

ユースケースシナリオ集

2020/3/31

一般社団法人データ流通推進協議会

Data Trading Alliance

(b-2-1) 「情報銀行」間の連携に関するアーキテクチャの実証研究の実施 - パーソナルデータ統合 -

- 大日本印刷株式会社、株式会社NTTデータ、富士通株式会社

(b-2-1) 「情報銀行」間の連携に関するアーキテクチャの実証研究の実施 - サービス事業者統合 -

- 大日本印刷株式会社、株式会社NTTデータ、富士通株式会社

(b-2-2) 「情報銀行」を通じたデータの流通・活用に関するアーキテクチャ の実証実験の実施

- 国立大学法人 大阪大学

(b-2-4) 生体認証データの事業者間の連携に関するアーキテクチャ の実証研究の実施

- 日本電気株式会社

(b-2-5) 特定エリアにおける行動データの事業者間の連携に関するアーキテクチャ の実証研究の実施

- KDDI株式会社

(b-2-1) 「情報銀行」間の連携に関する アーキテクチャの実証研究の実施 - パーソナルデータ統合 -

大日本印刷株式会社、株式会社NTTデータ、富士通株式会社

プロジェクト概要

以下にご記載ください

項目	記載内容
プロジェクト名	パーソナルデータ統合連携
記載者	岡田陽一、野村洋治
所属	大日本印刷株式会社、富士通株式会社
連絡先	Okada-Y2@mail.dnp.co.jp（岡田）、nomura_yoji@fujitsu.com（野村）
記載日	2020年3月24日
プロジェクト概要	購買、観光という異なる二つの情報銀行のサービス連携を疑似体験できる実証システムを構築し、ユーザ視点による情報銀行間連携サービスにおける受容性、課題点を確認する。 また、異業種間共創を目的とした既存アプリケーションを活用し、情報銀行事業者視点によるサービス連携の実現のための有効手段、課題を確認する。
備考	

1. ステークホルダリスト

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（主に個人情報保護法での位置づけ等）	役割
個人①	情報銀行Aと契約するユーザ	PII Principal
情報銀行A	日常の購買データを蓄積して、特売情報やお得なサービスを提案する情報銀行。 家計簿系情報銀行。	PII Controller
サービス事業者（A）	情報銀行Aと契約するサービス事業者	PII Principal (PIIを提供するため)
情報システムプラットフォームX	情報銀行A及びBが利用する情報銀行プラットフォーム	PII Processor
情報銀行B	観光サービスをベースに旅程や観光先でのイベントや店舗を提案する情報銀行。 旅行系情報銀行。	PII Controller/ PII Processor(情報銀行Aの要請)
サービス事業者（B）	情報銀行Bと契約するサービス事業者	非該当（PIIを扱わないため）

2. ビジネス関係

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

サービス事業者（A）

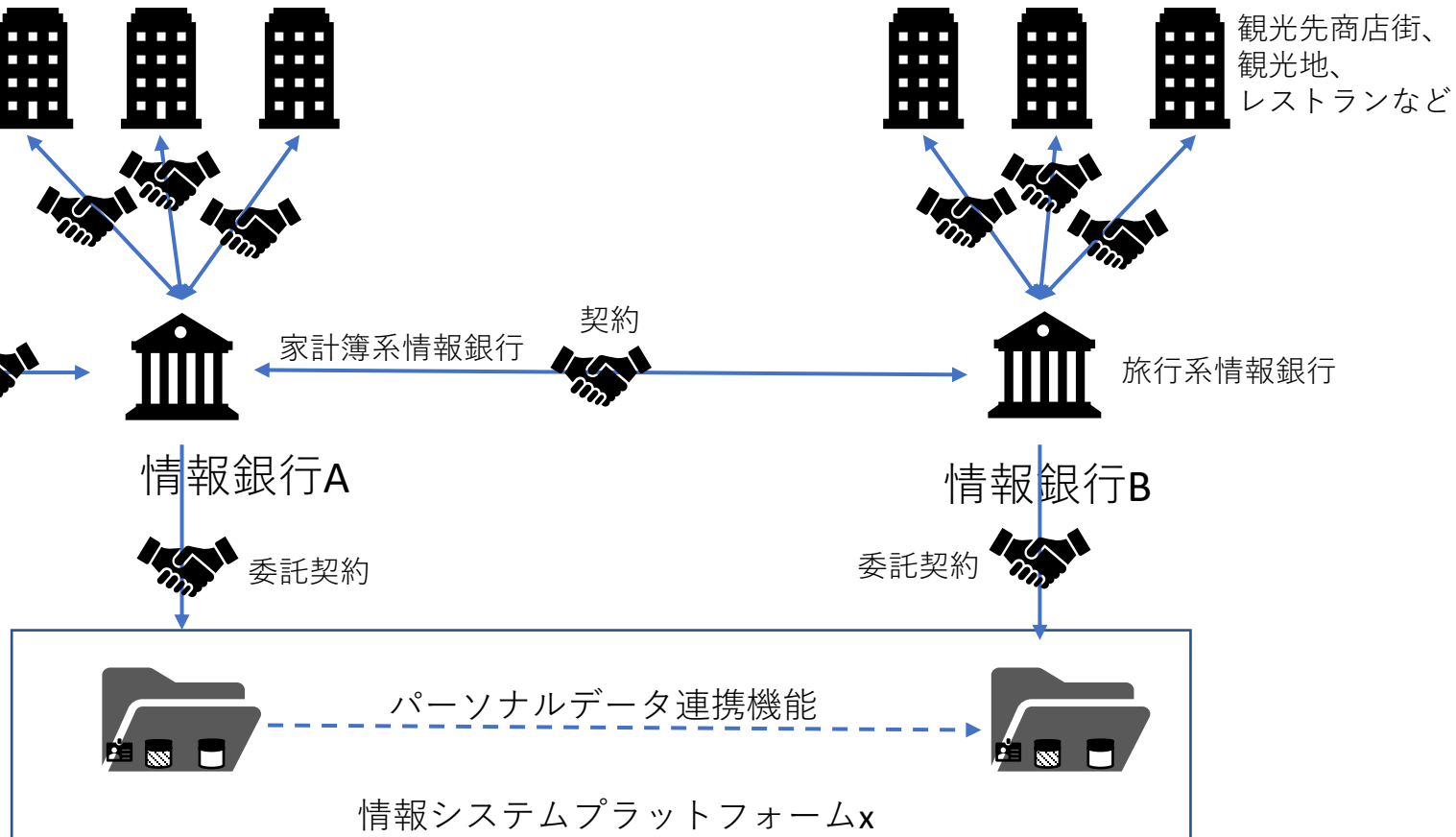
サービス事業者（B）

小売、スーパー
(クーポン)

観光先商店街、
観光地、
レストランなど

家計アプリ登録済
旅行アプリは未登録

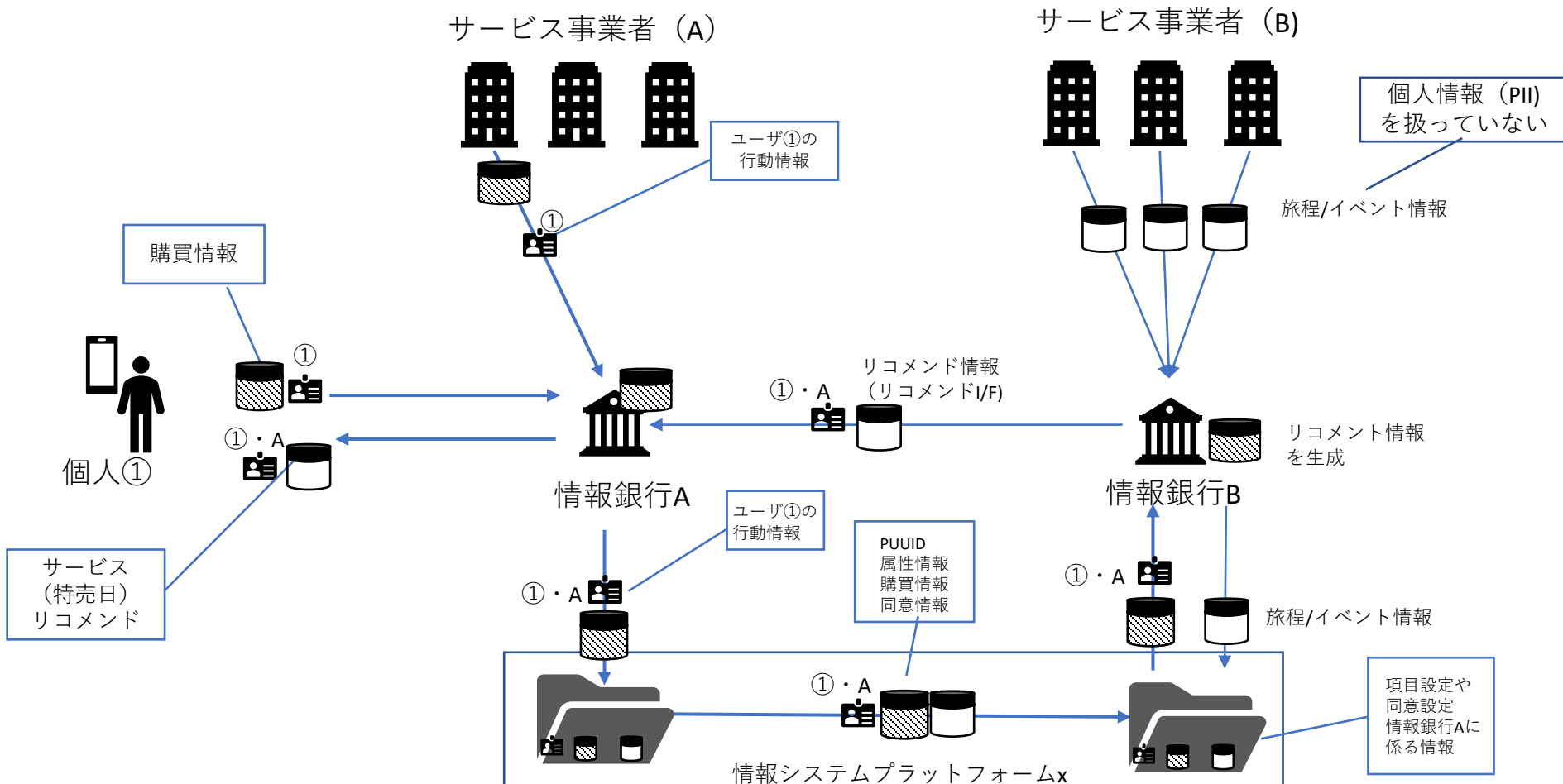
個人①



個人①はスマホを所持していることを前提とする

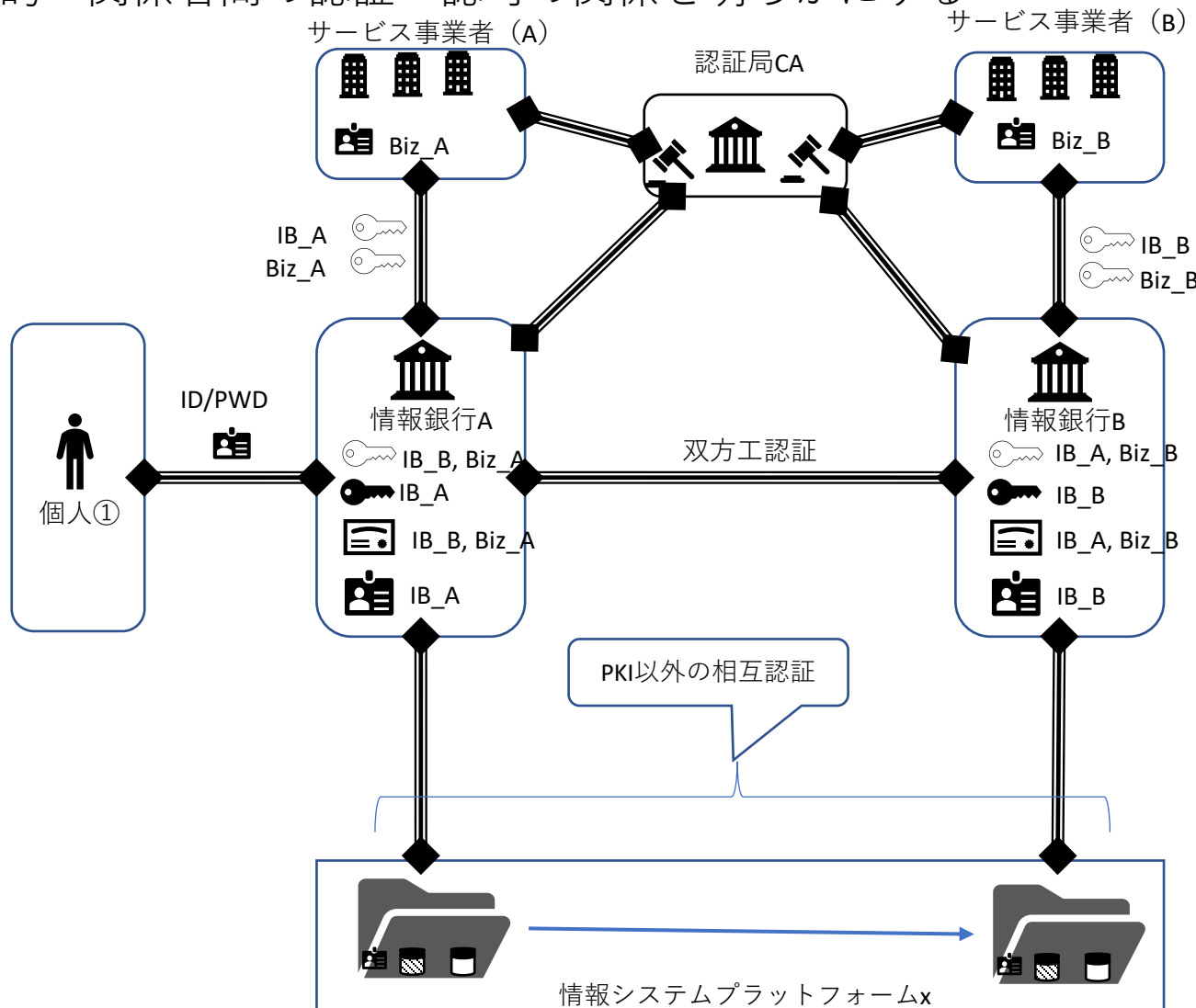
3. データリソースマップ

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。



4. トラスト関係

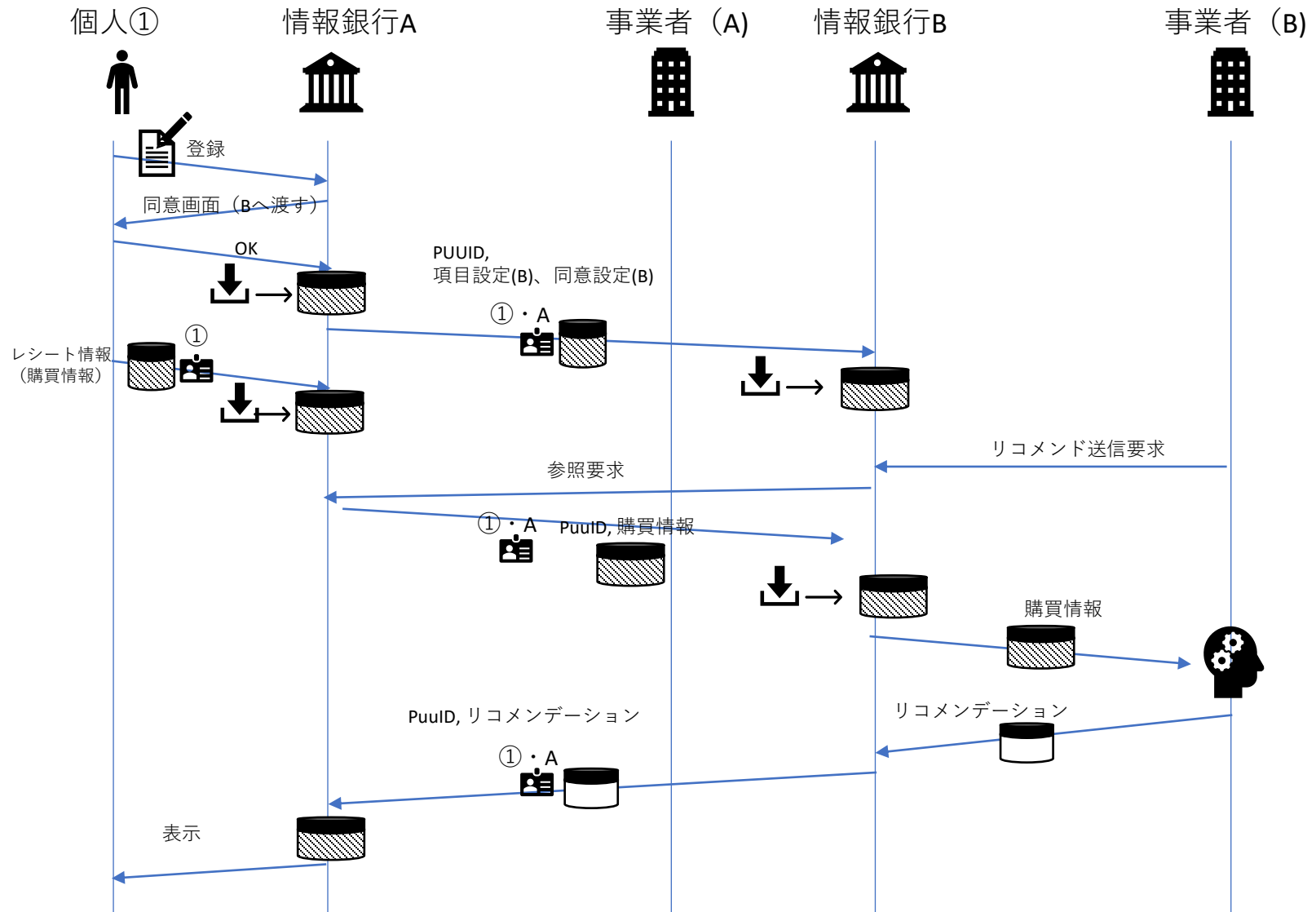
目的：関係者間の認証・認可の関係を明らかにする



※情報システムプラットフォームは一つのエンティティ（事業者）。共有材ではない。

5. データフローシーケンス

目的：関係者間でのデータセットの移動、処理フローなどの手順を明確化する



6. 法制関係図（行政規制）

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

	個人①	情報銀行A	事業者（A）	情報システムプラットフォームX運営事業者	情報銀行B	事業者（B）
個人①		第三者提供（個情法23条1項） 情報銀行A→情報銀行B	第三者提供（個情法23条1項） 事業者（A）→情報銀行A		第三者提供（個情法23条1項） 情報銀行A→情報銀行B ※ただし、提供先なので特段の規制はない（一般的な、利用目的の通知公表義務は存在）	（特定の個人に向けているのでなければ個情法とは無関係）
情報銀行A			第三者提供（個情法23条1項） 事業者（A）→情報銀行A	委託（個情法22条, 23条5項1号） 情報銀行A→X	第三者提供（個情法23条1項） 情報銀行A→情報銀行B	
事業者（A）						
情報システムプラットフォームX運営事業者					委託（個情法22条, 23条5項1号） 情報銀行B→X	
情報銀行B						（特定の個人に向けているのでなければ個情法とは無関係）
事業者（B）						

個人①を起点に、事業者（A）は同意に基づいて情報銀行Aに行動情報を提供する。

情報銀行Aは同意に基づいて行動情報、属性情報、購買情報及び同意情報（フラグ）を情報銀行Bに提供する。

事業者（B）はPDS上のフラグに基づいてリコメンド情報を提供する。リコメンドは特定の個人に向けているのでなければ個人情報保護法上の規制とは無関係。

6. 法制関係図（契約関係）

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

	個人①	情報銀行A	事業者（A）	情報システムプラットフォームX運営事業者	情報銀行B	事業者（B）
個人①		個人と「情報銀行」との間 利用 契約約款（モデル約款）（ver 1.0）			個人と「情報銀行」との間 利用 契約約款（モデル約款）（ver 1.0） ※契約関係を成立させるのかはビジネスモデルによる	
情報銀行A			「情報銀行」と情報提供元との間の個人データ 提供契約（モデル契約）（ver 1.0）	業務委託契約 ※いわゆる「業務委託契約」の法的性質は請負であったり委任（準委任）であったりする。本件の場合是一种の請負であろう。	「情報銀行」と情報提供先との間の個人 データ 提供契約（モデル 契約）（ver 1.0）	
事業者（A）						
情報システムプラットフォームX運営事業者					業務委託契約	
情報銀行B						広告（リコメンド）出稿に関する契約 ※パーソナルデータとは無関係である。
事業者（B）						

民法上、契約自由の原則が基本であり、行政規制を遵守している限り契約関係は自由である。もっとも、個人が（事業者としてではなく）参加する場合は消費者契約法等の消費者関係法により条項が無効となることがあり得る。

ここでは仮に、日本IT団体連盟が行っている情報銀行認定における参照文書と、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」におけるひな型を参照しているが、これらはいかなる意味においても規範ではないことに注意しなければならない。

気づきやコメント

- 本手法の実践での気づき
 - 生活者がもつ個人情報に応じた認証方式が必要。
 - 情報銀行間連携において、情報銀行事業者の相互チェックの仕組みがあれば、生活者の信頼につながる。
 - サービス分野の違いによる保有情報の差異なども考慮した連携データ共通仕様定義など、コストを下げる方策の検討が必要
- 個人の課題（便益の見える化）、企業の課題（魅力的サービスの創出）の解決に本手法を適用できるか？
 - 規約同意形成のアプローチ例（図示、概要→詳細の構成化等）のアプローチが必要。
 - 生活者自身によるコントローラビリティを実現、実感してもらうため、パーソナルデータごとに細かく提供可否を設定できる必要性の示唆。
 - 生活者間における同意設計への必要性の示唆。
 - 情報銀行事業者が連携先を募集する上で、IMDJの有効性の確認およびデータジャケット記載時に配慮すべきポイントの確認。
 - 同意設定、パーソナルデータの利用時の証跡管理における一元化の必要性、重要性を監査者、生活者の視点から確認。
- 社会実装する上で、本手法の役割・貢献・課題などは？
 - 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

(b-2-1) 「情報銀行」間の連携に関する アーキテクチャの実証研究の実施 - サービス事業者統合 -

大日本印刷株式会社、株式会社NTTデータ、富士通株式会社

プロジェクト概要

以下にご記載ください

項目	記載内容
プロジェクト名	サービス事業者統合連携
記載者	藤田 裕介
所属	株式会社 NTTデータ
連絡先	Yuusuke.Fujita@nttdata.com
記載日	2020年3月24日
プロジェクト概要	引越に関わる二つの情報銀行の連携を疑似体験できる実証システムを構築し、サービス事業者（電気、ガス等）視点による情報銀行間連携における流れを確認する。 その中で、個人情報の流通を支えるPFを介し、データフォーマット、データ項目の互換性および必要となる機能についての検証や運用上の課題の整理等を行った。
備考	

1. ステークホルダリスト

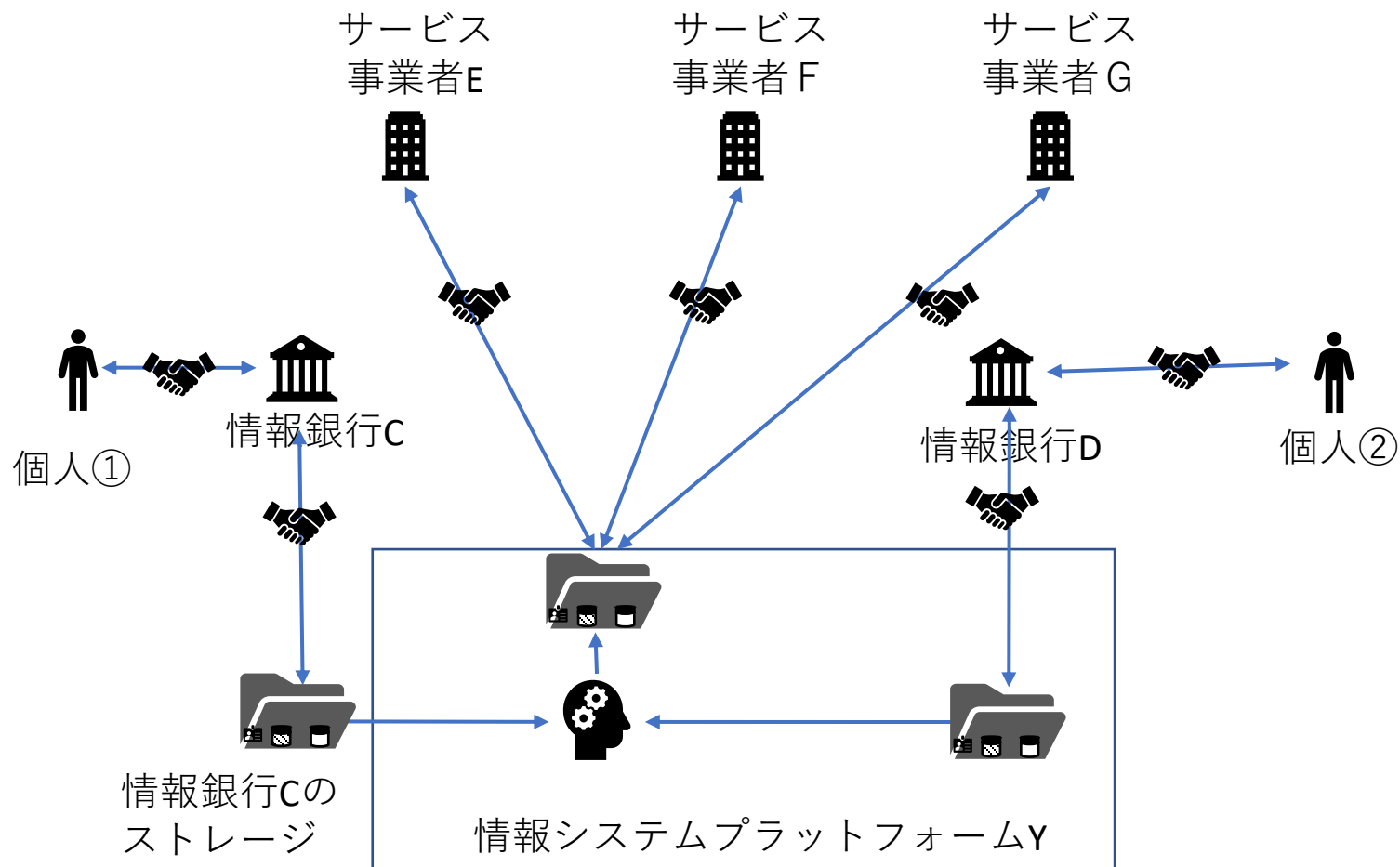
目的：関与する個人、事業者の一覧表を作成することで、パーソナルデータの取り扱われる範囲を明確し、プライバシー原則などを遵守すべきプレイヤーに抜けがないかを確認する

名称	概要（主に個人情報保護法での位置づけ等）	役割
個人①	情報銀行Cと契約するユーザ	PII Principal
情報銀行C	独自フォーマットの情報銀行	PII Processor
ストレージC	情報銀行Cが利用するストレージ運営事業者	PII Processor
情報システムプラットフォームY	情報銀行Dが利用し、フォーマット変換機能を備えた情報システムプラットフォーム事業者	PII Controller
情報銀行D	D独自のフォーマットを持つが、統一フォーマットへの変換機能を持つ情報システムプラットフォームYを利用する情報銀行	PII Processor
サービス事業者E	元々情報銀行Cと契約。統一フォーマットを利用できるようになった	3 rd Party
サービス事業者F	元々情報銀行Dと契約。統一フォーマットを利用できるようになった	3 rd Party
サービス事業者G	C,Dの両方の情報銀行のアカウントを持っていた。統一フォーマットへのニーズが高かったサービス事業者	3 rd Party
個人②	情報銀行Dと契約するユーザ	PII Principal

※ビジネスの主体者がどこかで、PII Controller/ PII Processorの役割は変わる。今回の場合、PF-Y事業者が管理権限を持っているビジネスで、PIIの扱いをコントロールしている。

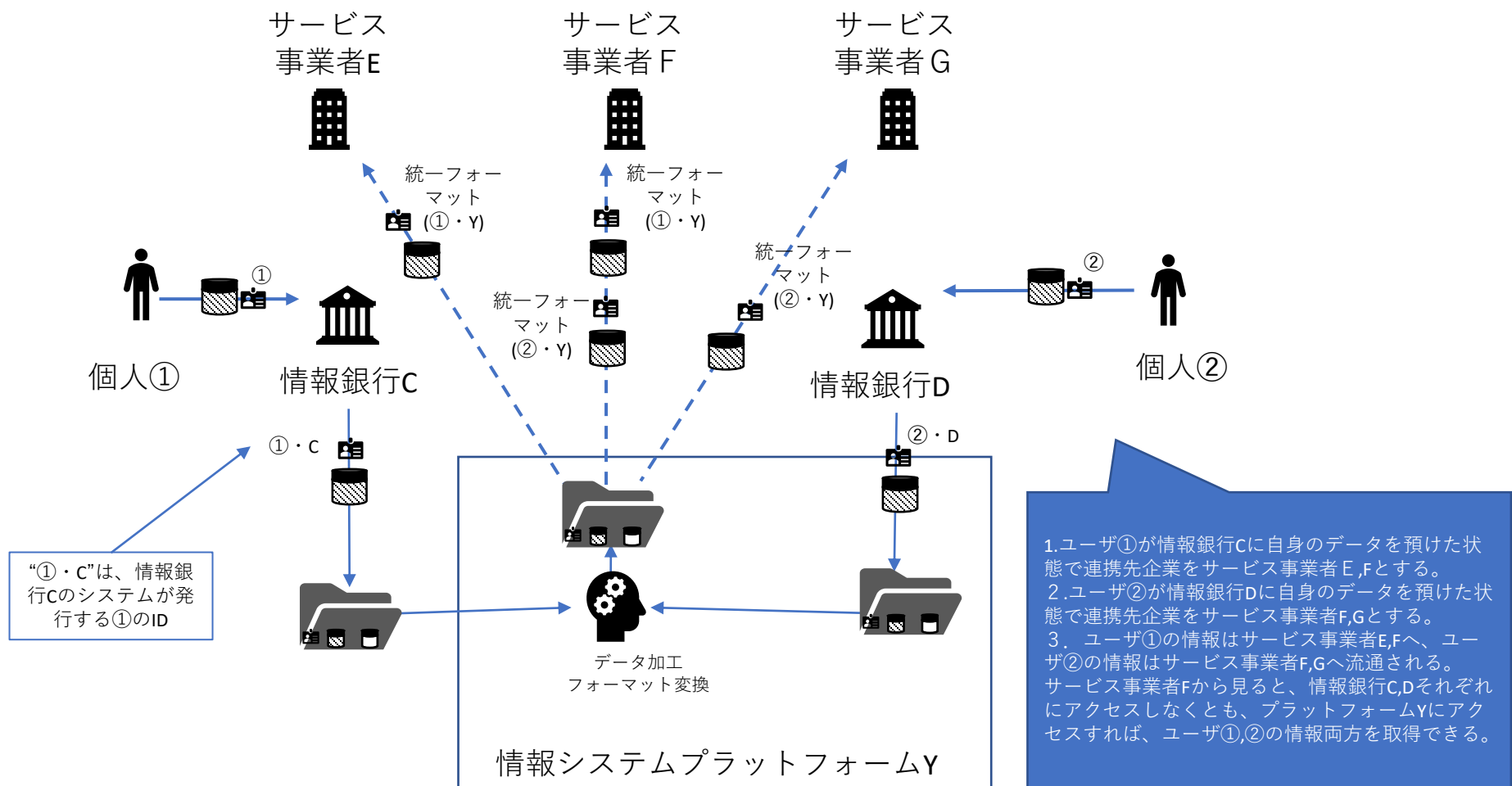
2. ビジネス関係

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



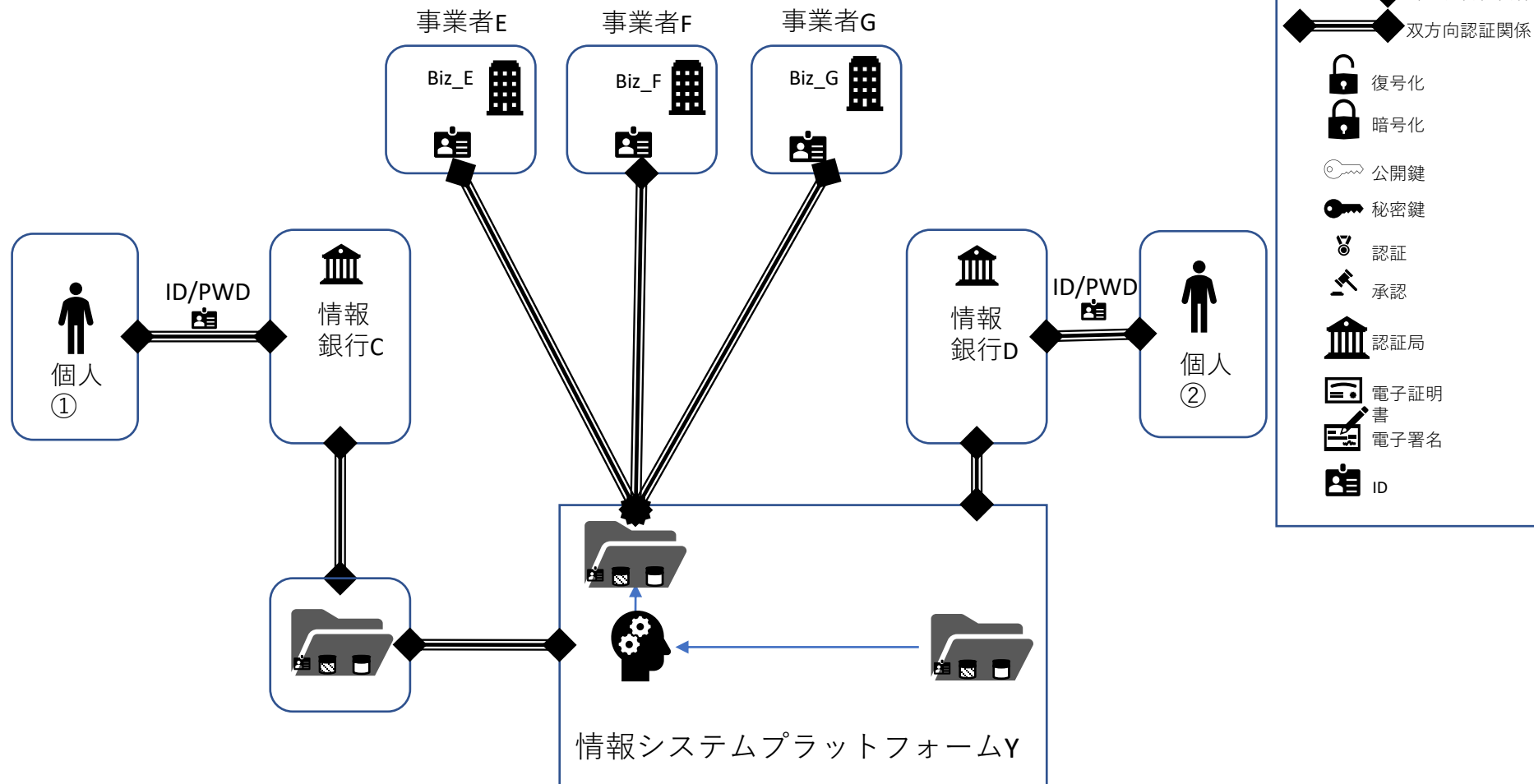
3. データリソースマップ

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。



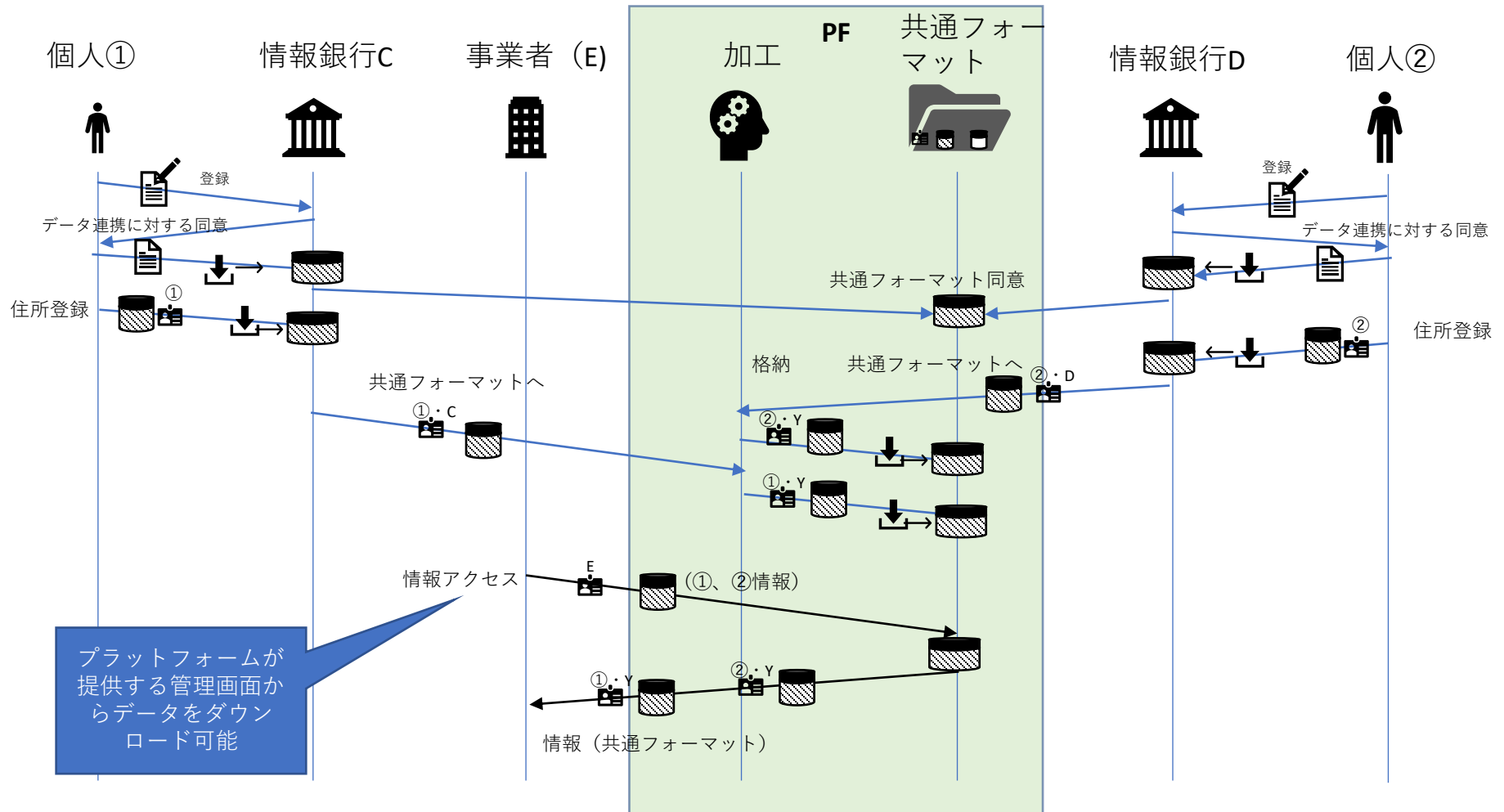
4. トラスト関係

目的：関係者間の認証・認可の関係を明らかにする



5. データフローシーケンス

目的：関係者間でのデータセットの移動、処理フローなどの手順を明確化する



6. 法制関係図（行政規制）

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

	個人①	情報銀行C	PDS事業者C	情報システムプラットフォームY運営事業者	情報銀行D	事業者E	事業者F	事業者G	個人②
個人①		第三者提供（個情法23条1項） 情報銀行C→事業者E, 事業者F	（情報銀行Cの一部なので？）			第三者提供（個情法23条1項） 情報銀行C→事業者E, 事業者F			
情報銀行C				委託（個情法22条, 23条5項1号） 情報銀行C→Y					
PDS事業者C									
情報システムプラットフォームY運営事業者					委託（個情法22条, 23条5項1号） 情報銀行D→Y				
情報銀行D							第三者提供（個情法23条1項） 情報銀行D→事業者F, 事業者G	第三者提供（個情法23条1項） 情報銀行D→事業者F, 事業者G	第三者提供（個情法23条1項） 情報銀行D→事業者F, 事業者G
事業者E									
事業者F									
事業者G									
個人②									

6. 法制関係図（契約関係）

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

	個人①	情報銀行C	PDS事業者C	情報システムプラットフォームY運営事業者	情報銀行D	事業者E	事業者F	事業者G	個人②
個人①		個人と「情報銀行」との間 利用 契約約款（モデル約款）（ver 1.0）	（情報銀行Cの一部なのは？）			「情報銀行」と情報提供先との間の個人 データ 提供契約（モデル 契約）（ver 1.0）			
情報銀行C				業務委託契約					
PDS事業者C									
情報システムプラットフォームY運営事業者					業務委託契約				
情報銀行D							「情報銀行」と情報提供先との間の個人 データ 提供 契約（モデル 契約）（ver 1.0）	「情報銀行」と情報提供先との間の個人 データ 提供 契約（モデル 契約）（ver 1.0）	個人と「情報銀行」との間 利用 契約約款（モデル約款）（ver 1.0）
事業者E									
事業者F									
事業者G									
個人②									

気づきやコメント

- 本手法の実践での気づき
 - データ提供が信頼し情報を預けられる仕組みづくり作りの必要性
 - データ連携に関する共通仕様の設定の必要性
- 個人の課題（便益の見える化）、企業の課題（魅力的サービスの創出）の解決に本手法を適用できるか？
 - データ提供ルールを統一的に定めることで、データ提供者主権型でのデータ流通が実現可能
 - 連携データに関する共通仕様を定義することで、各情報銀行での容易な連携が実現可能
- 社会実装する上で、本手法の役割・貢献・課題などは？
 - データ提供によるデータの管理に関する権限の強化と権限行使しやすい環境整備が今後必要
 - サービス事業者からの多様な連携仕様ニーズへの対応・対策を取りつつ共通仕様を定めることが課題

(b-2-2) 「情報銀行」を通じたデータの流通・活用に関するアーキテクチャの実証実験の実施

国立大学法人 大阪大学

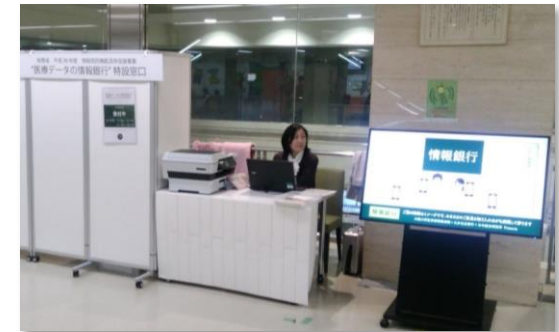
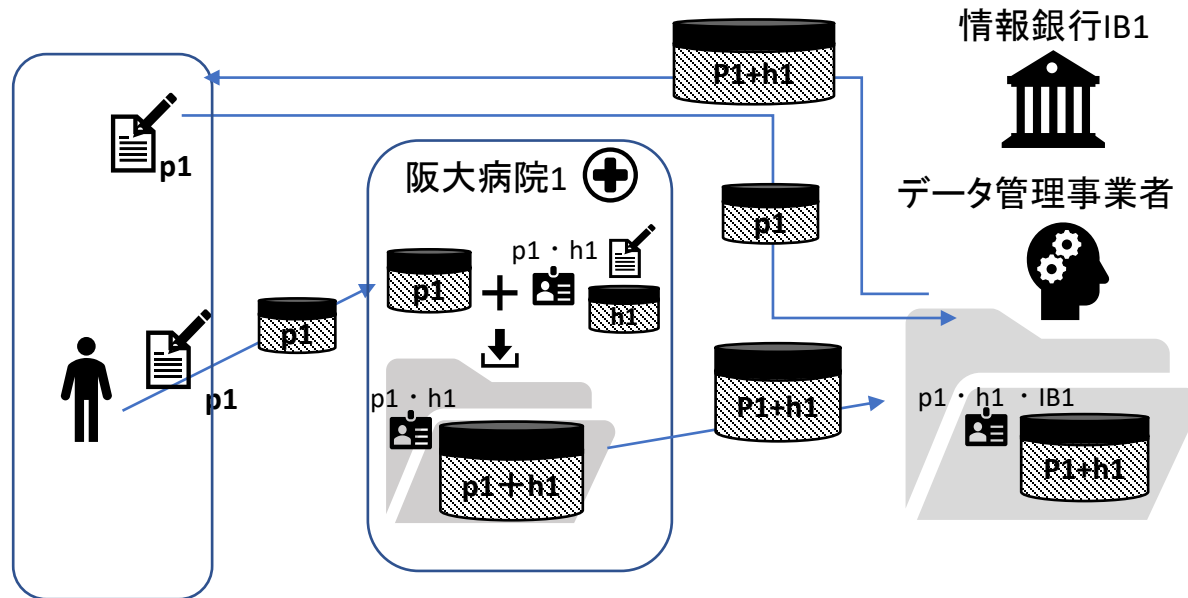
プロジェクト概要

項目	記載内容
プロジェクト名	個人起点での医療データ利活用の促進に向けた「医療版」情報銀行アーキテクチャの実証研究
記載者	松村泰志
所属	大阪大学大学院医学系研究科 医療情報学
連絡先	matumura@hp-info.med.osaka-u.ac.jp
記載日	2020年3月26日
プロジェクト概要	個人の信託を受けた医療情報銀行が、安全でかつ個人の意思を尊重した上で、医療データの、①医療での利用、②医療機関以外の組織が健康支援サービスを提供する際の利用、③生命保険等の給付手続きでの利用、④研究機関や製薬企業等の同一疾患の多数の仮名化した対象者データの解析利用を可能とするために医療データを流通させるアーキテクチャの設計とその部分的な実証。
備考	医療情報銀行を三井住友銀行が、データ管理事業者をNECが担う体制で、大阪大学医学部附属病院をフィールドとし、産科の患者を対象として実証を行った。

阪大病院での実証実験



- ・産科の患者を対象（申し込み者数：130人）
- ・妊婦健診データ、禁忌・アレルギー、検査結果、処方データ、超音波画像を情報銀行の個人のアカウントに送信
- ・自身のスマートフォンで閲覧可能
- ・地域連携システムとの連携



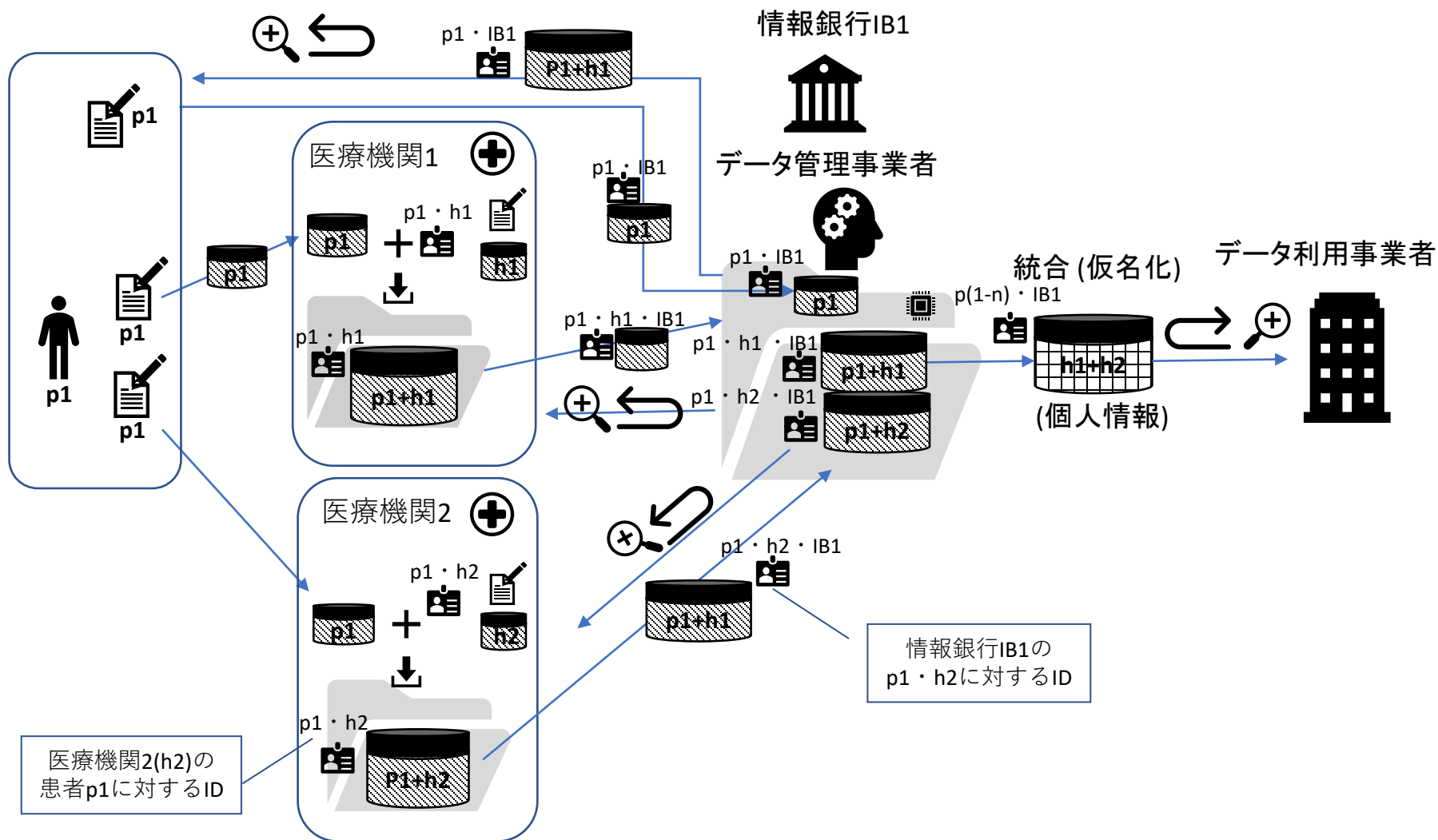
1. ステークホルダリスト

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（主に個人情報保護法での位置づけ等）	役割
個人	各医療機関を受診するなど、医療サービスを利用している個人	PII Principal
医療機関1	国立大学病院、国立病院（個人情報保護法上の独立行政法人）	PII Controller/ PII Processor
医療機関2	自治体により設置された病院（個人情報保護法上の地方独立行政法人）	PII Controller/ PII Processor
医療機関3	民間病院または診療所（個人情報保護法上の個人情報取扱事業者）	PII Controller/ PII Processor
調剤薬局	病院、診療所からの処方箋を受け取り、調剤を担当（個人情報取扱事業者）	PII Controller/ PII Processor
介護施設	介護施設（個人情報取扱事業者）	PII Controller/ PII Processor
健診センター	健診を主たる業務とする医療機関（個人情報取扱事業者）	PII Controller
情報銀行	個人の信託を受けて個人データを預かり、流通させる（個人情報取扱事業者）	PII Controller
データ管理事業者	情報銀行から委託により個人データを管理（個人情報取扱事業者に該当しない）	PII Processor
ヘルスサービス事業者	健康保険・介護保健の枠外で実施される民間の健康サービス提供事業者（個人情報取扱事業者）	PII Processor
データ利用事業者	匿名化された個人情報を仮想環境で利用する。原則的に、データ取得はしない（個人情報取扱事業者に該当しない）	PII Processor/ 3rd Party

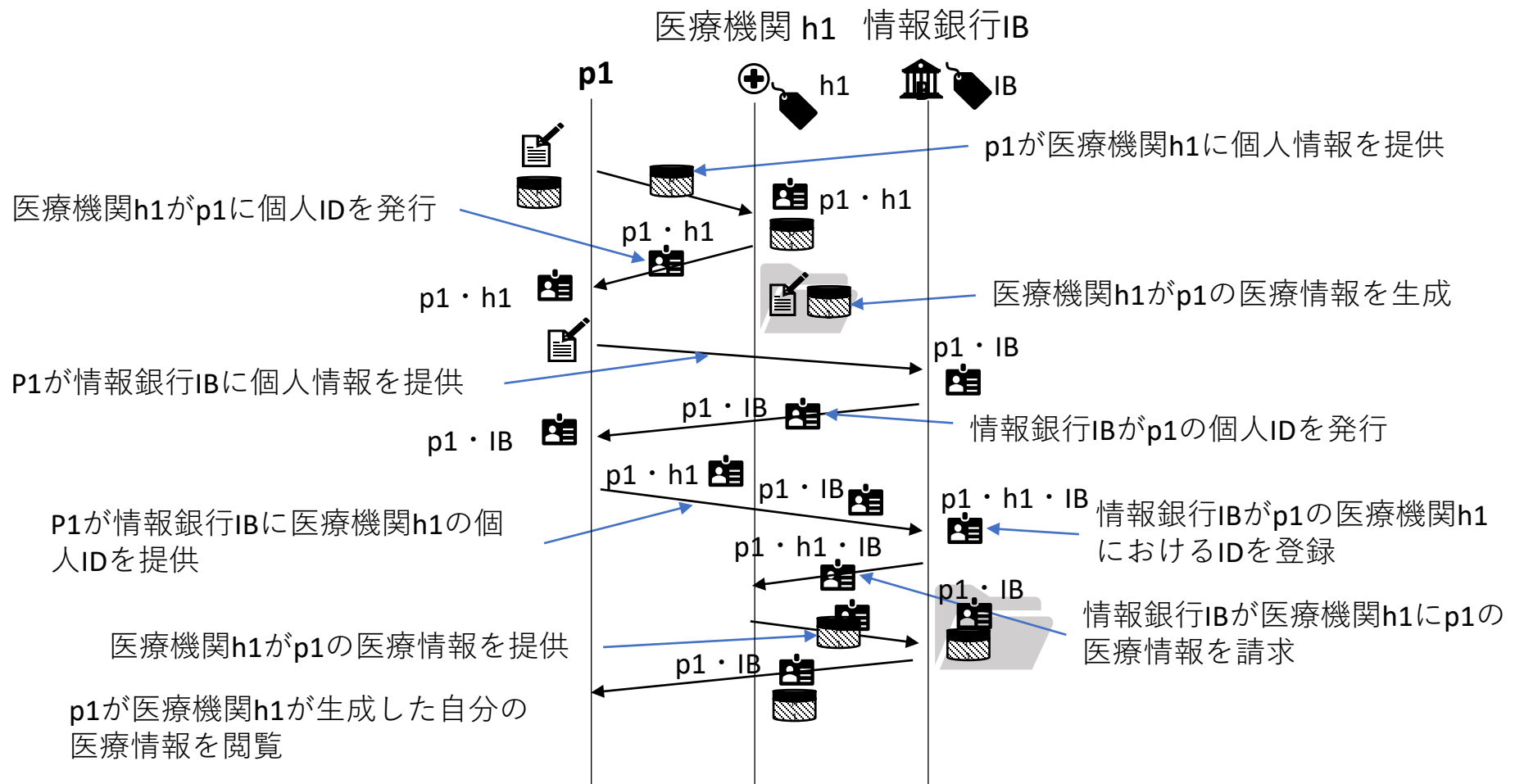
3. データリソースマップ

医療機関で発生するデータの閲覧・利用



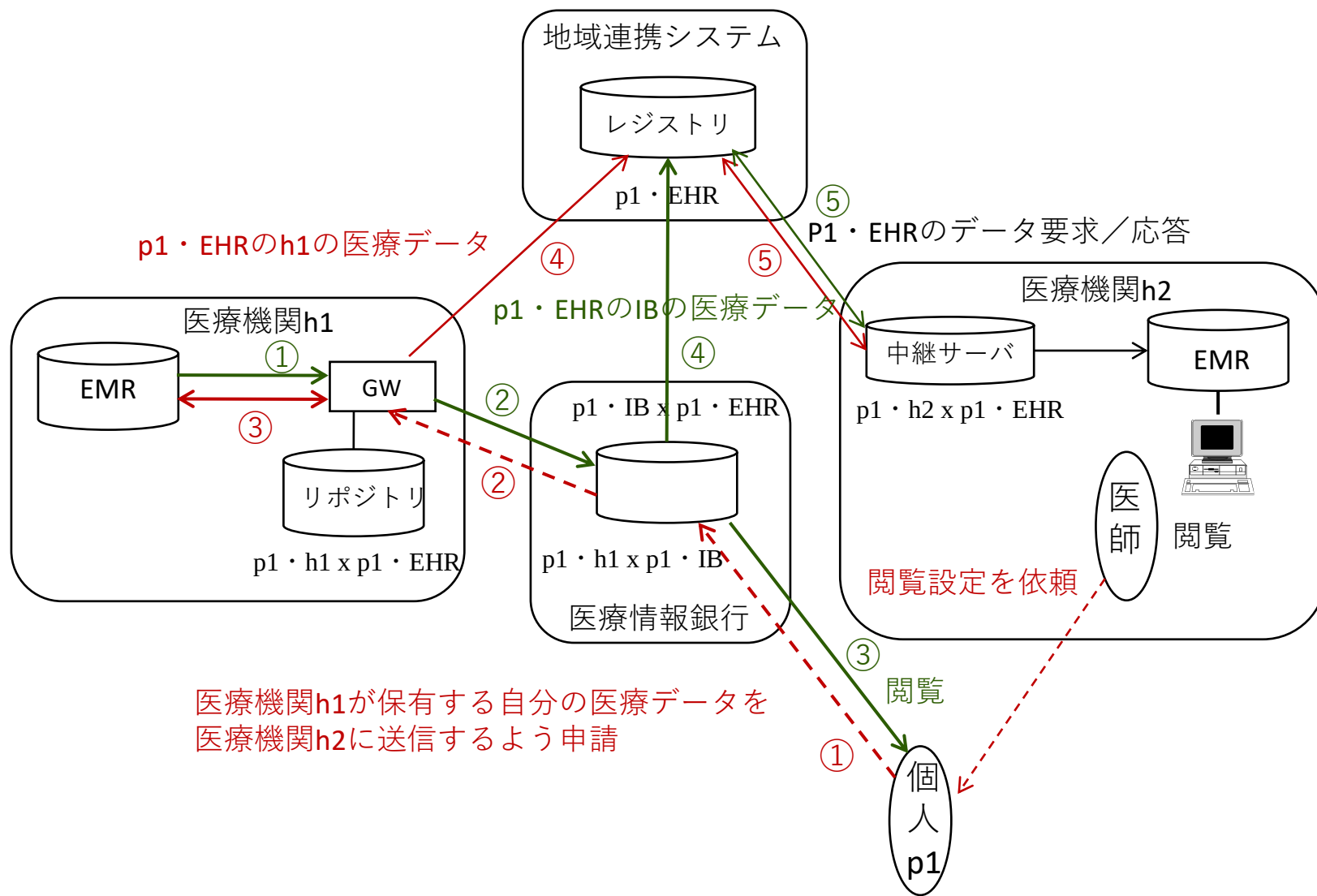
5. データフローシーケンス

個人が医療機関が生成した自分の医療情報を閲覧するまで

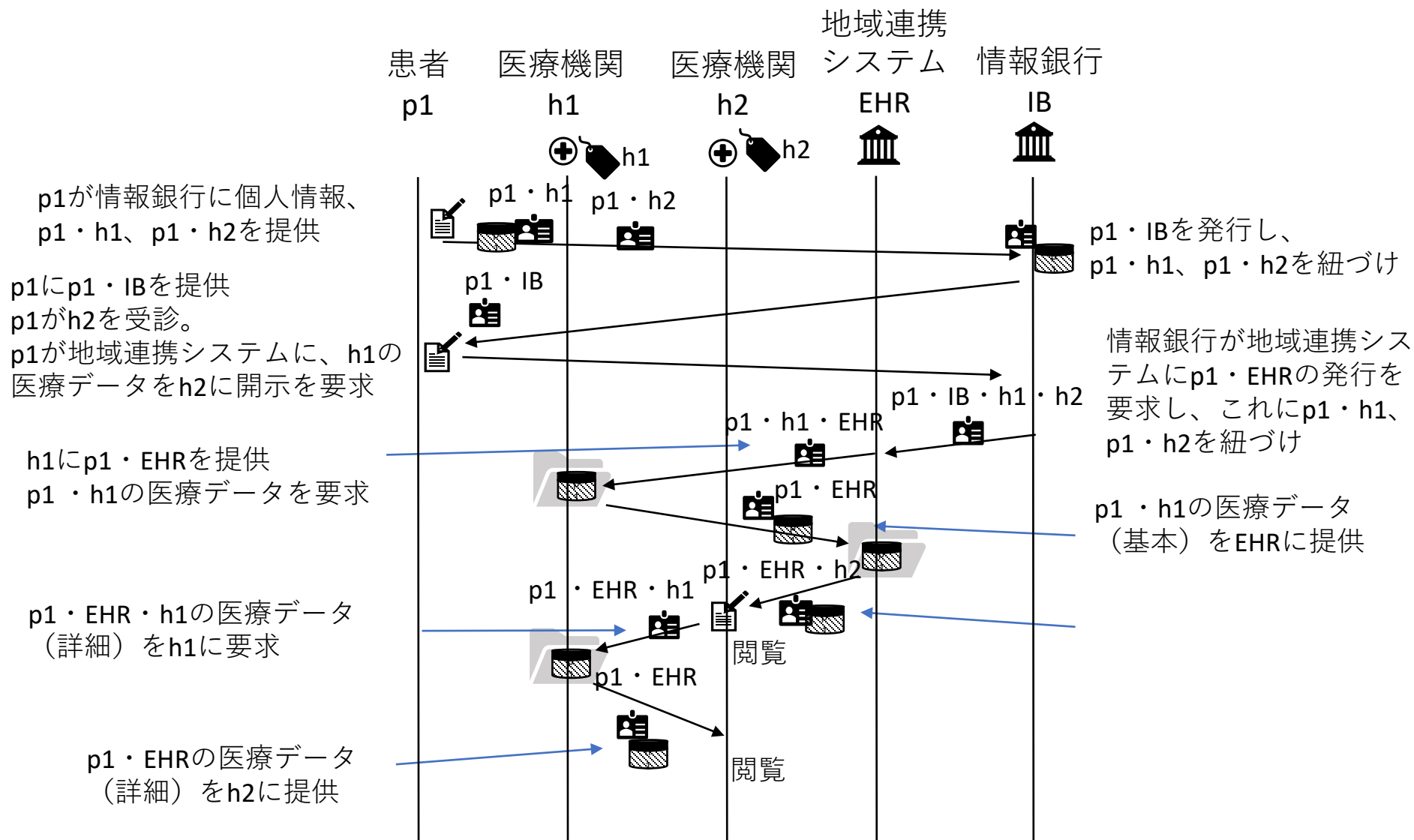


地域医療連携システム（EHR）と医療情報銀行（PHR）の連携

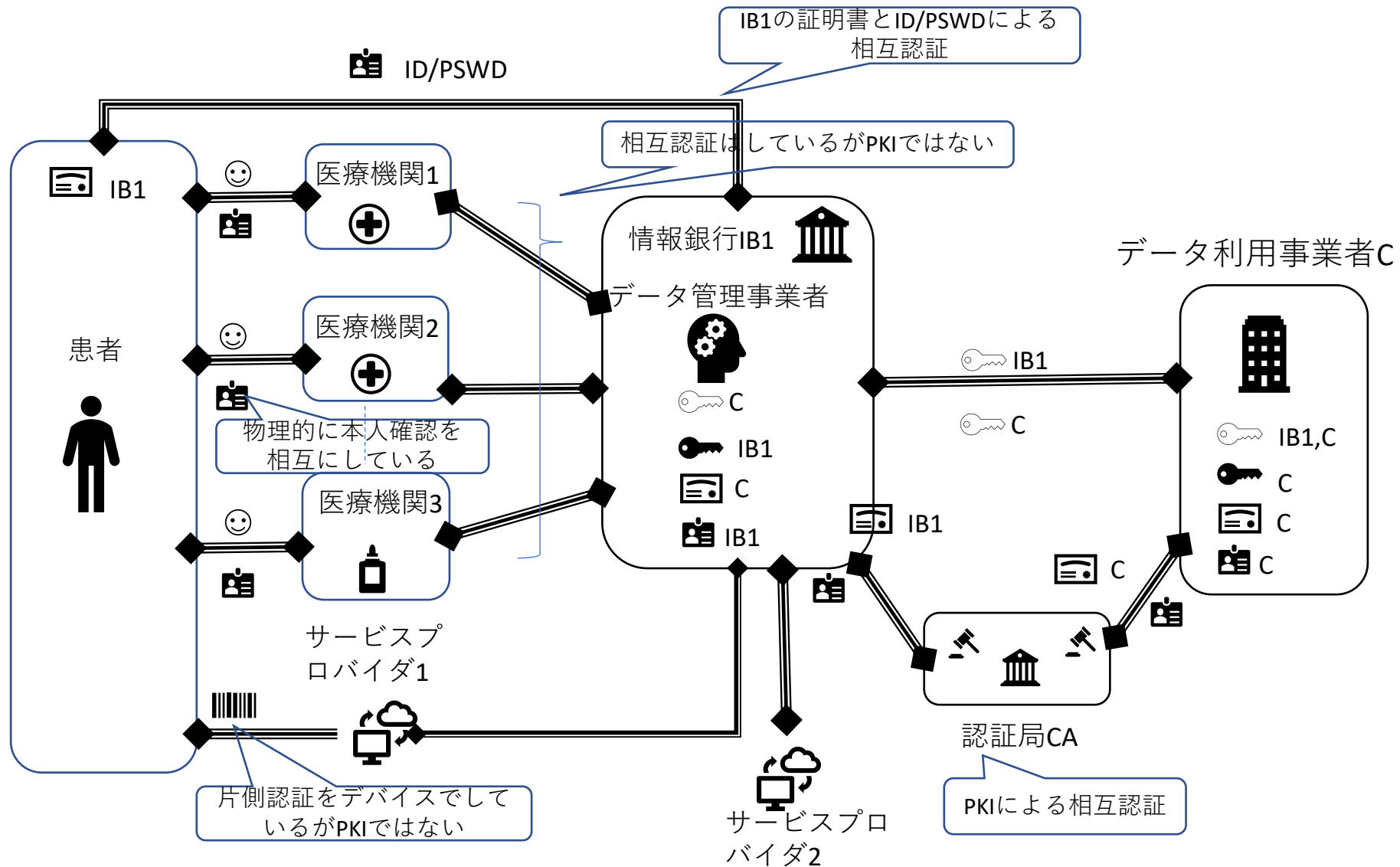
- ・ 情報銀行端末から医療機関h1の自分の医療データを医療機関h2の医師に見せる申請
- ・ 医療情報銀行の自分の医療データを医療機関h2の中継サーバを介し医師に見せる



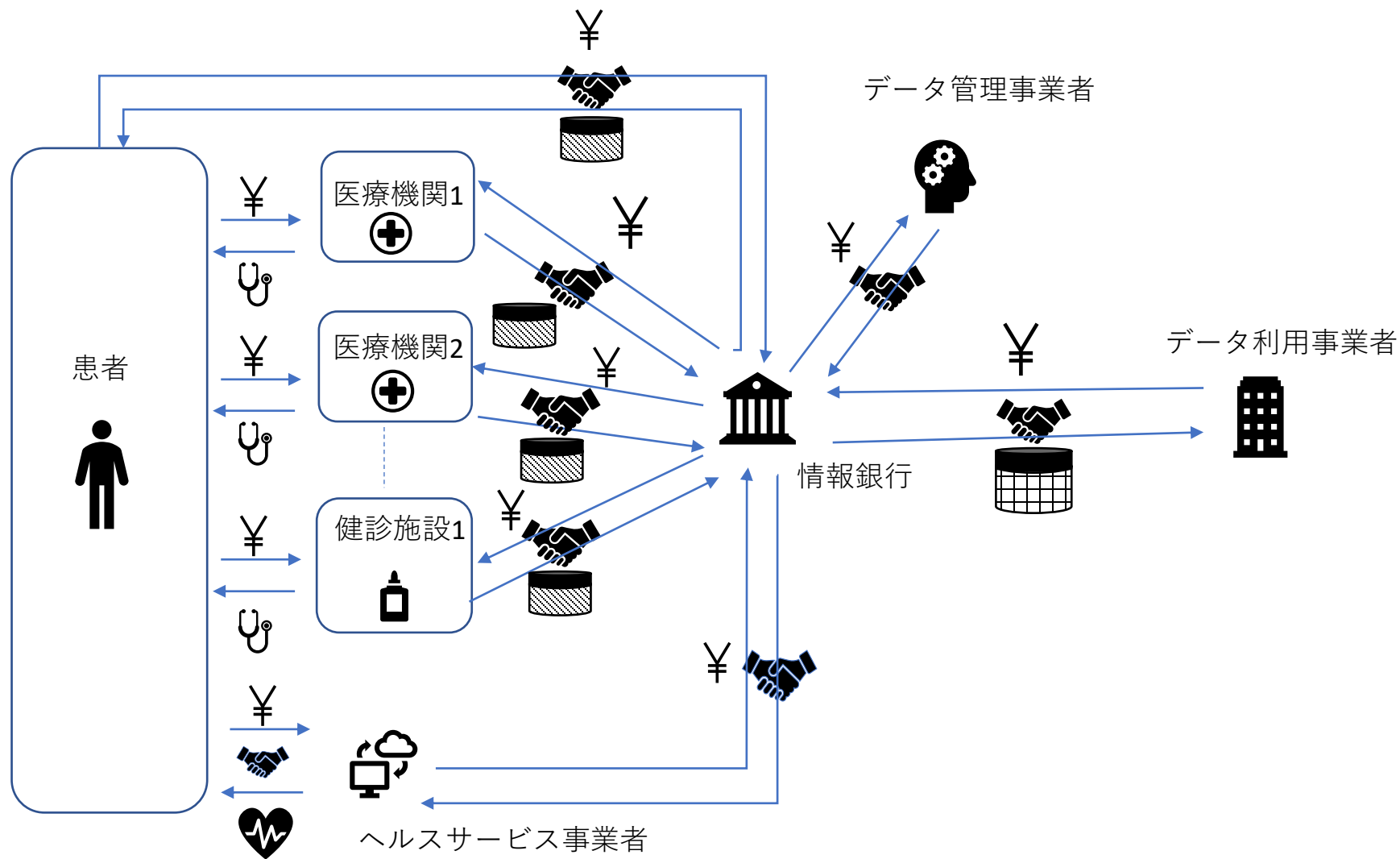
医療機関1の医療データを地域連携システムを介して医療機関2で閲覧



4. トラスト関係図



2. ビジネス関係図



6. 法制関係図

・「医療特化型情報銀行」については、要配慮個人情報を取り扱うものとなるため、現時点（2020年2月時点）では情報銀行としての認証対象とはならない。このため、情報銀行に係るモデル契約の適用有無については、本図面で言及をしていない。

	個人	医療機関1	医療機関2	医療機関3	情報銀行	データ加工事業者	データ利用事業者	ヘルスサービス事業者
個人		受診契約（個人情報利用・移転の同意）	受診契約（個人情報利用・移転の同意）	受診契約（個人情報利用・移転の同意）	要配慮個人情報の「情報銀行」類似サービス利用契約			サービスプロバイダのサービス利用契約
医療機関1（国）	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を遵守				サービス連携（情報の移転を含む）契約			
医療機関2（地方公共団体）	所在地の個人情報保護法令を遵守				同上			
医療機関3（民間）	個人情報の保護に関する法律を遵守				同上			
情報銀行	同上	サービス連携（情報の移転を含む）契約を遵守	同左	同左		業務委託契約（個人情報処理の委託を含む）	データ利用事業者の情報利用契約（個人情報の第三者提供を含）	サービスプロバイダの情報利用契約（情報移転の根拠となる）
データ加工事業者	個人情報の保護に関する法律の他事業分野の法令				業務委託契約を遵守			
データ利用事業者	同上				データ利用事業者の情報利用契約を遵守			
ヘルスサービス事業者	同上				サービスプロバイダの情報利用契約遵守			

気づきやコメント

- 本手法の実践での気づき

- 個人の医療データの管理・流通には、多くのステークホルダーがあり、多種の制約がある中で、全体像を詳細に描こうとすると、極めて複雑となる。
- 個人データの流通において、どのような視点で全体を俯瞰する必要があるかが与えられており、大きな視点での検討の抜けがなくなる利点がある。例えば、我々の医療情報銀行のプロジェクトでは、トラスト関係図の検討がなされていなかったが、そのことに気付くことができた（提出したトラスト関係図は、あるべき形を記載したものであり、現状のものではない）。
- 各視点毎に詳細を記載する手法が提示されており、詳細内容に至るまで、複数で認識を共有できる利点がある。これにより、詳細レベルで関係者間で議論ができるようになった。
- 最初に本アーキテクチャの記載法を教わった時には、意味が理解しにくかったが、取り組んでいるうちに意味していることとその重要性、記載することの意義が理解できるようになった。

気づきやコメント

- 個人の課題（便益の見える化）、企業の課題（魅力的サービスの創出）の解決に本手法を適用できるか？
 - 医療データの場合、医療での利用については理解されやすいが、医療機関以外の事業者による医療データの利用については、アイデアが潜在している可能性がある。医療データの流通サービスが実施できた場合、そのアーキテクチャが見えると、新たな事業者の参入が期待できる。
 - ビジネス関係図が、ビジネスを考える上では重要な図である。ビジネスモデルを検討する上で有効と思われる。
 - 医療情報銀行は、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。

気づきやコメント

- 社会実装する上で、本手法の役割・貢献・課題などは？
 - 医療データの流通サービスは、多くのステークホルダーが関わる事業であり、合意形成が難しいと予想される。議論すべきポイントは多方面に及ぶので、議論が噛み合いにくいことが懸念される。議論を始める前に、参加者が原案のアーキテクチャーを理解し、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。
 - データフローシーケンス図がデータフローを可視化する上で有効であるが、細かく記載すると全体的な流れが分かりにくくなる。複数のデータフローパターンをモジュール化して抽象的に表現できると、分かりやすい表現になるのではないだろうか。
 - アーキテクチャ図をPowerPointで作成したが、スライド原稿のスペースの範囲内に表現するのに苦労をした。アーキテクチャーを描く専用ソフトを開発し、スペースを気にせず記載ができ、アイコンを簡単な操作で貼り付け、矢印を引けることができると有用と思う。データフローシーケンス図とデータリソースマップは対応関係があり、データリソースマップ上でデータの動きを動画で見せることができると、より直感的に理解しやすくなると思われる。専用ソフトにより、こうしたことが可能になるのではないかと考える。

(b-2-4) 生体認証データの事業者間の連携に関するアーキテクチャの実証研究の実施

日本電気株式会社

プロジェクト概要

以下にご記載ください

項目	記載内容
プロジェクト名	生体認証（顔特徴量）データの事業者間連携に関するアーキテクチャ実証研究」
記載者	桑原 智宏
所属	日本電気株式会社 デジタルプラットフォーム事業部
連絡先	N/A
記載日	2020年3月24日
プロジェクト概要	生体認証（特に顔認証）の横断的活用に向けた、複数事業者によるID連携に関する実証を行うとともに、関係するインターフェース、標準化、連携に関するルール、制度などのアーキテクチャの設計・構築を行い、リスクの低減、社会的な消費者の受容性拡大を目指します
備考	

1. ステークホルダリスト

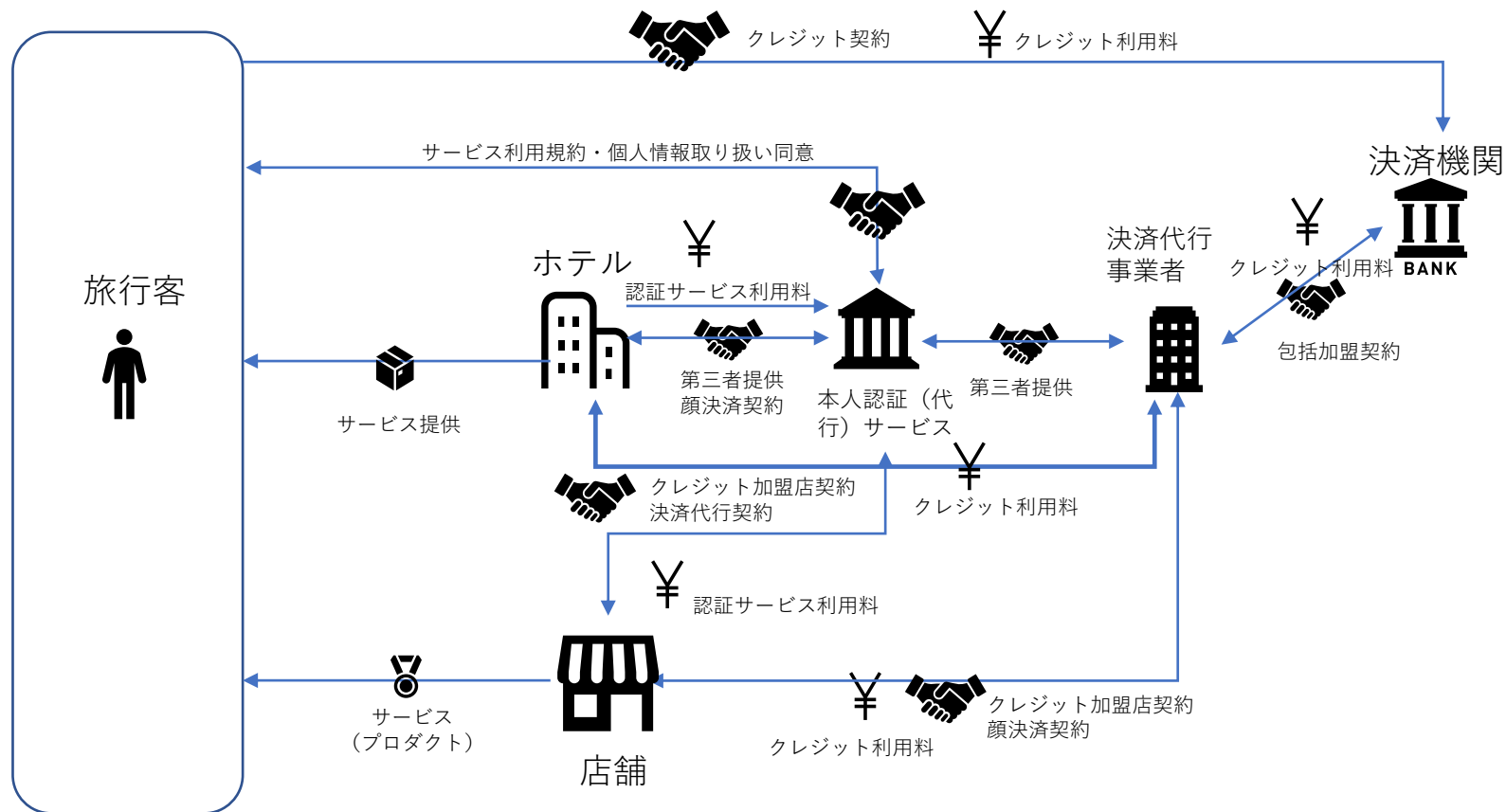
目的：関与する個人、事業者の一覧表を作成することで、パーソナルデータの取り扱われる範囲を明確し、プライバシー原則などを遵守すべきプレイヤーに抜けがないかを確認する

名称	概要（主に個人情報保護法での位置づけ等）	役割
旅行客	各施設でサービスを受ける利用者	PII Principal
ホテル	宿泊客の個人情報を取り扱い、予約者と事前登録された顔情報を紐づけるため、個人情報保護法上の個人情報取扱事業者に該当	3 rd Party
本人認証（代行）サービス	旅行客の顔情報を取り扱うため、個人情報保護法上の個人情報取扱事業者に該当	PII Controller/ PII Processor
決済代行事業者	（クレジットカード契約としての）旅行客の個人情報を取り扱うため、個人情報保護法上の個人情報取扱事業者に該当	3 rd Party
決済機関	（引き落とし口座としての）旅行客の個人情報を取り扱うため、個人情報保護法上の個人情報取扱事業者に該当	非該当
店舗	決済を実施するための端末を設置し、決済情報を端末に手入力し、認証結果に基づき本人確認を行うため、個人情報保護法上の個人情報取扱事業者に該当	3 rd Party

※役割は顔関連データに関するものだけ記載。決済機関はカード情報を扱うPII Controllerとしても良いが、顔関連データは扱っていないので、非該当とした。この辺りの考え方の統一性には課題が残る。

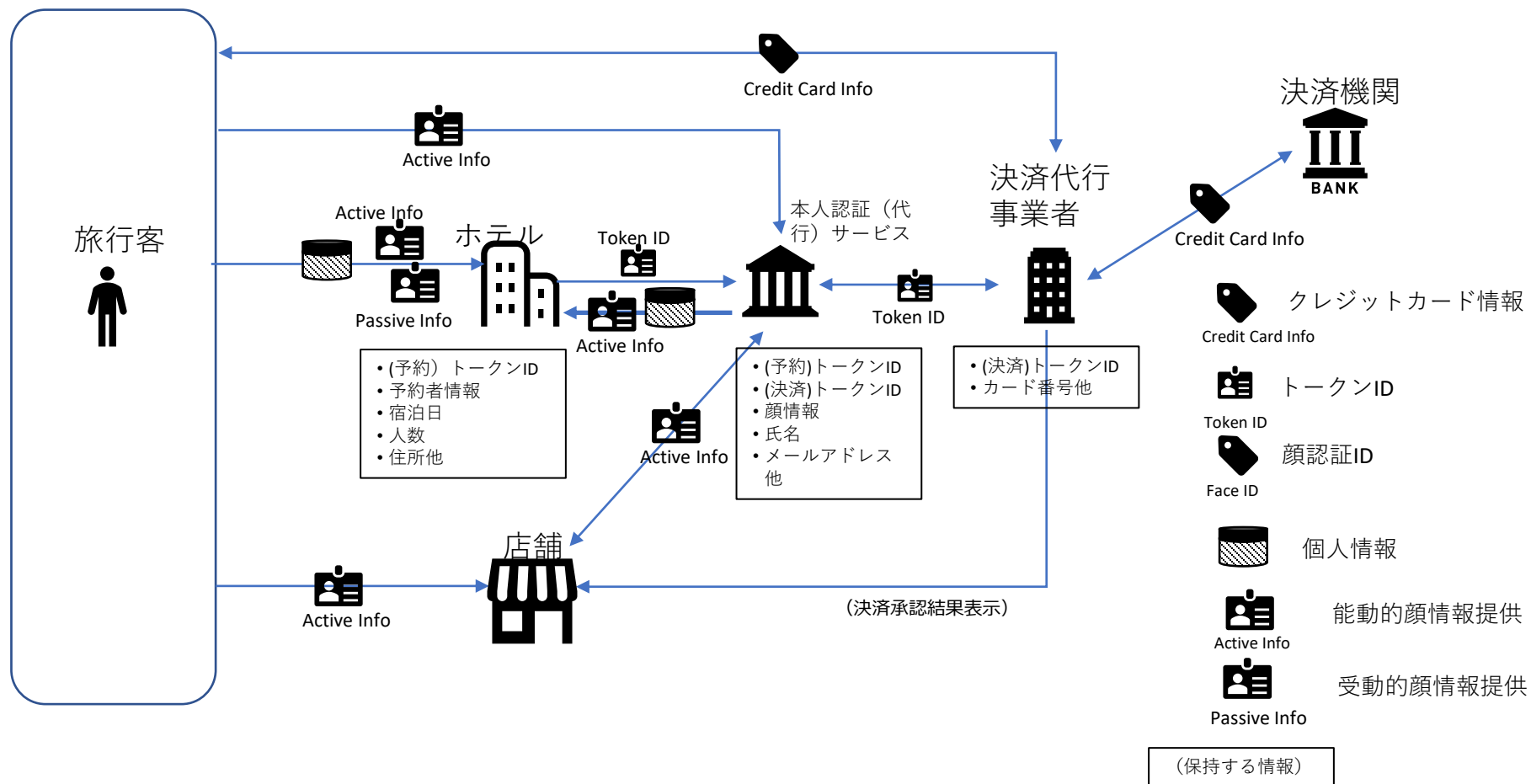
2. ビジネス関係

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



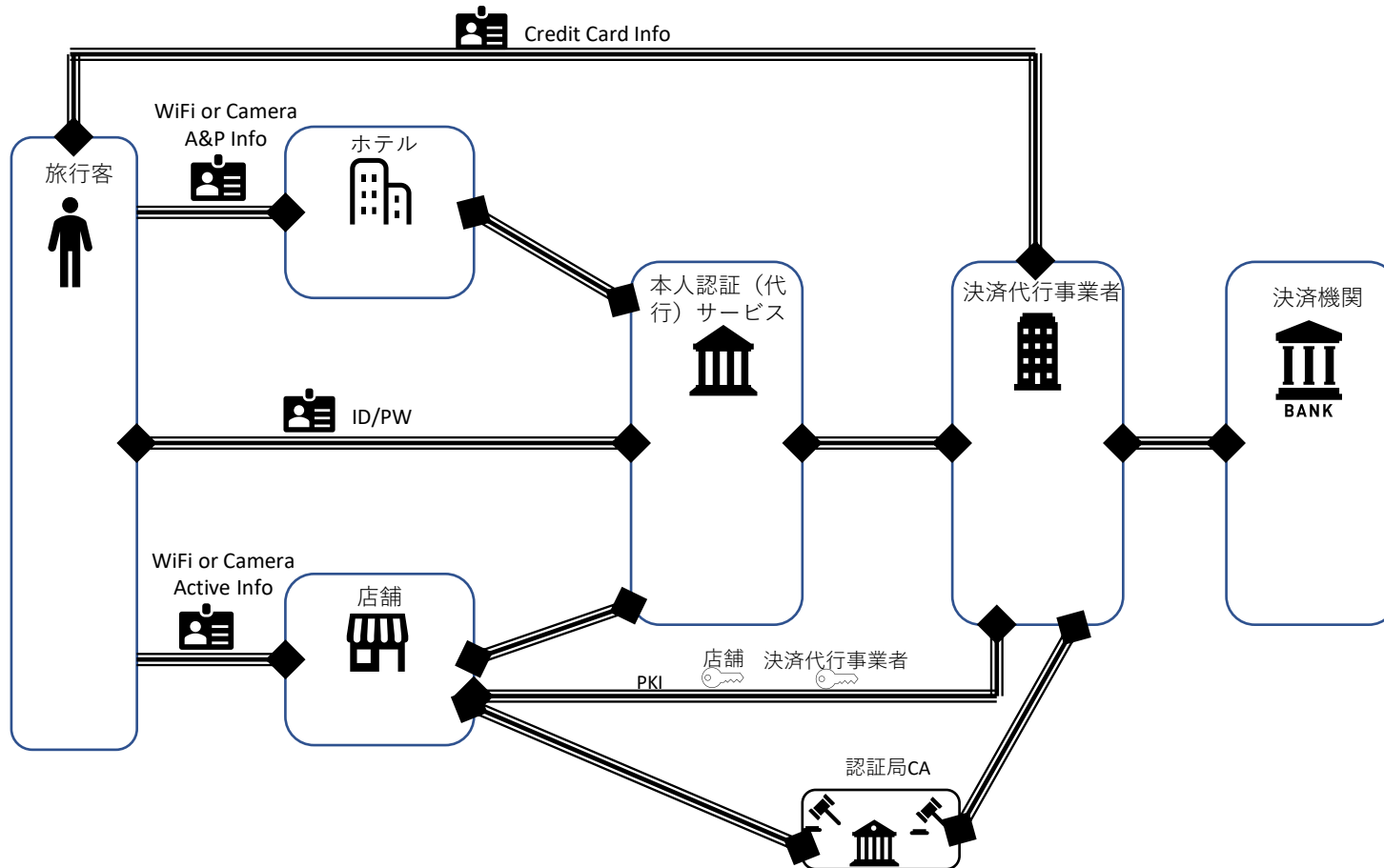
3. データリソースマップ

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



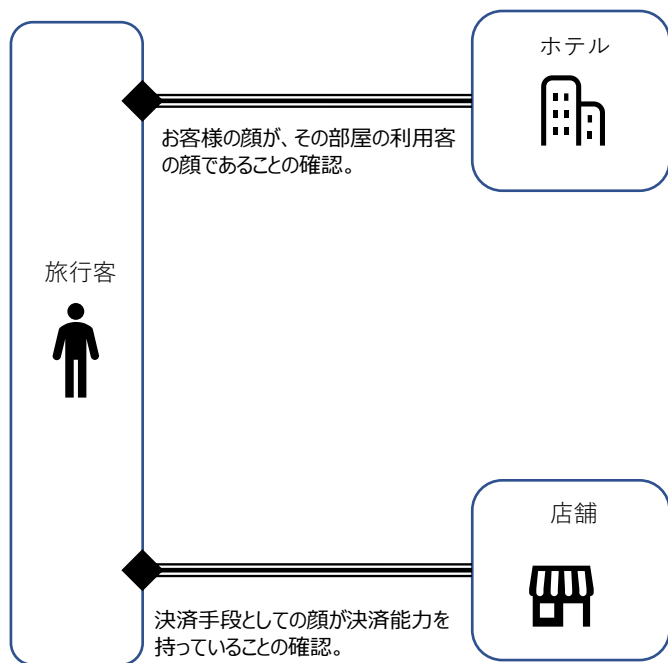
4. トラスト関係

目的：関係者間の認証・認可の関係を明らかにする



4. トラスト関係

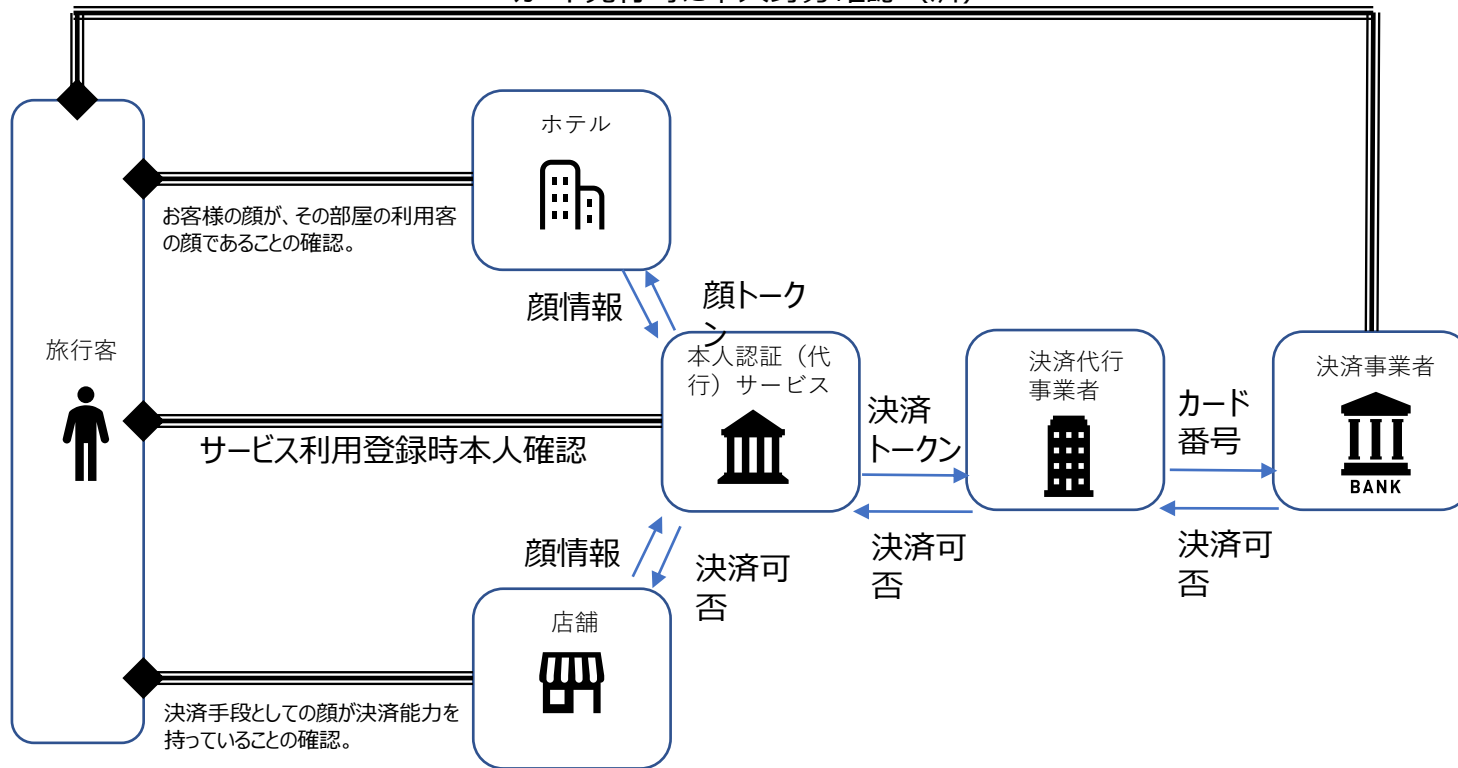
※各エンティティがサービスを提供するうえで必要なトラストに関する要求



4. トラスト関係

※各エンティティに必要なトラストのためのトラスト関係

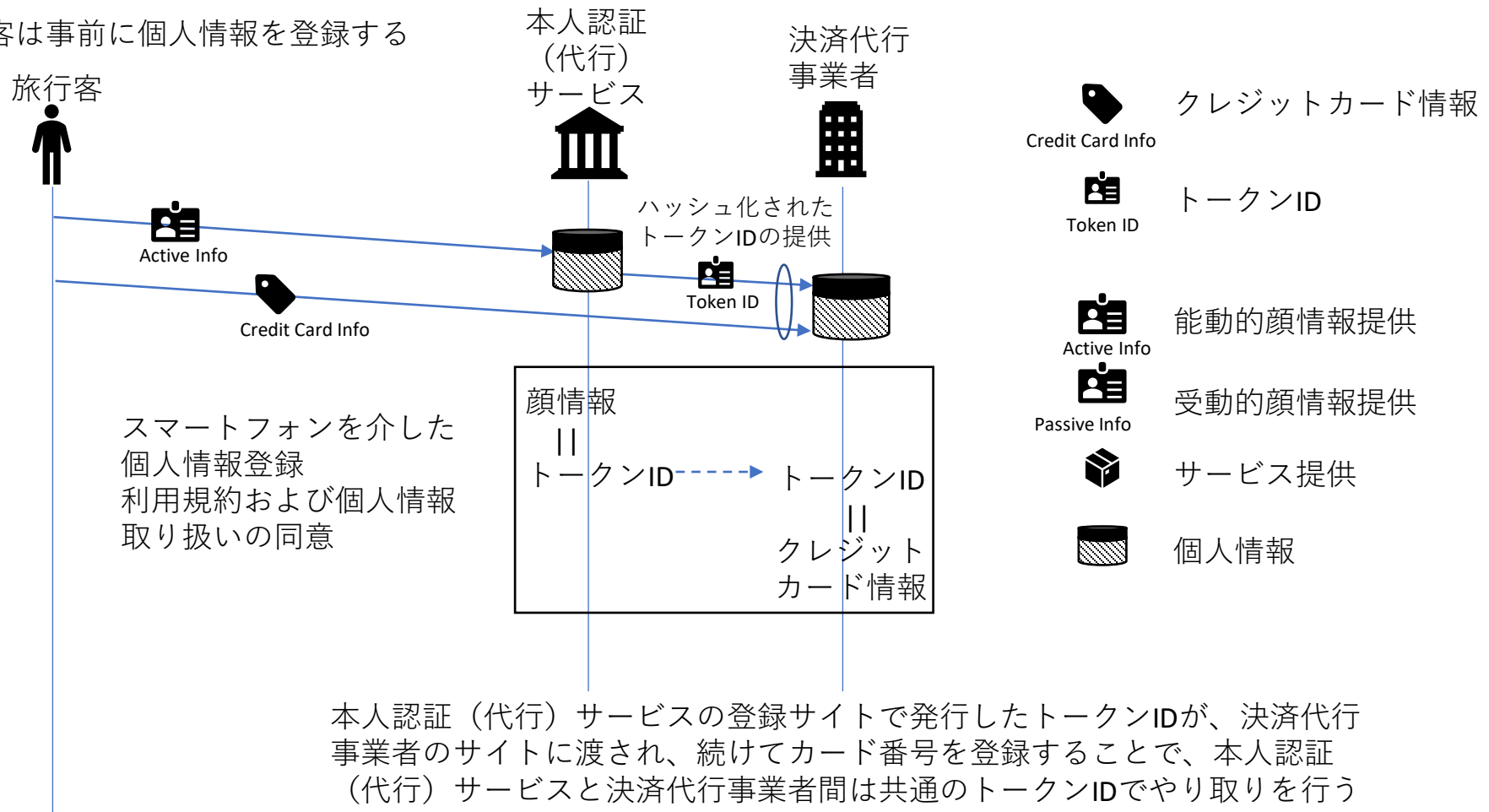
カード発行時に本人身分確認（済）



5. データフローシーケンス：ケース1

目的：関係者間でのデータセットの移動、処理フローなどの手順を明確化する

旅行者は事前に個人情報を登録する

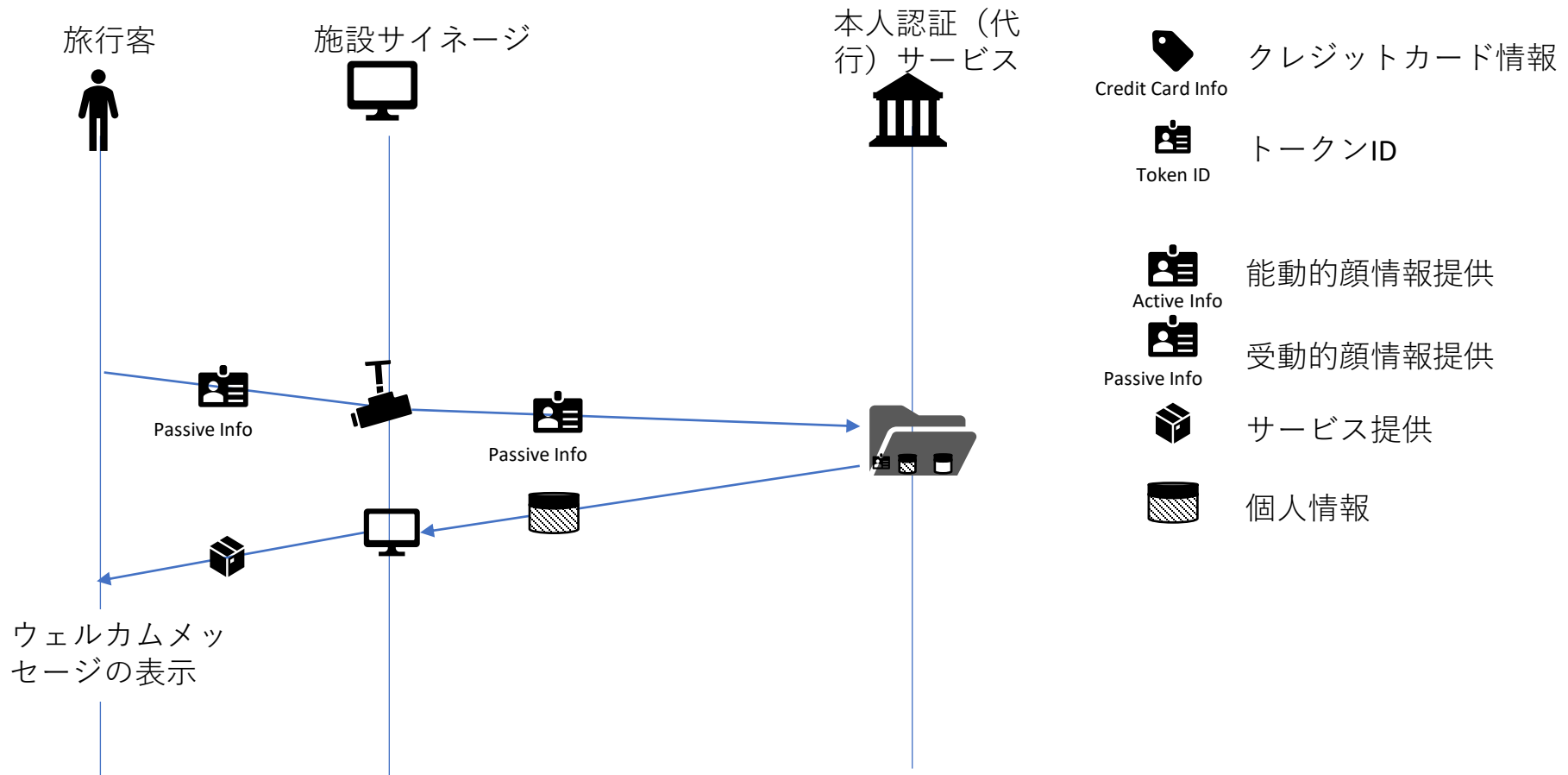


本人認証（代行）サービスの登録サイトで発行したトークンIDが、決済代行事業者のサイトに渡され、続けてカード番号を登録することで、本人認証（代行）サービスと決済代行事業者間には共通のトークンIDでやり取りを行う
※カード番号を流通させないよう、トークンを使った一般的な手法

5. データフローシナリオ：ケース2

目的：関係者間でのデータセットの移動、処理フローなどの手順を明確化する

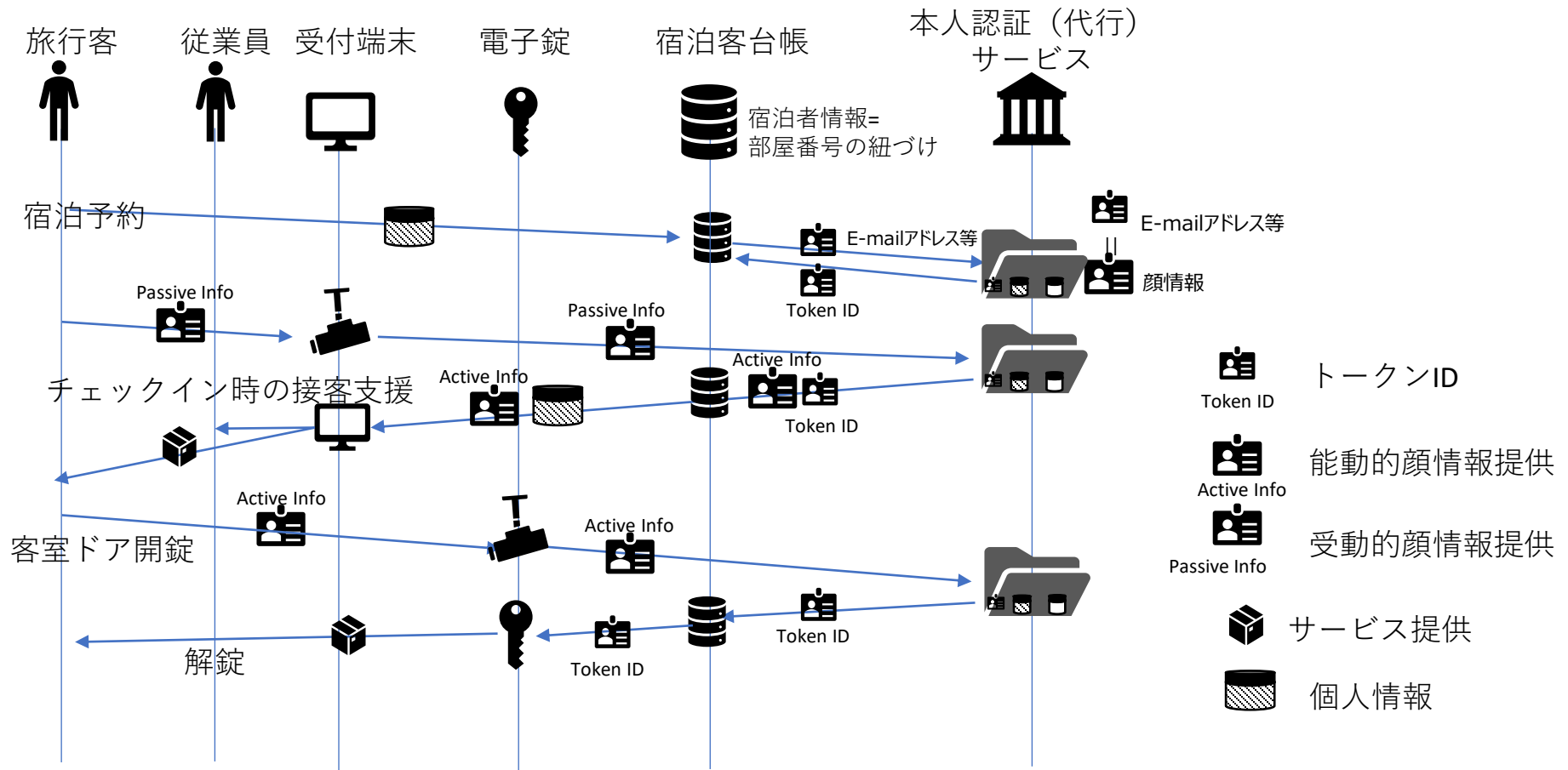
旅行者は事前に個人情報を登録し、空港や施設でサイネージからウェルカムメッセージを受け取る



5. データフローシーケンス：ケース3

目的：関係者間でのデータセットの移動、処理フローなどの手順を明確化する

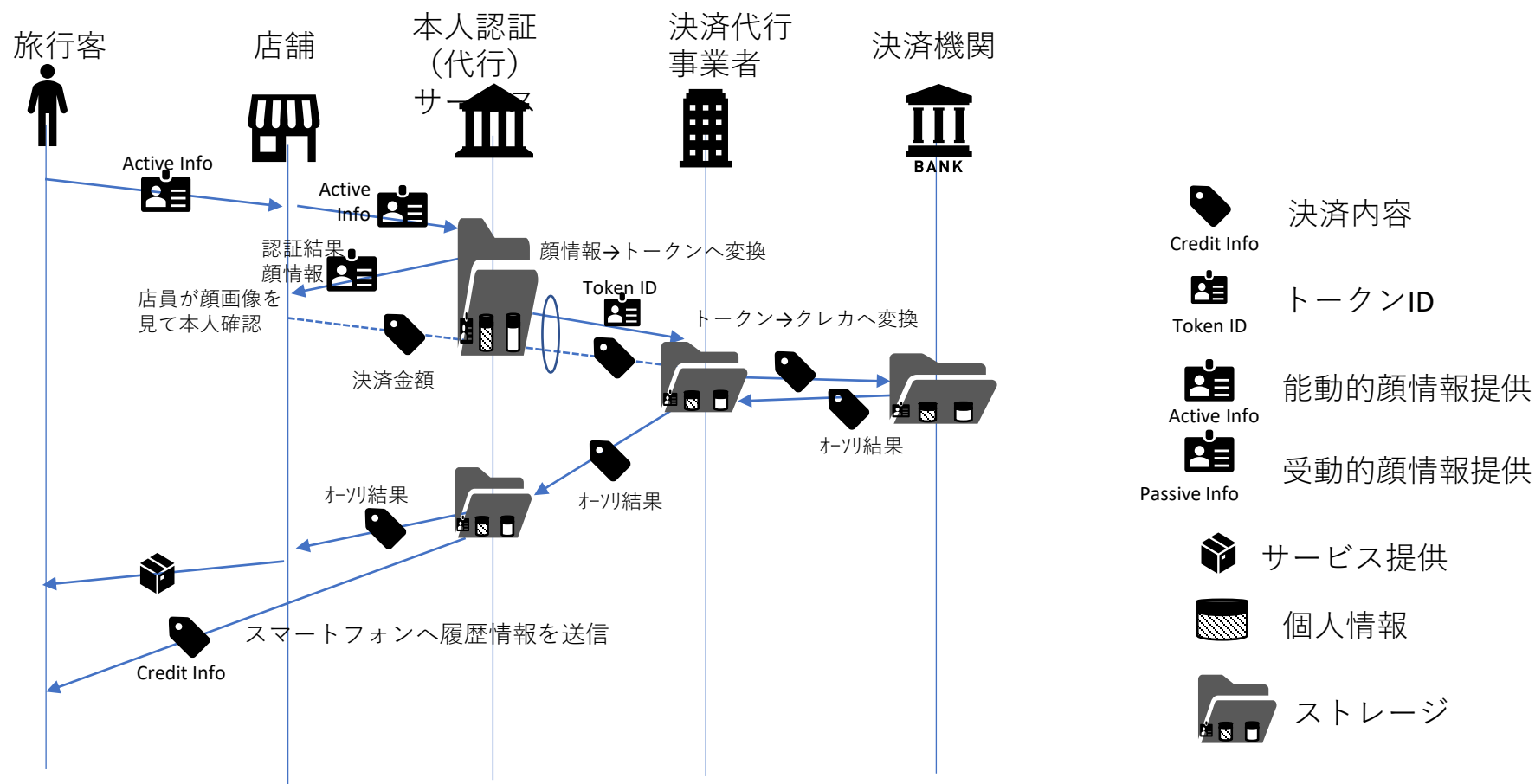
ホテルにおけるチェックインと部屋の解錠



5. データフローシーケンス：ケース4

目的：関係者間でのデータセットの移動、処理フローなどの手順を明確化する

店舗における決済



6. 法制関係図

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

	旅行者	ホテル	本人認証（代行）サービス	決済代行業者	決済機関	店舗
旅行者	NA	旅館業法 個人情報保護法	個人情報保護法	NA	クレジット 関連法制	NA
ホテル	旅館業法 個人情報保護法	NA	個人情報保護法 第三者提供顔決済 契約	クレジット 関連法制	NA	NA
本人認証 （代行） サービス	個人情報保護法	個人情報保護法 第三者提供 顔決済契約	NA	個人情報保 護法 第三者提供	NA	認証サービ ス利用契約
決済代行事 業者	NA	クレジット関連 法制	個人情報保護法 第三者提供	NA	クレジット 関連法制	クレジット 関連法制
決済機関	クレジット関連 法制	NA	NA	クレジット 関連法制	NA	NA
店舗	NA	NA	認証サービス利用 契約	クレジット 関連法制	NA	NA

気づきやコメント

- 本手法の実践での気づき
 - ステークホルダー間（事業者、利用者）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。
 - これにより、生体認証（顔特徴量）データの事業者間連携における、アーキテクチャの設計・構築に役立てることができた。
- 個人の課題（便益の見える化）、企業の課題（魅力的サービスの創出）の解決に本手法を適用できるか？
 - 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ます。
 - 本手法のような、顔情報連携における標準的な認証連携フローや法制度・ルールの整理により、顔認証を使ってサービスを提供する事業者のリスク低減につながると考えます。
- 社会実装する上で、本手法の役割・貢献・課題などは？
 - 上記に回答した通り、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と考えます。
 - 本手法についての課題は特にはありません。

(b-2-5) 特定エリアにおける行動データの事業者間の連携に関するアーキテクチャの実証研究の実施

KDDI株式会社

プロジェクト概要

以下にご記載ください

項目	記載内容
プロジェクト名	戦略的イノベーション創造プログラム（S I P）第2期／ビッグデータ・A I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／横浜スタジアムを中心とした行動データ利活用のアーキテクチャに関する実証研究
記載者	小原 孝介 マネージャー
所属	KDDI株式会社 パーソナル事業本部 ビジネス開発本部 パートナービジネス開発部
連絡先	ko-ohara@kddi.com
記載日	2020/03/30
プロジェクト概要	本研究開発実証では、パーソナルデータを扱うことにおける、都市・地域における課題とそのエリアで経済活動を行う商業施設や店舗を構える企業の課題を主なターゲットとして、行動データの事業者間の連携によって安全なデータ連携の仕組みや基盤整備と実用化を図ることを目的として実施した。 エリアマーケティング施策として、デジタルサイネージ広告を活用した施策、デジタルサイネージ広告を活用した施策、デジタルサイネージ広告を活用した施策、auPAY利用促進キャンペーンを実施、データ取得・効果検証とともに、アーキテクチャ検討の協議を実施した。
備考	

1.ステークホルダリスト

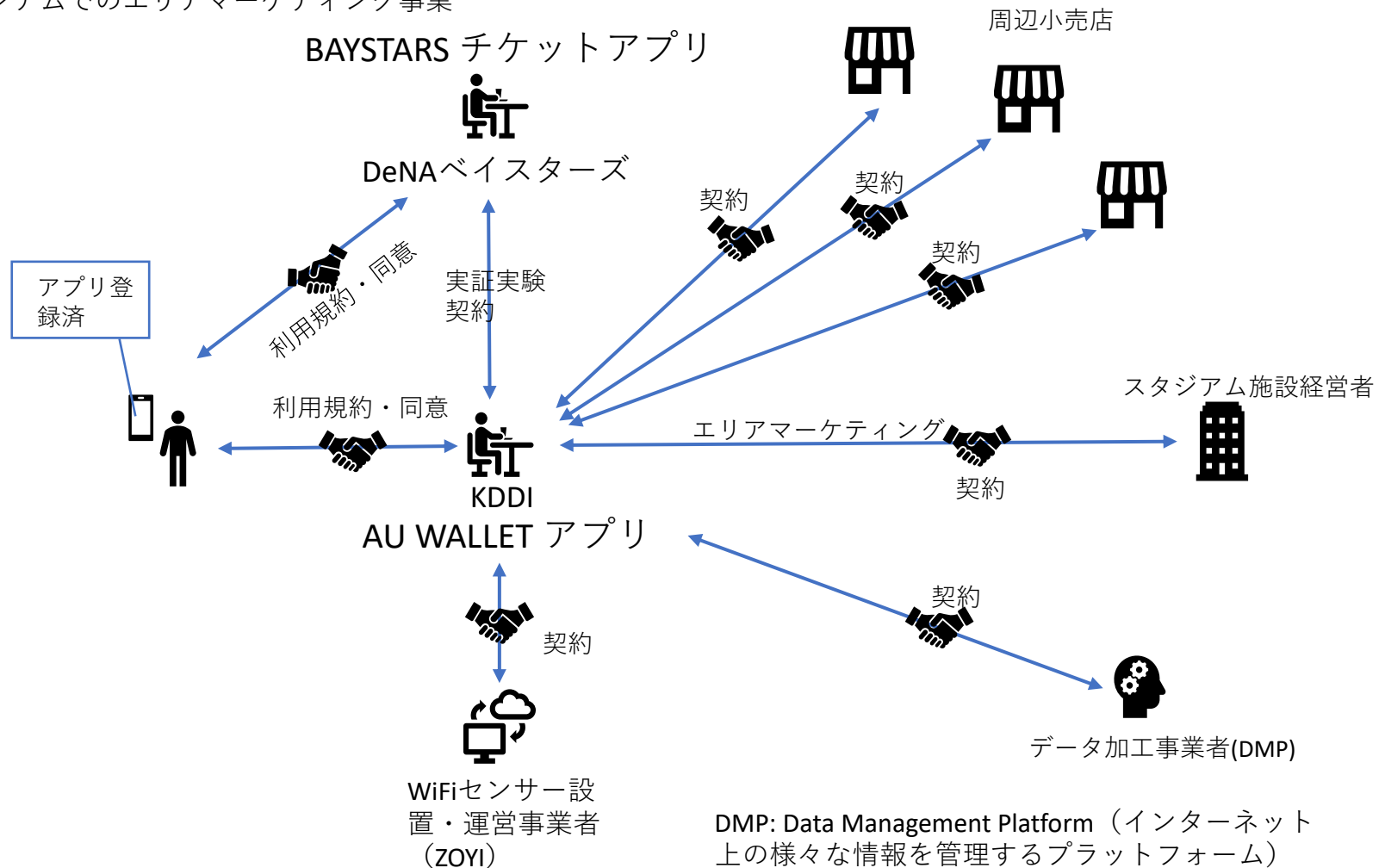
- ・ 国外の準拠法については不問

名称	概要（主に個人情報保護法での位置づけ等）	役割
来場者	アプリを通じてサービスを利用 ・利用規約	PII Principal
スタジアム	来場者に設備を提供、事業者(KDDI)とエリアマーケティング事業実施 ・プライバシーポリシー ・委託元との契約	PII Processor
ベ이스ターズ	アプリを提供、事業者(KDDI)とエリアマーケティング事業を実施 ・プライバシーポリシー ・委託元との契約 ・来場者との間で「個人情報保護法」遵守	PII Processor
KDDI	エリアマーケティング事業の企画、運営、実施。来場者にアプリ、サービスを提供。 ・プライバシーポリシー ・委託元としての「委託先監督義務」 ・来場者との間で「個人情報保護法」遵守 ・サービス提供において「独占禁止法」遵守 ・電気通信事業において「電気通信事業法」「施行規則」「携帯電話不正利用防止法」 「青少年インターネット環境整備法」「特定商取引法」「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」の遵守	PII Controller
周辺小売店	事業者(KDDI)からみてBtoB顧客。WALLETサービス、WiFiサービスの設備を設置 ・プライバシーポリシー ・委託元との契約	PII Processor
データ加工事業者 (DMP)	事業者(KDDI)の委託によりデータ加工、分析を実施。 ・プライバシーポリシー ・委託元との契約	PII Processor
WiFi設置・運営事業者 (ZOYI)	事業者(KDDI)からの委託によりWiFi設備の設置、運営。収集したデータの分析、加工の実施。 ・プライバシーポリシー ・委託元との契約	PII Processor

2. ビジネス関係

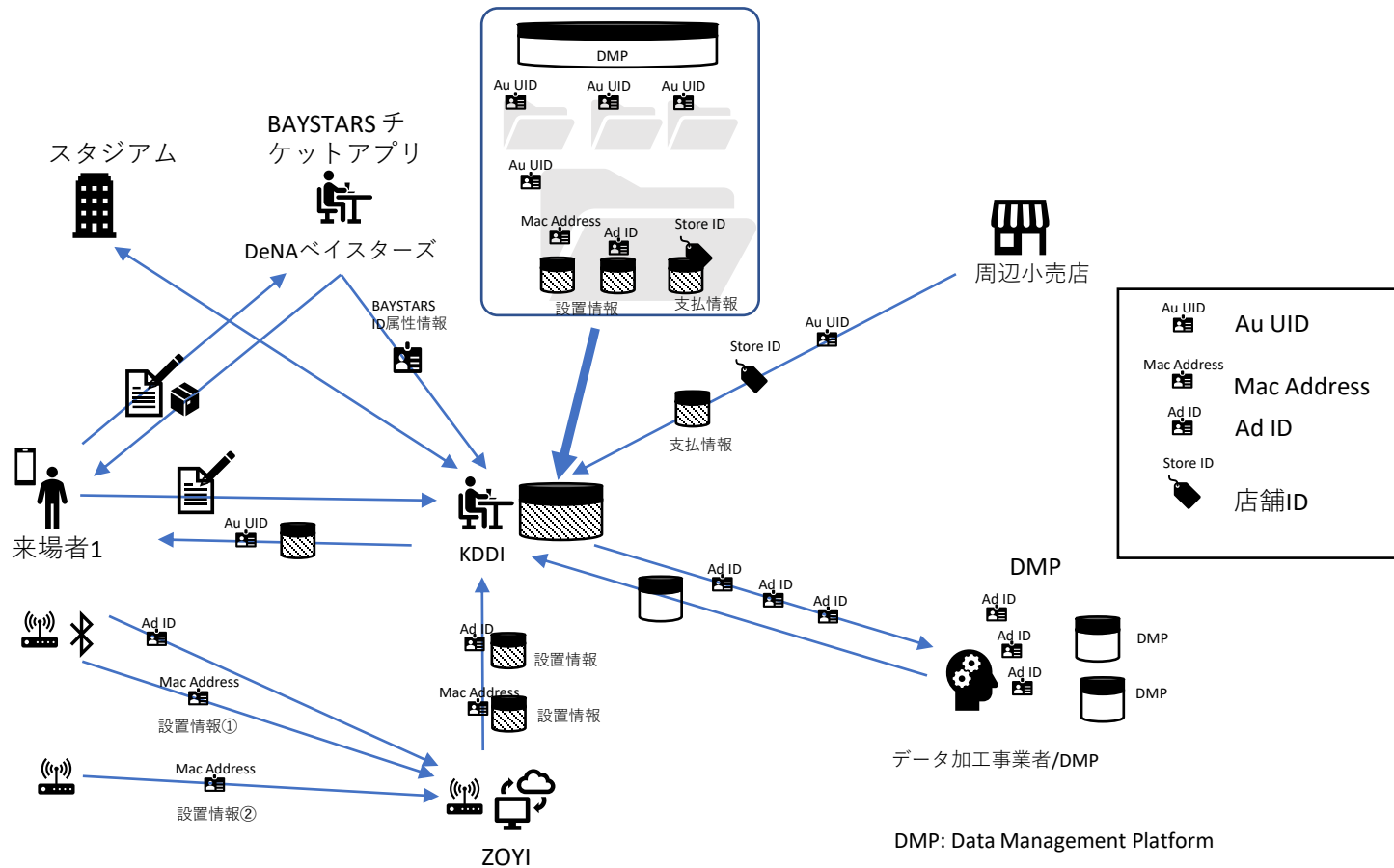
目的：関与する個人、事業者間のビジネス関係（契約など）を明確化する

スタジアムでのエリアマーケティング事業



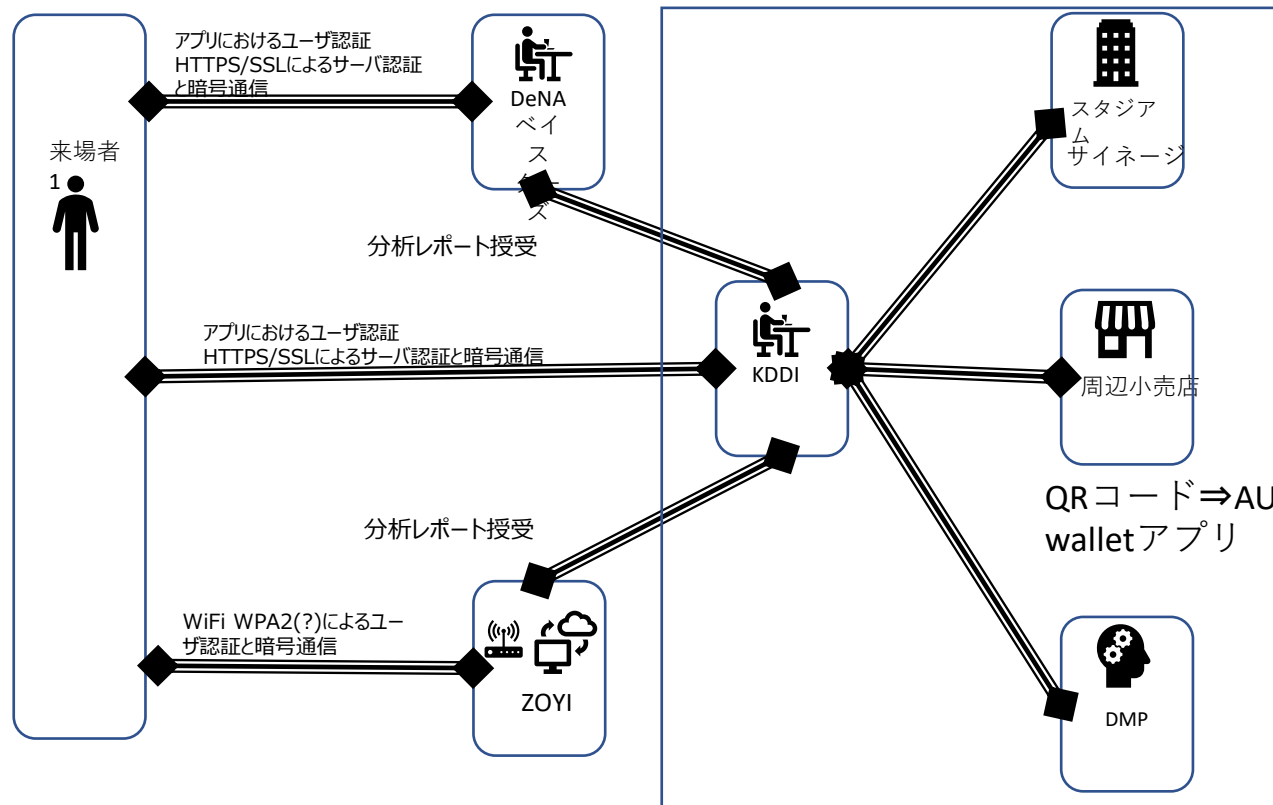
3. データリソースマップ

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。



4. トラスト関係

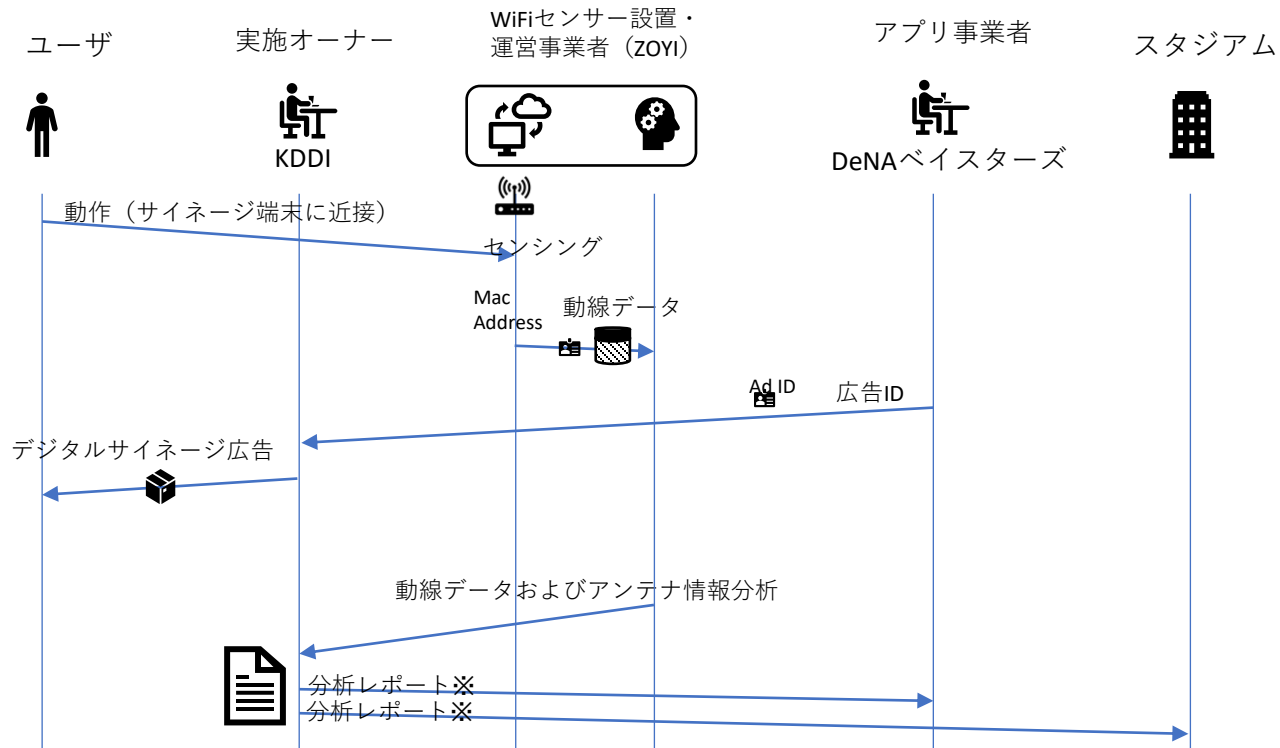
目的：関係者間の認証・認可の関係を明らかにする



KDDI自社システムで構築

5. データフローシーケンス

目的：関係者間でのデータセットの移動、処理フローなどの手順を明確化する



※ユーザを特定しない。ユーザ特性・属性分析せずにデータ抽出

6. 法制関係図

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

	来場者	スタジアム	ベ이스ターズ	KDDI	周辺小売店	データ加工事業者 (DMP)	WiFi設置・運営事業者 (ZOYI)
来場者		・試合観戦契約約款 ・試合観戦契約約款に記載がない範囲は、情報の取得・提供に関する契約/プライバシーポリシー等で情報の取得・提供の同意を得る	・チケットアプリ利用規約（個人情報の利用・提供に関する同意取得）	・AUPAY利用規約 ・プラットフォーム利用規約（個人情報の利用・提供に関する同意取得）	・売買契約/サービス利用契約（小売店ごとに定める内容。情報の取得及び移転を含む）		
スタジアム	個人情報の保護に関する法律を遵守		・試合実施等に関連する業務提携契約等	・情報の取得・提供に関する提携契約遵守			
ベースターズ	同上	・試合実施等に関連する業務提携契約等		・ID連携等も含めて、情報の取得・移転を含む契約締結			
KDDI	・個人情報の保護に関する法律を遵守 ・独占禁止法・電気通信事業において「電気通信事業法」「施行規則」「携帯電話不正利用防止法」「青少年インターネット環境整備法」「特定商取引法」「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」の遵守	・情報の取得・提供に関する提携契約	・ID連携等も含めて、情報の取得・移転を含む契約締結		・AUPAYに関する加盟店契約	・業務委託契約	・業務委託契約
周辺小売店	個人情報の保護に関する法律を遵守			・AUPAYに関する加盟店契約の遵守			
データ加工事業者 (DMP)	同上。但し、KDDIの委託先として、必要な範囲においてこれに準じた法令遵守対応が求められる。			・業務委託契約を遵守			
WiFi設置・運営事業者 (ZOYI)	同上			・業務委託契約を遵守			

気づきやコメント

- 本手法の実践での気づき

本実証研究を通して課題に感じたことは以下の4点。

- 1.Wi-Fiによる動線データ取得の周知対応
- 2.協力周辺店舗（飲食店等）への対応リソース
- 3.アプリプラットフォームのポリシー基準変更
- 4.実証実験に必要なデータを取得するための許諾取得や条件クリア

- 個人の課題（便益の見える化）、企業の課題（魅力的サービスの創出）の解決に本手法を適用できるか？

- 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ー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ーとの連携を推進することが可能と考える。

- 社会実装する上で、本手法の役割・貢献・課題などは？

- 今回作成したアーキテクチャのユースケーステンプレートは、標準アーキテクチャ形成に向けた手法の開発にとどまるため、実際に利用する場合の有効的な活用方法や啓蒙、普及させていくための活動を具体化させていく必要がある。