解説

車両データのプライバシー対策

Privacy Measures of Vehicle Data

竹森敬祐

Abstract

2017年に日本における改定個人情報保護法の施行，2018年に欧州における一般データ保護規則（GDPR：General Data Protection Regulation）の施行など，世界的に個人データ保護に関する規制が強まりつつある．車両データを活用した走行支援やリモート診断などが期待される中で，運転者との結び付きの強いがゆえに，プライバシー保護に向けた対策が求められる．ここで車両データには，整備や開発に必要なデータや運転者の走行ログなど，その利活用の目的が多様である．また，一つの車両に複数の運転者がいること，車両データを扱う販売店，自動車メーカ，サプライヤが世界に散在することなど，特有の課題がある．本稿では，主にGDPRでケアすべきポイントを整理して，車両データの利活用と法規対応のバランスを鑑みた対策について考える．

キーワード：GDPR，正当な利益，同意，消去・開示権

1. はじめに

車両がネットワークにつながることで，車両データの収集・分析によるメンテナンスへの誘導，車両開発へのフィードバック，近隣レストランなどのレコメンドなど，整備や開発の質の向上，豊かな利用シーンへの発展が期待される．車両に関わるデータには，(i) 所有者（本稿では運転者を含む）の氏名やローンに関するデータ，(ii) Vehicle Identification Number（VIN）や車種などのデータ，(iii) 位置やブレーキ頻度などの走行状態に関するデータ，(iv) Electrical Control Unit（ECU）の応答などを確認する整備データ，(v) 目的地や周辺施設の検索などの趣向に関わるデータなどがある．このように，多様なデータが含まれることから，技術的かつ組織的な保護対策が望まれる．ここで個人データ保護に関するルールや法規に注目すると，APECにはCross Border Privacy Rule（CBPR）というルールが[1]，欧州にはGDPRという法規があり[2]，個人データの安全な管理措置を図らないままデータを越境させることが原則禁止されている．特にGDPRにおいては，違反すると膨大な制裁金を課される恐れがある．

ここで車両に関わるデータには，整備や開発のために収集と分析を行わなければ人命が脅かされるケースや，周辺施設紹介などなくても利便性が下がる程度のケースなど様々である．データの種別や利用目的に合わせて，収集に関する同意取得の要否を検討する必要がある．また一つの車両から複数の運転者のデータが集まることになり，収集に関する全運転者への通知や同意取得が難しい課題もある．

そこで本稿では，車両データの利活用と法規対応のバランスを鑑みた対応案について考えてみる．これは従来からの車両整備の現場に与える影響を抑えつつ，車両メーカやサプライヤの間で適切な水準の安全管理措置を，技術的かつ組織的に図るものである．

2. 車両を中心としたデータ

表1に，車両を中心としたデータを整理する．所有者に関わるデータは，主に販売店で集められる契約に関するデータである．定期的なメンテナンスのお知らせや，新車への乗り換え案内などに利用される．車両に関わるデータは，VINや車種，ECUのファームバージョンなどである．このデータから，リコール対象車が特定される．走行ログは，位置や車速，燃費などである．次期開発や保険料率への還元，渋滞状況の把握などに用いられ

竹森敬祐　正員：シニア会員　(株)KDDI総合研究所スマートセキュリティグループ
Keisuke TAKEMORI, Senior Member (Smart Security Laboratory, KDDI Research Inc., Tokyo, 102-8460 Japan).
電子情報通信学会誌　Vol.101 No.4 pp.394-399 2018年4月

る．特に，Emergency Call（eCall）において，運転者や同乗者が会話できない場合でも，事故の場所と深刻度を推定できるため，人命保護に寄与するデータとして期待される．診断ログは，ECU に生じるエラーや所有者からの不具合申告であり，車両整備に欠かせない．趣向に関わるデータは，In-vehicle Infotainment System（IVI）を通じて入力する目的地や周辺施設，スマホなどから転送されるメールなどのデータである．お勧めスポットなどの広告などに活用される．

これらのデータが，VIN などの識別子で管理される場合，欧州域では全てが個人データの扱いとされている．

3. GDPR を鑑みた車両データのプライバシー対策

GDPR とは，EU 基本憲章において，基本的人権の保護を目的とした規則である．個人データを処理し，個人データを欧州経済領域（EEA：European Economic Area）である EU 加盟国 28 か国＋アイスランド，リヒテンシュタイン，ノルウェーから第三国への移転と処理に関する規則である．表 2 にポイントをまとめる．

以下，車両データのプライバシー保護に関わる GDPR の主な条項を振り返り，対策について考える．なお，GDPR は一般データについての規則であり，車両データに置き換える際に適切に解釈し切れていない点に注意されたい．

表 1　車両を中心としたデータの一例

種別	データの例
（ⅰ）所有者に関わるデータ	氏名，住所，保険，ローン，販売店や車両への意見，…
（ⅱ）車両に関わるデータ	VIN，車種，年式，オプション，ECU ファームバージョン，…
（ⅲ）走行ログ	位置，車速，積算距離，ブレーキ頻度，アクセル開度，排ガス量，燃費，ABS 作動，G センサ，エアバッグ作動，…
（ⅳ）診断ログ	ECU 応答（正常／エラー），申告される不具合，…
（ⅴ）趣向データ	目的地検索，Web 閲覧，メール，…

3.1　第 4 条 定義

様々な用語が定義される中，本稿では“同意”について取り上げる．同意は，強制を受けず，特定的に情報提供を受けた上で，かつ曖昧でないデータ主体からの意思表示でなされる必要があるとされている．ここで，車両に関わる同意が求められるデータ処理に対して，粒度の高い同意取得について議論されている[(3)]．これらより，所有者から，複数の処理行為に対して，個別の同意を取得することが望ましい．なお，車両の走行や IVI 操作に関わらない同乗者は，データ管理者にとって識別され得る自然人ではなく，同意の取得は不要と考えられる．

3.2　第 5 条 個人データの取扱いに関する原則

取扱いに関する原則として，「適法性，公正性及び透明性の原則」，「目的の限定の原則」，「データの最小化の原則」，「正確性の原則」，「保存の制限の原則」，「完全性及び機密性の原則」などが規定されている．

車両の運転者に対して，何のデータが，何の目的で，誰が扱っているのか，プライバシーポリシーを通知する必要がある．プライバシーポリシーは，車両メーカのホームページ（HP）や車両に関する他の説明書と独立した形式で，分かりやすく記載される必要がある．収集されるデータは，プライバシーポリシーに掲げる目的にのみ利用すること，必要最低限のデータに絞ること，不要になれば削除すること，正確かつ安全に管理されることが求められる．

3.3　第 6 条 適法な取扱い

適法な取扱いは，「データ主体からの同意の取得」，「契約の履行」，「法的義務の遵守」，「データ主体の重大な利益の保護」，「公共の利益」，「データ管理者の正当な利益」のいずれかに該当する場合とされている．

具体的には，車両の販売時における契約データ，リコール対応に必要なデータ，故障の未然防止に向けた車両整備に必要なデータ，排ガスの低減や安全運転支援などの開発に必要なデータ，販売店から新車の紹介や整備の案内に必要なデータの取扱いは，適法とみなされ得る．なお，走行ログの収集・分析に基づき，いわゆる走り屋と判断して，タイヤやマフラをお勧めする営業行為

表 2　GDPR における個人データ，処理と移転

	説明	例
個人データ Personal Data	識別されたまたは識別可能な自然人に関連する全てのデータである．自然人に特有な要素によって，直接的にまたは間接的に識別され得るデータ．	氏名，識別子，位置，人種，宗教，遺伝，医療，性的指向などのデータ．
移転 Transfer	第三国の第三者に対して個人データを閲覧可能にするためのあらゆる行為である．	クラウドへのアップロード，電子メールへの添付など．
処理 Processing	個人データまたは個人データの集合に対して行われるあらゆる作業または一連の作業である．	取得，記録，編集，構造化，修正，参照，利用，消去など．

表 3　取扱目的と対応の一例

目的	データ種別	対応	
（A）契約 （販売）	・個人データ ・車両データ	通知 保全	販売契約書を提示し，記載を頂く． 消去に応じない．
（B）法規対応 （eCell，盗難追跡，リコール）	・個人データ ・車両データ ・走行ログ ・診断ログ	通知 保全	法規対応に必要なデータを収集する行為について，企業の HP や車両の取扱説明書の別冊として，プライバシーポリシーを掲載する．消去に応じない．
（C）公共の利益 正当な利益 （整備，不具合解析，開発）	・個人データ ・車両データ ・走行ログ ・診断ログ	通知 保全	法規対応に必要なデータを収集する行為について，企業の HP や車両の取扱説明書の別冊として，プライバシーポリシーを掲載する．消去に応じない．
（渋滞ナビ，災害道路マップ）	・走行ログ （特に位置）	同意 消去	車両販売時にプライバシーポリシーを口頭説明の上で，同意を取得する．消去に応じる．
（D）マーケティング	・個人データ ・車両データ ・走行ログ ・診断ログ ・趣向データ	通知 消去：可能な場合	既存の購入車両を参考としたマーケティングについては，企業の HP や取扱説明書の別冊として，プライバシーポリシーを掲載する．消去，マーケティングの停止に応じる．
		同意 消去：可能な場合	走行ログや趣向データを活用したマーケティングを行う場合，車両販売時にプライバシーポリシーを口頭説明の上で，同意を取得する．消去やマーケティングの停止に応じる．

は，所有者にとって想定外のデータ利用と捉えられる可能性がある．こうした処理を行う場合は，所有者からの同意の取得が求められる．

3.4　第 9 条 特別な種類の個人データの取扱い

特別な種類の個人データとは，宗教的信条，生体データ，健康に関するデータ，性的指向に関するデータなどであり，これらデータの取扱いは原則禁止されている．ただし，データ主体から明示的な同意を得ている場合は，取扱いが認められる．

ここで車両の位置データについては，宗教施設や性的指向に関わる施設への立寄りが推定され得る特性を有する．位置データの収集については，eCall 対応などの法的義務の遵守を除いて，運転者から同意の取得が求められる．

3.5　第 17 条 消去の権利（忘れられる権利）

データ主体は，個人データがもはや必要ない場合，同意に基づく取扱いの同意を撤回した場合などにおいて，消去の権利を持つ．ただし，「データ管理者の法的義務の遵守」，「公共の利益」，「法的主張時の立証」などの理由があれば，消去権は適用されない．

車両の転売や廃棄，若しくは所有者による同意の撤回を契機に，車両に関わるデータの消去が求められる．ここで，前の所有者が ECU を不正に改造していて，中古車として転売し，次の所有者がその改造による不具合で，交通事故に遭ってしまうケースが考えられる．また，廃棄業者が車両から改造された ECU を取り外して転売してしまうケースも考えられる．メンテナンス事業者が悪意を持って ECU を改造してしまうケースも考えられる．こうした改造は人命侵害に至る懸念があり，事故原因の究明や真の加害者を追跡する必要がある．また，所有者が積算距離を短く詐称して，新車に近い状態に見せ掛けて高く売り飛ばすケースもある．これらに対して，ECU のファームウェアに関するデータやエラーログ，積算距離の保全が，有効な対策となる．事故原因の究明や犯人追跡，車両の価値判定に必要となる所有者に関するデータ，車両に関わるデータ，走行ログ，診断ログは，所有者から消去依頼があったとしても，対応すべきではなさそうである．

同意に基づき収集された位置，IVI を通じた目的地，周辺施設の検索履歴などは，消去の対象になり得る．

3.6　第 20 条 データポータビリティ権

データポータビリティ権とは，データ主体の個人データについて一般的に利用され機械可読性のある形式で受け取る権利であり，また他の管理者に移行する権利である．ただし，同意に基づく収集であり，かつ取扱いが自動化された手法で実行されている場合に，適用される．同意に基づき自動的に収集される位置データについては，車両の運転者にデータポータビリティ権がある．このため運転者からの申し出があれば，位置データの開示や，他社への提供が求められる．

GDPR 第 5，6，9，17，20 条を鑑みて，取扱目的ごとに，プライバシーポリシーの通知や同意の取得，データの保全や消去への対応の一例を，表 3 に考察する．通知とは HP や車両マニュアルに分かりやすくプライバシーポリシーを掲載することを意味し，同意とはプライバシーポリシーを説明して運転者から同意を得ることである．保全は，将来の交通事故の原因究明などに備えて，運転者から消去依頼があっても勘案でき得る事情がない限り応じないことを指し，消去は，運転者から依頼

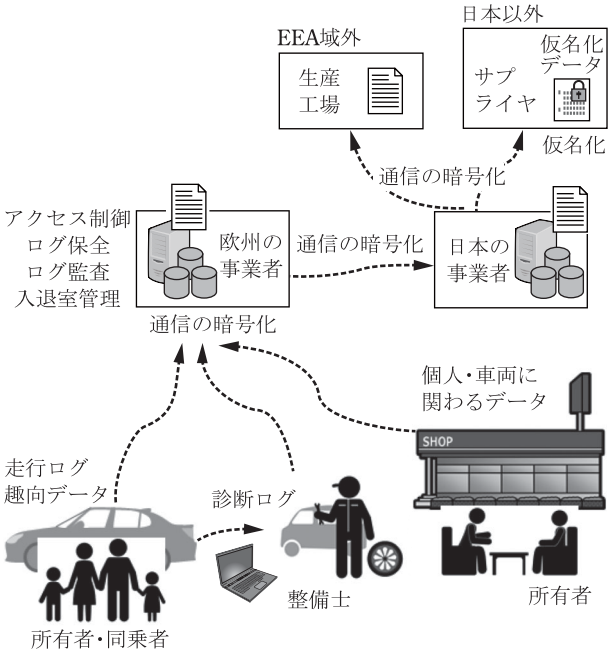

図 1　技術的な対策の一例　通信の暗号化，データセンターでのアクセス制御，ログ保全，ログ監査，入退室管理，サプライヤへの仮名化による提供などの対策が求められる．

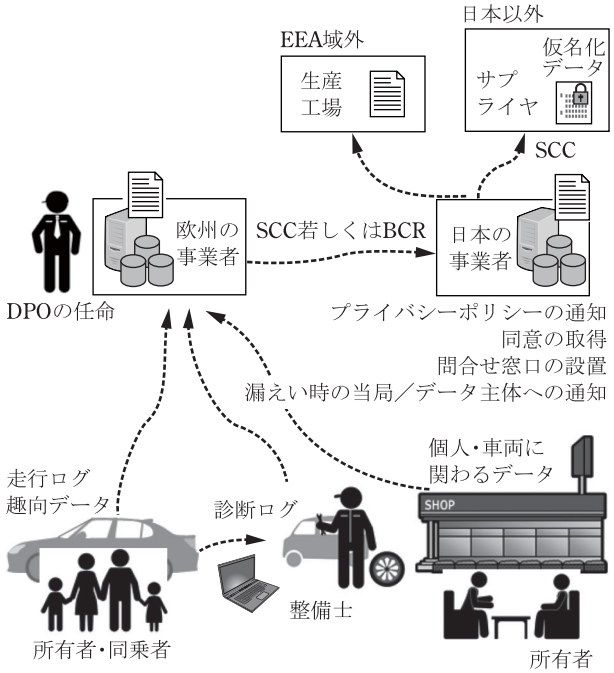

図 2　組織的な対策の一例　DPO の任命，プライバシーポリシーの通知，同意の取得，問合せ窓口の設置，漏えい時の当局／データ主体への通知などの対策が求められる．

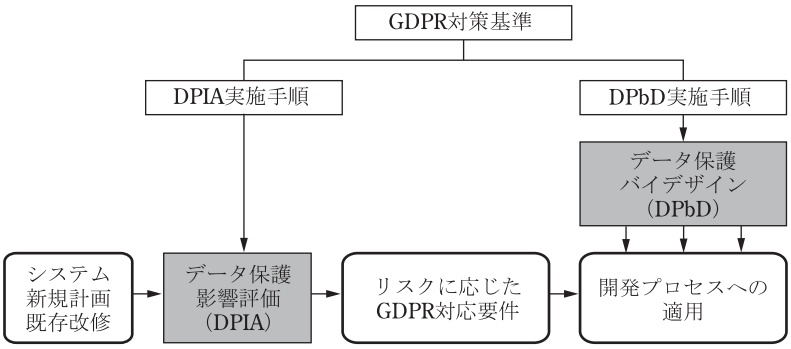

図 3　DPbD と DPIA の開発プロセスへの組込み　システム計画の初期段階での DPIA，開発段階での DPbD が求められる．

があった場合にデータを消去することを指す．

3.7　第 32 条 取扱いの保護

データの管理者及び取扱者は，データ保護のレベルをリスクに見合ったものにするため，適切な技術的及び組織的な対策を実施しなければならない．例えば，通信の暗号化，データセンターにおける人員の入退室管理などの対策が求められる．ECU の不具合解析をサプライヤへ依頼する場合には，誰もが知り得る VIN と合わせて ECU を渡すのではなく，ランダムに生成した ID へと付け替える仮名化により，運転者を容易に特定できないようにする保護措置が望まれる．これらの技術的並びに組織的な対策の一例を，図 1，2 にまとめる．

3.8　第 25 条 データ保護バイデザイン

データ保護バイデザイン（DPbD : Data Protection by Design）とは，システムの設計や開発の段階においてデータ保護施策を組み込むという考えである．システム開発プロセスの要件定義，開発，検証等の各フェーズを通じて GDPR 対応要件を確認するためのチェックリスト及び実施手順を規定する必要がある．

例えば，データ保護バイデザインに配慮すると，IVI に蓄積されているプライバシー性の高い目的地や自宅に関するデータについて，車両の転売時に所有者が自ら消去できる機能を提供するなどの配慮が求められる．

3.9　第 35 条 データ保護影響評価

データ保護影響評価（DPIA : Data Protection Impact Assessment）とは，システム計画の初期段階において

表 4　個人データ保護の観点での 6 か国調査

国	越境の条件	ローカリゼーション	削除権	開示権	DPO 設置
日本	同意	—	○	○	—
タイ（法案）	同意	—	○	—	—
マレーシア	同意	—	○	○	—
インドネシア	当局への報告 and 同意	○ （公共サービス）	○	○	—
インド	事業者の十分性認定（例：ISO27001）and 同意	○	○	○	△ （苦情処理者）
ロシア	対地の十分性認定 or 同意	○	○	○	○

実施するリスクアセスメントである．

DPbD と DPIA を開発プロセスへ適用した様子を図 3 に示す．計画段階で，DPIA を実施し，実際の開発フェーズにおいて DPbD を組み込んでいくことになる．

3.10　第 37 条 データ保護オフィサの指名

データ保護オフィサ（DPO：Data Protection Officer）は，大規模にデータ主体の定期的かつ系統的な処理を行う場合や，中心的な業務が第 9 条の特別な種類のデータを大規模に扱う場合に，指名する義務がある．

既存の車両販売や整備は，定期的かつ系統的なデータ収集が行われているとは言い切れない．しかし，車両がネットワークにつながるようになり，位置などの走行ログの定期的な収集やリモート診断が行われるようになると，DPO を指名する必要が出てくる．

3.11　第 46 条 適切な保護措置に従った移転

適切な保護措置による移転とは，データの管理者または取扱者が適切な保護措置を提供していることを前提として，拘束的企業準則（BCR：Binding Corporate Rules）の認定を受けている場合や，データの移転元と移転先の事業者間で，標準契約条項（SCC：Standard Contractual Clauses）に基づくデータの取扱いがなされている場合などにおいて，データ移転が認められる．

- SCC
  欧州委員会により策定されたひな形であり，適切な保護措置に基づきデータを安全に移転させる契約を事業者間で締結するものである．
- BCR
  EEA 域外に個人データを安全に移転させるための事業者としての自己ルールを認定する制度．BCR の審査監督機関で審査を受けて承認を得ることで，データ主体の同意を得ることなく，同一企業グループ内で個人データの移転が可能となる．

4. 世界的なプライバシー保護規制の動向

ここでは世界的にプライバシー保護への規制が強まっていく中で，日本を含めアジアを中心に筆者が独自に調査した 6 か国の現況を表 4 にまとめる．ここで，各国の限られた法規書しか調査できておらず，領域ごとの省令やガイドラインなどは調査し切れていない．また，法制の施行や改定が次々と進められている状況にあり，個人データを扱う事業者は，自ら調査や分析を行って頂きたい．

表中のローカリゼーションとは，オリジナルデータを当該国のデータセンターやバックアップサーバに置くことが義務付けられていることを指す．該当項目の中には，原則適用されるものの，人命保護などを理由に適用を除外されるケースがあることに注意されたい．

日本では，サービスの解約などで不要になったデータを消去する努力義務が課されている．また，生命，身体，財産その他の権利利益を害する恐れがある場合などを除き，開示権が認められている [4]．

タイでは，いまだ個人情報保護法に相当する法律がなく，10 年間審議が先延ばしされている法案（Personal Data Protection Act）はある [5]．

マレーシアでは，プライバシーリスクに比べて開示に要する費用が過大にならない限り，可読性のある形式で開示に応じる必要がある [6]．

インドネシアでは，大臣令としてデータの国外移転について当局への報告が規定されている．また，公共サービスを提供する電子システム運用者に対して，データセンターを国内に置くべきことが規定されている [7]．

インドでは，パスワード，性的指向，生体情報などがセンシティブデータとして厳しく規制されている．これらのデータを扱う事業者は，Information Security Management System（ISMS）/ISO27001 などの認定取得が求められ，国外にデータを移転させるには，オリジナルデータを国内に置きつつ，本人からの同意が必要とされている [8]．

ロシアでは，ローカリゼーション，削除権，開示権，DPO の設置義務などが制定されており，今回の調査の中では最も厳しい規制となっている [9]．

5. ま　と　め

本稿では，GDPR を中心に，個人や車両に関わるデータの保護策について考えてみた．その際，車両の安全走行に欠かせない整備や開発を制限するような対応を図ると，交通事故や地球環境の悪化を招くことになり，データの利活用とプライバシー保護とのバランスを図ることが重要であるとの立場で検討を進めた．主には，データ収集に関する透明性の確保，位置などのプライバシー性が高いとされるデータへの個別対応，データ移転に関する手続きなどである．なお，本稿は誌面の都合上，全てのルールや法規を取り上げて，考察できているわけではない．また，各国から次々と法令の施行や改定がなされている状況にあり，個人や車両に関わるデータを扱う事業者は，自ら調査や分析を行い，DPO の指導による自主的な対応を進めて頂きたい．

文　　献

（1） 経済産業省，“APEC 越境プライバシールールシステム，”Dec. 2016, http://www.meti.go.jp/press/2016/12/20161220004/20161220004-1.pdf

（2） JIPDEC アーカイブス，“EU 一般データ保護規則（仮訳）について，”Aug. 2016, https://www.jipdec.or.jp/library/archives/gdpr.html

（3） “Resolution on data protection in automated and connected vehicles,” 39th International Conference of Data Protection and Privacy Commissioners, Hong Kong, Sept. 2017, https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-data-protection-in-automated-and-connected-vehicles-.pdf

（4） 個人情報保護委員会，“改正個人情報保護法について，”Nov. 2016, http://www.meti.go.jp/committee/kenkyukai/sansei/daiyoji_sangyo_chizai/pdf/003_02_00.pdf

（5） タイ，“Personal data protection act,” http://web.krisdika.go.th/data/news/news11804.pdf

（6） マレーシア，“ACT 709 personal data protection act 2010,” June 2010, http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf

（7） インドネシア，大臣令，“Peraturan menteri komunikasi dan informatika nomor 20 tahun 2016,” Dec. 2016, https://jdih.kominfo.go.id/produk_hukum/view/id/553/t/peraturan + menteri + komunikasi + dan + informatika + nomor + 20 + tahun + 2016 + tanggal + 1 + desember + 2016

（8） インド，“Information technology（Reasonable security practices and procedures and sensitive personal data or information）rules, 2011,” April 2016, http://meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

（9） ロシア，“Russian federation federal law personal data,” July 2016, https://iapp.org/media/pdf/knowledge_center/Russian_Federal_Law_on_Personal_Data.pdf

（平成 29 年 11 月 2 日受付　平成 29 年 11 月 13 日最終受付）

竹森　敬祐（正員：シニア会員）

平 6 慶大・理工・電気卒．平 8 同大学院修士課程了．同年現在の KDDI 株式会社入社，㈱KDDI 総合研究所へ出向．平 16 慶大大学院博士課程了．情報セキュリティ，プライバシー保護に関する研究開発に取り組む．本会 100 周年マイルストーン認定，著書「Android セキュリティバイブル」など．