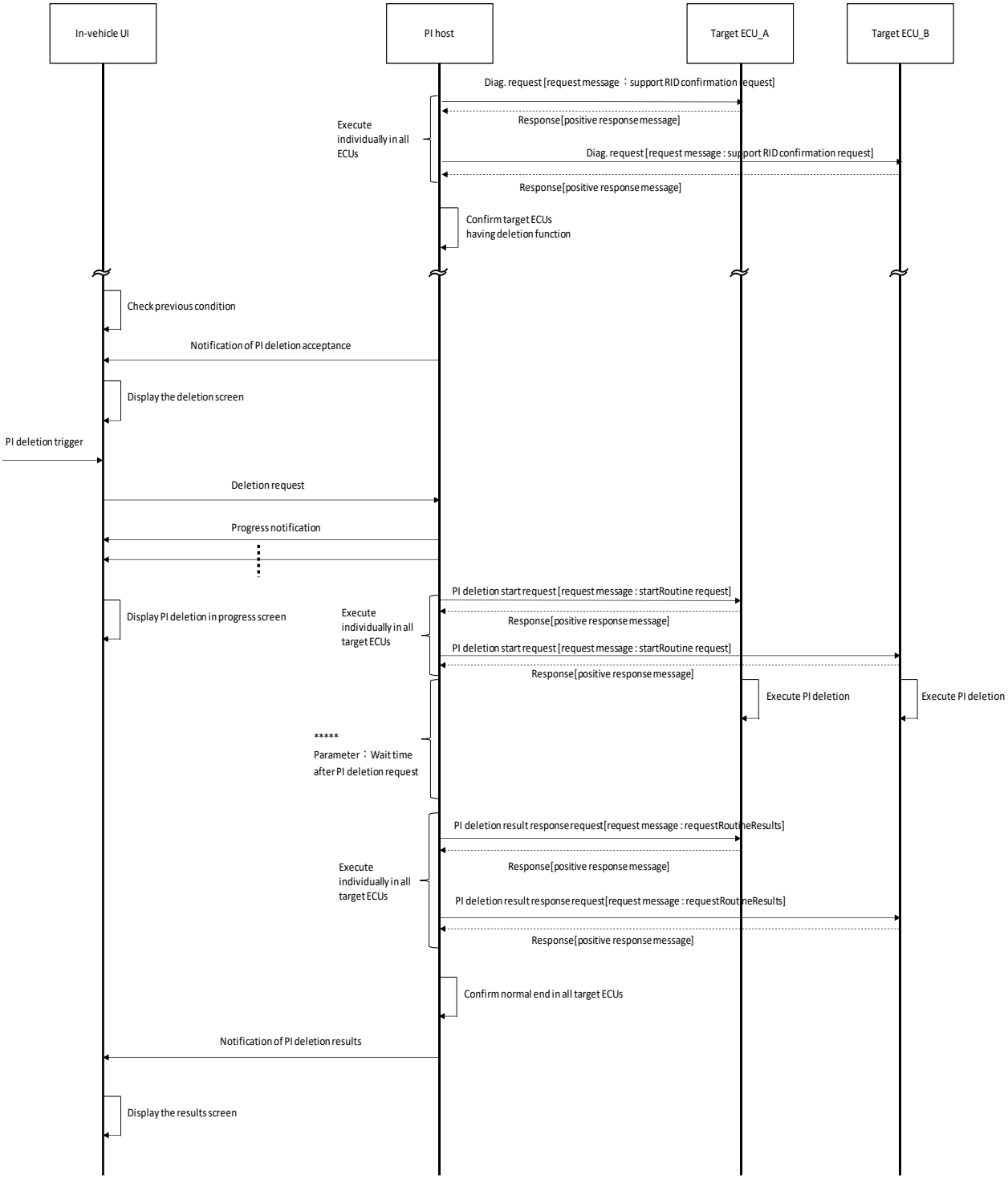

Fig. 3.2.1: Operation Sequence for PI Deletion Based on User Operation △2

2.2.2. Operation sequence for PI deletion based on dealer operation

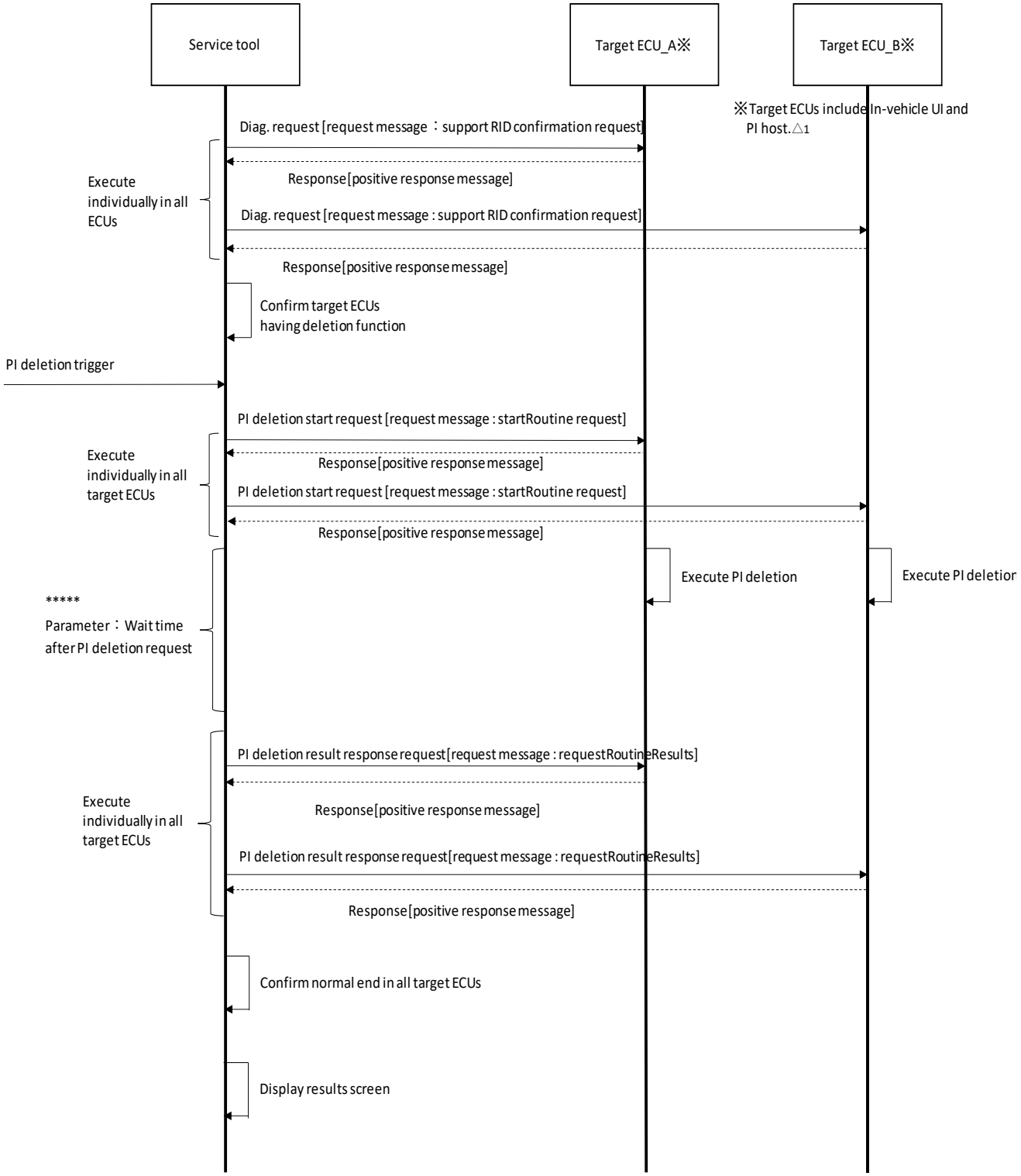

Fig. 3.2.2: Operation Sequence for PI Deletion Based on Dealer Operation△1△2

2.3. Requirement List

We show[△3] requirements in Table 2-2[△3] that the components shall satisfy[△3].

(○:Applicable、－:Not applicable)

Refer to chapter 3 and later for the requirements in detail.

Table 2-2[△3] Requirement Table[△2]

Requirement number	In-vehicle UI	PI host ※Not used in 19PF ver3[△3]	Target ECU
PPIDLR_01001	○	○	○
PPIDLR_01002	○	○	○
PPIDLR_01003	○	○	○
PPIDLR_01004	Deleted	Deleted	Deleted
PPIDLR_02001	－	○	－
PPIDLR_02002	－	－	○
PPIDLR_02003	－	○	－
PPIDLR_02004	－[△3]	－	－
PPIDLR_02005	－[△3]	－	－
PPIDLR_02006	－[△3]	－	－
PPIDLR_02007	－	○	－
PPIDLR_02008	－	○	－
PPIDLR_02009	－[△3]	－	－
PPIDLR_02010	－[△3]	－	－
PPIDLR_02011	－[△3]	－	－
PPIDLR_02012	－[△3]	－	－
PPIDLR_02013	－[△3]	－	－
PPIDLR_02014	－[△3]	－	－
PPIDLR_02015	－	○	－
PPIDLR_02016	○	○	○
PPIDLR_02017	○	○	○
PPIDLR_02029	○	○	○
PPIDLR_02018	○	○	○
PPIDLR_02019	○	○	○

PPIDLR_02020	○	○	○
PPIDLR_02021	○	○	○
PPIDLR_02022	○	○	○
PPIDLR_02023	○	○	○
PPIDLR_02024	○	○	○
PPIDLR_02025	○	○	○
PPIDLR_02026	○	○	○
PPIDLR_02027	○	○	○
PPIDLR_02028	○	○	○
PPIDLR_03001	○	○	○

3. Details of functional requirements

3.1. Functional requirements for the deletion of personal and privacy information

3.1.1. Description

The function to delete personal and privacy information ("PI") is a function that deletes personal and privacy information stored in the vehicle accordance with user request.

3.1.2. Scope of this document

This document describes the PI deletion function executed inside the vehicle.
Consequently, the points below are beyond the scope of this document.

・Function related in the deletion of PI stored outside the vehicle (e.g., on a server).

3.1.3. Conditions determining whether to implement the applicable function

[Requirement item: PPIDLR_01001]

In-Vehicle UI shall physically delete (*1) PI it has according to user request through its UI. In addition, In-Vehicle UI shall physical delete (*1) PI it has according to request from dealer tool. △3

However, data of severity B or lower does not require physically deletion, allowing for normally deletion which means that data itself remains in memory. △2

*1: Physically deleting the data means overwriting all of it with "0" or "1" or other processing that prevents easy recovery of the data.
*2: When dealer-operated deletion is implemented, inform the customer of that fact in the owner's manual or elsewhere.
*3: If the ECU is not applicable with diagnostic△3 command, the ECU may be implemented the deletion function with specific operation (e.g., Press and hold physical buttons simultaneously)
*4: We do not require physical PI deletion by the function of 3.2 on 19PF ver3. However, we require it in the later e-PF. △3

3.1.4. Information subject to PI deletion

[Requirement item: PPIDLR_01002]

Deletion target information of PI means information categorized into category whose column "deletion" is "○" (Category 1 ~ 7) in Appendix A of the related document [C]. However, "Table A-1 Data that can be excluded from deletion" in Appendix A in the related document may not be deletion target. △3

3.1.5. Interruption during PI deletion

[Requirement item: PPIDLR_01003]

The target ECU shall continue the deletion process as long as possible if the ECU start-up power (e.g., ACC or IG) is turned off during the PI deletion process. If the target ECU is not able to continue and then interrupts the process, the ECU shall preserve the data that was being deleted (maintain an index, for example, and prevent damage to the data due to the interruption).

3.1.6. PI deletion while the vehicle is in motion

(Supplement) △2

During PI deletion, the target ECU shall make sure that the process does not impair safety even if the vehicle starts moving.

3.2. PI deletion function based on user operation

3.2.1. Description

We do not require PI deletion function based on user operation in 19PFver3. Refer to the section 2.3 for the detail of what we do not require in 19PFver3. △3

The PI deletion function based on user operation provides a UI (e.g., multimedia) to enable PI to be deleted through user operation in the vehicle.

3.2.2. Display processing for PI deletion request

3.2.2.1. Confirmation of target ECUs

[Requirement: PPIDLR_02001]

PI host shall send a support RID confirmation request (RID$1000(Phase5)/RID$D1D9(Phase6)) to all of ECUs which are implemented in the vehicle and confirm all target ECUs subject to deletion function of PI. △2

[Requirement: PPIDLR_02002]

The target ECU subject to deletion function of PI shall support a support RID confirmation request (RID$1000(Phase5)/RID$D1D9(Phase6)). △2

3.2.2.2. Notification of PI deletion acceptance state

[Requirement item: PPIDLR_02003]

The PI host shall send an acceptance state of PI deletion request to the In-vehicle UI with the data labels below.

- Data label: PIDLT_ACEPT △2

*Supplementary information: PI deletion acceptance: 1 bit (0: Cannot be accepted, 1: Can be accepted)
Event & Periodic

3.2.2.3. Display of PI deletion request screen

[Requirement item: PPIDLR_02004]

In-vehicle UI shall switch to the PI deletion instruction screen and attendant processing in accordance with the reception state of the signal in 3.2.2.2.

*Supplementary information: Determine the acceptance state based on whether there is a PI master and on the processing that accompanies the PI master launch or similar process.

3.2.2.4. Display the confirmation screen for the PI deletion request

[Requirement item: PPIDLR_02005]

In-vehicle UI shall display a confirmation screen to users again when they press the deletion request button.

*Supplement: Make sure the user really intends to delete the information because the recorded data is reset and some functions may be reinitialized.

3.2.2.5. Sending the PI deletion request

[Requirement item: PPIDLR_02006]

In-vehicle UI shall send the PI deletion request to the PI host with the data label below.

- Data label: SYSRESET△2

*Supplement: PI deletion request: 1 bit (0: not requested, 1: requested)
Event: Send the event three times at 50 ms intervals

[Requirement item: PPIDLR_02007]

PI host shall execute the PI deletion process when it receives two or more PI deletion requests (requested) within 450 ms.

3.2.3. Display processing during PI deletion

3.2.3.1. Notification of the PI deletion progress

[Requirement item: PPIDLR_02008]

PI host shall send the progress of PI deletion with the data labels below to In-vehicle UI.

When PI deletion is finished, if all target ECUs are successfully completed, the ECU shall judge completed successful. If any target ECUs are not successfully completed, the ECU shall judge completed failed.

- Data label: PIDLT_PROG△2

*Supplement: PI deletion progress: 2 bits (0: not executed, 1: in progress, 2: completed_successful, 3: completed_failed)
Event & Periodic

3.2.3.2. Displaying the PI deletion in progress screen

[Requirement item: PPIDLR_02009]

In-vehicle UI shall switch to display of PI deletion in progress screen (e.g., success or failure) in accordance with the reception state of the signal in 3.2.3.1. In addition, while the PI deletion is in progress, the ECU shall keep a part of its screen active to show that the process has not stopped.

*Supplementary information: An indicator such as an animated progress bar is envisioned.

3.2.3.3. PI deletion timeout processing

[Requirement item: PPIDLR_02010]

After the PI deletion request in 3.2.2.5 has been sent, the In-vehicle UI shall display a failure screen if there is no response from the PI master for 60 seconds (provisional value). △2

3.2.3.4. Recording interruptions during PI deletion

[Requirement item: PPIDLR_02011]

After the PI deletion request in 3.2.2.5 has been sent, the In-vehicle UI shall treat it as an interruption if the power supply is cut off before completion or a timeout and record the interruption.

3.2.3.5. Displaying interruptions during PI deletion

[Requirement item: PPIDLR_02012]

If there is a record of an interruption when the power supply is turned on, the In-vehicle UI shall notify the user that PI deletion has failed. The ECU shall reset the interruption state at that time.

3.2.3.6. Retry indication after a PI deletion failure

[Requirement item: PPIDLR_02013]

If PI deletion fails, the In-vehicle UI shall ask users if they want to retry. If they request the retry, the ECU shall execute the user-operated PI deletion function again.

3.2.4. Executing PI deletion

3.2.4.1. Deletion process in In-vehicle UI_ECU

[Requirement item: PPIDLR_02014]

The ECU with In-vehicle UI may implement the user-operated PI deletion function of itself.

*Supplementary information: The PI deletion function may be implemented via MM operation, without receiving an instruction from the PI host.

3.2.4.2. Deletion process in PI host_ECU

[Requirement item: PPIDLR_02015]

The ECU with PI host may implement the user-operated PI deletion function of itself.

*Supplementary information: The PI deletion function may be implemented without receiving a PI host DIAG command.

3.2.4.3. Functional requirements

[Requirement item: PPIDLR_02016]

The ECU that implements the PI deletion function shall have the functions shown in Table 3.2.4-1. Concerning sessions that accept command and whether the security access cancellation shall comply with Table 3.2.4-1.

Table 3.2.4-1: Personal and privacy information deletion function[△2]

Function name	Overview	ID	Accepting session			Security access cancellation
			Default	Extended	Remote	
Personal and privacy information deletion function	Delete the stored personal and privacy information in accordance with a request from the tool.	SID$31 RID$1016(Phase5) RID$D906(Phase6)	Yes	Yes	Yes	Not required

[Requirement item: PPIDLR_02017]
When the target ECU receives the subFunction - startRoutine request of personal and privacy information deleting during IG-ON, the target ECU shall delete personal and privacy information stored in ECU except for the exclude information. △2

[Requirement item: PPIDLR_02029]
Target ECU shall complete the deletion processing within 50 seconds (provisional value) after receiving the subFunction - startRoutine request of personal and privacy information deleting.
*Supplement: The processing time is defined in consideration of3.2.3.3 PI deletion timeout processing.

[Requirement item: PPIDLR_02018]
If IG is turned OFF during deleting personal and privacy information, the target ECU shall keep deleting personal and privacy information as possible as it can.

[Requirement item: PPIDLR_02019]
When the target ECU receives the subFunction - startRoutine request of personal and privacy information deleting during deleting personal and privacy information, the target ECU shall continue the deleting process of personal and privacy information.

[Requirement item: PPIDLR_02020]
When the target ECU receives the subFunction - requestRoutineResults request, the target ECU shall respond with the control status of the state transition as indicated in Table 3.2.4-2 State Transition Table of Personal and Privacy Information Deletion

[Requirement item: PPIDLR_02021]
subFunction - stopRoutine shall not be supported. If the target ECU receives the stopRoutine request, the target ECU shall respond with a negative response (NRC 0x12). If personal and privacy information is being deleted, the target ECU shall continue the deleting process of personal and privacy information.

[Requirement item: PPIDLR_02022]
When the session transfer occurs, the process shall be continued. The target ECU shall not execute the state transition, and if personal and privacy information is being deleted, the target ECU shall continue the deleting process of personal and privacy information.

3.2.4.4. State Transition

[Requirement item: PPIDLR_02023]

The state transition in the personal and privacy information deletion function shall comply with Fig. 3.2.4-1 and Table 3.2.4-2

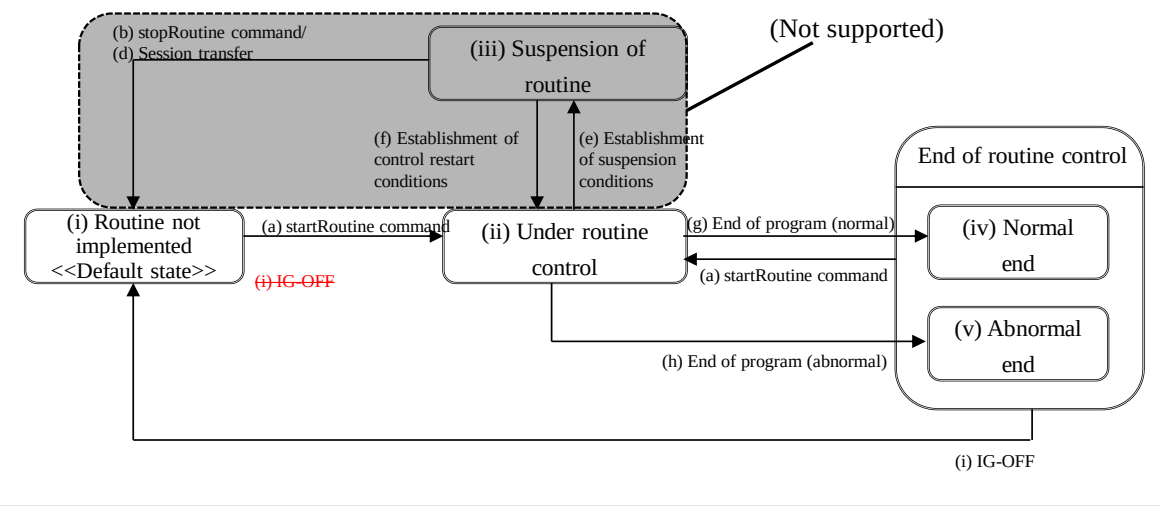

Fig. 3.2.4-1 State Transition Diagram of Personal and Privacy Information Deletion Δ2

The operation in each state shall be as follows:

Operation in each state

(i) Routine not implemented

No processing is implemented.

(ii) Under routine control

The target ECU shall execute erasing of personal and privacy information.

(iii) Suspension of routine

This is not supported by this function.

(iv) Normal end

No processing is implemented.

(v) Abnormal end

No processing is implemented.

Table 3.2.4-2 State Transition Table of Personal and Privacy Information Deletion△2

				Status			
				S1	S2	S3	S4
				Routine not implemented (0x00)	Routine being controlled (0x01)	Normal end (0x02)	Abnormal end (0x03)
Event	(a)	startRoutine command	Action	* Responds with a positive response. * Starts erasing of personal and privacy information. ~~(PPIREQ_01003)~~	* Transmits a negative response (NRC24). * Continues erasing of personal and privacy information. ~~(PPIREQ_01005)~~	* Responds with a positive response. * Starts erasing of personal and privacy information. ~~(PPIREQ_01003)~~	* Responds with a positive response. * Starts erasing of personal and privacy information. ~~(PPIREQ_01003)~~
			Transition to	S2	S2	S2	S2
	(b)	stopRoutine command → Not supported	Action	* Transmits a negative response (NRC12). ~~(PPIREQ_01007)~~	* Transmits a negative response (NRC12). * Continues erasing of personal and privacy information. ~~(PPIREQ_01007)~~	* Transmits a negative response (NRC12). ~~(PPIREQ_01007)~~	* Transmits a negative response (NRC12). ~~(PPIREQ_01007)~~
			Transition to	S1	S2	S3	S4
	(c)	Establishment of forced termination conditions	Action	N/A (Not Applicable)	N/A	N/A	N/A
			Transition to				
	(d)	Session transfer	Action	* Takes no action. ~~(PPIREQ_01008)~~ *1	* Continues erasing of personal and privacy information. ~~(PPIREQ_01008)~~	* Takes no action. ~~(PPIREQ_01008)~~ *1	* Takes no action. ~~(PPIREQ_01008)~~ *1
			Transition to	S1	S2	S3	S4
	(e)	Establishment of suspension condition	Action	N/A	N/A	N/A	N/A
			Transition to				
	(f)	Establishment of control restart condition	Action	N/A	N/A	N/A	N/A
			Transition to				
	(g)	End of program (normal)	Action	N/A	* Takes no action. *1	N/A	N/A
			Transition to		S3		
	(h)	End of program (abnormal)	Action	N/A	* Takes no action. *1	N/A	N/A
			Transition to		S4		
	(i)	IG OFF	Action	* Takes no action. *1	* Continue~~Stops~~ erasing of personal and privacy information.*2 ~~(PPIREQ_01004)~~	* Takes no action. *1	* Takes no action. *1
			Transition to	S1	S2~~1~~	S1	S1
	(x)	request Routine Results command	Action	* In the case of Phase5, Transmits a positive response (routineStatus#1=0x00). ~~(PPIREQ_01006)~~ * In the case of Phase6, Transmits a negative response (NRC24).	* In the case of Phase5, Transmits a positive response (routineStatus#1=0x01). * In the case of Phase6, Transmits a negative response (NRC21). ~~(PPIREQ_01006)~~ * Continues erasing of personal and privacy information.	* Transmits a positive response (routineStatus#1=0x02). ~~(PPIREQ_01006)~~	* Transmits a positive response (routineStatus#1=0x03). ~~(PPIREQ_01006)~~
			Transition to	S1	S2	S3	S4

*1 This action is described only the processing regarded to Personal and Privacy Information Erasing Function
*2 If the process can not be continued, the transition to S1 is made

3.2.4.5. Communication Commands

[Requirement item: PPIDLR_02024]

A command for the personal and privacy information deletion function shall support physical addresses.

(1) startRoutine command

[Requirement item: PPIDLR_02025]

The startRoutine command for the personal and privacy information erasing function shall comply with Table 3.2.4-3.

Table 3.2.4-3 Format of Request Message for Personal and Privacy Information Erasing (startRoutine)

A_Data byte	Parameter	Byte Value		Scaling/Bit
		Phase5	Phase6	
#1	RoutineControl Request SID	0x31		hexadecimal
#2	subFunction = startRoutine, suppressPosRspMsgIndicationBit = FALSE/TRUE	0x01/0x81		hexadecimal
	routineIdentifier[] = personal and privacy information erasing[			
#3	byte#1(MSB)	0x10	0xD9	hexadecimal
#4	byte#2]	0x16	0x06	hexadecimal

* There is no routineControlOptionRecord.

[Requirement item: PPIDLR_02026]

The response to startRoutine for the personal and privacy information erasing function shall comply with Table 3.2.4-4.

Table 3.2.4-4 Format of Response Message for Personal and Privacy Information Erasing (startRoutine)

A_Data byte		Parameter	Byte Value		Scaling/Bit
Phase5	Phase6		Phase5	Phase6	
#1		RoutineControl Response SID	0x71		hexadecimal
#2		subFunction = startRoutine	0x01		hexadecimal
		routineIdentifier[] = personal and privacy information erasing[			
#3		byte#1(MSB)	0x10	0xD9	hexadecimal
#4		byte#2]	0x16	0x06	hexadecimal
-	#5	routineInfo	NA	0x03	hexadecimal

*There is no routineStatusRecord.

The details of the positive response and the negative response shall comply with Diagnostic design specification UDS Protocol in Related Document [1] or RoutineControl service standard specifications (sid31-rd***) in Related Document [2].

(2) stopRoutine command

Not supported

(3) requestRoutineResults

[Requirement item: PPIDLR_02027]

The requestRoutineResults command for the personal and privacy information erasing function shall comply with Table 3.2.4-5.

Table 3.2.4-5 Format of Request Message for Personal and Privacy Information Erasing (requestRoutineResults)

A_Data byte	Parameter	Byte Value		Scaling/Bit
		Phase5	Phase6	
#1	RoutineControl Request SID	0x31		hexadecimal
#2	subFunction = requestRoutineResults, suppressPosRspMsgIndicationBit = FALSE/TRUE	0x03/0x83		hexadecimal
	routineIdentifier[] = personal and privacy information erasing[			
#3	byte#1(MSB)	0x10	0xD9	hexadecimal
#4	byte#2]	0x16	0x06	hexadecimal

* There is no routineControlOptionRecord.

[Requirement item: PPIDLR_02028]

The response to requestRoutineResults of the MAC key verification information transmission function shall comply with Table 3.2.4-6.

Table 3.2.4-6 Format of Response Message for Personal and Privacy Information Erasing (requestRoutineResults)

A_Data byte		Parameter	Byte Value		Scaling/Bit
Phase5	Phase6		Phase5	Phase6	
#1		RoutineControl Response SID	0x71		hexadecimal
#2		subFunction = requestRoutineResults	0x03		hexadecimal
		routineIdentifier[] = personal and privacy information erasing [			

A_Data byte		Parameter	Byte Value		Scaling/Bit
Phase5	Phase6		Phase5	Phase6	
#3		byte#1(MSB)	0x10	0xD9	hexadecimal
#4		byte#2]	0x16	0x06	hexadecimal
-	#5	routineInfo	NA	0x03	hexadecimal
#5	#6	routineStatusRecord[] = [routineStatus#1]	0xXX		hexadecimal

The response values of routineStatusRecord are as follows.

0x00 = Routine not implemented (only Phase5) △2

0x01 = Under routine control (only Phase5) △2

0x02 = Normal end

0x03 = Abnormal end

3.3. PI deletion function based on dealer operation

3.3.1. Description

The dealer-operated deletion function relies on an action by the dealer (e.g., a diagnostics command with the service tool).

3.3.2. Detailed requirements for service tools

This document does not describe the detailed requirements for service tools.

3.3.3. Requirements for target ECUs

[Requirement: PPIDLR_03001]

Since the PI deletion instruction sent by the service tool is equivalent to a PI deletion instruction sent by the PI host, [Requirement: PPIDLR_02002△3, PPIDLR_02016 to PPIDLR_02029] in 3.2.2.1 △3、3.2.4.3, 3.2.4.4 and 3.2.4.5 shall be similarly satisfied. △2

(Supplement) This requirement also applies to the In-vehicle UI_ECU and the PI host ECU.