# データガバナンスのアーキテクチャがデータ共有に与える影響

The Impact of Data Governance Architectures on Data Sharing Practices

左向　貴代/Kiyo SAKO

慶応義塾大学大学院　政策・メディア・研究科　博士課程

［Abstract］
As data utilization becomes essential for social and economic development, data governance to promote data sharing is being considered and implemented in various countries and regions. However, real-world data sharing has not necessarily progressed, suggesting that the ideal form of governance to promote data sharing may not yet be fully understood. This study focuses on "the impact of data governance on actual data sharing through corporate behavior" as its main theme. By comparing and analyzing the relationship between data governance and data sharing cases in Europe, the United States, China, and Japan, we attempted to elucidate the relationship between data governance and data sharing. The results verified that data governance has at least three fundamental elements: data sovereignty, data security, and data altruism. Furthermore, three distinct forms of data governance architecture were identified: the Western model prioritizing data sovereignty, the Chinese model prioritizing data security, and the Japanese model prioritizing data altruism. These three forms reflect the differences in data governance design philosophies among countries and regions. It was found that the differences in the prioritized elements and the existence of a legally enforceable environment for these elements have varying impacts on actual data sharing. Based on these findings, we presented an improved model of the Japanese architecture as an example of an architectural model suitable for avoiding obstacles to data sharing, promoting data sharing for public benefit, and creating new added value. Thus, the main theme of this study, "the impact of data governance on actual data sharing through corporate behavior," was elucidated from the perspective of how differences in data governance architecture affect data sharing. The results of this study are expected to provide valuable insights for countries and regions in formulating more effective data governance policies.

［キーワード］
データシェアリング、データガバナンス、データ主権、データ利他主義、プラットフォーム、ビジネスエコシステム

## 1.　序

近年は、デジタル機器や通信インフラの進化により大量のデータが生成できるようになり、サービスの普及によって生成されたデータの活用の幅が広がっている。生成データの活用は、組織内のみならず、他組織とのデータ共有により新たな価値を生み出すことができる。そのため、事業の革新や公共性の高いサービスと繋げることで組織の社会的価値を高める動きが出始めている。さらに、個人と企業間、あるいは異なる組織間でのデータ共有を積極的に支援する国や地域では、データ共有プラットフォームが持つネットワーク外部性(Katz & Shapiro, 1985) により、その国や地域のデジタル経済を飛躍的に成長させている。

一方で、個人と企業間、あるいは異なる組織間で共有されるデータにはプライバシーやデータ保護に対するリスクがある。例えば、データ共有空間を提供するプラットフォーム事業者や、その先で関わる他の組織にノウハウや情報が漏洩し、競争力へ影響が生じることや、データ提供先のガバナンスへの不安がある。さらに、データ共有空間を提供する巨大プラットフォーム企業によるデータの独占リスクがあげられる(Zuboff, 2019)。

このような背景から、個人と企業、企業とプラットフォーム事業者間でのデータ流通を阻害する要因を抑制し、データの利活用を活性化させるためのデータガバナンスについて、各地域で関連法規が現れている。

しかし、データガバナンスが有効に機能しているかについては懸念がある。例えば、自動車業界ではカーナビゲーションシステムなどの車載通信装置で車両データの取得を開始してから 20 年以上経過している。しかし、主要自動車メーカーは収集・蓄積された車両データを自社製品の進化に活用したり、外部パートナーとのデータ共

有により事業の付加価値向上に繋げたりすることができていない現状から、果たして、データガバナンスは有効に機能しているのかという疑問が生まれてくる。

もし有効に機能していないなら、その原因はどこにあるのか。原因が明らかになれば、より有効なデータガバナンスが設計できるのではないかと考える。企業間のデータ共有を活性化させ、新たな付加価値を生み出すためには、データガバナンスがデータ共有に与える影響を把握し、より有効なデータガバナンスについての知見を得ることが必要と考える。

## 2. 先行研究

はじめに、本研究におけるデータガバナンスとは、先行研究（Abraham et al., 2019）から援用し、「個人と企業、あるいは企業とプラットフォーム事業者間のデータ共有において、データ資産の価値を高め、データを管理、保護、活用するためのプロセス、ポリシー、権限の体系」と定義する。

次に、2001 年から 2019 年の間に発行されたデータガバナンスに関わる文献を研究分野ごとに分類、評価した先行研究（Abraham et al., 2019）によれば、データ主権はデータガバナンスにおける主要なテーマとなっている。そこで、本研究では、データ共有を行うための基本的要件とされるデータ主権に着目する。データ主権には個人や企業が自らのデータコントロールに対して技術的な主導権を持っていることとする立場（De Mooy et al., 2017）と、国家や地域が、その境界内にあるデータについて他国からの干渉を排除できる権利とする立場（Peterson et al., 2011）があるが、ここでは前者の立場をデータ主権の定義とする。

データ主権に関わるこれまでの文献から、データ主権の機能やデータ主権者の定義について論じている先行研究（Hummel et al., 2018）を本研究の基点とする。

先行研究によれば、データ主体から見て信頼できるデータ共有を可能するためには、データの保護、共有、撤回について自らの意思で常にコントロールできる機能、すなわちデータ制御の可用性が必要であり、それが可能な場合にデータ主権者と言える。データ制御の可用性は、相互信頼に基づくデータ共有を行うために必要なデータガバナンスの中心となるべきものである（Hummel et al., 2018）。

また、データ主体の主権を守るためには、データ主体の自由意志による権利の行使が尊重され、必要に応じて法的執行が可能な社会環境が必要になる。データ主体が権力に対して意思を明確に示せない場合や、データ主体が自ら生成するデータの性質や、誰がアクセスできるのかを認識していない場合、そのデータ主体はデータ主権者ではなくなる。さらに、異なるデータが絡み合うビッグデータの世界では、データ使用許可を与えるべき企業や第三者を将来にわたって全て特定することは困難である。そのため、データ主体に代わって意思決定を行うエージェントを導入することで、データ主体が労力と時間のかかる個別の監督努力をしなくても、データの制御を再度獲得し、維持できるようになる（Hummel et al., 2018）。

一方、データ主権によってステークホルダー間の相互信頼性が構築されたとしても、それは、個人や企業がデータ共有を行うための必要条件に過ぎない。これとは別に、個人や企業がデータ共有を決断する直接的な動機があるはずである。ゲーム理論を用いた先行研究（Kong et al., 2019）によれば、企業に対する合理的なインセンティブとペナルティの仕組みは、データ共有を促進する上で重要な役割を果たす（Kong et al., 2019）。

また、企業のレピュテーションリスクを刺激する仕組みを構築することも、データ共有の促進には有効である。企業がデータ共有に消極的な行動をとれば、企業の評判は低下し、企業が積極的にデータ共有戦略をとれば、企業の評判は向上し、より多くの協力の機会をもたらす（Kong et al., 2019）。

最後に、データガバナンスに関わる文献を研究分野ごとに分類、評価した先行研究（Abraham et al., 2019）によれば、近年、データガバナンスの重要性が高まっているにも関わらず、これまでの研究には、実務家と研究者の両方を導くことができるデータガバナンスの総合的な見方が欠けている。加えて、データガバナンスが企業のパフォーマンスに与える影響については、さらなる調査が必要な状況にある（Abraham et al., 2019）。すなわち、データガバナンスが企業の行動を通じて現実のデータ共有に与える影響を研究した文献は乏しいと言える。

従って、各国・地域のデータガバナンスが有効に機能しているか、現実の事例と関連づけて分析、評価し、より有効なデータガバナンスを生み出すための知見を得ることは、有意義な研究領域と考えられる。

## 3. リサーチクエスチョン

本研究の目的は、データガバナンスがデータ共有に与える影響を把握し、より有効なデータガバナンスについての知見を得ることにある。一方、先行研究（Abraham et al., 2019）によれば、データガバナンスが企業の行

動を通じて現実のデータ共有に与える影響を研究した文献は乏しい。すなわち、これまでにデータガバナンスとデータ共有の関係性を理論化した研究は不十分と考えられる。

こうした背景から、「データガバナンスが企業の行動を通じて現実のデータ共有に与える影響」を主題として、データガバナンスとデータ共有の関係性の解明および理論化に資する探索的アプローチを試みる。

主題を解明するため、考察には 2 つの先行研究を援用した。1 つ目は、データガバナンスの中心はデータ主権にあり、データ主権の存在はデータ制御の可用性に見出すことができるとする先行研究（Hummel et al., 2018）である。しかし、これはステークホルダー間の相互信頼性（Wang et al., 2015）に基づいてデータ共有を行うための必要条件に過ぎない。そこで、2 つ目には企業がデータ共有を決断する直接的な動機づけを行うために、企業に対して合理的なインセンティブやペナルティが働く仕組み、あるいは企業レピュテーションリスクを刺激する仕組みが存在している必要があるとする先行研究（Kong et al., 2019）を援用する。

先にあげた主題を探索するために、具体的に調査可能な対象として以下の 3 課題を設定した。

表 1 調査可能な対象としての課題

| | |
|---|---|
| 課題1 | ● 各国・地域のデータガバナンスにはデータ主権が存在しているか、また、データ主権以外のデータガバナンス要素は存在しているか。 |
| 課題2 | ● 各国・地域のデータ共有において、課題1で明らかになったデータガバナンスの要素は存在しているか。 |
| 課題3 | ● 企業がデータ共有を決断する動機づけとなっている要因は何か、データガバナンスの各要素はその動機づけにどのような影響を与えているか。 |

## 4. 研究方法

本研究では、データガバナンスにおけるデータ主権の役割や機能に関する先行研究（Hummel.et al.,2018）と、企業がデータ共有を決断する直接的な動機づけに関する先行研究（Kong. et al., 2019）を基盤として、データガバナンスの理論的側面とデータ共有の実践的側面の関係性を検証する。このように理論と実践の関係性を検証し、新たな洞察を得るには、事例研究が適している（Eisenhardt, 1989）。さらに、複数の国の事例を比較研究することで、より一般化された知見を得ることが可能になる（Ragin, 1987）。

そこで、欧州、米国、中国、日本におけるデータ共有プラットフォーム事例を取りあげ、各国・地域のデータガバナンスとデータ共有事例の関係性を比較分析する方法で対象課題の検証を進める。

また、事例の対象分野には、脱炭素、資源循環などの社会課題や、電動化や知能化などの技術革新に直面し、課題解決にはステークホルダー間でのデータ共有が不可欠と言われている自動車産業を取りあげる。

はじめに、課題 1 の観点から、各国・地域における主要なデータガバナンス関連法規・戦略を整理し、「データ主権」の存在検証を進めるとともに、データガバナンスを構成するデータ主権以外の要素についても検証する。

次に、課題 2 の観点から、各国・地域におけるデータ共有事例と特徴を整理し、課題 1 で明らかになったデータガバナンス各要素の存在を検証する。

さらに、課題 3 の観点から、データ共有の直接的な動機づけとなるインセンティブ・ペナルティやレピュテーションリスクを刺激する仕組みの存在を検証するとともに、影響を与えているデータガバナンスの要素について考察する。

課題 1～3 の検証結果を踏まえ、各国・地域におけるデータ共有の実態を決定づけているデータガバナンス各要素の優先順位や相対的関係、すなわちアーキテクチャモデルを考察する。データガバナンスとデータ共有の関係性を、アーキテクチャモデルとデータ共有の関係性として整理することで、より一般化された知見を得ることができると考えられる。

最後に、得られた知見から、データ共有の阻害要因を回避し、公益のためのデータ共有の活性化や新たな付加価値の創出に適したアーキテクチャモデルとその課題を考察し、より良いデータガバナンスのあり方について提言する。

## 5. 研究結果

### 5-1. 課題 1

各国・地域のデータガバナンスにデータ主権が存在するか、またデータ主権以外にどのようなデータガバナン

ス要素が存在するかを検証する。

### 5-1-1. 各国・地域のデータガバナンス

欧州、米国、中国、日本のデータガバナンスに関連する主要な法規および戦略について調査し、課題 1 であげた「データ主権」の扱いに注目しながら、主要な構成要素を整理する。

表2　各国・地域の主要なデータガバナンス関連法規および戦略

| 国・地域 | 関連放棄 |
|---|---|
| 欧州（EU） | GDPR（General Data Protection Regulation：EU一般データ保護規則）<br>データガバナンス法<br>データ法 |
| 米国 | カリフォルニアプライバシー権利法（CPRA）<br>ADPPA（American Data Privacy and Protection Act：米国プライバシー法） |
| 中国 | 中華人民共和国国家安全法<br>中国データ3法<br>（中華人民共和国サイバーセキュリティ法、中華人民共和国データ安全法、中華人民共和国個人情報保護法） |
| 日本 | 個人情報の保護に関する法律<br>包括的データ戦略 |

### 5-1-2. 欧州

#### (1) 総論

欧州では、2018 年に EU 域内外での安全な個人データ通流を目指す一般データ保護規則[1]が施行され、個人データに対する包括的な保護の枠組みが制定された。個人データを市場で取引するには、データの所有権を持つことが前提となる。データ生成主体となる個人に自身のデータコントロール手段が行使できることが個人データを保護する手段として最も重視されている。このようなデータ主権の考え方は、欧州のデータ関連規則の基本的なポリシーとなっている。

欧州委員会（EU）では、非個人データについても域内でのオープンかつ安全なデータ流通を実現するための検討が進められ、2020 年に欧州データ戦略[2]を発表した。背景には、米中など海外の巨大データプラットフォーム企業によるデータの独占や、今後の重要分野となる IoT や AI の競争力に対する危機感がある。この欧州データ戦略を支える法規制の中から欧州のデータガバナンスを特徴づける、データガバナンス法、データ法についてまとめる。

#### (2) データガバナンス法

データガバナンス法[3]では、信頼性を確保したデータ流通の促進のため、以下 4 つの特徴的な仕組みが提示されている。

1 一般データ保護規則（GDPR：General Data Protection Regulation）

2 欧州データ戦略（European Data Strategy）

3 データ流通の阻害要因となっているデータ共有サービス事業者への信頼性の改善、公共部門が持つデータの再利用の促進、公益のためのデータ提供などについて規定することなどを目的に 2022 年に制定された。

表3　データガバナンス法の特徴

| |
|---|
| ● 公的機関内にある機密性の高いデータを二次利用できる仕組み |
| ● データ共有やデータの保存を行うデータ共有サービスプロバイダの信頼性を確保する仕組み |
| ● 市民や企業が公益のためにデータを提供できるようにする仕組み |
| ● 目的とするデータを業界や国境を越えて利用できるようにするための仕組み |

全8章からなるデータガバナンス法の中で、これら4つの特徴における信頼性確保の要件は、第2章「公的機関が保有するデータの二次利用」、第3章「データ共有サービスプロバイダ」、第4章「データ利他主義」に記載されている。第4章の第2条にデータ利他主義という概念は、公共サービスの改善、気候変動への対応など、社会然体の利益の実現を目的としてデータ主体またはデータ保有者が自発的にデータを共有する努力や取り組みを指す。企業の利益最大化を目的とするこれまでの資本主義経済の常識を超えたもので、より進歩的な概念であるが、企業がその価値を認めて行動変容を起こせるか否かが問われる。

### (3) データ法

データ法[4]は、現状、大半が有効活用されていないと言われる欧州の産業データを社会全体で活用可能にすることを目的としている。消費者と企業、企業と企業、企業と政府などの関係性ごとにデータアクセスを強化する法案を定めることで、安心してデータ共有が行える環境の構築を目指している。

データ法の主な特徴としては、以下があげられる。

表4　データ法の特徴

| |
|---|
| ● 企業が製品などの利用者に対して生成データを利用させる義務 |
| ● 公的機関への情報提供義務 |
| ● 非個人データの国際移転に関する制限 |

この法案により、EU域内ではよりオープンなデータ活用の促進が期待できるが、一方で競争力のある多国籍企業が欧州のデータにアクセスすることは困難になる。このため、企業の研究開発能力の低下、製品コストの上昇、サービスの質の低下につながる懸念もある。

なお、データ法では、表4であげたように、企業に対しては利用者に生成データを利用させる義務を課すが、一方でユーザーおよび第三者に対しては、データ保有者から提供されたデータを競合製品の開発などに利用してはならない義務を課すなど、主体間相互にデータの取り扱いについて規定している。

## 5-1-3. 米国

### (1) 総論

米国では、公的機関のデータ活用について連邦データ戦略[5]が策定された。

一方、民間データ活用促進については、米国はGAFAM[6]で代表される世界的な巨大IT企業が多数存在することから、これまで政府が強く介入することはなかった。しかし、近年は、デジタルデータの多くは米国の巨大データプラットフォーム企業に独占されている状況であることから、個人データの取り扱いに関しては、州レベルで規制の検討が始まり、次いで連邦レベルでも検討が進められてきた。

こうした中で、2022年に、包括的な個人情報保護を目的とするADPPA（American Data Privacy and Protection Act：米国データプライバシー法）の草案が議会へ提出されたが、いまだに連邦レベルでの個人情報の取り扱いに関する法令は成立していない。

---

4 2020年の欧州データ戦略の法的枠組みの一つとして、2022年に発表された。

5 連邦データ戦略[5]（FDS：Federal Data Strategy）は、2019年2月策定され、全ての連邦政府機関がデータのセキュリティ、プライバシー、機密性を保護しながら統合的にデータを活用し、国民に対するサービス提供やリソース管理を行うための10年間のビジョンを掲げたものである。

6 Google, Amazon, Facebook/現Meta, Apple, Microsoft

### (2) 州法

米国のプライバシー保護法は、カリフォルニア州から始まった。カリフォルニア州では、消費者プライバシー法（CCPA）[7]が2018年に成立、2020年にはCCPAを改正するカリフォルニアプライバシー権利法（CPRA）[8]が可決された。これを皮切りに、バージニア州、コロラド州などで、州レベルのプライバシー法が成立した。

CPRAは消費者の権利の拡大、有効な同意基準の詳細化などいくつかの点で特徴がある。例えば、同意とは、自由に与えられた、具体的で、情報に基づいた、消費者の望みが明確に示されたものとする、GDPRとほぼ同様の定義としている。また、CPRAは、1974年以降、連邦政府に適用されてきた公正情報行動原則[9]（FIPPs）に従い、データの最小化、目的の特定、セキュリティ、透明性、正確性、説明責任といった原則を民間企業にも適用することを明記している。

一方、カリフォルニア州には規制がないものの、他州で規制されているものとして、機微情報の取得規制、データ保護アセスメント義務があげられる。

## 5-1-4. 中国

### (1) 総論

2015年に中華人民共和国国家安全法[10]（以下、国家安全法）が成立した結果、中国は対外的にはファイアーウォールを築いて内外を仕切り、データ流通を厳格に管理する方向に動き出した。特に、重要データの越境に関しては、重要情報インフラ運営者を政府の部門が審査することなどを取り決めた中華人民共和国サイバーセキュリティ法（以下、サイバーセキュリティ法）が2017年に制定、施行された。その後、2021年には中華人民共和国データ安全法（以下、データ安全法）、同年11月には中華人民共和国個人情報保護法（以下、個人情報保護法）が施行された。

サイバーセキュリティ法、データ安全法、個人情報保護法は、中国データ3法と呼ばれ、国家安全法と合わせて中国におけるデータガバナンスを特徴づける基本法となっている。

中国データ3法には次のような特徴がある。

表5　中国データ3法の特徴

| | |
|---|---|
| 国家が個人に優先する | ● 第一に、情報に関して優先されるのは、国家の安全である。 個人情報保護法および国家安全法はともに憲法に基づいて定めるとしているが、その憲法では、中国公民が国家の安全を毀損することは認められないとしている。 |
| データ流通に関する徹底した対外的防御 | ● 国家安全法、サイバーセキュリティ法、個人情報保護法では、いずれも中国国内でデータを収集し、生産した情報は中国国内に留めなければならないとしている。 |
| 個人情報関連法規制の整備 | ● 個人情報保護の枠組みは、2021年の民法、個人情報保護法、データ安全法の施行・成立で整ったとされている。民法（第1032条）では、いかなる組織または個人も、偵察、侵犯・いやがらせ、漏洩、公開などの方式により他人のプライバシー権を侵害してはならないとしている。 |

### (2) 自動車産業に見られるデータ政策

中国のデータガバナンスの特徴を把握するため、自動車産業に対して2021年に公表された自動車データ安全管理若干規定、自動車採取データ安全要求指南、およびデータ安全技術自動車収集データに関するパブリックコメントを整理する。

対象となる自動車データは、車外のデータ、コックピットデータ、稼働データなどとしているが、それぞれのデータ項目は多岐におよび、実質的に有益な車両データは全て対象となっている。

また、自動車産業において自動車データを取り扱う事業者とは、自動車メーカー、部品・ソフトウェアサプライヤー、ディーラー、メンテナンス会社、旅行会社など自動車関連業種を網羅している。

自動車データの流通に関して、中国データ3法の中核課題であるデータの越境については、重要なデータは、法律に基づいて領域内に保存されなければならず、業務上の必要性から国外で提供する必要がある場合は、国務

7 消費者プライバシー法（CCPA：California Consumer Privacy Act）

8 カリフォルニアプライバシー権利法（CPRA：California Privacy Rights Act）

9 公正情報行動原則（FIPPs：Fair Information Practice Principles）

10 国家安全法は、2015年に成立した。総体的国家安全を維持することを定め、第25条において、技術革新を通じて、国家のインターネット空間の主権、安全と利益を保護することを求めている。

院の関連部門と連携して国家ネットワーク情報部門が実施するセキュリティ評価に合格しなければならないとしている[11]。ここで重要なデータとは、改ざん、破壊、漏洩、不正アクセス、不正使用されると国家安全保障、公共の利益、または個人や組織の正当な権利や利益を危険にさらす可能性があるデータを指す。また、自動車採取データ安全要求指南によれば、車外のデータ、車内のデータ、位置追跡データは越境してはならないと定められている。こうした規定のため、海外の自動車メーカーは生産・開発活動に支障が生じていると言われている。

### 5-1-5. 日本

#### (1) 総論

データガバナンスの基盤をなす個人情報の保護に関する法律[12]（以下、個人情報保護法）が2003年に制定されているが、近年では個人データや企業が生成する非個人データを有効活用し、新たな経済を創出することで、企業や国家の国際競争力を高めるためのデータ戦略も検討された。その結果、2021年に包括的データ戦略[13]が閣議決定された。包括的データ戦略では、データの適正な利活用の推進に向けて、戦略・政策、組織、ルール、連携基盤、データ、利活用環境、インフラなど7つの階層における課題と方策を取りまとめている。

#### (2) トラスト基盤の構築

データガバナンスについては、主に包括的データ戦略のアーキテクチャのルール階層（第5層）においてトラスト基盤の構築およびトラスト基盤構築に向けた論点整理としてまとめられている。

第5層の説明[14]によれば、Society 5.0の実現には、フィジカル空間をサイバー空間に変換する層が必要となるが、両者の関連を確保するため様々なレベルのトラストを確保することが鍵であるとしている。

ここで指摘されるトラストには、サイバー空間におけるデータの真正性や完全性からなるデータそのものの信頼性、データの属性を含めた信頼やデータの提供者の信頼性などがあげられている。また、データのトラストの要素として、主体・意思（意思表示の証明）、事実・情報（発行元証明）、存在・時刻（存在証明）を指摘している。

一方、トラスト基盤の構築に向けた主要な論点に、トラストアンカーの機能、認定スキームの創設、トラスト基盤の創設、認定の効果、認定基準、クオリファイドサービスの公表、国際的な相互承認をあげている。

包括的データ戦略では、データを管理、保護、活用するための、プロセス、ポリシー、権限などについて一通りカバーしていると考えられることからデータガバナンスの指針は示しているものの、法規にはなっていない。

### 5-1-6. データガバナンスの構成要素

課題1の観点からデータ主権に関わる法規の存在を検証するとともに、各国・地域のデータガバナンスを構成する基本的要素を抽出する。

1つ目の構成要素としてデータ主権があげられる。データ主権は、主にプライバシー保護と自己決定権に基づく同意管理に関わる取り決めと言える。

欧州は、GDPR、データガバナンス法により、個人および企業のデータ主権が明示されている。米国は、カリフォルニアプライバシー権利法などの州法において個人情報保護の形でデータ主権が明示されている。中国は、同じく個人情報保護法の形で個人のデータ主権が表明されている。日本は、個人情報保護法および包括的データ戦略において、個人および企業のデータ主権が明示されている。以上のように、4地域全てのデータガバナンス関連法規において、データ主権は共通の構成要素として存在している。

2つ目の構成要素として、データ安全性があげられる。ここで安全性とは、安全なデータ共有を担保する技術的な信頼性に加えて、安全なデータ利用を行うための基準や制限に関わる取り決めを指す。具体的には、データセキュリティ、データ品質、データ越境などのリスク管理についての取り決めと言える。

---

11 自動車データ安全管理若干規定（試行）の第11条

12 個人情報の保護に関する法律（個人情報保護法）は2003年に制定され、2005年に全面施行された。その後、デジタル化やグローバル化などの社会変化や、個人情報に対する世論の高まりの中で、これまでに3度の改革が行われ、現在に至っている。個人情報保護法における個人情報とは、特定の個人を識別できる情報を指し、個人識別が可能な情報が含まれる情報は全て個人情報とされる。また、個人データを本人以外に提供する時は、原則として、事前の同意が必要とされている。

13 包括的データ戦略は、2021年に国と地方公共自治体のデジタル化を主導するデジタル・ガバメント閣僚会議がデジタル国家にふさわしいデータ戦略を策定するデータ戦略タスクフォースを開催し、その成果として同年閣議決定された。

14 包括的データ戦略 各論1.トラスト 参照

欧州は、データガバナンス法およびデータ法で、技術的な信頼性確保やデータ越境に関する規則を定めている。米国は、CPRAなどの州法で、個人情報保護に必要な技術または必要機能についての取り決めや、機微情報[15]に関わるデータの扱いを定めている。中国は、国家安全法、サイバーセキュリティ法、データ安全法などで、データ安全性の技術的な取り扱いやデータ越境に関する規則を定めている。日本は、個人情報保護法および包括的データ戦略において、個人や企業のデータ共有が安全に行われるための必要機能やデータ共有基盤作りに関わる取り決めが明示されている。

3つ目の構成要素として、データガバナンス法（欧州）の特徴であるデータ利他主義があげられる。データ利他主義は「公共の利益のためにデータを自発的に共有すること」と定義される（Micheli et al., 2020）。公益性や社会に新たな価値創造をもたらすデータ共有に関わる取り決めと言える。

欧州以外のデータガバナンス法規においては明記されていないが、各国ともにデータ共有の主要な目的の一つに公益性を掲げており、データガバナンスの潜在的かつ重要な構成要素と考えられる。

課題1の研究結果として、データガバナンスを構成する基本的な3要素の機能（図1）および法規との関係性（表6）についてまとめる。

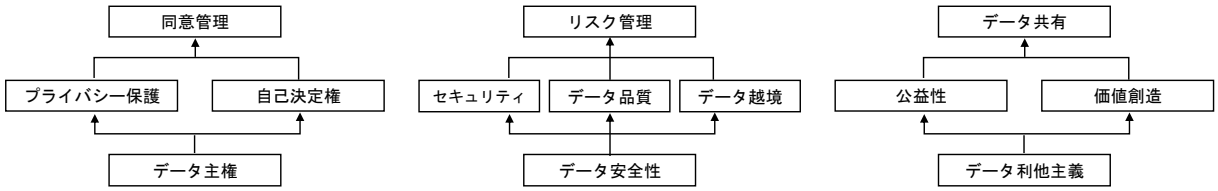


図1　データガバナンスの構成要素と機能

表6　データガバナンスの構成要素と各国法規との関係

| 基本的要素 | 欧州 | 米国 | 中国 | 日本 |
|---|---|---|---|---|
| データ主権 | • データ生成主体となる個人に自身のデータコントロール手段が行使できることを最も重視。（GDPR）<br>• 上記データ主権の考え方は、欧州のデータ関連規則の基本的なポリシー。（GDPR） | • 同意とは、自由に与えられた、具体的で、情報に基づいた、消費者の望みが明確に示されたものとし、GDPRとほぼ同様の定義。（カリフォルニア州法） | • いかなる組織または個人も、偵察、侵犯・いやがらせ、漏洩、公開などの方式により他人のプライバシー権を侵害してはならない。（個人情報保護法） | • 個人情報とは、特定の個人を識別できる情報を指し、個人識別が可能な情報が含まれる情報は全て個人情報。（個人情報保護法）<br>• 個人データを本人以外に提供する時は、原則として、事前の同意が必要。（個人情報保護法） |
| データ安全性 | • データ共有やデータの保存を行うデータ共有サービスプロバイダの信頼性を確保する。（データガバナンス法）<br>• 非個人データの国際移転に関する制限。（データ法） | • データの最小化、目的の特定、セキュリティ、透明性、正確性、説明責任といった原則を民間企業にも適用。（カリフォルニア州法）<br>• 機微情報の取得規制、データ保護アセスメントの義務化。（他の州法） | • 総体的国家安全を維持するため、技術革新を通じて、国家のインターネット空間の主権、安全と利益を保護する。（国家安全法）<br>• 情報に関して優先されるのは、国家の安全。（国家安全法）<br>• 中国公民が国家の安全を毀損することは認められない。（国家安全法）<br>• 中国国内でデータを収集し、生産した情報は中国国内に留めなければならない。（国家安全法、サイバーセキュリティ法、データ安全法） | • サイバー空間におけるデータの真正性や完全性からなるデータそのものの信頼性、データの属性を含めた信頼やデータの提供者の信頼性がトラストの基本。（包括的データ戦略）<br>• トラストの要素は、主体・意思（意思表示の証明）、事実・情報（発行元証明）、存在・時刻（存在証明）。（包括的データ戦略） |
| データ利他主義 | • 公的機関内にある機密性の高いデータを二次利用できる。（データガバナンス法）<br>• 市民や企業が公益のためにデータを提供できるようにする。（データガバナンス法）<br>• 企業が製品などの利用者に生成データを利用させる義務。（データ法）<br>• 公的機関への情報提供義務。（データ法） | | | |

## 5-2.　課題2

各国・地域のデータ共有において、課題１で明らかになったデータガバナンスの要素が存在し、機能しているか否かを検証する。

15 個人の走行履歴情報など。

### 5-2-1. 各国・地域のデータ共有事例

自動車業界における、各国・地域の代表的なデータ共有プラットフォーム事例を選定し、内容を整理する。

### 5-2-2. 事例調査のフレームワーク

データ共有事例のシステムアーキテクチャと分析の視点を示す（図2）。右側がシステムアーキテクチャ、左側が分析の視点となる。まず、データ共有システムのアーキテクチャは、図のようなレイヤー構造になる。今回対象としている自動車分野を例にすると、一番下に顧客である個人、その上に個人情報の集約先として企業、その上に自動車メーカーのデータを束ねて編集するデータ共有プラットフォーム事業者、そして、一番上に、プラットフォームから取得した共有データに基づいてデータ活用サービスを行うサービス事業者が位置する。

この構図は、どのような分野のデータ共有においても、共通の構造と考えられる。システムアーキテクチャを示すことで、データ生成主体、データ収集主体、データ編集主体、データ活用主体が明確になる。

システムアーキテクチャに基づく1つ目の分析視点として、課題1より、データ主権の存在があげられる。個人および企業のそれぞれにデータ制御の可用性が確保されているか否かに着目することで検証できる。また、データ主権の実現に関わる分析視点として、データの安全性があげられる。データ主権およびデータ安全性は、事例におけるプライバシー保護やデータセキュリティへの取り組みに着目することで検証できる。

2つ目に、課題3に繋がる分析視点として、企業にインセンティブやペナルティが働く仕組み、あるいは企業のレピュテーションリスクを刺激する仕組みの存在があげられる。これらを検証するために、2つの項目を整理した。データ提供を行う企業やデータを活用するサービス事業者、すなわちメンバーシップと、プレイヤー間の契約や収益モデルの構造、すなわちビジネスモデルである。

企業にとって、個人とデータ共有契約を結ぶ主要な目的は顧客囲い込みにあるため、顧客にとってサービス事業者のサービスが魅力的であり、それが企業とデータ共有契約を結ぶ動機になるのであれば、データ共有プラットフォーム事業者とデータ共有を行うインセンティブが働く。一方、顧客にとって、サービス事業者が提供するサービスが魅力的であるにも関わらず、企業がデータ共有プラットフォーム事業者やサービス事業者との契約を行わないためにサービスを享受できなければ、企業とのデータ共有契約を結ばない可能性がある。その場合、企業がデータ共有プラットフォーム事業者とデータ共有を行わないことは、企業にとって、顧客を囲い込む機会の損失リスク、あるいは必要なサービスを提供しない企業というレッテルを貼られるレピュテーションリスクが生まれる可能性がある。

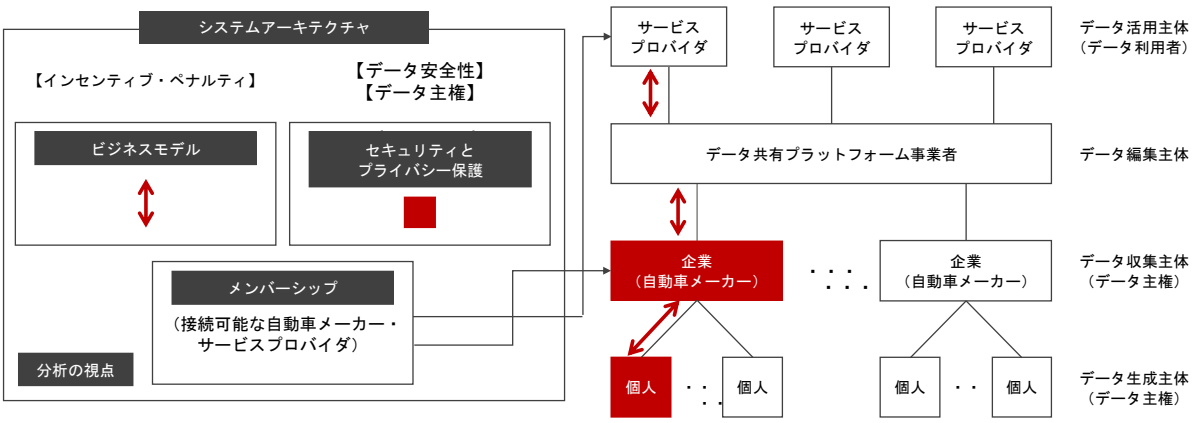


図2　データ共有事例のシステムアーキテクチャと分析の視点

#### (1) 欧州

欧州においては、自動車データ共有プラットフォームを運営する主要企業の一つである、ドイツのCARUSO[16]

[16] CARUSOは、自動車アフターマーケット業界の独立した取り組みとして、2017年に創業された事業会社で、持続可能なエコシステムを構築するために、多様性、オープン性、中立性を最重視している。それは、主要な自動車メーカー、サプライヤーなど468以上の法人を代表する10名の株主よりなる株主構造にも反映されている。CARUSOが提供する自動車データ共有プラットフォームは、欧州自動車部品協会からニュートラルサーバーとして支持されている。

を取りあげる。

表7　欧州：CARUSOの自動車データ共有プラットフォーム

| | |
|---|---|
| システムアーキテクチャ | • 各自動車メーカーの車両データは車載通信機を通じて各メーカーのデータサーバーに集約される。<br>• 自動車メーカー各社とCARUSOとの個別契約に基づき、自動車メーカー各社のデータサーバーはCARUSOの自動車データ共有サーバー（CARUSO dataplaceと呼称される）に接続される。<br>• CARUSOの自動車データ共有サーバーでは、自動車メーカーごとに異なる車両データをCARUSOが定義する項目ごとに整備し、これらのデータは標準インターフェース（Application Programming Interface, 以下API）を介して外部のサービスプロバイダーに提供される。 |
| セキュリティとプライバシー保護 | • CARUSOは、全てのデータ保護法およびGDPR に準拠している。<br>• サービスプロバイダは車の所有者との契約内容に基づき、車両識別番号（Vehicle Identification Number）を使用して車のデータをリクエストするが、その際に車両の所有者がどのデータを誰と共有できるかを完全に制御できる「同意管理技術」を用いるため、セキュリティを確保され、プライバシーは守られるとしている。 |
| 接続可能な自動車メーカーとサービスプロバイダー | • 現在、CARUSOには欧州の主要自動車メーカー16社の車両が接続可能になっている<br>• CARUSOが提供する自動車データ共有サーバーは、フリート管理、テレマティクス保険、カーシェア、緊急通報、充電サービス、などのサービスプロバイダが利用している。 |
| ビジネスモデル | • サービスプロバイダよりCARUSOに対して各種支払方法に応じたサービス料を支払う。<br>• 支払い方法は、車両毎の月払い、定額払い、都度払いの他、決められた車両に対して任意データにアクセスできるパッケージなどがある。 |

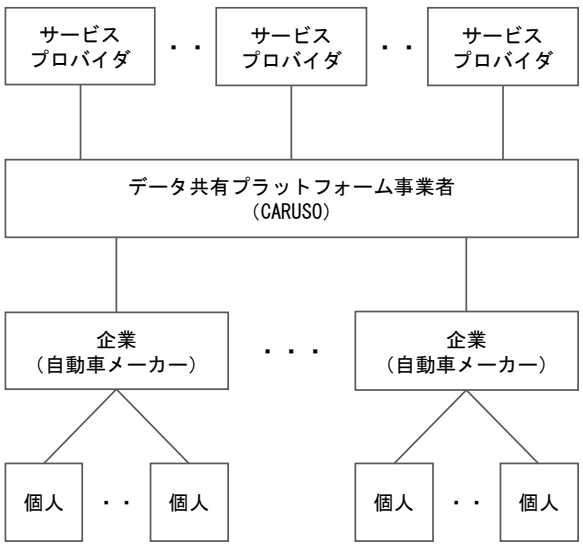


図3　欧州：CARUSOのシステムアーキテクチャ

### (2) 米国

米国における自動車データ共有プラットフォームとして、主要企業の一つであるSmartcar[17]を取りあげる。

17 2015 年に設立されたSmartcarは、モビリティ関連サービスを提供する事業者に、車両データを用いたサービスアプリケーションの開発環境とサービス時に必要な車両データを提供するプラットフォームで、米国と欧州を対象市場としている。自動車保険、カーシェアリング、EVの充電制御やフリート管理に至るまで、多くの企業が、SmartcarのAPIを使用して、各企業のサービスに必要な顧客の車両データにアクセスできる。Smartcarは、コネクテッドカーのみを対象としている。コネクテッドカーとは、自動車に内蔵されたセルラーモデムを経由してインターネットに接続できる車両を指す。Smartcarによれば、現在、米国で販売されている自動車の80%が、各自動車メーカーのデータサーバーに接続されている。

表8　米国：Smartcar の自動車データ共有プラットフォーム

| | |
|---|---|
| システムアーキテクチャ | • 各自動車メーカーの車両データは車載通信機（セルラーモデム）を通じて、各自動車メーカーのデータサーバーに集約される。自動車メーカーは各社のデータサーバーを通じて、顧客に独自のモバイルサービス（スマートフォンアプリなどを用いて利用できるアプリケーション）を提供する。<br>• 一方、スマートフォンアプリでSmartcarを利用するサービスプロバイダーの車両データ要求に対する顧客の同意が得られると、Smartcarは顧客のアカウントを使って当該自動車メーカーが提供するモバイルサービスから必要な車両データをスクレイピング（抜き取り）し、Smartcar APIで接続されるサービスプロバイダーにデータを提供する。 |
| セキュリティとプライバシー保護 | • Smartcarは、一般データ保護規則（GDPR） に準拠し、顧客にサービスを提供するために必要なデータのみを処理する同意ベースのプラットフォームであるとしている。<br>• セキュリティと可用性のトラストサービス基準であるSOC 2 Type 2に準拠し、サービスへの全てのリクエストは HTTPS 経由で通信され、プラットフォームで保存される全データは Advanced Encryption Standard 256 ビット暗号化で保護される。<br>• また、独立したセキュリティ会社による侵入テストと脆弱性スキャンを定期的に受けており、プラットフォームは業界標準とされるクラウドインフラ上でホストされるため、最大のパフォーマンス、復旧力、サービスの展開性を保証できるとしている。 |
| 接続可能な自動車メーカーとサービスプロバイダー | • 現在、Smartcarで利用可能な自動車メーカーは北米および欧州を合わせて39 社となっている。<br>• Smartcarは、自動車保険、フリート管理、電力事業、カーシェア、充電サービスを提供するサービスプロバイダーなどに利用されている。 |
| ビジネスモデル | • サービスプロバイダーよりSmartcarに対して、無料のお試しから、開発用、事業用など用途や規模に応じたサービス料を支払う。 |

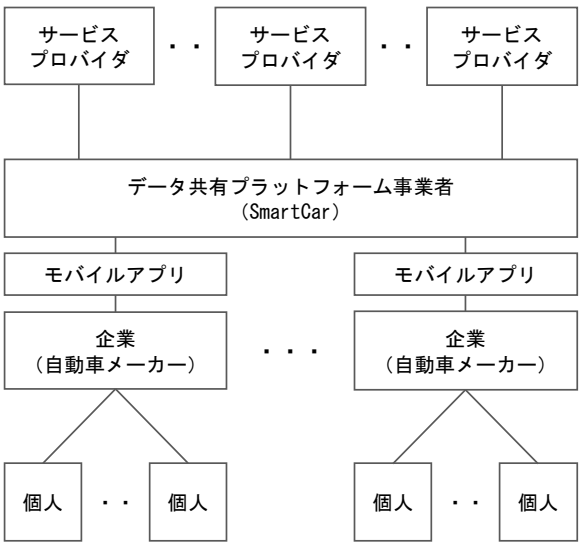


図4　米国：Smartcar のシステムアーキテクチャ

### (3) 中国

中国における自動車データ共有プラットフォームには、新エネルギー車（New Energy Vehicle、以下NEV）を対象に、地域または国家のトレーサビリティ管理プラットフォームが存在する。ここでは、地域プラットフォームの一つである上海新エネルギー車公共データ収集観測研究センター[18]を取りあげる。

中国においては、NEV ビジネスに参入する自動車メーカーの資格要件として、車両データをリアルタイムで観測・収集可能なRTM[19]装置の装着が義務づけられている。これは、2017年に工業情報化部が省令第39号新エネルギー車メーカーおよび製品アクセス管理規定で定めているものである。

さらに、同省令の第十七条では、新エネルギー自動車生産企業は、新エネルギー車製品の運転安全状態観測プラットフォームを設置し、新エネルギー自動車製品のユーザーとの合意に基づき、販売された新エネルギー自動車

18 上海新エネルギー車公共データ収集観測研究センターは、2014 年に正式に設立され、事業指導は上海経済情報委員会によって提供されている。 現在、当該地域における世界最大のNEVデータ収集プラットフォームであるとともに、上海で唯一のNEVの公的データ収集、保管、分析サービスプラットフォームである。

19 Real Time Monitor

製品の運転安全状態を観測する。 また、企業観測プラットフォームは、地域および国の新エネルギー車普及アプリケーション観測プラットフォームとドッキングする必要があるとしている。

表9　中国：上海新エネルギー車公共データ収集観測研究センターの自動車データ共有プラットフォーム

| | |
|---|---|
| システムアーキテクチャ | • 基本的なシステム構成は、工業情報化部が制定した省令第39号の第十七条に基づいている。<br>• はじめに、NEVを販売する各自動車メーカーの車両には全車にRTMが装着される。<br>• 次に、自動車メーカー各社のデータサーバーは地域および国のNEV普及アプリケーション監視プラットフォームに接続される。<br>• 地域および国のNEV普及アプリケーション監視プラットフォームは、各自動車メーカーから収集される車両データを国家規格（GB/T32960）に準拠した形式で項目毎に整理し、これらのデータを政府や地方自治体、自動車メーカー、サプライヤー、サービス事業者などに提供する。 |
| セキュリティとプライバシー保護 | • 各自動車メーカーが運用するデータサーバーとの接続は、「企業とユーザーとの合意に基づく」とされる。ただし、その方法は明らかではない。<br>• また、省令第39号第十七条には、「新エネルギー自動車メーカーおよびその職員は、新エネルギー車製品の運転安全状態に関する情報を適切に保管し、開示、改ざん、破壊、販売、または違法に他人に提供したり、製品の運転安全状態に関係のない情報を監視したりしてはならない。」とあり、これに基づく技術的措置を講じていると考えられる。 |
| 接続可能な自動車メーカーとサービスプロバイダー | • 2018年時点で、上海新エネルギー車公開データ収集監視研究センターには、乗用車60社、商用車53社の車両23万台が接続されている。<br>• 一方、上海新エネルギー車公開データ収集監視研究センターが提供する自動車データの利用者は、自動車産業、部品産業、保険業界、政府および地方自治体、コンサルティング業界などである。 |
| ビジネスモデル | • 個人の車両と各自動車メーカーが運用するデータサーバーとの接続は、各自動車会社が運用する有償のコネクテッドサービス契約に基づく。<br>• 一方、上海新エネルギー車公開データ収集監視研究センターは、センターの利用者に対して有償、無償（政府、地方自治体向けなど）で車両データを提供しているが、支払い方法やサービス料については明確でない。 |

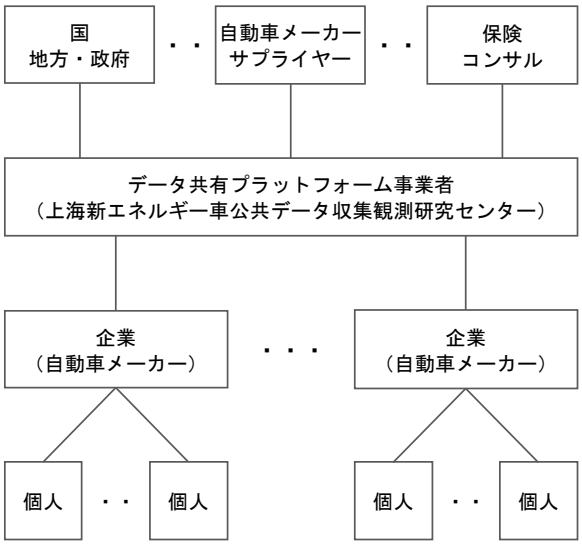


図5　中国：上海新エネルギー車公共データ収集観測研究センターのシステムアーキテクチャ

### (4) 日本

日本においては、欧州、米国、中国に見られるような自動車データ共有プラットフォームは存在しないが、公共的なサービスにおいて自動車各社がデータ共有を行っている事例として、VICS センター[20]が提供するプローブ情報活用サービス（実証実験中）を取りあげる。

VICS により、ドライバーはカーナビゲーションを通じて、広範囲な交通情報が取得できるようになり、渋滞を回避したルート案内や到着予想が可能になった。一方、交通情報の取得には、道路に設置された感知器を用いる

[20] 交通情報提供プロバイダである VICS センターは、警察庁、郵政省、建設省を発足メンバーとして、1990 年にスタートし、1995 年財団法人 道路交通情報通信システムセンター（VICS センター）として設立。会員数は 201 法人・団体におよぶ。

ため、感知器のない道路の情報は反映することができなかった。

この課題を解決するため、自動車メーカーやカーナビゲーションメーカーがそれぞれの顧客向けに提供していたプローブ交通情報[21]を VICS センターが集約し、感知器のない道路の交通情報も提供する実証実験を 2020 年に開始した。プローブ交通情報は、独自の交通情報として各社のコネクテッドサービスでのみで利用されていたが、2011 年の東日本大震災の際、ITS Japan が各社プローブ情報を統合した通行実績情報を道路マップ上に無料公開したところ、東北地方への物流支援などにおいて非常に有益な情報となることが判明した。それ以降、ITS Japan は、地震や津波などの大規模災害が発生した際、通行実績情報を迅速に集約し公開する仕組みを再構築した。公益性の高い企業間データ共有を実現するため、国内自動車メーカー3社とカーナビゲーションメーカー1社がVICSセンターの呼びかけに同意する形で実証実験がスタートした。2022 年 7 月からは日本全国へエリアが拡大されている。

表 10　日本：VICS センターの自動車共有プラットフォーム

| | |
|---|---|
| システムアーキテクチャ | • はじめに、個人は、自動車メーカーやカーナビゲーションメーカーが運用するコネクテッドサービスに加入する。<br>• 各自動車メーカーまたはカーナビゲーションメーカーは、各社独自のコネクテッドサービスの規約に基づき、顧客の走行データを車載通信機を通じて各社のデータサーバーに集約する。<br>• 各社のデータサーバーに集約された走行情報は、個人識別情報を分離した後に統計処理され、各社が定義する道路毎の交通情報に編集・加工される。<br>• 一方、各社のプローブ交通情報は、VICSが定義する道路リンクごとの交通情報に変換された後にVICSセンターへ集約される。<br>• VICSセンターでは4社全てのプローブ情報に基づく高密度なプローブ交通情報を生成し、これを既存のVICSメディア（FM多重、ビーコン、テレマティクスなど）を通じて各社のカーナビゲーションに配信する。 |
| セキュリティとプライバシー保護 | • 各自動車メーカーが運用するデータサーバーとの接続や、機微情報（車両の位置情報や走行軌跡情報など）を含む特定のデータ項目を共有するか否かは、個人がカーナビゲーション画面などで選択できる。<br>• 一方、各社のコネクテッドサービスは、車載通信機を通じてインターネット経由で各社データサーバーと接続される仕組みであるが、インターネット上のセキュリティ対策の具体的内容については明示されていない。<br>• 各社データサーバーとVICSセンターとの接続についても同様であるが、クラウドインフラ上でホストされているため、データ保護規則、暗号化、セキュリティ会社による定期的な侵入テストや脆弱性チェックなどは行われていると考えられる。 |
| 接続可能な自動車メーカーとサービスプロバイダー | • 現在、VICSプローブ情報活用サービスに向けてプローブ情報を提供しているメーカーは、トヨタ、日産、ホンダの自動車メーカー3社と、カーナビゲーションメーカーのパイオニア1社の合計4社である。一方、サービスプロバイダは　VICSセンターのみである。 |
| ビジネスモデル | • 各社のコネクテッドサービスは、顧客と各社間で月額または年額の有償サービス契約を結んでいる。また、VICSセンターはVICS対応車載器に直接ライセンス料を課金するか、当該車載器を搭載する自動車メーカーと有償のライセンス契約を結んでいる。<br>一方、VICSプローブ情報活用サービスは未だ実証実験であるため、VICS対応車載器が搭載されていれば、どのような自動車メーカーの車両でもVICSプローブ交通情報を無償で利用できる。各自動車メーカー3社およびカーナビゲーションメーカー1社とVICSセンター間の契約内容は不明である。 |

21 プローブ情報とは、コネクテッドサービスを通じて顧客の車両から得た走行軌跡データのこと。

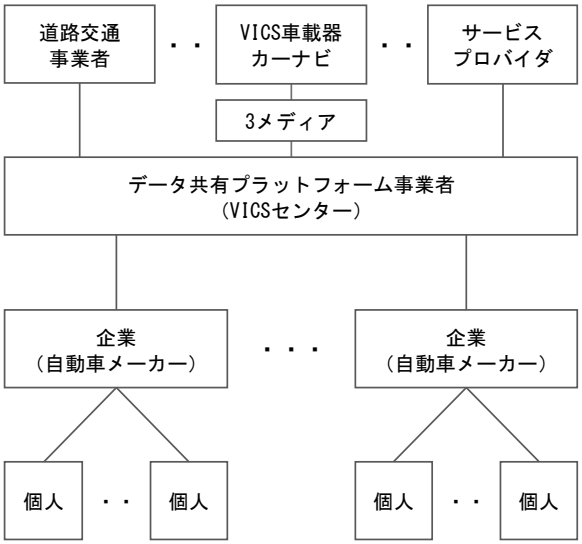


図6　日本：VICS センターのシステムアーキテクチャ

### 5-2-3.　事例におけるデータガバナンス要素の存在検証

データガバナンスを構成する3要素、すなわち、データ主権、データ安全性、データ利他主義が、各国のデータ共有事例においてどのように存在し、影響を与えているかを検証する。

#### (1) データ主権

##### ①　欧州

CARUSOは、全てのデータ保護法およびGDPR に準拠し、個人データの合法的な処理のみを行うことをデータポリシーで明記している。特に、サービスプロバイダが要求する個人情報（車両識別番号、データ項目など）を、特定の相手のみに共有するための許諾を同意管理技術により実行している点が重要と考えられる。これは、GDPRにおけるデータ主体である個人にデータの自己コントロールを高める技術を与え、これを個人データ保護の手段として最重視するという考えに沿ったものであり、同時に、データ制御の可用性が確保された状態、つまり、個人がデータ主権者である条件を満たした状態と言える。

また、自動車メーカーと CARUSO との相互信頼性構築については、CARUSO が自動車メーカー、サプライヤーなど 468 以上の法人に支持された非営利志向のニュートラルサーバーであることも重要な要因の一つと考えられる。業界関係者全てに対して中立的な立場にあり、個人とサービスプロバイダ間のデータ取引を仲介し、公正な取引を担保する存在に徹している存在とみなされている。

##### ②　米国

Smartcarは、米国のみならず欧州も対象市場としているため、同社が提供するデータ共有プラットフォームは、一般データ保護規則（GDPR）に準拠している。データ共有は、データ主体である個人が、スマートフォンアプリで個人情報の共有について同意した場合、Smartcarは顧客のアカウントを使って、自動車メーカーの特定車両データを特定の相手（顧客の同意を得たサービスプロバイダ）に共有する。これは、データ制御の可用性が確保された状態、つまり個人がデータ主権者であるための条件を満たしていると言える。

また、自動車メーカーと Smartcar との相互信頼性構築に影響する要因の一つとして、Smartcar が対象とする車両データが、自動車メーカーが既に顧客に提供しているモバイルサービス向け車両データに限定される点があげられる。このデータは、顧客の意思による第三者への共有が避けられないデータであり、自動車メーカーにとっては共有されても秘匿上問題のないデータであることが一般的である。すなわち、技術ノウハウや知見の流出、競合他社への横展開、共有先のデータガバナンスなどの不安が少ない限定的なデータであるため、自動車メーカーは警戒感を持つことなくデータ共有を許可していると考えられる。

**③ 中国**

自動車メーカーが生産、販売する NEV は、全車 RTM を装着するコネクテッドカーである。[22]コネクテッドカーの車両データは、中国データ 3 法に従って扱われるため、個人の車両と自動車メーカーのデータサーバーとの接続は、同第十七条にて企業とユーザーとの合意に基づくとされている。つまり、データ主権が確保された状態に見える。

しかし、自動車会社のデータサーバーに接続された後は、同じく第十七条にて新エネルギー自動車製品の運転安全状態を観測する目的で共有が必要とされる車両データ項目を、個人が変更したり削除したりすることはできないとされている。また、これらの車両データが上海新エネルギー車公共データ収集観測研究センターに共有されることを個人が拒否することもできない。これは、個人にデータ制御の可用性が確保された状態とは言えない。つまり、実質的には個人にデータ主権は存在していない。

また、各自動車メーカーについても、車両データ項目の内容を変更したり削除したりする権利や上海新エネルギー車公共データ収集観測研究センターへのデータ共有を拒否する権利はない。すなわち、上海新エネルギー車公共データ収集観測研究センターが扱う車両データは国家安全法を背景としたデータ政策に準拠すべきデータであるため、国家は組織や個人に優先するとする国家安全法を背景としたデータ政策のもとでは、個人も企業もデータ主権を持ち得ないと考えられる。

NEV のコネクテッドサービスの契約率は 100%近いと言われているが、必ずしも個人の自動車メーカーに対する信頼の高さや国家安全法を背景としたデータ政策の強制力によるものではない。自動車メーカーのコネクテッドサービスは中国の主要な検索サイトや SNS への接続を基本メニューとしており、個人は高い魅力を持つサービスを利用するために契約しているとも言える。この場合、個人と自動車メーカーとの間には、巨大 IT 企業[23]への信頼を背景とした間接的な相互信頼が構築されていると考えられる。

**④ 日本**

個人と企業はコネクテッドサービス契約を行うが、その際に企業のデータサーバーに接続するか否か、さらに機微情報を共有するか否かは、データ生成主体である個人がカーナビゲーションなどで選択できる。これは、個人情報保護法に準拠しており、個人にデータ制御の可用性が確保された状態と考えられるため、個人はデータ主権を持つと考えられる。

ただし、個人がデータ共有する際の目的、内容、共有先、共有方法などについて全てを理解し承諾し、契約しているとは考えにくい。個人は、相手が大企業であることで信頼し、一度預けたデータの活用については一任していると思われる。これは、企業がデータ主体である個人に代わって意思決定を行うエージェントの役割を果たしている状態と考えることもできる。その場合、個人と企業間の相互信頼性は、個人のデータ制御の可用性にあるのではなく、企業の社会的信用に基づいて構築されたものと言える。

一方、各企業が、第三者である VICS センターに対してデータ共有するプローブ交通情報は、個人識別情報を分離した後に統計処理された情報、つまり個人情報にはあたらないため、各企業がデータ主体となる。そして、各企業は、互いのデータ共有を拒否することも、データ共有を行うことも企業の自由意志で選択できることから、各企業にはデータ制御の可用性があり、データ主権を持つと言える。

**⑵ データ安全性**

**① 欧州**

CARUSO と接続される欧米自動車メーカー各社のコネクテッドサービスは、それぞれ業界トップレベルのクラウドサービス上で運用されているため、CARUSO もデータ共有やデータの保存の仕組みにおいて同等の信頼性を確保していると言える。

**② 米国**

データセキュリティについては、トラストサービス基準である SOC 2 Type 2 に準拠し、プラットフォームはクラウドインフラ上でホストされるとともに、保存される全データは Advanced Encryption Standard (AES) 256 ビット暗号化で保護され、定期的に独立したセキュリティ会社による侵入テストと脆弱性スキャンを受けているとしている。このような技術的措置は、全て GDPR や米国の一部の州法を反映したものであり、データ共有におけ

22 工業情報化部が省令第 39 号第十七条による。

23 バイドゥ、アリババ、テンセントなど。

る個人、企業、プラットフォーム事業者の相互信頼性の基盤をなしていると考えられる。

**③ 中国**

自動車メーカー各社のデータセキュリティに関わる情報はないものの、自動車データは国家安全に関わる重要データとして国家の管理下にあり、国外とのファイアウォールは最も厳重に管理されている。さらに、自動車メーカー各社のシステムは、バイドゥ、アリババ、テンセントなど業界トップレベルのクラウドサービスとの接続が前提となっているため、NEV センター、自動車メーカー各社ともに同等の高い信頼性を確保していると考えられる。

**④ 日本**

VICS センターと接続される自動車メーカー各社のコネクテッドサービスは、それぞれ業界トップレベルのクラウドサービス上で運用されているため、VICS センターもデータ共有やデータの保存の仕組みにおいて同等の信頼性を確保していると言える。

**⑶ データ利他主義**

**① 欧州**

データ利他主義はデータガバナンス法でポリシーが明記され、データ法では、企業に対して製品などの利用者に生成データを利用させる義務を課している。すなわち、個人が CARUSO と契約を結ぶサービス事業者のサービスを望めば、自動車メーカーはサービス事業者にデータ共有を行うことで、製品利用者である個人に企業の生成データを利用させなくてはならない。一方で、データ共有は個人のニーズに基づくサービス実現のために実行され、背景に個人や企業の利他的倫理が存在するか否かは不明である。

**② 米国**

データ利他主義については、欧州のような明示的なデータガバナンス法規は存在しない。データ共有は個人のニーズに基づくサービス実現のために実行され、背景に個人や企業の利他的倫理が存在するか否かは不明である。

**③ 中国**

データ利他主義については、欧州のような明示的なデータガバナンス法規は存在しない。データ共有は国家安全法に基づく強制力によるものであり、背景に個人や企業の利他的倫理が存在するか否かは不明である。

**④ 日本**

プローブ交通情報におけるデータ共有事例では、その背景に、東日本大震災の際に提供された通行実績情報があり、VICSプローブ情報活用システムでは、データ提供をしていない企業にもサービスが提供される。すなわち、データ共有を実践する各企業は、成果物の利益をデータ共有に参加していない他者にもあまねく分配している。データ利他主義を明示するデータガバナンス法規は存在しないが、個人や企業の利益追求を超えた、公益を優先する行動が企業自らの判断で実践されており、データ利他主義の思想が潜在的に存在すると考えられる。

以上のように、課題２の研究結果として、各国・地域におけるデータ共有事例と特徴を整理し、課題１で明らかになったデータガバナンス各要素がデータ共有事例においてどのように存在し、影響を与えているかを明らかにした（表 11）。

表11　各国事例における基本的要素の存在検証

| 基本的要素 | 欧州 | 米国 | 中国 | 日本 |
|---|---|---|---|---|
| データ主権 | **存在する**<br>• 個人による情報共有を同意した上で、個人情報（車両識別番号、データ項目など）を特定の相手のみに共有することができる。<br>• データ共有プラットフォームが中立的存在であることが相互信頼性を高めている。 | **存在する**<br>• 個人による情報共有を同意を受け、プラットフォーム事業者を介してサービス事業者にデータ共有される。<br>• 秘匿性の高くないデータに限定されていることが、相互信頼性を高めている。 | **存在しない**<br>• 個人が企業のサービス利用契約に同意することで、データ共有が行われる。<br>• 個人も企業も、当該データが政府に共有されることへの拒否や、データの変更や削除はできない。 | **存在する**<br>• 個人がカーナビゲーションの設定などで情報共有を行うか否か選択できる。<br>• ただし、背景には大企業の社会的信用に基づく相互信頼性がある。<br>• 集約したコネクテッドデータを共有するか否かは企業が自らの利害に基づいて判断する。 |
| データ安全性 | **存在する**<br>• 業界大手企業が運営するクラウドインフラ上でホストされている。<br>• 非個人データの国際移転に関しては制限がある。 | **存在する**<br>• 業界大手企業が運営するクラウドインフラ上でホストされている。<br>• 暗号化などの仕組みにより、安全性の高いデータ管理が行われている。 | **存在する**<br>• 自動車データは国家安全に関わる重要データとして国家が管理。<br>• 国外とのファイアウォールは最も厳重に管理される。<br>• 業界トップレベルのクラウドサービスとの接続が前提になっている。 | **存在する**<br>• 業界大手企業が運営するクラウドインフラ上でホストされている。 |
| データ利他主義 | **どちらとも言えない**<br>• データガバナンス法およびデータ法によりデータ利他主義に関するポリシーや権限が明示されている。<br>• データ共有は個人ニーズに基づくサービス実現のために実行され、背景に個人や企業の利他的倫理が存在するか否かは不明。 | **どちらとも言えない**<br>• データ利他主義に関わる明示的なデータガバナンス法規は存在しない。<br>• データ共有は個人ニーズに基づくサービス実現のために実行され、背景に個人や企業の利他的倫理が存在するか否かは不明。 | **どちらとも言えない**<br>• データ共有は国家安全法に基づく強制力によるものであり、背景に個人や企業の利他的倫理が存在するか否かは不明である。 | **存在する**<br>• データ利他主義に関わる明示的なデータガバナンス法規は存在しない。<br>• 企業が各社プローブ交通情報のデータ共有を判断する背景には、2011年東日本大震災の際に実施された通行実績情報提供の経験がある。<br>• VICSプローブ情報活用システムでは、データ提供をしていない企業にもサービスが提供されており、データ利他主義が実践されている。 |

### 5-3. 課題3

企業がデータ共有を決断する動機づけとなっている要因は何か、データガバナンスの各要素はその動機づけにどのような影響を与えているかを検証する。

#### 5-3-1. 欧州

データ法では、顧客が希望する場合は自動車メーカーが保有する生成データをサービス事業者に利用させる義務が生じる。そのため、自動車メーカーはプラットフォーム事業者を介してサービス事業者との接続が必要となる。例えば、自動車メーカーがプラットフォーム事業者としてCARUSOとデータ共有契約を行えば、顧客はCARUSOと繋がるサービスを享受でき、顧客が自動車メーカーとデータ共有契約を結ぶインセンティブとなる。自動車メーカーにとっても、データ共有を通じた顧客囲い込みの機会創出に繋がるため、CARUSOとデータ共有契約を結ぶインセンティブとなる。これは、個人から見ればデータ主権の行使であり、企業から見ればデータ利他主義の遂行と言える。

一方、自動車メーカーがCARUSOとデータ共有契約を行わず、顧客がCARUSOと繋がるサービスが選択できない場合、顧客は当該自動車メーカーからは欲しいサービスを享受できないと判断して、自動車メーカーとのデータ共有契約を行わない可能性がある。その場合、自動車メーカーにとって、データ共有を通じた顧客囲い込みの機会を失うリスクが生まれることになる。あるいは必要なサービスを提供しない企業というレッテルを貼られ、CARUSOとデータ共有契約を結ぶ競合他社に車両自体の契約を奪われるリスクが生まれる。

これは、個人のデータ主権の行使を起点に、データ共有を行う、あるいは行わないことで生じるインセンティブとリスクをめぐる企業間の駆け引きが、企業のデータ共有の動機に影響を与える（Kong et al., 2019）状況と言える。

#### 5-3-2. 米国

米国では、データ法（欧州）のように製品利用者が望む場合は生成データを利用させる義務を課すような法案は存在しない。しかし、自動車メーカーがSmartcarとデータ共有契約を結ぶ動機は、欧州と同様と考えられる。

すなわち、データ共有によって顧客はSmartcarと繋がるサービスを享受できるようになるため、自動車メーカーにとっては、顧客囲い込みの機会創出に繋がる。

逆に、自動車メーカーがSmartcarとデータ共有契約を結ばず、顧客が欲するサービスを提供できないと、データ共有を通じた顧客囲い込みの機会を失うリスクが生まれることになる。あるいは必要なサービスを提供しない企業というレッテルを貼られ、Smartcarとデータ共有契約を結ぶ競合他社に車両自体の契約を奪われるリスクが生まれる。

この状況は欧州の場合と同様に、個人のデータ主権の行使を起点に、データ共有を行う、あるいは行わないことで生じるインセンティブとリスクをめぐる企業間の駆け引きが、企業のデータ共有の動機に影響を与える(Kong et al., 2019) 状況と言える。

### 5-3-3. 中国

個人および自動車メーカーにとって、上海新エネルギー車公共データ収集観測研究センターとデータ共有を行う動機は、欧米のような個人のデータ主権の行使や、これを起点とした企業間の駆け引きによるものではなく、国家安全法を背景としたデータ安全性に関わる強制力である。自動車メーカーが上海新エネルギー車公共データ収集観測研究センターとのデータ共有に応じなければ、国家安全法を背景とした規則により、自動車メーカーには営業停止などの厳しいペナルティが課せられる。

企業から見れば、データ共有を行わない場合に課されるペナルティを回避することがデータ共有の動機づけとなっている状況と言える。

### 5-3-4. 日本

米国、中国と同様に、製品利用者が望む場合は生成データを利用させる義務を課すデータ法（欧州）のような法案は存在しない。日本のデータ共有事例は、欧米のような個人のデータ主権の行使を起点とした企業間の駆け引きによる動機づけでは、説明できない。

VICSセンターに自社のプローブ交通情報を共有することは、他社より高密度なプローブ交通情報を持つ企業にとっては、強みを失うことになる。しかも、データ共有の成果物である高密度なプローブ交通情報は、データ共有企業のみならず、データ共有に参加していない他社にもあまねく提供されている。それにも関わらず、企業がデータ共有を行う決断を下すのは、東日本大震災の際に提供された通行実績情報の経験から、高密度で高精度な交通情報は公益に資するものであり、企業の利益追求より優先させるべきものであるというデータ利他主義の考え方が働いていると考えられる。

### 5-3-5. データガバナンス要素と企業の動機の関係性

課題3の研究結果として、企業がデータ共有を決断する直接的な動機づけとなっている要因と、データガバナンス要素との関係性を整理し、企業の動機づけの起点となるデータガバナンス要素を明らかにした（表12）。

表12　企業の動機づけの起点となるデータガバナンス要素

| 欧州 | 米国 | 中国 | 日本 |
|---|---|---|---|
| **データ主権**<br>• データ法により、企業には製品利用者が望む場合は生成データを利用させる義務が生じる。<br>• 個人の「データ主義」の行使（欲しいサービスを享受するためのデータ共有要求）がデータ共有の起点。<br>• データ共有を行う、あるいは行わないことで生じるインセンティブとリスクをめぐる企業間の駆け引きが、企業のデータ共有の動機となっている。 | **データ主権**<br>• 個人の「データ主権」の行使（欲しいサービスを享受するためのデータ共有要求）がデータ共有の起点。<br>• データ共有を行う、あるいは行わないことで生じるインセンティブとリスクをめぐる企業間の駆け引きが、企業のデータ共有の動機となっている。 | **データ安全性**<br>• 国家安全法を背景とした「データ安全性」に関わる強制力がデータ共有の起点となっている。<br>• データ共有を行わない場合に課せられるペナルティを回避することが企業のデータ共有の動機となっている。 | **データ利他主義**<br>• 高密度で高精度な交通情報は公共に資するものであり、企業の利益追求より優先させるべきものであるという「データ利他主義」が企業のデータ共有の起点となっている。 |

## 6. ディスカッション

課題1～3の検証結果を踏まえ、各国・地域におけるデータ共有の実態を決定づけているデータガバナンス各要素の優先順位や相対的関係、すなわちアーキテクチャモデルを考察する。

データガバナンスのアーキテクチャモデルを考察する主なメリットとしては、各要素が構造化されることで企業の意思決定の流れが説明しやすくなること、構造から生まれる利害得失が明らかになること、課題に対する対策や最適な構造が議論できることなどがあげられる。

データガバナンスとデータ共有の関係性を、アーキテクチャモデルとデータ共有の関係性として整理することで、より具体的かつ一般化された知見を得ることができると考えられる。

### 6-1. 欧州型アーキテクチャモデル

欧州は、CARUSOの事例から明らかなように、GDPRで象徴される個人のデータ主権が全てに優先され、データガバナンスの基盤をなしている。データ共有サービスを欲する個人が、データ主権に基づくデータ共有を望めば、データ利他主義に実効性を与えるデータガバナンス法およびデータ法により、企業は生成データの共有を行う義務が生じ、必然的にデータ共有が進む。データ安全性はデータ主権を保護するための技術的、制度的な取り決めと言える。

以上のことから、欧州においては、データ主権を最優先基盤にしながら、データ安全性とデータ利他主義が並立するアーキテクチャモデルを想定することができる（図7）。

このモデルが企業のデータ共有に与える影響を事例に基づいて考察する。個人のデータ主権が技術的、制度的に最優先されるため、自動車メーカーは個人ニーズに応じる必要が生じるが、これは顧客囲い込み機会にもなる。

一方、もしCARUSOとデータ共有契約を行わなければ、顧客囲い込みの機会を失うリスクや、必要なサービスを提供しない企業というレピュテーションリスクが生まれる可能性がある。さらに、データ法に基づくデータ共有義務の不履行によるペナルティを被る可能性もある。

すなわち、データ主権を最優先したアーキテクチャでは、企業に対して顧客囲い込みのインセンティブとともに、不履行によるペナルティリスクやレピュテーションリスクを刺激する仕組みが必然的に構築され、結果的にデータ共有が促進される構造になると考えられる。

一方で、機微情報に対して、データ共有の拒否という形でデータ主権が行使されると、プローブ交通情報などは生成できない。つまり、実現サービスに制約が生まれる懸念がある。

### 6-2. 米国型アーキテクチャモデル

米国は、Smartcarの事例に見られるように、基本的に欧州と同様で、個人のデータ主権が全てに優先される。ただし、データ利他主義については、欧州のような実効性のある明示的なデータガバナンスは存在しない。

以上から、米国においては、データ主権とデータ安全性を基本的な構成要素として、データ主権を最優先基盤としたアーキテクチャモデルを想定することができる（図7）。

このモデルにおいては、欧州と同様、企業に対して顧客囲い込みのインセンティブとともに、不履行によるペナルティリスクやレピュテーションリスクを刺激する仕組みが、必然的に構築され、結果的にデータ共有が促進される構造になると考えられる。

一方で、機微情報に対して、データ共有の拒否という形でデータ主権が行使されると、オープンなデータ共有に制約が生まれる懸念があることも欧州と同様である。

### 6-3. 中国型アーキテクチャモデル

中国は、個人情報保護法は存在するものの、国家安全法を背景としたデータ政策が象徴するように、国家の安全や利益の保護が最優先される。また、米国同様に、個人や企業に対するデータ利他主義については明示的なデータガバナンスの存在が認められない。さらに、事例においてはデータ主体にデータ制御の可用性がないため、データ主権は存在しない。しかし、個人情報保護法は厳然と存在するため、国家安全法に触れない分野ではデータ主権が存在すると考えられる。

そこで、中国においては、データ主権とデータ安全性を基本的な構成要素として、データ安全性を最優先基盤としたアーキテクチャモデルを想定した（図7）。

このモデルが企業のデータ共有に与える影響を事例に基づいて考察する。国家安全法のようなデータ主権を超越する権力により、データ共有が強制的に実行されるため、国や地方政府が取り扱うサービスに関連するデータ活用は促進される。そのため、データ共有を必要とするサービスが国や地方政府のニーズに基づくものである限り、データ共有は直ちに、大規模に達成されるメリットがある。しかし、欧米のように車両データの共有を行う民間プラットフォームを立ち上げることは困難と考えられることから、国や地方政府が取り扱うサービス以外の目的に使われるデータ共有に制約が生まれる懸念がある。また、国内では公益に資するデータ共有の加速が期待

できるが、競争力のある多国籍企業が中国のデータにアクセスすることも持ち出すことも困難なため、企業の研究開発能力の低下、製品コストの上昇、サービスの質の低下につながる懸念もある。

### 6-4. 日本型アーキテクチャモデル

日本は、米国と同様に、法規として存在しているものは個人情報保護法のみである。しかし、包括的データ戦略では、欧州のデータガバナンスを雛形として、データ流通の信頼性や安全性といった観点から、技術的側面を中心に方針が示されており、事例においてもデータ主権、データ安全性がともに存在する。さらに、プローブ交通情報におけるデータ共有事例では、その背景に、東日本大震災の際に提供された通行実績情報があり、データ提供をしていない企業にもサービスが提供されることから、個人や企業の利益追求を超えた、公益のためのデータ利他主義が明確に存在すると考えられる。

従って、日本においては、データガバナンス関連法規として明示的には存在していないものの、事例においては、データ主権、データ安全性、データ利他主義が全て存在し、潜在的なデータガバナンスとして機能していると考えられる。データアーキテクチャの基盤をなしているのはデータ利他主義であり、その前提のもとに、データ主権とデータ安全性が併存する構造と考えられる（図7）。

このモデルが企業のデータ共有に与える影響を考察する。まず、データ主権やデータ安全性を最優先基盤としないことから、個人欲求や国家の強制力によって生じるデータ共有の制約は生じない。しかし、事例では、企業の利他的倫理に依存したデータ共有となっており、個人の強い権利に根ざすデータ共有欲求や、国家強制力に基づくデータ共有の推進力が構造的に存在しない。このため、災害時のように、非日常的な状況下で強い利他的倫理が発動するケースでない限り、企業が積極的なデータ共有を行う動機は生まれにくいと考えられる。実際、日本においては、データガバナンスに関わる関連法規の未整備という背景も加わって、欧州、米国、中国で見られるようなデータ共有事例は生まれていない。

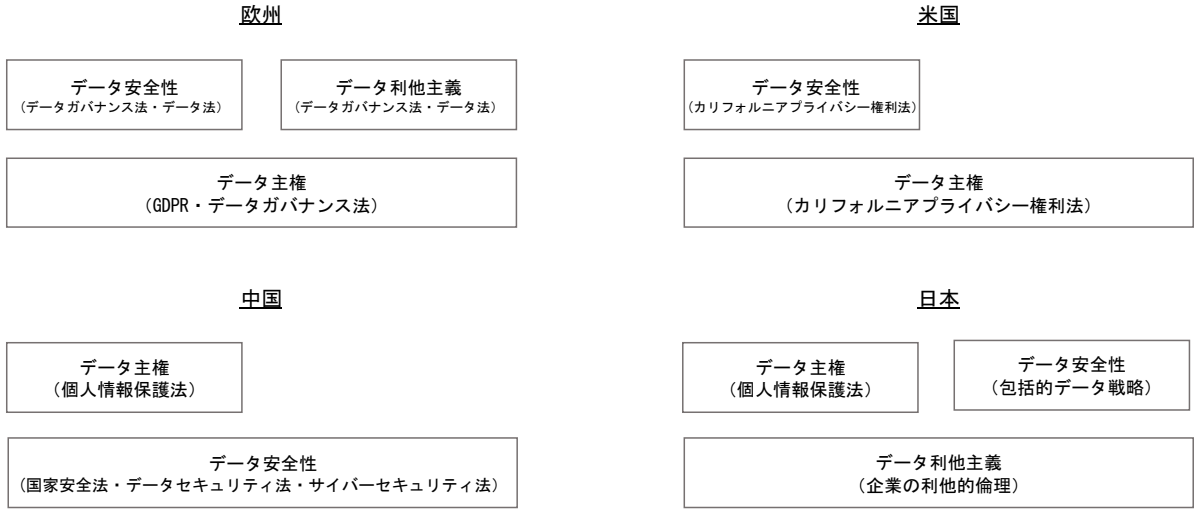


図7　各国・地域におけるデータガバナンスのアーキテクチャモデル

### 6-5. 日本型アーキテクチャモデルの改善

最後に、得られた知見から、データ共有の阻害要因を回避し、公益のためのデータ共有の活性化や新たな付加価値の創出に適したアーキテクチャモデルとその課題を考察し、より良いデータガバナンスのあり方について提言する。

各アーキテクチャモデルの特徴を5-1-6.項の図1に示した機能で整理すると、欧米型では、データ主権、すなわち同意管理機能がデータのリスク管理を支え、同意管理機能の行使がデータ共有を実現する。その結果、個人がデータ共有に同意すればデータ共有は安全に実現され、拒否すればデータ共有は公益性の有無に関わらず実現しない（図8）。

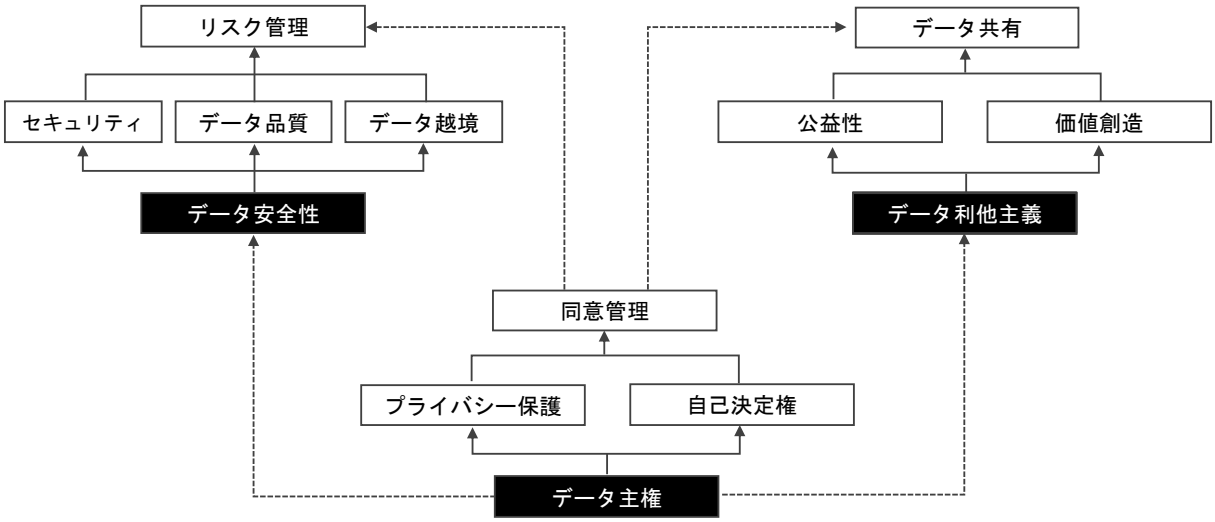


図8　欧米型：同意管理がリスク管理とデータ共有を制する流れ

次に、中国型では、データ安全性、すなわちリスク管理が同意管理を制する。その結果、国や地方政府が必要と認めたデータ共有は、個人や企業の同意とは関係なくデータ共有が実現されるが、国や地方政府にとって必要のないデータ共有は推進されない（図9）。

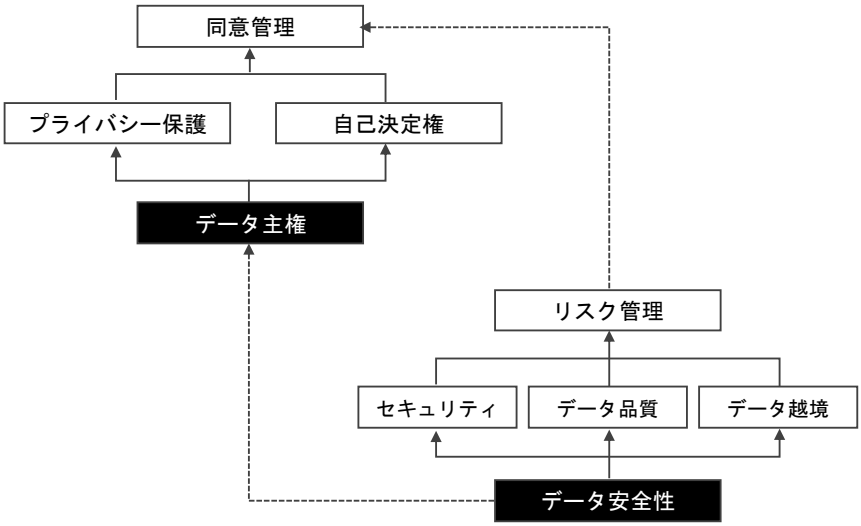


図9　中国型：リスク管理が同意管理を制する流れ

一方、日本型アーキテクチャモデルの特徴として、欧米型や中国型のようにデータ主権やデータ安全性を最優先基盤としないため、個人欲求や国家の強制力によって生じるデータ共有の阻害要因が生まれにくいメリットがあげられる。すなわち、公益のためのデータ共有の活性化や新たな付加価値の創出を阻害する可能性がなく、他のアーキテクチャモデルより優れたモデルとなる可能性がある。しかし現状は、最優先基盤であるデータ利他主義には法的執行力がなく、データ共有を企業の利他的倫理に依存しているため、データ共有を活性化する推進力が弱い。

そこで、日本型アーキテクチャを前提に改善モデルを考察する。まず、他のアーキテクチャモデルと同様に、データガバナンス要素の全てに法的執行力を与える必要がある。とりわけ最優先基盤であるデータ利他主義に法的執行力を持たせることは重要である。例えば、公益性が認められるデータ共有事案に対しては、欧州のデータガバナンス法やデータ法に見られるようなデータ共有義務が発生する法規を定めることが考えられる。データ利他主義について法的執行が可能な環境が構築できれば、企業の利他的倫理のみに頼ることなく、データ共有が促進される必然性が生まれる（図10）。

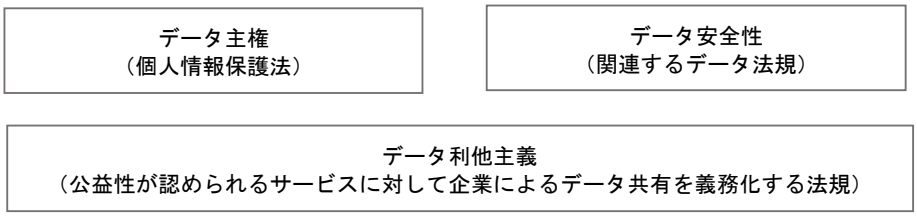


図 10　日本型アーキテクチャの改善モデル

すなわち、改善モデルにおいては、公益性や社会に新たな価値創造をもたらすデータ共有であると認められた場合は、これが個人や企業の同意管理を制し、データのリスク管理を促す（図 11）。

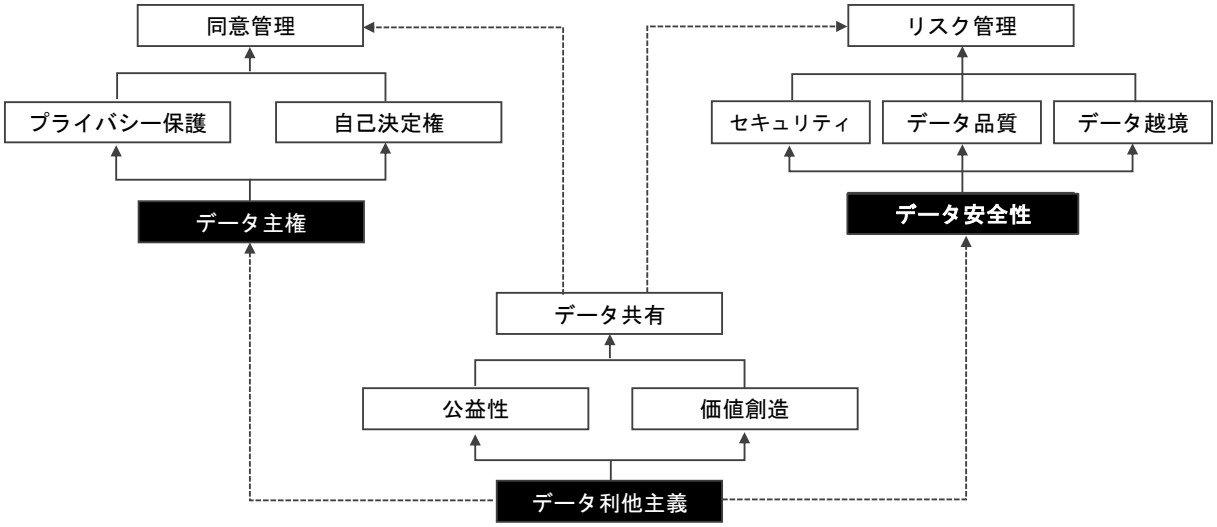


図 11　日本型（改善モデル）：公益や価値創造に資するデータ共有が同意管理とリスク管理を制する流れ

このようなアーキテクチャモデルを持つ国や地域は未だ存在しない。しかし、日本においては、潜在的なアーキテクチャモデルとして既に存在していることから、関連法規を立ち上げ、施行していくことで、より優れたデータガバナンスを実現できる可能性がある。

## 7. 結論

本研究では、「データガバナンスが企業の行動を通じて現実のデータ共有に与える影響」を主題とし、これまで十分な理論化が行われていない、データガバナンスとデータ共有の関係性の解明を試みた。

研究方法としては、欧州、米国、中国、日本におけるデータガバナンスとデータ共有事例の関係性を比較分析する事例研究とし、データガバナンスにおけるデータ主権の役割や機能に関する先行研究（Hummel et al., 2018）と、企業がデータ共有を決断する直接的な動機づけに関する先行研究（Kong et al., 2019）を考察の基盤とした。

その結果、データガバナンスの基本的要素には、少なくともデータ主権、データ安全性、データ利他主義の3要素が存在し、データガバナンスのアーキテクチャには、データ主権を最優先基盤とする欧米型、データ安全性を最優先基盤とする中国型、データ利他主義を最優先基盤とする日本型、の異なる3形態が存在することが検証された。

欧米型はデータ主権に支えられた個人欲求がデータ共有を推進し、中国型は国家安全法を背景とするデータ安全性の強制力によりデータ共有が推進される。日本型はデータ利他主義について法的執行が可能な環境が存在しないため、データ共有の推進力は乏しい。一方、欧米型では個人情報保護、中国型では国家安全の過剰行使が、共有可能なデータ、実現可能なサービス、利用可能な技術や知識に制約を与える可能性も示唆された。

データ共有の阻害要因を回避し、公益のためのデータ共有の活性化や新たな付加価値の創出に適したアーキテクチャモデルとして、日本型アーキテクチャの改善モデルを例示した。公益性が認められるデータ共有事案に対しては、企業のデータ共有義務が発生する法規を定めることで、データ利他主義に法的執行力を与えるものである。

以上のことから、本研究の主題である「データガバナンスが企業の行動を通じて現実のデータ共有に与える影響」は、データガバナンスのアーキテクチャの違いがデータ共有に与える影響という観点で明らかにされた。

データの利活用が社会や経済の発展に不可欠となる中、適切なデータガバナンスの構築は喫緊の課題である。

本研究の成果は、各国・地域がより効果的なデータガバナンス政策を策定する上で、有益な示唆を提供するものと期待される。今回は、自動車産業に焦点を当てたが、他の産業分野においても同様の分析が可能である。それぞれの産業分野に応じたデータガバナンスのあり方や、より多くの国や地域を対象とした研究を進めることで、データガバナンスのさらなる理解と改善に貢献できると考えられる。

また、日本型アーキテクチャの改善モデルにおいて、公益性や社会に新たな価値創造をもたらすデータ共有事案をどのように定義し、どのようなプロセスで認定するのかなどは本研究では明らかになっていない。これらは今後の課題としたい。

[参考文献]

[1] California Consumer Privacy, https://oag.ca.gov/privacy/ccpa/

[2] CARUSO, https://www.caruso-dataplace.com/

[3] Charles C. Ragin, “The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies”, University of California Press, 1987.

[4] Deutscher Ethikrat (German Ethics Council), “Big Data und Gesundheit.Datensouveränität als informationelle Freiheitsgestaltung”, Deutscher Ethikrat (German Ethics Council), 2017.

[5] Eisenhardt, K. M., “Building Theories from Case Study Research”, Academy of Management Review, Volume 14, No.4, Pages 532-550, 1989.

[6] European Commission, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

[7] Federal Data Strategy (FDS), https://strategy.data.gov/

[8] General Data Protection Regulation (GDPR), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[9] Kathleen M. Eisenhardt, “Building Theories from Case Study Research”, The Academy of Management Review, 14(4), Pages 532-550, 1989.

[10] Liyuan Wang, Hans-Christian Pfohl, Ulrich Berbner, Anna Katharina Keck, “Supply Chain Collaboration or Conflict? Information Sharing and Supply Chain Performance in the Automotive Industry”, Commercial Transport, Conference paper, First Online, Pages 303-318, 2015.

[11] Luciano Floridi, “The 4th Revolution: How the Infosphere Is Reshaping Human Reality”, Oxford University Press, 2014.

[12] Marina Micheli, Marisa Ponti, Max Craglia, Anna Berti Suman, “Emerging models of data governance in the age of datafication”, Big Data and Society, ISSN 2053-9517(online), 7(2), 2020.

[13] Michelle De Mooy, “Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data: Considerations for Future Policy Regimes in the United States and the European Union”, Bertelsmann Stiftung, 2017.

[14] Michael L. Katz, Carl Shapiro, “Network Externalities, Competition, and Compatibility”, The American Economic Review, Volume 75, No.3, Pages 424-440, 1985.

[15] Patrik Hummel, Matthias Braun, Steffen Augsberg, Peter Dabrock, “SOVEREIGNTY AND DATA SHARING”, ITU Journal: ICT Discoveries, Special Issue No. 2, 2018.

[16] Proposal for a Regulation harmonised rules on fair access to and use of data, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

[17] Regulation (EU) of the European Parliament and of the Council, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

[18] Rene Abraham, Johannes Shneider, Jan vom Brocke, “Data governance: A conceptual framework, structured review, and research agenda”, International Journal of Information Management Volume 49, Pages 424-438, 2019.

[19] Shoshana Zuboff, “The Age of Surveillance Capitalism: The Fight for a Human Future at the New

Frontier of Power”, Profile Books, 2019.
[20] Smartcar, https://smartcar.com/
[21] T. K. Das, Bing-Sheng Teng, “Trust, Control, and Risk in Strategic Alliances: An Integrated Framework”, Organization Studies, Volume 22, Issue 2, 2001.
[22] VICSセンター, https://www.vics.or.jp/
[23] Xiaodan Kong, Qi Xu, Tao Zhu, “Dynamic Evolution of Knowledge Sharing Behavior among Enterprises in the Cluster Innovation Network Based on Evolutionary Game Theory”, MDPI Sustainability, Volume 12, Issue 1, 2019.
[24] Zachary N J Peterson, Mark Gondree, Robert Beverly, “A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud”, USENIX Workshop on Hot Topics in Cloud Computing, Page9, 2011.
[25] デジタル庁　包括的データ戦略,
https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/576be222-e4f3-494c-bf05-8a79ab17ef4d/210618_01_doc03.pdf
[26] 個人情報の保護に関する法律, https://elaws.e-gov.go.jp/document?lawid=415AC0000000057
[27] 国务院关于印发社会信用体系建设规划纲要（2014-2020 年）的通知。国发〔2014〕21 号,
http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm
[28] 自動車データ安全管理若干規定（試行）,
https://www.miit.gov.cn/xwdt/gxdt/art/2021/art_9ede57a5600d4020a848c4bd1ba90bf7 .html
[29] 中華人民共和国サイバーセキュリティ法, https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm
[30] 中華人民共和国データ安全法, https://www.gov.cn/xinwen/2021-06/11/content_5616919.htm
[31] 中華人民共和国個人情報保護法, http://www.gov.cn/xinwen/2021-08/20/content_5632486.htm
[32] 中華人民共和国国家安全法, http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm
[33] 中華人民共和国国務院令第 631 号『征信管理条例』, http://www.gov.cn/zwgk/2013-01/29/content_2322231.htm
[34] 國領二郎, オープンアーキテクチャ戦略, ダイヤモンド社, 1999.
[35] 國領二郎, 「情報社会のプラットフォーム：デザインと検証」, 情報社会学会誌、Volume1, No.1, Pages 41-49, 2006.

(2024 年 11 月 20 日受理)