

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

# **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**

2020年3月18日初版

2020年3月24日改定

一般社団法人データ流通推進協議会

# パーソナルデータ分野に対する課題

## ■課題

個人の課題：データ扱いを把握・制御できない不安

企業の課題：企業・業界を超えたデータ流通・活用が進まない

⇒便益の見える化

⇒魅力的サービスの創出

## 背景

第5期科学技術基本計画(2016年)  
**Society5.0の提唱と実装**

**官民データ活用推進基本法**

**デジタル手続き法案**

サイバー空間

データ連携  
による融合

フィジカル空間

制度設計から  
社会実装へ

## 課題

### 個人の課題

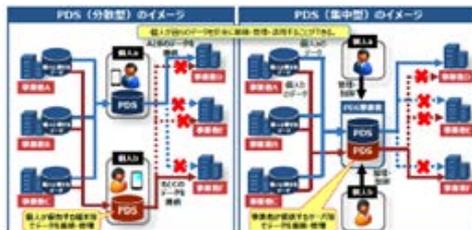
データ扱いを把握・制御  
できない不安

⇒便益を実感できない不  
満や不公平感

### 企業の課題

企業・業界を超えたデー  
タ流通・活用が進まない

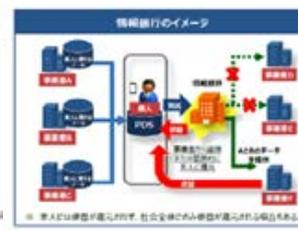
⇒魅力的サービスが創出  
がされない



PDS



データ取引市場



情報銀行

# 研究開発の目的

## ■目的・狙い

### 目的

個別分野を超えた総合的なアーキテクチャの  
グラウンドデザインの整備

- アーキテクチャ設計（スタックモデルも含めた体系的設計図）
- 情報銀行連携
- 分野間データ連携（標準仕様の展開で連携を加速）
- 国際標準化の推進

### 狙い

実務者と豊富な標準化経験者の連携により、  
実ビジネスの創出を支援

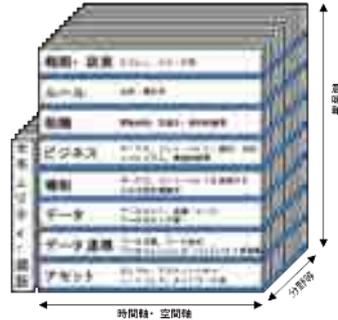
- データ流通市場に関わる事例に基づいてS5RA(Society5.0 Reference Architecture)を分解・整理（⇒仕組みの見える化）
- 実務者会議等を運営し、成果物セットを策定
- 国際的標準化団体で本成果物の標準化スキームを構築・リーダーシップを取る
- 便益の見える化、サービス共創実現、データトレード・チャート創造（再委託先：東京大学）

# 研究開発の実施内容と成果

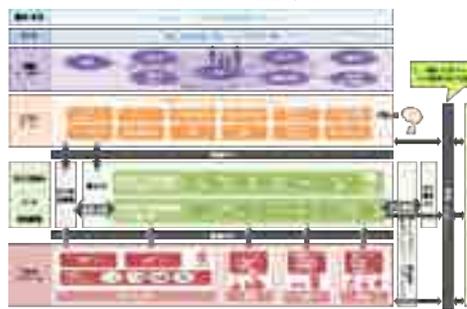
## モデル



## S5RA



## 分野間連携

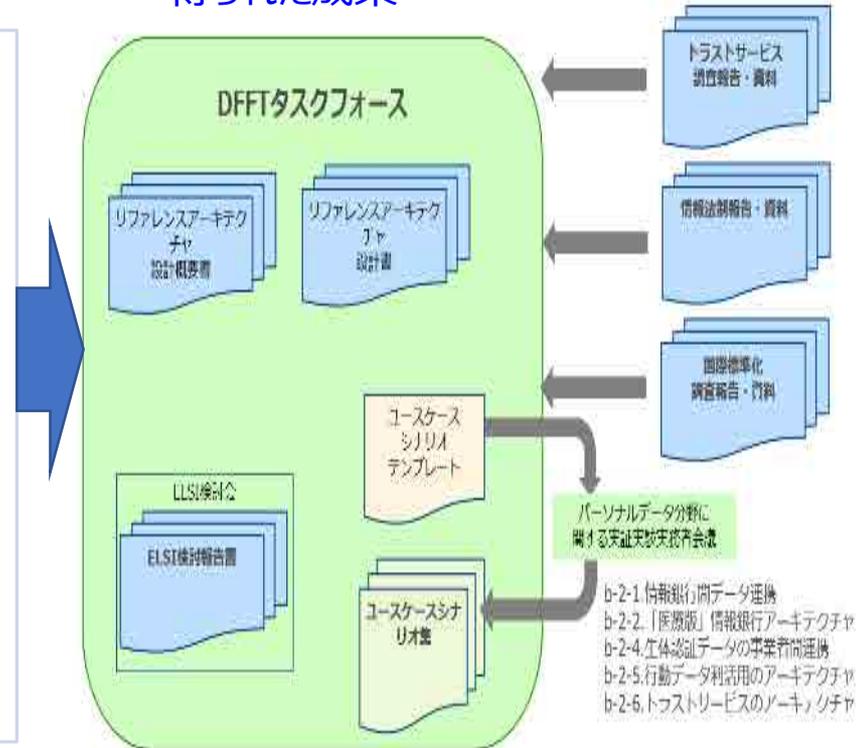


## 実施した活動

- ユースケースを構成する要素の抽出・整理**：「分野間データ連携基盤」の実施者と協議し、アーキテクチャ構築に反映
- アーキテクチャ構築**：アーキテクチャ設計・UCシナリオ策定、SIP DFFT TFの設置&運営、外部有識者や監督官庁連携
- ルール・制度、ビジネスモデル等の検討**：ELSI(Ethical, Legal and Social Issues)検討会にて報告書取りまとめ
- アーキテクチャの継続的な維持・発展に資する体制の検討**：フォーラム系やデジュール系標準化団体との長期協業関係の構築。国内関係協議会での承認と運営規則の策定
- 国内外パーソナルデータの活用に関する情報収集と分析**：WEFと連携
- 実証研究による検証**：「パーソナルデータ分野に関する実証実験実務者会議」(仮称)を設置し各設計書に反映
- パーソナルデータ分野アーキテクチャ検討会議の設置と運営**：有識者の助言のもとに検討する会議運営
- 標準化等の推進**：IEEEにてDTSI(Data Trading System Initiative)活動実施。ISO/TC提案。データジャケット (アイデア創出ツール) 標準化インプット、W3C等との協力協定書を締結・協業、CA/Browser Forum活動

次ページ以降で説明

## 得られた成果



# リファレンスアーキテクチャ(設計)書とは

## 設計書の定義

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となる設計書。

## 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り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。

## 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)

## 制約事項

この設計書は、パーソナルな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。

この設計書は、パーソナルな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。

## 使い方

この設計書に照らして、自身のビジネスを解析し課題を明確にするチェックリストとする。

# リファレンスアーキテクチャ(設計)書の構成

## 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やその進捗に関わらずぜひご一読**いただくことを想定している。

## 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り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。

## 研究報告編

- 本書の作成にあたり、当協議会では、国内での有識者会合および実証実験事業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。これらの活動および、その調査内容について報告する。
- 各事業者がより**深い検討や国際展開を検討する際の参考**としていただきたい。

## 付属資料

- 用語の定義を取りまとめた、別冊「用語・定義書」

# 導入編

# 導入編の構成

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ぜひご一読いただくことを想定している。

- 第2章 本書の目的と利用
- 第3章 基本理念
- 第4章 パーソナルデータを扱う事業モデル
- 第5章 パーソナルデータを扱う上で必要なELSI
- 第6章 パーソナルデータと関連法制
- 第7章 トラストサービスの概要と現状

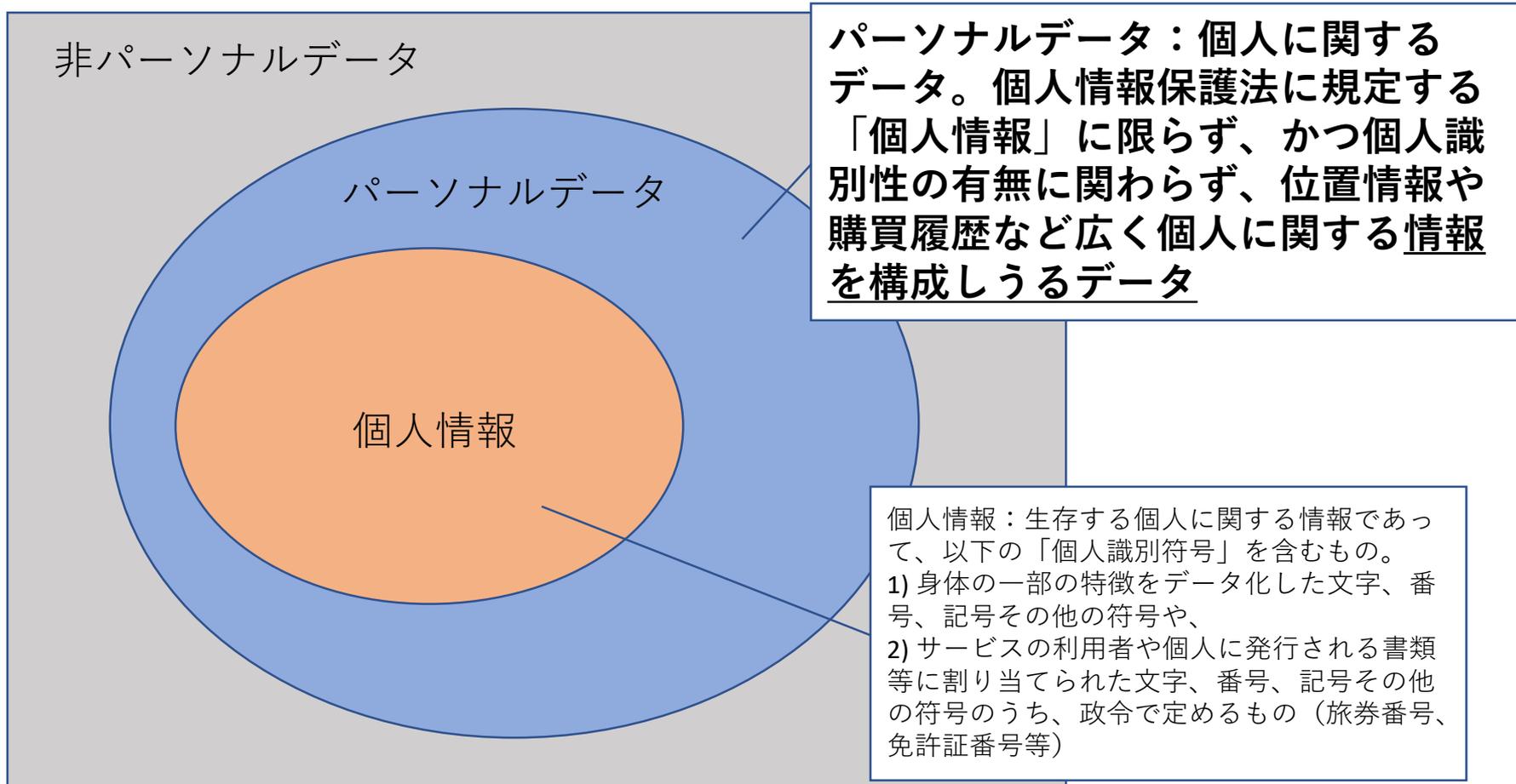


# 基本理念



# パーソナルデータとは

- 改正個人情報保護法で定義される「個人情報」よりも範囲は広い



※改正個人情報保護法(平成29年施行)

# データと情報

## データ Data

- 「**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。**」

## データセット Dataset

- 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。

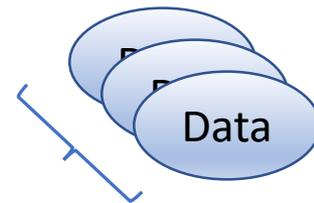
## 情報 Information

- 事実、事象、事物、過程、着想およ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)およ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。
  - (ISO/IEC 2382-1, JIS X 0001)

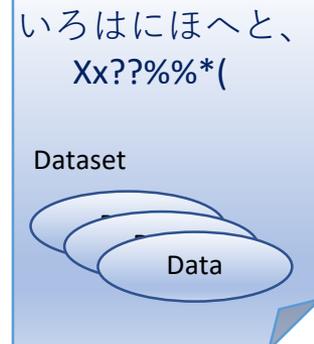
Data



Dataset



Information



# Personally Identifiable Information(PII)

## Personally Identifiable Information(PII) とは

- 情報が、その情報と関連する自然人とを結びつけるために利用できるもの。
- 情報が、直接または間接的に関連する自然人を特定している特定しうるもの。
- (ISO/IEC 29100:2011 Amendment 1: 2018 における定義)

# データ・オーナーシップとは

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。

**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)

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、**限定的**である。

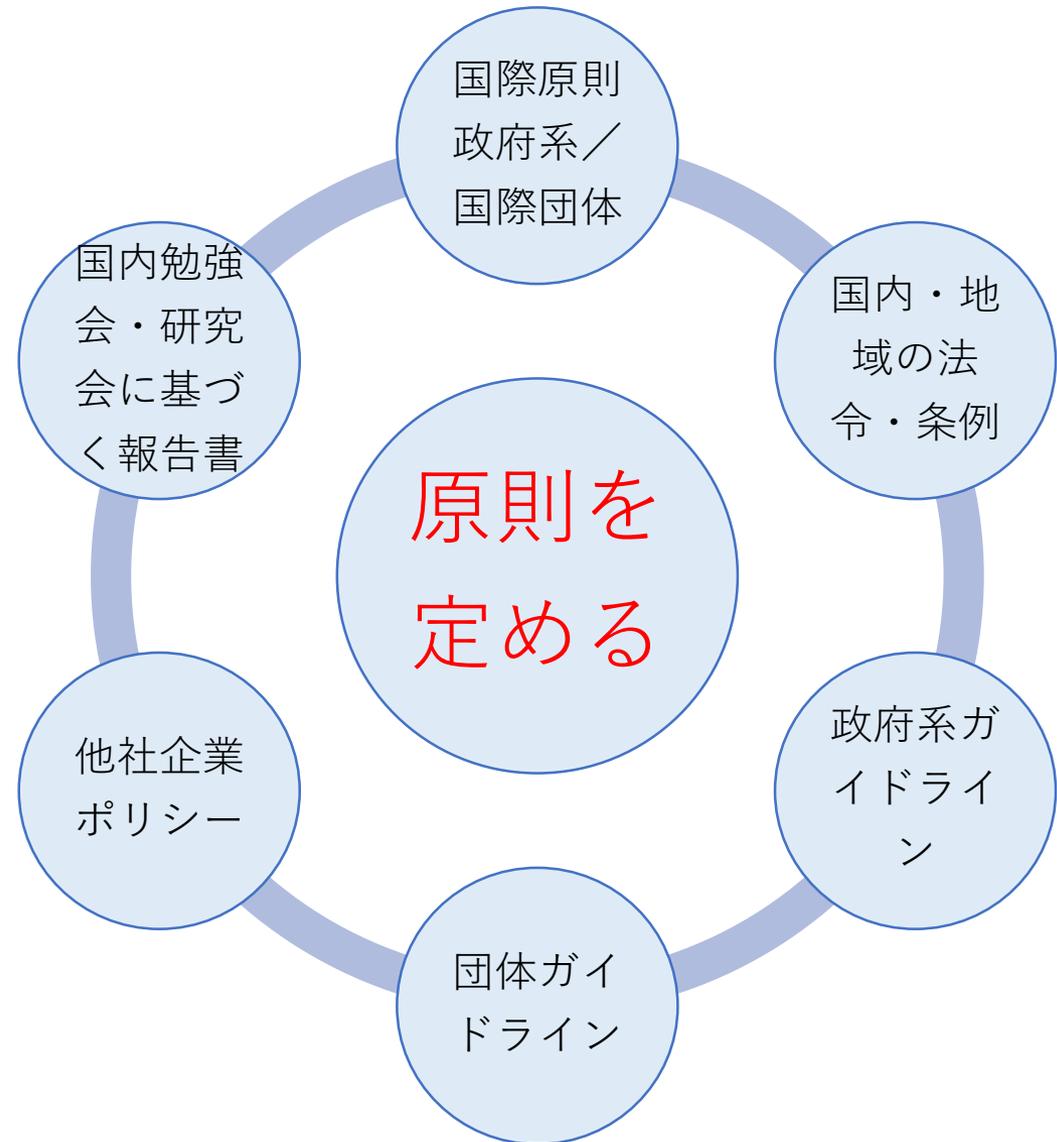
データの**保護**は原則として**利害関係者間の契約**を通じて図られる。

「データ・オーナーシップ」という言葉の**法的な定義**はない。

「データに対する**所有権を観念できる**」という意味ではない。

# パーソナルデータを取り扱う上での原則

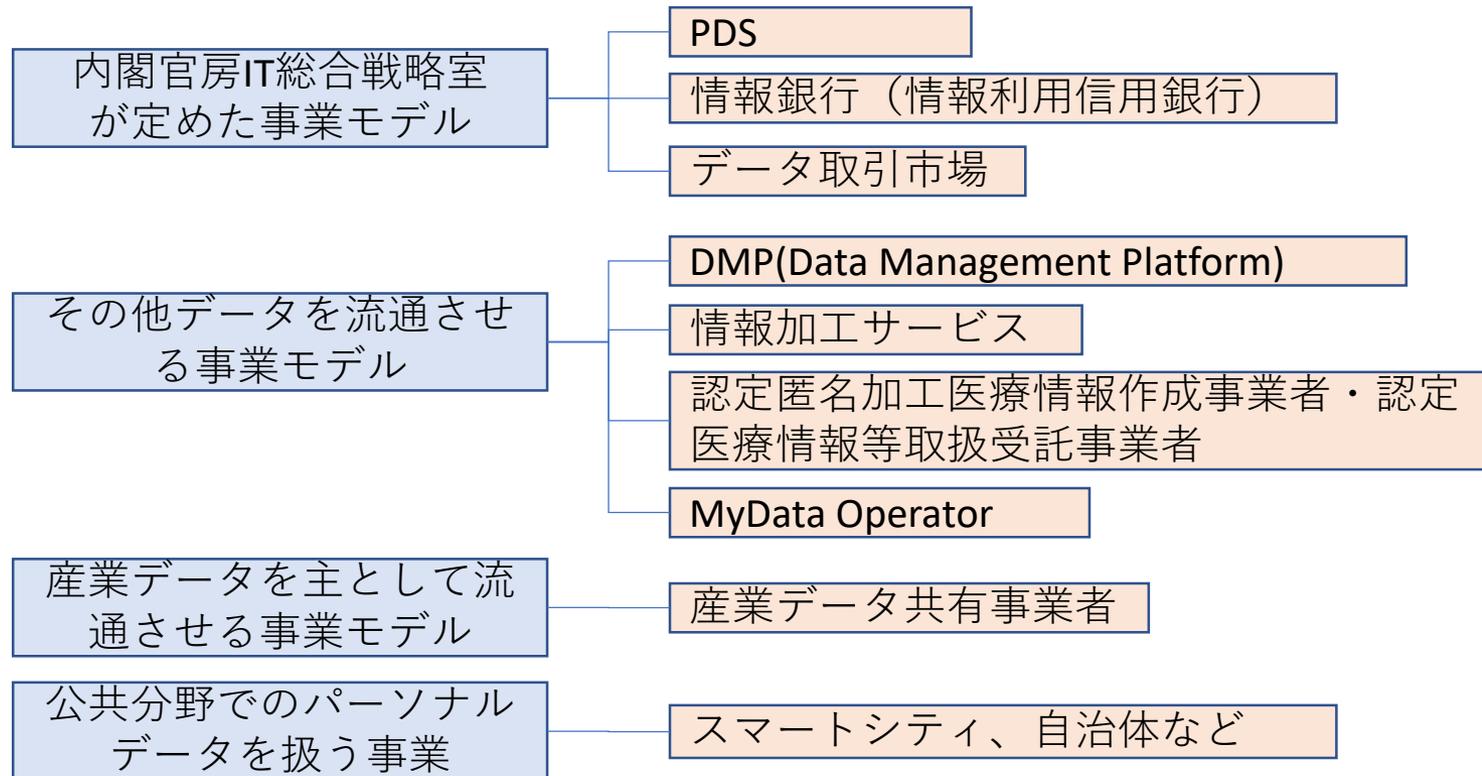
- パーソナルデータの取り扱いについては、ISO/IEC 29100、OECDプライバシー8原則、米国FTC FIPPs(Fair Information Practice Principles), OECD8原則、など **様々な取り扱い原則**が存在する。
- また、各国や団体、企業などが定めガイドラインなど、**事業に関する規範が多数**存在している。
- これらにおいて、その分類などは異なるが、その**目指す**ところ、あるいは**前提**とするところに大きな**齟齬**はない。
- そこで、パーソナルデータを取り扱う事業を行う者は、第五章および別冊の「パーソナルデータ分野に関するELSI検討会報告書」を一読し、**自らの原則を定める**ことが重要となる。



# 事業モデル

# 事業モデルの確認

- 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、あるいは**疑義**がある事業者は、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**いただくことを期待している。





# ELSI(Ethics, Legal, and Social Issues)



# パーソナルデータのアーキテクチャー（ルール層）

ルール層においては、**法制度に留まらず**、広義の社会規範やPEST分析における**社会的要因をスコープに入れるべき**ではないか？

## P:Politics

(政治的要因)

規制など市場のルールを変化させるもの

- ・法律、法改正（規制・緩和）・税制、現在・増税
- ・政治、政権交代 ・裁判制度 ・政治団体、デモ

## E:Economy

(経済的要因)

景気や経済成長など、価値連鎖に影響を与えるもの

- ・景気動向 ・経済成長率 ・物価 ・為替 ・株価
- ・金利 ・原油 ・消費動向

## S:Society

(社会的要因)

人口動態の変化など需要構造に影響を与えるもの

- ・人口動態 ・密度 ・構成 ・流行 ・世論 ・世帯
- ・宗教 ・教育 ・言語 ・高齢人口 ・少子化

## T:technology

(技術的要因)

I Tなど、競争ステージに影響を与えるもの

- ・インフラ ・I T活用 ・イノベーション ・特許
- ・新技術、技術開発

# 6つの基本要件と3つの行動に関する提言

## 6つの基本要件

- 基本要件① グローバルな目線の必要性
- 基本要件② 責任あるビジネス、バリューチェーンの推進
- 基本要件③ 消費者（個人）を主役に据えた事業全体のデザイン
- 基本要件④ 消費者目線を踏まえた通知および同意
- 基本要件⑤ フェアネス
- 基本要件⑥ 透明性と説明責任

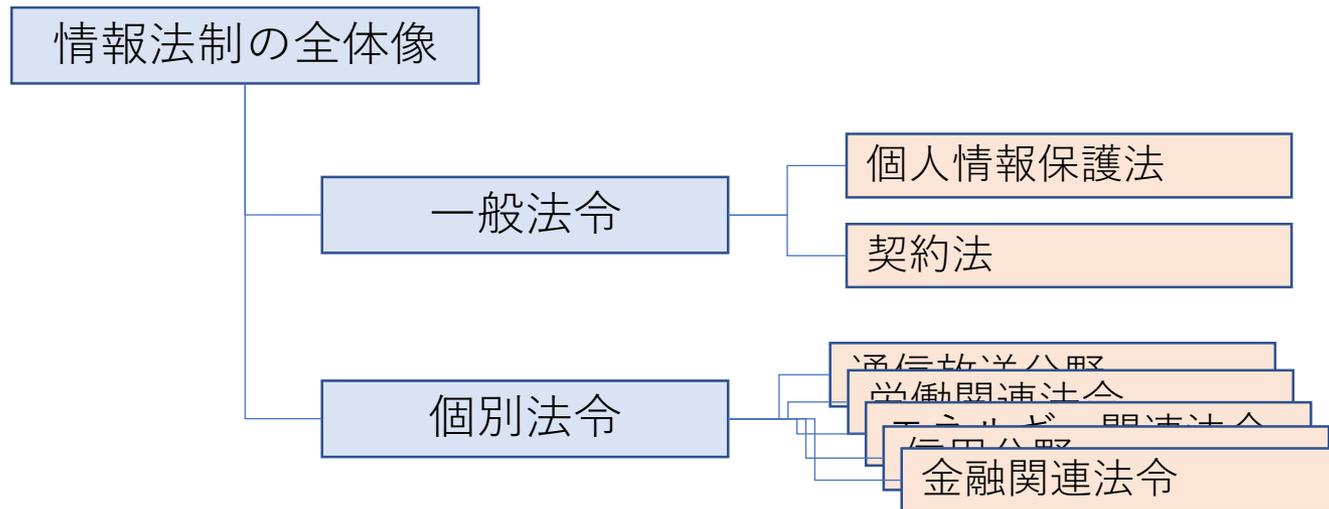
## 行動に関する提言

- 認定制度の創設
- 認定制度自体のブランド力強化
- 市民社会との対話と共働



# パーソナルデータと関連法制

- パーソナルデータの取り扱いでは、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り扱いなどでは、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」の概要を解説する。





# トラストサービスの概要と現状

# トラストサービス

- 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。
  - ① 第二節 認証の種類
  - ② 第三節 認証と認可
- 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照とするために、外部の学術研究者により実施した「トラストサービス調査報告」の概要を簡潔に解説する。
  - ③ 第四節 欧州の取り組み（eIDAS規制）
  - ④ 第五節 米国の取り組み（トラストフレームワーク）
  - ⑤ 第六節 日本の取り組み

# 認証の種類、認証と認可の違い

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**を必要に応じて行う必要があるが、この認証には以下のようなレベルが存在する

- **未認証**
  - 認証をしない
- **片側認証**
  - 関連する人や組織、モノの対において、片側だけが相手を認証する。
- **相互認証**
  - 関連する人や組織、モノが相互に相手を認証する
- **第三者認証**
  - 関連する人や組織、モノが第三者の介在により相手を認証する

- **認証 Authentication**
  - 対象の人や組織、モノの正当性を確認すること。
- **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。