戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

Data Trading Alliance

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

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**　　**⇒便益の見える化**
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

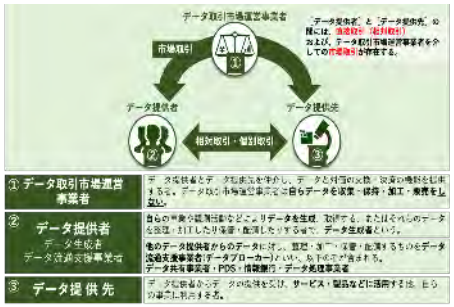
実務者と豊富な標準化経験者の連携により、実ビジネスの創出を支援

- 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）

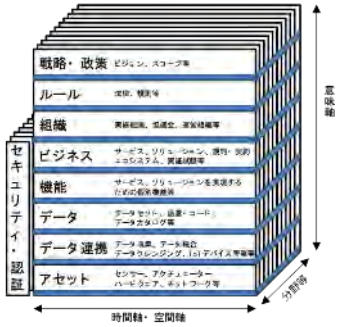
研究開発の実施内容と成果

Data Trading Alliance

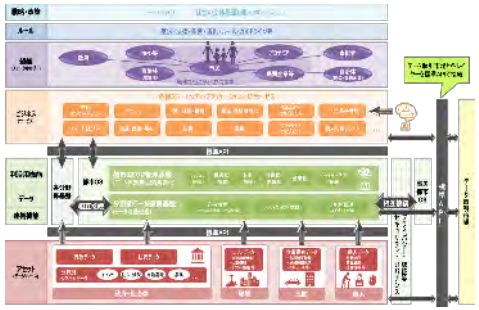
モデル



S5RA



分野間連携

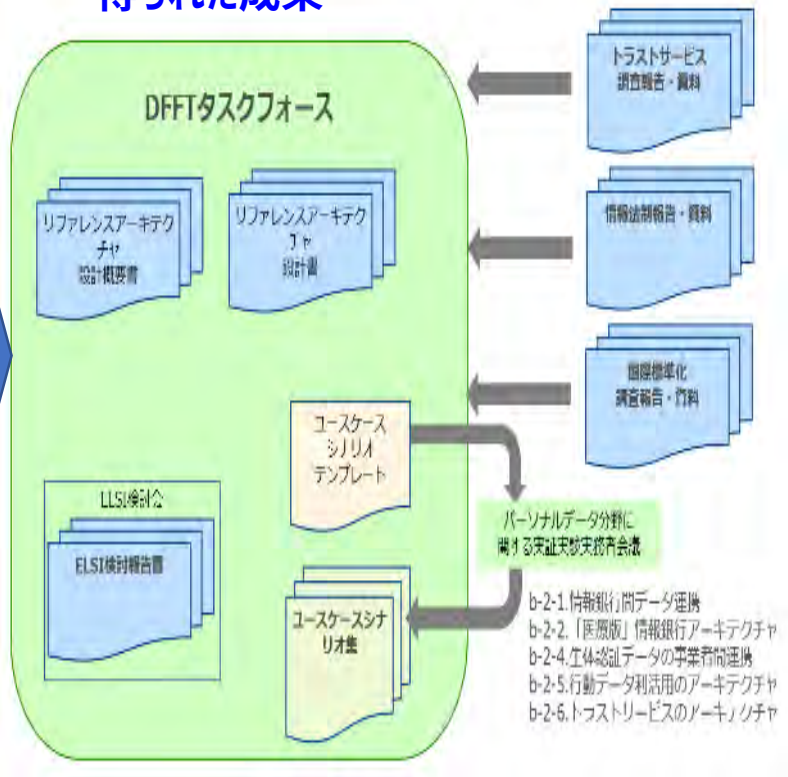


実施した活動

1. 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
2. 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
3. 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
4. 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
5. 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
6. 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
7. 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
8. 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（アイディア創出ツール）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、バ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、バ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

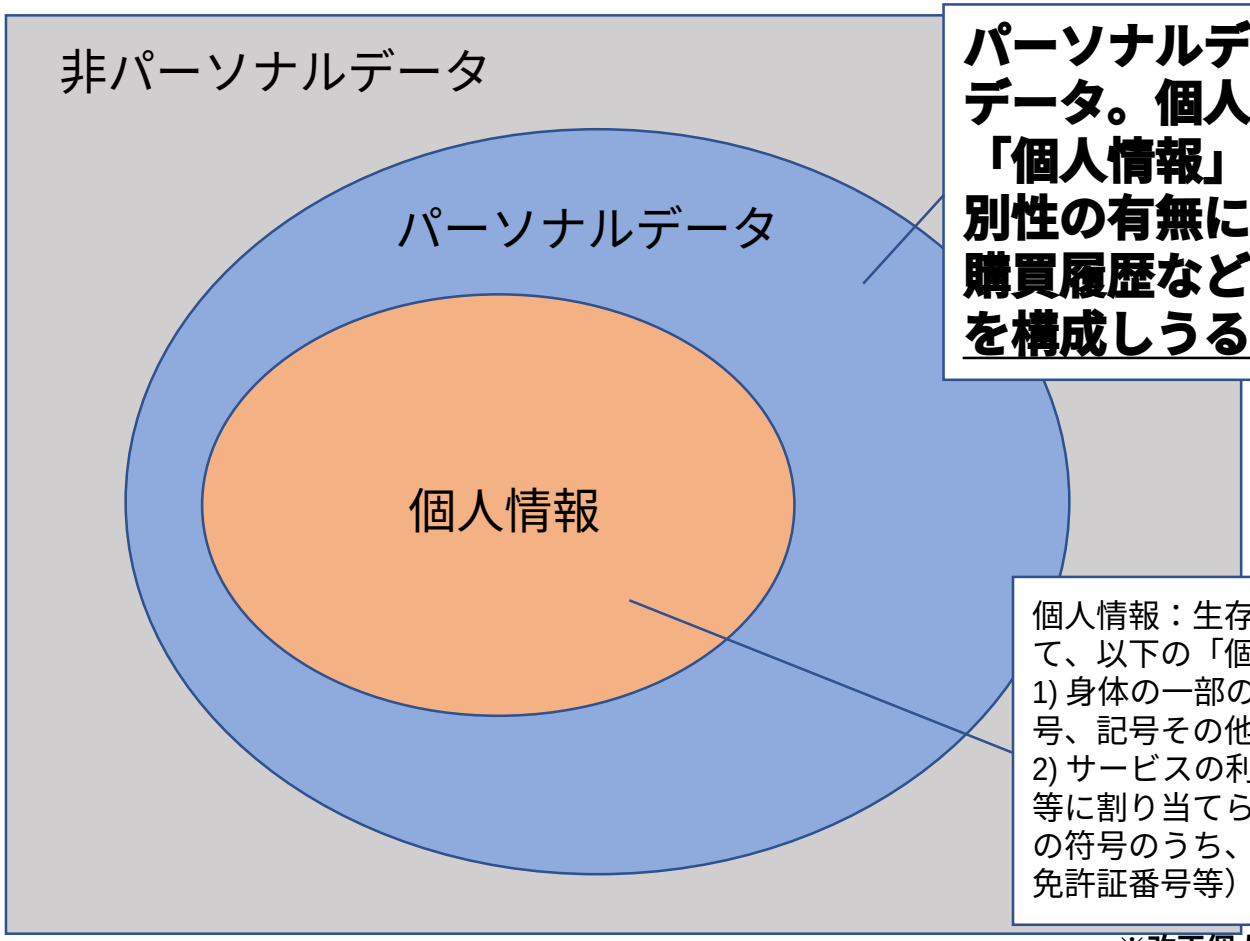
パーソナルデータを取り扱う事業者が理解し、または留意すべき事項を解説しており、特定の事業や計画の実態の有無やその進捗に関わらずぜひご一読いただくことを想定している。

- 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



パーソナルデータ：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

個人情報：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うち、政令で定めるもの（旅券番号、免許証番号等）

※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

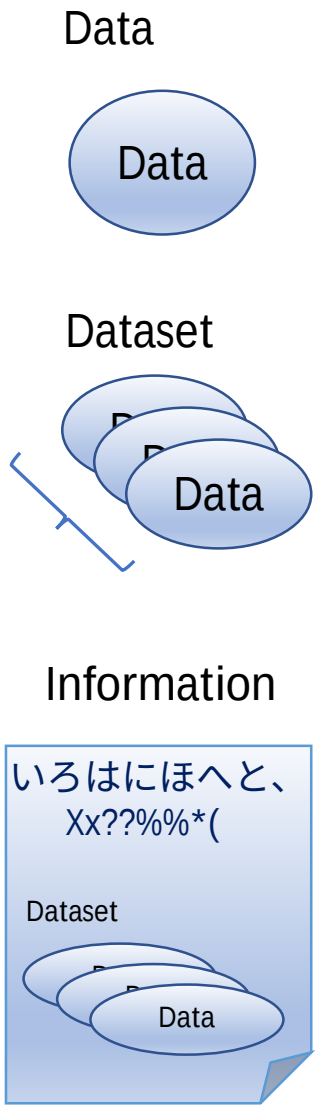
- 「**データとは**、情報の表現を構成する要素であり、伝達、解釈または処理に適するように**形式化され**、複数のデータの組み合わせにより、**情報を構成しうるもの**である。」

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 Trading Alliance

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てできない**

(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。

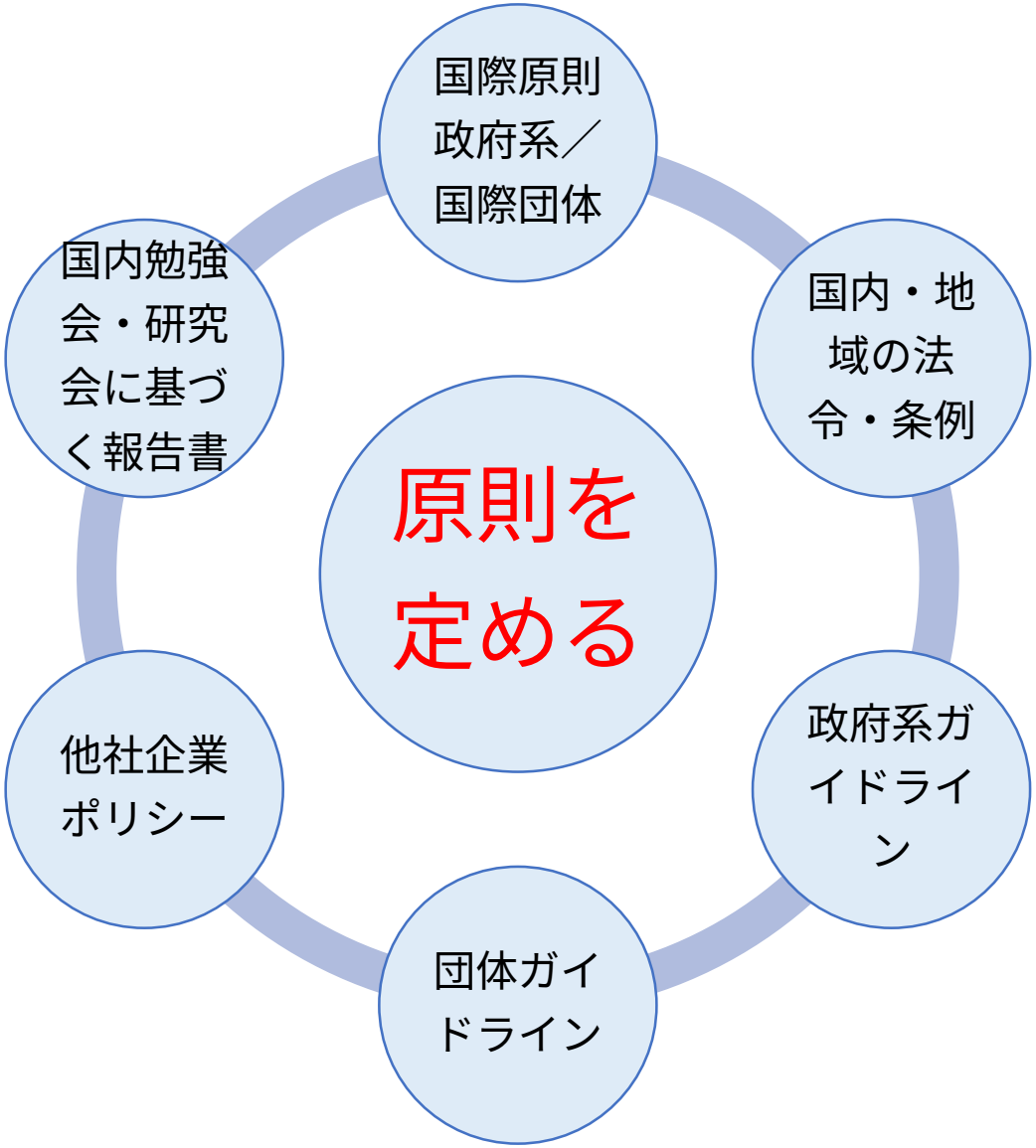
データの**保護は**原則として**利害関係者間の契約**を通じて図られる。

「**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

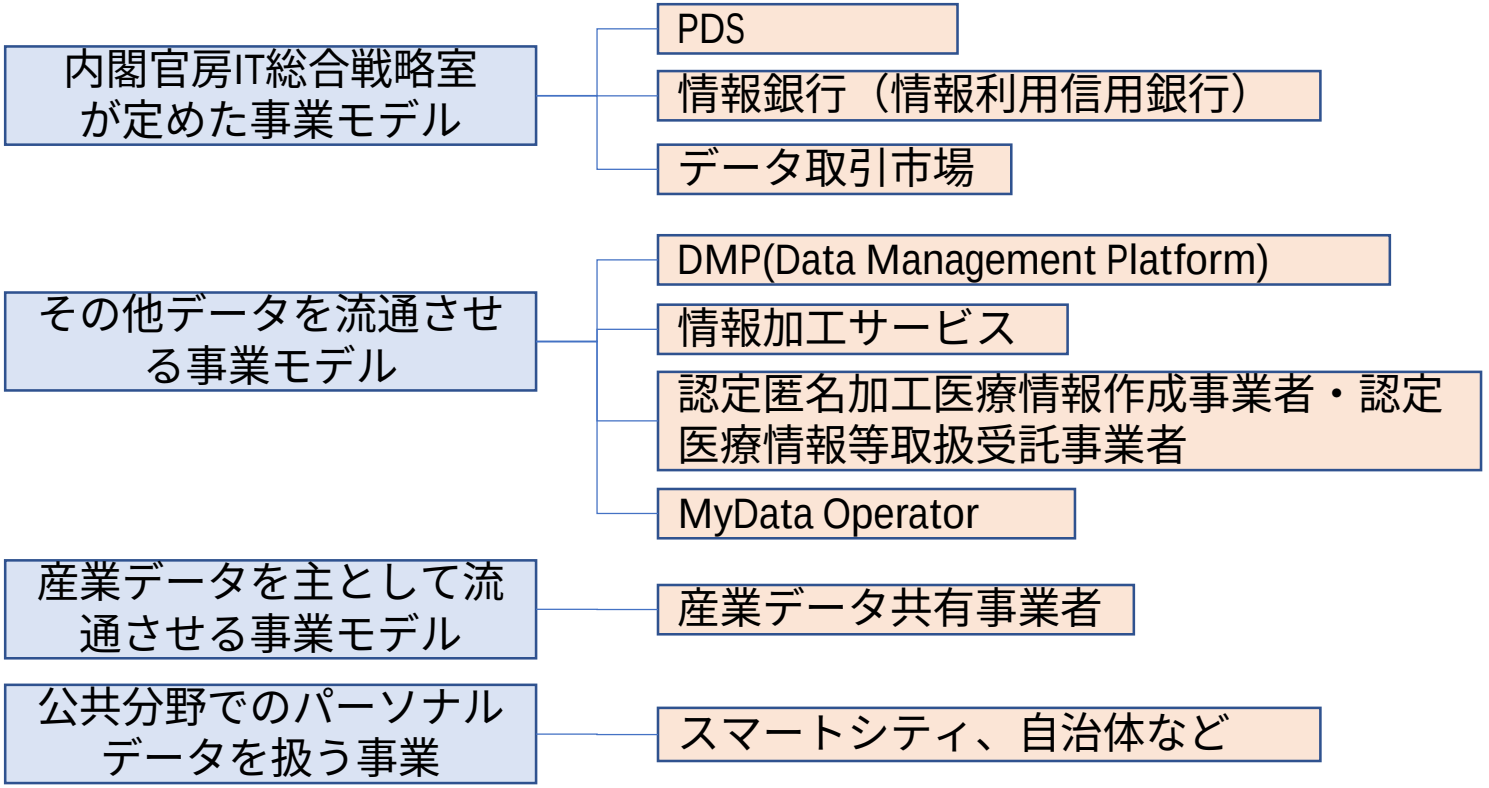
- パーソナルデータの取り扱いについては、ISO/IEC 29100、OECDプライバシー8原則、米国FTC FIPPs(Fair Information Practice Principles), OECD8原則、など様々な取り扱い原則が存在する。
- また、各国や団体、企業などが定めガイドラインなど、事業に関する規範が多数存在している。
- これらにおいて、その分類などは異なるが、その目指すところ、あるいは前提とするところに大きな齟齬はない。
- そこで、パーソナルデータを取り扱う事業を行う者は、第五章および別冊の「パーソナルデータ分野に関するELSI検討会報告書」を一読し、**自らの原則を定める**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　・老齢人口　・少子化
T:technology（技術的要因）	**ＩＴなど、競争ステージに影響を与えるもの** ・インフラ　・ＩＴ活用　・イノベーション　・特許 ・新技術、技術開発

検討結果）
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

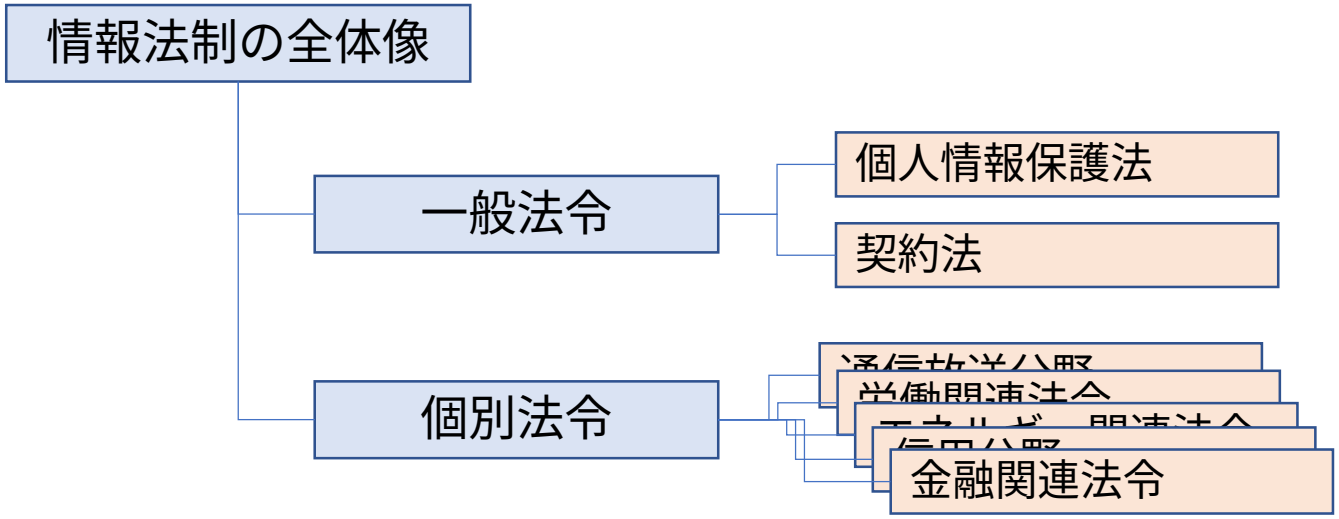
行動に関する提言

- 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、バ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。

活用編

活用編の構成

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

- 第８章 用語・定義
- 第９章 リファレンスアーキテクチャ(設計)書
- 第１０章 ユースケーステンプレートの使い方

用語・定義

用語・定義集

定義項目

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たもの。当該用語の利用範囲を規定するものではなく、定義集の整理の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。

用語

•当該用語の日本語表記

英語表記

•当該用語の英語表記

本書での定義

•当該用語の本書における定義

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

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

アイコン

•本書およびユースケースなどで当該用語を表す場合のアイコン

分類の内訳

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。

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

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

データ処理

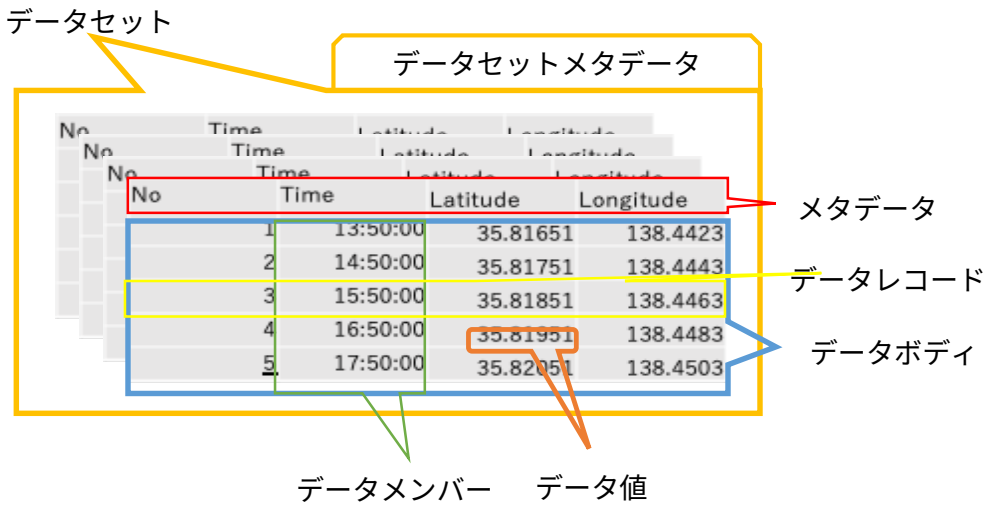
•データまたは、データセットの処理に関する用語

契約・トラスト

•契約・トラストに関する用語

用語・定義 集（一部抜粋）

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	アイコン
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ーの集合	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	データボデイ、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	



本書でのデータセットのアイコン定義

個人データを含まない場合

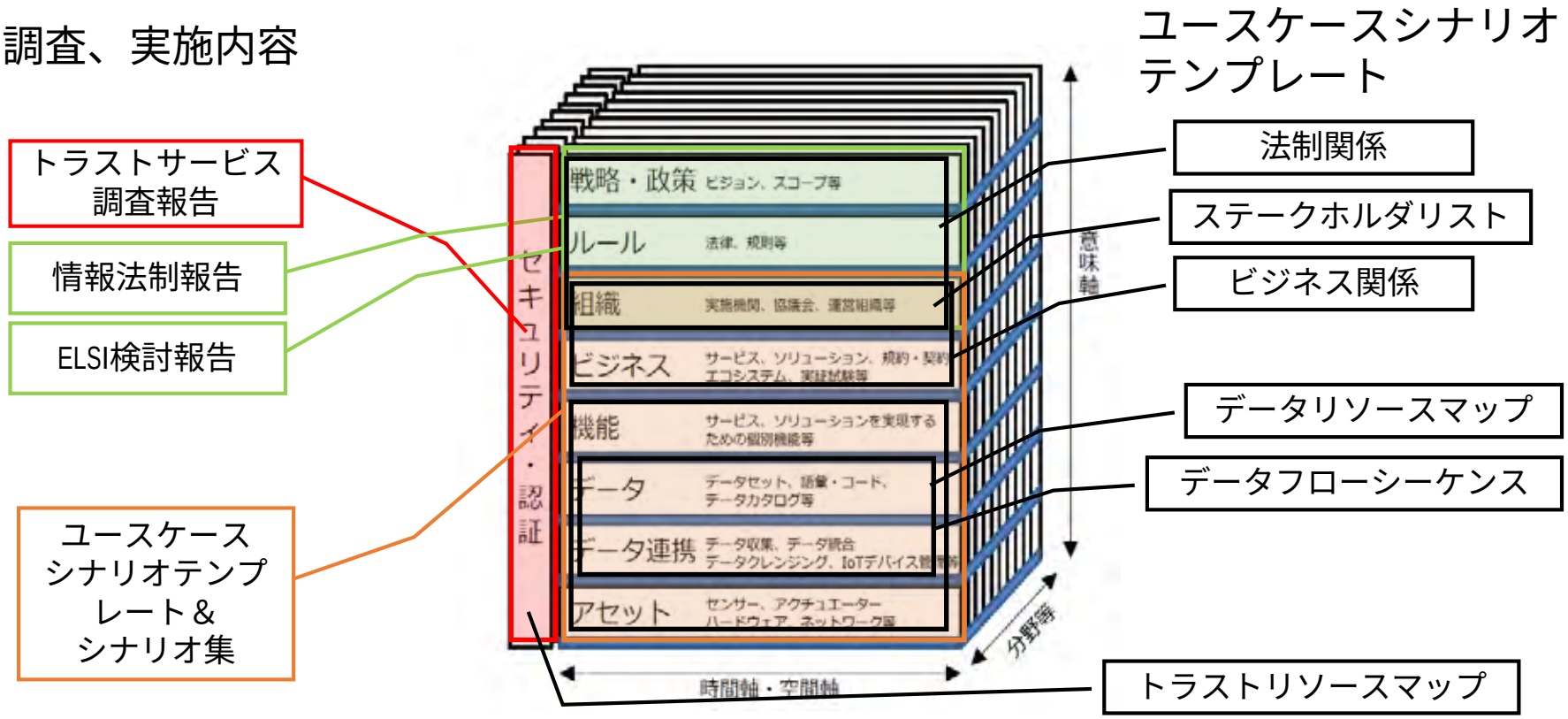
個人データを含む場合

仮名化された情報の場合

本書でのデータセット保管場所定義

アーキテクチャ

Society5.0 RAとの実施事項マッピング



（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」公募要領におけるSociety 5.0リファレンスアーキテクチャ図を記載）

Society5.0　RAと本書での実施事項との対応関係。具体的な利用を促進するためのユースケースシナリオにフォーカスする

アーキテクチャ設計書の利用

アーキテクチャ設計書の利用方法

- 自身の事業がパーソナルデータを扱う事業かを確認
  - 導入編の「事業モデル」で確認
- パーソナルデータを扱う場合
  - テンプレートに示された６つの図面を作成する

ステークホルダリスト	**どのような機関が関係するのか**
ビジネス関係	**各機関のビジネス関係はどうなっているか**
データリソースマップ	**どのようなデータが、どこでどう扱われるのか**
トラストリソースマップ	**各機関の間での認証・認可に関わるリソースがあるか**
データフローシーケンス	**各機関間におけるデータの収受の流れは**
法制関係	関係する法制は

1. ステークホルダリスト ドライブレコーダビジネスの事例

目的：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 の取り扱われる範囲を明確し、プライバシー原則などを遵守すべきプレイヤーに抜けがないかを確認する

名称	概要	ISO/IEC 29100での分類
ドライバー	ドライブレコーダーで録画した映像を提供する。	PII principal
ドライブレコーダー販売事業者	ドライブレコーダーを販売する。	非該当
データ蓄積事業者	ドライバー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。	3rd party
通行人	ドライブレコーダーが録画した映像に映り込んでいる人	PII Principal

次ページ参照

チェックポイント

- ü ドライブレコーダー販売事業者は、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?
- ü 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る

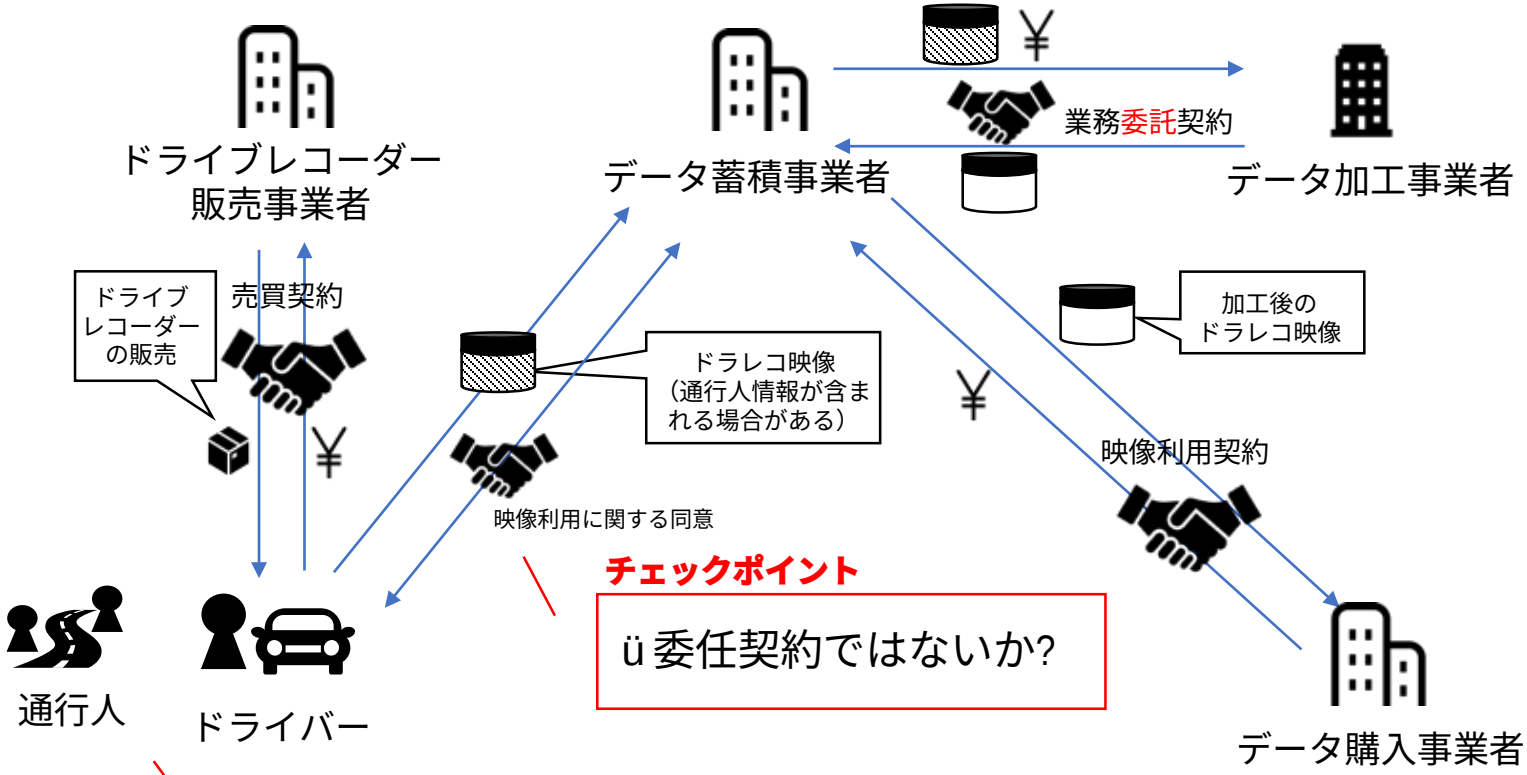
ISO/IEC 29100 アクターとその役割定義

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）を決定する
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する
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

2. ビジネス関係

ドライブレコーダビジネスの事例

目的：関与する個人、事業者間のビジネス関係（契約など）を明確化する



チェックポイント

ü委任契約ではないか?

チェックポイント

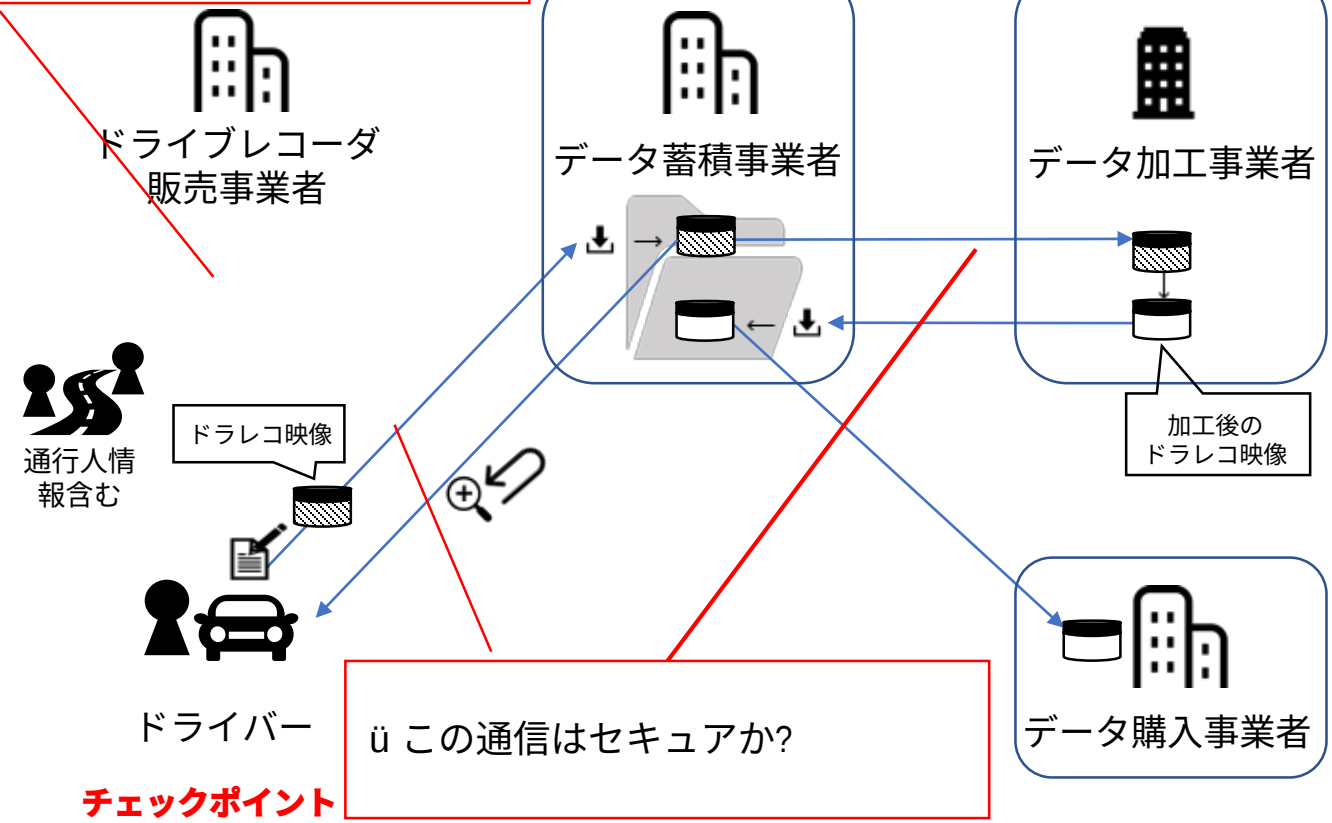
ü通行人とは、何の約定も、結ばれていない
üプライバシー原則に照らしてドラレコ映像を利用している旨の通知が通行人他に対しては必要ではないか?

3. データリソースマップ　ドライブレコーダビジネスの事例

目的：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。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。

チェックポイント

ü ドライブレコーダ販売事業者はステークホルダには入っているが、まったくパーソナルデータに関与しないのか? (例えば、機器番号がと個人情報が紐づけるられることによる影響はないか?

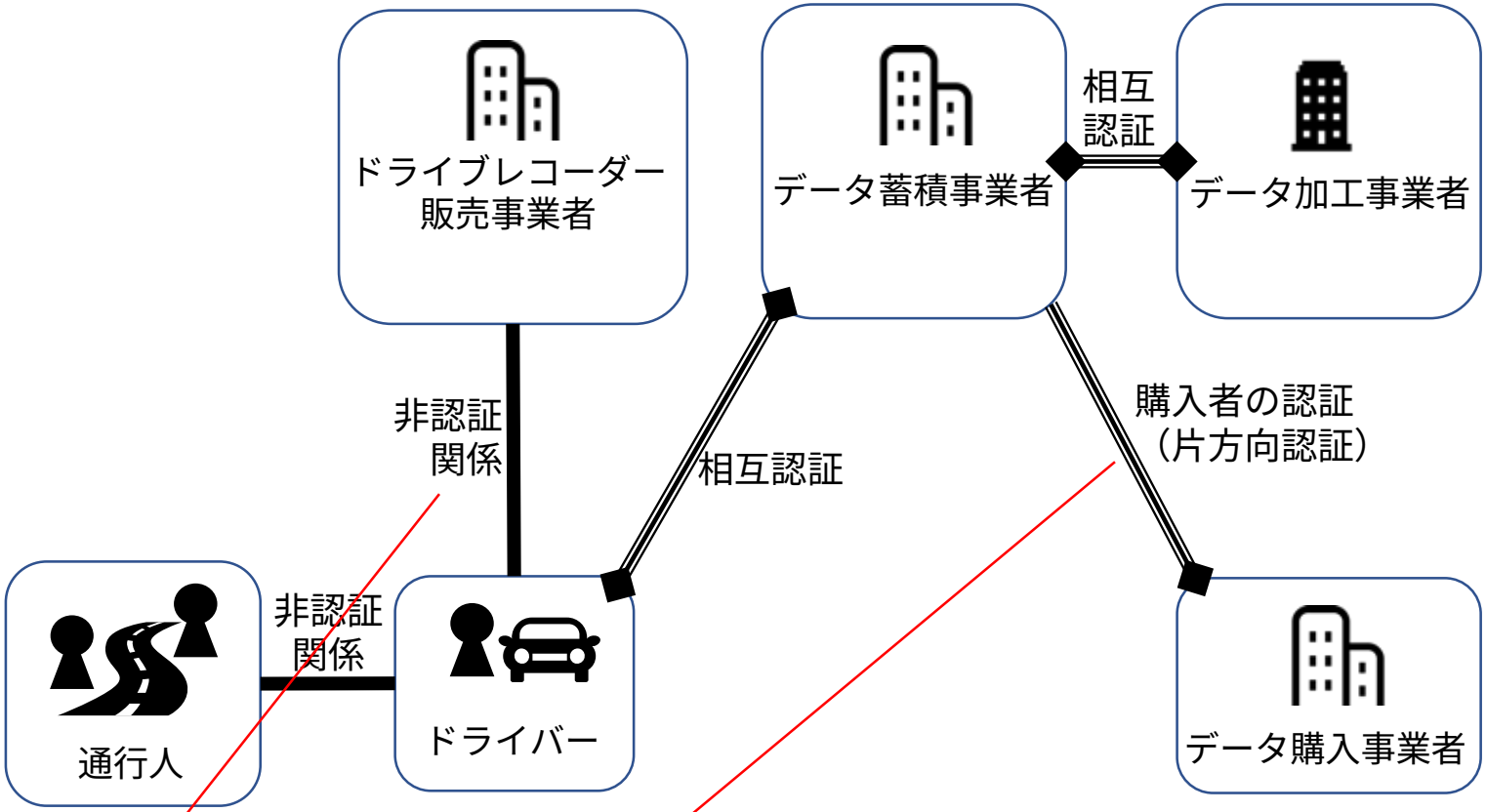


チェックポイント

4. トラスト関係

ドライブレコーダビジネスの事例

目的：関係者間の認証・認可の関係を明らかにする



チェックポイント

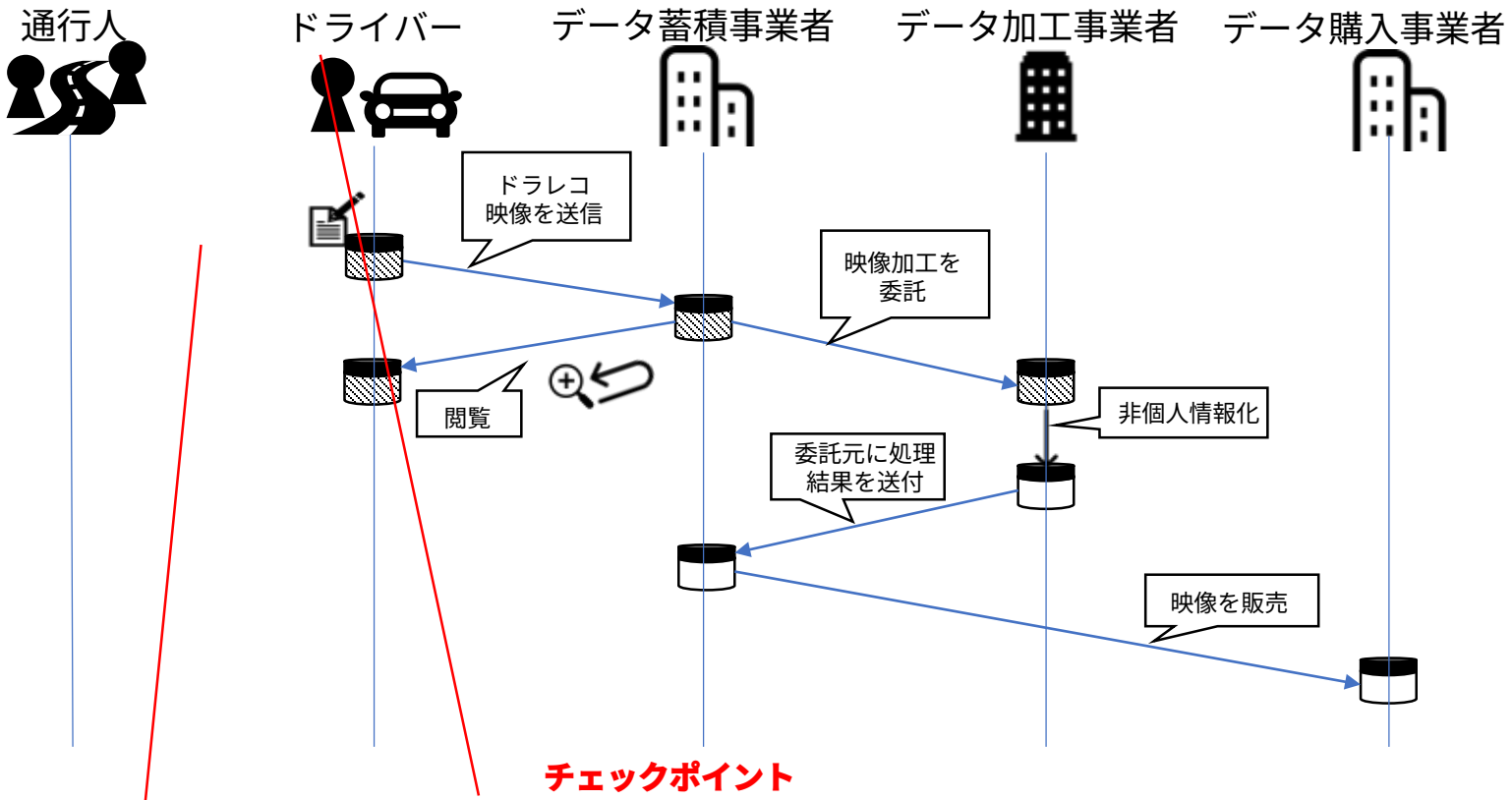
ü 片方向認証としているが、相互認証は必要ないのか?

チェックポイント

ü ドライバーと、ドライブレコーダー販売事業者や通行人との間には認証関係が存在しなのか?

5. データフローシーケンス ドライブレコーダビジネスの事例

目的：関係者間でのデータセットの移動、処理フローを、許可などの手順を明確化する



チェックポイント

ü 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?

チェックポイント

ü 通行人は全くデータフローには入ってこないのか?

6. 法制関係図

ドライブレコーダビジネスの事例

目的：各ステークホルダの事業ならびに相互の契約などにおいて、遵守すべき法制の範囲を明確にする

	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

ü 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。

ü 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。

国際標準化活動の実績

IEEE DTSI(Data Trading System Initiative)の設置
実施内容と今後の予定

Data Trading Alliance

ICAID Approved • 2019/06

HP launch • 2019/08

SASB meeting • 2019/11

Internal meeting • 2019/12

新規WGの設置のため、ICComの承認によるDTSI設置を提案し承認を得た。

IEEEの公式活動として、電話会議、HPの策定、グループウェアの運用を開始。

DTSI 1st Call • 2020/01

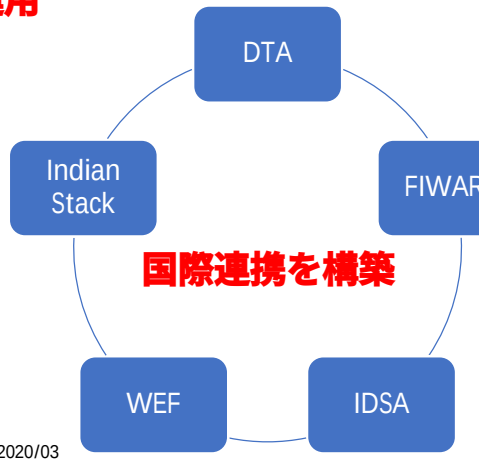
EU meeting • 2020/02

SASB meeting Workshop • 2020/03

PAR Submission • 2020/04

PAR Approval •2020/06

PARの策定と承認がゴール



国際連携を構築

総務省の「データ流通に関する国際標準化の推進と関連動向調査」事業と連携しながらこの活動を持続的に推進している。

国際標準化に向けた取り組み

- データジャケットの国際標準化（再委託: 東京大学）
  - データ取引においてデータジャケットは、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。
  - 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を作成。データの利用のためのアイデア創出ツールとして、将来の標準化への寄与を目指す。

Data Trading Alliance

EOF