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

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

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

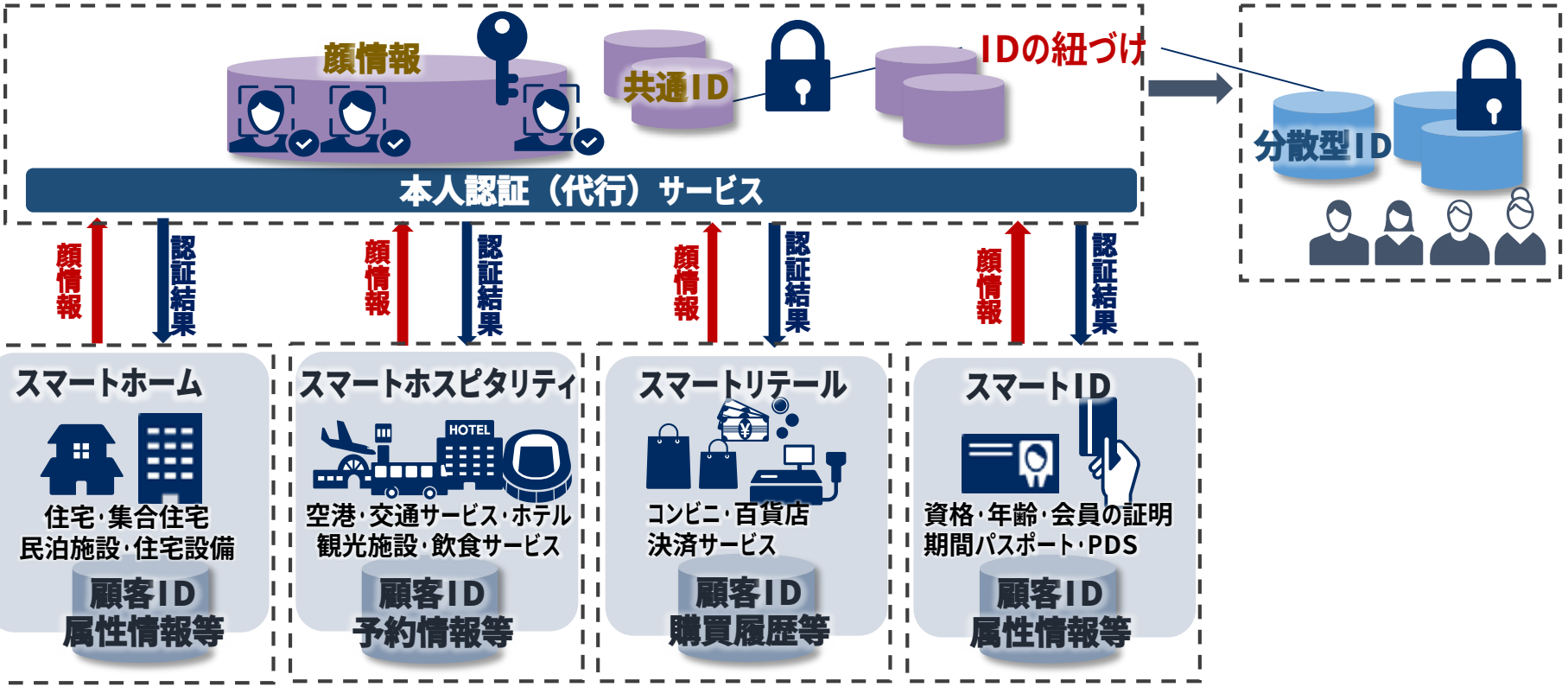
2020年3月18日

日本電気株式会社

Data Trading Alliance

1．研究開発の背景と目的

利用者の利便性向上と事業者の生産性向上、および日本型パーソナルデータ活用モデル創出を目指し、以下を目的として研究開発を推進



- 顔認証は、「なりすまし」に対する厳格性と「手ぶら」で認証できる利便性の高さから、生活における様々な領域において、利用が期待される一方、漏洩時やプライバシーに関する懸念が大きい
- 生体認証（特に顔認証）の横断的活用に向けた、基盤整備、政策推進の基本戦略としてのアーキテクチャを検討する
- 具体的には、顔認証技術を活用し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を設計・構築する
- これにより、リスクの低減、社会的な信頼や消費者の受容性の拡大を目指す

2. 顔認証技術、顔特徴量の活用に関する課題認識

負のイメージの払拭

•報道やソーシャルメディアを契機とした炎上の対象、監視社会を助長する技術としての負のイメージ

グローバルで重要視される技術と人権課題への対応

•他の情報との紐づけた行動のトレースや無秩序なプロファイリングへの懸念

•人種やマイノリティに対する差別や、国家機関による国民監視など、人権の観点からの顔照合技術に関する懸念

個人情報保護法に対する適切な対応

•個人識別符号としての義務の遂行への懸念（多様化する利用目的や状況に応じた消費者説明、安全管理措置、プライバシーや人権への配慮など対応すべき事柄が複雑化）

生体認証（顔認証）の本格的な社会実装に向けた取り組み

•POCから本格展開のシナリオ、サービス毎に顔情報を登録する手間や管理リスク、ID連携によるCX重視のモデルケース構築

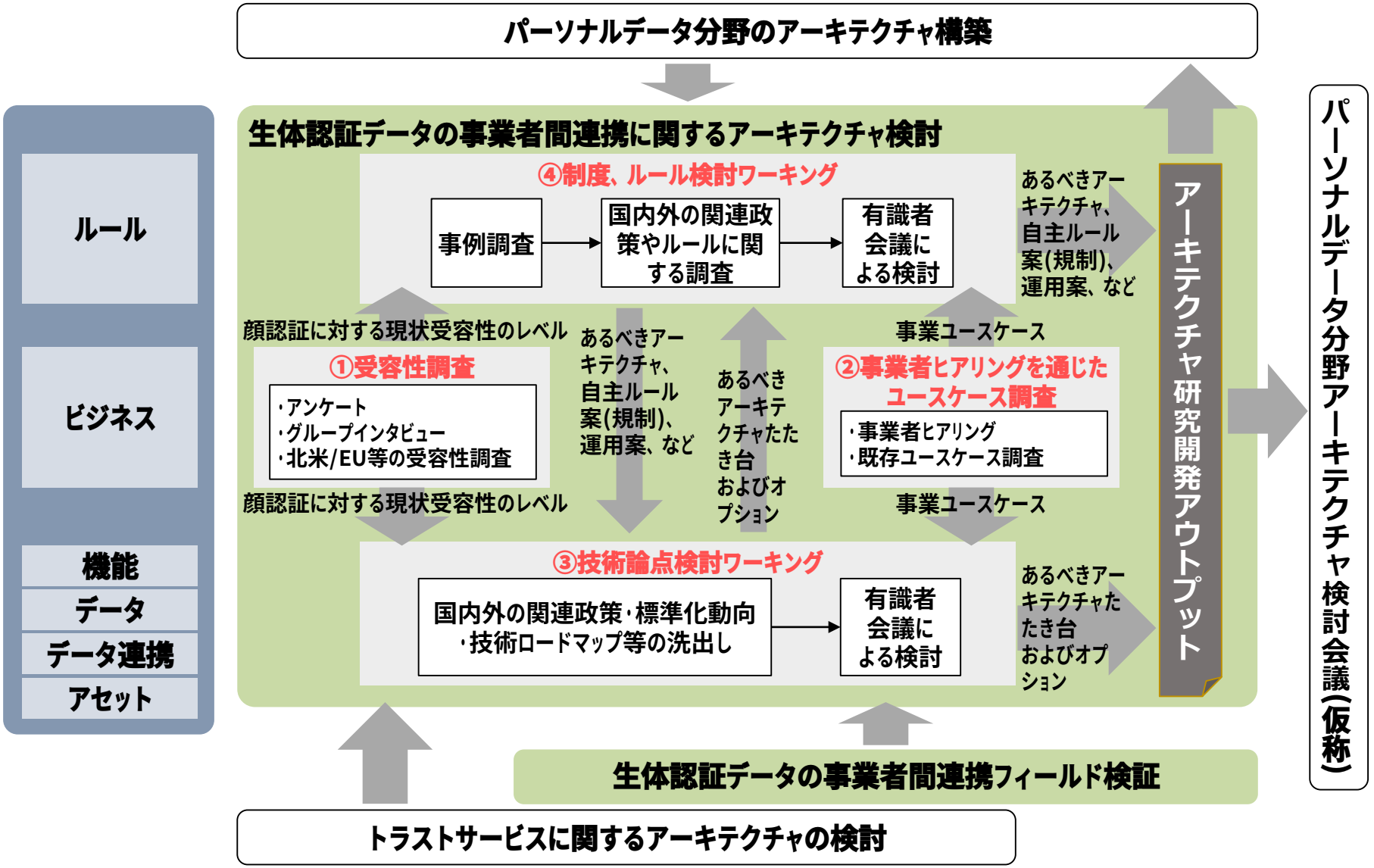
顔認証技術を活用したID連携ルールの整備や技術の標準化の推進

•ID連携技術や標準の推進、一段高い安全管理に貢献する技術や運用形態の必要性、本人の確からしさの確保、認証精度の補完（誤認証への対応）や消費者保護のルールの枠組み

我が国における安全管理基準やルールが明確ではない

3．研究開発の内容

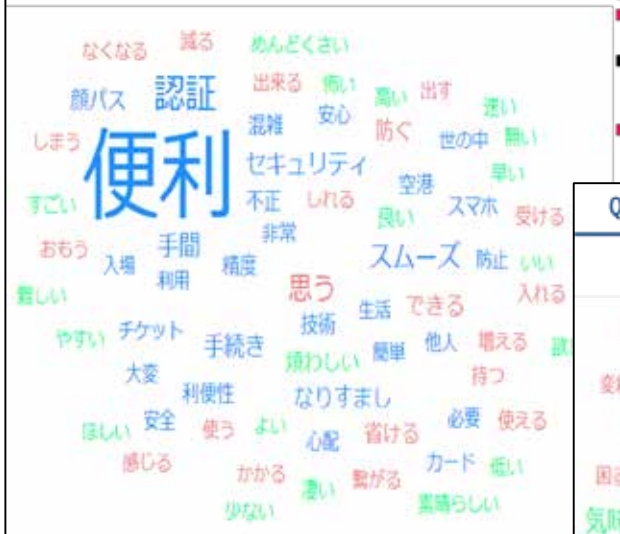
a. アーキテクチャ検討



①受容性調査：インターネットを通じた5157名への調査

「顔認証」に対する消費者意識は、「便利だ」などの声がある一方で、「なりすまし」「監視されている」「なんとなく嫌だ」などの声が半々。調査の結果、ネガティブな声に対しては、**トラブル発生後の補償・情報漏洩リスクの軽減対応**と、**自身で利用するか／削除するかを選択できるコントロール可能**であることが有効

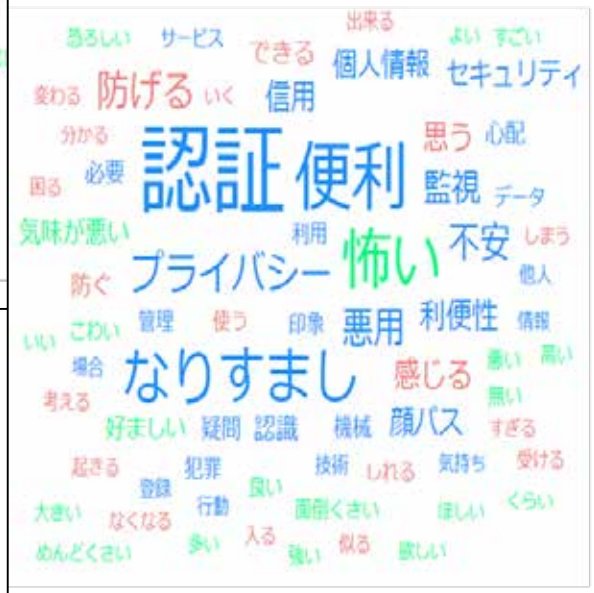
Q2 【顔認証技術を使ったサービス】に対する印象 「とても利用したい」回答者（n=738）



便利・楽

- 利便性が優れており、人的リソースやコストなど削減することができる。(男性/37歳)
- 物事がスムーズになり非常に便利で良い。物をなくしたり、災害で一文なしになった時など使えることができれば助かる。自分自身が身分の証明になるのが便利。(女性/32歳)
- 大変便利です。この様な世の中になったらどんなに便利か。(男性/64歳)

Q2 【顔認証技術を使ったサービス】に対する印象 「まったく利用したくない」回答者（n=522）



監視されている気がする

- 常に**監視されているよう**で気持ちの良いものではない(男性/43歳)
- 便利だが、**監視されているよう**に感じる(男性/38歳)
- 利便性より**管理されすぎること**の**気持ち悪さ**のほうがより強く感じる(男性/65歳)

精度が不安

- 結局マスクや帽子をかぶっていたら**認識されないんじゃ意味が無い**(男性/34歳)
- **絶対に誤認する**。100%でなければ行うべきでない。(男性/62歳)
- 体調や化粧によって驚くほど**顔が変わると思う**ので、引っかからないか心配になる。(女性/41歳)

悪用されないか不安

- **不正に利用されないか**心配です(女性/64歳)
- 利便性は理解できるが、**その情報が他に流出**し、何らかの不利益につながる恐れは拭いきれない。(男性/63歳)

なんとなく嫌だ

- 犯罪防止には良いが、**個人的には好きではない**。(女性/67歳)
- 怖い。**自分の顔を記録されたり見られること**に**抵抗がある**(自信がない)ので、こういったサービスは避けたい(男性/19歳)
- **気持ち悪い**ので登録したくない(女性/54歳)

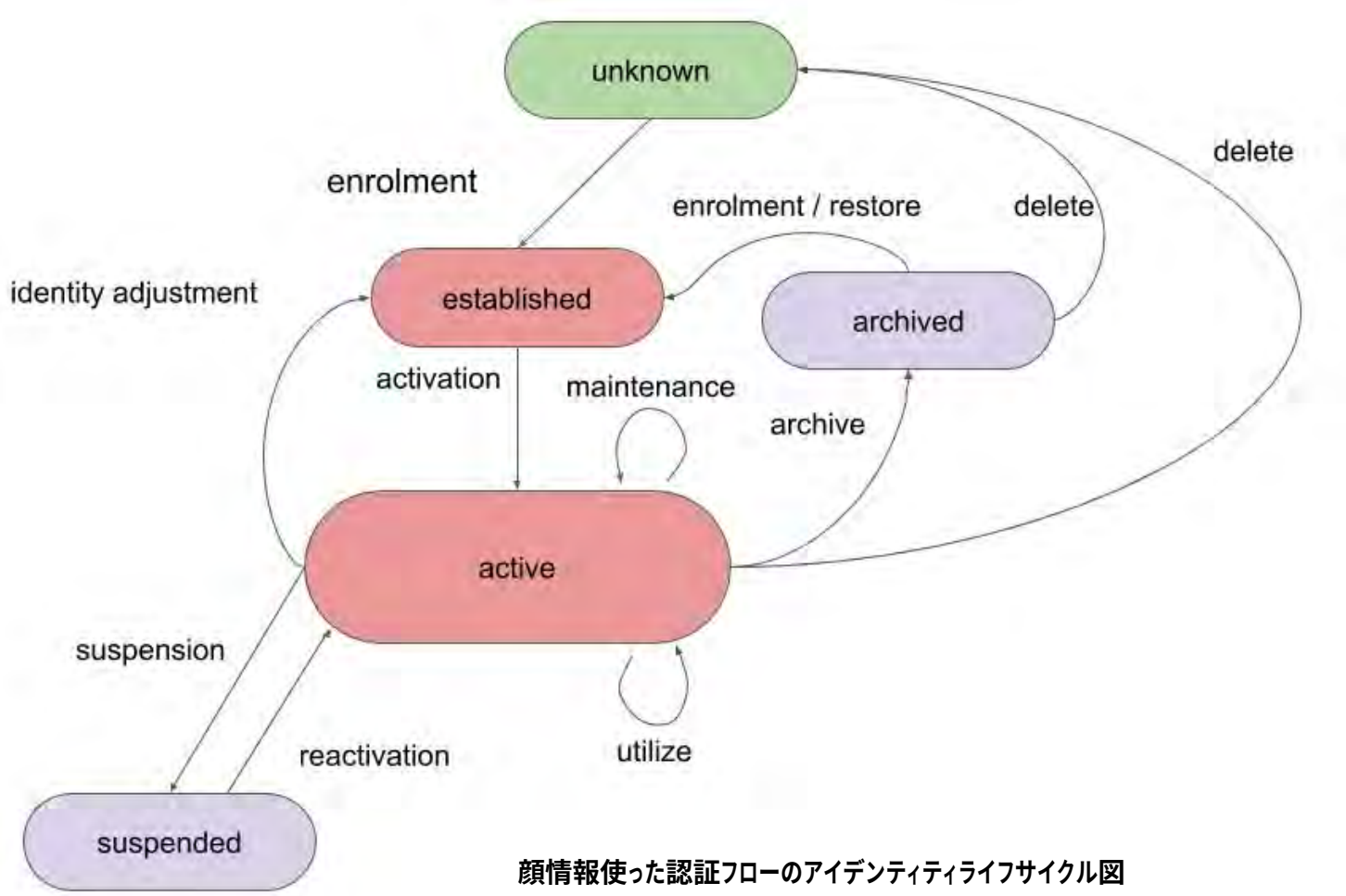
②事業者ヒアリング：利用検討中または実証参加企業

	【目的、期待効果】	【課題】
①小売業（コンビニ）	重要課題である人手不足に対する施策として、**店舗の省人化や無人化を期待**入店管理、レジレスによる決済、24時間営業における深夜無人化に期待。	顔照合を望まない顧客への対応を考慮すると、**投資対効果の点から課題**。
②スタジアム運営	チケットレス入場の導入を検討、**なりすましの防止や転売防止、自然に手ぶらで入場できること**、紛失リスク回避、待ち時間短縮などの顧客利便性を実現したい。	まずは厳格な認証までは求められない領域で活用していく
③地方空港運営事業者	空港に到着後にウェルカムメッセージを表示するサービスを試行。空港を起点に、二次交通、温泉、ビーチ、レジャー施設、飲食といった一連のサービスを顔認証で行うことによる、**観光ルート全体としての利便性の向上**も期待	空港運営事業者としては、**極力個人情報を取得、管理することは避けたい**。
④ホテル業	地方の宿泊業が共通に抱える根本の課題は、**人手不足の解消と生産性の向上**であるが、**客単価と客数の向上**との両輪といえる。客室の解錠を顔認証によりキーレス化し、家族が別々に浴場を利用したり散策したりできる。**宿泊客に満足度の向上や新たな付加価値**を提供し、ついては集客や客単価の向上に期待	ホテル予約システムと連動し、**宿泊者予約情報や属性情報と紐付けられて価値が最大化**
⑤レジャー施設	**チケット販売や入場オペレーションに関わる事務手続き削減による省人化**と、顧客満足度向上の両立を目指したい。事務負荷軽減の期待としては、QRコード決済は団体予約の際に個別発行が必要で事務効率が悪く、個人に紐づいた顔パスであれば入場オペレーションの省力化が実現できる。	実証では顔情報の登録サイトが、施設オフィシャルのサイトと別であり、不安に思う顧客がいるユーザがいる。
⑥地域振興施設	土産の販売での利用者の利便性に加え、セルフ化による省人化に期待。**釣りやダイビングの海洋レジャーサービスなどの「手ぶら」のニーズが高いサービス**に期待	顔認証決済について、端末やシステムを個々に導入することは、**小売り店舗が導入するには投資がかかりすぎる。**
⑦飲食店	繁忙期の人手不足や省力化を狙っている。将来は、**顧客管理とともに、アレルギー情報、食の好み、履歴などを管理できると、顧客満足度の向上とリピートが期待**できる。	地域の飲食店が単独でシステムを導入することは、**顔情報の管理や運用負荷を考えても現実的ではない**。
⑧ゴルフ場	**ピーク時間の混雑緩和による利用客の待ち時間の短縮**に期待する。将来的には、貴重品ロッカーの顔パス開閉、顔パスによるチェックインなどにも活用できると考える。	**予約管理や顧客管理との連携によるさらなる合理化効果と、接客の質の向上**。

③技術論点検討ワーキング:顔情報の認証連携

標準的なアイデンティティ・ライフサイクル*を参考に、顔情報を使った認証フローのアイデンティティ・ライフサイクル作成し、委員会で検討を行い定義。

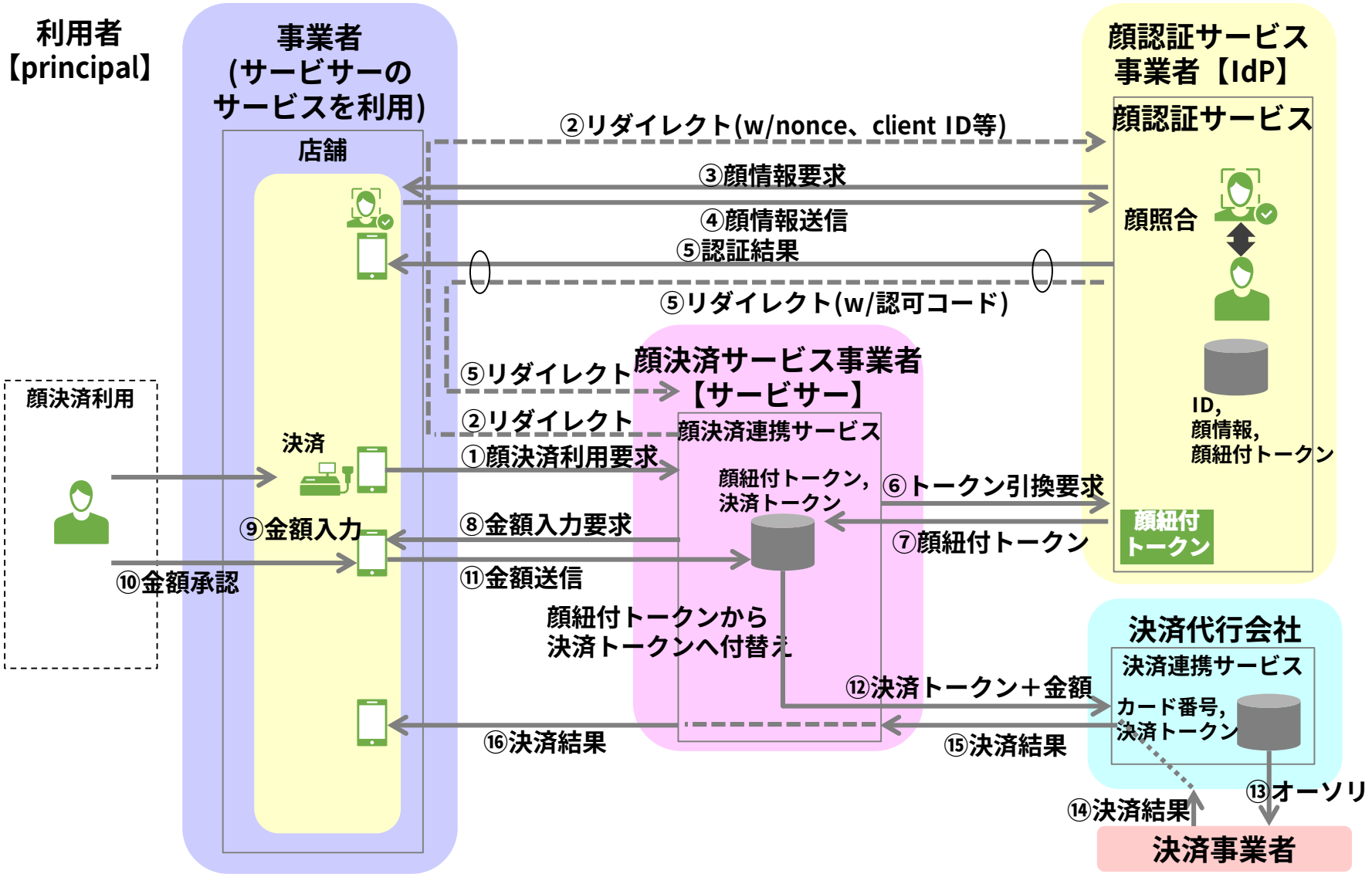
*「ISO/IEC 24760-1 A framework for identity management—Part 1: Terminology and concepts」と「ISO/IEC 24760-2 A Framework for Identity Management—Part 2: Reference architecture and requirements」



顔情報使った認証フローのアイデンティティライフサイクル図

③技術論点検討ワーキング:ユースケース毎のシーケンス図

検討したアイデンティティライフサイクルのユースケースの一例（顔決済サービス利用時）



④制度、ルール検討ワーキング:国内・米国・EUの関連する規範

監視社会を助長するという負のイメージの払拭、グローバルで重要視される、プライバシーや人権のトレンドへの対応を考慮し、以下のような法令・ガイドライン・事案を参考に、あるべき制度やルール、合意形成のあり方等を導出

<参照した法令・ガイドライン・事案の一例>

カテゴリー	名称	実施主体	分類	主な保護法益等
国際原則（政府系）	国連ビジネスと人権に関する指導原則	民間企業	—	人権の尊重、社会的弱者の自立支援
国際原則（政府系）	AIに関する分析レポート“AI in Society"とAIに関する理事会勧告	—	AIシステム	
国内・地域の立法（法律）	自己情報コントロール権（情報自己決定権）	—	—	—
国内・地域の立法（法律）	消費者基本法	—	—	消費者の利益
国内・地域の立法（法律）	市当局による顔照合技術の使用を禁止するサンフランシスコ市条例	地方自治体	顔照合全般	プライバシー、市民権
国内・地域の立法（法律）	顔照合技術の使用を一時禁止する英国法案	—	顔照合全般	大衆監視
裁判例	南ウェールズ警察による顔照合技術の使用に関する判決	法執行機関	顔照合	個人の自由、人権、プライバシー、平等
政府系ガイドライン	プライバシー・バイ・デザイン（PbD） 7つの基本原則	—	ITシステム	プライバシー
政府系ガイドライン	Guidelines 3/2019 on processing of personal data through video devices	*法執行機関は対象外	顔照合全般（但し、本人の同意等がある場合を除く）	基本権、自由
政府系ガイドライン	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）	民間企業	本人確認	プライバシー
企業ポリシー	マイクロソフト「顔認識テクノロジに関する当社の見解について」	民間企業	顔照合全般	偏見と差別、プライバシー、民主主義の自由と人権
事案	Amazon Rekognitionに関する報道	法執行機関	顔照合	人種差別、表現の自由（への萎縮）、プライバシー
事案	2017年UEFAチャンピオンズリーグ決勝戦における顔照合技術の使用に関する報道	法執行機関	顔照合	プライバシー、大衆監視（誤認証）
事案	NICT大阪ステーションシティ実証に関する報道	独立行政法人	顔照合（追跡）	肖像権、プライバシー、監視社会

④制度、ルール検討ワーキング:顔照合技術の適正利用原則（案）

民間企業が本人同意を得た上で顔認証技術による本人確認サービスを提供する場合に、事業開発部門や事業企画部門の担当者が、**適正な利用をはかるために検討すべき項目**を列挙。必ず遵守しなければならないものではないが、**事業者が自主的に取り組むことにより、消費者からの信頼を獲得するとともに、リスク・マネジメントの観点からも有益**と考える。

＜顔照合技術の適正利用原則（案）の一部抜粋＞

1. 情報自己決定の原則

（参照：自己情報コントロール権、EUビデオ機器ガイドライン等）

- 事業者は、利用者による情報自己決定権の行使を現実に可能にするためのユーザ・インターフェースの設計・実装を目指す。例えば、以下の事項の実現が考えられる。
  - 利用者が、サービスの具体的な範囲 （本人確認情報の連携先等）を自由に選択できること
  - 利用者が、一般的に本人確認サービスに同意していたとしても、文脈や状況に応じて同サービスの利用を一時的に拒否できること（利用者の好むタイミングで連携する場合としない場合を選択できること）
  - 利用者が、本人確認情報に連携（紐付け）されている属性情報や本人確認等の履歴を確認でき、いつでも連携を解除できること（本人が知らないなかでネガティブ情報が不当に拡散することをよって生じるスティグマ化・烙印化を防止すること）
  - 利用者 が、自己の本人確認情報が漏えいした場合などに、本人確認情報そのものの登録を解除し、再登録できること＊
- 事業者は、利用者の顔情報を取得する際に、利便性だけではなくリスクを含めたわかりやすい説明を行うとともに、明確な本人同意を取得する（インフォームド・コンセント）。なお、事業者が利用目的を類型化し、アイコン化することなどにより、利用者に利用目的が一見してわかるように表示することも考えられる。

2. 実効的な救済の原則

（参照：ビジネスと人権に関する指導原則、消費者基本法等）

- 事業者は、誤認証、他人受け入れ等により利用者に被害を与え得ることを理解し、利用者からの苦情相談対応窓口の設置など、利用者への回復措置や補償を含む実効的な救済を行うための体制を整備する。
- 事業者は、利用者が本人確認情報に連携（紐付け）されている属性情報や本人確認等の履歴を確認でき、いつでも連携を解除できるようにする（本人が知らないなかでネガティブ情報が不当に拡散することをよって生じるスティグマ化・烙印化をの防止すること）。
- 事業者は、実効的な救済のために、契約等により事業者間（システム提供者とシステム利用者間等）での責任の所在を明確にする。

3. 代替手段の提供の原則

（参照：EUビデオ機器ガイドライン、NICT調査報告書、国交省ONE-IDガイドブック等）

- 事業者は、顔照合を望まない利用者向けに、顔照合技術を利用せずに、従来通りのサービスを受けられる方法を提供する。

4. 利用目的の限定の原則

（参照：国交省ONE-IDガイドブック等）

- 事業者は、予め定めた利用目的に限定して利用者の顔情報を利用する。例え、事後的に新たなニーズが生じた場合でも、安易な拡張や変更は行わない（複合目的の回避）。

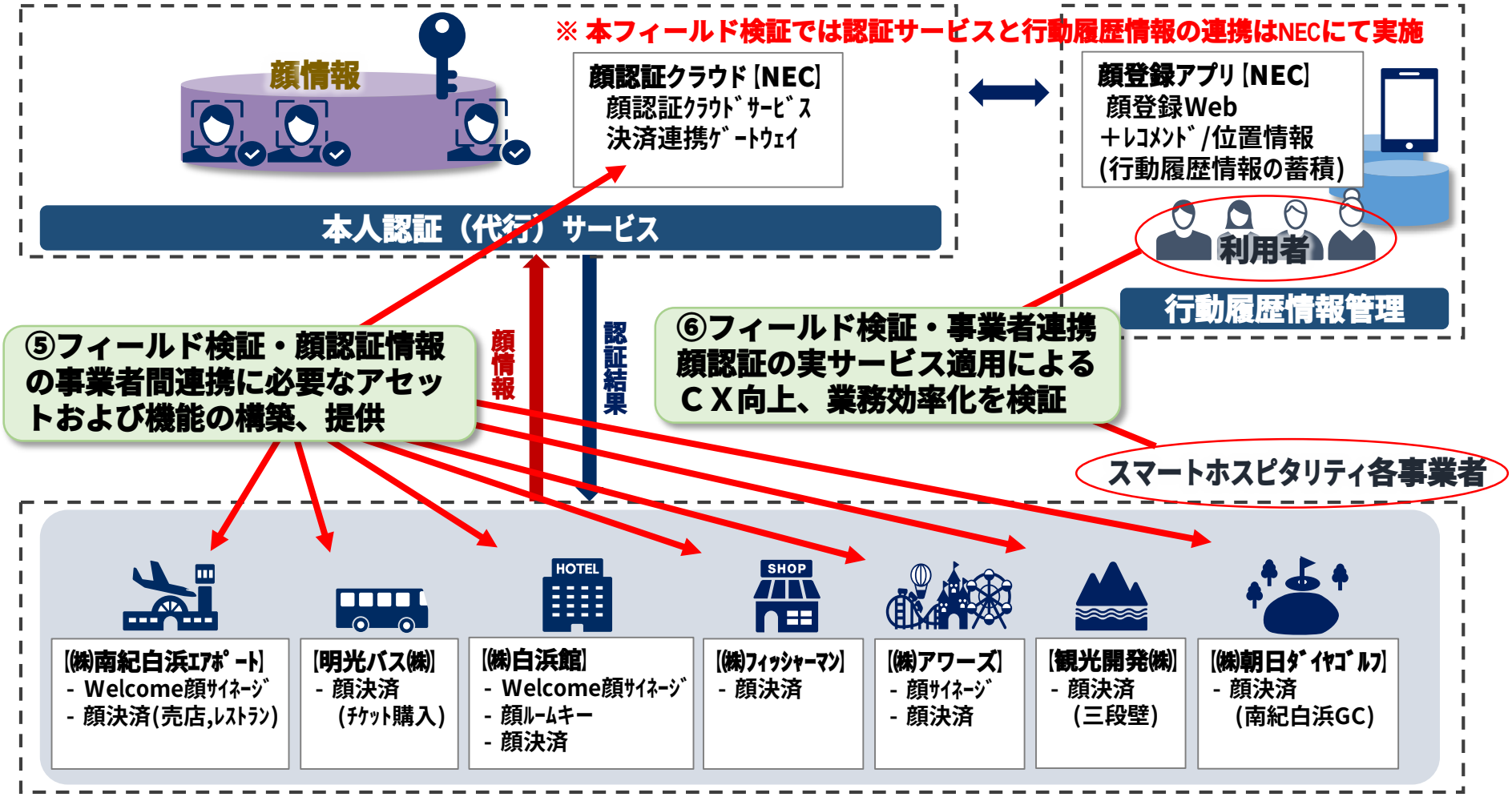
5. 安全管理の原則

（参照：技術論点検討WGによる実施報告書等）

- 事業者は、顔情報がパスワード等と異なり基本的に変更できない特性をもつことに鑑み、暗号化や非保持化等のセキュリティ対策や、第三者による情報セキュリティ監査等を実施する。また、生体情報保護の機能等を用いた安全管理を行うことを検討する 。

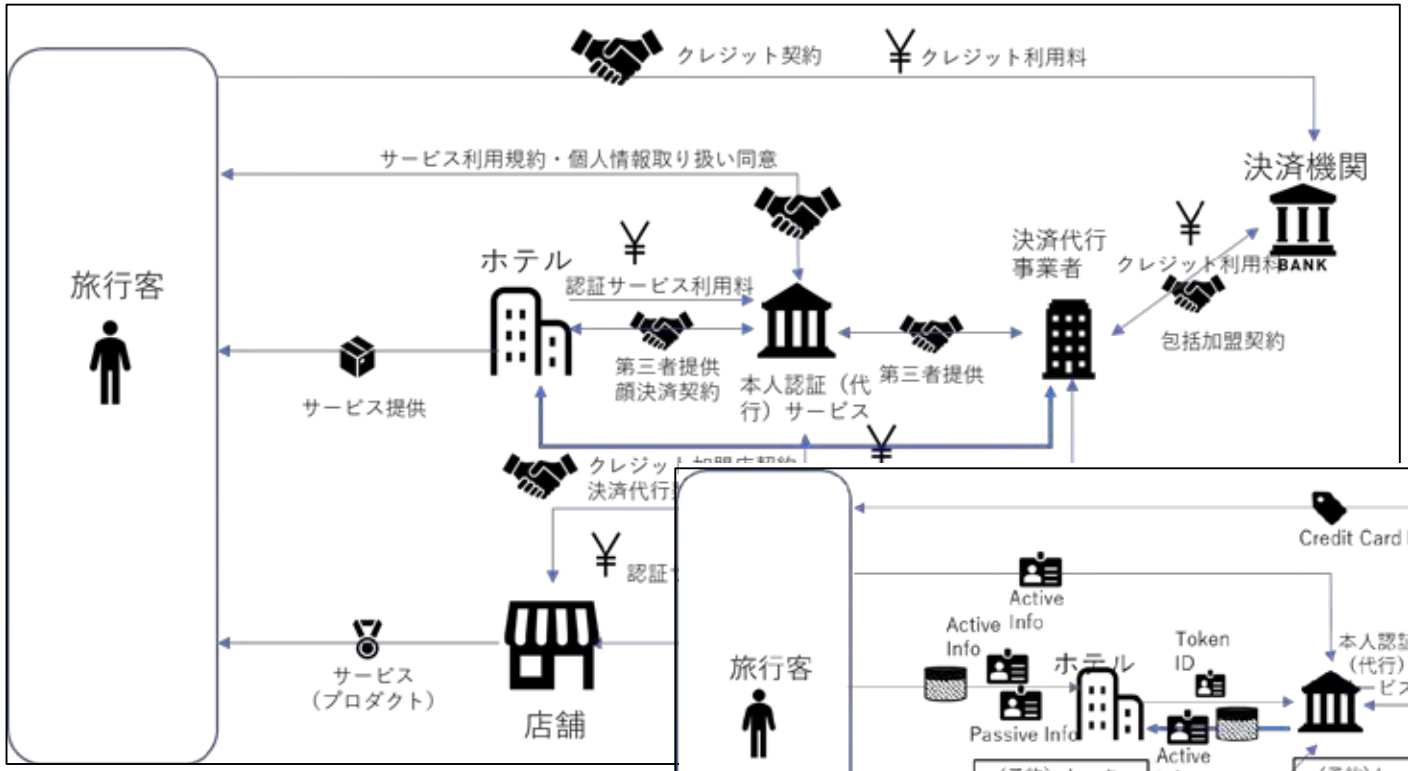
4. 生体認証データの事業者間連携フィールド検証

和歌山県南紀白浜を実証フィールドとし、顔認証サービス連携の機材やサービスを構築。顔認証の連携が**利用者のCXに与える影響**や、フィールド事業者間での顔認証情報連携により、**業務の効率化に与える影響についてヒアリング**実施

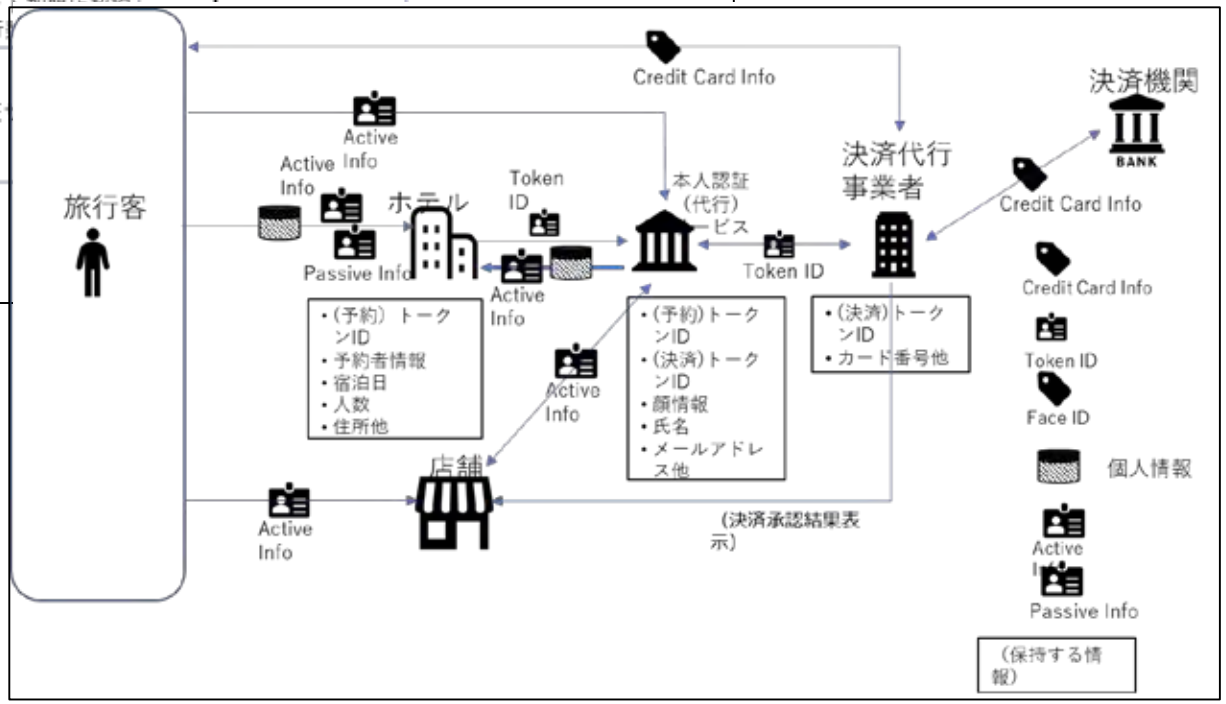


4-1. フィールド検証：実証を元にユースケースを作成

ビジネス関係



データリソースマップ



5.実証研究の検討結果

顔認証技術、顔特徴量の活用に関する課題認識

①生体情報としての厳格な
安全管理基準、ルールの必要性
（参照：NIST SP 800-63B）

②負のイメージの払拭
（参照：本研究での受容性調査結果）

③グローバルで重要視される技術
と人権課題への対応
（参照：各国の法令、条例等）

④改正個人情報保護法に対する適切な
対応への懸念
(参照：NPO/市民社会の指摘、炎上事案)

⑤生体認証(顔認証)の本格的な
社会実装に向けた取組みの必要性
(参照：本研究での事業者ヒアリング結果)

⑥顔認証を複数事業者間で連携する
ルール整備や技術の標準化推進
(参照：アイデンティティライフサイクル)

必要な対応・配慮すべき事項

A：顔情報連携における標準的な
認証連携フローの適用

B：生体情報保護テンプレート

C：ユーザ自身での
情報コントロール

D：トラブル発生時の補償

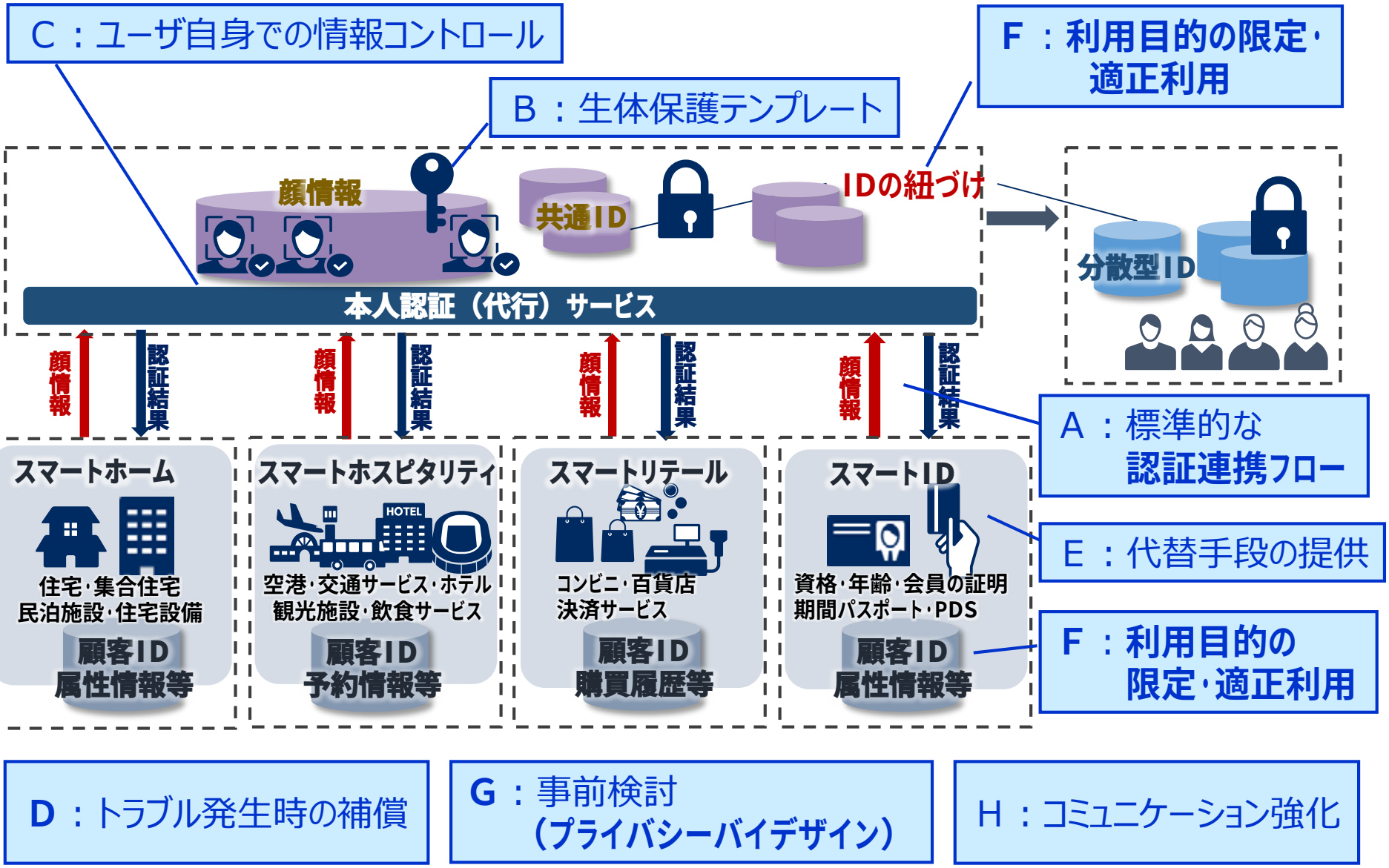
E：代替手段の提供

F：適正利用(利用目的の限定)
公正・公平・透明性の確保

G：事前検討
(プライバシーバイデザイン)

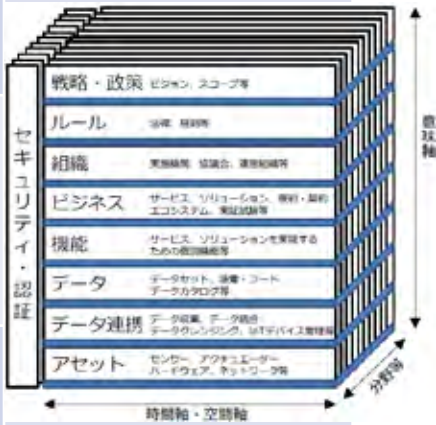
H：コミュニケーション強化
(マルチステークホルダとの対話)

5-1.実証研究の検討結果



6.顔認証データの事業者間連携に関するアーキテクチャ

			セキュリティ・認証
戦略・政策	• 個人起点による日本型パーソナルデータ活用モデルの創出		• 基本的に変更できない特性を鑑みた対策（暗号化、顔情報の非保持化など） • 第三者による情報セキュリティ監査 • Ｂ：生体情報保護テンプレート（ISO/IEC 24745） • 認証時のセキュリティレベル（NIST SP800-63）
ルール	• 顔特徴量活用、顔照合サービスに関するガイドライン、認定指針	• D:トラブル発生時の補償 • E:代替手段の提供 • G:事前検討（プライバシーバイデザイン）	
組織	• 生体認証の活用、カメラ映像情報の活用などにおける認定個人情報保護団体の枠組みや認定機関	• H:コミュニケーション強化	
ビジネス	• コンビニなどの省人型店舗、無人店舗、キャッシュレス促進 • 空港、交通機関、ホテル、観光施設などのエリア内ホスピタリティ向上、混雑や待ち行列の削減による効率化 • チケット転売、年齢や資格の詐称防止	• C:ユーザ自身での情報コントロール • F:利用目的の限定、適正利用	
利活用機能	• リアル空間におけるスムーズな本人認証（スマートチェックイン、手ぶらでの決済・開錠・搭乗、会員資格に応じたサービスなど） • 個人の履歴情報の二次活用（リピート分析、ＯＤ調査、誘導サービスなど）	• A:標準的な認証連携フロー • C:ユーザ自身での情報コントロール • G:事前検討（プライバシーバイデザイン）	
データ・データ連携	• 顔特徴量データ（識別符号） • 各種ID情報（会員ID、社員ID、カード番号など） • 属性情報等（性別、年齢、資格、権利、チケット情報、予約情報など） • 履歴情報（購買履歴、決済データ、訪問履歴、移動経路、待ち時間など）	• F:利用目的の限定、適正利用	
アセット	• カメラ（顔情報取得） • その他顔特徴量取得、認証のエッジデバイス（決済端末、ドアホン、チェックイン機、チケット販売所等）	• G:事前検討（プライバシーバイデザイン）	



7. 今後の検討課題

■技術WG：

1. 「顔画像と実体の確認を行う」方法についての検討
2. 事業者間の契約のあり方について

■制度・ルール検討WG

1. 安全管理基準の検討
2. 我が国の基本ポリシー（原則）の策定と世界発信
3. 立法の必要性
   - 技術やデータ対象か、目的対象か
4. その社会実装に向けた取り組み（事業開発とガバナンスの論点）
   - 標準化検討（技術、契約）
   - 運用基準、認定指針の検討（認定制度のブランディング）
   - アカンタビリティや救済窓口
   - サプライチェーンのガバナンス
   - 「顔照合技術を活用した適正な事業開発の基本要件」策定
5. トラストフレームワークの各機能のアクター検討
   - 制度モニタリング、トラストのアンカー、認証代行
6. 企業の社会的責任、市民社会との向き合い方
   - NPOとの連携（世界的認定、認証）
   - SDGs、ESG課題（デジタル公害）としての経営対応
   - デジタルバリューチェーン（責任あるデータ調達など）の概念実装