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

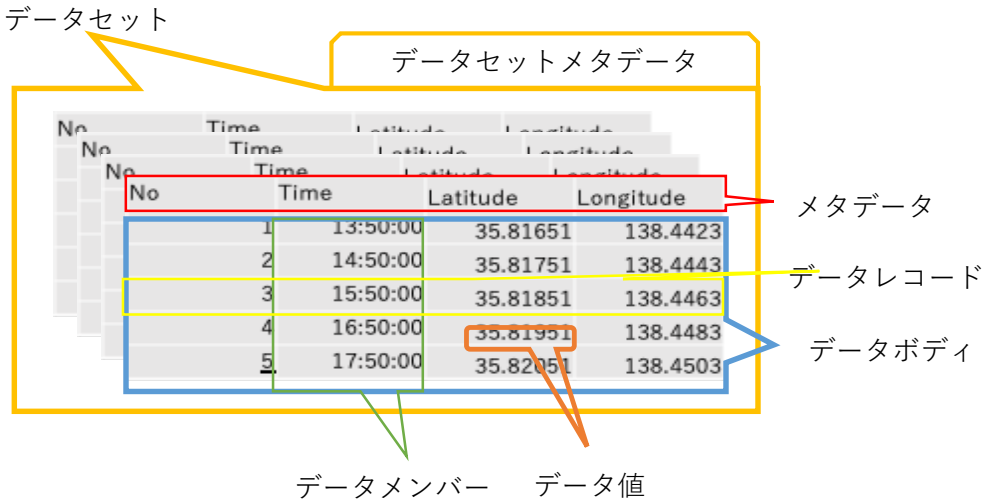
契約・トラスト

- 契約・トラストに関する用語

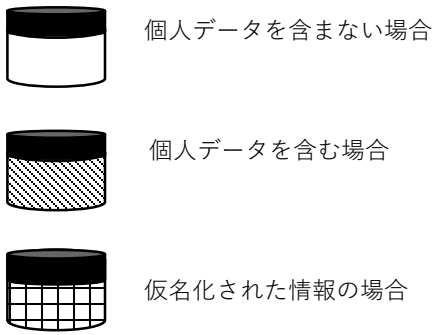
用語・定義集（一部抜粋）

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	

本書でのデータセット保管場所定義



本書でのデータセットのアイコン定義



アーキテクチャ

Society5.0 RAとの実施事項マッピング

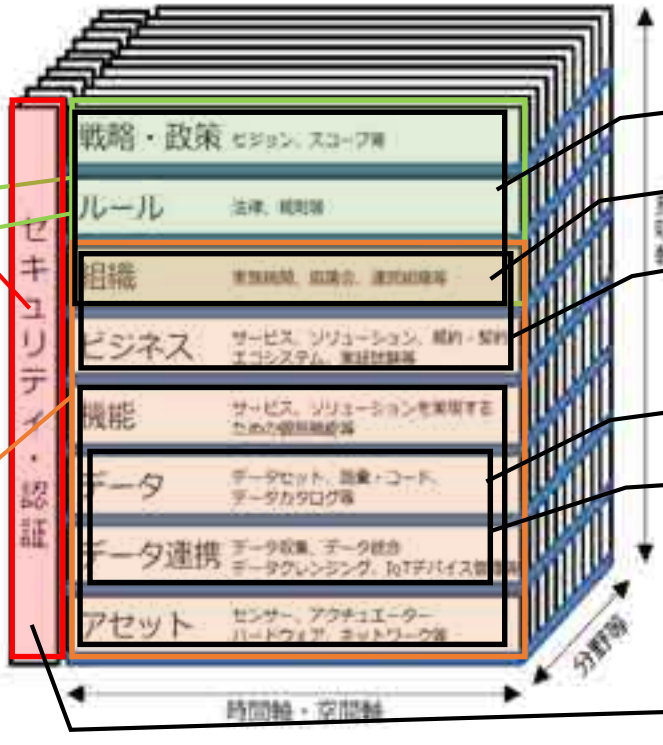
調査、実施内容

トラストサービス
調査報告

情報法制報告

ELSI検討報告

ユースケース
シナリオテンプ
レート＆
シナリオ集



ユースケースシナリオ
テンプレート

法制関係

ステークホルダリスト

ビジネス関係

データリソースマップ

データフローシーケンス

トラストリソースマップ

（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

✓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?

✓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

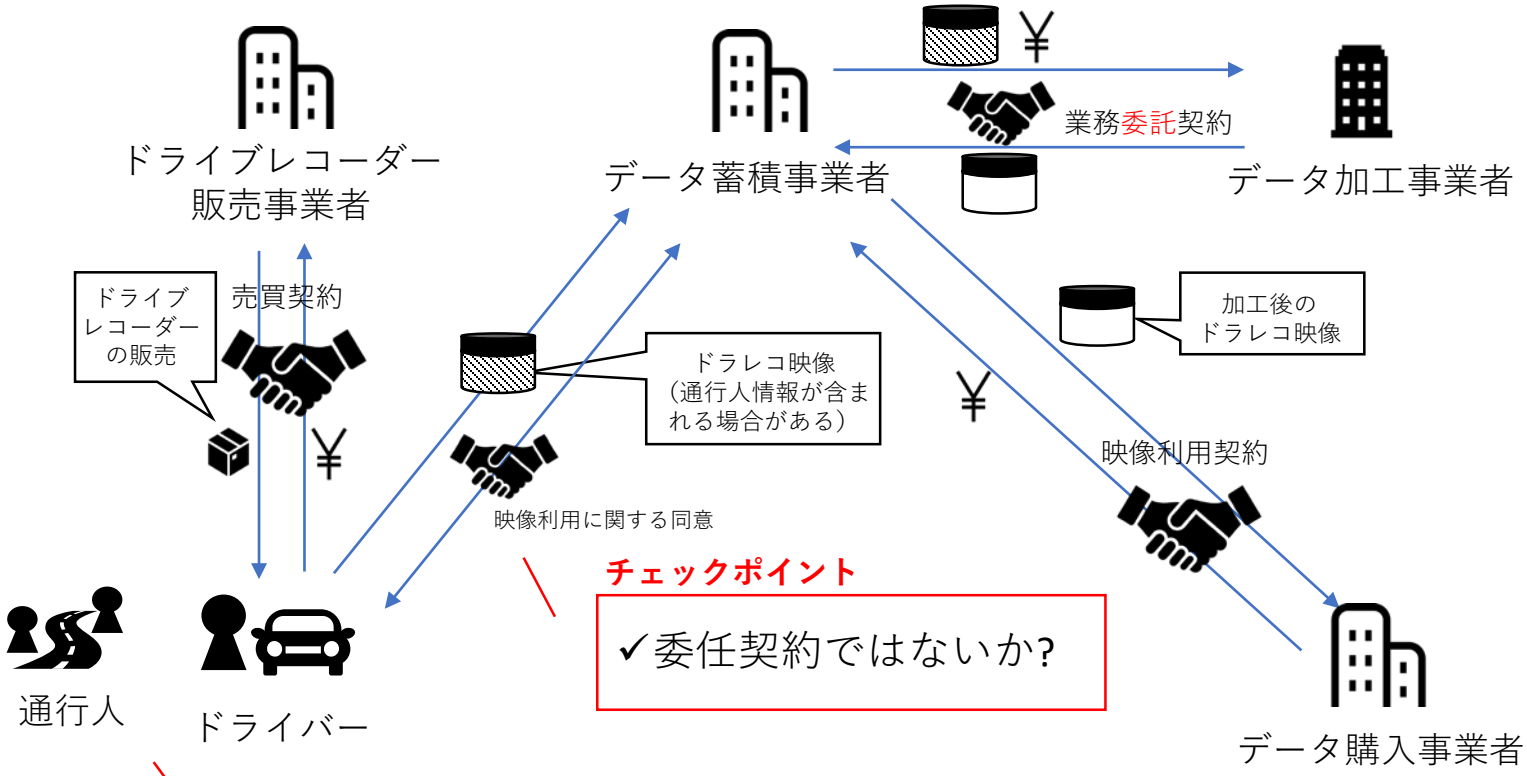
ISO/IEC 29100 アクターとその役割定義

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

✓委任契約ではないか?

チェックポイント

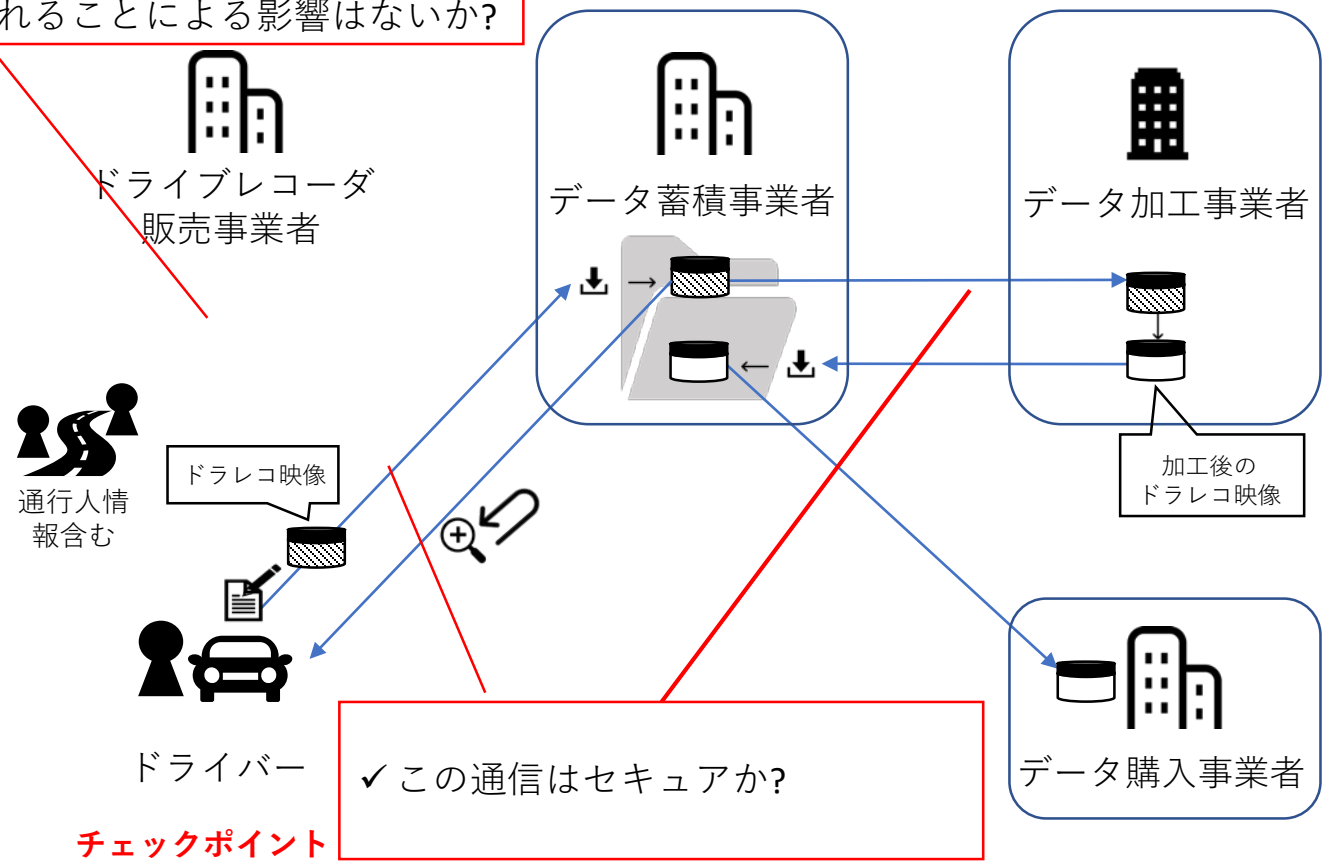
✓通行人とは、何の約定も、結ばれていない
✓プライバシー原則に照らしてドラレコ映像を利用している旨の通知が通行人他に対しては必要ではないか?

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

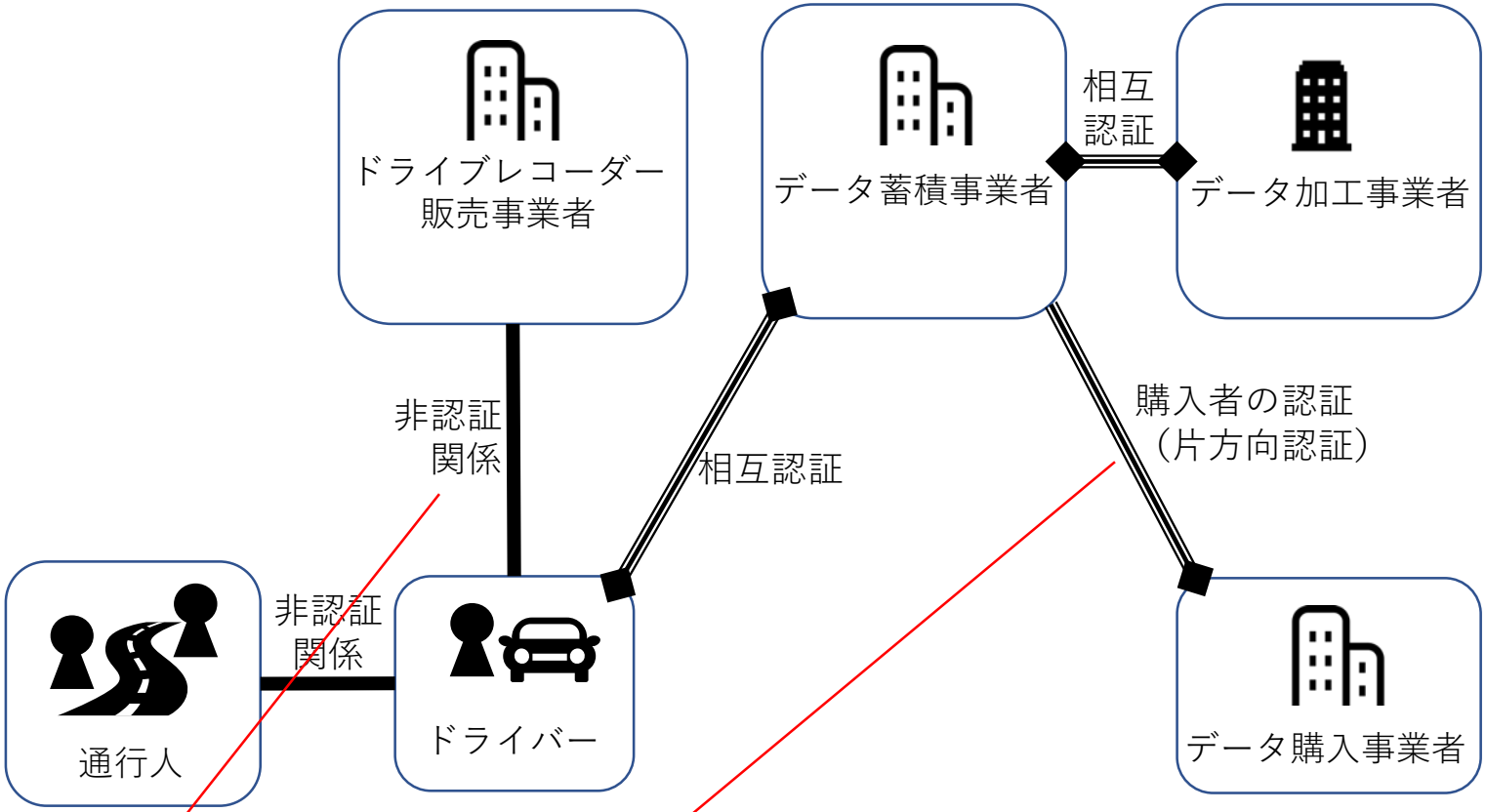
✓ドライブレコーダ販売事業者はステークホルダには入っているが、まったくパーソナルデータに関与しないのか? (例えば、機器番号がと個人情報が紐づけるられることによる影響はないか?



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

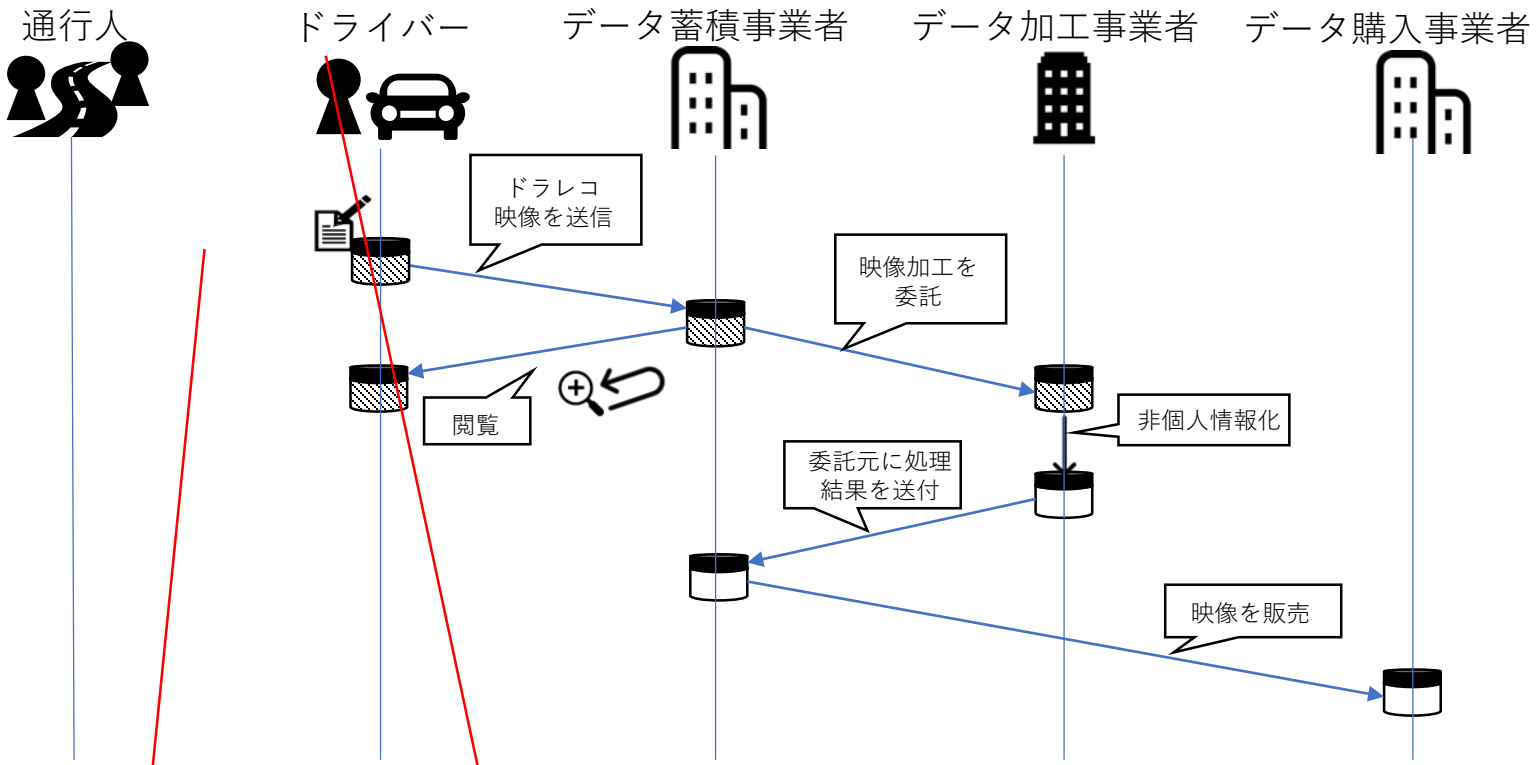
✓片方向認証としているが、相互認証は必要ないのか?

チェックポイント

✓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

✓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

✓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

✓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。

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

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

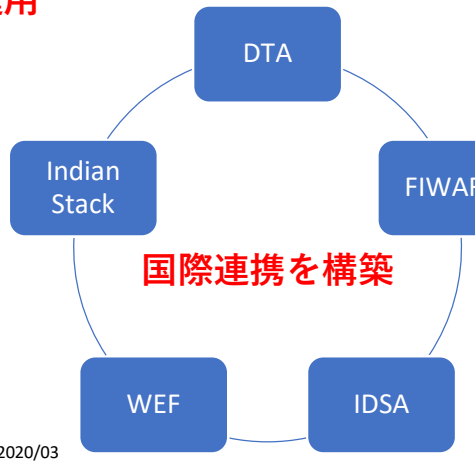
EU meeting • 2020/02

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。

データジャケットの国際標準化（再委託: 東京大学）の成果

- 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。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して、将来の標準化への寄与を目指す。

- 具体的には
  - 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
  - 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
  - DJの使用事例
  - 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。

本スライドの44-51に、その成果の一部を掲載する。

Data Jackets as a Global Technology for Trading Data with Trust

Yukio Ohsawa（大澤幸生）, Teruaki Hayashi（早矢仕晃章）, Gensei Ishimura（石村源生）, The University of Tokyo

A Data Jacket (DJ) is a piece of digest information of a dataset, that does not open the content of the data but includes the title, the abstract, and variables, that may represent the subjective expectation of data owner or potential data users about the utility of the data.

Definition a data jacket (***DJ***$_i$) for a dataset *d*, suffixed by *i* is defined by information corresponding to DJ_i (*d*) := {F_i (*d*), P_i (*d*), V_i (*d*), U_i (*d*),} where

F_i (d) : the set of functions defined on the variables in V_i (*d*)

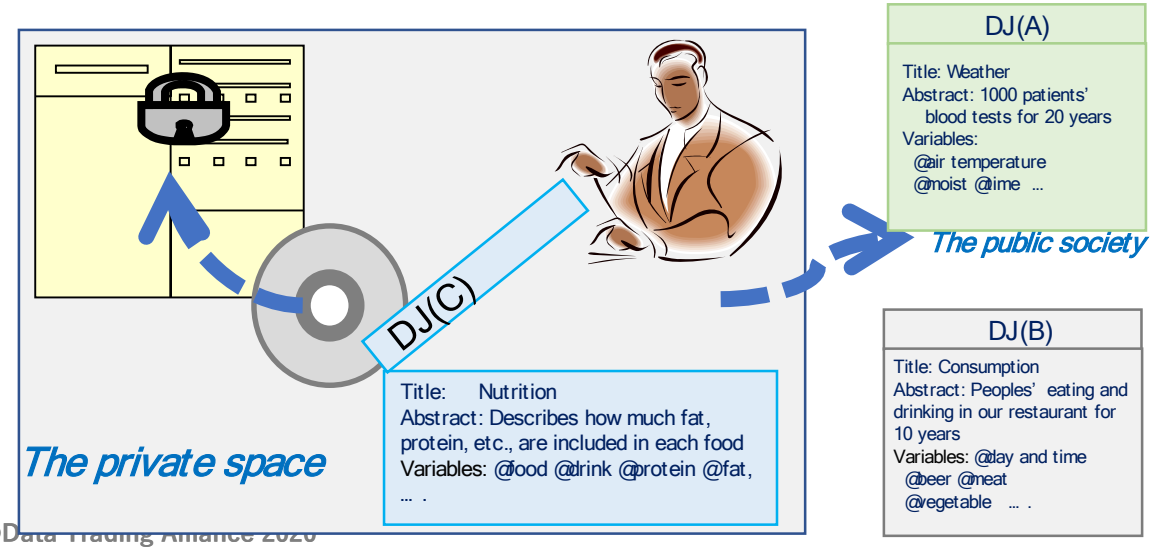
P_i (d) : the set of predicates that express relations among variables in V_i (*d*)

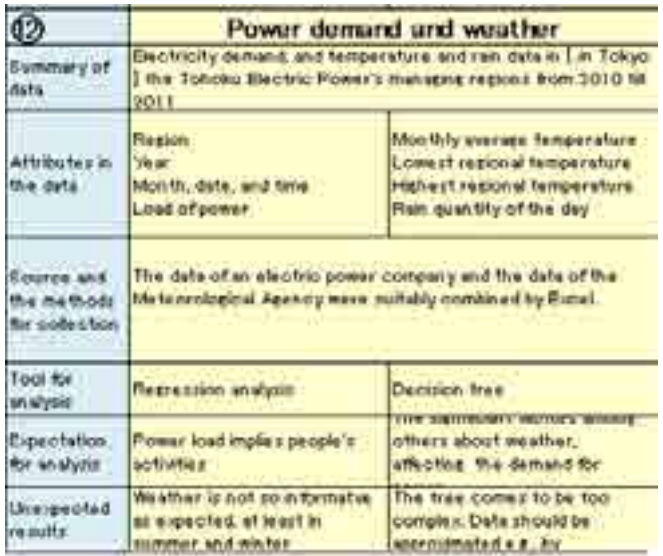
V_i (d) : the set of variables in DJ_i (*d*)

U_i (d) **:** the set of use cases of (*d*) and their values based on the information in DJ_i (*d*).

In U_i (*d*), hypothetical scenarios are expressed in logical formulae using the elements of F_i (*d*), P_i (*d*), and V_i (*d*) or corresponding explanation by human(s) in natural language.

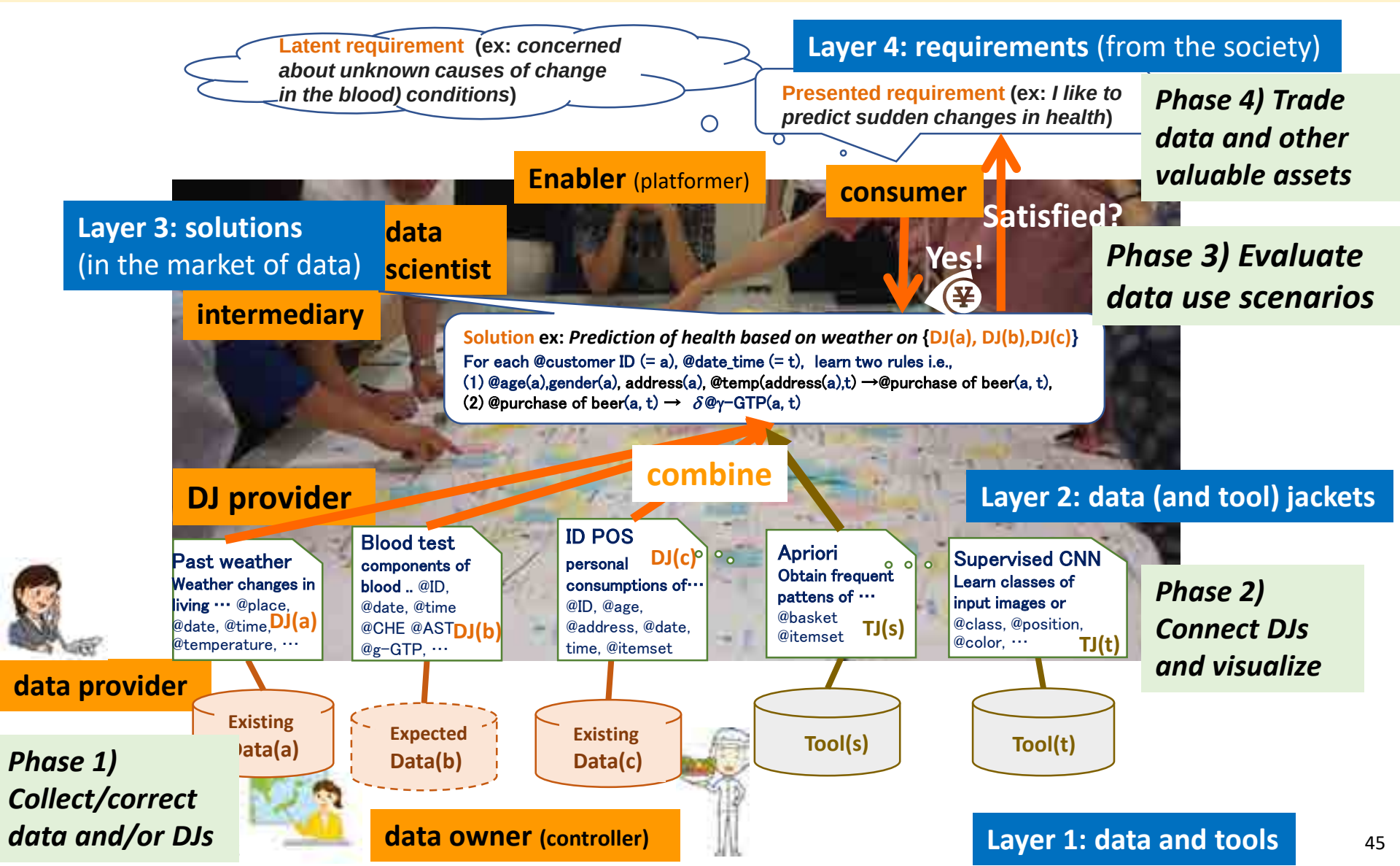
Ohsawa Y., Hayashi T., Kido H., Restructuring Incomplete Models in Innovators Marketplace on Data Jackets. Magnani L., Bertolotti T. (eds) *Handbook of Model-Based Science*, 1015-1031 Springer (2017)



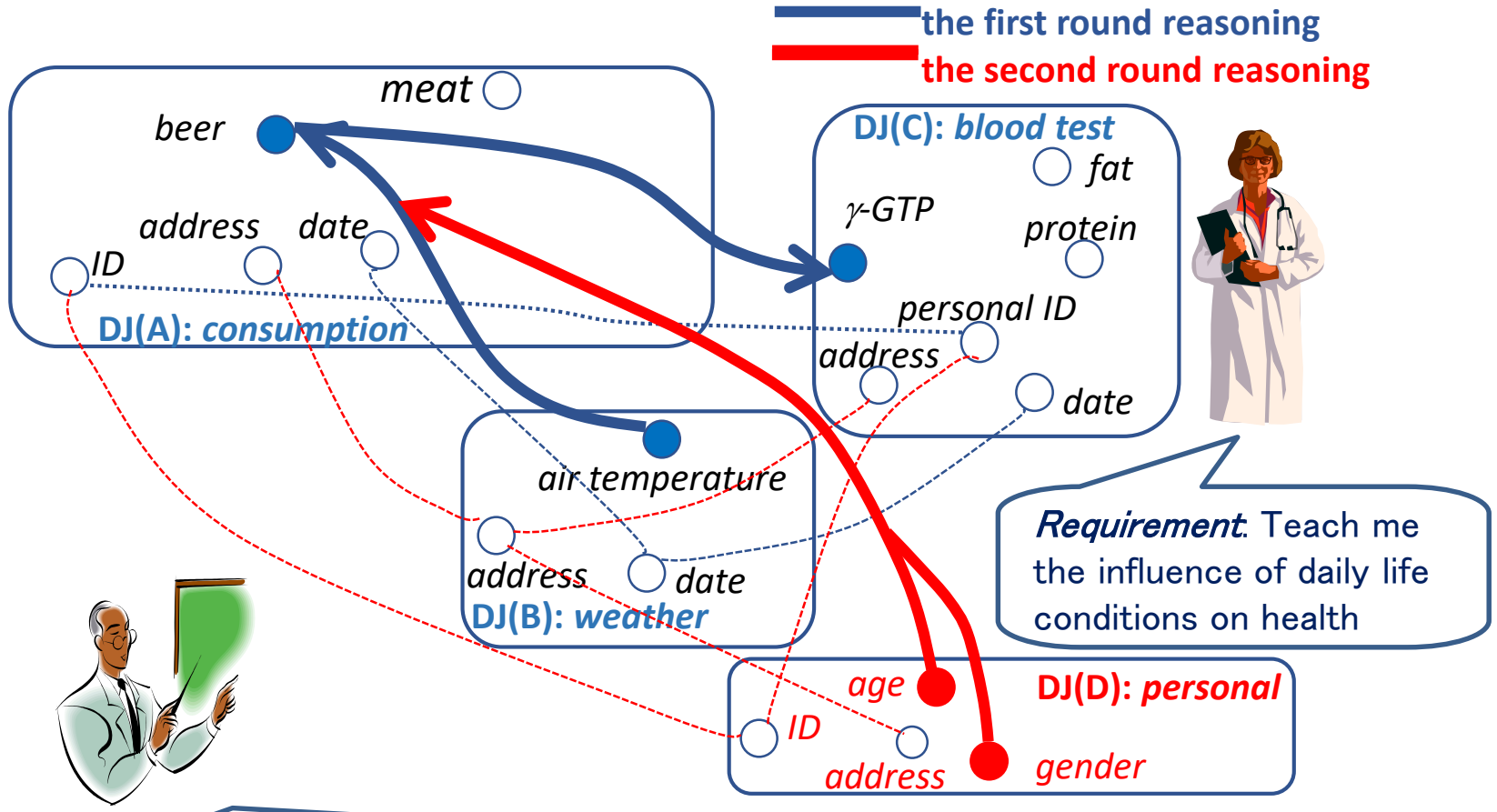


The Four Phases crossing the Four Layers of IMDJ for the Seven Stakeholders in the market of data

Extending Ohsawa, et al, Innovators Marketplace on Data Jackets for Externalizing the Value of Data via Stakeholders' Requirement Communication *AAAI 2014 Spring Symposium on "Big data becomes personal: Knowledge into Meaning*, March 2014, Stanford (2014)



The abductive communication in IMDJ creating use cases of datasets



Proposed plan: Combine data behind DJ(A) though DJ(C), to learn

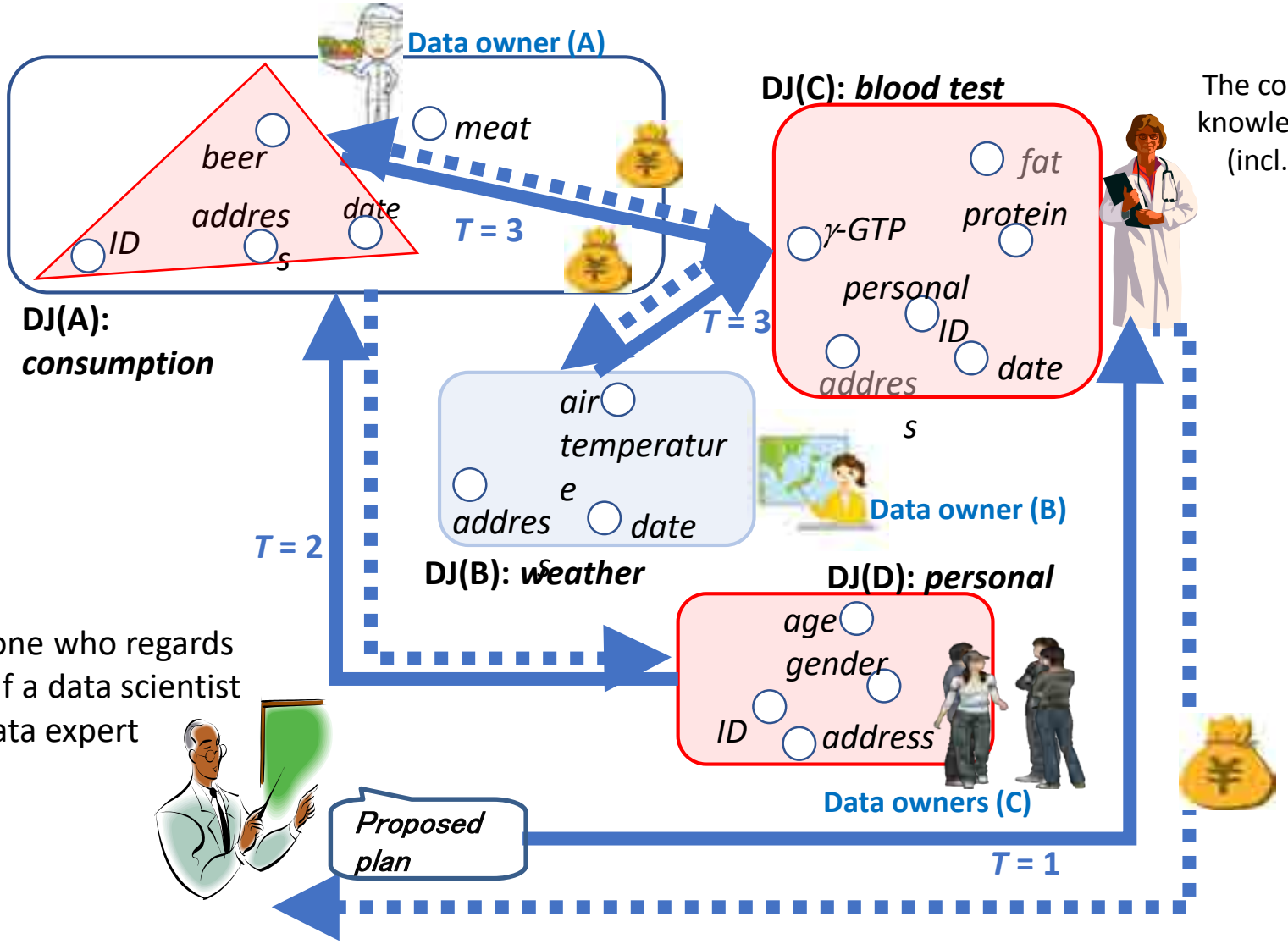
(1) tempr_up(**adr** =Tokyo, date) –> beer_drink(**adr** =Tokyo, **gndr**:man, **age**:30, date) (DJ: A, B, **D**)

(2) beer_drink(Tokyo, man, 30, date) –> up_γ-GTP (Tokyo, man, 30, date) (DJ: A, C, **D**)

Confidence increases (e.g. from 1% to 9%) by adding the red variables in the personal dataset **D**.

Ohsawa, Y., Kondo, S., Hayashi, T. (2019) Data Jackets as Communicable Metadata for Potential Innovators – Toward Opening to Social Contexts, 19th Int'l Conf. on Intelligent Systems Design and Applications (ISDA 2019)

The stakeholders' value exchange after the abductive communication



大澤幸生, 早矢仕晃章, 石村源生, 近藤早映, 白水督久: データジャケット論理に基くデータ価値連成の可視化, 信学技報 119(413) AI2019-48 pp.33-38, 2020.

The definition of Trust in the context of IMDJ

The trust in/of IMDJ is established *iff* the following rights and reliabilities are ensured.

1. **Right of DJ's providers in IMDJ (conditions promised to providers)**
   - DJ's providers are ensured that they can control how their DJ should be used.
     - The information of DJ is absolutely ***kept among defined stakeholders***. The definition is noticed to the providers in advance. If no definition is made, it means that DJ are open to the public. Participants in IMDJ are restricted to the defined stakeholders.
     - The provider can request ***withdrawal*** of their DJ and/or data sets and ***restriction*** of their circulation/use whenever they want after IMDJ. Their request is reported immediately to the related stakeholders, and is executed appropriately.
2. **Right of participants in IMDJ (conditions promised to participants)**
   - Participants in IMDJ, *and* ***only they***, are ensured to be able to use any ideas of solutions for given problems proposed in the IMDJ, under the CROP principle (see the next page).
   - They are ensured to express opinions freely in IMDJ except for illegal or unethical ones.
3. **Reliability of DJ treated in IMDJ (conditions promised to DJ's users)**
   - DJ's users are ensured that DJ which they use are ***sufficiently*** reliable.
     - Data sets represented by DJ are authentic (not falsified, fabricated, nor stolen).
     - Any unethical intension such as exposure of confidential information is prohibited.
     - The reliability doesn't necessarily mean "accuracy" - DJ can be described subjectively.
4. **Reliability of IMDJ in the society (conditions promised to the society)**
   - The society is ensured that IMDJ follows laws, social norm, and ethics (referring to "ELSI").

The rules for the participants in IMDJ

The CROP principle in IMDJ

Based on all the definition for trust in and of IMDJ (see the last page), all the ideas created in IMDJ are right-protected under the boundary defined by the Controlled (in or after the session) Reach Of the Presentation.

(1) Each participant, and each participant only, has the right to use any idea for any solutions, and to use related DJs for any problems proposed by the others in the IMDJ freely.
(2) The above right is assured only if it is exercised fairly and ethically, and it is allowed by all of the providers of the referenced DJ.
(3) Any proposer of any idea in the IMDJ can request the restriction of the rights of the others at any time later, and this should be realized as far as possible.
(4) However, the proposers have to accept that the use and propagation of their idea might not be able to be interrupted by their ex-post facto requests.

大澤幸生, 早矢仕晃章, 石村源生, 近藤早映, 白水督久: データジャケット論理に基くデータ価値連成の可視化, 信学技報 119(413) AI2019-48 pp.33-38, 2020.

The cases of IMDJ in businesses and sciences

Six cases: bold letters show datasets corresponding to the combined DJs

A. Visualized safe walking paths by **streetlight locations + Google maps**

B. **Discovered positive correlation of stock price vs the number of payed holidays**

C. Football coaching system from **full-view video images of a soccer stadium**

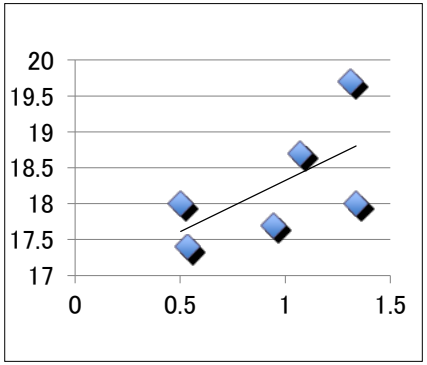
D. Change explanation in markets from **POS** or **stock chart data**

E. Change explanation in earthquakes diverting from D using DJ store (next page)

F. City planning in Tokyo and Yokohama using **datasets from various industries**

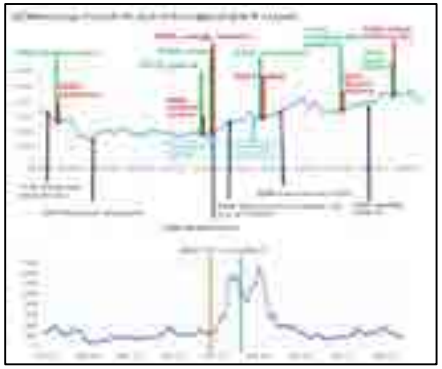
A

B

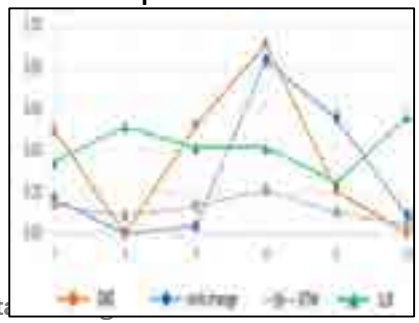


C

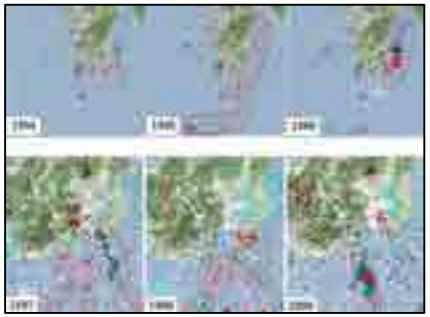
D for the stock market



D for supermarkets



E CE in earthquakes



F IMDJ in Marunouchi Data Consortium

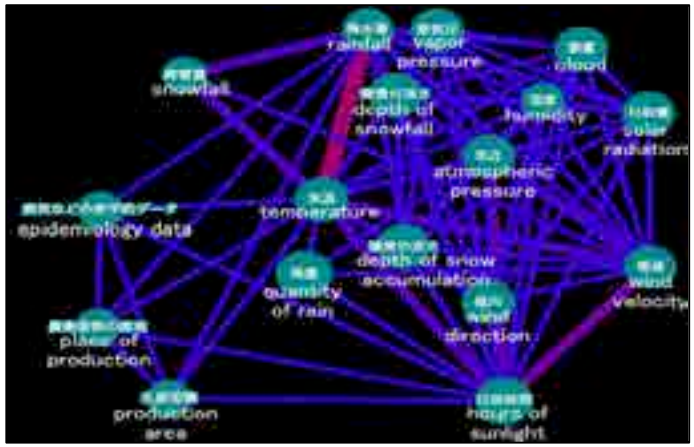
Tools for aiding the creative thoughts in IMDJ

A. **Data Jacket Store**: a data retrieval system burying the knowledge gap between stakeholders on the structure of solutions

B. **Variable Quest**: a matrix-based inferring method of variable labels (VLs), which are the names/ meanings of variables in Data Jackets.

C. **Web-based IMDJ**: for supporting the communication on DJs reducing the load for crossdisciplinarity data collaborations.

D. **Virtuora DX**: A digital transformation system introducing DJs and visually connecting them, and DJ Store functions.



Data Trading Alliance

EOF