パーソナルデータ
リファレンスアーキテクチャ

DFFT（DATA FREE FLOW WITH TRUST）実現のための

アーキテクチャ設計と国際標準化推進の研究開発

一般社団法人　データ流通推進協議会

２０２０年３月

第1章　はじめに

このパーソナルデータリファレンスアーキテクチャ書(以下、本書)は、パーソナルデータを扱う全ての事業者、ステークホルダが、ビジネスモデルや内部統制などのシステム設計を行うためのガイドとなる設計書である。

本書の示す手順により、各事業者が自らの事業のアーキテクチャを設計・整理することで、パーソナルデータの取扱いの適正性や潜在する課題を顕在化させ、適切なパーソナルデータの利活用モデルが構築されることを期待している。

加えて、本書は、特定の事業分野、事業内容に限定することなく、パーソナルデータを取り扱う事業の共通要件を示している。このため、異分野間の事業であっても、本書に従って設計される共用のアーキテクチャを持つことにより、異分野間でのデータ共有を推進する一助となることも期待される。

1.1　　適用

本書は、内閣府が実施し国立研究開発法人　新エネルギー・産業技術総合開発機構（NEDO）が管理法人を務める「戦略的イノベーション創造プログラム（SIP）第 2 期／ビッグデータ・AI を活用したサイバー空間基盤技術」（以下、本プロジェクトという）の「パーソナルデータアーキテクチャ構築」事業において、一般社団法人データ流通推進協議会(以下　DTA)が提案し、採択された「DFFT(Data Free Flow with Trust）実現のためのアーキテクチャ設計と国際標準化推進の研究開発」（以下、本テーマという）の成果物である。

1.2 本書の位置付け

本書は、「DFFT（Data Free Flow with Trust）実現のためのアーキテクチャ設計と国際標準化推進の研究開発」の研究の成果物として、表 1 に示す各文書とともに、DTA が発行し、内閣府の HP[1]及び DTA の HP[2]より公開予定の文書である。

表 1　DFFT（Data Free Flow with Trust）実現のためのアーキテクチャ設計と国際標準化推進の研究開発事業の成果物一覧

No	文書名	文書形態	概要
1	パーソナルデータリファレンスアーキテクチャ概要書（以下、リファレンスアーキテクチャ概要書）	PPT スライド	下記 2 のリファレンスアーキテクチャ書（設計書）の概要をまとめたスライド
2	パーソナルデータリファレンスアーキテクチャ書（設計書）	ワード文章	パーソナルデータを扱う全ての事業者、ステークホルダが、ビジネスモデルや内部統制などのシステム設計を行うためのガイドとなる設計書
3	ユースケースシナリオテンプレート	PPT スライド	パーソナルデータを取り扱う事業者が活用するテンプレートドキュメント
4	ユースケースシナリオ集	PPT スライド	本プロジェクトの採択事業実施者が記載したユースケースシナリオをまとめたもの
5	ELSI 検討報告書	ワード文章および PPT スライド	パーソナルデータの取扱いについて、ELSI の視点から必要な事項をまとめたもの

[1] 内閣府の HP:　https://www8.cao.go.jp/cstp/stmain/20200318siparchitecture.html

[2] DTA の HP:　https://data-trading.org/sipb-1_personaldataarchitecuture_dta/

本書の作成にあたり、表 2 に示す各文書を調査業務および再委託先による研究業務により取りまとめた。これらの文書は、本書の公開に合わせて、DTA が発行し、DTA の HP で公開予定である[3]。

表 2　関連資料

No	文書名	文書形態	概要
1	トラストサービス調査報告書	ワード文書およびPPT スライド	欧米トラストサービスの動向調査などをまとめた文書
2	情報法制調査報告書	ワード文書	情報法制の全体像、一般法令（個人情報保護法、契約法）、個別法令をまとめた文書
3	データジャケットの国際標準化報告	ワード文書およびPPT スライド	再委託先である東京大学大澤研究室が作成したデータジャケットを中心とした標準化インプット案の文書
4	国際標準化調査報告書	ワード文書	IEEE-DTSI(Data-Trading System Initiative)を中心とした活動状況をまとめた文書

[3] DTA の公開ページ：https://data-trading.org/room/sipb-1_personaldataarchitecuture_for_dta_member/

1.3　本書の構成

本書は表 3 に示すように、四編１１章及び付属資料より構成され、各章の詳細は、次の各項に述べる。

表 3　本書の構成

分類	想定する読者と利用形態	章
導入編	パーソナルデータを取り扱う事業者が理解し、または留意すべき事項を解説しており、特定の事業や計画の実態の有無、その進捗に関わらず一読することを想定している。	第 2 章基本理念
		第 3 章パーソナルデータを扱う事業モデル
		第 4 章パーソナルデータを扱う上で必要な ELSI
		第 5 章パーソナルデータと関連法制
		第 6 章トラストサービスの概要と現状
活用編	各事業者が自らの事業のアーキテクチャを設計・整理し、パーソナルデータの取扱いの適正性や潜在する課題を顕在化し、適切なパーソナルデータの利活用モデルを構築するためのリファレンスアーキテクチャとその記載方法について解説する。 設計書本体に当たるこれらの章は、パーソナルデータを扱う全ての事業者、ステークホルダが、ビジネスモデルや内部統制などのシステム設計を行うためのガイドとして、パーソナルデータを扱うまたは、扱う予定の事業を実施している、または計画している事業者が活用することを想定している。	第 7 章用語・定義
		第 8 章リファレンスアーキテクチャ本体（設計部）
		第 9 章ユースケースシナリオテンプレートの使い方
研究報告編	本書の作成にあたり、DTA では、国内での有識者会合及び実証研究実施者との会合を開催するほか、国際標準化の調査と推進を実行し	第 10 章パーソナルデータに関わる標準化

	た。ここでは本テーマに掲げる国際標準化活動について報告する。各事業者の事業実施における国際展開を検討する際の参考となることを想定している。また、本テーマの今後の進め方を記載した。	第 11 章今後の進め方
付属資料	リファレンスアーキテクチャ及び関連文書において用いられる用語の定義を取りまとめた「用語・定義書」、及び、データジャケットの国際標準化報告書を添付した。	第 12 章【付属資料】

1.3.1 導入編(第 2 章～第 6 章)

導入編は、第 2 章～第 6 章の 5 章により構成されている。これらの章は、パーソナルデータを取り扱う事業者が理解し、または留意すべき事項を解説しており、特定の事業や計画の実態の有無やその進捗に関わらず、一読されることを期待している。

1.3.1.1 第 2 章基本理念

パーソナルデータの取扱いは、個人のプライバシーという主権に大きな影響を及ぼすだけでなく、社会生活や企業活動とも密接に関わる。そこで、パーソナルデータを取り扱う事業者が、その事業の形態や立場に関わらず理解、または考慮すべき基本的な理念について述べる。

1.3.1.2 第 3 章パーソナルデータを扱う事業モデル

本書の利用者として想定されるパーソナルデータを取り扱う事業モデルについて、その概要を解説する。自らがパーソナルデータを扱う事業者なのかどうか、パーソナルデータを取り扱うとしたらどのような事業者に分類されるかなどについて明確な判断ができない、又は疑念を持っている事業者が、この章の示す類型化を参考にして、自らの事業モデルを確認することを想定している。

1.3.1.3 第 4 章パーソナルデータを扱う上で必要な ELSI

パーソナルデータは、個人のプライバシーや倫理に配慮した扱いが重要であることから、本書の作成と併行して有識者によるパーソナルデータ分野に関する ELSI 検討会を設置した。本章では、この検討会が取りまとめた、別冊の「パーソナルデータ分野に関する ELSI 検討会報告書」の概要を簡潔に解説する。

1.3.1.4 第 5 章パーソナルデータと関連法制

パーソナルデータの取扱いでは、個人情報保護法はもちろんのこと、その取り扱う事業によっては、各種業法に対する遵法性も重要となる上、国を越えたデータの取扱いなどでは、各国や地域の法制に照らして自らの事業内容との整合性に留意することが重要となる。

そこで、本書の作成において参照とするために、情報法制を専門とする弁護士により実施した「パーソナルデータ分野のアーキテクチャ構築における情報法制の調査」の概要を簡潔に解説する。

1.3.1.5　第 6 章トラストサービスの概要と現状

パーソナルデータを取り扱う事業では、パーソナルデータを提供する個人と事業者に限らず、複数の事業者が連携して事業を行うことが想定される。このような複数のステークホルダが連携して一つのシステムを構成する場合には、各機関や個人との間での認証や認可といった信頼関係の構築が重要となる。このような信頼関係を確立するために用いられる電子署名や認証などのトラストサービスは、国内外を問わず広く検討され、その導入や法令による導入なども進められている。そこで、本書の作成において参考とするために、外部の学術研究者が実施した「トラストサービス調査報告」の概要を簡潔に解説する。

1.3.2　活用編(第 7 章～第 9 章)

活用編はリファレンスアーキテクチャ本体(＝設計部)に当たる部分である。活用編は、各事業者が自らの事業のアーキテクチャを設計・整理し、パーソナルデータの取扱いの適正性や潜在する課題を顕在化させ、適切なパーソナルデータの利活用モデルを構築するためのリファレンスアーキテクチャとその記載方法について解説するもので、第 7 章～第 9 章により構成されている。

これらの章は、パーソナルデータを扱う全ての事業者、ステークホルダが、ビジネスモデルや内部統制などのシステム設計を行うためのガイドとして、**パーソナルデータを扱うまたは、扱う予定の事業を実施している、または計画している事業者に活用される**ことを期待している。

1.3.2.1　第 7 章用語・定義

リファレンスアーキテクチャ本体（設計部）をメインに本書において用いられる用語の定義を取りまとめた、別冊「用語・定義書」の概要とその利用方法について解説する。ここでは、法令などにより明確な定義のある用語以外に、慣例的に使われているものの、その定義や適用範囲の解釈が多様であるために、混乱や誤解を招く用語を整理してとりまとめている。

1.3.2.2　第 8 章 リファレンスアーキテクチャ本体（設計部）

リファレンスアーキテクチャ本体（設計部）は、各事業者が自らの事業のアーキテクチャを設計・整理するための手引書に当たる。冒頭では内閣府の提唱する Society5.0 リファレンスアーキテクチャとの位置付けを解説し、このリファレンスアーキテクチャ本体（設計部）の利用手順と利用上の留意点などを解説する。

1.3.2.3　第 9 章　ユースケースシナリオテンプレートの使い方

本章では、リファレンスアーキテクチャ本体（設計部）に従って、各事業者が記載するための様式(別冊のユースケースシナリオテンプレート)とその記載方法について解説する。また、ドライブレコーダのデータを収集し、個人情報を除去し、第三者に統計データを提供する事業の事例を用いて、実際の記載事例や、記載結果から得られた評価点を示している。

なお、この事業事例は民間事業者が実際に検討している事業についてヒアリングし記載したものである。「戦略的イノベーション創造プログラム（SIP）第 2 期／ビッグデータ・AI を活用したサイバー空間基盤技術／パーソナルデータアーキテクチャ構築」（以下、本プロジェクトという）の「パーソナルデータ実証研究」の採択事業とは異なる。なお、別冊の「ユースケースシナリオ集」には、同事業で実施された四つの実証研究のアーキテクチャについてテンプレートを用いて記載したものを収録している。

1.3.3　研究開発編(第 10 章～第 11 章)

本書の作成にあたり、DTA では、国内での有識者会合及び実証研究実施者との会合を開催するほか、国際標準化の調査と推進を実行した。これらの活動の内、パーソナルデータに関わる標準化について報告する。実証研究実施者等との会合内容別途報告する成果報告書に詳しく記載した[4]。本編は、各事業者が国際展開、国際標準化を検討する際の参考になることを期待している。

1.3.3.1　第 10 章パーソナルデータに関わる標準化

パーソナルデータの取扱いは、国内に閉じることなく、広く世界的に様々な取り組みがされている。本書の取りまとめと併行して、国際標準化にも取り組んでいる。国際標準化に関わる具体的な取り組みと、これらの活動について解説する。

1.3.3.2　第 11 章今後の進め方

本書の今後の展開方法を記載した。

1.3.4　付属資料（第 12 章）

1.3.4.1　リファレンスアーキテクチャ用語・定義書

1.3.4.2　データジャケットの国際標準化報告およびその概要

[4] NEDO　ホームページにて公開予定。

1.4　本書の目的と利用方法

本書の取りまとめを行なった背景と本書により解決が期待される課題などについて述べる。

1.4.1　パーソナルデータ分野に対する背景

パーソナルデータ分野を含むデータ流通において、我が国は信頼のおけるデータ流通のルール作りに取り組む方針 DFFT(Data Free Flow with Trust)を提唱している。その実現に向けたアーキテクチャ構築は喫緊の課題である。

パーソナルデータの流通を含む DFFT の実現に対して、個人生活者の視点では、自らがデータの扱いを把握・制御できないことに対する漠然とした不安がある。一方、パーソナルデータを取り扱う事業に取り組む企業や組織においては、このような個人生活者が漠とした不安が存在する状況において、その不安を解消し、企業・業界を超えたデータ流通・活用を推進するためのコンセンサスや共通の課題対応方式が確立されていないという課題がある。

今回の DTA の受託テーマでは、こうした問題点に対し、個人に対しては“便益や使途の見える化”によるデータ提供の促進、企業に対しては“魅力的なサービスの創出”のためのデータ活用の促進に資するための共通的なリファレンスアーキテクチャ設計手法を示すことが求められた。

1.4.2　研究開発の狙いと課題

データ流通は、特定の業種業態に閉じたものではない。つまりアーキテクチャの構築には、業種業態を超えた連携が必要となり、どこに技術的・制度的課題が存在するかを明確にし、解決策を見出す必要がある。また、データ流通市場を構成するデータ提供者、パーソナルデータストア(PDS)、情報銀行、データ共有事業者、データ処理事業者、データ取引市場運営事業者、データ利用者らが相互に接続するために、以下の課題を克服する個別分野を超えた総合的なアーキテクチャを構築するグランドデザインの整備が必要である。

1.4.2.1　アーキテクチャ設計の課題

アーキテクチャ設計にあたり、アーキテクチャ構築による成果がどのように社会実装に寄与し、どう使われ、データ提供者にどのように価値を還元するかなどを明らかにするユースケースシナリオを十分に示す必要がある。現状は、ユースケースシナリオテンプレートが定式化されていないため、ユースケースシナリオ自体が集積されず、その効用が社会に十分に認知されていない。

1.4.2.2　情報銀行とデータ取引市場の連携の課題

パーソナルデータを取り扱うと想定されている PDS、情報銀行、データ取引市場や各種関連事業者のうち、情報銀行とデータ取引市場については、総務省の検討会を受けて、民間による認定への取り組みが進められている。そこで、本プロジェクトの実証研究テーマの実施者と連携し、実証研究における具体的な課題を顕在化し、共有することが必要である。

1.4.2.3　分野間データ連携の課題

本プロジェクトでは、パーソナルデータ分野とともに、スマートシティ分野と地理空間情報分野の研究開発が行われるが、パーソナルデータは、当然ながらこれらの分野においても重要なデータ資源である。分野にとらわれず、パーソナルデータであることに配慮したデータ連携ができるユースケースシナリオテンプレートが求められている。

1.4.2.4　国際標準化の推進の課題

アーキテクチャの階層的整理と構築から、社会実装を進めるには、標準化の推進が求められる。特に、データ流通は国内に閉じないことを念頭におくと、国際標準化への展開が必要となる。この国際標準化への取組みにおいては、グランドデザインの欠如、ユースケースシナリオの集積不足、成果物の形態定義不明瞭がある。国際標準化推進政策の課題として、デジュール・フォーラム包括的標準化推進体制の欠如、SDO との連携の明確なミッションの欠如、リーダーシップ人材の不足などの課題がある。

1.4.3　課題解決への対応

前節の課題を解決するため今回推進体制（SIP DFFT タスクフォース）を組成し、このリファレンスアーキテクチャを作成した。この作成にあたり行った各課題への対応箇所（対応頁と章節項）を下記にまとめる。

① アーキテクチャ設計の課題

アーキテクチャ設計の課題は、まずアーキテクチャとは何かという基本的な概念の共有知の不足がある。そこで本研究では、アーキテクチャとは各事業者が自らの事業を設計・整理するための手引書であるとの定義を明確にし、アーキテクチャを設計するための手順を整理した（本書第 8 章)。また、実際の設計成果となる書面を定式化し、ユースケースシナリオテンプレートとしてまとめ、その使い方の実例を示した（本書第 9 章)。

このユースケースシナリオテンプレートを用いアーキテクチャ設計を行うことで、適切に、社会実装への寄与やデータ提供者への価値還元、パーソナルデータ保護や考慮すべき法制などを顕在化し、より良いアーキテクチャ設計となることが期待される。今回、併行して行われた複数の実証実験者に、本書の示す指針や手順を示し、実際にユースケースシナリオテンプレートを用いて、各々の実証実験のアーキテクチャ構築を整理検討していただいた結果、その有益性が以下の実務者の声に表れている（表 4)。

表 4　本プロジェクトの実証研究実務者の方々の声（気づきやコメント）

項目	ユースケースシナリオ集の頁	内容
社会実装	P12 P50	情報銀行に関する機能実装方針、情報銀行事業者間の連携促進に必要な条件、手法の確認ができる。 サービスを受ける利用者やサービスを提供する事業

		者にとって、リスクを低減することができ、社会的な消費者の受容性拡大および本格的な社会実装につながる。
使われ方	P36 P34 P50	アーキテクチャの図を共有し、図を示しながら議論をすることで、効率的で効果的に議論ができ、合意形成に役立つと思われる。 詳細レベルで関係者間の議論ができるようになった。 ステークホルダ間で、やり取りするデータ（個人情報、仮名化データ、匿名化データ）の整理、およびやり取りするデータ種別に基づいた、必要な契約・フローを洗い出すことができた。
データ提供者への価値の還元	P35 P50 P59	サービスを総合して利益を出すビジネスとなるが、各部分についてのお金の流れ、単価、頻度をパラメータとして設定することで全体のシミュレーションが可能となる。本アーキテクチャをベースとして、ビジネスのシミュレーションが可能になると期待できる。 生体認証（特に顔認証）は、「手ぶら」などの利便性の観点から利用が期待されている一方で、情報保護やプライバシーの観点での課題が多い。本手法によって、課題を見える化ができ、安心・安全な生体認証（特に顔認証）の利活用促進に寄与すると考える。 将来的に本手法を活用することにより、経済社会・地域社会やステークホルダにとって新たな付加価値の提供につながるデータのエコシステムを構築すべく、企業や各自治体等のステークスホルダとの連携を推進することが可能と考える。

② 情報銀行とデータ取引市場と連携の課題

情報銀行とデータ取引市場の連携については、今年度はその実証研究が実施されなかった。そこで、内閣府、総務省などの関連検討会の報告書などの内容を精査し、パーソナルデータを扱う事業モデルを整理した解説をした（本書第 3 章）。

③ 分野間データ連携の課題

分野にとらわれず、パーソナルデータであることに配慮したデータ連携ができるアーキテクチャとするために、パーソナルデータの本書における定義設定（本書 2.1）とパーソナルデータを扱う原則のあり方を示した（本書 2.4）。

また、パーソナルデータを扱うユースケースシナリオにおいては、そのステークホルダ

を ISO/IEC29100 の分類に沿って整理することを推奨した(本書 9.3)。加えて、少なくとも本プロジェクトの実証研究の分野、すなわち、情報銀行間連携、医療版情報銀行、生体認証（顔認証)、行動データの分野の実証実験実務者が統一されたユースケースシナリオテンプレートにより、各々のアーキテクチャの記載をすることが可能であるとともに、その記載により課題の顕在化が行われて有効に利用可能であることを示した。

④ 国際標準化の推進の課題

DTA では国際標準化推進の課題に取り組み、データ流通を活発化させるために、”データ取引システム“の概要、用語定義、利用のためのリファレンスモデル等に関わる国際標準を開発する標準化の必要性を IEEE-SA(Standard Association)に提案し、IEEE-SA DTSI(Data Trading System Initiative)が設置された（本書 10.1.2.1)。この活動は、具体的な標準仕様を策定する標準かプロジェクトの設置を求める PAR(Project Authorization Request)の策定を行うための活動である。この活動において、DTA は Chair と Secretary のポジションを獲得し、リーダーシップ人材を構築している（本書 10.1.2.1)。

また、ISO/TC 設立に対する協力と連携を進めるなどで、デジュール・フォーラム包括的標準化推進体制を構築した（本書 10.1.2.2)。加えて、SDO との連携の明確なミッションを定める一例として W3C との関係構築を図った（本書 10.1.2.3)。

なお、アーキテクチャ設計手順や定式化されたユースケースシナリオテンプレートは将来の標準化対象の候補である。

1.4.4 Society5.0 リファレンスアーキテクチャにおける本書の位置付け

Society5.0 リファレンスアーキテクチャに対して、本テーマでの実施内容をマッピングすると図 1 のようになる。本テーマの実施内容が Society5.0 リファレンスアーキテクチャの各々の層に関連していることが分かる。

即ち、トラストサービス調査はセキュリティ・認証、情報法制報告及び ELSI 検討報告はルール層（戦略・政策、組織に一部跨る)、また、今回本テーマで開発したユースケースシナリオテンプレート及びシナリオ集はアセットから組織層（法制関係表はルール層にも跨る）に跨る領域を複数の定式化された様式で表現するものである。

ユースケースシナリオテンプレートの 6 種は、それぞれが Society5.0 リファレンスアーキテクチャの複数の層に対応する。法制関係は戦略・政策、ルール層に、ステークホルダリストは組織に、ビジネス関係はビジネス、データリソースマップは、機能、データ、データ連携、アセットのそれぞれの層に関わる。データフローシーケンスはデータ連携に主に関わる。トラストリソースマップは、セキュリティ・認証に関わっている。

これらは、第 8 章と第 9 章で詳述される。即ち、アーキテクチャとは単なるスタックモデルではなく、複数のビューで記述されるべきであること、また、本テーマでは Usage 視点（利用やシナリオ視点）のアーキテクチャ構築であることを記述した。

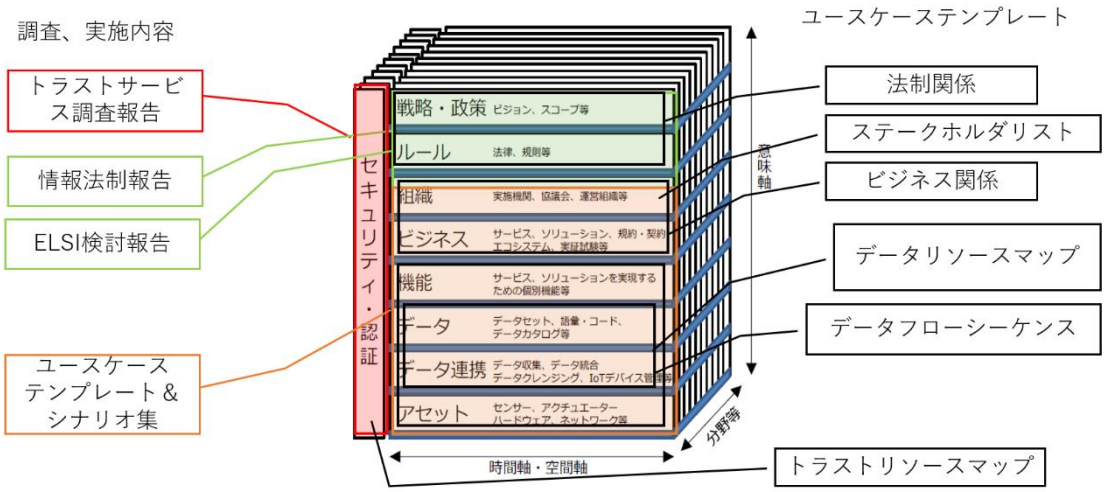


図 1　Society5.0 リファレンスアーキテクチャへの本書のマッピング[5]

[5] 出所：NEDO　「戦略的イノベーション創造プログラム（ＳＩＰ）第２期ビッグデータ・AI を活用したサイバー空間基盤技術におけるアーキテクチャ構築及び実証研究」公募説明会資料（https://www.nedo.go.jp/content/100893078.pdf）における Society 5.0 リファレンスアーキテクチャ図を記載

【導入編】

第2章　基本理念

パーソナルデータの取扱いは、個人のプライバシーという主権に大きな影響を及ぼすだけでなく、社会生活や企業活動とも密接に関わる。そこで、パーソナルデータを取り扱う事業者が、その事業の形態や立場に関わらず、理解または考慮すべき基本的な理念について述べる。

2.1　　パーソナルデータとは

パーソナルデータを扱う事業においては、パーソナルデータとは何かということについて、共通の認識を理解することが第一歩である。しかしながら、”パーソナルデータ”とは何かについて、法令などにおいて明確な定義を本書の作成時点で見出すことは容易ではなかった。

我が国においては、総務省主催の「パーソナルデータの利用・流通に関する研究会」[6]が平成 24 年 11 月から開催されており、”パーソナルデータ” という用語が使われたのが初出と思われる。その後、平成 29 年版情報通信白書の第 2 章、第 1 節のビッグデータの定義及び範囲[7]において、個人・企業・政府の 3 つの主体が生成しうるデータに対する 4 つの分類において、次のように記載されている。

個人：個人の属性に係る「パーソナルデータ」

「パーソナルデータ」は、個人の属性情報、移動・行動・購買履歴、ウェアラブル機器から収集された個人情報を含む。また、後述する『改正個人情報保護法』においてビッグデータの適正な利活用に資する環境整備のために「匿名加工情報」の制度が設けられたことを踏まえ、特定の個人を識別できないように加工された人流情報、商品情報等も含まれる。そのため、本章では、「個人情報」とは法律で明確に定義されている情報を指し、「パーソナルデータ」とは、個人情報に加え、個人情報との境界が曖昧なものを含む、個人と関係性が見出される広範囲の情報を指すものとする。

これらの定義や「パーソナルデータの利用・流通に関する研究会」の報告などにおいて、”データ”と”情報”の用語が混在しており、例えば上記の定義では、「パーソナルデータとは(略)情報を示すものとする。」と結ばれている。これらの用語の定義や厳密さについては本書における取扱いを別途定めるが、すくなくとも、平成 29 年版情報通信白書における表現から、パーソナルデータの指し示すものは、個人情報保護法の規定する範囲よりも広範

---

[6] 参照：https://www.soumu.go.jp/main_sosiki/kenkyu/parsonaldata/

[7] 引用：
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/pdf/n2100000.pdf

囲であり、かつ”個人と関係性が見出される”という表現により、そのデータまたは情報自体が明確に、個人識別性を持つものに限定されないものと解釈できる。

そこで、本書では、”パーソナルデータ” を
「個人に関するデータ。個人情報保護法に規定する「個人情報」に限らず、かつ個人識別性の有無に関わらず、位置情報や購買履歴など広く個人に関する情報を構成しうるデータ」
とする。

なお、個人情報に関しては、「個人情報の保護に関する法律」（平成 27 年改正、平成 29 年全面施行）（以下、「改正個人情報保護法」という）の第二条に定義されている。すなわち、「個人情報とは、**生存する個人**に関する情報であって、以下の**「個人識別符号」を含む**もの。1)身体の一部の特徴をデータ化した文字、番号、記号その他の符号や、2)サービスの利用者や個人に発行される書類等に割り当てられた文字、番号、記号その他の符号の内、政令で定めるもの（旅券番号、免許証番号等)」である。

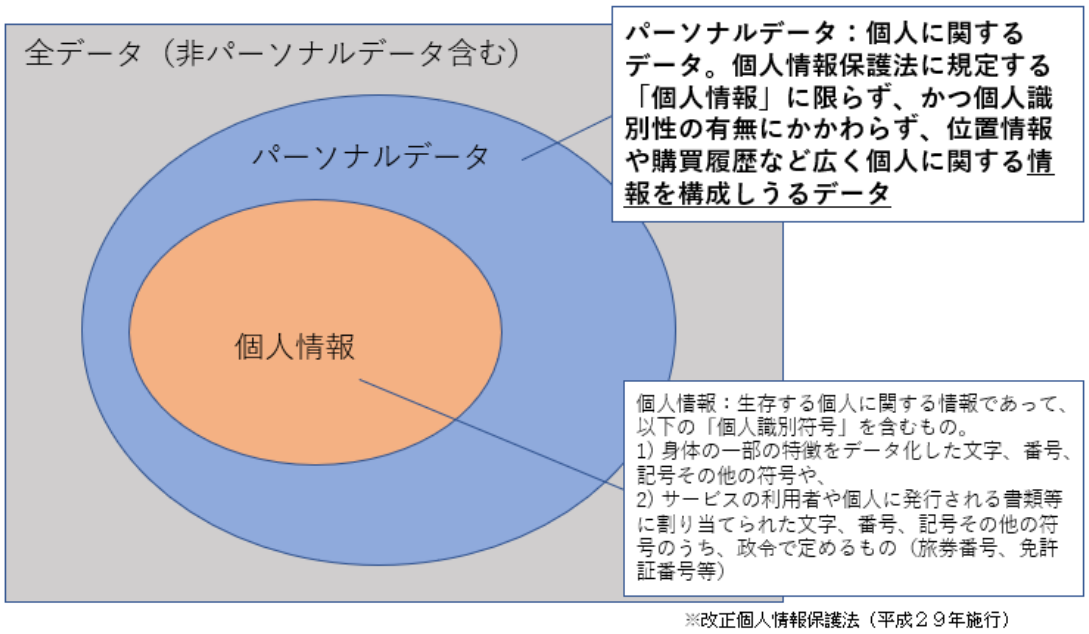


図 2　パーソナルデータ の適用範囲

パーソナルデータと個人情報の関係を図 2 に示す。個人情報保護法では、生存する個人に関する情報であって、個人識別符号を含むものとしているが、この定義に比べると、パーソナルデータの定義はより広いものとなっている。

なお、国際的には、Personal Data に関しては ISO 22857:2013(en), 3.9 において、次のように定義されている。

Personal data:　any information relating to an identified or identifiable natural person

すなわち、「特定または特定可能な人（以下、自然人[8]）に関するあらゆる情報」）とある。EU においては、次のように表現している[9]。

Personal data is any information that relates to an identified or identifiable living individual. （特定または特定可能な生存する個人に関するあらゆる情報）

ここで、特定可能（identifiable）」の解釈について整理する。個人を特定できる情報 Personally identifiable information（PII）について、ISO/IEC29100:2011 Amendment 1: 2018 改訂版に定義が記載されている。

Personally identifiable information(PII)とは、any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural

NOTE The “natural person” in the definition is the PII principal (2.11). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

すなわち、Personally identifiable information(PII)とは、

（a） 関連する自然人と結びつけるために利用できる情報

（b） 直接または間接的に関連する自然人を特定しうる情報

ノート：ここで、「自然人」は PII Principal（PII が関係する自然人）(2.11)。 PII principal が識別可能かどうかを判断するには、PII のセットと自然人の間の関連性を確立するために、データを保持するプライバシー関係者またはその他の当事者が合理的に使用できるすべての手段を考慮する必要がある。

国際標準におけるこの定義は、平成 29 年版情報通信白書及び本書での定義と比較すると、その範囲は狭く、個人情報の定義との間に位置づけられる。

---

[8] 「自然人」は法律関連用語。法人に対する個人（人間）。法人が法律によって人格が与えられるのに対して、人間は、この世に生まれて自然に人格が備わっている。

[9] 引用：https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

2.2　　データと情報

2.1 で述べたように、本書においてパーソナルデータとは、「個人に関するデータ。個人情報保護法に規定する「個人情報」に限らず、かつ個人識別性の有無に関わらず、位置情報や購買履歴など広く個人に関する情報を構成しうるデータ」
と定義した。これにより、その対象となる範囲は、社会において自然人の活動に起因して生じる全てのデータとなるが、”個人識別性の有無に関わらず”及び”情報を構成するデータ”としているが、これは、データと情報は異なるという考えに基づいた定義である。

そこで、本書では、この点をより厳密にするために下記のように定義する。

2.2.1.1　データ

「データとは、情報の表現を構成する要素であり、伝達、解釈または処理に適するように形式化され、複数のデータの組み合わせにより、情報を構成しうるものである。」
と定義する。

また、データは、一般に名前と年齢などのように、複数のデータとデータの属性などを示すメタデータから構成されるデータセットとして取り扱われる。

一方で情報とは、 ISO/IEC 2382-1,JIS X 0001 にて次節のように定義されている。

2.2.1.2　情報

「事実、事象、事物、過程、着想及び概念により構成され、対象物に対して一定の文脈中で特定の意味をもつもので、データセットを含むものもある。」

データセットと付帯情報(事実、事象、事物、過程、着想)及び概念により構成され、対象物に対して一定の文脈中で特定の意味をもつもの。

すなわち、データは、情報を構成する要素を示している。このため、パーソナルデータは、個々のデータやそれを含むデータセット自体が単体で直接に個人に関する情報を構成しうるものとは限らない点に留意が必要である。

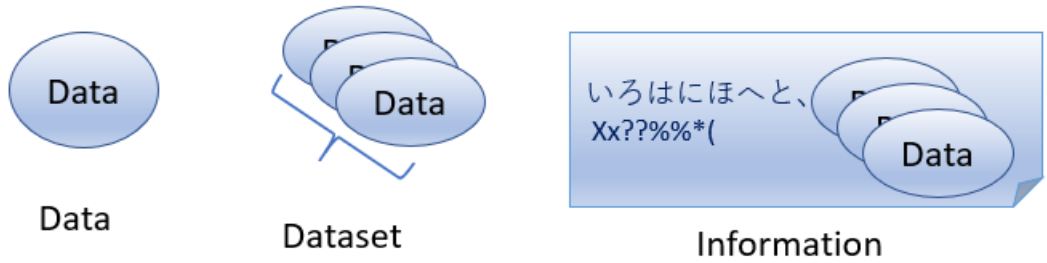


図 3　データと情報の区別

例えば、ある商店における販売場所、販売日時、商品分類により構成されるデータセッ

トには、直接には個人に関する情報を構成しないが、携帯電話や Wi-Fi などから取得される位置情報などを含むデータセットと連携することで、個人に関する情報を構成することが可能となることは、容易に想定できる。

このケースでは、

販売日時、商品分類により構成されるデータセットは、個人の活動に起因し生成されたデータが含まれている。携帯電話や Wi-Fi などから取得される位置情報を含むデータセットも、個人の活動に起因し生成されたデータが含まれている。

であり、いずれもが個人の活動に起因したデータセットであるという点である。

そして、このようなデータセットは、事後の加工、集計、解析などにより、個人に関する情報を構成しうるものであることは、十分に留意される必要がある。

このため、データセットを取り扱う事業者は、それらを取り扱う関係者がどのような加工、集計、解析を行うかを常に留意する必要がある。また、複数の機関やステークホルダにより構成される事業においては、各々の認証(Authentication)のレベルや、個々のデータセットの利用や提供に対する承認(Authorization)を明確にすることが必要である。

2.3　　データの特徴とオーナーシップ

データ及びその派生となるデータセットや情報は、土地や有形財などとは異なり、排他的所有が出来ない無形財という特徴を持っている。

有形財である土地や家屋、現金などは、その所有者から他の所有者に売買や譲渡により財が移動する場合には、原則的に複数の所有者がこれを所有することが出来ないため、所有権という権利で保護することが可能である。

これに対して、データは、複製可能でありその存在が排他性を持たないことから、所有権という概念では保護することは馴染まない。

このことは、平成 30 年 6 月に経済産業省が策定した「AI・データの利用に関する契約ガイドライン」[10]の、1 データの法的性質及び分類等の(1)総論において、次のように示されている。

データは無体物であり、民法上、所有権や占有権、用益物権、担保物権の対象とはならないため、所有権や占有権の概念に基づいてデータに係る権利の有無を定めることはできない(民法 206 条、同法 85 条参照)。 そして、知的財産権として保護される場合や、不正競争防止法上の営業秘密として法的に保護される場合は、後記第 3-2-(2)で述べるよう

[10] 引用：https://www.meti.go.jp/press/2019/12/20191209001/20191209001-1.pdf

に限定的であることから、データの保護は原則として利害関係者間の契約を通じて図られることになる。

同ガイドラインにおいて、(2)「データ・オーナーシップ」については、以下のように記載されている[11]。

データ契約の議論に際して、「データ・オーナーシップ」という言葉が用いられることがある。これには現在のところ法的な定義がなく、必ずしも「データに対する所有権を観念できる」という意味で用いられているわけではない。むしろ、データが知的財産権等により直接保護されるような場合は別として、一般には、データに適法にアクセスし、その利用をコントロールできる事実上の地位、または契約によってデータの利用権限を取り決めた場合にはそのような債権的な地位を指して、「データ・オーナーシップ」と呼称することが多いものと考えられる。

前記(1)のとおり、データは所有権、占有権、用益物権及び担保物権の対象とはならないため、著作権等の知的財産権が発生する場合は別として、わが国の現行法上、データに所有権その他の物権的な権利を観念することはできない。契約実務上、あるデータについて一方の契約当事者に 「データ・オーナーシップ」を帰属させるといわれる場合があるが、当該 契約当事者に所有権等の物権的な権利があると考えるのは困難であり、このような表現は、当該契約当事者が他の当事者に対して、データの利用権限を主張することができる債権的な地位を有していることを指すものと考えられる。

これらの考えは、我が国固有のものではなく、欧州においても特段の疑義はないものであろう。そこで、「当該契約当事者が他の当事者に対して、データの利用権限を主張することができる債権的な地位」を示すものとして、などの観念を用い、これらの権利の保護を行う取り組みがされている。

たとえば、欧州連合（EU）一般データ保護規則（General Data Protection Regulation: GDPR）は、個人データの処理に関する個人の保護、及び個人データの自由な流通のための規則を定めているが、これはデータそのものに対する保護ではなく、その利用権、コントロール権の保護という観念であることは、これらの規則が欧州域外に個人データを移転する場合の所定の手続きを定めていることからも理解できる。

---

[11] 引用：https://www.meti.go.jp/press/2019/12/20191209001/20191209001-1.pdf

2.4　パーソナルデータを扱う原則

パーソナルデータの取扱いについては、ISO/IEC 29100、米国 FTC FIPPs(Fair Information Practice Principles)、 OECD8 原則、など様々な取扱い原則が存在する。また、各国や団体、企業などが定めガイドラインなど、事業に関する規範が多数存在している。これらにおいて、その分類などは異なるが、その目指すところ、又は前提とするところに大きな齟齬はない。

そこで、パーソナルデータを取り扱う事業を行う者は、第 5 章及び別冊の「パーソナルデータ分野に関する ELSI 検討会報告書」を一読し、自らの原則を定めることを推奨する。

ここでは、ISO/IEC 20100、FIPPs、OECD8 原則について紹介する。

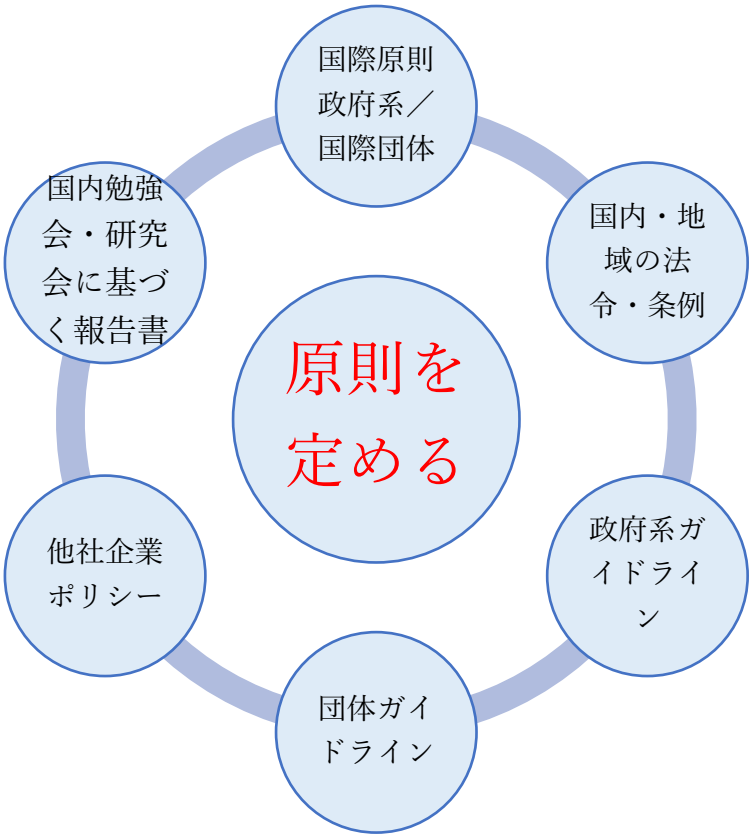


図 4　パーソナルデータを扱う原則の参照

2.4.1　ISO 29100:2011[12]におけるプライバシー原則

ISO 29100:2011 では、プライバシーと ICT システムでの Personally identifiable information（PII）処理に関連する要素であるプライバシーフレームワークが定義されて

[12] ISO/IEC 29100:2011 はフリーで入手可能。改訂版 ISO/IEC 29100:100 Amendment 1: 2018 は改定部分のみ記載したもので購入の必要がある。両者を併せて読む必要がある。

いる。また、プライバシーポリシーとプライバシーコントロールの設計、開発、及び実装の指針となるプライバシー原則が、多くの国及び国際機関によって開発された既存の原則に基づいて定義されている。ここには、OECD 8 原則や次項の各 FIPPs の原則が取り込まれていることが分かる。

a)プライバシーフレームワーク

4 種のアクターとその役割が定義されている。

・PII Principals: PII が関係する自然人
・PII controller: PII 処理の行われる理由（目的）及び方法（意味）を決定
・PII processor: PII コントローラに代わって PII 処理を実行し、また PII コントローラの指示に従って動作し、規定のプライバシー要件を順守し、対応するプライバシーコントロールを実装
・3rdParty: PII を PII コントローラや PII プロセッサから受け取ることができるが、処理はしない

b）プライバシー原則

プライバシー原則として次の 11 個が定義されている。

表 5　ISO 29100 におけるプライバシー原則

1.Consent and choice(同意と選択)
2.Purpose legitimacy and specification（正当性と仕様の目的）
3.Collection limitation（収集の制限）
4.Data minimization（データの最小化）
5.Use, retention and disclosure limitation（使用、保持、開示の制限）
6.Accuracy and quality（精度と品質）
7.Openness, transparency and notice（オープン性、透明性、通知）
8.Individual participation and access（個人の参加とアクセス）
9.Accountability（説明責任）
10.Information security（情報セキュリティ）
11.Privacy compliance（プライバシーコンプライアンス）

例えば、

1 (同意と選択)においては、PII Principal の選択は自由に、具体的に、知識に基づいて行われるべきこと、PII の収集または処理するためには PII Principal の Opt-in の同意（事前の同意）を取得すること、などが規定されている。

3 (収集の制限）では組織は無差別に PII を収集することを禁じられている。

2.4.2　FIPPs (Fair Information Practice Principles)の事例

FIPPs(Fair Information Practice Principles)は、1974 年のプライバシー法の中核、多くの米国の州、及び多くの外国及び国際機関の法律に反映されたフレームワークである。厳

密な法的要件ではなく、利益とプライバシーの必要性とのバランスを取るための原則の枠組みである。FIPPs はいくつかの組織から提案され、その中身は異なる。

米国 FTC(連邦取引委員会)は、「Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks」[13]の中で IoT 事業者が採用すべき FIPPs を示している。下記表はこれに Traceability を加えた 8 原則である。

表 6　IoT 事業者のプライバシーとセキュリティリスクに対する FIPPs

Notice	情報の収集について、情報提供者に通知すること
Choice	情報の提供可否を、情報提供者が選択すること
Access	情報へのアクセス権を適切に管理すること
Accuracy	情報の正確さについて明確にすること
Data Minimization	必要以上の情報を収集しないこと
Security	情報漏洩や改竄に対しセキュリティを確保すること
Accountability	情報の取扱いに対する責任を明確にすること
Transability	情報の第三者移転等の流れを明確化すること

FTC は公正な情報取扱原則として 2009 年に次の 5 原則を発表している[14]。

表 7　FTC FIPPs

Notice/ Awareness	消費者は、個人情報が収集される前に、エンティティの情報慣行(Information practice)の通知を受け取る必要がある。通知なしに、消費者は個人情報を開示するかどうか、どの程度まで、情報に基づいた決定を下すことができない
Choice/ Consent	消費者から収集した個人情報をどのように使用するかについて消費者に選択肢を与えること。Opt-in、 Opt-out が典型的な選択モデル。Opt-in 方式では、肯定的な手順を実施しないと情報収集者は情報を他の目的に使用できない。Opt-out 方式では、肯定的な手順を実施しないと情報収集者は情報を他の目的に使用できる
Access/ Participation	個人に関するデータにアクセスする能力と、そのデータの正確

13　引用：https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

14　引用：
https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm

	性と完全性を争う能力の両方を指す。アクセスを意味のあるものにするためには、データへのタイムリーで安価なアクセス、不正確または不完全なデータに異議を唱える簡単な手段、データ収集者が情報を検証できるメカニズム、および修正や消費者の反対意見を追加できる手段を含める必要がある
Integrity/ Security	データが正確で安全であること。データの整合性を保証するために、収集者は信頼できるデータソースのみを使用するなどの対策が必要。セキュリティには、データの損失及び不正アクセス、破壊、使用、または開示から保護するための管理的及び技術的な手段が含まれる
Enforcement/ Redress	これら原則は、施行メカニズムが存在する場合にのみ有効であることが一般的に合意されている。施行と救済のメカニズムがない場合、公正な情報慣行の指令は示唆的なものに留まる

2008 年の国土安全保障省（DHS）が掲げる FIPPs[15]は、Transparency（透明性）、Individual Participation（個々の参加）、 Purpose Specification（目的の仕様）、 Data Minimization（データの最小化）、 Use Limitation（使用の制限）、 Data Quality and Integrity（データの品質及び完全性）、 Security（セキュリティ）、 Accountability and Auditing（説明責任と監査）の８つを挙げる。

2012 年の Berkley Privacy Office の FIPPs[16]は、オンラインでの購買、ソーシャルネットワークに関わるもので、Transparency（透明性）、 Accountability（説明責任）、Information Protection（情報保護）、 Information Review and Correction（情報のレビューと修正）、 Choice（選択）の５つを挙げる。

2.4.3 OECD８原則

1980 年制定の「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 OECD 理事会勧告」(OECD プライバシーガイドライン）[17]は下記表８に示す８原則である。

表 8 OECD 8原則

収集制限	個人データを収集する際には、法律にのっとり、また公正な手段によって、個人データの主体（本人）に通知または同意を得て収集するべきで

[15]引用：https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf

[16] 引用：https://ethics.berkeley.edu/sites/default/files/fippscourse.pdf

[17] 引用：https://www.kantei.go.jp/jp/singi/it2/pd/dai7/siryou1-2b.pdf

	ある
データ内容	個人データの内容は、利用の目的に沿ったものであり、かつ正確、完全、最新であるべきである
目的明確化	個人データを収集する目的を明確にし、データを利用する際は収集したときの目的に合致しているべきである
利用制限	個人データの主体（本人）の同意がある場合、もしくは法律の規定がある場合を除いては、収集したデータをその目的以外のために利用してはならない
安全保護	合理的な安全保護の措置によって、紛失や破壊、使用、改ざん、漏えいなどから保護すべきである
公開	個人データの収集を実施する方針などを公開し、データの存在やその利用目的、管理者などを明確に示すべきである
個人参加	個人データの主体が、自分に関するデータの所在やその内容を確認できるとともに、異議を申し立てることを保証すべきである
責任	個人データの管理者は、これらの諸原則を実施する上での責任を有するべきである

2.5 Society5.0 と DFFT

サイバー空間とフィジカル空間を融合して、新しい経済や産業や生活を豊かにしていくことが Society5.0 のビジョンである。そのサイバー空間とフィジカル空間を融合させるのはデータによる連携であり、日本では、DFFT(Data Free Flow with Trust)を提唱している。データ連携においては、前節のプライバシー原則を定めるとともに、その取り扱いが原則に合致するシステムを設計する必要がある。そのためには、システムを構成する人や機関の関係、各々の機能、諸々の手続きを明確にする基礎となるアーキテクチャ設計が必要となる。

第3章　パーソナルデータを扱う事業モデル

本章では、パーソナルデータを取り扱う事業モデルについて、その概要を解説する。事業者自らがパーソナルデータを扱う事業者なのかどうか、パーソナルデータを取り扱うとすれば、どのような事業者に分類されるかなどについて明確な判断ができない、又は疑念を持っている場合、この章の示す類型化を参考にして、自身の事業モデルを確認することを想定している。

そこで、本章では、パーソナルデータを扱う事業モデルについて、公的な分類とそれ以外の分類に分けて解説する。公的な分類として、内閣官房 IT 総合戦略室　データ流通・活用ワーキンググループの取りまとめから引用する[18]。それ以外の分類としては、すでに確立しているデータの流通を前提としている事業形態を取り上げる。

なお、本章に示す各モデルは、もっぱらパーソナルデータの取り扱いを、その事業の主たる取り扱い対象とするものであり、全てのビジネスモデルが、これらのモデルのいずれかに単純に類型化されるものではない。むしろ、パーソナルデータは多くの事業に利用されるため、多くのビジネスモデルは本章の示す事業モデルの一部または全部を包含或いは組み合わせにより実現される。

3.1　内閣官房 IT 総合戦略室が定めた事業モデル

3.1.1　PDS

Personal Data Store（PDS）とは、他者保有データの集約を含め、個人が自らの意思で自らのパーソナルデータを蓄積・管理し、第三者への提供を含めその活用方法を自ら決定するための仕組み（システム）である。運用形態としては、個人が設定するパーソナルクラウドや個人が保有するスマートフォン等の端末のローカルストレージでデータを蓄積・管理する分散型（Decentralized）と、事業者が設定するサーバまたはクラウドでデータストアサービスとして集中的にデータを蓄積・管理する集中型（Centralized）がある。

蓄積管理する対象は、個人情報を含むパーソナルデータであり、問題がある場合には個人情報保護法の定める罰則や個人情報保護委員会による指導が課せられる。

---

[18] 引用：https://www.kantei.go.jp/jp/singi/it2/detakatuyo_wg/

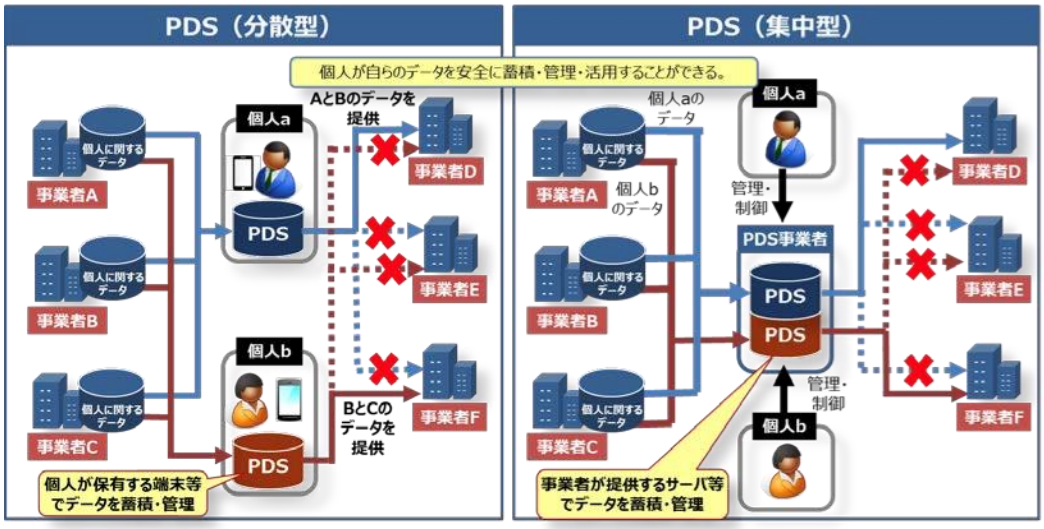


図 5　PDS の事業イメージ

表 9　PDS の事業概要

概要			
事業への認定制度と関連法規	なし	個人情報を含むデータ保護に関しては、 ・プライバシーマーク認証制度 ・認定個人情報保護団体の制度 などがある	
主な事業者と提供サービス	分散型	digi.me(英)	digi.me
		DataSign（日）	paspit
		アセンブローグ（日）	PLR：Personal Life Repogitory
		富士通（日）	Personium
		サイバーエージェント（日）	DataFoward
	集中型	DataSign（日）	paspit
パーソナルデータの扱い	有	情報銀行（信託機能を提供）と一体型の場合、自ら決定するための仕組みに基づく信託内容に限定される可能性がある	
データライフサイクル	各事業者の利用規約に従う。連携する他事業者とデータ保管について廃棄のサイクルが違う場合も想定される		
データ提供者の権利	データ提供者（プラットフォームユーザ、PU）がデータに対する利用権（コントロール権）を制御		

3.1.2　情報銀行（情報利用信用銀行）

「情報銀行」とは、実効的な本人関与（コントローラビリティ）を高めて、パーソナルデータの流通・活用を促進するという目的の下、本人が同意した一定の範囲において、本人が、信頼できる主体に個人情報の第三者提供を委任するというものである。「情報銀行」の機能は、個人からの委任を受けて、当該個人に関する個人情報を含むデータを管理するとともに、当該データを第三者（データを利活用する事業者）に提供することであり、個人は直接的又は間接的な便益を受け取る[19]。

総務省及び経済産業省により「情報信託機能の認定スキームの在り方に関する検討会」で、認定基準・モデル約款の記載事項・認定スキームから構成されるガイドライン「情報信託機能の認定に係る指針」[20]が取りまとめられ、民間による情報銀行の認定団体は本指針に基づき、認定制度を構築・運用する。ただし、認定は任意のものであり、認定を受けることが事業を行うために必須ではない。

上記指針に基づき、一般社団法人日本 IT 団体連盟が認定制度「Trusted Personal Data Management Service（TPDMS）」を運用している。2020 年 3 月現在、事業の準備段階を認定する「P 認定[21] 」を取得した情報銀行事業者は 4 社、通常認定（開始されている「情報銀行」サービスの PDCA によるマネジメント実施状態に対する認定）の事業者は 1 社となっている。

情報銀行の認定基準の中には、情報セキュリティやプライバシー保護対策の取り組み項目もあり、事業者には法律順守が義務付けられている。情報銀行が、個人情報漏洩などの事故が発生した場合や認定基準に違反した場合は、認定の留保、一時停止、停止、認定の取り消し、事業者名の公表などを含めて検討し、第三者委員会（監査（諮問）委員会）に諮問、判断がなされる。

---

[19] 情報信託機能の認定に係る指針 ver2.0（https://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000290.html）

[20] https://www.soumu.go.jp/main_sosiki/kenkyu/information_trust_function/index.html

[21] 「情報銀行」サービスが開始可能な状態である運営計画に対する認定（ https://itrenmei.jp/topics/2019/3646/）

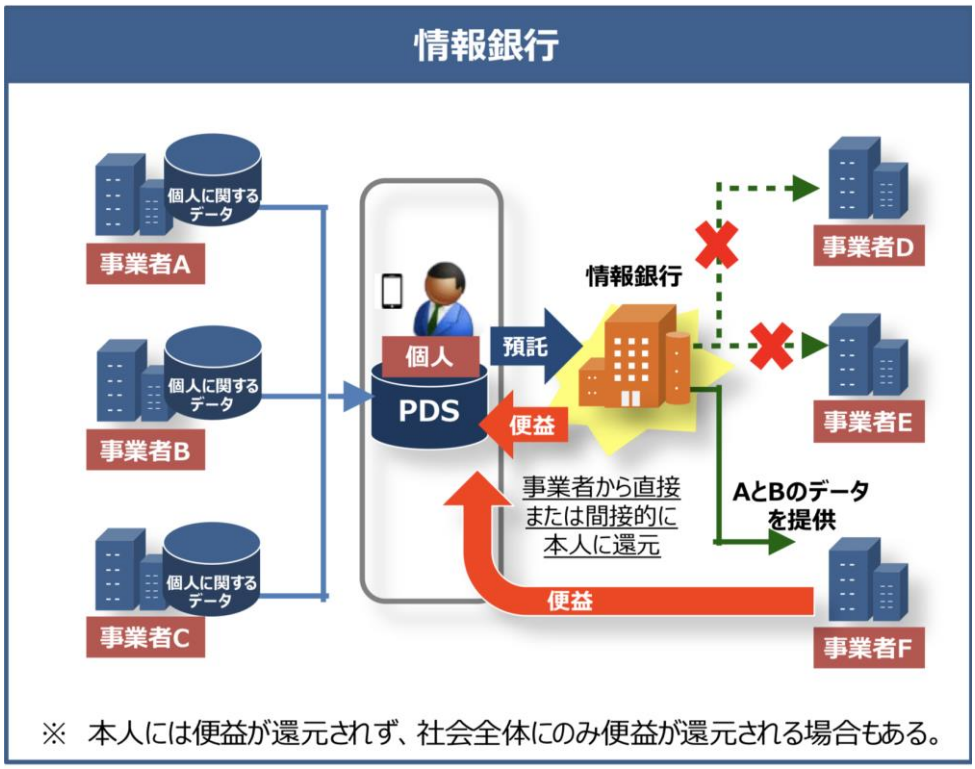


図 6　情報銀行の事業イメージ

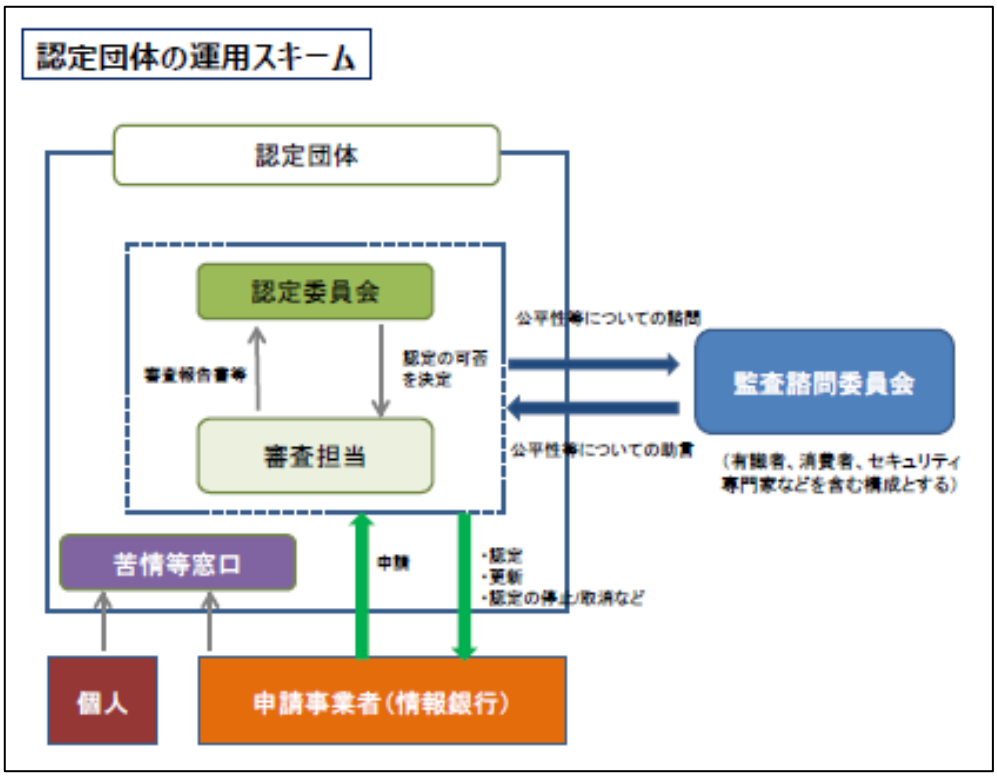


図 7　情報銀行の民間認定スキーム

表 10 情報銀行の事業概要

概要			
事業への認定制度と関連法規		情報銀行認定制度（P 認定及び通常認定）	総務省、経済産業省の「情報信託機能の認定に係る指針 ver1.0,ver2.0 に基づいて、一般社団法人日本 IT 団体連盟が認定
主な事業者と提供サービス	P 認定	三井住友信託銀行株式会社	「データ信託」サービス（仮称）
		フェリカポケットマーケティング株式会社	地域振興プラットフォーム（仮称）
		株式会社 J.Score	情報提供サービス（仮称）
		中部電力株式会社	地域型情報銀行サービス（仮称）
	通常認定	株式会社 DataSign	「paspit」
パーソナルデータの扱い		有	
データライフサイクル		各事業者の利用規約に従う。連携する他事業者とデータ保管について廃棄のサイクルが違う場合も想定される	
データ提供者の権利		データ提供者（プラットフォームユーザ、PU）がデータ利用権を情報銀行に委譲し、情報銀行が制御	

3.1.3　データ取引市場

データ取引市場とは、データ保有者と当該データの活用を希望する者を仲介し、売買等による取引を可能とする仕組み（市場）である。そこでは、価格形成・提示、需給マッチング、取引条件の詳細化、取引対象の標準化、取引の信用保証等の機能を担うことが想定され、重要な社会機能の１つとして期待されている[22]。

このデータ取引市場は、データ提供者とデータ利用者(データ提供先)の仲介を行うとともに、データ取引の決済機能を提供するものである。一般には”データ取引所” と言われる場合もあるが、金融における証券取引や商品取引とはその性質がいささか異なるため、混同を避ける意味から本書では”データ取引市場”という言葉を用いて説明する。

現在、AI による社会進化の源泉として、データが新しい価値資産であることは、広く認知されつつあり、ビッグデータという言葉も広く使われている。しかしビッグデータの示すものは、単純にデータの量が多いことと、その種類が多いことではその意味が異なる。例えば、成人男子の血圧データが大量にあるという場合と、血圧、運動量、睡眠時間、購買履歴、移動履歴などの多種のデータがある場合では、それらのデータから AI などが導き出せる推論の範囲が自ずと違ってくることは、容易に想像できる。

一方、IoT(Internet of Things)機器の普及により、様々な機器やセンサからのデータが収集され利活用されるようになりつつあるが、個々の会社や個人が設置し利用できる機器やセンサは、その業界内や業態内に限定されている。

そこで、業態や業界、個社や個人の限定された範囲で生成、収集するデータを、相互に流通させ利活用させる仕組みとして、”データ取引”がある。ここで**”データ取引”とは、「異なる組織や個人の間で、データが提供元から提供先へ提供されるのに対して、データ提供先からデータ提供元に何らかの便益が戻される関係」**を示すものである。

このデータ取引を実現する場が、データ取引市場であり、その場を提供する者をデータ取引市場運営事業者と言う。また、このデータ取引市場を介したデータと便益の取引行為を、データの市場取引と言う。

これに対して、従来からデータ提供元とデータ提供先が直接に相対で、データの提供と便益の提供を取引すること形態は多く存在している。例えば、SNS では、利用者の様々なデータが SNS のサービス会社に提供される代わりに、SNS サービスという便益が提供されており、これも一つのデータ取引の事例と言えるが、この場合には相対取引であり、データ取引市場を介した市場取引とは異なる。

つまり、**データ取引市場とは、「異なる複数のデータ提供元とデータ提供先が参加し、デ**

---

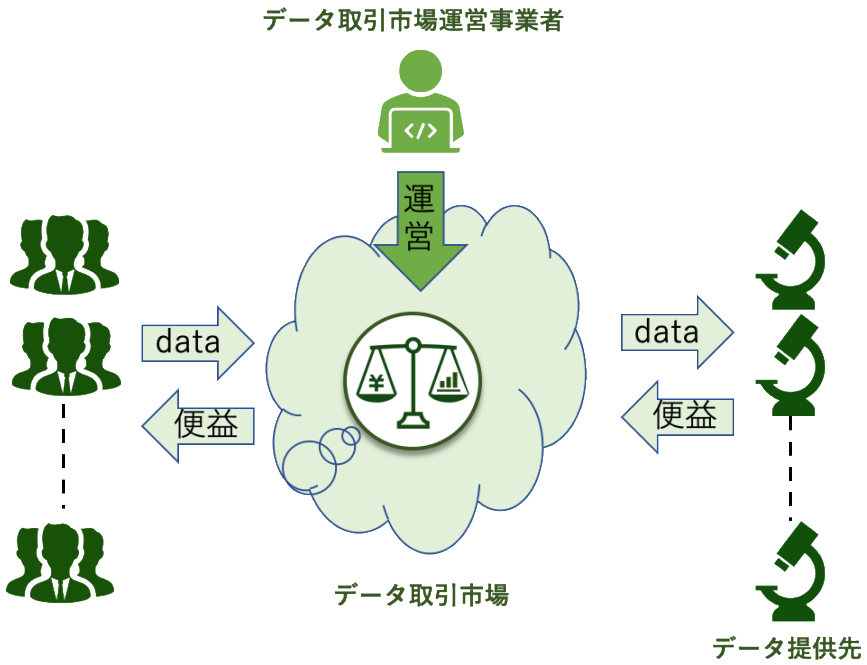
[22] 内閣官房 IT 室のデータ流通環境整備検討会、AI、IoT 時代におけるデータ活用ワーキンググループの中間とりまとめより引用：
http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/detakatsuyo_wg_dai9/siryou1.pdf

ータの提供と便益の提供が取引される場」ということになる（図 8）。

このような社会基盤に類似のものとしては、証券や商品取引所、または青果や魚などの卸売市場があるが、データ取引市場で取り扱うデータは、証券や商品、青果市場と以下の点が大きく異なる。

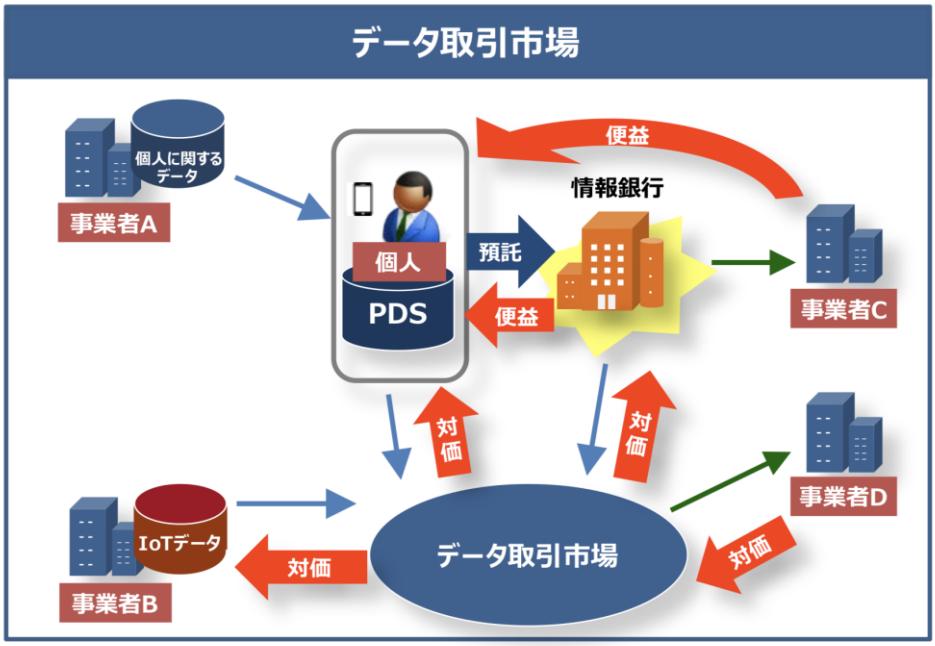
1. データは排他的所有が出来ない無形財である
   データは、どのような形で提供されたとしても、その実体や記憶、記録は提供元に残る点が、有形財取引とは大きく異なり排他的な所有が出来ない。このため、法による所有権という概念での保護が適さないと言える。
2. データ取引により移転するのは、データの写像である
   データの提供とは、データの実体の原本の移転ではなく、その写像の移転となる。
3. データ取引では、その一部または全部の利用権が移譲される
   データ取引では、データ提供元と提供先の間で、そのデータの利用に関する約定を定めることにより、その利用権が移譲される。(所有権ではないことに注意)

例えば、提供元がその原本を消滅させることや、他の第三者に提供しないことを約定で定めることにより、排他的所有と等価な移転は実現できる。



異なる複数のデータ提供元とデータ提供先が参加し、データの提供と便益の提供が取引される場

図 8 データ取引市場と取引市場運営事業者



※ データ取引市場におけるデータ提供主体としては、事業者、個人、情報銀行が想定される。

図 9 データ取引市場の事業イメージ

表 11 データ取引市場の事業概要

概要		
事業への認定制度と関連法規	データ取引市場運営事業者認定	一般社団法人データ流通推進協議会が基準を定めて認定
主な事業者と提供サービス	なし	
パーソナルデータの扱い	有	仲介するデータの制約は特になし
データライフサイクル	各事業者の利用規約に従う。連携する他事業者とデータ保管について廃棄のサイクルが違う場合も想定される	
データ提供者の権利	データ取引市場運営事業者は仲介業のため、データ提供者の権利は各事業者のサービスに依存する	

3.1.3.1 データ取引市場運営事業者の提供する仲介機能

異なる複数のデータ提供元とデータ提供先が参加し、データの提供と便益の提供が取引されるデータ取引市場がデータ提供元とデータ提供先である参加者に対し提供する基本機能の一つが仲介機能である。

データ取引市場では、データ提供者が提供可能なデータセットの概要やメタデータ、サンプルデータや提供条件などを取引市場に開示し、これをデータ提供先が検索、閲覧でき

る仕組みが提供される。また、実装によっては、データ提供先側から求めるデータセットの概要やメタデータの要求要件を示し、これを適切なデータ提供元に通知するなどの仕組みを提供する場合もある。

仲介機能を中立かつ公平に提供する上で最も重要なことは、データ取引市場運営事業者は、マッチングに必要な情報の登録や検索機能を提供することのみを行い、自らが特定のデータセットの登録や検索、要求などを行わない事である。特に、取引の有無に関わらず、データ取引市場運営事業者が、定常的にデータを配備、保管することは、それらのデータを積極的に販売させるインセンティブを誘発し、中立性を損なう要因となるため、これを行わない事が重要になる。また、提供価格などのデータ取引条件の交渉は、データ提供者とデータ提供先により行われ、データ取引市場運営事業者は、その交渉を円滑に進めるためのシステムの提供のみを行うことで、価格に対する恣意性を排除する事が求められる。

総務省の情報通信審議会　情報通信政策部会　IoT 政策委員会　基本戦略ワーキンググループ「データ取引市場等サブワーキンググループ取りまとめ」[23]では、具体的なルールの事例として、体制の整備の項目において、以下のように検討結果が記載されている。

売買を行わない、自らデータを保持しない、価格決定をしない(公正・中立の立場から取引を仲介)

この総務省**の**取りまとめを受けて、一般社団法人データ流通推進協議会(DTA)が制定したデータ取引市場運営事業者認定基準の説明文章では、データ取引市場運営事業者を図 10 のように定義している。

データ提供者とデータ提供先を仲介し、データと対価の交換・決済の機能を提供する者。データ取引市場運営事業者は**自らデータを収集・保持・加工・販売をしない。**

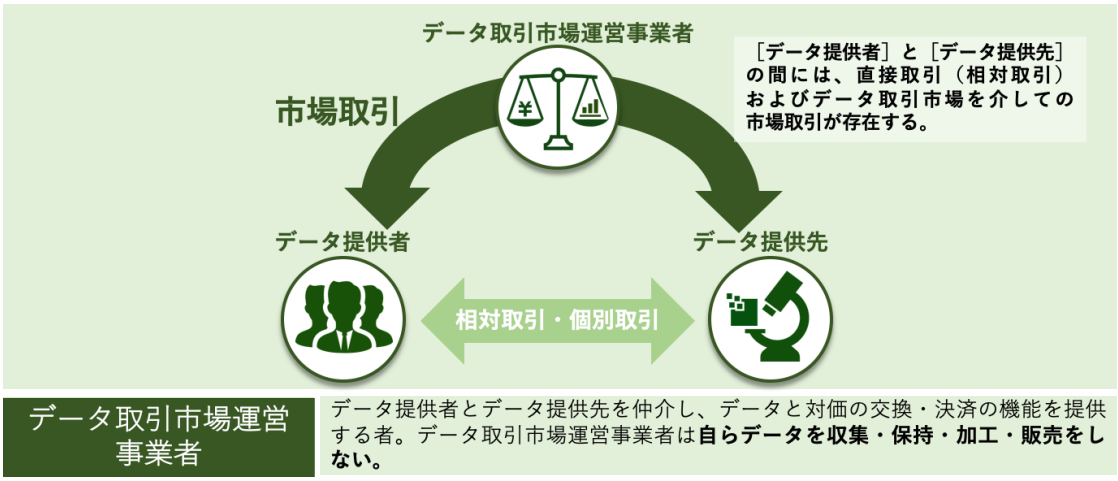


図 10 DTA によるデータ取引市場運営事業者の定義

[23] 引用：https://www.soumu.go.jp/main_content/000501157.pdf

3.1.3.2　データ取引市場運営事業者の提供する決済機能

データ取引市場運営事業者が提供するもう一つの中心的な機能は、データ取引に係る対価とデータの確実な交換を行うための決済機能である。一般に、代金決済は、電子決済であれクレジットカード支払いや現金決済であっても、その基本は、品物や役務の提供と対価の支払いの両方の行為が確実に実行されることが重要である。

データ取引においては、データ提供者とデータ提供先が合意した条件に合致したデータセットとその利用条件が確実に移転し、その対価が確実に支払われることを意味する。

一般的なデータ取引市場を介したデータ取引の流れの事例を図 11 に沿って説明する。

1)データ提供者は、自らが提供可能なデータの概要やその提供条件などを、データ取引市場に登録する。

1-1)あるいは、データ 提供先が登録したデータ要求概要を検索し、それに対応したデータがある場合には、そのデータ概要を登録する。

2)データの提供を受けるデータ提供先は、データ取引市場にアクセスし、提供を受けたいデータを検索する。

2-1)あるいは、適当なデータがない場合には、要求するデータの要求概要を登録する。

3)、3’）データ提供者とデータ提供先は、取引したいデータを見つけた場合、データ取引市場運営事業者の提供するプラットフォーム上で、価格やデータ提供項目の詳細を交渉する。

4)交渉の結果、取引条件について合意形成が出来た時点で、データ提供先は、データ取引市場運営事業者の提供するプラットフォーム上で注文書を発行する。

5)注文書を受け取ったデータ提供者は、その内容を受諾する場合、データ取引市場運営事業者の提供するプラットフォーム上で注文請書を発行する。

この時点で、データ取引の合意が成立したことになり、データ提供者とデータ提供先には、それぞれデータ提供の履行義務とデータ受領の履行義務が確定する。大事なことは、この時点までは、提供されるデータは取引市場に存在せず、かつ交渉にデータ取引市場運営事業者が介在しないことである。

6)データ提供者は、指定された期日までにデータをデータ取引市場運営事業者の提供するストレージエリアに納品する。

6’)一方、データ提供先は、対価をデータ取引市場運営事業者に収める。

7)、7’)データと対価が間違いなく揃った時点で、データ取引事業者は、対価とデータをそれぞれデータ提供者、データ提供先に送達する。

以上は、一般的な流れであり、対価の支払い方法やデータの収受などの方法は、データ取引市場運営事業者のサービスにより異なる。

ここで、重要なことは、データ取引市場運営事業者は、このような仕組みを参加者に対して公平かつ一様に提供し、その内容を約款などで明確に定めていることである。

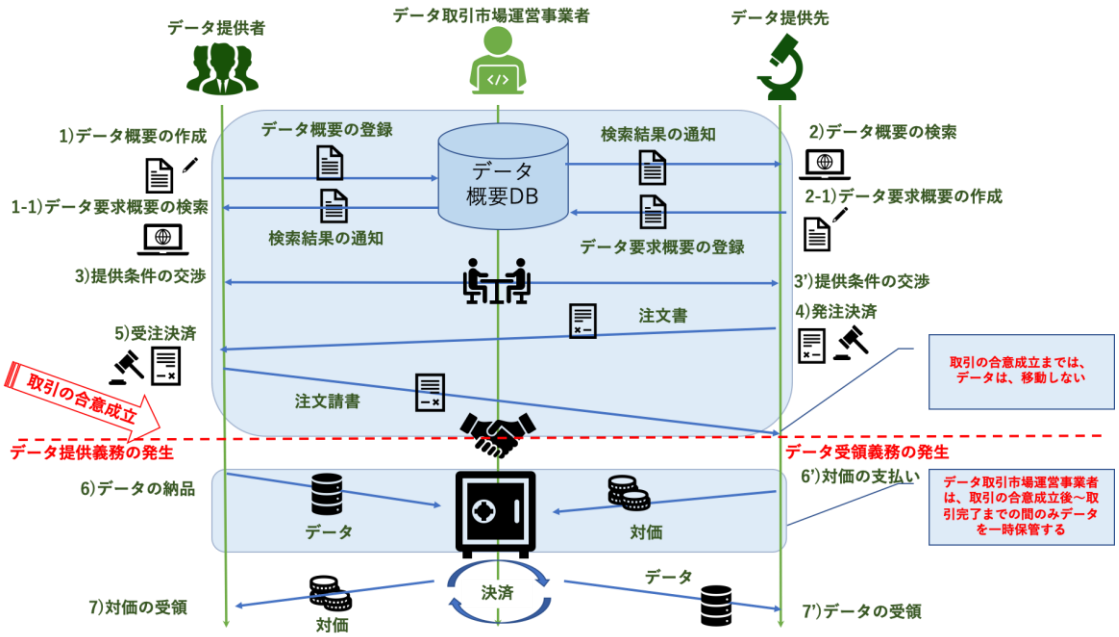


図 11 データ取引市場によるデータ取引の流れ

3.1.3.3 データ流通支援事業者(データブローカー)とデータ取引市場運営事業者の違い

データ取引市場への参加者という視点からデータ流通市場の各ステークホルダを整理した分類は、一般社団法人データ流通推進協議会(DTA)が制定したデータ取引市場運営事業者認定基準[24]の説明文章に示されている（図 12)。

ここで、データを提供するものとして、自らの事業や観測活動などによりデータを生成、取得する、またはそれらのデータを整理・加工したり保管・配備したりする者をデータ生成者、他のデータ提供者からのデータに対し、整理・加工・保管・配備し提供するものを、データ流通支援事業者(データブローカー)と定めている。

これに対して、データ提供者からデータの提供を受け、サービス・製品などに活用する他、自らの事業に利用する者がデータ提供先として分類されている。

これらは、役割の分類なので、実際に多くの事業者は、データ提供者であるとともに、データ提供先となると想定されている。

---

[24] 参考：https://data-trading.org/wp-content/uploads/2019/01/dta_20180928_01.pdf

例えば、情報銀行は、個人からのデータを収集し、整理、加工し、第三者へ提供をするので、この分類ではデータ流通支援事業者（データブローカー）になる。

その他、産業界において特定の産業のデータを共有するデータ共有事業者も同様に他のデータ提供者からのデータに対し、整理・加工・保管・配備し提供するものである為、データ流通支援事業者(データブローカー)となる。

すなわち、データ流通支援事業者(データブローカー)とデータ取引市場運営事業者は、自らデータを収集・保持・加工・販売を行うか行わないかという点が異なる。

図 12 データ取引市場の参加者

3.1.3.4 データ取引市場と情報銀行の違い

情報銀行では、情報銀行からデータの提供を受け取る者は、その情報を第三者に提供できない。しかしながら、データ取引市場は、透過型の仲介・決済機能を提供する透過型モデルのため、情報銀行とデータ提供先の中間に位置付けられることが想定されている（図 13）。

また、情報銀行がデータ取引市場の仲介により個人から情報の提供を受けることも、想定されている（図 14）。

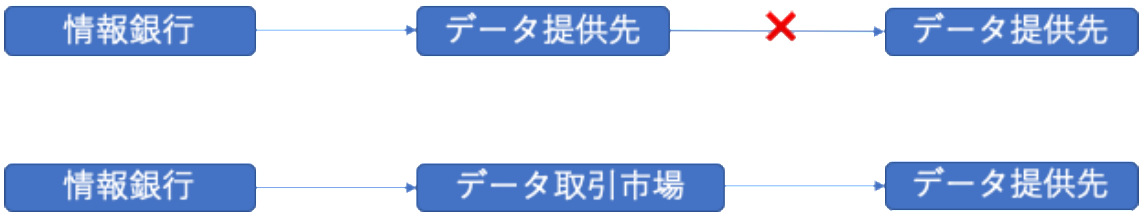


図 13 データ取引市場と情報銀行の連携

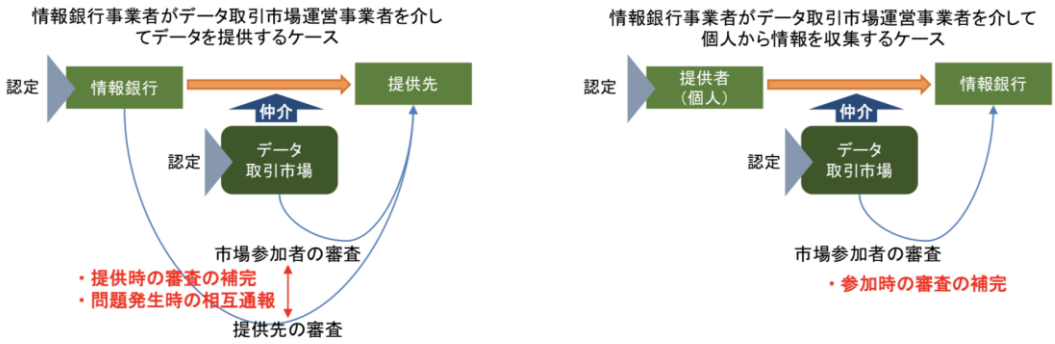


図 14 データ取引市場と情報銀行の相互補完

3.2 その他データを流通させる事業モデル

3.2.1 DMP (Data Management Platform)/ CDP (Consumer Data Platform)

DMP（データ・マネジメント・プラットフォーム）は、マーケティングのための統合されたデータ基盤であり、大別すると、様々なサイトのアクセスデータを収集・蓄積するパブリック DMP と、自社の保有する顧客情報を中心に収集・蓄積・統合管理するプライベート DMP がある。

パブリック DMP は、Cookie 等のオンライン識別子で収集された Web サイト上の行動データであるオーディエンスデータを主に収集し、推計も含めた性別・年代等のデモグラフィックデータや趣味趣向などの属性情報を付与することで、広告配信のターゲティングや分析に活用する。主に、そのデータだけでは特定の個人を識別できない個人に関する情報として取り扱うが、他のデータと連携して活用する場合は容易照合性についても考慮しなければならない。自社の顧客データとの連携する場合や、複数のデータや項目を組み合わせることで特定の個人を識別しうる蓋然性があり、その場合は個人情報として取り扱う必要がある。

プライベート DMP は、CDP（カスタマーデータプラットフォーム）とも呼ばれている。顧客個人単位のデータを集約・統合し活用するためのプラットフォームであり、対象となるデータは、オーディエンスデータだけでなく、オフラインの購買情報や位置情報等も含まれる。そのため、特定の個人を識別できる場合は個人情報として取り扱うことが求められる。

プライベート DMP であっても、他社のデータを突合することでマーケティング上のターゲティング精度を向上させることが行われている。最後に、そのような複数のデータの突合を前提として、提供元で個人識別性がある場合と提供先で個人識別性がある場合の組み合わせによって個人情報保護法第 23 条データの第三者提供の規制が適用されるかどうかを表 12 に示す。インターネット広告の世界では、データ収集の入り口（提供元にある段階）では非個人情報でも、第三者に提供された結果、提供先の事業者が保有する情報との突合により、個人を特定する情報に変わることがある。DMP 事業者が端末やブラウザに紐づけられた端末識別情報を、顧客情報を保有する企業に提供するケースが典型例とされている。提供元と提供先のいずれかで個人が識別される可能性が高い場合は、個人情報を取り扱う可能性を予見して対処をしておくべきである。

表 12 個人の識別性と個人情報保護の適用性の検討[25]

提供元での個人識別性	提供先での個人識別性	適用対象
×	×	第三者提供の規制対象とならない
×	○	第三者提供の規制対象とみなされる可能性が高い※
○	×	第三者提供の規制対象となる
○	○	第三者提供の規制対象となる

※令和 2 年改正個人情報保護法で規制対象となる予定

表 13　DMP の事業概要

概要			
事業への認定制度と関連法規		なし	
主な事業者と提供サービス	パブリック	ヤフー株式会社「Yahoo!DMP」	
		デジタル・アドバタイジング・コンソーシアム株式会社「AudienceOne」	
		株式会社インティメート・マージャー「インティメート・マージャ（IM-DMP)」	
		Supership 株式会社「Fortuna」など	
	プライベート	トレジャーデータ株式会社「TREASURE CDP」	
		株式会社ブレインパッド「Rtoaster」	
		株式会社フロムスクラッチ「b→dash」	
		株式会社アクティブコア「activecore marketing cloud」など	
パーソナルデータの扱い		有	一般社団法人日本インタラクティブ広告協会（JIAA）によるガイドラインがある
データライフサイクル		各事業者の利用規約に従う。連携する他事業者とデータ保管について廃棄のサイクルが違う場合も想定される	
データ提供者の権利		データ提供者の権利は各事業者のサービスに依存する	

[25] 総務省　学術雑誌『情報通信政策研究』第 2 巻第 2 号　「オンライン広告におけるトラッキングの現状とその法的考察―ビッグデータ時代のプライバシー問題にどう対応すべきか」本文を参考に表を作成（https://www.soumu.go.jp/iicp/journal/journal_02-02.html）

3.2.2　情報加工サービス（音声文字起こしサービス）

情報加工サービスにおけるパーソナルデータの扱いの事例として、音声文字起こしサービスを例にとる（表 14)。

アマゾン・ウェブ・サービス（AWS）が提供する「Amazon Transcribe[26]」は、音声からテキストに変換する自動音声認識技術による文字起こしサービスである。日本語を含む複数の言語に対応しており、医療関連の音声をテキストに変換する医療向け機能を搭載した「Transcribe Medical」も提供されている。(いずれも有料)

このサービスは、コールセンターでの個人情報を含んだやり取りや患者と医師間の医療相談など個人情報への配慮を求められるシーンでの活用も想定しており、機密性の高い個人識別情報(PII)対策として、社会保障番号、クレジットカード番号、銀行口座番号、名前、メールアドレス、電話番号、郵送先住所などの情報を識別し、「PII」という文字列に置き換える機能[27]を有している。本件は、サービスの 1 機能であるが、同様の動きは、Web ブラウザの Cookie 廃止の動き[28]と新プロトコル[29]の提案などにも見られる。パーソナルデータ活用にあたっては、法令や事業認定制度などの整備と併行して、技術的な対応策の取扱いの推進も重要である。

表 14 情報加工サービスの事業概要

概要		
事業への認定制度と関連法規	なし	
主な事業者と提供サービス	多種多様な形態がある	
パーソナルデータの扱い	有	個人情報の自動編集機能の提供が普及するかは今後の状況次第
データライフサイクル	各事業者の利用規約に従う。連携する他事業者とデータ保管について廃棄のサイクルが違う場合も想定される。	
データ提供者の権利	データ提供者の権利は各加工事業者のサービスに依存する	

[26] https://aws.amazon.com/jp/transcribe/

[27] 「Amazon Transcribe で、個人情報の自動編集機能を提供開始」
https://aws.amazon.com/jp/blogs/news/now-available-in-amazon-transcribe-automatic-redaction-of-personally-identifiable-information/

[28] third party cookies obsolete　https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html

[29] Web Advertising Business Group　https://github.com/w3c/web-advertising/blob/master/README.md

3.2.3　認定匿名加工医療情報作成事業者・認定医療情報等取扱受託事業者

医療分野の研究開発に資するための匿名加工医療情報に関する法律「次世代医療基盤法」（平成 29 年法律第 28 号）が、平成 30 年 5 月に施行され、個人の権利利益の保護に配慮しつつ、匿名加工された医療情報を安心して円滑に利活用するため、高い情報セキュリティを確保し、十分な匿名加工技術を有するなどの一定の基準を満たし、医療情報を取得・整理・加工して作成された匿名加工医療情報を提供するに至るまでの一連の対応を適正かつ確実に行うことができる者を認定する仕組みが設けられた。主務府省（内閣府、文部科学省、厚生労働省及び経済産業省）において、事業者の認定が行われる（図 15）。

そのうち、医療情報を取得・整理・加工して匿名加工医療情報を作成・提供する事業者が認定匿名加工医療情報作成事業者として認定され、認定匿名加工医療情報作成事業者の委託を受けて医療情報等又は匿名加工医療情報を取り扱う事業者が認定医療情報等取扱受託事業者として認定される。

この次世代医療基盤法のもとでは、医療機関、介護事業所、地方公共団体等は、あらかじめ本人に通知し、本人が提供を拒否しない場合、認定事業者に対し、医療情報を提供することができる。（医療機関等から認定事業者への医療情報の提供は任意）また、個人情報保護法での個人情報は生存する個人に対するものであるのに対して、生存する個人に関する情報に加え、死亡した個人に関する情報も保護の対象としている点に違いがある。事業概要を表 15 にまとめる。

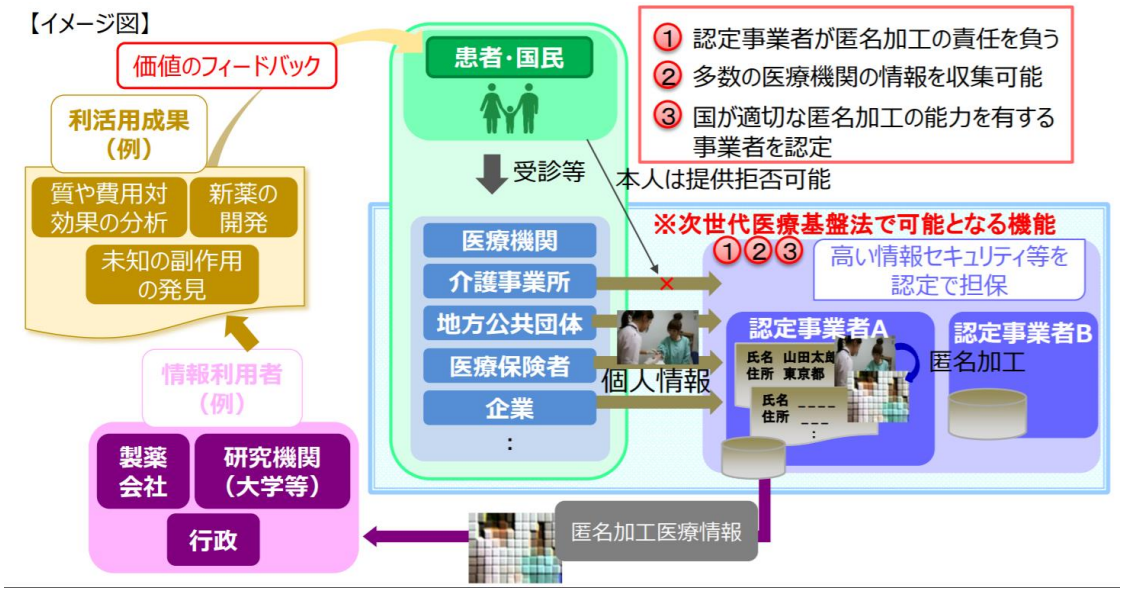


図 15 次世代医療基盤法の全体像

表 15 認定匿名加工医療情報作成事業者・認定医療情報等取扱受託事業者の事業概要

概要		
事業への認定制度と関連法規	事業者認定制度	次世代医療基盤法に基づいて、主務府省（内閣府、文部科学省、厚生労働省及び経済産業省）が事業者を認定
主な事業者と提供サービス	認定匿名加工医療情報作成事業者	一般社団法人ライフデータイニシアティブ
	認定医療情報等取扱受託事業者	株式会社エヌ・ティ・ティ・データ
パーソナルデータの扱い	有	※生存する個人に関する情報に加え、死亡した個人に関する情報も保護の対象
データライフサイクル	各事業者の利用規約に従う。連携する他事業者とデータ保管について廃棄のサイクルが違う場合も想定される	
データ提供者の権利	本人が事業者への情報提供を拒否できる	

3.2.4 MyData Operator のリファレンスアーキテクチャ（機能層例）

3.2.4.1 MyData と MyData Operator

MyData とは”パーソナルデータに関する個人の関与をエンパワーメントすることで、人間中心のデータ活用を実現する“というビジョンである。これを推進する国際的な非営利団体である MyData Global は、2012 年～2013 年にかけて Open Knowledge Finland という団体内に MyData の Working Group が立ち上がり、国際的なコミュニティ活動を推進した後、2018 年 10 月に正式にフィンランドに設立され、2020 年現在で 20 以上のローカルハブ（地域ごとに MyData を推進するコミュニティ）が存在し、40 カ国以上から 600 以上の法人・個人会員がいる。

MyData を実現するためのエコシステムには図 16 のような各アクターの役割が存在する。

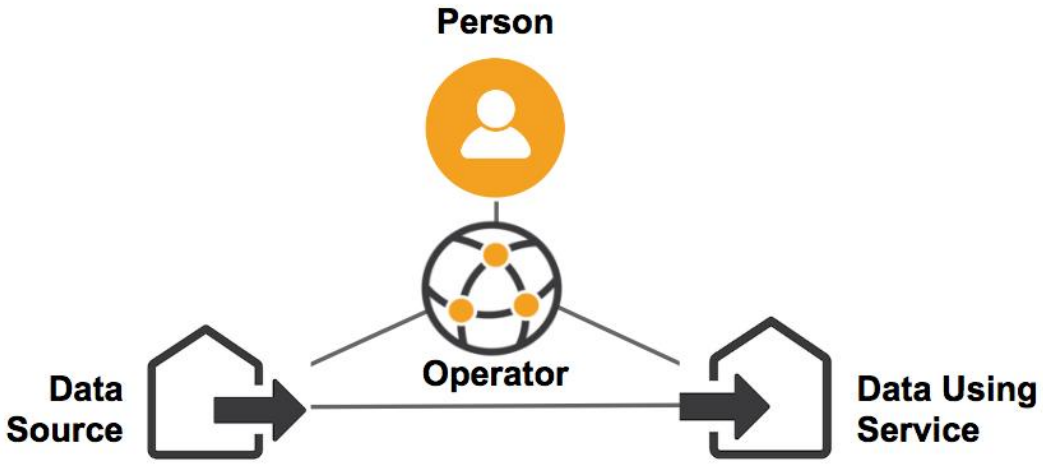


図 16　MyData エコシステムにおける各アクターの役割[30]

・Person（データ主体である個人）：自身に関する個人データの利用を管理し、自身の目的のために管理し、他の個人、サービス又は組織との関係を維持する。
・Data Source（データソース）：他の役割（個人を含む）がアクセスして利用する可能性のあるパーソナルデータの収集・処理を担う。
・Data Using Service（データ利用サービス）：1 つまたは複数のデータソースからパーソナルデータを取得して利用する権限を付与される役割を担う。
・Operator（オペレータ）： 個人が個人のデータに安全にアクセスし、管理し、使用することを可能にし、データソースとの間及びサービスを使用するデータとの間の個人データの流れを制御することを可能にする。個人は自分自身でオペレータを担うことができる。その他のケースとして、オペレータは情報そのものを利用するのではなく、他者との接続や、エコシステム内の他の役割間でのデータの安全な共有を可能にする。

この Operator には様々な形式と名前があり、日本独自の情報銀行もこの Operator の一つとして挙げられており、他にも PDS (Personal Data Store/Space)、Personal Information Management Services (PIMS)、Information Fiduciaries 等が挙げられている。実際のこれらのサービスの実例を図 17 に示す。

30 参照：https://mydata.org/declaration/

図 17　MyData Operator のサービス例[31]

3.2.4.2　MyData Operator の類型化

図 17 をサービスの特徴で類型化すると次のようなものが挙げられる。

Consent Manager（同意マネージャー）

主にデータストレージではなく、同意機能に重点を置いている。つまり、この Operator は主に、どのデータが 2 者間で共有されているか、どのくらいの期間共有されているかなどを調整する機能を提供する。また、データ交換する機能も提供するが、Operator は実データを保存や処理しない。デジタルマーケティング分野では CMP（Consent Management Platform）とも呼ばれているサービスも該当する。

例：Privacy Policy Manager（日・KDDI 総研）、PranetCross（日・Planetway）、Consentua（英・KnowNow Information Ltd）、iGrant.io（瑞）

Vaults（データストア）

同意マネージャーとは異なり、個人のデータを保管する。これは、ユーザーが実際に保存しているデータを Operator 自身が「知っている」という意味である必要はない。Operator がデータ交換をする機能を提供するものもある。

31　参照：https://mydata.org/wp-content/uploads/sites/5/2019/09/Discussion-paper-MyData-operator-final.pdf

例：Mydex（英）、Digi.me（英）、Solid（米・Inrupt）、Cozy Cloud（仏）

ID manager（アイデンティティマネージャー）

ユーザー自身の属性情報の共有とデジタル世界での署名に重点を置いている。サービスに必要な属性のみを共有することができ、余分な情報は含まれない。例えば、ユーザーは自分が成人であることを証明するだけで、生年月日を共有する必要はない。eKYC（electronic Know Your Customer）サービスも該当する。

例：Civic Wallet（米・Civic Technologies）、uPort（米・ConsenSys）

3.2.4.3 MyData Operator のアーキテクチャの機能コンポーネント

図 18 は、いくつかのコア要素の相互関係をまとめたもので、この構成要素は既存の MyData Operator のソリューション（例：Mydex や digi.me 等）から抽出したものである。Operator は、全ての機能を提供しなければならないということではなく、類型によって必要な機能は変わってくる。

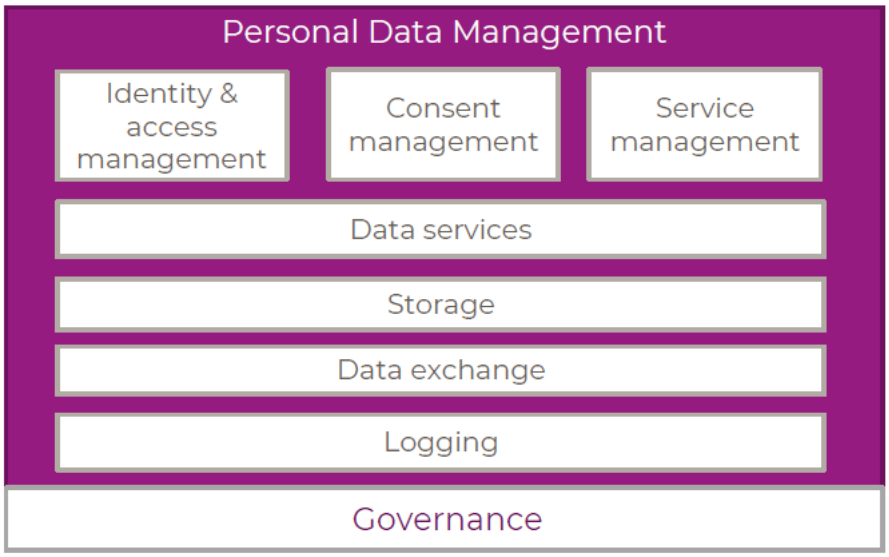


Figure 4. Personal Data Management model – top level.

図 18　MyData Operator の Reference Architecture[32]

MyData Operator には、次のような機能コンポーネントが重要とされている。

Consent management（同意管理）

データソースとデータ利用者間で特定の個人データを共有するための明示的な同意を管理する。同意契約の概要、及び明示的な同意を得て提供されたアクセス許可を取り消

32 参照：https://mydata.org/wp-content/uploads/sites/5/2019/09/Discussion-paper-MyData-operator-final.pdf

して適用する機能が含まれる。

Data services（データサービス）：

Operator は、データのフィルタリング、匿名化、分析、集約、または 1 つのメタモデルから別のメタモデルへのデータ変換により、データに価値を付加できる。データの使用に対する請求も含まれる場合がある。

Identity & access management（ID とアクセス管理）：

Authentication（認証）と Authorization（認可）から構成される。

Service management（サービス管理）：

データソースとデータ利用者を結合する。データは様々なソースで利用でき、複数のデータ利用者が使用できる。さらに、さまざまな方法で交換できます。エコシステムに複数の Operator が存在する環境では、Operator が共有サービスレジストリを使用するか、各 Operator がサービスを個別に管理するかを決定することが重要である。

Data exchange（データ交換）：

標準化された安全な方法で、データソース、データ利用者、及びオペレータ間のデータ交換を可能にするインタフェース。これには、構造化データ、自動化トランザクションのサポート、PDF などの非構造化データなど、様々な形式がある。情報はローデータでも属性データであってもよい。データソースとデータ利用者との間でエンドツーエンドでの暗号化での処理や、Operator による処理でもよい。

Logging（ロギング）：

行われるすべての情報交換を追跡し、誰が何にいつアクセスしたかを明確にする。

Storage（ストレージ）：

個人データをキャッシュ、分析、再利用等を行うために保存する。再利用や分析のためではなく、交換のためにデータを一時的に保存する場合、GDPR の下ではデータ処理者とみなされるかもしれないが、これを保管とはみなさない。

Governance（ガバナンス）：

ビジネスモデルの管理と透明性を含む、エコシステムの使用と開発、及び基礎となる原則を管理する。

Information Security & transparency（情報セキュリティと透明性）：

エコシステムと個人データの管理に関与するアクターへのアクセスと情報を提供する。

Value exchange（価値交換）：

サービスに対する支払いをサポートし、データ共有から発生する価値を分配する。

表 16 に事業概要をまとめる。

表 16　My Data Operator の事業概要

概要		
事業への認定制度と関連法規	なし	“MyData の原則に関する宣言(DECLARATION OF MYDATA PRINCIPLES)”に賛同し、活動することになっている
主な事業者と提供サービス	Personium	富士通（日）
	midata	イギリス連邦政府 BIS 省ほか（英）
	MesInfos など	Fing（Foundation Internet Nouvelle Generation）（仏）
パーソナルデータの扱い	有	
データライフサイクル	データソースとの間及びサービスを使用するデータとの間の個人データの流れを制御することを可能にする機能が提供されており、個人が主体となって制御できる	
データ提供者の権利	データ主体である個人が、自身に関する個人データの利用を管理	

3.3　産業データを主として流通させる事業でパーソナルデータを扱う事業

生産性向上特別措置法（平成 30 年 6 月 6 日施行）[33]において、IoT の進展により流通量が爆発的に増えているデータについて、産業における競争力強化や社会課題解決に向けた利活用を促進するため、協調領域におけるデータの収集・活用等を行う民間事業者の取組を、セキュリティ確保等を要件として主務大臣が認定する「産業データ共有事業の認定制度」が創設された（図 19）。産業データ共有事業者とは、この制度において「革新的データ産業活用の計画」と「データの安全管理基準への適合」が認定された業者である。

令和 2 年 2 月現在、株式会社シップデータセンター（ShipDC）が認定されている。株式会社シップデータセンター（ShipDC）では、船舶の運航データを、データ提供者の利益を損なわずに、ステークホルダ間での共有や、造船所やメーカ等への利用権販売、各種サービスへの提供を可能とすべく、海事業界内で合意されたルールとデータセンターで構成された共通基盤である「IoS-OP」を提供している（表 17）。

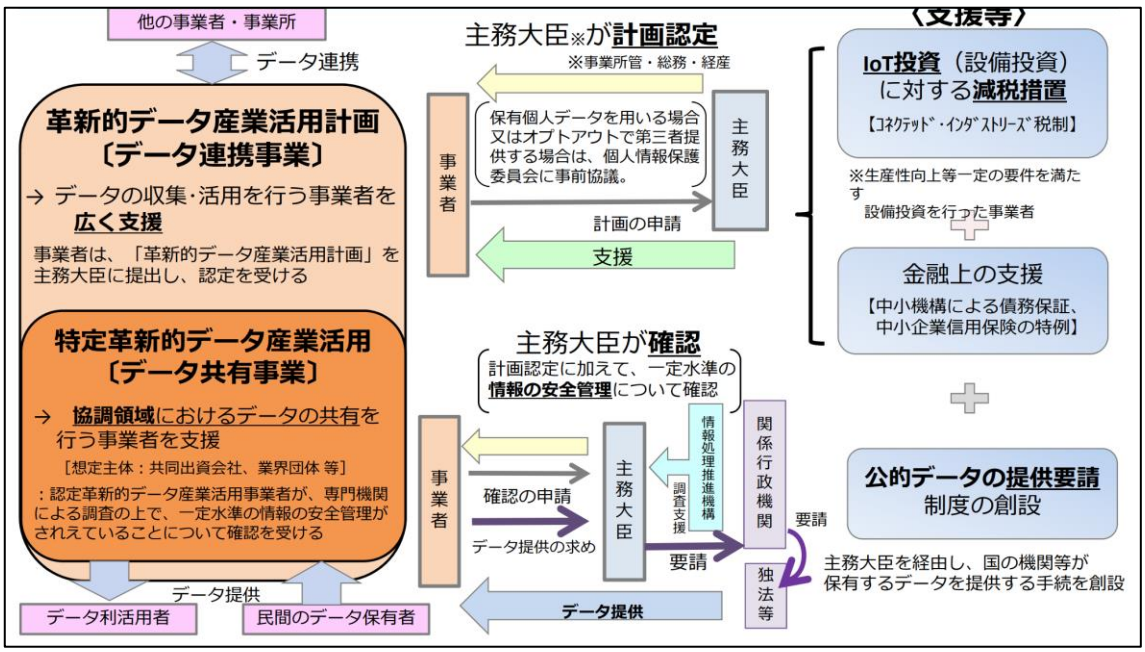


図 19　産業データ共有事業の認定スキーム

[33] 参考：https://www.meti.go.jp/press/2018/06/20180606001/20180606001.html

表 17　産業データ共有事業者の事業概要

概要		
事業への認定制度と関連法規	産業データ共有事業の認定制度	生産性向上特別措置法
主な事業者と提供サービス	株式会社シップデータセンター（ShipDC）	IoS-OP （ Internet of Ships Open Platform）
パーソナルデータの扱い	有	船上で収集されたデータに含まれる可能性
データライフサイクル	IoS-OP 利用規約に従い、船上で発生する様々なデータに対し、データ保管、取り出し方法をプログラムレスで対応可能とする仕組みを提供	
データ提供者の権利	データ提供者（プラットフォームユーザ、PU）がデータ利用権を制御	

3.4　公共分野でパーソナルデータを扱う事業

公共分野でのデータ流通の取り組みについて取り上げる。地方公共団体が保有するパーソナルデータの活用の検討[34]も進んでいる。地方公共団体が保有する「非識別加工情報」を介護や教育などに活用する事例が想定されており、データの作成にあたっては、地方公共団体とは別に国の認定を受けた作成組織が作成、管理を行うイメージが提示されている（図 20）。この作成組織は、地方公共団体に代わって、民間事業者への当該データの提供も実施する事業体[35]となる（図 21）。ただし、企業が非識別加工情報を利用するためには、各行政機関が Web 等に公示する募集要項に沿って、提案書を提出し、行政機関側で審査・見積もりを経て、契約するフローに従って手続きが必要となっている（図 22）。市区町村には、複数人の個人データを分類ごとに集計して得られる統計データ（オープンデータ）とは異なる、家族構成、所得情報、医療・介護及び福祉サービスの受給状況、乳幼児健診やがん検診の結果など、多種多様な個人情報がある。個人のデータをベースとした非識別加工情報から商圏分析など企業内での事業判断に用いるなど、官民での連携したデータ活用が期待されている。

これに先立ち、国の行政機関や独立行政法人等における非識別加工情報の提供は、平成

---

[34] 総務省、平成 30 年 4 月、「地方公共団体が保有するパーソナルデータの効果的な活用のための仕組みの在り方に関する検討会　報告書」

[35] 作成組織の具体的なニーズ、データのやり取りに対するコスト、事業の採算性が不明確な部分について、「地方公共団体の非識別加工情報の作成・提供に係る効率的な仕組みの在り方に関する検討会」で取りまとめられた。

28 年の行政機関個人情報保護法等の改正を受けて、仕組みを導入済みである。平成 30 年度は、20 行政機関及び 130 独立行政法人等において、提案募集が実施され、複数の提案書が提出されている。（提案の募集対象となった個人情報ファイル数：行政機関 286 ファイル、独立行政法人等 1,733 ファイル）

表 18 に事業概要をまとめた。

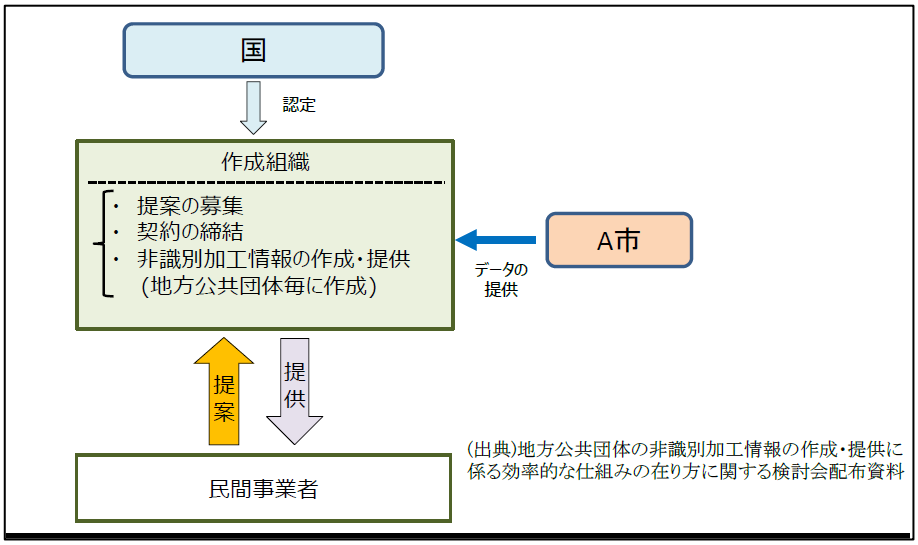


図 20　非識別加工情報の作成組織のイメージ

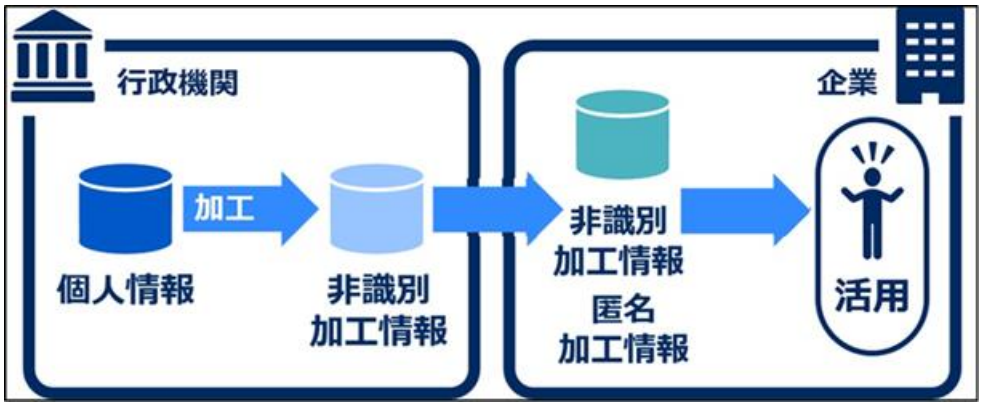


図 21　非識別加工情報の活用イメージ[36]

[36] 出典　日本電気株式会社　Web サイトコラム「ご存知ですか？ 企業が使える住民データ　～非識別加工情報～」を DTA の判断で一部修正

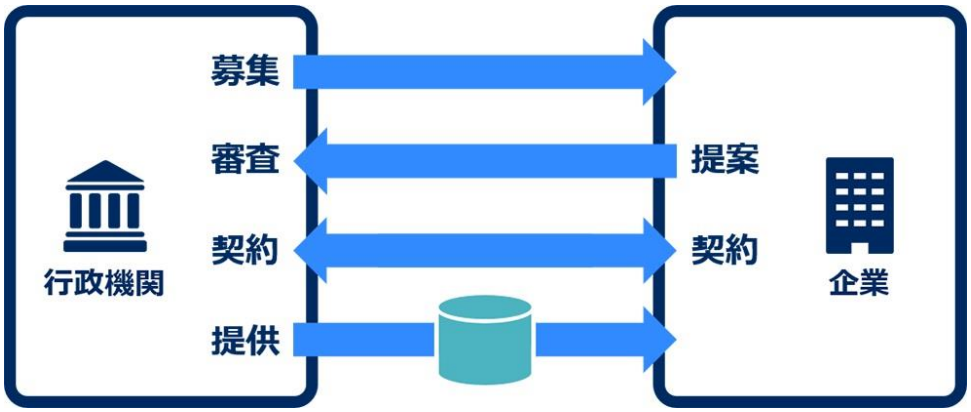


図 22　利用にあたってのフロー[37]

表 18　行政機関等非識別加工情報の事業概要

概要		
事業への認定制度と関連法規	行政機関非識別加工情報制度 独立行政法人等非識別加工情報制度	改正個人情報保護法、改正行政機関個人情報保護法及び改正独立行政法人等個人情報保護法
主な事業者と提供サービス	国の行政機関や独立法人	
パーソナルデータの扱い	有	省庁が作成するものを行政機関非識別加工情報、国立研究開発法人といった独立行政法人等が作成するものを独立行政法人等非識別加工情報
データライフサイクル	法制度のほか、非識別加工情報の提供に関する契約と個人情報の保護に関する法律についてのガイドラインに従った運用	
データ提供者の権利	非識別加工情報に関する事項を個人情報ファイル簿に記載し、当該個人情報ファイル簿を「電子政府の 総合窓口」（e-Gov）ホームページで公表[38]することが行政機関個人情報保護法で規定されている（44 条）	

[37] 出典　日本電気株式会社　Web サイトコラム「ご存知ですか？ 企業が使える住民データ　～非識別加工情報～」

[38] 行政機関等非識別加工情報（個人情報保護委員会にリンク）
https://www.ppc.go.jp/personalinfo/HishikibetsukakouInfo/

総務省の情報通信白書[39]において、公共分野として、医療・ヘルスケア、教育、交通、防犯、防災・減災があげられている。

例えば、交通分野では首都圏において、公共交通オープンデータ協議会が公共交通オープンデータセンター[40]を通じて、鉄道・バス・航空事業者・施設などの公共データを利用したい開発者向けにデータ提供するスキームを構築している。「過度に自動車に頼る状態」から、「公共交通や徒歩などを含めた多様な交通手段を適度に（＝かしこく）利用する状態」への転換のため、国土交通省をはじめとした行政機関では、モビリティ・マネジメント施策（環境や健康などに配慮した交通行動を、大規模、かつ、個別的に呼びかけていくコミュニケーション施策）の中では、実態把握から行動改善に至るまでデータをもとにしたデータドリブンな施策がとられている例が数多くあり、今後もデータ利活用による事業推進は継続するものと予想される。

---

[39] 総務省、平成 28 年版情報通信白書、第 1 部第 3 章第 3 節 公共分野における先端的 ICT 利活用事例

[40] 「公共交通オープンデータセンターとは」https://www.odpt.org/overview/

第4章　パーソナルデータを扱う上で必要な ELSI

パーソナルデータは、個人のプライバシーや倫理に配慮した扱いが重要であることから、本書の作成と併行して有識者によるパーソナルデータ分野に関する ELSI（Ethical, Legal and Social Issues）検討会を設置した。本章では、この検討会が取りまとめた、別冊の「パーソナルデータ分野に関する ELSI 検討会報告書」の概要を簡潔に解説する。

パーソナルデータの利活用は、ユーザーや消費者にとっても大きなメリットをもたらす一方で、事業者によるデータの収集・利用について個人が把握できているわけではないため、プライバシーを含めた人権に対する配慮について、海外を中心に問題提起されている。そのため、パーソナルデータ分野に関係する事業者は、国内における法令遵守はもちろんのこと、海外での事業展開やインバウンドの拡大も視野に入れたグローバルな視点をもち、国内に留まらず海外における「規範」や、消費者の目線から法令に留まらず様々な「規範」へも目配りする必要ある。そこで、本章は、本書の作成と併行する形で有識者や実務者の助言や意見を反映させるべく設置されたパーソナルデータ分野に関する ELSI 検討会と、その検討会における議論を踏まえてまとめられた報告書の概要について解説する。

4.1　ELSI 検討会の位置づけ及びアプローチの方法

4.1.1　ELSI 検討会の位置づけ

ELSI 検討会においては、パーソナルデータを扱う、またはこれから扱う予定の事業者が、自己のビジネスモデルやサービス設計を行う際に、どのような「規範」に目配りすべきかの調査・整理を行った。ELSI 検討会で行われた検討は、Society5.0 リファレンスアーキテクチャ（本書 1.4.4）のうち、主として「戦略・政策」、「ルール」、「組織」の部分である。すなわち、①「規範」の調査の過程で明らかになった「規範の不在」からは、今後の企業に期待されるべきアクションが明らかになり、②またパーソナルデータ分野における「規範」の整理・検討が行われることで、事業者の目線によるシステム全体の「俯瞰（overview）」を可能となっている。③そして、「規範」の調査・整理の際の軸として「事業に関係する規範の形成主体」が置かれている。

これら ELSI 検討会における「規範」の調査と整理は図 23 が示すように、「戦略的イノベーション創造プログラム（SIP）第 2 期／ビッグデータ・AI を活用したサイバー空間基盤技術／パーソナルデータ実証研究」として採択されている医療版情報銀行、顔認証、そして人物行動データという異なるタイプのパーソナルデータを扱うテーマとそれぞれ論点を共有し、全体の整合性が図られている。

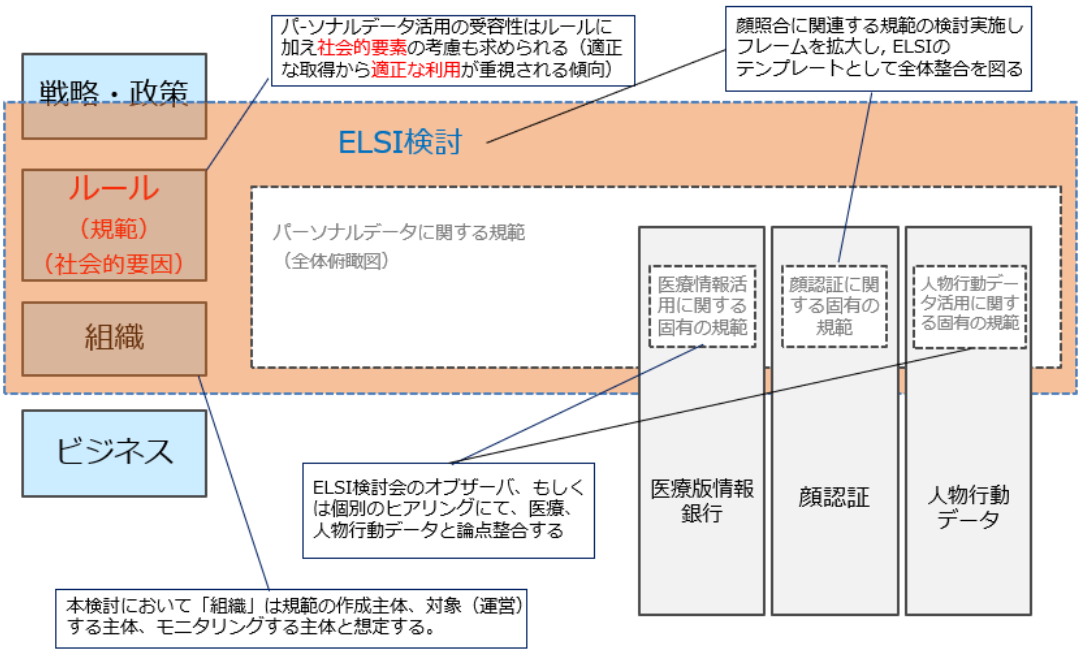


図 23　ELSI 検討会における規範調査の実施方法

4.1.2　ELSI 検討会におけるアプローチ方法

ELSI 検討会は、以上のようにパーソナルデータ分野に関係する事業者の主体性を重視し、どのような「規範」に目配りをしていく必要があるか（その上で、欠けている「規範」は何か）を探り出していくことを目的としている。そうした目的を達成するために、ELSI 検討会では、国や地域社会、更には業界団体などにおいて形成されている重層的な「規範」のシステム全体を、事業者が「俯瞰」できるように規範の調査と整理を行っている。特に、目的に鑑みると、消費者やユーザーと事業者が信頼関係を構築するために必要性の高いものに焦点を絞り、さらに我が国の統合イノベーション戦略推進会議が策定した「人間中心の AI 社会原則」に則り「人間中心」という価値を共有しうるアメリカとヨーロッパの二地域に重点を絞り調査を進めることが妥当と考えられた。

この点、「規範」の中には、公的機関が形成する法律や条例といったものに加えて、業界団体や企業といった私的団体が定めるガイドライン等、様々な形式のものが混在している。これらは、それぞれ事業者に対して影響力を有するものの、その規範の執行性（規範に違反した場合にどのような対抗措置がとれるか）等については大きな差異がある。そのため、整理の際に、当該規範がどのようなカテゴリに属するかを整理・分類している。そこでは、Ⅰ国際原則（政府系/国際団体）、Ⅱ国内・地域の法令・条例、Ⅲ政府系ガイドライン、Ⅳ団体ガイドライン、Ⅴ企業ポリシー、Ⅵ国内勉強会・研究会に基づく報告書というカテゴリが設けられている。

加えて、海外における事業展開や、インバウンド拡大における外国人旅行者への対応を

考えた場合、国内における「規範」に目配りをするだけでは不十分であり、海外における「規範」の動向にも目配りすることが必要不可欠であり、事業者が事業展開を行う地域についても考慮されている。

また新技術の発展に対して、国や自治体が規範形成を行う前に、業界団体などが先導して規範を形成することも十分考えられることであり、そこから、事業者自身がより主体的に規範形成に参加していくことも鑑みると、誰が規範形成主体となっているのかを把握できるように整理されている。

さらに、「規範」以外にも、過去にパーソナルデータ分野に関して、どのような問題が消費者団体や人権団体などユーザー側から指摘されたかを参照するため、これに関係する国内外で問題となった事案にも目配りする必要があることから、代表的な事案が整理されている。

4.2　パーソナルデータ分野に関連する「規範」の層

ELSI 検討会における以上のようなアプローチ方法に基づく調査と整理により、パーソナルデータ分野に関連する「規範」の層は次のように形成されていることが分かった（表19）。

表 19　パーソナルデータ分野に関連する「規範」層

事業に関係する規範カテゴリ	名称	規範形成主体
国際原則（国際団体）	倫理的に配慮されたデザイン（第 2 版）	IEEE
	ヘルシンキ宣言	世界医師会（WMA）
国際原則（政府系）	国連ビジネスと人権に関する指導原則	国連
	AI に関する理事会勧告	OECD
	Data Free Flow with Trust	G20
	信頼のおける AI のための倫理ガイドライン	EU
国内・地域の法令・条例	憲法 13 条　プライバシー権（情報自己決定権、肖像権）	日本
	消費者基本法	日本
	消費者安全法	日本
	個人情報保護法	日本
	次世代医療基盤法（及び同法施行規則、基本方針等）	日本
	医療法、及び医療・介護関係事業者における個人情報の適切な取扱いのためのｶﾞｲﾀﾞﾝｽ等	日本

	臨床研究法（及び医学研究関連法令ガイドライン）	日本
	医薬品医療機器法及び GCP 省令等関連規範	日本
	電気通信事業法	日本
	強制処分（刑事訴訟法 197 条 1 項ただし書）	日本
	令状主義（憲法 35 条）	日本
	捜査関係事項照会（刑事訴訟法 197 条 2 項）	日本
	個人情報保護条例	各自治体
	防犯カメラ条例	各自治体
	FTC 法 5 条	アメリカ
	児童オンラインプライバシー保護法（COPPA）	アメリカ
	第三者法理（アメリカ合衆国憲法修正 4 条より派生）	アメリカ
	HIPAA(Health Insurance Portability and Accountability Act of 1996;医療保険の携行性と責任に関する法律)	アメリカ
	一般データ保護規則（GDPR）	EU
	EU 警察指令	EU
	e-Privacy 規則案	EU
	カリフォルニア消費者プライバシー法	カリフォルニア州
	ワシントン州生体識別子法	ワシントン州
	イリノイ州生体情報プライバシー法（BIPA）	イリノイ州
	サンフランシスコ市当局による顔認識技術の使用を禁止する条例	サンフランシスコ市
	防犯カメラに係る補助制度	各自治体
政府系ガイドライン	Facing Facts	FTC
	FIPPs（Fair Information Practice Principles）	FTC 等
	プライバシー・バイ・デザイン（PbD）	FTC 等
	Privacy Framework: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT	NIST

	データ保護影響評価（DPIA）及び取扱いが EU 規則 2016/679 の目的に照らして「高度のリスクをもたらす可能性」があるか否かの判断に関するガイドライン	EU
	ビデオ機器を通じた個人データの処理に関するガイドライン（最終版）	EU
	人間中心のＡＩ社会原則	内閣府
	AI 利活用原則案／AI 利活用ガイドライン案	総務省
	国際的な議論のための AI 開発ガイドライン案	総務省
	位置情報プライバシーレポート	総務省
	電気通信事業における個人情報保護に関するガイドライン	総務省
	スマートフォンプライバシーイニシアティブ	総務省
	顔認証技術を活用した One ID サービスにおける個人データの取扱いに関するガイドブック（案）	国土交通省
	無人航空機（ドローン、ラジコン機等）の安全な飛行のためのガイドライン	国土交通省
	個人情報の保護に関する法律についてのガイドライン（通則編）	個人情報保護委員会
	３省３ガイドライン	厚生労働省・総務省・経済産業省
	カメラ画像利活用ガイドブック	IoT 推進コンソーシアム
	カメラ画像利活用ガイドブックの事前告知・通知に関する参考事例集	IoT 推進コンソーシアム
団体ガイドライン	プライバシーフレームワーク	米国公認会計士協会
	企業行動憲章	経団連
	経団連サイバーセキュリティ経営宣言	経団連
	個人データ適正利用経営宣言	経団連

	JIS Q 15001:2017　個人情報保護マネジメントシステム要求事項	日本情報経済社会推進協会
	個人情報保護指針	認定個人情報団体
企業ポリシー	Artificial Intelligence at Google Our Principles	Google
	NEC グループ AI と人権に関するポリシー	NEC
	パーソナルデータ憲章	NTT ドコモ
	プライバシーポリシー	ヤフー
	顔認識テクノロジに関する当社の見解について	マイクロソフト
	人工知能（AI）に関する行動規範	SAP
	特設 Web サイト「プライバシー」	Apple
	IBM 顔認証ポリシー	IBM
国内勉強会・研究会	HRbD に基づくチェックリスト	NEC＆KGRI
	プロファイリングに関する提言案	パーソナルデータ＋α研究会
	大阪ステーションシティ ICT 大規模実験に関するレポート	映像センサ使用大規模実証実験検討委員会

4.3　パーソナルデータ分野に関連して問題となった事案

ELSI 検討会における以上のようなアプローチ方法に基づく調査により、パーソナルデータ分野に関連する問題となった事案は次のように整理できる（表 20）。

表 20　パーソナルデータ分野に関連する問題となった事案

どのような問題か	事例	地域・対象
反対運動	大阪ステーションシティ人流分析	日本
反対運動	Amazon「Rekognition」	アメリカ
反対運動	再犯予測アルゴリズム	アメリカ
反対運動	企業採用アルゴリズム	アメリカ
報道	万引き犯検知システム	フォーチュン誌
報道	リクナビ問題	日本経済新聞
報道	PROJECT EXOGRAPH 問題	ダイヤモンドオンライン
報道	難民データベース	WIRED
報道	GooglePhotos の誤認識	Guardian
報道	パレスチナ人の監視技術	JapanCnet
報道	ウイグル族の監視技術	東京新聞

訴訟及び報告書	事例	地域・対象
訴訟	BIPA に基づく Facebook ユーザーによる集団訴訟	アメリカ
訴訟	BIPA に基づくユナイテッド航空に対する訴訟	アメリカ
訴訟	あいりん地区防犯カメラ訴訟	日本
訴訟	Google ストリートビュー訴訟	日本
訴訟	R v The Chief Constable of South Wales Police	イギリス
報告	Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products	MIT Media Lab
報告	America Under Watch: Face Surveillance in the United States	Georgetown LAW Center

		on Privacy & Technology
報告	Biometrics in the Humanitarian Sector 2018.3	The Engine Room & Oxfam
報告	ニューヨーク州ロックポート市学区における学校向け顔認識技術の導入に反対する書簡	NYCLU
報告	Artificial Intelligence: A Rights-Based Blueprint for Business	BSR
報告	税関国境取締局（CBP)の生体データ収集出国プログラムに対する懸念を表明する書簡	電子フロンティア財団

4.4　パーソナルデータ分野に関連する事業者に求められる視点

4.4.1　事業者に求められる視点

以上のような調査と整理から、ELSI 検討会の報告書はいくつかの知見を提示している。まず、我が国がダボス会議を通じて提唱した「DFFT（信頼のおけるデータ流通)」を鑑みても、事業展開における「信頼」確保は必要不可欠な条件となりつつあることがわかる。そのうえで、本章第三節でも取り上げられた Amazon の「Rekognition」システムの公的機関への導入や、NICT（情報通信研究機構）による「大阪ステーションシティ」における反対運動などからは、差別やプライバシーに対する懸念が主な理由となって、パーソナルデータ分野に関連する事業者に対する消費者の信頼関係を揺さぶっていることがわかる。

報告書がまとめた規範の一覧（本章第二節）からは、我が国における個人情報保護法はもちろん重要ではあるものの、全体から見ればほんの一部を占めているにすぎないことがわかり、特に EU における GDPR（一般データ保護規則）や、アメリカのカリフォルニア州における CCPA（カリフォルニア州消費者プライバシー保護法）の成立は、パーソナルデータ分野に関する共通感覚がグローバルに展開・形成されつつあることを示唆するものと言える。ここから、各事業者もまた、国際コンセンサスを取りつつ、国際標準化を図っていくことを視野に入れ、日本国内法令に対する「閉じた」目線だけでなく、海外の規範動向に対しても視線を移す必要があることがわかる。また主要な国際原則では、基本的権利に対する配慮や透明性・説明責任、さらには公平性といった事項が取り上げられ、一種の「デフォルト」を形成しつつある。これらは、各種法令や、企業におけるポリシーなどにも取り込まれつつあることから、こうした影響力のある「デフォルト」を事業者が率先して目配りし、事前に対応しておくことが大きなメリットとなる。またその点でいえば、我が国の消費者基本法とそれにも基づく消費者基本計画の施策内容は、消費者をパーソナルデータ分野に関する主役と見る観点からは非常に示唆的である。

「規範」の層と過去に問題となった事案から浮き彫りになるのは、地域や少数民族、宗教などにおけるサービスの受容性についての違いである。例えば、アメリカとヨーロッパ

では、法制度の違い（FTC 法と GDPR）を見れば明らかなように、自由を重視するか尊厳を重視するかという社会における基底的価値観に若干の違いが見受けられ、アメリカについては州によってもそうした価値観に違いが見られる（e.g. CCPA）。ここから事業者は事業展開をどのような価値観を有した地域で行うかを常に配慮しておく必要がある。さらに、迫害を受ける可能性の高い少数民族や宗教は、パーソナルデータ技術によって「監視」される懸念が常に付きまとうことも考慮に入れ、事業者は自社の技術の B to B やエンドユーザーにまで視野を広げておく必要がある。

この他にも、規範相互のインターオペラビリティの不足が指摘されている他、アメリカの児童オンラインプライバシー保護法（Children's Online Privacy Protection Act: COPPA）が示すように、児童や高齢者、さらに障害を有している人々といった脆弱な主体に対する配慮や、CCPA が示すように、消費者に対して事業者が優越的な立場にあることを利用してデータを提供させてしまうような構造に対する注意といった、インクルージョンの視点もまた事業者にとって重要性を増していると考えられる。

4.4.2　適正な事業開発に際しての基本要件

以上のように、パーソナルデータ分野でサービスの展開を行っていく（または行う予定の）事業者に求められる視点を踏まえるならば、適正な事業開発を行い、ユーザーや消費者との間に信頼関係を構築していくうえで必要となる基本要件というべきものが浮かび上がってくる。この点、すでに、我が国の政府によって「人間中心の AI 社会原則」が策定されているが、ここでいう「人間中心」が具体的には何を事業者に求めているのか、ビジネスサイドが何をすればよいのかが具体化されていない。そこで、ELSI 検討会で調査が行われた「規範」の層や問題となった事案を踏まえ、ELSI 検討会の報告書では、以下で示すような６つの「パーソナルデータを活用した適正な事業開発の基本要件」が具体的に示されている。

4.4.2.1　グローバルな目線の必要性

- 事業者は、パーソナルデータ分野の事業開発にあたって、たとえ日本国内に限定して事業を行う場合であっても、日本国内のみに目を向けるのではなく、常に諸外国の「規範」にも備えておく必要がある（e.g. GDPR の域外適用の可能性）。
- 特に昨今のインバウンド拡大により、大勢の外国人旅行者が訪れることを想定すれば、単に日本国内の所管法令を遵守するだけでは事足りない可能性がある。
- 事業者もまた、国際社会の構成員であり、人権尊重の役割を担うために、国際的な常に国際的動向に目配りを行う必要があるのではないだろうか（e.g. 国連**ビジネスと人権に関する指導原則**）

4.4.2.2　責任あるビジネス、バリューチェーンの推進

- 事業者は、データの流通におけるサプライチェーン（「責任ある調達」）を行うための

取り組みを推進することが必要となる（パーソナルデータの調達・提供）。

・事業者は、自社のパーソナルデータを収集する技術が、販売先や取引先においてどのように扱われるのかを注視し、末端のユーザー・消費者の「信頼」の確保に向けて行動を行う必要があるのではないか。

4.4.2.3　消費者（個人）を主役に据えた事業全体のデザイン

・事業者は、単に技術的な視点だけではなく、事業全体のデザインとして、消費者が主体的に選択を行うことのできる事業設計を行う必要がある。

・例えば、いわゆる情報自己決定権の実装を目指した事業設計などがそれにあたる（e.g. 情報自己決定権、PbD（Privacy by Design）、GDPR）。またその一環として、データ・ポータビリティの実現が考えられる（e.g. GDPR、CCPA(California Consumer Privacy Act)）。

・なお技術的な点に目を向ければ、ユーザー・インターフェース・デザインのコンセプトとして注目すべきものに、Ethical Design がある[41]。また「ユーザーの積極的な関与及び、ユーザー並びにタスク要求の明確な理解」と定義される「人間中心デザイン（Human-Centered Design, HCD）」という概念も注目されている[42]。

4.4.2.4　消費者目線を踏まえた通知及び同意

・通知及び同意については、各国の法制度や原則の中でも大前提なものとなりつつある（e.g.個人情報保護法）。この点、事業者は、通知及び同意について、ユーザーや消費者の目線に立ち、過度な形式主義に陥るのではなく、システム的要件やアジェンダとして仕様書に書き込むといった方向で実質化を図っていく必要がある（e.g. GDPR における「同意の条件」）。

・さらに「受容性・インクルージョン」の視点から、児童や高齢者といった「脆弱な主体」に対する通知及び同意については、保護者の関与に配慮する必要がある（e.g. GDPR、COPPA（Children's Online Privacy Protection Act）、消費者安全法）

・例えば、事業者は、消費者（個人）のコントローラビリティの実質化として、情報審

---

[41] これは、デザインの実践における、道徳的行為及び責任ある選択に関係するものであり、デザイナーが、製品のクライアント・同僚・エンドユーザーらとの連携方法、設計プロセスの実施方法、製品の機能、設計段階における製品の倫理的・道徳的意義の検討といったものをガイドするものである。その際に、デザイナーは、①利便性、②アクセシビリティ、③プライバシー、④ユーザー関与、⑤説得、⑥焦点、⑦持続可能性、⑧社会といった点について注目すべきとされる。*See,* at https://alistapart.com/article/daily-ethical-design/

[42] *See,* at https://www.smashingmagazine.com/2018/03/ethical-design-practical-getting-started-guide/ ;*See also,* at https://vimeo.com/300109442

査機能などを積極的に取り入れていく必要がある。その際に、契約の要素に着目し、モデル契約書を参照軸として自社の標準化を行う必要がある（e.g. AI データ契約ガイドラインの契約書ひな形、情報信託機能の認定に係る指針）

4.4.2.5 フェアネス

・事業者は、パーソナルデータの分析・活用による差別的な結果がでてくることを常に意識し、ユーザー・消費者が差別を受けないよう配慮する必要がある（e.g. 倫理的に配慮されたデザイン、信頼のおける AI のための倫理ガイドライン）。

4.4.2.6 透明性と説明責任

・例えば、事業者は、目的の明確化は当然のこと、ガバメントアクセスなどに対し、どのように対応していくのかについてのポリシーを形成しておく必要がある（e.g. 捜査関係事項照会）。

・事業者は、ユーザー・消費者と継続的にコミュニケーションを行う仕組みをサービス設計に組み込んでいく必要がある（e.g. 倫理的に配慮されたデザイン、信頼のおける AI のための倫理ガイドライン）。

第5章　パーソナルデータと関連法制

パーソナルデータの取扱いでは、個人情報保護法はもちろんのこと、その取り扱う事業によっては、各種業法に対する遵法性も重要となる上、国を超えたデータの取扱いなどでは、各国や地域の法制に照らして自らの事業内容との整合性に留意する必要がある。

そこで、本書の作成において参照とするために、情報法制を専門とする弁護士が実施した「パーソナルデータ分野のアーキテクチャ構築における情報法制の調査」の概要を簡潔に解説する。

5.1　情報法制の全体像

情報法制はどのように適用されるかについては、アーキテクチャとの関係では行政規制と民事法関係（契約関係）に分類することが適当である。「消費者委員会消費者法分野におけるルール形成の在り方等検討ワーキンググループ」は、その報告書において、消費者取引分野に関し、行政規制と民事ルールの関係を適切に整理している[43]。

同報告書の考え方をパーソナルデータに当てはめた場合に、消費者取引分野とは幾つかの点で差異が存することに注意しなければならない。まず、行政規制の中心である個人情報保護制度自体が例を見ない縦割りであり、しかも、外部からの監視・監督を伴わない分野を内包しているということである。具体的には、民間分野に適用される個人情報保護法は、監視・監督機関として主として個人情報保護委員会が存在し、一般的な行政規制と同様であるが、公的部門（国の行政機関、独立行政法人等）及び地方公共団体については、行政機関個人情報保護法、独立行政法人等個人情報保護法及び、各地方公共団体の個人情報保護条例が存在するものの、外部からの監視・監督が存在しないため、適切に規律されているとすら言えない状態である[44]。もう一つは、民事ルールの根拠法がないことである。

---

[43] 消費者委員会消費者法分野におけるルール形成の在り方等検討ワーキング・グループ「消費者法分野におけるルール形成の在り方等検討ワーキング・グループ報告書～公正な市場を実現するためのルール及び担い手のベストミックスを目指して～」（令和元年6月）9-10頁。

[44] この点に関しては，内閣官房・個人情報保護制度の見直しに関するタスクフォース（国の行政機関及び独立行政法人等に関して）及び，個人情報保護委員会・地方公共団体の個人情報保護制度に関する懇談会（地方公共団体に関して）が議論を開始しているが，特に後者は，明らかに議論を停止させたいという意向を含んだ地方公共団体作成の資料が公表されており，重大な懸念がある。なお，外部からの適切な監視・監督が存在しないことから，欧州からの日本の十分性認定が民間分野の個人情報保護法に限定されている点については，Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the

いや正確にいえば、民法分野に属することは明らかであるが、民法上、パーソナルデータに関する規律を直接含む条項が存在しないことである。民法上のプライバシーや肖像権の保護は人格権や人格的利益に基づくとされており、裁判実務はそれがほぼ定着しているが[45]、民法の条文上の根拠は存在しないのである。勿論、パーソナルデータの取扱いの全部又は一部を委託するということであれば、それは一般的には業務委託契約（請負又は準委任であり、その内容は具体的な契約による）の範囲で理解できることになるが 、根拠となる権利利益の曖昧性は、パーソナルデータを巡る民事ルール、契約関係の理解をより困難なものとしている。

5.2 一般法令

5.2.1 個人情報保護法

パーソナルデータの取扱いについての最も基本的な法令は個人情報保護法である。取扱主体が民間事業者でない場合は別の法令が適用されることは既に述べた。この点を間違えた場合、当然ながら適用される規範は全て誤りということになるので、十分に注意されたい。

ここでは、民間事業者のみでスキームが組まれていることを前提として、個人情報保護法を用いたスキーム構築の要点のみを言語化してみる[46]。

まず、もっとも重要なのが、問題となる個人情報の保有者又は管理者を特定することである。これが、欧州一般データ保護規則（GDPR）等、一般的なデータ保護法であれば、管理者（Controller）と処理者（Processer）の義務を別々に定めており、「管理者」を中心に適用関係を考えるのが一般的であるが、日本の個人情報保護法は、GDPR でいう「管理者」と「処理者」をいずれも「個人情報取扱事業者」としており、分けていない。しかしながら、実際には委託先（個人情報保護法 23 条 5 項 1 号、22 条）と、委託元では義務に

Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Text with EEA relevance), C/2019/304/.

[45] 例えば，最判平成 29 年 10 月 23 日判時 2351 号 7 頁は比較的単純な個人情報の漏えいについて，「プライバシーに係る情報として法的保護の対象となる」とする。

[46] いわゆる有名企業であっても，個人情報保護法の適用関係を適切に判断できているわけではない。いわゆるリクナビ事案においては，リクルートキャリアに対する勧告の中で「法における適用関係等について適切な検討を行っておらず」とされ（個人情報保護委員会「個人情報の保護に関する法律第 42 条第 1 項の規定に基づく勧告等について」（令和元年 8 月 26 日），リクナビを利用していた企業に対する指導でも「個人データを外部に提供する際の法的検討ない当該法的整理に従った対応等が不適切であった。」とされている（個人情報保護委員会「個人情報の保護に関する法律に基づく行政上の対応について」（令和元年 12 月 4 日）。

は差がある。個人データの取扱いの委託が存在している場合に、利用目的の通知公表義務があるのは委託元であり、保有個人データの開示等の請求等について対応する義務があるのも委託元である。

複数のステークホルダが現れる場合、保有者から個人データの提供が行われるとすれば、その根拠は、大きく分けて①同意（個人情報保護法 23 条 1 項 1 号）か、②それ以外か、である。特に、個人データの取扱いの委託に伴う提供（個人情報保護法 23 条 5 項 1 号）が代表的である。同意に基づいて提供されたから、常に個人データの本人の権利利益の保護に適切であるかというと、必ずしもそうではない。日本の個人情報保護法では、個人情報の利用目的は、「できる限り特定」されてさえいれば、どのようなものでも定めることができる。そして、個人データが第三者提供される場合、第三者提供先は、提供元の利用目的とはまったく別個に、新たに利用目的を定めることができる。要するに、同意に基づいて第三者提供を行うというのは、本人の権利利益に配慮しているようであって、提供元がどのような事業者であるとか、提供元の利用目的であるとかを適切に示さなければ、本人がそのリスクを判断できないという構造になっているのである。保有者が委託先を適切に監督することを前提に、委託に伴う提供であると整理される方が、本人にとっては理解しやすいという場面が確実に存在する[47]。

他方、情報銀行（情報信託機能）については、同意に基づく第三者提供を基本とした制度であるものの、第三者提供先を拘束するような様々な仕掛けがなされている。もっとも、情報銀行（情報信託機能）の枠組みは、総務省及び経済産業省が「情報信託機能の認定に係る指針 ver2.0」を公表し、民間団体である日本 IT 団体連盟がこれを参考に、情報銀行の認定事業を行っているに過ぎず、何らかの強制力を伴うものではない。しかしながら、本人に対して適切な情報を与えた上で同意を取得しようとすれば、このような仕掛けが必要になるということである[48]。

5.2.2　契約法

パーソナルデータを巡る契約において、最も基本とすべきは、データには原則として何らの権利も付着しないということである。この点は、「AI・データの利用に関する契約ガイドライン」が端的に、「データは無体物であり、民法上、所有権や占有権、用益物権、担保物権の対象とはならないため、所有権や占有権の概念に基づいてデータに係る権利の有無を定めることはできない（民法 206 条、同法 85 条参照）。そして、知的財産権として

---

47 一般財団法人情報法制研究所 個人情報保護法研究タスクフォース「「顔認証技術を活用した One ID サービスにおける個人データの取扱いに関するガイドブック」に対する意見」（2020 年 2 月 4 日）。

48 経済産業省『AI・データの利用に関する契約ガイドライン 1.1 版』（令和元年 12 月）データ編 14 頁。

保護される場合や、不正競争防止法上の営業秘密として法的に保護される場合は、（省略）限定的であることから、データの保護は原則として利害関係者間の契約を通じて図られることになる。」と述べるとおりである。

ここでいう、「利害関係者間の契約」は、データの提供元と提供先などを指しているため、パーソナルデータの本人についての考慮は別途為されなければならない。個人情報保護法等の行政規制を遵守することはもちろん、プライバシー権を含む人格権又は人格的利益についても契約上の処理が（消費者契約法等の消費者法に抵触しないことを当然の前提として）なされることが望ましい。このような契約ないし契約書を、専門家抜きに作成することはほとんど不可能であり、上記AI・データガイドラインに付属するひな型は、極めて有益な参照文書である。また、前述した情報銀行の認定事業で提供されているひな型も、専門家の検討を経ているという点で有益な参照文書である。

パーソナルデータの取扱いの委託に関する契約や、その中での人格権又は人格的利益の処理などは、前述するように、民法の中でも、典型契約に直ちに当てはまるものでなく[49]、更に、条文のない分野を把握していなければ作成できないものであって、あるアーキテクチャとの対応関係を処理するためには、行政規制についての正確なスキームの構築を経た上で、ステークホルダ間の利害関係等を加味して契約条項が定められる必要がある。その具体的内容は、繰り返すように、自動的に決まるような性質のものではないが、利害関係等を加味した交渉のポイントを含めて、AI・データガイドラインに付属するひな型とその解説の参照をお勧めするところである。

[49] 請負か，委任（準委任）かですら，直ちには決まらない。

第6章　トラストサービスの概要と現状

パーソナルデータ を取り扱う事業では、パーソナルデータを提供する個人と事業者に限らず、複数の事業者が連携して事業を行うことが想定される。このような複数のステークホルダが連携して一つのシステムを構成する場合には、各機関や個人、モノとの間での認証や認可といった信頼関係の構築が重要となる。このような信頼関係を確立するために用いられる電子署名や認証などのトラストサービスは、国内外を問わず広く検討され、その導入や法令による導入なども進められている。

本章では、まず、6.1 で、認証の種類について解説する。次に、6.2 では、データに対する認証と技術について解説する。次に 6.3 では、認証と同時に多くの実用では、認可という概念を併せ持つとから、認証と認可の違いを解説する。6.4 では、これらの認証や認可で用いられるトラストサービスについて、欧州、米国、日本におけるサービスの概要を簡潔に解説する。

6.1　　認証の種類

複数の人や組織でパーソナルデータを取り扱うシステムを構築する場合、個々の相手先となる人や組織の正当性の確認や認証にとどまらず、ネットワークにつながるモノの認証、データそのものの真正の認証などを必要に応じて行う必要があるが、この認証には次のレベルが存在する。

6.1.1　　未認証

未認証とは、その対象となる人や組織、モノ、データなどについて、その真正を特段の方法による認証を行わないレベルである。

例えば、一般の消費者が小売店などで物品の購入を行う場合、店舗の看板や場所などにより相手方の確認を行なっているが、都度店舗の登記簿の確認などを行うことはない。これは、インターネット上の ｅ コマースや各種サービスで、同様のレベルが存在している。しかし、昨今はフィッシングサイトなどによる犯罪防止のため、ブラウザやセキュリティソフトなどにより、次項以下に述べる接続先サイトの真性を確認するレベルが普及している。

一方、実店舗や一般のサービスでは、広く誰でも利用できるサービス提供を目指しており、都度消費者の本人確認を行うことはない。もちろん、法令や条例の定めにより、特定の商材の販売やサービスの提供においては、本人の確認を求めることがある。例えば、酒類やタバコの販売では、消費者が成人であることの認証が行われているし、携帯電話などの契約では本人の確認を実施している。

これは、インターネットを介したｅコマースや各種サービスでも同様で、不特定多数に対して広くその利用を求める場合、サービス提供者は、一定のサービスや情報提供の範囲内においては、接続する相手方の真性の認証を行わない。とはいえ、これらは有償サービ

や高付加価値サービスへの移行に伴い、接続者の真性の認証を行う形態となることが一般的である。

6.1.2　片側認証

関連する人や組織、モノ、データの対において、片側だけが相手の真性を認証するレベルである。

前項に期したように法令や条例の定めにより、小売店において特定の商材の販売やサービスの提供する場合、本人の確認が求められるものがある。例えば、酒類やタバコの販売では、消費者が成人であることの認証を行う。また、携帯電話などの契約では、年齢だけでなく本人の確認を実施している。このような場合、顧客側は小売店の真性の認証を特段の証憑などにより明示的に行っていないが、小売側は明示的な認証行為を実施している。つまり、販売店側は、顧客を認証し、顧客は販売店の認証をしないという片側認証のレベルにある。

また、インターネット上の e コマースや各種サービスにおいて、サービス提供者側は、初期のアクセス者に対して特段の認証行為をせず、広く利用者のアクセスを受け付けているものが多い。しかし、利用側は、フィッシングサイトなどによる犯罪防止のため、ブラウザやセキュリティソフトの機能により、接続先サイトの真性を確認する仕組みが用いられているが、これも片側認証のレベルにある。

6.1.3　相互認証

関連する人や組織、モノ、データの対において、相互にその真性を認証するレベルである。

実社会においては、契約行為などは、印鑑証明などにより相互の真性を認証する行為が行われている。

インターネット上のサービスにおいても、初期のアカウント作成時は、未認証、または片側認証によりサービスの提供を開始し、有償サービスなどへ移行する段階において、本人確認や事業者確認という認証行為を行い、最終的に相互の認証を伴うサービスが行われることが多い。

6.1.4　第三者認証

関連する人や組織、モノ、データに対して、第三者の介在により相手の真性を認証するレベルである。

実社会において、小規模の組織の会員証などのように自己申告に基づき発行される証票により、その利用者の真性を認証することは多々ある。これは、インターネット上のサービスにおいて、利用者が ID とパスワードの登録をする事例でも同様で、あくまでも自己申告による基づく認証である。

これに対して、実社会でも免許証、パスポートなどの当事者以外が発行する証票により認証行為が行われるものが、第三者認証となる。

また、インターネット上のサービスでは、認証局(CA: Certificate Authority)の発行する証明書により認証を行うことは、第三者認証/TTP(Third Trust Party)による認証という

6.2　データに対する認証と技術

関連する人や組織、モノ、データの認証行為のうち、データについては、データ自身の正当性を保証するための認証技術として以下に示す各種技術が開発され実用化されている。

6.2.1　電子署名

電子署名（デジタル署名）とは、データの真正性を証明するために付加される短い暗号データである。この署名は、署名者の真性を証明し、改ざんやすり替えが行われないこと保証する目的で利用される。

6.2.2　タイムスタンプ

タイムスタンプとは、作成または更新されたファイルにメタデータとして記録されている、ファイルの更新日時に関する情報のことである。電子署名の一種で、特に重要な文書を電子化して扱う場合などに用いられる。このタイムスタンプにより、データの生成や更新の日時を証明することにより、複数の関連する人や組織、モノ間でデータが収受される場合、その時系列的な真性が保証される。

6.2.3　e シール

本書 6.4.1 の eIDAS 規則[50]でトラストサービスのひとつとして規定された「法人向けのツール」。総務省のトラストサービス検討ワーキンググループのとりまとめにおいては、「e シール（組織名の電子証明書）：電子データを発行した組織として、組織の正当性を確認できる仕組み」と定義されている。これは、実社会における社印などと同様に、印鑑証明まではないが、その提供元の組織が、組織としての提供主体性を表する仕組みである。

6.2.4　ウェブサイト認証

ウェブサイトが正当に開設されたものであるかを確認する仕組みで、インターネットサービスにおいては広く利用されている。本書 6.1.4 に示した第三者認証のための仕組みである。なお、CA/ブラウザフォーラムでは、ウェブサイト認証のための電子証明書を発行する認証事業者に求められる基準を議論している。

6.2.5　モノの正当性の認証

モノ（IoT 機器）から発信されるデータの真性の確認を行うために、モノ（IoT 機器）と通信の相手方において用いられる各種電子的手法が開発されている。ただし、モノ（IoT 機器）であっても、その多くはインターネットに接続可能な機能を有する組込システムで

---

[50] eIDAS の略は、The Electronic IDentification Authentication and trust Services であるが、eIDAS 規制の正式名称は、Electronic Identification and Trust Services Regulation であり、Authentication が付かない。

あるだけで、用いられる技術概念に基本的な差異はない。なお、様々な単位(機器毎か、製造ロット毎か等)で認証を行うことが想定されており、我が国ではその制度の在り方については、実証実験などと合わせて検討されている段階である。

6.2.6 e デリバリー

データの送達などを保証する仕組みが e デリバリーである。厳格にヒトや組織の確認された送受信者双方が登録することで成立するサービスであるが、現時点においてその制度化やニーズが顕在化していない。このため、我が国ではその制度の在り方については、実証実験などと合わせて検討されている段階である。

6.3 認証と認可

複数の人や組織でパーソナルデータを取り扱うシステムを構築する場合、個々の相手先となる人や組織の正当性の確認や認証にとどまらず、ネットワークにつながるモノの認証、データそのものの真正の認証などを必要に応じて行う行為が認証である。つまり、認証により人や組織、モノ、データの真性を確認することは、連携の第一段階である。

多くのサービスでは、認証により真性が確認された相手方が利用可能なサービスや操作範囲は一ではなく、相手方の属性により制御される。すなわち、認証された相手方の行為に対する認可が行われる。

認証と認可は、それぞれ英語では Authentication と Authorization と評されるが、この二つは異なる概念であるが、同時に密接無関係をもつ。

パーソナルデータを扱うビジネスでは、サービスの利用者に対して、そのアクセス範囲などを適切に管理することで、パーソナルデータの漏洩などのリスク管理をすることが重要となるため、常に認証と認可を念頭にアーキテクチャ設計をすることが求められる。

端的に、これら二つを定義すると以下の様になる。

認証 Authentication

対象の人や組織、モノ、データの真性を確認すること。

認可 Authorization

認証済みの人や組織、モノに対し、与えられた適切な権限による操作を許可する（権限外の利用を拒否する）こと。

6.4 トラストサービスの各国の取り組み

6.4.1 欧州の取り組み（eIDAS 規制）

欧州では、1999 年に定められた電子署名指令に代わり、「Electronic Identification and Trust Services Regulation（eIDAS 規則）」[51]が 2014 年 7 月に採択された。EU 加盟国はそれぞれ電子署名指令に従った独自の電子署名法を定めていたが、これらの各加盟国の電子

[51] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

署名法は、すべて「eIDAS 規則」に上書されることになった。「eIDAS 規則」は、電子署名の法的効力を承認した電子署名指令を継承するもので、その適用範囲は電子署名を含むトラストサービスと eID に拡大されている。

eID とは、電子認証（つまり、電子的な本人確認）を行うことができる機能のことであり、我が国のマイナンバーカードも電子認証の機能を有していることから、eID の概念に含まれると言える。「eIDAS 規則」は、この eID の認証結果を各国で受け入れ合うことを定めている。EU 全域で、トラストサービスと eID に関する統一的な法的効力を承認することで、確定申告や銀行口座の開設、入札への参加、大学への入学手続等をオンラインで申請できるようになり、また、他の加盟国への申請も行えるようになる。

つまり、「eIDAS 規則」とは、eID とトラストサービスの法的効力を承認し、電子申請、オンライン決済、電子契約等における信頼性が紙の世界と同等であることを担保することで、電子化と効率化の促進を狙いとした法律である。この電子化と効率化による競争力の向上及び経済成長を狙いとすると同時に、加盟国間の隔たりをなくすことで、欧州全体で 1 つの大きなデジタル市場を形成しようとしている。

トラストサービスには、電子署名、e シール、タイムスタンプ、e デリバリー、ウェブ認証が含まれる。また、各 EU 加盟国は自国の適格トラストサービスプロバイダとそのトラストサービスに関する情報をトラステッドリストに掲載し公開する義務を負っている。また、加盟国のトラステッドリストとは別に、欧州委員会はリストオブトラステッドリスト（LoTL）と呼ばれるリストを公開しており、このリストには各加盟国のトラステッドリストへのリンクと、トラステッドリストの署名検証を行うための公開鍵に関する情報が記載されている。これにより、トラストサービスの依拠当事者は LoTL を通じてトラステッドリストの有効性検証を行い、当該トラストサービスがリストに載っているトラストサービスであるか否かを自動で検証できるようになっている。

FutureTrust は、欧州研究・イノベーション枠組み計画（Horizon 2020）より資金を提供され、2016 年 6 月 1 日から 2019 年 8 月 31 日まで実施されたプロジェクトである。このプロジェクトは、EU 域内市場での電子識別(eID)及びトラストサービスに関する eIDAS 規則 の実用的な実装をサポートしており、世界中で法的効力に裏付けられた電子取引を実現するために、ヨーロッパ以外でも、信頼できる eID 及びトラストサービスの利用と普及することを主目的としている。FutureTrust は、現在の eIDAS 規則のエコシステムを補完するオープンソースのコンポーネントとサービスを設計及び開発し、開発されたコンポーネントを使用して、eIDAS 準拠の実用的なアプリケーションを構築及び使用する方法を示している。

UNCITRAL（The United Nations Commission on International Trade Law、 国際連合商取引法委員会）は、1966 年に国連総会において国際商取引法の調和と統一の促進を目的に設置された委員会である。この委員会の中で欧州は eIDAS 規則のトラストサービス及びそのフレームワークをモデル法の中に組み込む活動をしている。モデル法とは、法整

備が整っていない国に向けた国連の推奨法案である。MLTER（The Model Law on Electronic Transferable Records）は UNCITRAL で検討され 2017 年に国連総会で採択されたモデル法の一つであり、この中に電子署名やｅシール、タイムスタンプといった eIDAS 規則における用語や定義が組み込まれている。欧州委員会はこのモデル法を通じて eIDAS 規則のエコシステムの拡大を狙っていると思われる。

6.4.2　米国の取り組み（トラストフレームワーク）

トラストマーク及びトラストマークフレームワークは、米国の NSTIC(National Strategy for Trusted Identity in Cyberspace)、サイバー空間における信頼できるアイデンティティに関する国家戦略)のパイロットプロジェクトの一つとして、ジョージア工科大学において 2013 年から 2016 年にかけて検討／開発された。トラストマーク及びトラストマークフレームワークでは、単一のトラストフレームでは複数のコミュニティにおけるニーズを満たすことができないという課題に対して、各トラストフレームワークをモジュール化し、再利用可能なコンポーネントとして扱うことを解決策としている。再利用可能なコンポーネントはトラストマークと呼ばれる。

NIEF（National Identity Exchange Federation）は米国政府における法執行に関する機微なデータ共有を目的とした米国政府機関の集合体であり、CISA（Criminal Information Sharing Alliance)、RISS (Regional Information Sharing Systems）、 DHS (US Department of Homeland Security ）や FBI (Federal Bureau of Investigation）等が参加しており、情報共有時の信頼保証にトラストマーク及びトラストマークフレームワークを採用している。

NIST は Cyber-Physical System（CPS）のフレームワークとして NIST SP 1500-201 を 2017 年に公開している。これに基づいて、ドメイン固有の CPS フレームワークが定義されている一例として IES-City(Internet of things Enabled Smart City)フレームワークがある。スマートシティのさまざまなアーキテクチャ設計の原則、分類法、及び標準は複数の場、組織において開発及び提案されているが、IoT の可能性をスマートシティで実現するための標準化の取り組みはまだ収束していない。NIST は、米国内及び国外パートナーと共に、「IoT 対応スマートシティフレームワークに関する国際テクニカルワーキンググループ」を設立し、既存アーキテクチャ全体の相互運用性（PPI）の要点を特定し、共通のアーキテクチャ機能のコンセンサスフレームワークドキュメントを作成した。このフレームワークドキュメントは、都市がコミュニティのニーズを満たす相互運用可能でスケーラブルなスマートシティソリューションを採用する際にサポートとなる文書である。

6.4.3　日本の取り組み

2019 年 4 月経済産業省が 「サイバー・フィジカル・セキュリティ対策フレームワーク

Ver1.0」（以下、CPSF)を公表した。CPSF では、「Society5.0」における新たな形のサプライチェーンにおいて全産業にほぼ共通して求められるセキュリティ対策をわかりやすく示すために、サイバー空間とフィジカル空間が高度に融合した産業社会を 3 つの切り口（「企業間のつながり」、「フィジカル空間とサイバー空間のつながり」、「サイバー空間におけるつながり」）から捉え、サプライチェーンの信頼性（trustworthiness）を確保する観点から、それぞれの切り口において守るべきもの、直面するリスク源、対応の方針等を整理している。サイバー空間におけるリスク源に対応した対策要件として「暗号化によるデータ保護」、「データの提供者の信頼性確認」が挙げられている。

総務省においては、令和 2 年 2 月 7 日にプラットフォームサービスに関する研究会最終報告書が公開され、その別紙として「プラット フォームサービスに関する研究会トラスト サービス検討ワーキンググループ最終取りまとめ」を報告している。サイバー空間において、正当でないモノがネットワークにつながることや、誤ったデータや改ざんされたデータが紛れ込まないよう、データの真正性を確保した上でデータを流通させる必要が生じるため、ヒトだけではなく、組織やモノの正当性、また、それらから発信されるデータの完全性を確認できる仕組みをトラストサービスとしている。

今後の取り組みや関連事業において注目されるのが、IoT 社会に対応したサイバー・フィジカル・セキュリティ研究開発計画、である[52]。 図 24 に、サプライチェーンの各構成要素についてのセキュリティ確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーン（連鎖）を構築することで、製品・サービスのライフサイクルにわたるサプライチェーン全体のセキュリティを社会実装するために必要となる技術開発項目の全体像を示す。信頼のチェーン（連鎖）構築には、（A）「信頼の創出・証明」技術、(B)「信頼チェーンの構築・流通」技術、(C)「信頼チェーンの検証・維持」技術、の 3 つの技術を必要とする。

[52] 引用： https://www8.cao.go.jp/cstp/gaiyo/sip/keikaku2/3_iot.pdf

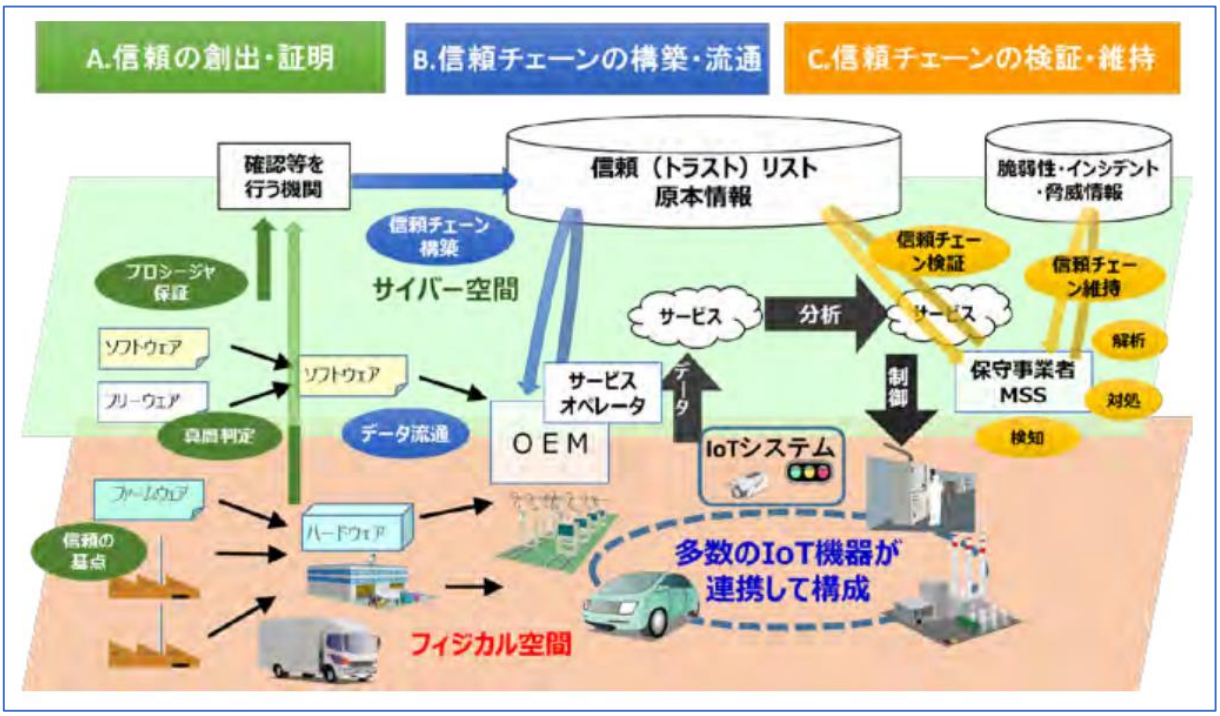


図 24　信頼チェーンで構築されるサイバー・フィジカル・セキュリティ対策基盤のイメージ

【活用編】

第7章　用語・定義

リファレンスアーキテクチャ書及び付帯資料において用いられる用語の定義を取りまとめた、別冊「用語・定義書」の概要とその利用方法について解説する。ここでは、法令などにより明確な定義のある用語以外に、慣例的に使われているものの、その定義や適用範囲の解釈が多様であるために、混乱や誤解を招く用語をできる限り整理してとりまとめている。

7.1　　用語・定義集の項目

用語・定義集は、次の項目を記載している。

7.1.1　　分類

分類は、当該用語が主として利用される範囲を以下に類型化して示しているが、当該用語の利用範囲を規定するものではなく、定義集の整理を目的として付したもので、利用者が任意の用語を検索することを容易にするための分類である。

7.1.1.1　全般

当該用語がアーキテクチャ全般にて利用されている。または、適切な分類が未定のもの。

7.1.1.2　データ種類

データまたは、データセットの構造、及びその内容に関する用語である。

7.1.1.3　情報種類

データまたは、データセットにより構成される情報に関する用語である。

7.1.1.4　データ処理

データまたは、データセットの処理に関する用語である。

7.1.1.5　契約・トラスト

契約・トラストに関する用語である。

7.1.1.6　事業モデル

事業に関わるアクターの定義である。

7.1.2　　用語

当該用語の日本語表記である。

7.1.3　　英語表記

当該用語の英語表記である。

7.1.4　本書での定義

当該用語の本書における定義である。

7.1.5　アイコン

本書及びユースケースシナリオなどで当該用語を表す場合のアイコンである。表 21 ではスペース上、アイコンを省略した。本書 7.3 にまとめて記載した。

7.1.6　リファレンス

当該用語について、既出の定義などがある場合の外部参照情報である。

7.1.7　リファレンス先での定義

当該用語について、外部参照先での定義である。

7.2　用語定義集の記載例

表 21 に用語定義集の記載例を示す。別冊「用語・定義書」においては、アイコンも表内に定義しているが、紙面の制約上、7.3 アイコンの例にまとめて示す。

表 21　用語定義集記載例

分類	用語	英語表記	本書での定義	リファレンス	リファレンス先での定義
全般	データ	Data	データとは、情報の表現であって、伝達、解釈または処理に適するように形式化され、再度情報として解釈できるもの	ISO/IEC 2382-1、JIS X0001 情報処理用語-基本用語	A reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing. 情報の表現であって、伝達、解釈または処理に適するように形式化され、再度情報として解釈できるもの。
全般	データボディ	Data Body	1 以上のデータの集合でメタデータを含まない。	No definition in ISO	
全般	メタデータ	Meta Data	データのうち、データの属性などを示すデータ。	ISO/IEC 11179-3:2013, 3.2.74	data that defines and describes other data
全般	データ値	Data Value	個々のデータの持つ値	ISO/IEC 25000:2005	content of data item
全般	データメンバ	Data Member	同一のメタデータに紐づくデータの集合	No definition in ISO and ITU	
全般	データレコード	Data Record	共通の識別子により関連づけられたデータメンバの集合	ISO 18739:2016(en), 3.1.13	one or more data items treated as a unit within a data set
全般	データセット	Data Set	データボディ、メタデータの集合で、データセット自体にもメタデータが含まれる	ISO 8000-2:2018, 3.2.4	logically meaningful group of data

7.3　　アイコンの例

用語定義集および別冊のユースケースシナリオテンプレートでは、以下のようなアイコンを利用している。これらのアイコンを、アーキテクチャを設計する際に適宜用いることにより、可読性を向上させ、課題の抽出に役立つことを期待している。

本来であれば、このようなアイコンも含めて、標準化仕様として発行されることが望ましいが、本書の発行時点では、標準化には至っていない。

そこで、パーソナルデータを扱う事業者が自らの事業モデルのアーキテクチャを設計するに際しては、適宜コピーして利用いただくか、自ら同等のアイコンを設計されることが望ましい。ただし、異なる事業者間においての比較や連携のためには、可能な範囲で一定の要件の範囲での創作されることが望ましいため、以下のような点に留意することを望む。

- ✓ 既存アイコンの有無を確認し、既存者がある場合には、これを用いる。
- ✓ 同等の機能や意味を表すものの、詳細を付すことでより可読性を高めるものタグなどを併記して利用する。
- ✓ 新たなアイコンを作成する場合には、白黒での設計を原則とする。
- ✓ 新たなアイコンを作成した場合には、7.5 に示す改定方法により共有化を行う。

図 25 アイコン例 1

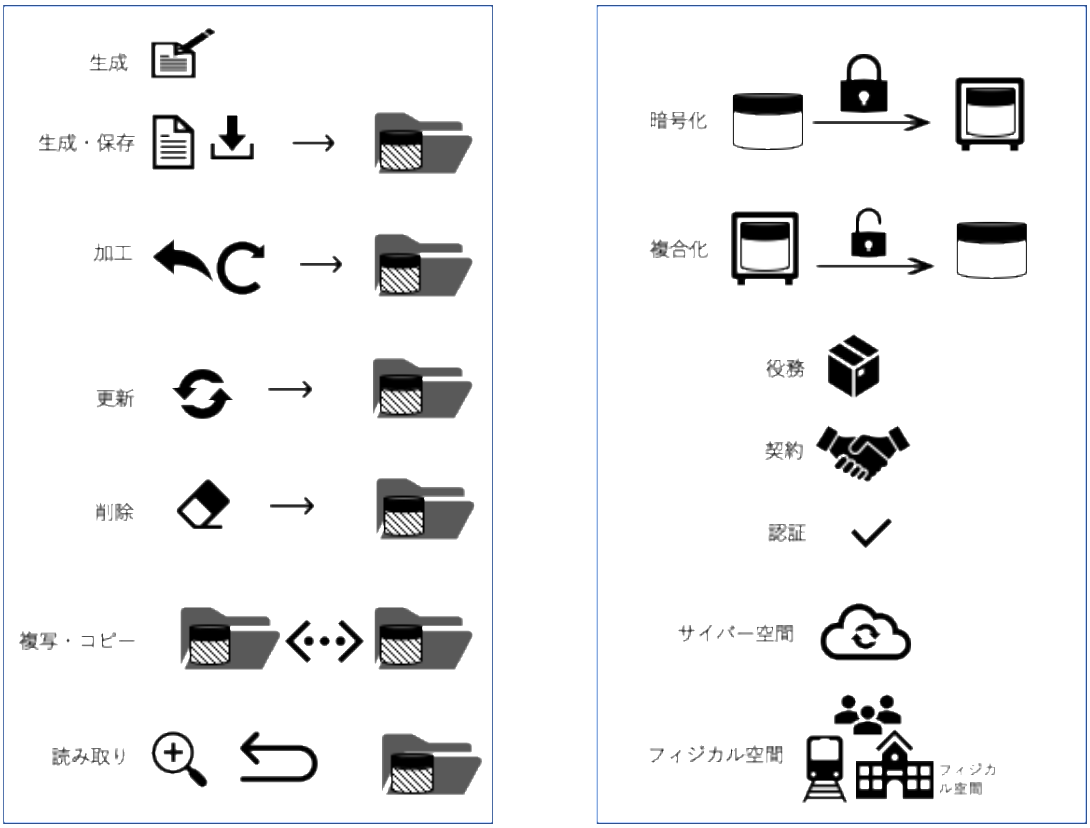


図 26　アイコン例 2

7.4　　用語・定義集の公開と入手

本書ならびに定義書は、DTA または別途内閣府の用意するホームページにて公開される予定である[53]。

7.5　　用語・定義集の改定と追記

本書ならびに定義書に対して、加筆、修正を求める場合には、DTA または別途内閣府の用意するホームページなどにより修正提案を受け付ける予定である。

本書初版発行時点では、改定提案のフォームなどが開設されていないが、今後これらの改定や追加の受付フォームなどを用意する予定である。

[53] https://data-trading.org/sipb-1_personaldataarchitecuture_dta/
https://www8.cao.go.jp/cstp/stmain/20200318siparchitecture.html

第8章　リファレンスアーキテクチャ本体（設計部）

リファレンスアーキテクチャ本体（設計部）は、各事業者が自らの事業を設計・整理するための手引書である。このリファレンスアーキテクチャ本体（設計部）の位置づけや内閣府の提唱する Society5.0 リファレンスアーキテクチャとの関係、各事業者が自らの事業のアーキテクチャ設計を行うために用いる別冊のユースケースシナリオテンプレートの利用手順を本章で解説する。

8.1　設計部の位置づけ

設計部の定義、利用目的等は次のとおりである。

8.1.1　設計部の定義

パーソナルデータを扱う全ての事業者、ステークホルダが、ビジネスモデルや内部統制などのシステム設計を行うためのガイドである。

8.1.2　利用目的

リファレンスアーキテクチャを設計・整理することで、各事業者がパーソナルデータの取扱いの適正性や潜在する課題を顕在化し、適切なパーソナルデータの利活用モデルを普及させる。

パーソナルデータを取り扱う事業の共通要件を明確にすることで、分野・事業間の一定の協業を推進する。

8.1.3　対象者

パーソナルデータを取り扱う事業者(事業の計画時、検討時も含む)、パーソナルデータを取り扱う可能性を有する事業者(事業の計画時、検討時も含む)。

8.1.4　制約事項

設計部を含む本書は、パーソナルデータを取り扱う事業に対して、免責を付すものではない。本書は、パーソナルデータを取り扱う事業に対して、実装を制限するものではない。

8.1.5　使い方

本書記載のユースケースシナリオテンプレートに照らして、自身のビジネスのユースケースシナリオを構築する。ユースケースシナリオテンプレート記載のチェックポイントを参照しながら、自身のビジネスを解析し課題を明確にしていく。解決すべき課題がどこに存在するかを明確化するチェックリストとして使用する。

8.2　Society5.0 リファレンスアーキテクチャとの対比

8.2.1　５つのビューポイントによるアーキテクチャ

Society5.0 リファレンスアーキテクチャにおける本書の位置づけは、1.4.4 で述べた。ISO/IEC42010 は、複雑なシステム SoS （System of Systems)のアーキテクチャ構築手順を示しているが、この手法を用いると、アーキテクチャは、５つのビューポイントで表す

ことができる[54]。即ち、Implement（実装視点）, Function（機能視点）, Usage（利用/シナリオ視点）, Business（ビジネス視点）, Society（社会課題・ルール視点）[55]の 5 視点である。図 27 は、その 5 つと Society5.0 リファレンスアーキテクチャとの関係を対比したものである。5 視点の内、本書においては、Usage 視点に最も重点を置き、Business 視点、Society 視点を考慮していると言える。Function 視点（必要となる機能群）、Implementation 視点（具体的な実装モデルなど）までの深堀はしていない。

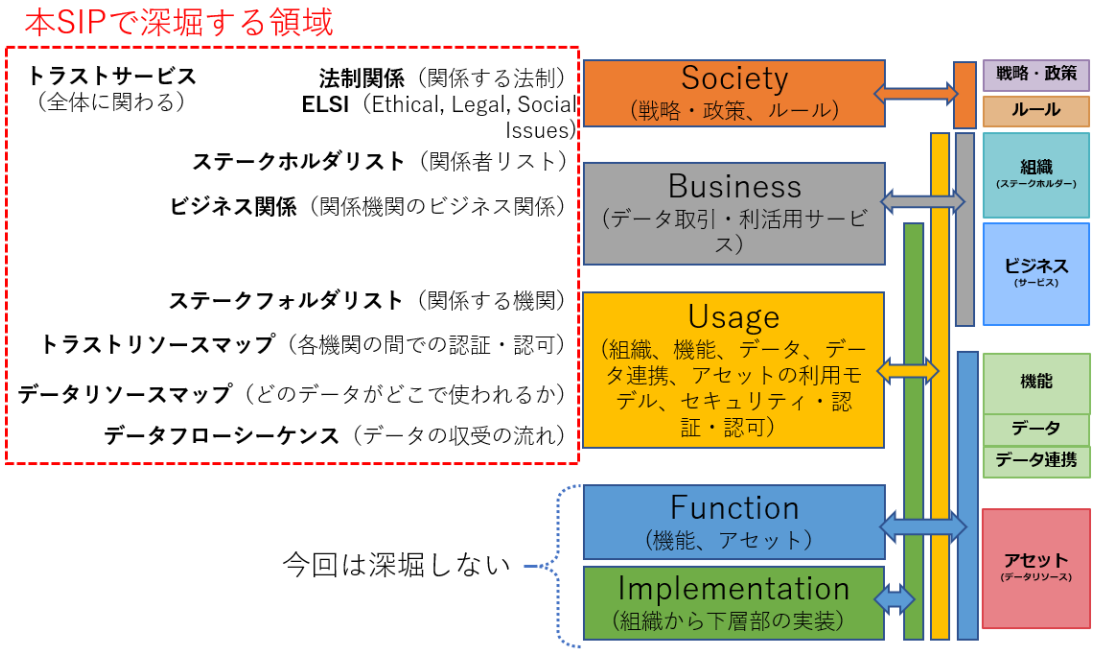


図 27　5 つのビューポイントと Society5.0RA との対応関係

8.2.2　リファレンスアーキテクチャと各実証事業の位置づけ（ELSI）

第 4 章図 23 が示すように ELSI(Ethical, Legal, and Social Issues)は、ルール層を中心に一部戦略・政策や組織に関わる領域である。この領域については、別冊「パーソナルデータ分野に関する ELSI 検討会報告書」を熟読のうえ、本書 4.2 に示す規範などに照らして、みずからの規範のよりどころを明確にすることを推奨する。また、本書 4.3 にある問題事案などを参照し、同様のインシデントや社会的問題が内包しないかを確認することも重要である。

---

[54] ISO/IEC 42010 は関わるステークホルダの関心事に合わせて視点（Viewpoint）を設定することが推奨されている。これに基づいてアーキテクチャ構築された事例が IIC(Industrial Internet Consortium)の IIRA(Industrial Internet Reference Architecture)である。ここには、4 層（Implementation, Function, Usage, Business）が定義されている。図はさらに Society 層を追加した 5 層で表している。

[55] 参照：https://www.jstage.jst.go.jp/article/trafst/12/1/12_33/_pdf/-char/ja

加えて、別冊のユースケースシナリオ集には、本書の作成と併行して本プロジェクトの実証研究実施者が記載したアーキテクチャがまとめられているので参照にして頂きたい。

このような作業の結果、本書 4.4 にあるパーソナルデータ分野に関する事業者に求められる視点と、本書 2.4 に示したようにパーソナルデータ原則を定めることが重要となる。

8.3　アーキテクチャ設計の手順

本書に従って、パーソナルデータに関する事業を行う方は、以下の手順によりそのアーキテクチャを明確にすることが可能となる。

（1）　対象事業の適用性確認

対象とする事業の概要を掴む。関係するステークホルダやパーソナルデータの関与があるかを確認する。例えば、対象事業が第 3 章に示した各事業モデルに照らして、同類なのか？全く別物なのか、如何に位置づけられるかを定義して置くことを推奨する。これは将来の事業モデルの類型化につながる。

ただし、第 3 章に示す各モデルは、もっぱらパーソナルデータの取り扱いを、その事業の主たる取り扱い対象とするものであり、全てのビジネスモデルが、これらのモデルのいずれかに単純に類型化されるものではない。むしろ、パーソナルデータは多くの事業に利用されるため、多くのビジネスモデルは本章の示す事業モデルの一部または全部を包含或いは組み合わせにより実現される。

さらには、本書 10.2 に示したデータジャケット（DJ）は、人間中心のダイナミックな創造活動の場を生み出すためのツールになりえる。即ち、DJ は直接的にはデータセットの中身を明かさずとも、その概要を共有できる手段を提供する。この手法を用いるならば、様々な DJ の交換によって新たな価値を生み出す場を創出できる。対象事業の検討に当たっては、DJ の手法を用いることで新たな事業領域の創出を検討することができる。

（2）　プライバシー原則の制定

プライバシー原則については、本書 2.4 に記載した。ここにはプライバシー原則についての考え方やいくつかの事例を示した。どれかをピックアップし、それが自身の事業にとって十分かどうかを考え、足りなければ他の原則の項目を持ってくるなどして、自身の事業のプライバシー原則を定める。

（3）　ユースケースシナリオテンプレートに従った記載

「ステークホルダリスト」、「ビジネス関係図」、「データリソースマップ」、「トラストリソースマップ」、「データフローシーケンス」、「法制関係表」の各アーキテクチャ図面を記載する。

（4）　プライバシー原則や関連法性に照らして、作成した各図面の整合性を評価

評価に当たっては、第 9 章及び別冊「ユースケースシナリオ集」の記載方法、記載例、評価例、評価結果からの想定される事業への反映などの各項目を参考にすること。

（5）　確認の結果

評価結果を確認し、修正すべき事項があれば修正し、（3）からを繰り返す。最終確認においては、本書 8.2.2 のように ELSI 視点での問題がないかを確認することを推奨する。

第9章　ユースケースシナリオテンプレートの使い方

本章の活用編に従って、各事業者が記載するための様式(別冊のユースケースシナリオテンプレート)とその記載方法について解説する。また、別冊の「ユースケースシナリオ集」には、本プロジェクトで実施された四つのパーソナルデータに関する実証研究をモデルに、各実施者がそのアーキテクチャについてテンプレートを用いて記載したものを収録している。

ユースケースシナリオテンプレートを使った具体的な使い方を示すために、ドライブレコーダのデータを収集し、個人情報を除去し、第三者に統計データを提供する事業の事例を用い、実際の記載事例や、記載結果から得られた評価点を示している。

なお、本事例は、国内の今回の SIP 採択事業者とは異なる民間事業者が検討している事業をヒアリングし記載したものである。

9.1　　ユースケースシナリオテンプレート

ユースケースシナリオテンプレートは、パーソナルデータ流通に関するユースケースシナリオのアーキテクチャを記述するにあたって、Society5.0RA の各層の詳細化、及び層間の関係性を明確にすることを目的としている。

ユースケースシナリオテンプレートとして、「ステークホルダリスト」、「ビジネス関係図」、「データリソースマップ」、「トラストリソースマップ」、「データフローシーケンス」、「法制関係表」の６つのテンプレートを用意している。

これらのテンプレートを利用することによって、パーソナルデータを扱う事業を検討する者が事業のアーキテクチャを設計・整理し、パーソナルデータの取扱いの適正性の確認や潜在する課題の顕在化を行った上で、適切なパーソナルデータの利活用モデルを構築し、社会実装に寄与できることが期待される。

なお、ユースケースシナリオテンプレートの開発に当たっては、パーソナルデータの流通に関する複数の実証プロジェクトと連携している。具体的には、ユースケースシナリオテンプレートがこれらの実証プロジェクトのユースケースシナリオの構造や、パーソナルデータの流通フローなどを表現可能かについて実証プロジェクトチームの確認をとりながらユースケースシナリオテンプレートを構築した。連携した実証プロジェクトについては、本書において概要を記述するが、ユースケースシナリオテンプレートを用いた実証プロジェクトの表現については、ユースケースシナリオ集（別紙）としてまとめているので参考にされたい。

次節以降、各テンプレートの利用方法等について述べる。

9.2　　ユースケースシナリオテンプレートの利用手順

パーソナルデータに関する事業について、そのユースケースシナリオを上述の６つのテ

ンプレートを用いて記述する際、６つのテンプレートが独立して記載するものではなく、テンプレートの１つを修正するとそれにより他のテンプレートが影響を受けることになる。ユースケースシナリオテンプレートを効果的に利用するためには、各テンプレートの他への影響度を考慮すると、以下に示す（１）～（６）の順序に従って記載することが望ましい。

（１） ステークホルダリストを利用し、ビジネスに関わるエンティティを洗い出す。その際、パーソナルデータのデータ主体は、個人、組織、機器も含め漏れなくリスト化する。

（２） ビジネス関係図を利用し、ステークホルダリストに記載された各ステークホルダ間のビジネス関係（事業者間の契約や同意の取得、物販や役務等）を記載する。

（３） データリソースマップを利用し、ビジネス関係図に重なるように、どのエンティティがどんなパーソナルデータを持つことになるのか、パーソナルデータが転送されるのかなどを記載する。

（４） トラストリソースマップを利用し、ビジネス関係図やデータリソースマップを参照しながら、各ステークホルダ間の認証関係の有無、認証方法を整理する。

（５） 法制関係表を利用し、各ステークホルダ間の遵守事項とその拠り所を明確にする。拠り所は個別の契約による場合もあれば、法制に基づくものもある。

（６） データフローシーケンスを利用し、ビジネス関係図、トラスト、法制を考慮した上で、誰がどの情報をどういう順序で流通させるのかを時系列に記載する。

9.3 ステークホルダリスト

9.3.1 記載方法

ステークホルダリスト作成の目的は関与する個人、事業者の一覧表を作成することで、パーソナルデータが取り扱われる範囲を明確にし、プライバシー原則など遵守すべきプレイヤ（ステークホルダ）に抜けがないかを確認することである。取り扱うデータが個人情報保護法制の定める個人情報に該当する場合は、個人情報取扱事業者に該当するかなどの、個人情報保護法での位置づけを明確にする。

この時、ISO/IEC 29100:2011 で定義されるプライバシーフレームワークの定義に示される PII：Personally Identifiable Information（個人を特定できる情報)の取扱者を役割に沿って類型化することで、事業に関わるプレイヤと個人情報（PII）との関係性を明確にすることができる。

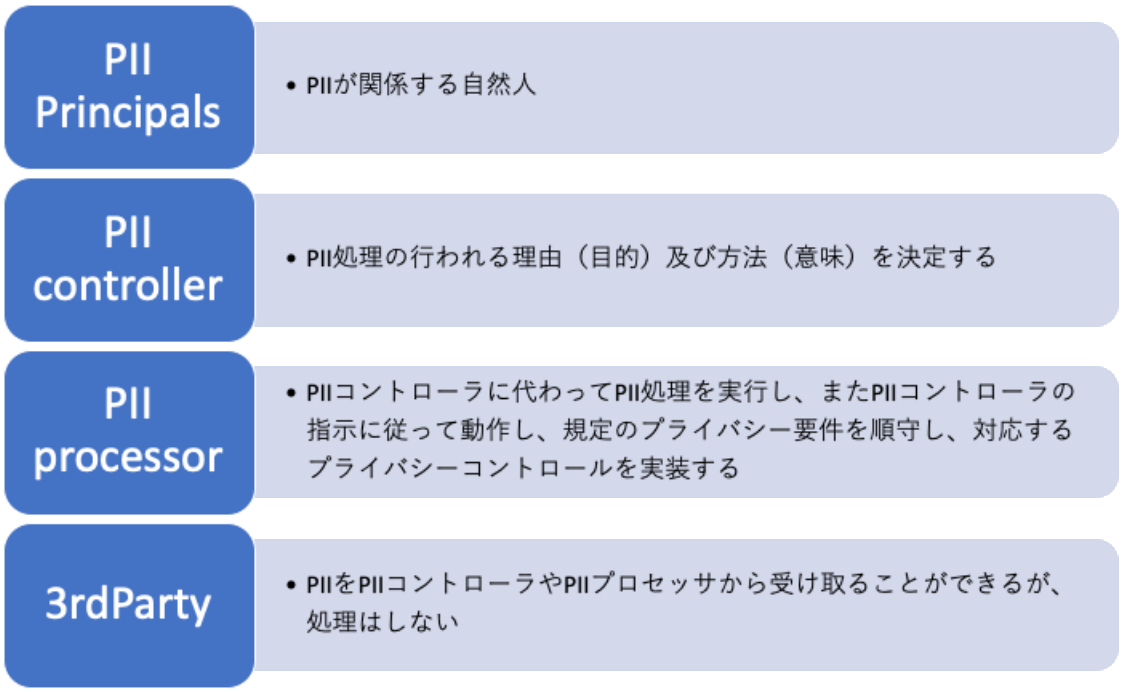


図 28　PII：Personally Identifiable Information（個人を特定できる情報)の取扱者分類

9.3.2　記載例

ステークホルダリストの記載例として、ドライブレコーダのデータを収集し、個人情報を除去し、第三者に統計データを提供する事業の記載事例を表 22 に示す。

表 22　ドライブレコードビジネスにおけるステークホルダリストの記載事例

名称	概要（主に個人情報保護法での位置づけ等）	ISO/IEC 29100 での分類
ドライバ	ドライブレコーダで録画した映像を提供する	PII principal
ドライブレコーダ販売事業者	ドライブレコーダを販売する	非該当
データ蓄積事業者	ドライバから提供された映像を蓄積管理する。映像加工（非個人情報化）をデータ加工事業者へ委託する。映像を購入したい事業者へ販売する。個人情報保護法上の個人情報取扱事業者に該当	Data controller
データ加工事業者	データ蓄積事業者から映像加工（非個人情報化）を受託する個人情報保護法上の委託先に該当	Data processor
データ購入事業者	データ蓄積事業者から映像を購入する	非該当
通行人	ドライブレコーダが録画した映像に映り込んでいる人	PII Principal

9.3.3　評価例

表 22 の記載例に対して、プライバシー原則などとの整合性という視点から評価すると以下のような課題点が顕在化する。

9.3.3.1　ドライブレコーダ販売事業者は、パーソナルデータの取り扱いについて特段の役目を持たないのか?

例えば、ドライブレコーダ販売事業者や製造事業者は、製品保証やサービスのために、購入者情報を得る場合が想定される。この場合、製品のシリアル番号と利用者の個人情報が紐付けられる。

そこで、たとえば収集されたドライブレコーダのデータに、製品情報としてシリアル番号が含まれる場合、ドライブレコーダ販売事業者や製造事業者がデータ購入者となった場合は、個人情報との名寄せが行われる可能性があることは、容易に想定される。

このように、ステークホルダの役割をリストアップすることで、パーソナルデータの取り扱いに影響を与える可能性のある関係を洗い出すことが可能となる。

9.3.3.2 通行人は、パーソナルデータ の視点では、システムを構成する一構成者としてリストされているのは適切か?

表 22 には、通行人がリストアップされている。この事業モデルにおいて、ドライブレコーダに映り込む通行人は、事業を実施する側の関係者ではないが、システム全体の中に通行人のパーソナルデータが入り込むことが自明である。この通行人をステークホルダリストに記載される事は、重要な視点であり、このようなリスト化により顕在化される事が判る。

9.3.4 評価結果からの想定される事業への反映

データ蓄積事業者にとっては、ドライバだけではなく、通行人の PII に関わる処理が課題であることが分かる。そのため、データ加工事業者への処理仕様が明確化されることが期待できる。

9.4 ビジネス関係図

9.4.1 記載方法

ビジネス関係図の目的はステークホルダリストに示された個人、事業者間のビジネス関係（契約など）を明確化することである。事業者間においては、パーソナルデータを契約に基づいて他者にその処理や利用を委任する順委任契約のような形態や純粋に他社にデータの提供を行う場合の契約など、さまざまな契約形態が存在する。

また、各ステークホルダの間では、契約に基づきデータ意外にも物品や役務の提供が行われ、このような行為に起因したデータが生成される場合もある。

さらには、このような特定の個別契約を有しない、サービス提供や物販などに起因してパーソナルデータは生成されている。

ビジネス関係図には、まずステークホルダリストに記載されたステークホルダを配置し、そのステークホルダ間に存在する契約や物販や役務の提供などを、アイコンと矢印により記載する。

この時、アイコンだけでなく、その詳細を示す簡単なタグ名を付す事で、契約の形態なども表現する。

9.4.2 記載例

記載例として、ドライブレコーダ（ドラレコ）の映像（ドラレコ映像）等のデータを収集し、個人情報を除去し、第三者に統計データを提供する事業の記載事例を図 29 に示す。

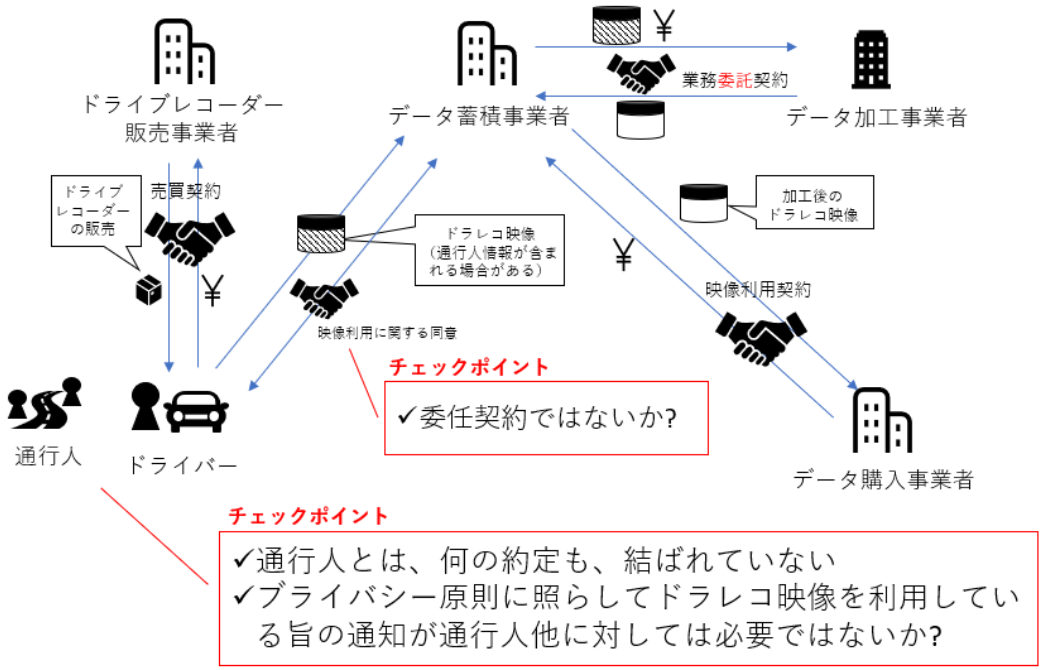


図 29　ドライブレコーダビジネスのビジネス関係図記載事例

9.4.3　評価例

図 29 に示す記載例に対して、プライバシー原則などとの整合性という視点から評価すると以下のような課題点が顕在化する。

9.4.3.1　通行人とは、何の約定も、結ばれていない

図 29 では、ステークホルダの一つである通行人は、他のステークホルダとの間で、なんら約定などによる自明な契約関係が存在しないことが明確にわかる。

しかしながら、プライバシー原則に照らして考えると、ドライバはドラレコ映像を第三者に提供しているので、その旨を通行人他に対して通知する必要が浮かび上がる。

9.4.3.2　委任契約ではないか?

図 29 では、ドライバは、自己の保有するドライブレコーダの画像を、データ蓄積事業者に提供しているが、この時の契約は準委任契約なのか、純粋に第三者であるデータ蓄積事業者への提供契約なのかが不明であり、この点について明確に検討する必要があることが浮かび上がる。

9.4.4　評価結果からの想定される事業への反映

ステークホルダ間での契約、物販、サービス提供、役務の存在を確認できる。牽いては、データ提供者にどのような価値を還元するかも明確にすることができる。

9.5　データリソースマップ

9.5.1　記載方法

データリソースマップの作成目的はパーソナルデータを含むデータセットがどこに存在するのかを明確にすることである。また、それらのデータが個人情報なのか、個人情報に対して仮名化したものなのか、匿名加工したものなのか、又は統計化（非個人情報化）したものなのかなど、データの遷移を明確にすることである。このデータリソースマップを記載する事により、事業遂行する上で、セキュリティを確保すべき箇所や、インシデント発生時の影響範囲、事業譲渡や事業終了などに伴う処理範囲を明確に把握することが可能となる。

データリソースマップは、まずステークホルダリストに記載されたステークホルダを配置し、そのステークホルダ間にて移動、偏在するデータの種類や移動、加工処理を、アイコンと矢印により記載する。なお、ステークホルダの配置は、基本的にはビジネス関係図と同じものを用いることで記載漏れがなくなる。

アイコンだけでなく、必要に応じて詳細を示す簡単なタグ名を付す事で、データ加工の形態なども表現する。

9.5.2　記載例

記載例として、ドライブレコーダのデータを収集し、個人情報を除去し、第三者に統計データを提供する事業の記載事例を図 30 に示す。

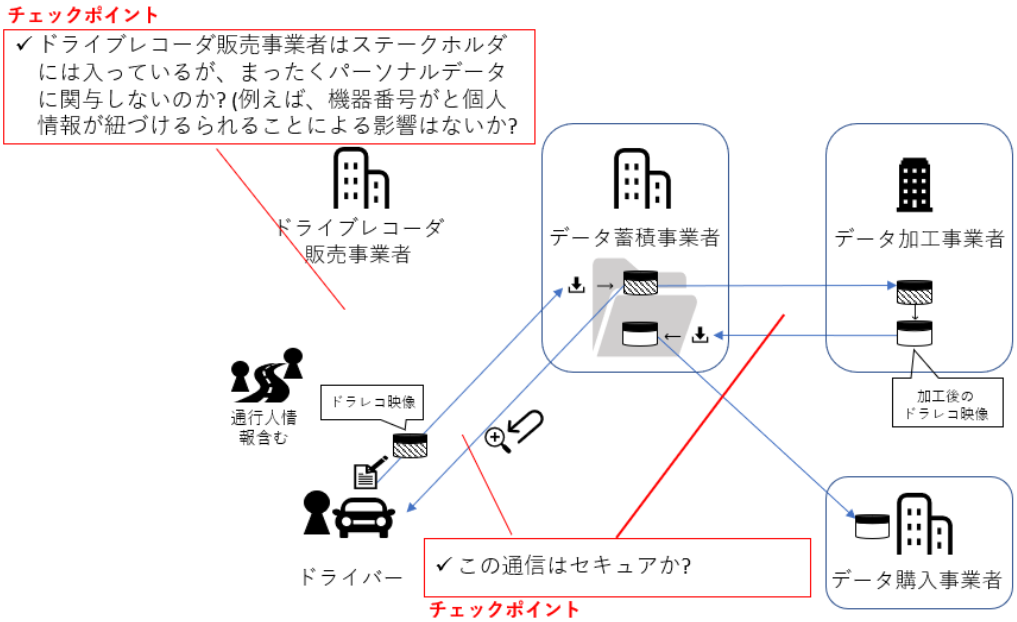


図 30　ドライブレコーダビジネスのデータリソースマップ記載事例

9.5.3　評価例

図 30 に示す記載例に対して、以下のことが事業上の留意点として顕在化する。

9.5.3.1　ドライブレコーダ販売事業者の扱い

ドライブレコーダ販売事業者は、ステークホルダリストに記載されており、ビジネス関係図では、ドライバとの物品の売買契約を行っている。しかしながら、図 30 のデータリソースマップには、なんらデータの取り扱いが示されていない。

本書 9.3.3 で示したように、例えば、ドライブレコーダ販売事業者や製造事業者、製品保証やサービスのために、購入者情報を得る場合が想定される。この場合、製品のシリアル番号と利用者の個人情報が紐付けられる。

そこで、収集されたドライブレコーダのデータに、製品情報としてシリアル番号が含まれる場合、ドライブレコーダ販売事業者や製造事業者がデータ購入者となった場合は、個人情報との名寄せが行われる可能性がある点が課題として浮かび上がる。

9.5.3.2　パーソナルデータの偏在箇所

図 30 から当該事業おいて、少なくともデータ蓄積事業者とデータ加工事業者の二つのステークホルダに、パーソナルデータが存在していること示されている。このため、当該事業の譲渡や終了時は、これらのステークホルダにおいてパーソナルデータに対する適切な処置が求められることがわかる。

また、ドライバとデータ蓄積事業者およびデータ蓄積事業者とデータ加工事業者の間では、パーソナルデータの移動が行われていること示されている。このことは、これらの間の通信経路に対する適切なセキュリティ保護が必要なことが自明となる。

9.5.4　評価結果からの想定される事業への反映

パーソナルデータの偏在箇所が特定できる。全体を管理するデータ蓄積事業者は自部門および他事業者が必要な管理を施しているかどうかを確認することができる。また、事業の譲渡や終了時に取るべき手続きを事前に準備しておくことが可能となる。

9.6　トラストリソースマップ

9.6.1　記載方法

トラストリソースマップの作成目的は各ステークホルダ間でのトラスト関係を明らかにすることである。ここで、トラストには、ステークホルダに対するトラスト、そこで取り扱われるデータに関するトラストの二点が存在する。ステークホルダに関するトラストとしては、ステークホルダの真正認証をどのように行っているかを明確にする。一方、そこで取り扱われるデータの真正認証としては、そのデータが事実に基づくことや、一度生成されたデータが改ざんされていないことの確からしさの確認方法を明確にする。これらの認証は、6.1 に示した認証の形態がある。従ってトラストリソースマップでは、どんな種類の認証が行われているかを明確に表現する。

トラストソースマップは、まずステークホルダリストに記載されたステークホルダを配置し、そのステークホルダ間での認証の有無を、アイコンと矢印により記載する。なお、

ステークホルダの配置は、基本的にはビジネス関係図と同じものを用いることで記載漏れがなくなる。

アイコンだけでなく、必要に応じて詳細を示す簡単なタグ名を付す事で、認証の形態なども表現する。

9.6.2　記載例

記載例として、ドライブレコーダのデータを収集し、個人情報を除去し、第三者に統計データを提供する事業の記載事例を、図 31 に示す。

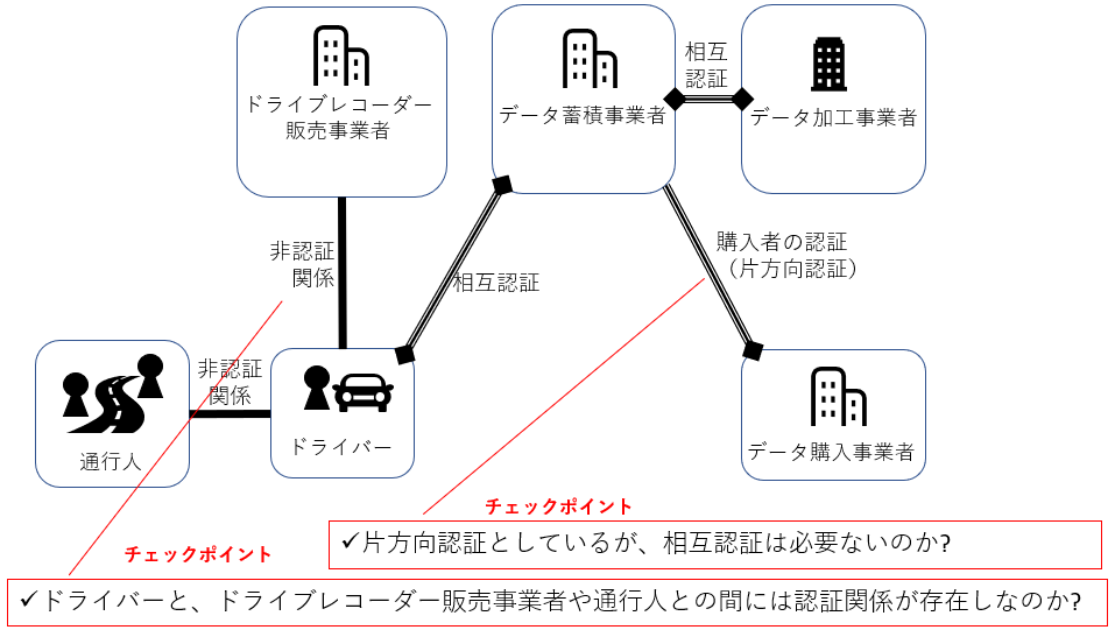


図 31　ドライブレコーダビジネスのトラストリソースマップの記載事例

9.6.3　評価例

図 31 に示す記載例に対して、以下のことが事業上の留意点として顕在化する。

9.6.3.1　ドライバとドライブレコーダ販売事業者の認証

ビジネス関係図では、ドライバとの物品の売買契約を行っている。しかしながら、図 31 のトラストリソースマップには、非認証であると示されている。これは、その売買契約で、契約当事者の確認が行われていない可能性を示唆している。

また、当該事業に利用されるドライブレコーダ製品に対して、なんらかの認証を伴わないとすると、製品そのものにスパイウェアなどが仕込まれるなどのインシンデント時のトレーサビリティに疑義が生じることが判る。

9.6.3.2　通行人とのドライバ間の認証

図 31 では、ステークホルダの一つである通行人とドライバの間は、相互に相手が誰であるかの認証を伴わないことがわかる。

しかしながら、通行人が映り込んだドラレコ映像が第三者に提供される場合、プライバシー原則に照らすなら、その旨が通行人他に通知される必要性が生ずる。この場合、その当事者であるドライバは何らかの形で、自己の真性を示すことが求められるかという論点が存在する。

9.6.3.3　データ蓄積事業者とデータ購入事業者間の認証

図 31 では、データ購入事業者は、データ蓄積事業者を認証してない。このことは、データ購入事業者へのなりすましなどの入り込む余地があることがわかる。

9.6.4　　評価結果からの想定される事業への反映

全体のサービスフローに鑑みて、認証方式に妥当性があるか、また、認証に応じてどこまでのサービスレベルを認可できるかの確認ができる。

9.7　　データフローシーケンス

9.7.1　　記載方法

データフローシーケンスの作成目的は当該事業で利用されるパーソナルデータについて、その発生、又は作成された時点からサービスが完了する時点までのデータの遷移や遷移に対する制御の手順を、時系列に沿って明確にすることにある。

データフローシーケンスは、まずステークホルダリストに記載されたステークホルダを横方向に配置し、そのステークホルダ間でのやりとりを時系列に縦方向に、アイコンと矢印により記載する。

記載にあたっては、アイコンだけでなく、必要に応じて詳細を示す簡単なタグ名を付す事で、手順上とりかわされる情報や ID の形態なども表現する。

9.7.2　　記載例

ドライブレコーダのデータを収集し、個人情報を除去し、第三者に統計データを提供する事業の記載事例を図 32 に示す。

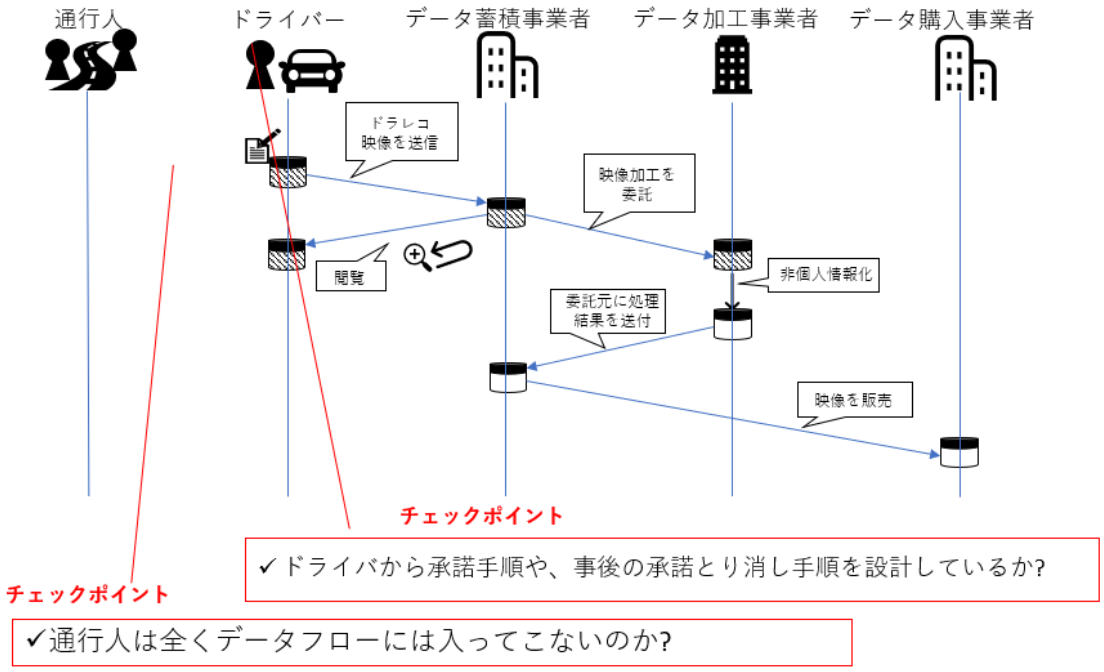


図 32　ドライブレコーダビジネスのデータフローシーケンス記載事例

9.7.3　評価例

図 32 に示す記載例に対して、以下のことが事業上の留意点として顕在化する。

9.7.3.1　通行人は全くデータフローには入ってこないのか?

図 32 のデータフローシーケンスでは、ドライバと通行人の間には、なんら情報のやりとりが存在しないことがわかる。

しかしながら、プライバシー原則に照らして考えると、ドライバはドラレコ映像を第三者に提供しているので、その旨を通行人他に対して通知する必要が浮かび上がる。

9.7.3.2　ドライバから承諾手順や、事後の承諾とり消し手順を設計しているか?

図 32 のデータフローシーケンスでは、ドライバがデータ蓄積事業者に対してドラレコ映像を提供しているが、データ蓄積事業者がデータ加工事業者やデータ購入事業者へデータを提供する際には、なんら通知などが無いことがわかる。この事は、ドライバから提供以後の全てのデータ取り扱いに個別・逐次の関与がなく、包括的なデータ提供がなされていることを示している。

また、このフローシーケンスでは、ドライバが当該サービスの停止や解約を行う場合、提供済みデータの抹消などの手順が、記載時点では明確になっていないことが判る。

9.7.4　評価結果からの想定される事業への反映

サービスフローを確認することができる。手順に誤りが無いかなど、システム設計の確認を行うことができる。

9.8 法制関係表

9.8.1 記載方法

法制関係表の作成目的は、ステークホルダ間に存在する契約や遵守すべき法制を明確化することにある。第三者提供（個情法 23 条 1 項）、業務委託契約、独立行政法人等の保有する個人情報の保護に関する法律など、パーソナルデータを取り扱う事業では、個別の事業に関する行法と併行に考慮すべき情報法制が多数存在するため、これらをリストアップすることで、留意すべき法制を明確にする。

法制関係表は、ステークホルダを縦、横に配置したマトリックスを作成し、その交点に関係する法制や契約をマッピングすることで、網羅性を確認する。

なお、一般的には、このようなマッピングは、弁護士などの専門家に相談の上作成することが適切である。

9.8.2 記載例

ドライブレコーダのデータを収集し、個人情報を除去し、第三者に統計データを提供する事業の記載事例を表 23 に示す。

表 23　ドライブレコーダビジネスの法制関係表記載事例

	ドライバー	ドライブレコーダー販売事業者	データ蓄積事業者	データ加工事業者	データ購入事業者	通行人
ドライバー	NA	販売契約	映像利用に関する同意 個人情報保護法			
ドライブレコーダー販売事業者	販売契約	NA				
データ蓄積事業者	映像利用に関する同意 個人情報保護法		NA	業務委託契約 個人情報保護法	映像利用契約	個人情報保護法
データ加工事業者			業務委託契約 個人情報保護法	NA		
データ購入事業者			映像利用契約		NA	
通行人			（個人情報保護法）			NA

チェックポイント

✓ドライバーとデータ蓄積事業者との間には映像利用に関する同意書が存在。そこには、二次利用（データの加工・販売）の旨の記載が必須であることがわかる。
✓通行人とデータ蓄積事業者との間には、個人情報保護法に関わる可能性があることがわかる。

9.8.3 評価例

9.8.3.1 映像利用の同意書の適用

ドライバとデータ蓄積事業者との間には映像利用に関する同意書が存在し、そこには、二次利用（データの加工・販売）の旨の記載が必須であることがわかる。

9.8.3.2 通行人に対する保護

通行人とデータ蓄積事業者との間には、個人情報保護法に関わる可能性があることがわかる。

9.8.4　評価結果からの想定される事業への反映

ステークホルダ間の関わる契約や制度を概観できる。準備すべき契約や考慮すべき制度の対応策について、これを起点として準備することができる。

【研究開発編】

第10章 パーソナルデータに関わる標準化

パーソナルデータの取扱いは、国内に閉じることなく、広く世界的に様々な取り組みがされている。本書の取りまとめと併行して、国際標準化にも取り組んでおり、これらの活動について解説する。今回のテーマでは、国際標準化等の推進活動とデータジャケットの国際標準化という２つのテーマを実施した。それぞれの概要は次のとおりである。

10.1　国際標準化等の推進活動

10.1.1　目的

・IEEE-SA DTSI 活動の推進：IEEE（the Institute of Electrical and Electronics Engineers）の Data Trading System Initiative(DTSI) WG のリーダーシップをとり、PAR（Project Authorization Request）に対する寄与文章の共同作成を進める。

・ISO/TC 設立の動きに対する協力と連携：将来的に IEEE 規格を ISO 化することを念頭に、必要な要件の調査を行い、関係機関との連携を図る。

・W3C（World Wide Web Consortium）との関係構築の提案：W3C は IEEE とはリエゾン関係にある。一般社団法人データ流通推進協議会（DTA）においてはデータカタログ（DCAT）などで規格を参照しており、W3C とは更なる関係構築が望まれる。今後の国際展開に必要な事項を本書に反映することを目的に調査・連携案を提案する。

10.1.2　実施事項

10.1.2.1 IEEE-SA DTSI（Data Trading System Initiative」活動の推進

IEEE-SA ICCom(インダストリーコネクション委員会）に対して、データ流通に関する標準化を行う PAR(Project Authorized Request)の起草を行うための ICAID ドキュメント「Data Trading System Initiative- Industry Connections Activity Initiation Document (ICAID)」が、2019 年 6 月に DTA により提案され承認された。今後、Data Trading System のための標準化プロジェクトの開始を求める PAR を策定し、2020/4 に IEEE-SA NesCom (New Standard Committee)へのアジェンダとして提案することを目指す。

これらに対するこれまでの取り組みと、今後の予定は下記にようになる。

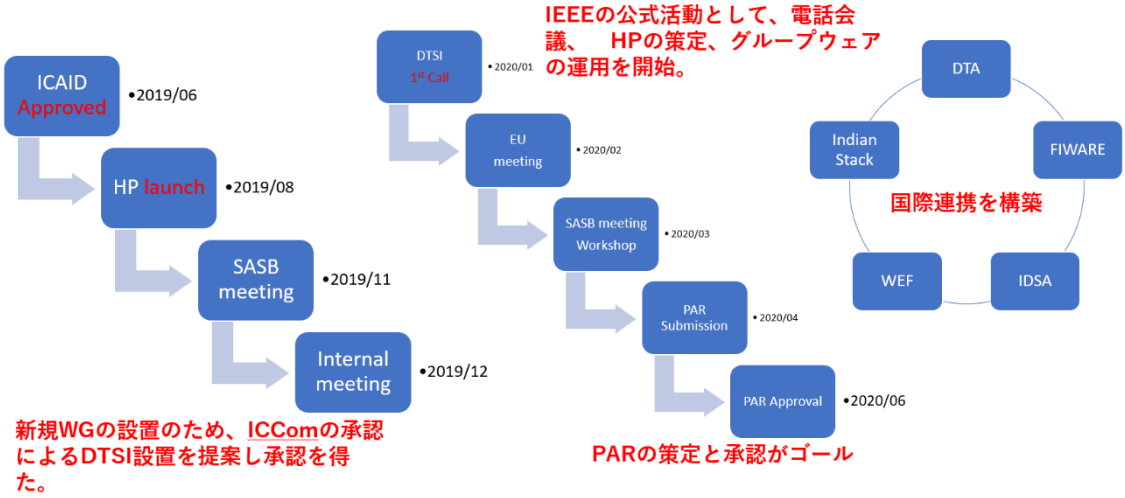


図 33　IEEE-DTSI のこれまでの取り組みと今後の取り組み

これまでの成果物としての、DTSI のホームページは、

https://standards.ieee.org/industry-connections/datatradingsystem.html

また、参加者のためのワークスペースはこちらになる。

https://ieee-sa.imeetcentral.com/dtsi/

ただし、このワークスペースへの参加は、DTSI のホームページに従った参加申請が必要である。

このような標準化活動では、その運営を取りまとめ推進するリーダーシップが必要である。DTSI では、DTA 事務局長の真野が Chair を務めることになった。また、Secretary も DTA が担当することになった。現在、グローバルな規格化の推進のため、外部エキスパートの募集、The World Economic Forum (WEF)、 FIWARE、the International Data Spaces Association (IDSA) らとの連携を進めている。

10.1.2.2 ISO/TC 設立の動きに対する協力と連携

将来的に IEEE 規格を ISO 化することを念頭に、国内体制の連携を強化した。具体的には、2019 年 8 月に DTA 内に国際標準化推進委員会を発足させ、関係する ISO と IEEE 活動の状況が共有できる体制を整えた。

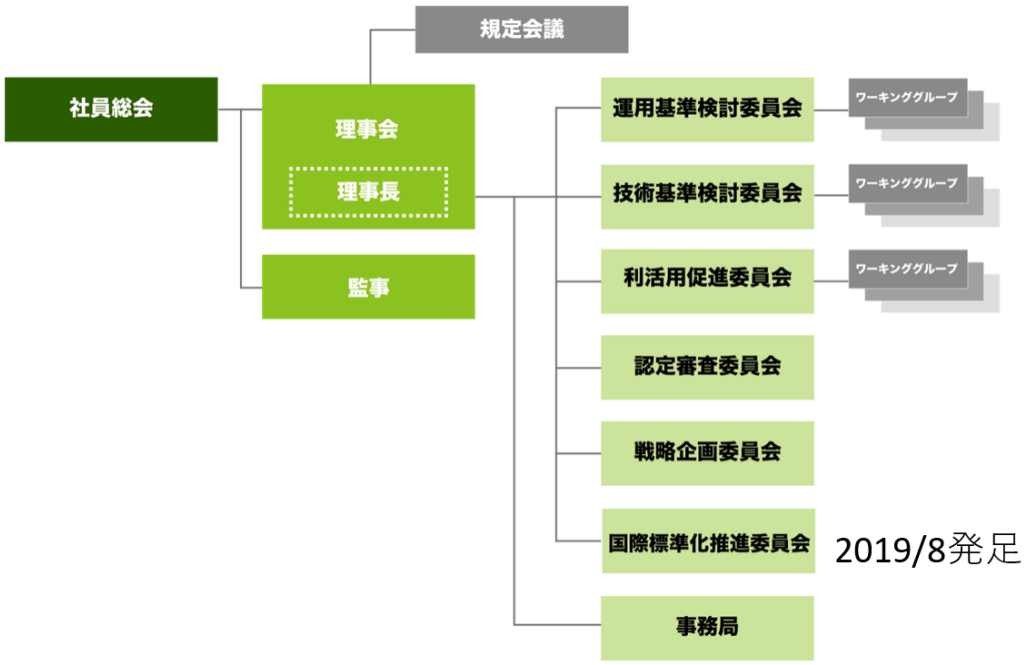


図 34　一般社団法人データ流通推進協議会（DTA）内組織図

10.1.2.3 W3C との関係構築の提案

DTA は 2019 年 10 月 1 日に W3C に加入し、会員として W3C における標準仕様策定に関与できる体制を整えた。

また入会直前の 2019 年 9 月 15 日(日)～20 日(金)に福岡市で開催された Technical Plenary and Advisory Committee Meetings (TPAC)に参加し、関連仕様策定状況を調査した。TPAC は年 1 回開催され、様々な作業部会の対面会合が併催される。タイムテーブルは大会ウェブサイト[56]を参照されたい。TPAC における作業部会会合参加を通じて関連仕様の抽出を行った。当該仕様と策定作業が行われている作業部会は次のとおりである。

- Web of Things Working Group
  - WoT Architecture
  - WoT Thing Description
  - WoT Scripting API
  - WoT Binding Templates
- JSON-LD Working Group
  - JSON-LD (Syntax) 1.1
  - JSON-LD 1.1 Processing Algorithms and API

[56] https://www.w3.org/2019/09/TPAC/schedule.html

  - JSON-LD 1.1 Framing
- Decentralized Identifiers Working Group
  - Decentralized Identifier Use Cases & Requirements
  - Decentralized Characteristics Rubric
  - Decentralized Identifiers Data Model and Syntax

尚、DTA として参照してきた仕様である Data Catalog Vocabulary (DCAT)は、Version 2 が 2020 年 2 月 4 日に勧告となり、策定作業が完了している。DCAT の仕様策定を担う Dataset Exchange Working Group (DXWG)は、会員の多くが公共オープンデータ（public sector information: PSI)関連の組織である。前述の Web of Things など多様な種類のデータを取り扱うための拡張や、仕様間調整の活動はこれからといった状況である。

上記抽出した作業部会の中で、事業期間内である 2020 年 1 月 29 日(水)～1 月 31 日(金)にオランダ・アムステルダムで開催された Decentralized Identifiers Working Group (DID WG) の対面会合を調査した。この対面会合には Open ID Foundation、Identity Commons、Sovrin Foundation、My Data Global といった個人のデータ主権や ID 技術に関する活動を推進している組織の創設者ならびに中心人物が参加している。また産業データ分野の団体からは GS1[57]に所属する Phil Archer も参加している。GAFA による独占的な支配に対する危機感を有する各国政府や企業の姿勢もあり、 DID WG はある程度の影響力をもつ WG としてプレゼンスを確立する可能性があると考える。

発足してまだ半年の WG であり、 DID Identifiers v1.0 (DID-core)と Use Cases & Requirements は FPWD(First Public Working Draft)が公開されてまだ 2 ヶ月、Rubric はまだ Editor‘s draft のステータスである。そのため、各技術文書の詳細を詰めるというよりは、各文書の全体構成の確認や方向性のすり合わせ、関連技術の評価、ユースケースシナリオ整理のための論点整理、W3C 内外のリエゾン戦略などが主な議論の内容であった。

将来有力であると評価できる関連仕様の策定を進める作業部会であることから、DTA としても連携を進めていきたい。また他の関連作業部会とも同様に連携していきたいと考えている。

10.2　データジャケットの国際標準化

10.2.1　目的

データ取引においてデータジャケット（DJ）は、人間中心のダイナミックな創造活動の場を生み出すためのデータセットのダイジェストである。即ち、DJ は直接的には中身を

[57] "GS1" はサプライチェーンの効率と透明性を高めるための国際規格を設計・策定する国際組織である。バーコードや QR コードなどが有名。特定組織の略称ではなく the organization offering one global system of standards に由来する。

明かさずにデータセットの概要を共有できる手段を提供できる。様々な DJ の交換は新たな価値を生み出す創造的な場を提供する。DJ を国際標準化し利用拡大することは、データの価値を高めデータ流通推進に寄与する。このため、DJ を中心とした標準化に関わる文書の作成を目指した。

10.2.2 実施事項

参加者のコミュニケーションが重要なデータ市場において、データジャケット（DJ）を中心とした標準化文書を提示することができた。データの中身を明かさずにデータのダイジェストを共有可能とする記法、そして、DJ を介したコミュニケーション過程とそのレギュレーション（信頼性・創造性を高めるための制約)、その他約束事、DJ の利用事例、関連して有効となる技術について記載した。

具体的には

（1） DJ が含む要素やその論理的位置づけ：コミュニケーションの前提知識となる

（2） 信頼性と創造性を高めるコミュニケーション IMDJ（Innovators Marketplace on Data Jackets）のプロセスと参加者同士の約束事

（3） DJ の使用事例

（4） IMDJ におけるコミュニケーションと思考の支援技術

を標準化対象とする。

活動に関する詳細は、データジャケットの国際標準化に関わる報告書にまとめた。

第11章 今後の進め方

11.1　アーキテクチャの継続的な維持・発展

今後のアーキテクチャの継続的な維持・発展に資するには、我が国内だけでなく広く国際標準化を進め、周辺各国との政策協議が必要となる。

そこで今年度は下記を実施した。

・DTA 内に国際標準化委員会を組織した。この中で、ISO 及び IEEE プロジェクトを相互に連携して進められる環境を構築した。

・フォーラム系では FIWARE との MOU を結び、IDSA との MOU 締結の方向で手続きを進めた。また、国内においては、RRI(ロボット革命イニシアティブ)とも連携し、IDSA との統合的窓口は DTA が対応することになった。

今年度の活動をもとに、次年度以降において、以下のような取組みを継続して行うことが望ましい。

11.1.1　普及促進に向けた啓蒙

本研究は、内閣府の「戦略的イノベーション創造プログラム（SIP）第 2 期／ビッグデータ･AI を活用したサイバー空間基盤技術」の一環として行われたが､本書の理解と普及、社会実装を進めるためには、その啓蒙のためのセミナーなどの啓蒙活動を継続的に行う必要がある。本書は、特定の分野やステークホルダに限定しないため、さらに個別の事業などに合わせた、より実践的なハンズオンセミナーなどが有効となる。

このような啓蒙活動は、官民共同のもとに公的支援のもとに展開されることが、普及の鍵となる。

11.1.2　アーキテクチャの持続的改版

アーキテクチャは、技術や制度と連携し持続的な改版を行うことが重要となる。特に、現在は、様々な機器がインターネットに接続され、自動運転や自動検診、AI の活用などにより、従前の法体系では十分にその社会的価値が享受できない場合も生じている。

特に、パーソナルデータは、個人の人権やプライバシーという、社会生活に重大な影響を及ぼす。そこで、法制やビジネス、制度の各視点から持続的に見直し、改定や修正を促すためのガバナンス体制を確立することが望ましい。

11.1.3　国際標準化への寄与と推進

パーソナルデータの取り扱いについては、世界的な課題として国の内外を問わず議論が行われ、日々新しいガイドラインやステートメントが発表されている。このため、我が国の国内だけに閉じず、広く国際展開が可能な標準化へと進めることが望ましい。

国際標準化において、ITU/ISO など、国や地域を代表する形態と IEEE や IETF などの民間や個人を中心とした形態の SDO(Standard Development Organization)があるが、い

ずも最終的にはWTOにおける批准が大きな効果を発揮する。

そこで、本研究の標準化展開においては、ISOにおける活動と連携するIEEEでの活動を中心に、リーダーシップをもって国際標準化を推進する予定である。

既に、本研究の成果展開の場の一つとして、IEEE では DTSI (Data Trading System Initiative)が設立されており、ここではアーキテクチャが成果展開として期待されている。国際標準化は、その適切なプロセスとガバナンスのため、多くの場合その出版までは数年の期間を要することから、これらの活動を持続的に行う体制を整えることが重要となる。

すでに、我が国では関係官庁と連携し、これらの標準化活動の調査や推進を進めており、これらの活動が適切に推進されることを期待している。

11.1.4　採用に向けたコンフォーマンステストや認定の検討

標準仕様やガイドラインなどは、それらを実社会において導入し実用化されることが最終的なゴールである。世界的にみても普及し社会実装される標準仕様の背景には、仕様だけでなく、それらの導入者に対するコンフォーマンステストや認定制度が用意され、確実な社会展開や、導入者へのインセンティブ、市場優位性の確保が示されている。

これらの活動は、民間におけるフォーラムが、その認定サービスを提供し、認定書や認定ロゴの発行、市場啓蒙のためのマーケティングを担うことが多い。

そこで、本研究の成果展開においては、国の内外を問わず民間のフォーラムとの連携を図り、事後の展開を視野に入れた活動を継続する予定である。

11.2　メンテナンス

本書を含む成果物は、内閣府およびDTAの用意するホームページにて公開する。

https://www8.cao.go.jp/cstp/stmain/20200318siparchitecture.html

https://data-trading.org/sipb-1_personaldataarchitecuture_dta/

ここには、ユースケースシナリオテンプレートを再利用可能な形（PPTファイル）で公開され、まずは興味を持つ事業者は自身のビジネスシナリオをこれらのツールを使って表現することが可能な形態とした。

しかしながら、このままでは結果的に派生物だけが拡散し、アーキテクチャがもつべき統一性が損なわれ、結果として持続的発展が阻害される恐れがある。そこで、今後は、改版や新しいユースケースの登録などのプロセスを明確にし、それらに取り組むためのサイト運営なども必要となる。また、アイコンなどは、既存の意匠などとの衝突を避けるためにも、標準化や意匠登録を行うための仕組みを構築する必要がある。

DTA として次年度以降は、このようなメンテナンスのためのサイト構築やプロセスの明確に取り組み、利用促進を図る予定である。また、個別に提供される提案や代案について、適切で公平なプロセス審議を経て、採用された修正を反映させていく予定である。

第12章 【付属資料】

下記２種の成果物が、内閣府の HP[58]及び DTA の HP[59]より公開予定である。

リファレンスアーキテクチャ用語・定義書

本書公開時点で８３用語、分類別で、全般１６、情報１５、データ７、処理１４、契約・トラスト１２、事業モデル１２、その他７を収録した。

データジャケットの国際標準化報告とその概要

成果報告書とその概要書を公開した。

[58] 内閣府の HP:　https://www8.cao.go.jp/cstp/stmain/20200318siparchitecture.html

[59] DTA の HP:　https://data-trading.org/sipb-1_personaldataarchitecuture_dta/