関係各部署　御中

表示	Protected 関係者外秘	原紙保管	M/Y:6/2031
		コピー保管	M/Y:6/2031

車載個人・プライバシー情報対策基準書

制御電子プラットフォーム開発部車載ネットワーク・アーキ開発室

No. SEC-ePF-PPI-STD-a00-03-a

承認	調査	作成	
河井	平林	三河 垣 澤合 屋	2021/7/6

署名省略　(電子回覧で承認取得済)

適用

・Post17CY マルチメディアシステム　or

・19PF Ver.2 以降の個人・プライバシー情報を取扱う車載部品 or

・UNR155 法規対象車両に搭載され、下記に当てはまる車載部品

　・プライバシー情報を外部と通信する ECU or

　・プライバシー性高の情報を車両機器の画面、音声などでユーザ通知する ECU

変更履歴

Version	発行理由	日付	変更者
00a	初版発行	2018/5/31	51F1G 尾﨑
01a	記載内容見直し	201811/12	51F1G 市原
02a	同意・撤回内容修正	2019/8/21	46F3G 市原
03a	UNR155 法規対応のため、適用を見直し	2021/7/6	46F3G 河合 46F4G 垣屋

特記

【入手先】

本文書は BBS からダウンロードしてください。

URL：https://softsite-1.bbs2.tec.toyota.co.jp/

Folder：/lan/P3.情報セキュリティ/10.仕様・要件書/19PF 車載個人・プライバシー情報対策基準書/

必要に応じて、関係会社・関係部署への展開をお願いします。

【問合せ先】

制御電子プラットフォーム開発部 車載ネットワーク開発室 3G/4G

Mail：epf-sec-sp@mega.tec.toyota.co.jp

変更履歴

記号	Version	日付	変更者	項目	変更内容
	a00-00-a	2018/5/31	尾﨑	全項目	初版発行
△1	a00-01-a	2018/11/9	市原	関連文書	文書追加
				３.	診断ツールでの同意不要の理由を記載
					不要分削除
				表４．１	消去対象外の情報明確化
				表４．２.	HMI を使った方法では消去しなくてもよい情報を追加
				４	プライバシー性低の情報を完全消去要件から除外
				５．２.	「・」の意味を明記
				６.	取説記載事項を追加
△2	a00-02-a	2019/8/21	市原	関連文書	文書追加
				3	同意・撤回内容を修正
△3	a00-03-a	2021/7/6	垣屋 河合	表紙	UNR155 法規対象 ECU のへの適用を明記
				表紙	文書名を Gr 内管理台帳に合わせ修正
				各章	適用 ECU を明確化
				2	図 2.1 の例に生体認証情報追加(JASPAR プライバシー対策ガイドに基づく)
				4	次ユーザが HMI 操作(画面表示、音声通知等)等により簡単に取得可能なプライバシー性高の情報は、ECU 世代、電子 PF に関係なく削除機能が必要(CS 法規要件)な旨追記
				4	適用時期について表 4.1.追記
				4	消去トリガーについての記載を明確化 （および→もしくは　に変更）
				4	外部記憶装置を利用する場合の完全消去について追記
				5.1	外部通信時の暗号化、アクセス制御は UNR155 法規対象であり世代によらず必須とする旨追記
				6	外部記憶装置の取り扱いについて追記

関連文書

本書の関連文書を以下に示す。

表 1.1.　関連文書一覧

仕様書番号	名称
gnsec_std	19PF 情報セキュリティ対策基準書
SEC-ePF-PPI-REQ-SPEC	車載個人・プライバシー情報対策要求仕様書

表 1.2.　公的関連文書一覧

本文中の略称	名称/外部リンク
OECD 8 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 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） 情報技術－セキュリティ技術－プライバシーの枠組み Information technology -- Security techniques -- Privacy framework
GDPR	個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州理事会規則（Apr. 2016） REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
ACEA データ保護原則	ACEA PRINCIPLES OF DATA PROTECTION IN RELATION TO CONNECTED VEHICLES AND SERVICES（Sep. 2015） http://www.acea.be/publications/article/acea-principles-of-data-protection-in-relation-to-connected-vehicles-and-se
CNIL コンプライアンスパッケージ コネクテッドビークルとプライバシーデータ	CNIL Compliance package CONNECTED VEHICLES AND PERSONAL DATA www.cnil.fr △2

目次

1. はじめに

『19PF 情報セキュリティ対策基準書』において、19PF における個人・プライバシー情報の取扱いについて、以下の４項目が示されている。

(a) 各国のプライバシー定義のベースとなっている『OECD８原則』を遵守
(b) 車両外に出す全ての車両情報をプライバシーに該当するとして扱う
(c) 重要なプライバシー情報は車両内のストレージに暗号化して保存
(d) エントリポイントからは、認証がないと情報を取り出せないようにする

(a)の OECD８原則の遵守のため、(1) 個人・プライバシー情報の取扱いに対する同意、(2) ユーザの求めに応じた個人・プライバシー情報の消去、(3) 情報セキュリティ、について車載機における考慮が必要である。さらに(3)の情報セキュリティとして、(b)～(d)により、外部通信の暗号化・認証、保存データの暗号化・アクセス制御が必要となる。

本書では、車載機における、個人・プライバシー情報としての保護が必要な情報を定義し（２章)、個人・プライバシー情報の取扱いに対する同意および同意の撤回（３章)、ユーザの求めに応じたプライバシー情報の消去（４章)、情報セキュリティ（５章）の要件について記述する。

2. 個人・プライバシー情報およびプライバシー性のレベルの定義

＜対象 ECU＞

・Post17CY マルチメディアシステム　or

・19PF Ver.2 以降の個人・プライバシー情報を取扱う車載部品 or

・UNR155 法規対象車両に搭載され、下記に当てはまる車載部品

・プライバシー情報を外部と通信する ECU　or

・プライバシー性高の情報を車両機器の画面、音声などでユーザ通知する ECU

個人・プライバシー情報における“プライバシー性”を定義する。プライバシー性のレベルは、識別性と機微性の２軸によって分類する。

1　機微性（2 段階）

(ア) 高：次の①～③のいずれかに該当する情報

① 『ISO/IEC29100』における Sensitive PII (Sensitive Personally Identifiable Information)

1. 人種、民族、宗教的又は哲学的な信条、政治的見解、労働組合への加入、性生活又は性的指向、肉体的又は精神的な健康を明らかにする情報
2. なりすましを容易にするか、多大な経済的被害を個人にもたらす可能性がある情報（例：クレジットカード番号、銀行口座情報、又はパスポート番号、社会保障番号若しくは運転免許証番号のように政府が発行した識別子）
3. PII（Personally Identifiable Information）主体の現在地を判別するために利用することができる情報
4. 刑事上の有罪判決に関する個人のデータ

② 日本国の『個人情報の保護に関する法律』における要配慮個人情報

③ 『EU 一般データ保護規則（General Data Protection Regulation：GDPR)』第 9 条における特別な種類の個人データ

“人種若しくは民族的素性、政治的思想、宗教的若しくは哲学的信条、又は労働組合員資格に関する個人データの取扱い、及び遺伝データ、自然人の一意な識別を目的とした生体データ、健康に関するデータ又は自然人の性生活若しくは性的指向に関するデータ”

(イ) 低：高以外の情報

2　識別性（4 段階）

(ア) 高：個人特定できる情報

(イ) 中：個人特定の可能性がある情報

(ウ) 低：個人識別の可能性がある情報

(エ) なし：個人特定・個人識別の可能性がない情報

ここでの“特定”とは「ある情報が誰の情報であるかが分かること」、“識別”とは「ある情報が誰か一人の情報であることが分かること（ある情報が誰の情報であるかが分かるかは別にして、ある人の情報と別の人の情報を区別できること）」である。

（出典元：第 5 回パーソナルデータに関する検討会 資料 2-1、2013 年 12 月 10 日、事務局：日本国政府内閣官房）

図 2.1 のように、識別性と機微性の２軸を配置する。

図 2.1 において、識別性高かつ機微性高の象限は“プライバシー性高”の情報、識別性低かつ機微性低の象限は“プライバシー性低”の情報、識別性なしの象限は“プライバシー性なし”の情報、それ以外の残りの４個の象限は“プライバシー性中”の情報と定義する。

プライバシー性が高・中・低のいずれかであるものは、“個人・プライバシー情報”と定義する。

	個人・プライバシー情報ではない	個人・プライバシー情報		
	識別性なし 個人特定・個人識別の可能性がない情報	**識別性低** 個人識別の可能性がある情報（「個人の特徴または行動を示すもの」はここに該当する）	**識別性中** 個人特定の可能性がある情報(「個人の特定に役立つもの」はここに該当する)	**識別性高** 個人特定できる情報(「個人特定できる識別子」「個人とやりとりするために利用することができる識別子」はここに該当する)
機微性高	-	<u>プライバシー性中</u> 例）健康情報	<u>プライバシー性中</u> 例）位置情報・履歴、カメラ画像（顔画像除く）	<u>プライバシー性高</u> 例）クレジットカード番号、リアルタイム位置情報、顔画像、音声、生体認証情報
機微性低	<u>プライバシー性なし</u> 例）単なる 1 個の設定値(例：ON/OFF、OFF/Low/Mid/Hi)、セキュリティログ、部品劣化考慮の学習パラメータ	<u>プライバシー性低</u> 例）車速、シート位置、平均燃費、運転・操作履歴(位置、顔画像、音声除く)、制御履歴、(ドライバが限定される場合の)総走行距離、ドアロック履歴、SOC 履歴	<u>プライバシー性中</u> 例）氏名、年齢、性別	<u>プライバシー性中</u> 例）VIN、サービス用-ID、車載機 ID、ECU シリアル番号 （ユーザや VIN 等と紐づけて管理されている想定)、メールアドレス、アドレス帳、住所、グローバル IP アドレス

図 2.1.　個人・プライバシー情報のレベル

個人・プライバシー情報のうち、情報漏えいした場合に個人の財産の損失につながるものを“個人財産情報”と定義する。個人財産情報は、プライバシー性高の情報に含まれる。

3. 個人・プライバシー情報の取扱いに対する同意および同意の撤回

＜対象 ECU＞

プライバシー情報を車両外部と通信する ECU

車載機の情報を車両の外部へ取り出す際は、VIN や車載機 ID を特定して取り出される。このため、取り出された情報は、すべて個人・プライバシー情報に該当する。故に、車載機の情報を車両の外部へ取り出すには、原則としてユーザから個人・プライバシー情報の取扱いに対する同意の取得が必要である。ただし、例外として、ディーラにおいて修理や故障のために診断情報を収集する場合は、ユーザーの求めに応じて診断サービスを提供するために必要であることから△1、車載機での同意の取得は必要ではない。

＜以下欧州向けのみ＞

『OECD８原則』および、次の３件を根拠とし、“いつでも位置情報の取得を非アクティブにできる選択権”、“位置情報の取得がアクティブであることを示すインジケータを備えること”△2（契約もしくは法的義務のため位置データを取扱う必要がある場合を除く）

なお本件の位置情報の定義は、デジタル変革推進室(元情報セキュリティ推進室)からの指示による。△2

GDPR 第７条３項“データ主体は、いつでも同意を撤回する権利があるものとする。また、同意の撤回は撤回前の同意に基づく取扱いの合法性に影響を与えない。データ主体は、同意を与える以前にその旨が通知されていなければならない。同意の撤回は、その付与と同程度に容易なものでなければならない。”

- ACEA データ保護原則第２章“ACEA 会員企業は、コネクテッド車両およびコネクテッドサービスにおいて、位置を扱う機能を利用者が非アクティブ化できるようにする。ただし、契約もしくは法的義務のため、位置データを取扱う必要がある場合を除く（例：緊急通報)。”△1
- CNIL コンプライアンスパッケージ コネクテッドビークルとプライバシーデータ “いつでも位置情報の取得を非アクティブにできる選択権”、“位置情報の取得がアクティブであることを示すインジケータを備えること”△2

4. 個人・プライバシー情報の消去

＜対象 ECU＞

プライバシー情報を有する ECU

車両の譲渡および廃棄による情報漏えいの対策のため、車載機のメモリ上に保存された個人・プライバシー情報を、ユーザの求めに応じて完全消去できる機能を提供する。

なお、車両内装置のユーザ操作でプライバシー性高の情報を、画面表示・音声で通知する等次の車両ユーザが簡単に情報を得ることが出来る ECU においては UNR155 法規対象とする。

＜導入時期＞

表 4.1. 消去対象 ECU

	消去対象 ECU の適用条件	～19PF	Ver2(Post17CY)	Post19～
1	UNR155 法規対象 ECU	必須	必須	必須
2	1 に当てはならない MM	推奨	必須	必須
3	1,2 以外の ECU	推奨	推奨(変更タイミングあれば対応)	必須

車載機のメモリ上に保存された、プライバシー性高・中・低の情報は、いずれも消去の対象とする。ただし、表 4.2.に該当するものは、消去の対象外にできる。

表 4.2. 消去の対象外にできる情報

#	条件	対象外にできる理由	具体例
1	短時間で上書き・消滅するもの	特別な消去機能がなくても情報が消去される	1 トリップ以内で上書き・消去されるデータ
2	車両△1 工場出荷時から設定されているもの	車の機能のために必要な情報	VIN、車載機 ID
3	+B 電源 OFF で消滅するかつマイコン外部に出力されない(*1)	第三者が外部から情報を取り出す手段がない	+B 電源動作のマイコン内蔵 RAM のデータ
4	ユーザに理由を説明できるもの(*2)△1	品質保証のための情報(*3)△1	故障解析のための走行ログ、制御ログ
		車両の資産価値に寄与する情報、既存の社会ビジネスに影響	総走行距離、バッテリー劣化情報
		法規（消去しない規定）	EDR(エアバック展開後)

*1) 直接メモリにアクセスできる特権機能（例：ダイアグ通信、デバッグポート）を含めて、マイコン

外部に情報が出力されないこと。

*2) データ活用や制御のため、センターへアップロードする情報を一時保存されたものを除く△1

*3) プライバシー性中以上を除く△1

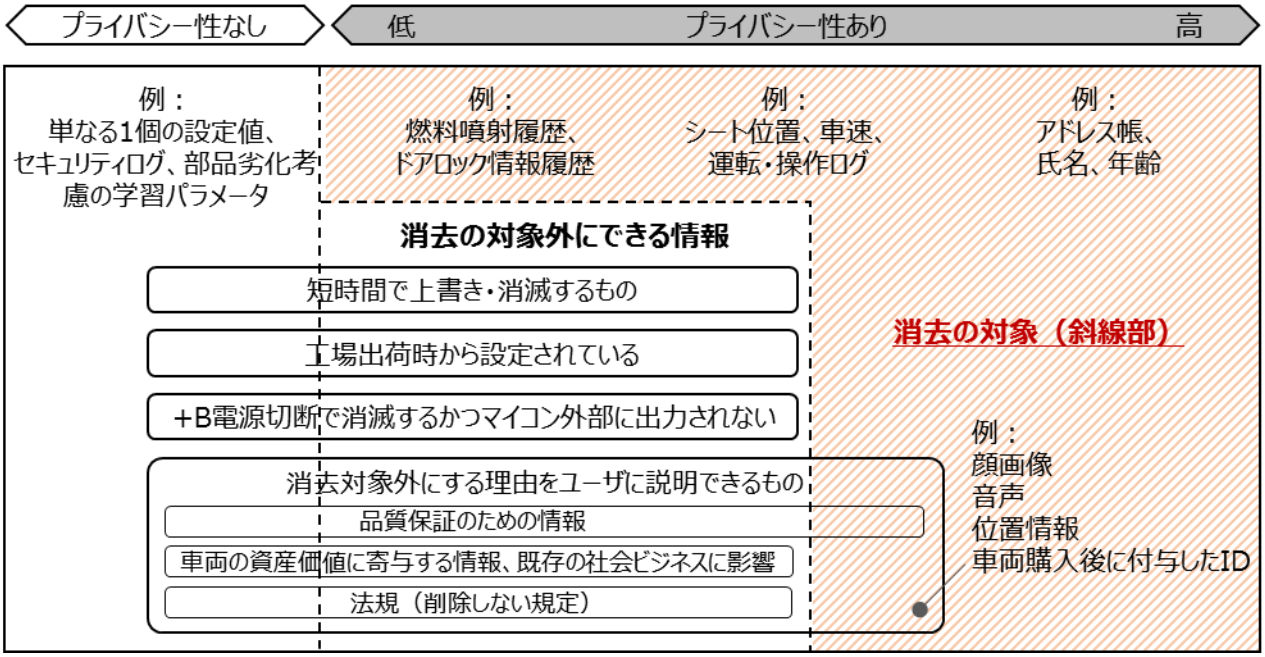

図 4.1.　消去の対象となる情報のイメージ

消去のトリガーは、車載機の HMI を使った方法、もしくは診断ツールを使った方法を用意する。(△4)

但し、トヨタが法的主張のために保存した情報であって消去されると証拠情報が消失するもの、盗難防止用セキュリティ機能のために必要な認証情報であって消去されると盗難防止ができない情報については、HMI を使った方法には対応しなくてもよい(表 4.2)。△1

表 4.3.　HMI を使った方法では消去しなくてもよい情報△1

#	条件	理由	具体例
1	トヨタが法的主張のために保存した情報	証拠情報が消失すると法的主張ができない	画像 FFD、改造歴
2	盗難防止用セキュリティ機能のために必要な認証情報	消去されると盗難防止ができない	暗証番号、生体認証情報

なお、車両の譲渡および廃棄時の消し忘れは、お客様責任として免責とする。

上書き・削除をしても、メモリ上のデータ本体を上書きしないと、データが残る場合がある（例：ハ

ードディスク上のファイル削除コマンド、フラッシュメモリのウェアレベリング（書換え回数均等化））。このため消去の際は、データ復旧ツールによって情報を取り出すことができないように、完全消去をすること。

例として、以下の方法は完全消去に該当する。

1） Secure Erase：ストレージに用意されているデータ消去のコマンドを用いる方法

2） Crypto Erase：データを強固な暗号アルゴリズムで暗号化し、第三者による閲覧を不可能にするデータ消去を行う方法

3） 上書き消去：メモリの特性（ウェアレベリングや予備ブロック等）を考慮し、元データを 1 回以上の上書きしてデータ消去をする方法

なお、プライバシー性低の情報は、完全消去は必須ではなく、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。ただしこの場合、消去後のデータ本体が、ECU 非開封の状態において特権機能を使っても外部に出力できないこと。△1

プライバシー情報を外部記憶装置(SD カード、USB 等)に保存する場合、ECU 自体に完全消去の機能が無くてもよい。ただし、ユーザが車両からプライバシー情報を完全に除去する手段があること。（例：ユーザ自身で PC を使って完全消去が実現可能、車両譲渡時には外部記憶装置を抜く等の運用ができる）。また、その手段・運用等を 6 章に従いユーザへ注意喚起すること。

5. 情報セキュリティ

情報セキュリティ上の想定脅威としては下記の情報漏えいを想定する。

- 車両が外部と通信する際の情報漏えい
- 車両および車載機の盗難による情報漏えい

車両が外部と通信する際の情報漏えい（例：遠隔からの不正アクセス、マルウェア等による情報漏えい）の対策として、車載機から外部と通信をする際は暗号化・認証を行う。車両および車載機の盗難による情報漏えいの対策のため、暗号化保存およびアクセス制御を行う。

5.1. 外部通信時の暗号化・認証

＜対象 ECU＞

プライバシーデータを車両外部と通信する ECU

第三者によりなりすましや盗聴がされる可能性のある通信路（例：無線通信、インターネット）を介して、車載機からセンター等の外部と通信をする際は、通信の暗号化・認証を行う。

センターと通信する際は、センターにおいて車載機 ID や VIN 等を確認して通信することになる。このため、センターと通信するすべての情報は、個人・プライバシー情報として取扱う。

本機能は UNR155 法規対象とし、UNR155 対象車両においては ECU の世代に関わらず必須とする。

5.2. 暗号化保存・アクセス制御

＜対象 ECU＞

マルチメディアシステム

マルチメディアシステムの不揮発メモリ上に、個人財産情報を保存する際は、暗号化かつアクセス制御（必須）の対象とする。また、マルチメディアシステムの不揮発メモリ上に、プライバシー性高とプライバシー性中の情報を保存する際は、暗号化またはアクセス制御（推奨）の対象とする。ただし、表 5.1 に該当するものは、暗号化の対象外にできる。

暗号化またはアクセス制御（推奨）の情報を、暗号化またはアクセス制御の対象とせずに保存する場合は、セキュリティ主管部署に通知したうえで、了解を得ること。

表 5.1. 暗号化保存の対象外にできる情報

#	条件	対象外にできる理由	具体例
1	短時間で上書き・消滅するもの	暗号化保存しなくても情報が消去される	1 トリップ以内で上書き・消去されるデータ

6. お客様への周知[△1]

＜対象 ECU＞

プライバシー情報を有する ECU

透明性の観点から、購入後に事実を知って不快に思うお客様がいないよう、個人・プライバシー情報について取扱書等において次の情報を周知すること

- 車両が保有している情報
- 消去可能な情報と消去方法
- 車両の譲渡および廃棄時の消し忘れは、お客様責任であること
- 外部記憶装置(SD カード、USB メモリ等)についての取扱いに関する注意点
  (ECU は完全消去に対応していないため、お客様責任で外部記憶装置を抜く、データを完全消去する必要がある等)

7. あとがき

本書は、JasPar プライバシーチームにおいて 2018 年 3 月 22 日に合意された文書『プライバシー対象情報の決定について』を参考とした。