資料２－４

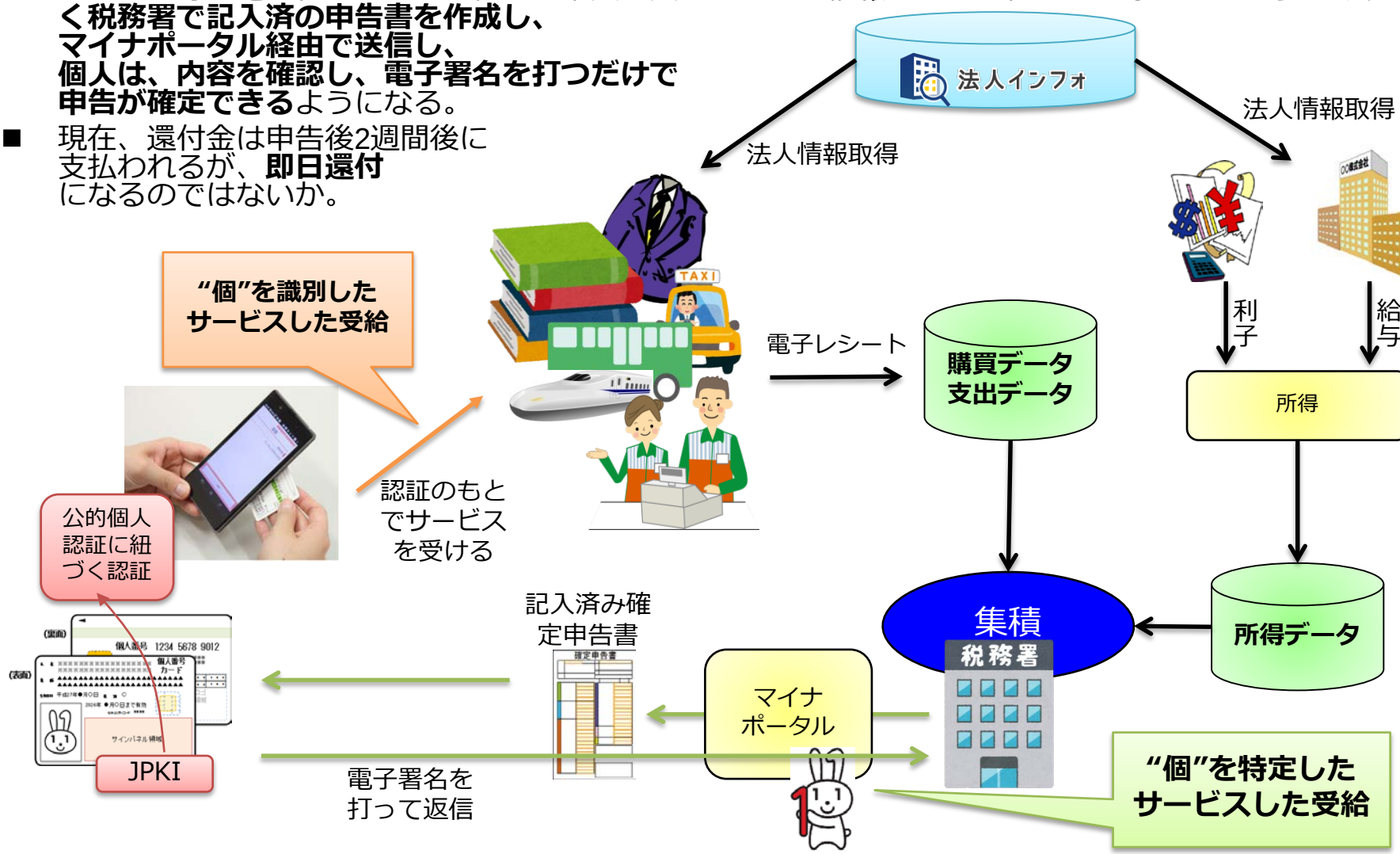
第2回 制度検討SWG

ＩＤ連携トラストフレームワークについて

（一財）日本情報経済社会推進協会
電子情報利活用研究部
保木野　昌稔
（法人番号：1 0104 0500 9403）

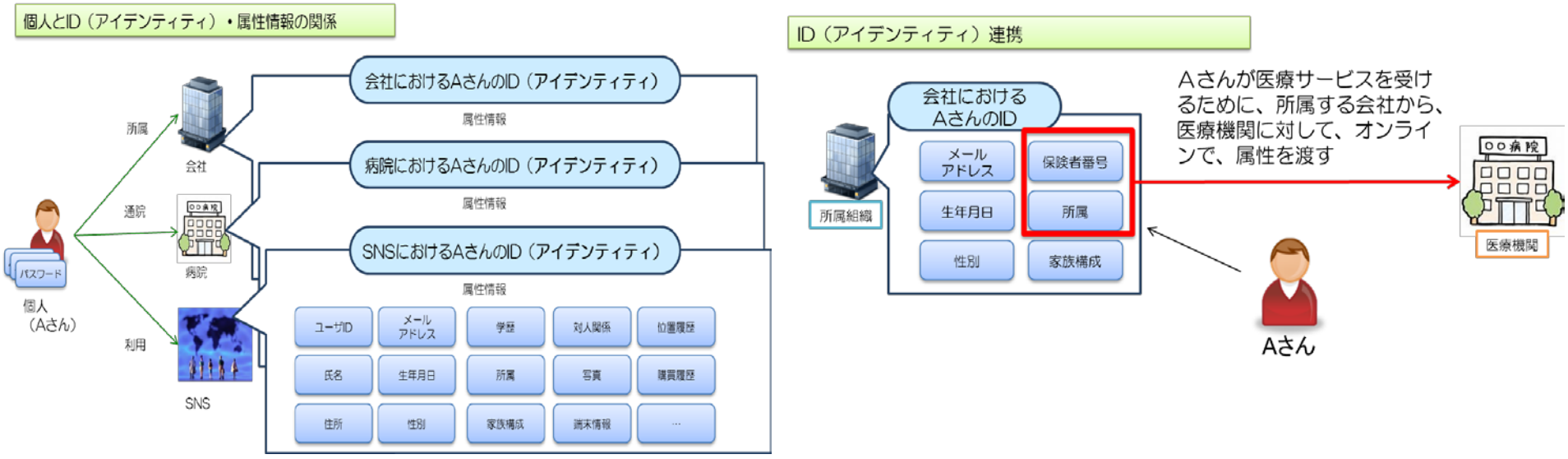
目指す姿（オンライン完結社会・電子政府）

- ID連携TFを用いた将来の行政サービスについて検討を実施。
- 確定申告をしている人は約2142万人（平成26年に確定申告が行われた平成25年分の確定申告者数）。そのうち税金を戻してもらえる還付申告者数は約1240万人。確定申告を行うことで、還付申告が可能な人は、それ以上いるとみられている。
- レシート等の電子化によって、個人の購買や支出に関する情報がデータ化され、**申告書を自ら記載するのではなく税務署で記入済の申告書を作成し、マイナポータル経由で送信し、個人は、内容を確認し、電子署名を打つだけで申告が確定できる**ようになる。
- 現在、還付金は申告後2週間後に支払われるが、**即日還付**になるのではないか。



【参考】ID（アイデンティティ）、 ID連携とは

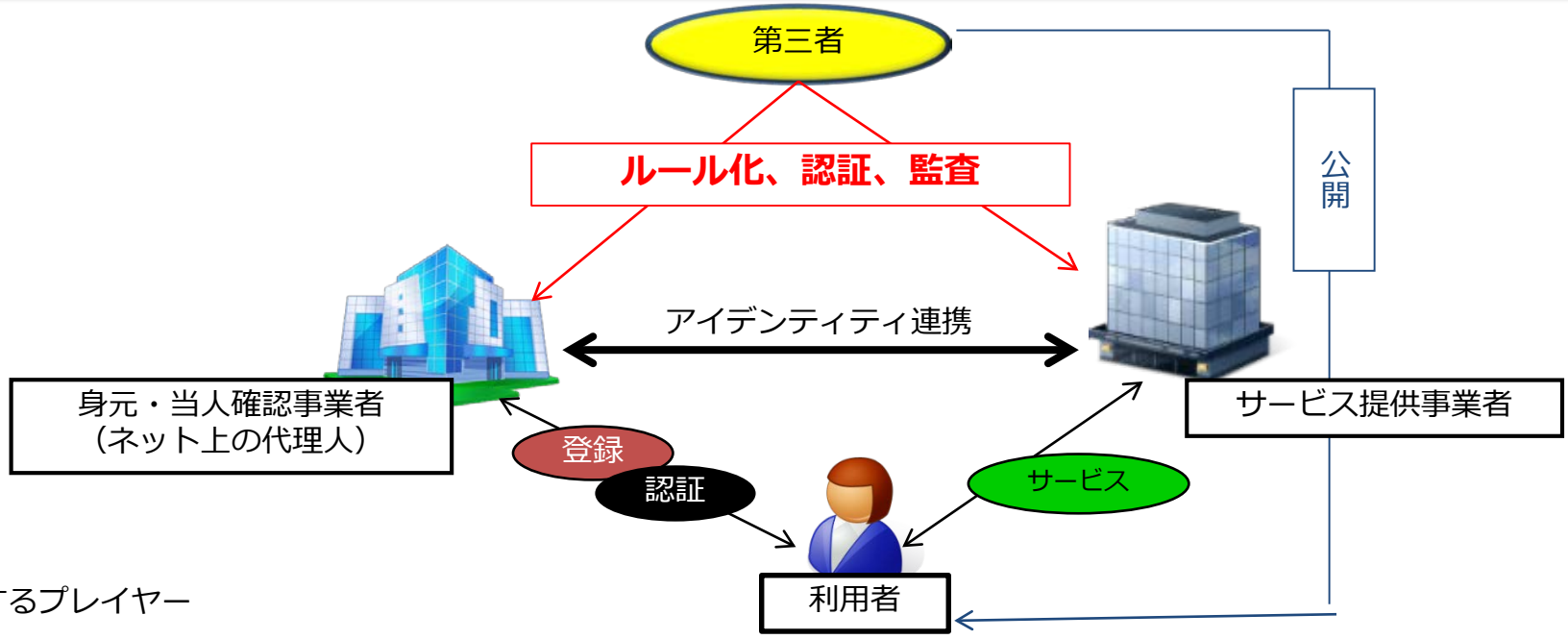
- ID連携トラストフレームワークにおける『ID』とは、「アイデンティティ：Identity」のことである。当該主体に関する（認証結果を含む）属性の集合を指す。
- ID連携とは、「複数のサービスの間で、（主に、ある主体を識別するために、）当該主体に関する（認証結果を含む）属性の集合(identity)を交換・利用すること」を言う。



- 米国では、OMB M-04-04、NIST SP800-63、FIPPs（Fair Information Practice Principles）等に準拠し、プライバシーを保護しつつ、民間事業者の発行するIDを行政機関が受け入れるID連携が行われている。

【参考】ID連携トラストフレームワークとは

- 利用者と事業者同士が、インターネット上のID連携を伴う取り引きにおいて、互いを信用し合い任せられる状態（トラスト）を、枠組み（フレームワーク）として実現するものである。
- **事業者の要件とルールを明確化**し、**第三者による認証や監査**によって、アイデンティティを取扱う**事業者の信頼性を担保**する。



■構成するプレイヤー

役割	名称	上図では
サービスを受ける主体。自分自身を証明する情報を認証する主体に渡す必要がある。	利用者	利用者
利用者を認証する主体。保証レベルによって、IDの確からしさの確認を行う。	アイデンティティ・プロバイダ（IdP）	身元・当人確認事業者
サービス提供事業者であり、IdPから必要な属性情報のみを受け取り、利用者にサービスを提供する。	リライング・パーティ（RP）	サービス提供事業者
利用者に関する属性情報を、IdPやRPに提供する。	アトリビュート・プロバイダ（AP）	該当無（注１）

※１）利用者が求めるサービスを提供するにあたり、IdPが保有する属性情報だけでは足りない場合に、該当するデータを提供する主体をいう。

アジェンダ

- ■ID連携トラストフレームワーク基準について
- ■ユースケース実証について
- ■まとめ
- ■ID連携を伴うユースケースの紹介
  - ➢（ID連携トラストフレームワーク推進コンソーシアムにおける検討）

ID連携トラストフレームワーク基準について

ID連携トラストフレームワーク基準策定の視点

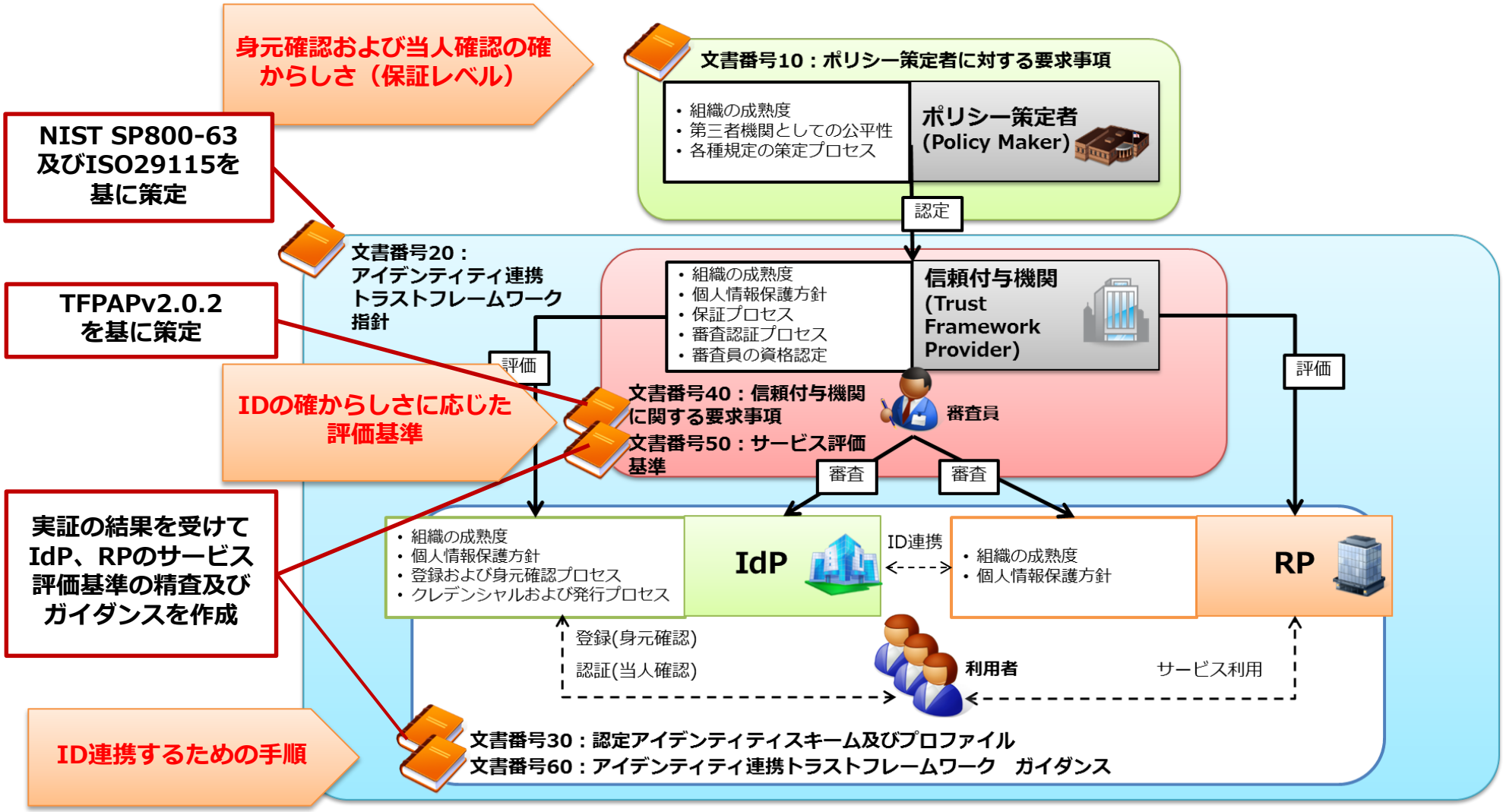
JIPDEC

- 米国のトラストフレームワーク及び基準文書（**FICAM TFPAP、NIST SP800-63**）を参考に、日本版ID連携トラストフレームワーク推進に必要な基準について
  - **「身元確認および当人確認の確からしさ（保証レベル）」**
  - **「ID（アイデンティティ）の確からしさに応じた評価基準」**
  - **「ID（アイデンティティ）連携するための手順」**

  の観点から検討
- 国際的なID連携（認証連携、パーソナルデータ連携）を視野に入れ、**ISO/IEC 29115**等とも整合を取った
- なお、日本版の基準案については、**個別の要件を含まない汎用的に用いられる規定部分のみ**を作成した

ID連携トラストフレームワークの構成

策定した基準の構成と各文書が対象としている範囲を、以下に示す。



【参考】ID連携トラストフレームワーク基準案の文書構成

JIPDEC

文書番号	文書名	対象読者	概要
00	文書体系	関係者全て	アイデンティティ連携トラストフレームワークに関連する文書の体系を一覧化したもの。
10	ポリシー策定者に対する要求事項	ポリシー策定者	ポリシー策定者に求められる事項を定めたもの。ポリシー策定者が自身を束縛する。 以下について規定する。 ・　ポリシー策定者の組織の成熟度 ・　アイデンティティ連携トラストフレームワーク指針の策定と手順 ・　アイデンティティスキーム及びプロファイルの認定と手順 ・　信頼付与機関に対する要求事項の策定と手順 ・　信頼付与機関の認定と手順
20	アイデンティティ連携トラストフレームワーク指針	信頼付与機関 審査人 IdP、RP	アイデンティティ連携トラストフレームワークを概説し、その指針を定めたもの。 以下について解説する。 ・　アイデンティティ連携トラストフレームワーク ・　保証レベル ・　認証フレームワーク
30	認定アイデンティティスキーム及びプロファイル	IdP、RP	アイデンティティ連携で用いられるアイデンティティスキームとプロファイルを定めたもの。
40	信頼付与機関に関する要求事項	信頼付与機関 審査人 (IdP、RP)	信頼付与機関に求められる事項を定めたもの。以下について規定する。 ・　信頼付与機関の組織の成熟度 ・　信頼付与機関による組織認証審査基準に関する要求事項 →　IDプロバイダの組織認証審査基準 →　リライング・パーティの組織認証審査基準 →　審査人の組織認証審査基準 ・　信頼付与機関による組織認証審査手順に関する要求事項
50	サービス評価基準案	信頼付与機関 審査人 (IdP、RP)	信頼付与機関に関する要求事項に則って、IDプロバイダおよびリライング・パーティに対して審査する評価項目を例示したもの。
60	アイデンティティ連携トラストフレームワーク　ガイダンス	IdP、RP	アイデンティティ連携トラストフレームワークにおける認証基準のポイントを整理し、それぞれの分野に背景や状況に即した基準を整理したもの。

【参考】保証レベルと信頼レベルの規定

基準案では、「身元確認」の保証を身元確認保証レベルとし、「当人確認」の保証を当人確認保証レベルをとする。並びに「プライバシー及び個人情報保護」を信頼レベルとし、それぞれ4つのレベルに分類し定義した。

区分	身元確認保証レベル （登録時のレベルを規定）	当人確認保証レベル （クレデンシャル管理,ユーザの認証, アサーション等の			信頼レベル
評価軸	登録	クレデンシャル管理	ユーザの認証	アサーション	個人情報保護
レベル4 （特高）	（対面のみ）写真付き公的身分証明書２種又は公的身分証及び金融／携帯電話の個別番号を提示。全ての申請情報を記録と照合。 生体情報の記録。	レベル3に加え • ハードウェア暗号モジュールでの保持 • 更新/再発行の機密データの転送時には常にユーザ認証に紐づけられた鍵を使用した認証を実施 • クレデンシャルの回収と破棄または無効化	レベル3に加え • 強中間者攻撃対策	レベル3に加え • ユーザによるアサーションの否認	プライバシー及び個人情報保護状況証明の程度の基準
レベル3 （高）	（対面）LV2に加え、申請情報を記録と照合。録音等による否認防止。 （非対面）LV2に加え、申請情報を公的機関および金融／携帯事業者の記録と照合。録音等による否認防止	レベル2に加え • 共有秘密の保護、暗号化（レベル2以上の物理保護、レベル3以上の暗号化）	レベル2に加え • 多要素認証 • フィッシング/ファーミング対策	レベル2に加え • 検証者によるアサーションの否認	
レベル2 （中）	（対面）写真付き公的身分証明書の提示 （非対面）公的身分証及び金融／携帯電話の個別番号を提示。申請情報を記録と照合。	レベル1に加え • 共有秘密の保護（ソルトハッシュの利用、暗号の利用） • 長期共有秘密鍵の開示はIDプロバイダが運営する検証者に限定 • 更新/再発行のポリシーの作成	レベル1に加え • セッションハイジャック対策 • 盗聴対策 • 弱中間者攻撃対策	レベル1に加え • アサーションの漏洩、リダイレクト	
レベル1 （低）	レベル1+ （対面／非対面）身分証明書の提示 （対面／非対面） 自己申告。身元確認は不要。	• 共有秘密のアクセス管理 • アクセス者の限定 • 長期共有秘密の第三者開示は絶対的な理由が存在する場合のみ	• 単要素認証 • オンライン推測攻撃対策 • リプレイ攻撃対策	以下の対策を行う • アサーションの自作/改ざん • アサーションの再利用	

行政機関における個人に相当

民間サービス（ビジネス、プライベート）における個人

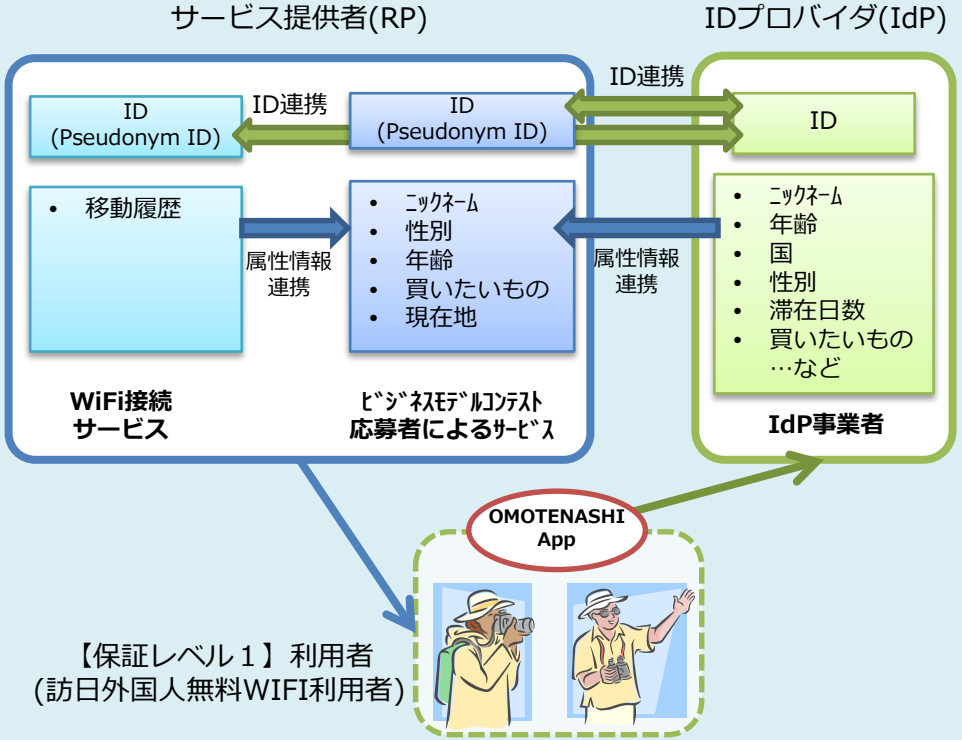
ユースケース実証について

平成26年度（ID連携トラストフレームワークの試験プラットフォームを活用したビジネスモデルの実証事業）

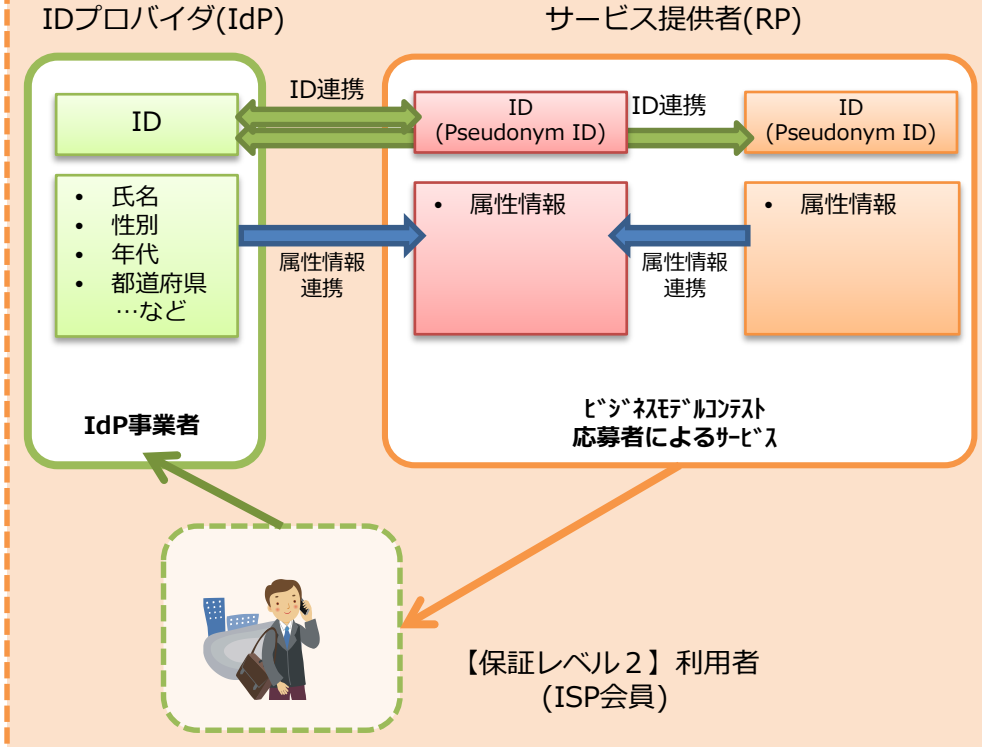
オンラインで完結する仕組み（保証レベル１および２のID連携PF）を提供し、実利用者を対象としてサービス・アプリケーションの実証を行うことで、**産業界がID連携トラストフレームワークを利用する際の課題を抽出**

- **コンテストを通じたID連携を活用するビジネスモデルの発掘**
- **実証に基づくID連携を活用したビジネスにおける課題の抽出**
- **事業者を保証レベル１、2の基準で評価することで基準の内容を精査**

①保証レベル１（おもてなし）



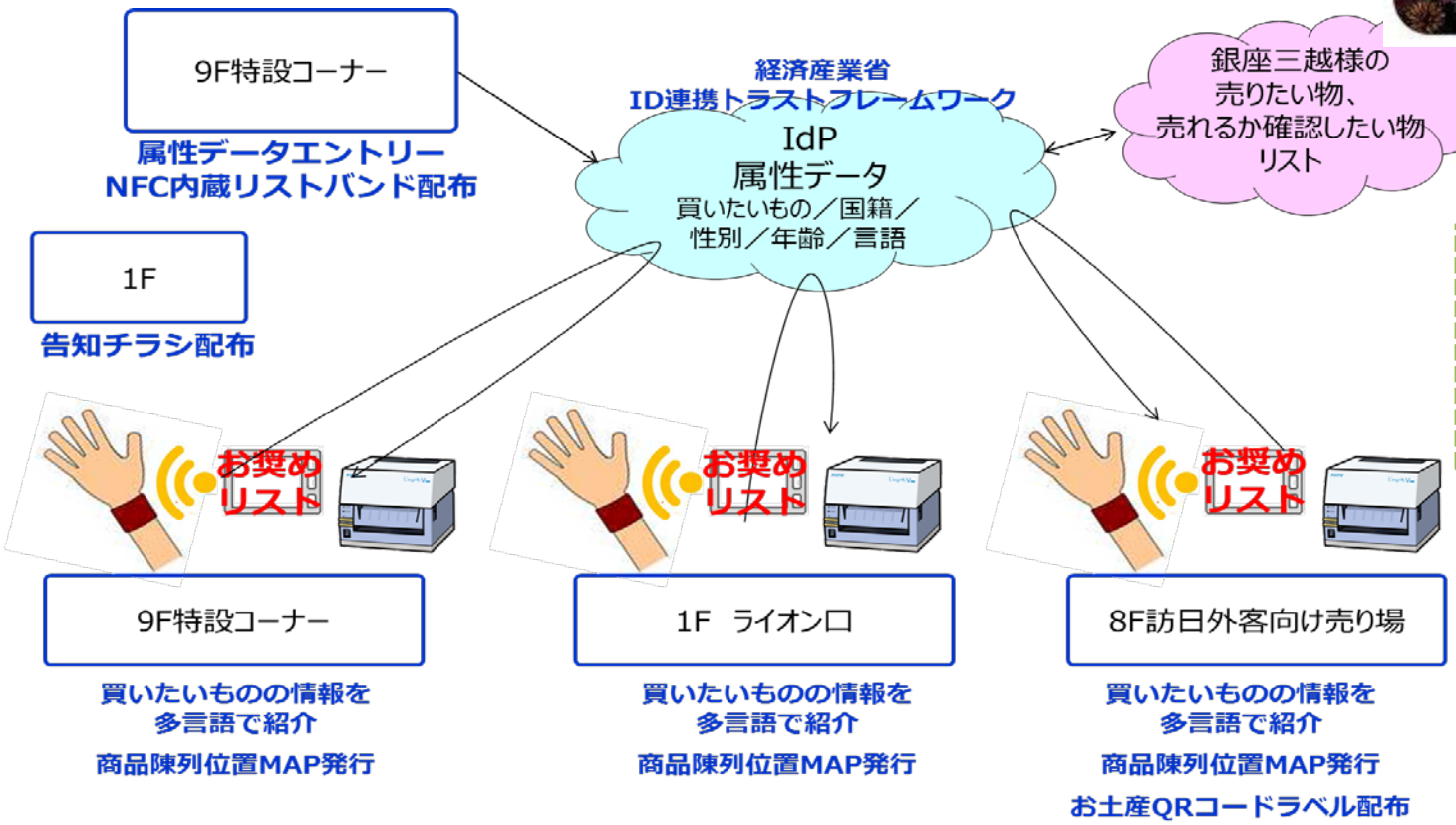
②保証レベル２（確からしさ）



【参考】保証レベル１（最優秀賞：株式会社サトー）

利用者（訪日外国人）に属性情報が格納されたNFC内蔵リストバンドを配布し、各タッチポイントで読取端末にNFCをかざすことで、属性情報に基づいて日本の新しい魅力的な商品を紹介し、売り場までナビゲーションする。

実施期間　2015年2月18日（水）～22日（日）
利用者数　398名



9階特設コーナーで利用者登録を行い、リストバンドを配布する。利用者は、1階、8階、9階で端末へのアクセスし、各売り場で買い物する。

【参考】保証レベル２（BIGLOBE、キレナビ）

BIGLOBEの回線契約などにより（保証レベル２相当）身元確認が行われている会員に対して、医療コスメの販売・医療エステのクーポンサイトである会員サイト「キレナビ」の会員限定コンテンツ（**医療広告の観点から、メディカルエステは会員のみが閲覧可**）を、「キレナビ」会員登録なしにID連携によって提供する。

実施期間　2015年2月19日（木）～3月13日（金）
利用者数　同期間の一般新規利用者数166名
　　ID連携を活用した利用者数33名

認証結果を通知

BIGLOBE
ログイン画面
（BIGLOBE ID、PW 入力）

会員サイト「キレナビ」は、皮膚科などの美容医療を行うクリニックの施術（メディカルエステ）のクーポンと、そのクリニック監修のもと、一般販売されている化粧品（ドクターズコスメ）を販売するサイトである。

【参考】ID連携トラストフレームワークのメリット

ID連携トラストフレームワークによる利用者、事業者メリット

■ 利用者

①利便性	• オンラインで繋がることで情報収集が簡単になり、時間節約できる。 • 紙での処理、保管がなくなる。
②透明性	• 提供先、提供される情報項目が提示され同意を取得できる（連携する際に）。
③信頼性	• 個人情報保護やプライバシー保護のルールが明確されることで、事業者が信頼できるか判断の尺度になる。

■ 事業者

①手間の削減	• IdPが行ってる身元確認や当人確認の程度がわかることで、RPは自身に適したIdPが採用でき、身元確認や当人確認を実施する必要がなくなる。
②事業者の評価	• 個人情報保護やプライバシー保護のルールが明確されることで、事業者同士でも信頼性の評価ができる。
③連携の可能性の増大	• 事業者同士でも信頼性の評価ができ、安心安全になることで、分野横断に繋がり、情報の流通が活発になり、新しいサービスが生まれる。

サービス実証においてIdPおよびRPを担う事業者のモチベーション

テーマ	IdP	RP
LoA1 (おもてなし)	• 訪日外国人向けのオンラインサービス市場は新規開拓の対象である • 訪日外国人向けのサービスについては、企業の事業戦略の一環で先行投資がし易い状況である	• IdPと同様に、訪日外国人向けのオンラインサービス市場を開拓するため • 訪日外国人向けのサービスについては、企業の事業戦略の一環で先行投資がし易い状況である
LoA2 (確からしさ)	• ID連携に取り組むことにより、既存会員へのサービス向上や新規サービスの開拓が期待できる • マイナンバー/マイガバメント対応を想定したID連携への関与することにより、将来事業への発展が期待できる	• IdPの会員を対象として、新規会員（新規顧客）の獲得が期待できる • 確かな本人であることを保証されることで、 炎上防止や情報・サービスへの付加価値が期待できる

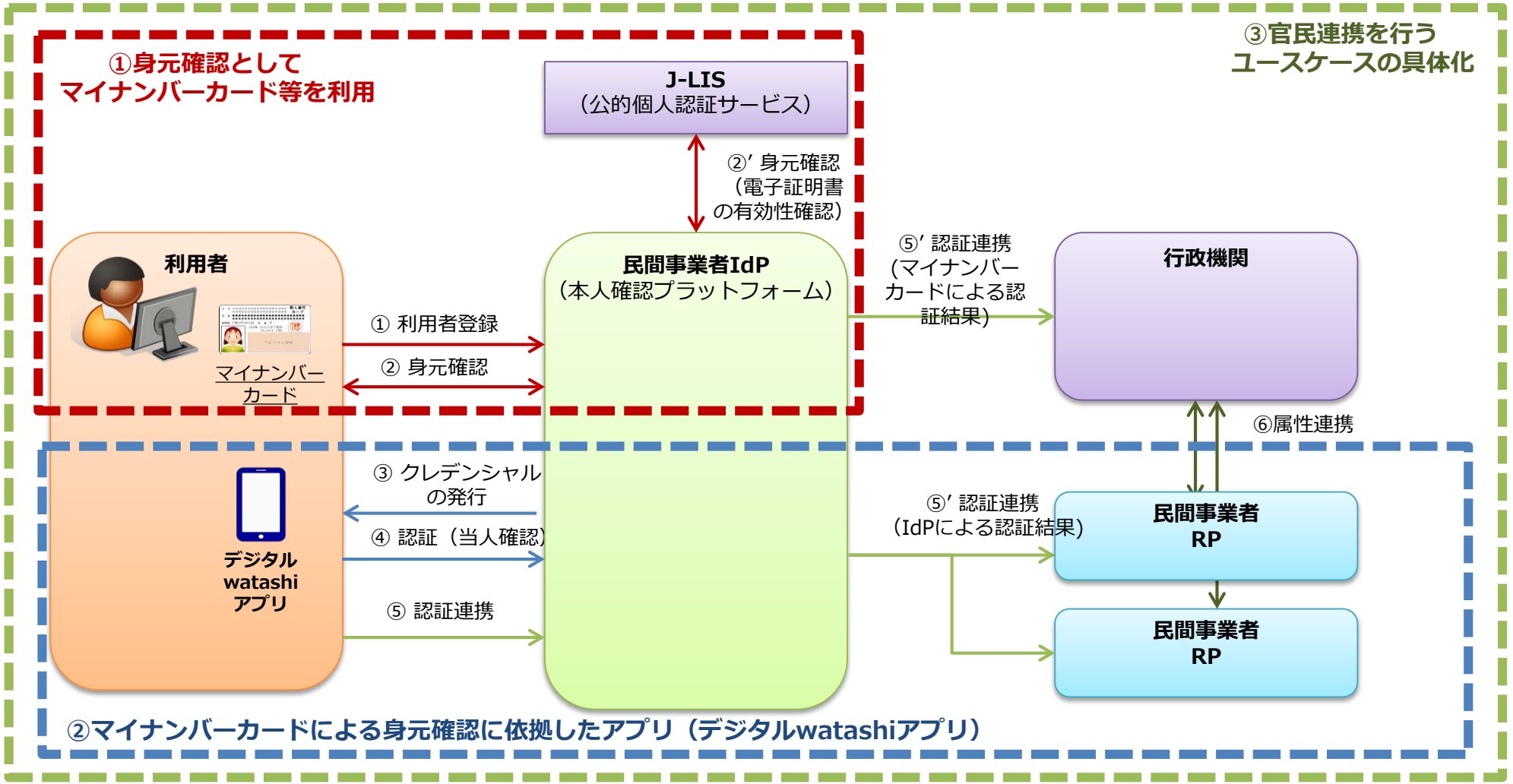
【参考】実証から明らかになった課題

サービス実証を通じて明確になった、ID連携を事業化するに当たっての課題

テーマ	IdPの課題	RPの課題
共通	• IdPの**単独事業では、利用者に対するメリット（サービスの提供など）が示し難い**ため、利用者の獲得が難しい（利用者数が少ない段階で利用料を支払うRPがいない） • 既にサービスを提供する事業者がIdPサービスを提供する場合、既存の利用者に対して追加で情報連携に関するオプトインが必要となるため、IdPサービスを開始するまでに時間を要する	• ID連携の技術知見がなく、仕様への準拠や実装に時間を要する • ID連携により**新規顧客の獲得をどの程度見込めるか**が不明（顧客獲得の可能性は、IdPの会員数や分布が影響） • ID連携自体がレベル１での普及に留まっている
保証レベル１ (おもてなし)	• ユーザ登録時に、個人情報でなくても、**複数項目の登録がある時点で、ユーザの利用意向が下がる**（登録の手間を軽減しなければ、利用者の獲得が難しい） • IdP単独事業として運営する場合の価格設定（単独運営が難しい） • 外国人旅行者を対象とする場合、退会やオプトアウトの設定が難しい（今回は実証であるため期限を区切った）	• 利用者が使いたい場所に、無料のWiFi APが存在するか、確認する方法がない（無料の公衆無線LANがインセンティブにならなくなる） • アンケート等で収集した（個人情報ではない）属性項目の詳細度については、**業種・サービスに応じた詳細な情報が必要となるためIdPとの調整**が必要（業種・サービスごとのデータの定義が必要か）
保証レベル２ (確からしさ)	• 実在する利用者の本人確認をした属性情報を受け渡すこととなり、ID連携トラストフレームワークが一般化されていないことから、**実証実験と言えどもRP事業者との契約に時間を要する。**（IdPとRPに対して、基準案を適用した監査作業を行っており、規格化することによる効率性の定性評価を実施している。）	• 実証実験で提供される属性情報の粒度（例：年齢（21歳）を年代（20代）で渡す等）に応じたサービス内容を検討する必要がある。 • 既にサービスを行っている事業者が、**IdPと組んで事業を進める場合に、それまでの利用者の移管**について懸念がある。（移管時にサービスを止めてしまう等）

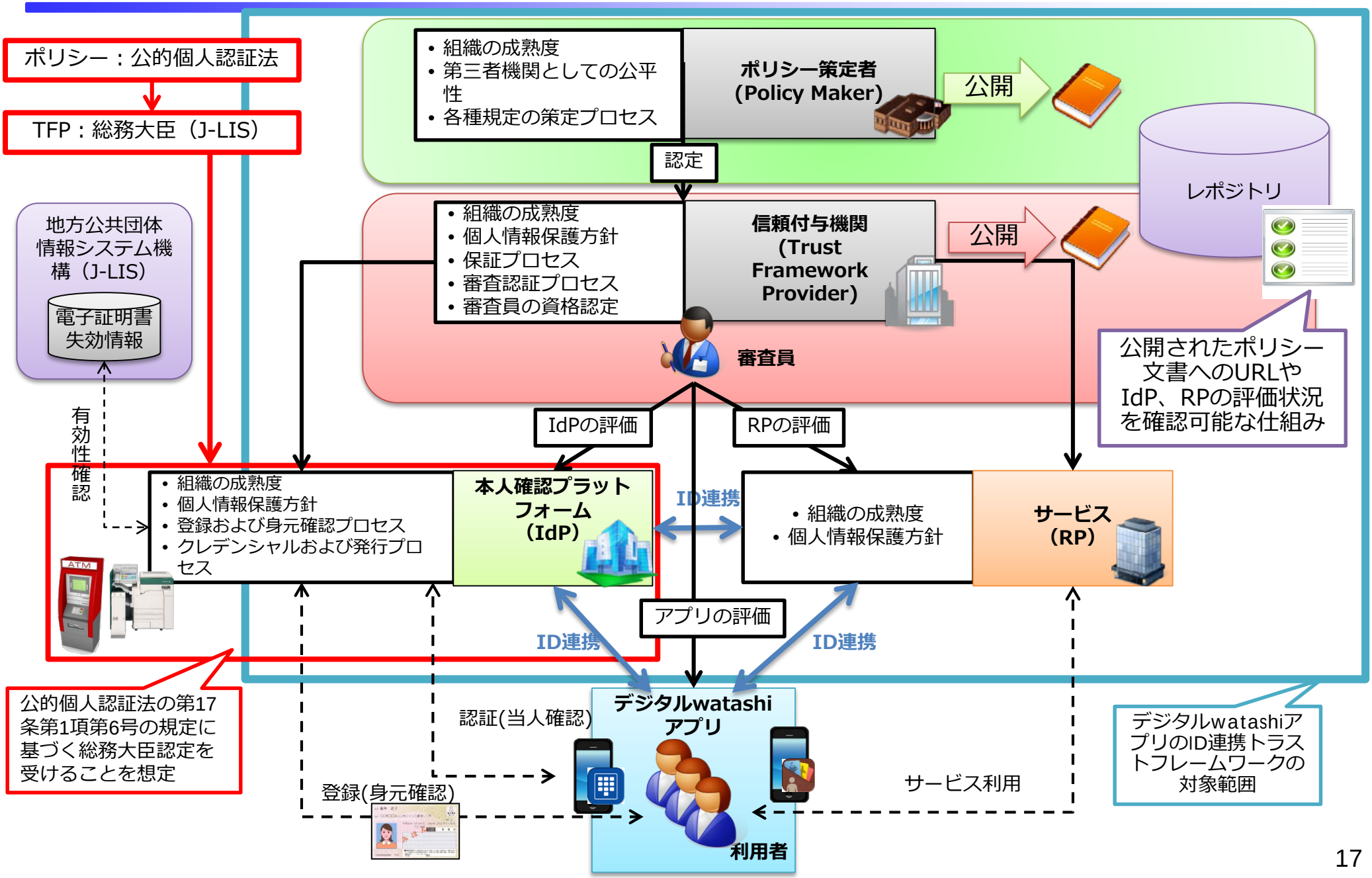
平成27年度（ID連携トラストフレームワークを活用した官民連携の在り方に関する調査研究）

「マイナンバーカード」、「公的個人認証サービス」および「官民連携」についての民間サービス事業者による利用方法の明確化や具体的なユースケースからID連携トラストフレームワークに求められる事項について検討し、課題の抽出及び要件を整理



【参考】デジタルwatashiアプリID連携トラストフレームワーク構成

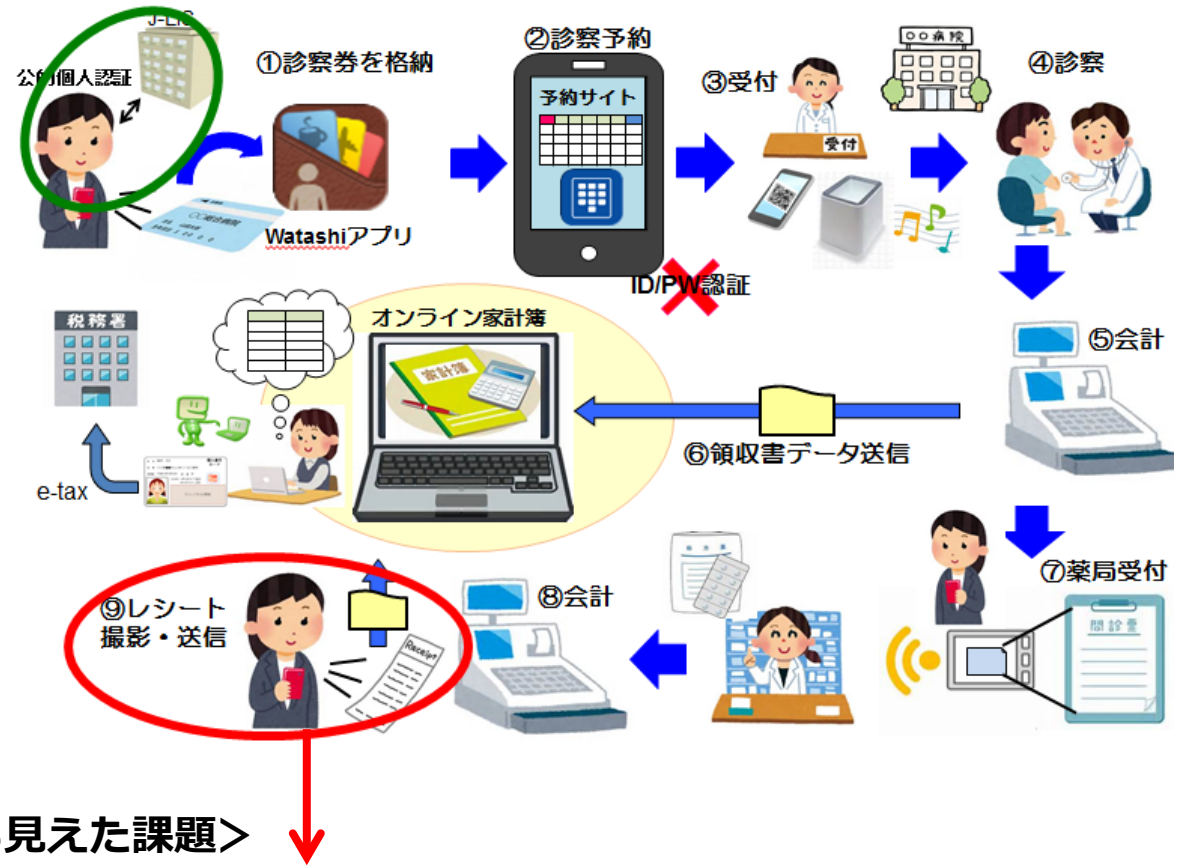
JIPDEC



【参考】家計簿アプリでのユースケース実証

JIPDEC

<家計簿アプリによるID連携調査研究>



<調査研究から見えた課題>

- ●レシートの読み取りなどオンライン完結できないという課題が見えた
  - ⇒利用者もオンライン完結を望む声が多かった
- ●スマホアプリにもトラストが必要はないか
  - ⇒正当なアプリであることを確認できる環境(リポジトリ)の必要性

平成28年度（ＩＤ連携トラストフレームワークのためのリポジトリ検討）

JIPDEC

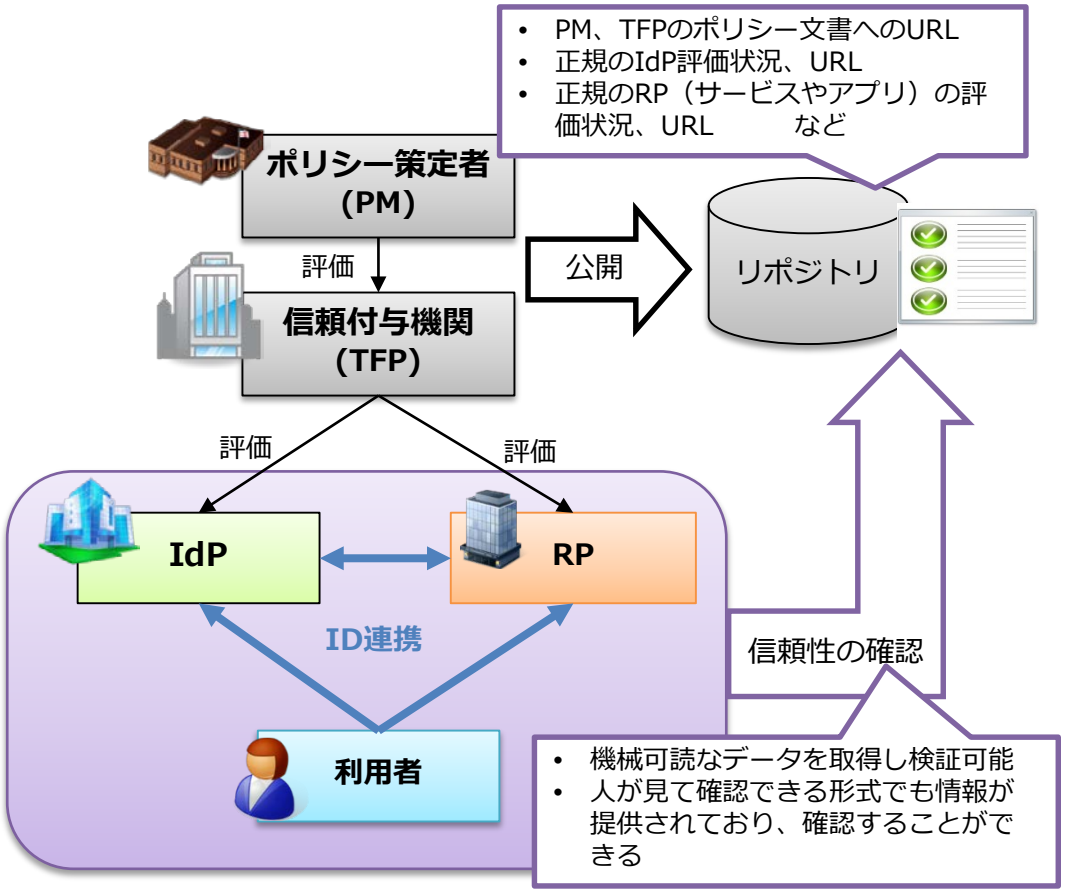
- リポジトリの活用により、例えばフィッシングサイト等によるサイバーセキュリティリスクを低減させることが可能となることで、行政手続を始めとする様々な紙媒体による業務や手続の電子化推進の一助となることが期待される。
- 本事業はリポジトリに求められる必要な要件や運用方法など、リポジトリに関する在り方を検討。

■ リポジトリ（またはレポジトリ）

- 【英】repository
- 情報システムの設計、開発、保守に関する、ソースコードや設計、データの仕様といったあらゆる情報を統合的に保管するデータベースを指すことが多い。

■ トラストリポジトリ（本プロジェクトにおいて定義する用語）

- 【英】trusted service repository
- トラストフレームワークにおいて、PMやTFPなどのTrust Authorityによって評価されたIdPやRP（またはRPの提供するサービスやアプリ）について、当事者が相互に信頼性を確認するための情報（ポリシー文書やサービスの評価結果、状態等）を、管理し公開する場所のことである。



【参考】検討対象のユースケース

- 政府ドメインリスト
  - 政府機関が持つ公開しているドメインおよび各ドメインの代表的なサイト一覧
- デジタルwatashiアプリ
  - マイナンバーカードで本人確認の上発行したインターネット上の身分証明書やオンライン認証手段を提供するアプリ

リポジトリWebサイト（イメージ）

repos-trial.trust.s3-website-ap-northeast-1.amazonaws.com/jpdomains/

TWOperatorOrganizationUnit	経済産業政策局　新規産業室
TWSummary	起業家教育の充実を目指し、各種イベントの開催や関連情報の提供を行う。
TWURL	http://www.jeenet.jp/
TWUpdateDate	2017-03-08T18:30:00+09:00

[-] TrustWebsite ベンチャー創造協議会

TWCreateDate	2017-03-01T00:00:00+09:00
TWExpireDate	2020-03-31T23:59:59+09:00
TWName	ベンチャー創造協議会
TWOperator	経済産業省
TWOperatorOrganizationUnit	経済産業政策局　新規産業室
TWSummary	ベンチャー創造協議会の活動やベンチャー関連イベントに関す
TWURL	http://vbcc.jp/
TWUpdateDate	2017-03-08T18:30:00+09:00

[-] TrustWebsite 製品含有化学物質情報伝達スキームchemSHERPA

TWCreateDate	2017-03-01T00:00:00+09:00
TWExpireDate	2020-03-31T23:59:59+09:00
TWName	製品含有化学物質情報伝達スキームchemSHERPA
TWOperator	経済産業省


```
        <TWExpireDate>2020-03-31T23:59:59+09:00</TWExpireDate>
        <TWName>起業家教育ひろば</TWName>
        <TWOperator>経済産業省</TWOperator>
        <TWOperatorOrganizationUnit>経済産業政策局　新規産業室</TWOperatorOrganizationUnit>
        <TWSummary>起業家教育の充実を目指し、各種イベントの開催や関連情報の提供を行う。</TWSummary>
        <TWURL>http://www.jeenet.jp/</TWURL>
        <TWUpdateDate>2017-03-08T18:30:00+09:00</TWUpdateDate>
    </TrustWebsite>
    <TrustWebsite>
        <TWCreateDate>2017-03-01T00:00:00+09:00</TWCreateDate>
        <TWExpireDate>2020-03-31T23:59:59+09:00</TWExpireDate>
        <TWName>ベンチャー創造協議会</TWName>
        <TWOperator>経済産業省</TWOperator>
        <TWOperatorOrganizationUnit>経済産業政策局　新規産業室</TWOperatorOrganizationUnit>
        <TWSummary>ベンチャー創造協議会の活動やベンチャー関連イベントに関する情報提供等を行う。</TWSummary>
        <TWURL>http://vbcc.jp/</TWURL>
        <TWUpdateDate>2017-03-08T18:30:00+09:00</TWUpdateDate>
    </TrustWebsite>
    <TrustWebsite>
        <TWCreateDate>2017-03-01T00:00:00+09:00</TWCreateDate>
        <TWExpireDate>2020-03-31T23:59:59+09:00</TWExpireDate>
        <TWName>製品含有化学物質情報伝達スキームchemSHERPA</TWName>
        <TWOperator>経済産業省</TWOperator>
        <TWOperatorOrganizationUnit>製造産業局　化学物質管理課</TWOperatorOrganizationUnit>
        <TWSummary>製品に含有される化学物質の情報をサプライチェーンを通して伝達する取組「chemSHERPA」を紹介する
        <TWURL>https://chemsherpa.net/</TWURL>
```


リポジトリ掲載データ（イメージ）

まとめ

まとめ

JIPDEC

■ 成果
- 適切な身元確認と当人確認の保証レベルの整理
- ID連携を活用し、民間サービスにおける認証コストの抑制
- 多要素・帯域外認証等による認証レベルの向上（ID/パスワード認証からの脱却）

■ 課題
- マイナンバーカード利用環境（多様なアクセス手段など）の普及
- ID連携を活用したビジネスモデルの発掘・創出
- ID連携トラストフレームワークの整備（制度面・技術面等）

■ 今後の展望
- デジタルファースト、コネクテッド・ワンストップ、ワンスオンリーの実現
- 官民データ活用推進等を通じて、オンライン完結社会を推進する環境づくり

ID連携を伴うユースケースの紹介

（ID連携トラストフレームワーク推進コンソーシアムにおけるユースケース検討）

コンソーシアムについて

JIPDEC

■ 名称

- アイデンティティ連携トラストフレームワーク推進コンソーシアム

■ 組織体制

- 会長　　：中村 素典（国立情報学研究所）
  事務局　：アイデンティティ連携トラストフレームワークコンソーシアム事務局
  （一般財団法人日本情報経済社会推進協会　電子情報利活用研究部）

■ 活動目的

- 本コンソーシアムは、産業界のニーズを通して、アイデンティティ情報を異なる組織間で連携するための環境整備を推進し、組織間の相互運用性、効率性を確立するとともに、利用者に対する利便性、透明性を向上させ、新規ビジネス創出、オンライン完結社会の推進を目的とする。

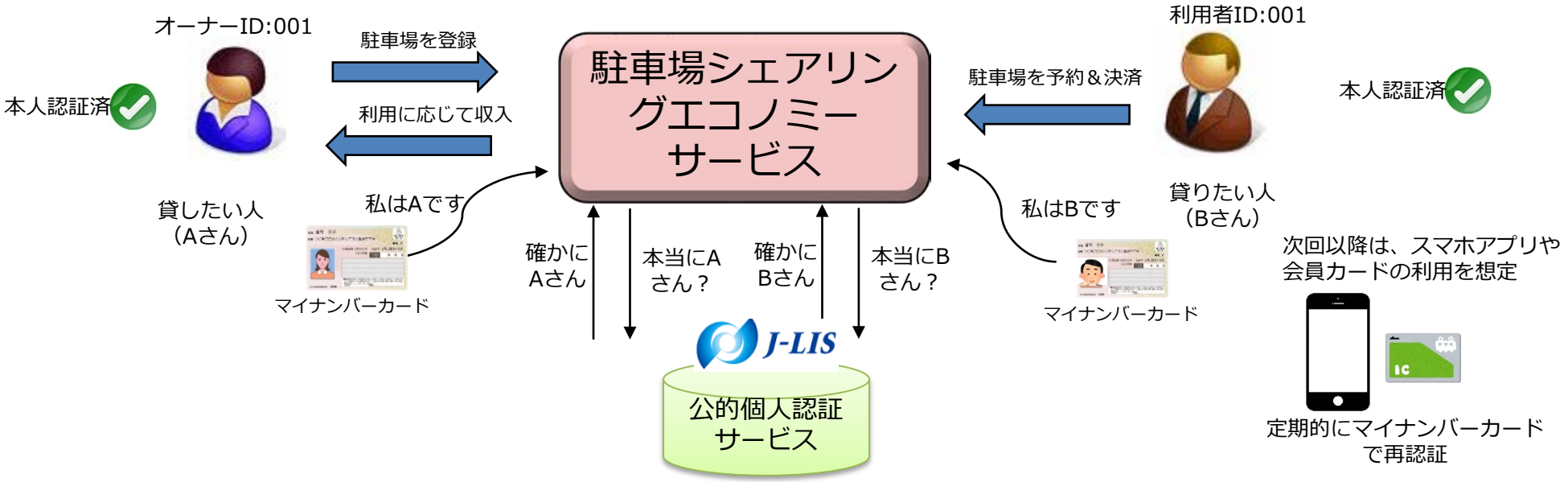
■ 事業概要

- 本コンソーシアムは、活動目的を達成するため、次に掲げる事業を行う。
  1. マイナンバー制度を視野に入れたアイデンティティ連携トラストフレームワークの制度および技術等の検討
  2. アイデンティティ連携によってサービスの効率化、高度化が図れるユースケースの創出

シェアリングエコノミー（駐車場サービス）

■ 課題
- 駐車場を貸したい人は、どんな人が借りるのか不安
- 駐車場を借りたい人は、どんな人が所有している駐車場か不安

■ 対策
- 公的個人認証サービスで本人確認を行うことで、双方の不安を解消
- 次回以降はスマホアプリ、会員カード等の利用を想定
- 駐車場オーナーが法人の場合は、法人DBとも連携



1．登録時（身元確認）
①駐車場を貸したい人は、シェアサービスの登録時にマイナンバーカードを使って、本人確認を実施し、本人確認情報を登録
②駐車場を借りたい人は、シェアサービスの登録時にマイナンバーカードを使って、本人確認を実施し、本人確認情報を登録
※どちらの場合も定期的（例：年1回）にマイナンバーカードを用いて更新作業を行う）

2．利用時（当人確認）
ユーザ登録時に端末内のアプリに本人確認済みであることも記録するため、次回以降の予約利用時にはスマホアプリや会員カードを利用。

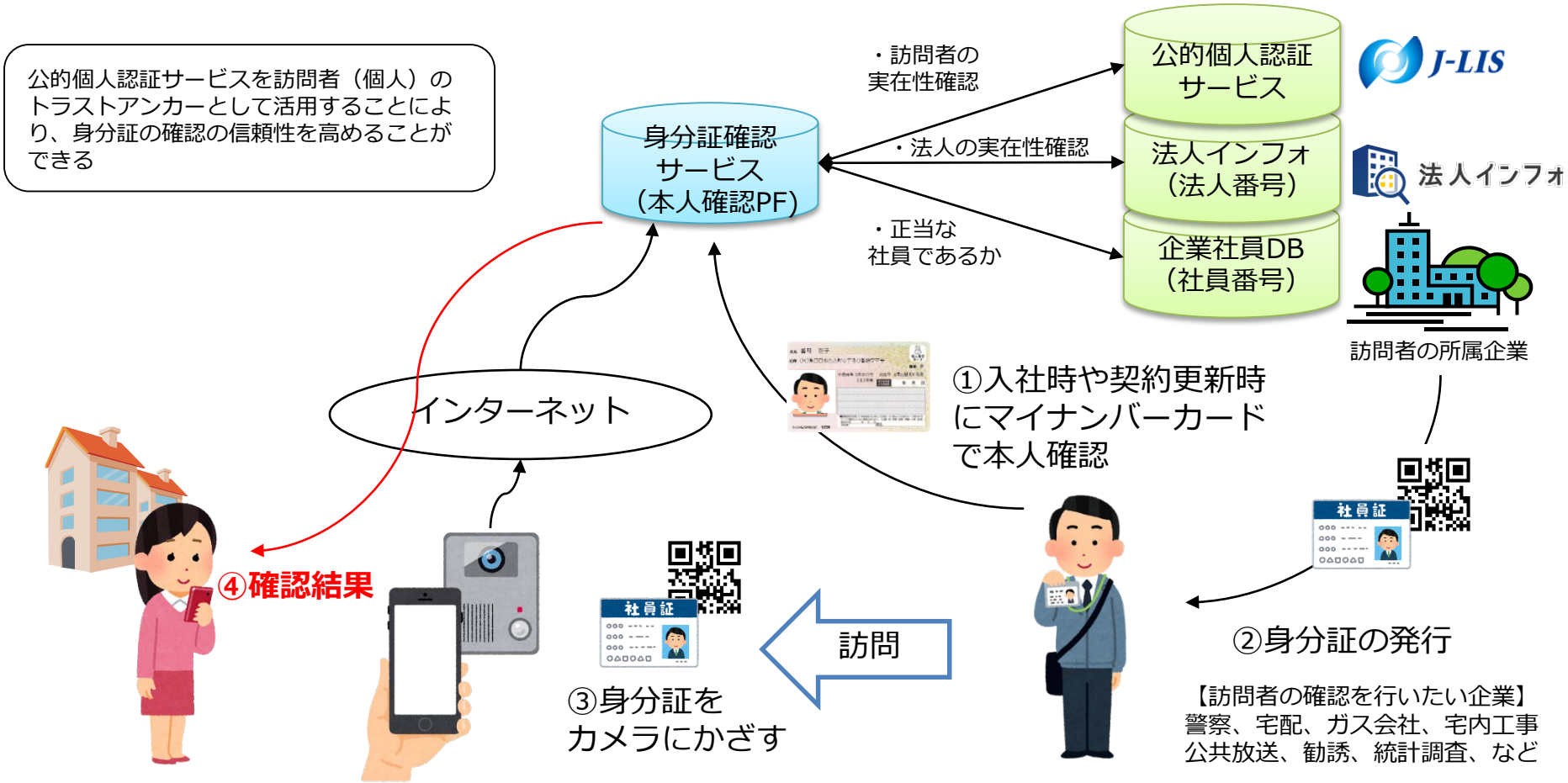
身分証の確認

■ 課題

- 電気・ガスの検針や、自治体の職員などが個人宅を訪問した際に、身分証を提示するが、来訪された個人は、それが本物かどうかの判断ができない。

■ 対策

- 玄関先で（扉を開ける前に）インターホンのカメラ、スマホのカメラで写すだけで、訪問者が本物かどうか（本当の社員かどうか）が確認できる。



各自治体独自サービスへの展開

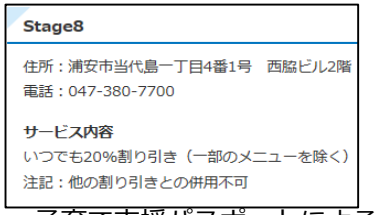
■ 課題

- 運転経歴証明によるタクシー割引、子育て支援パスポートによる学校制服の割引など、個別の状況にあった割引が行われており、その受給には個別の“紙”が必要。（財布が膨らむ問題）

■ 対策

- 公的個人認証サービスを用いた本人確認を用いて、利用者本人を特定しサービス提供

運転経歴証明書による
タクシー料金割引（静岡）



子育て支援パスポートによる
理美容院割引（浦安）

シニアパスポートによる
着物割引（群馬）