インキュベーションラボ成果報告

対象テーマ
公的個人認証基盤（JPKI）の民間利活用を推進するための
デジタルID基盤を実現するアーキテクチャ

2023年9月
独立行政法人情報処理推進機構（IPA）
デジタルアーキテクチャ・デザインセンター（DADC）

インキュベーションラボ
公的個人認証プロジェクト

本資料・本活動の位置づけ

本資料は、第三回インキュベーションラボテーマの活動成果報告の詳細を説明する資料である。

本活動では、「Society5.0の基盤としてのデジタルID・アーキテクチャ」の設計に向けた、事前検討及びアーキテクティングの試行を行った。

目次

背景

背景

デジタルIDの現状

マイナンバー

国民全員に付与された
唯一の
悉皆性のある識別ID

利用は法律で
定められた行政手続き
のみ

マイナンバーカードに関する政府の取組

★普及率：77.9%（2023年8月6日現在：申請ベース）
★各種カードとの一体化
●健康保険証（2024秋予定）●運転免許証（2024末予定）
★マイナポータル（政府運営）
個人の行政機関からの情報閲覧できるオンラインサービス
★公的個人認証基盤（JPKI）
民間事業者も利用できるオンラインでの本人確認基盤

マイナンバーカードに関する民間の取組

★初回身元確認として、JPKIが
より信頼性が高い本人確認として
利用が広がりつつある。
★ただし、高度な利用に関しては、
制度面・技術面からの課題が多く
利活用が進んでいない。

デジタルIDトラスト関連動向

現在の社会情勢

・DFFT(Data Free Flow with Trust)
信頼性のある自由なデータ流通（DFFT）の推進
・関連国際動向（eIDAS 2.0、mDL、デジタルIDウォレット）

将来への展望

・匿名認証、自己主権型アイデンティティへの移行に
社会コスト低減と自由度拡大
※注釈　自己主権型＝開示する個人情報を本人がコントロール

１章　目指すべき社会・あるべき姿

プライバシーを保護しつつパーソナルデータの信頼できる高度利用を実現する社会システム

Society5.0の実現に向けて

Society5.0が目指すパーソナルデータを中心としたデータが高度利用できる社会

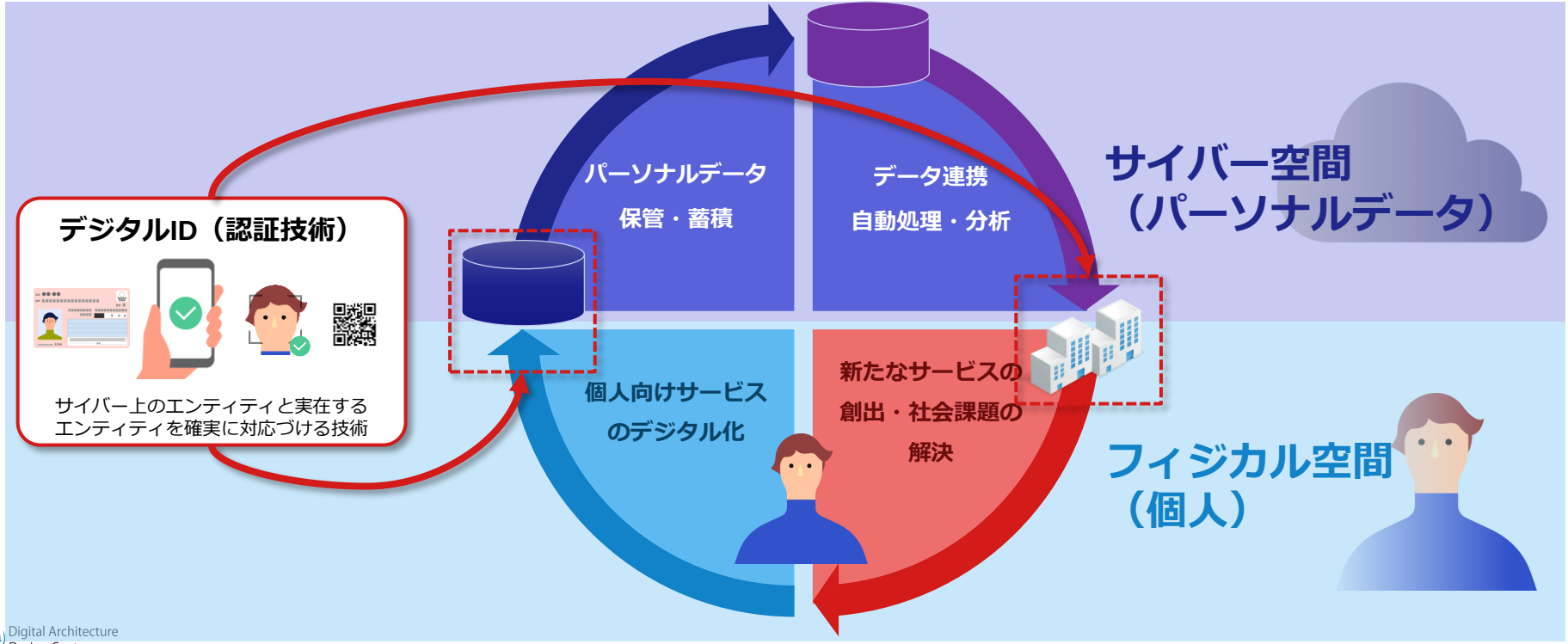
各社が様々なデータをデータベースに保管・収集するだけではなく、それらの**データを業種や企業を跨いだAPIで連携**させ、さらに**AIやデータ解析等の自動処理**によってビジネスを変革し、新たなサービスを生み出すことがSociety5.0の目指す社会像である。

出所) 内閣府, 「Society 5.0とは」, https://www8.cao.go.jp/cstp/society5_0/

出所）IPA Society5.0を実現するデジタルアーキテクチャ・デザインセンターの戦略
https://www.meti.go.jp/shingikai/mono_info_service/governance_model_kento/pdf/011_01_00.pdf

Society5.0におけるパーソナルデータ高度利用とデジタルID

サイバーフィジカルシステム（CPS）におけるパーソナルデータ活用では、サイバー空間に存在するパーソナルデータと、フィジカル空間に実在する個人とを確実に結びつけるために**【民間も活用可能な】信頼性の高いデジタルID**の役割が不可欠である。



名寄せによるプライバシーの課題

パーソナルデータを事業者間で流通・連携させることにより、新たなサービスの創出や利便性の向上が見込まれるものの、同時にプライバシーが侵害されるリスクも増大する。

- 複数のサービス事業者が、共通する識別子を用いて、それぞれの個人情報を管理していた場合、事業者間で個人情報を照合すると、個々のサービスでは明らかにならなかった個人情報を集約し、**個人の行動を追跡（トラッキング）**したり、**新たな情報を推知（プロファイリング）**することが可能になる。
- パーソナルデータが様々なサービス間で連携されていくなかで、識別子を共有してデータを連携すると、こういったトラッキング・プロファイリングの技術によって利用者の意思と異なる文脈でデータが利用され、プライバシーが侵害される恐れがある。

同意（オプトイン）による名寄せの課題

現行の個人情報保護法の規定に従い、利用者の同意を取得することで、識別子を含む個人情報の第三者提供や、プロファイリングによるマーケティング利用は可能である。しかし、以下のような課題がある。

■ **選択肢のない付合契約**

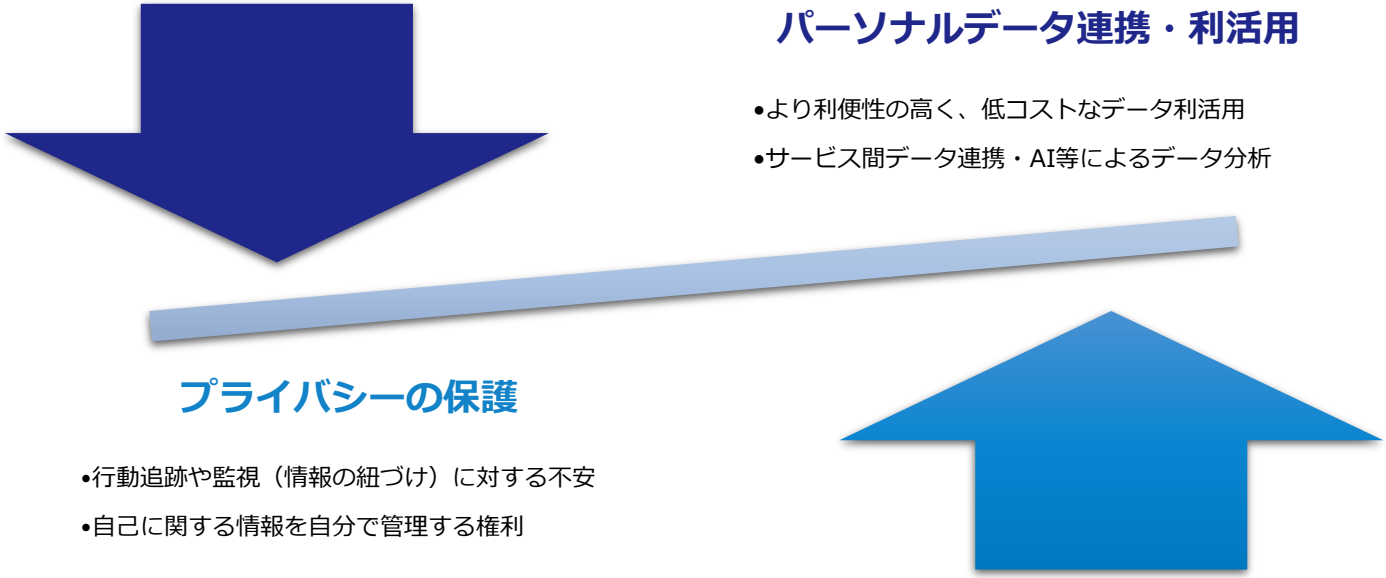
一般的にサービスの利用規約は一方的に合意するか、サービスの利用を取りやめるかの二択となっており、立場の強いサービス提供者が立場の弱い消費者に対して十分な選択肢を提供しているとは限らない。

■ **情報漏洩や不法行為**

規約により目的外利用や第三者提供を禁じていたとしても、一度何らかの事情で共通する識別子が漏洩してしまった場合、それらをすべて追跡し消去することは困難である。また、データの不正利用を外部から察知することは一般的に容易ではなく、事業者の順法意識に頼らざるを得ない側面が大きい。

相反する二つの要求

マイナンバーカード利活用が進んでいない要因として、利便性の高いサービスが生まれていないことだけでなく、プライバシーに対する国民の根強い懸念が払しょくされていないことにも、丁寧に目を向ける必要がある。



パーソナルデータ連携・利活用

- より利便性の高く、低コストなデータ利活用
- サービス間データ連携・AI等によるデータ分析

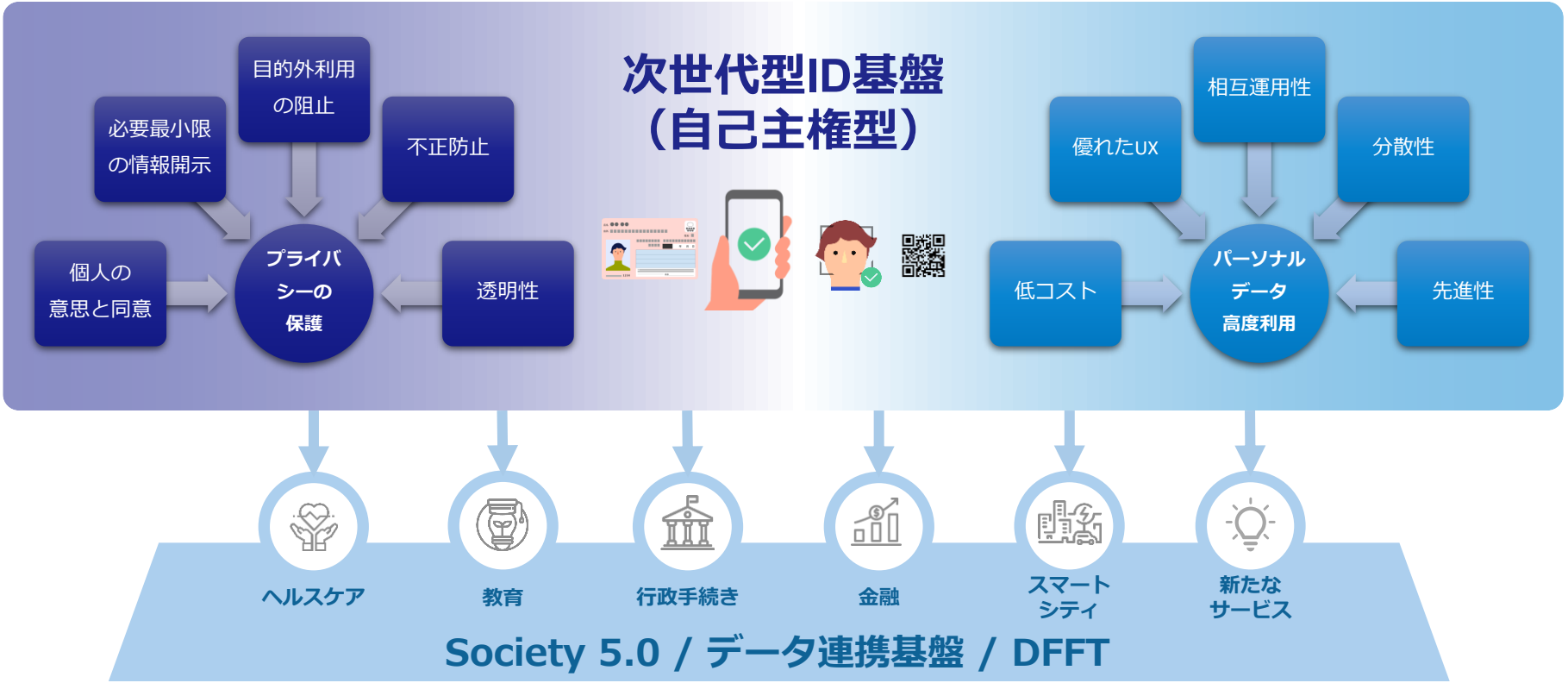
プライバシーの保護

- 行動追跡や監視（情報の紐づけ）に対する不安
- 自己に関する情報を自分で管理する権利

パーソナルデータの利活用とプライバシーを新たな水準に引き上げるアーキテクチャ設計が求められる

目指すべき社会、あるべき姿

プライバシーを保護をしつつ、パーソナルデータの信頼できる高度利用を実現する社会システム。



実現した場合の社会的インパクト

CPS上では、個人のあらゆる活動に関して、デジタルIDの信頼性が必要不可欠。
デジタルIDの信頼性がなければ、**Society5.0**は成り立たない。社会的影響は甚大。

国民にとって
- 自分の情報が、自分の意志によって選択的（情報連携先、情報種別）に安心して共有可能になる。
- 自分の知らないところで、勝手に自分のデータを悪用・乱用されることを防げ、安全性が担保できる。

民間事業者にとって
- 個人のプライバシーを保護した上で、各種サービスを開発・展開できる。
- 協調領域が整備されることにより、競争領域に経営資源を集中することができる。

官庁にとって
- 国民の信頼を得たうえで、Society5.0が目指すパーソナルデータを中心としたデータが高度利用できる社会を実現できる。
- インフラとして整備を進めてきたマイナンバーを核としたユースケースの拡大が図れる。

国家にとって
- プライバシーを保護しつつパーソナルデータの信頼できる高度利用を実現することで、
  他国の模範となるモデルを示し、先駆的IT国家を目指すことが出来る。

目指すべき社会のまとめ

- Society5.0実現において、デジタルアイデンティティ（ＩＤ）は不可欠。
- データ連携には、トラッキングやプロファイリングといった潜在的なプライバシーリスクがある。
- マイナンバーカードを含むデジタルIDは、多くの国民が漠然と抱くプライバシーへの懸念を払しょくしきれていない。

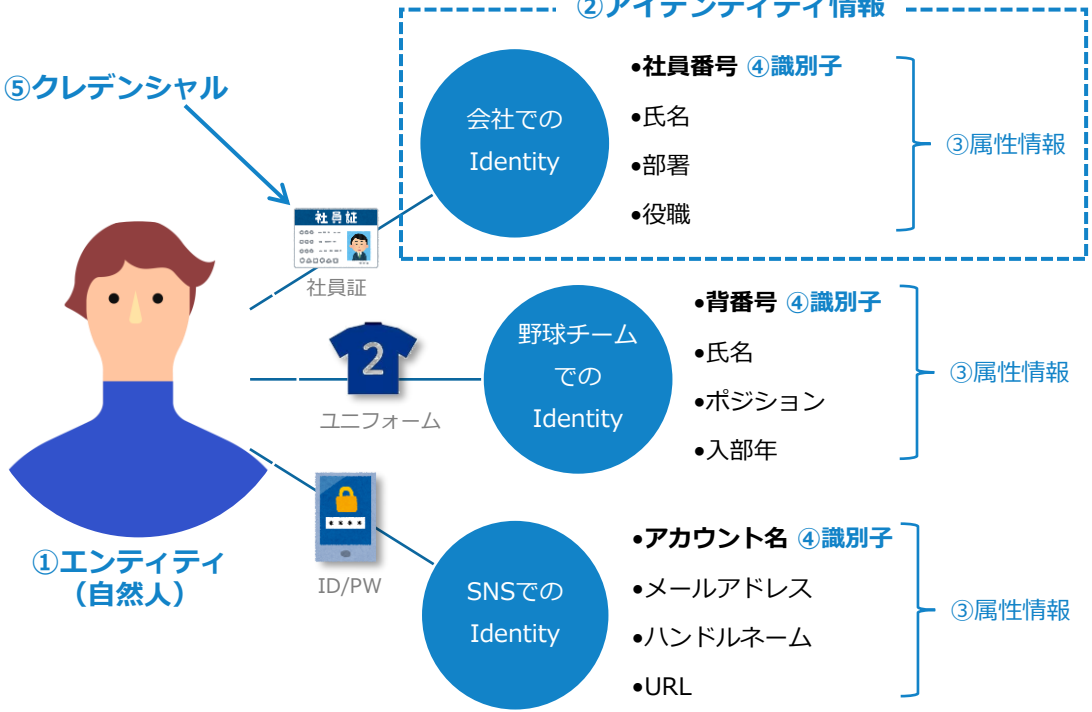
2章　現状の仕組み

（1）マイナンバーカード（JPKI）の仕組み
（2）デジタルIDの役割と本人確認
（3）識別子によるプライバシー侵害を保護する仕組み

（1）マイナンバーカード（JPKI）の仕組み

ID = アイデンティティ情報とは？

人・物・サービス等、**属性情報**を管理する単位をエンティティと言い、システムに登録されたエンティティに関する**属性情報の集合を**
アイデンティティ情報という。一般社会ではアイデンティティ情報を広義のIDと呼ぶことが多いが、ITシステム設計においては識別子を（狭義の） IDと呼ぶことが多い。



① **エンティティ・主体**（Entities/Subjects）
システムが管理する対象となる単位となる実体。人、物、組織、デバイス、サービスなど

② **アイデンティティ情報**（Identities）
エンティティに関する属性情報の集合体。ユーザー情報、デバイス情報など

③ **属性情報**（Attributes）
エンティティに関する情報。姓名や住所、電話番号など

④ **識別子**（Identifiers）
エンティティの集合から、あるエンティティを１つに識別するために用いられる一意の属性情報。社員番号、会員番号など

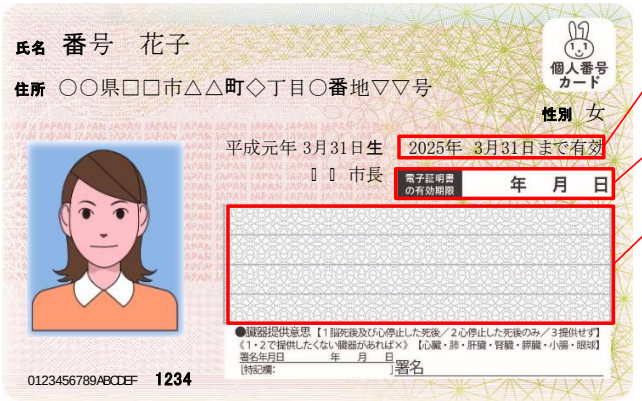
⑤ **クレデンシャル**（Credentials）
アイデンティティ情報が特定のエンティティのものであることを証明するための情報。ID/パスワードや電子証明書など。

参考文献：独立行政法人情報処理推進機構「アイデンティティ管理技術解説」

マイナンバーカードの券面に記載されている情報

表面には、提示することを前提とした個人情報が記載されている。
裏面には、マスキングされた状態で個人番号が記載されており、特定事務以外で裏面をコピーすることは禁じられている。

マイナンバーカードの表面



○ おもて面には、住所・氏名・生年月日・性別が記載され、写真が表示され、身分証明書として利用できる。

○ **カードの有効期間が満了する日**
発行の日から10回目の誕生日、
ただし、20歳未満は、発行の日から5回目の誕生日

○ **電子証明書の有効期間が満了する日**
発行の日から5回目の誕生日

○ **追記欄**
住所や氏名等の記載事項に変更があった場合に、
新しい情報が追記される

失効
- 海外に転出したとき
- 引っ越しの際、転出予定日からから30日、転入した日から14日を経過しても転入届を行わなかったとき
- 引っ越しの際、転入先の市区町村でカードの提出を行うことなく90日を経過したとき、又はその転入先市区町村から転出したとき
- 死亡したとき

出典：マイナンバーカードを活用した オンライン取引等の可能性について（令和2年4月 総務省自治行政局住民制度課）

券面に記載されている個人情報

- 基本4情報（氏名・住所・生年月日・性別）
- 顔写真
- 有効期限（2種類・誕生日が類推可能）
- 追記欄（記載事項の変更を追記）
- 臓器提供意思

マイナンバーカードICチップに搭載されている機能

マイナンバーカードに搭載されているICチップには、券面情報に加えて**「利用者証明用電子証明書」・「署名用電子証明書」**の2種類の電子証明書（及び、それに対応する秘密鍵）が搭載されている。これらを用いることで、非対面においても本人確認を行うことができる。この仕組みをJPKIと呼ぶ。

利用者証明用電子証明書

利用者の認証（同一性の検証）に用いる電子証明書。電子証明書内には、氏名を含めて基本4情報は含まれておらず、カードの持ち主が同一の本人であることのみを検証することができる。

署名用電子証明書

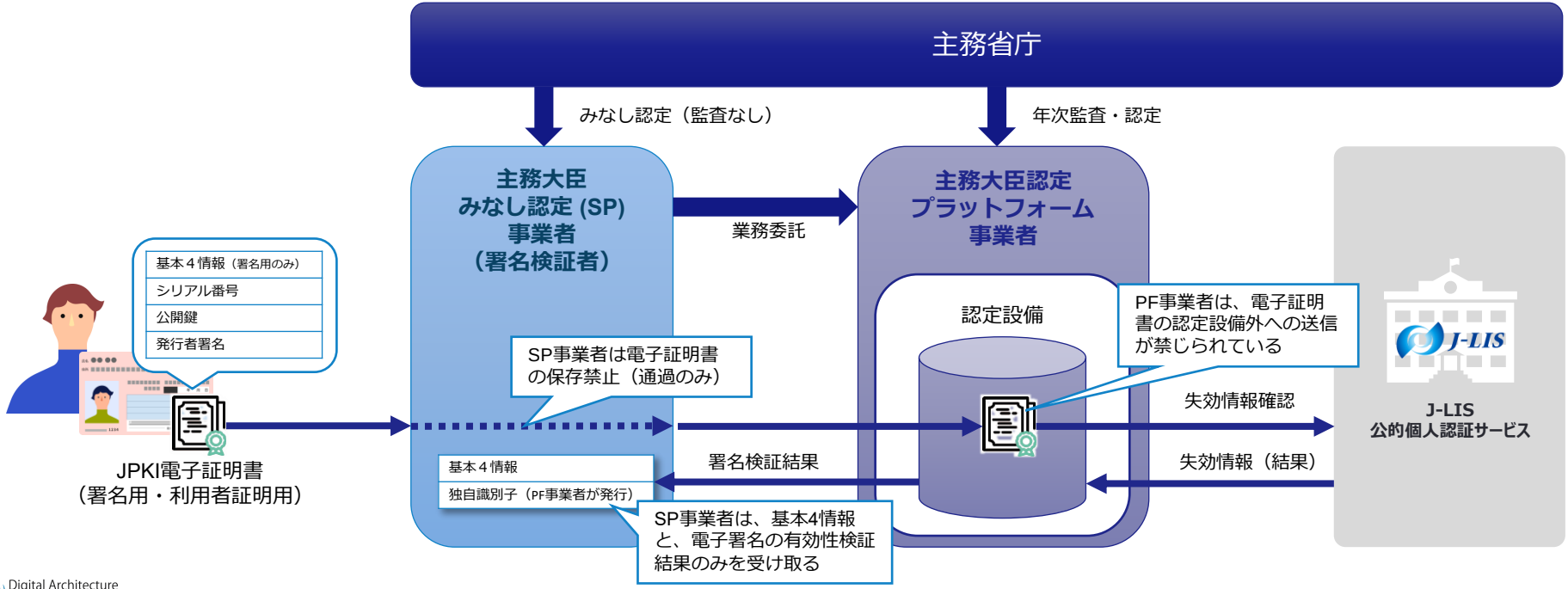
利用者の意志の表明（電子署名）に用いる電子証明書。電子証明書内には基本4情報が記載されており、署名文書に対して、検証可能な身元情報を与えることができる。

利用者証明用電子証明書	署名用電子証明書	券面情報	その他
•シリアル番号	**•シリアル番号**	**•表面記載のテキストデータ**	•住民基本台帳関連
•発行年月日	**•基本4情報（氏名・生年月日・性別・住所）**	**•顔写真**	•空き容量（拡張用）
•有効期限	•発行年月日	**•券面画像**	
	•有効期限	**•個人番号**	
公開鍵	公開鍵		
J-LISによる電子署名	J-LISによる電子署名	J-LISによる電子署名	
秘密鍵	秘密鍵		

※秘密鍵は外部から読み出すことは不可能

公的個人認証プラットフォーム（PF）事業者制度

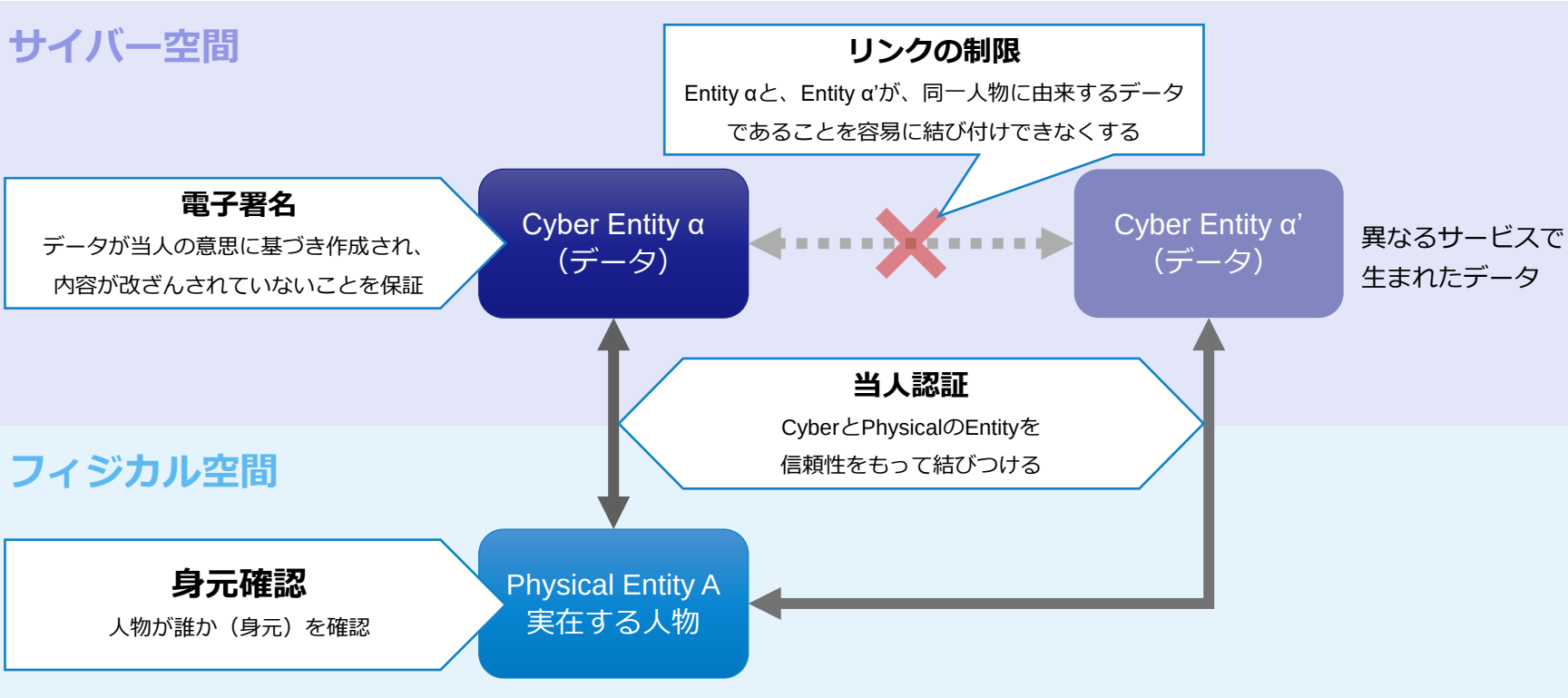
- 民間事業者が、マイナンバーカードの電子署名を検証（認証）するためには、主務大臣より監査をうけ認定を取得する必要がある。
- 認定事業者は、利用者の電子証明書を安全な認定設備内に保管することが義務付けられ、外部送信や目的外利用が厳しく禁じられている。
- 認定事業者に、電子証明書の保管を含めた署名検証業務のすべてをPF事業者へ委託することで、設備監査を受けることなく簡易な手続きで認定事業者としてみなす（みなし認定＝SP事業者）制度がある。



（2）デジタルIDの役割と本人確認

CPS上でのデジタルIDの4つの機能

デジタルIDは、実在する人物のトラストをサイバー空間で担保するための、4つの重要な機能を提供する。



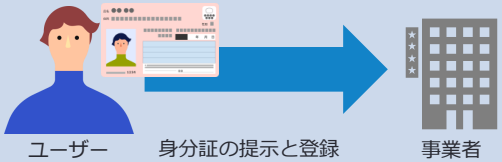
デジタルIDの4つの機能とその目的

デジタルIDが用いられる機能は、以下の４つに分類される。

機能	例	目的
身元確認 （初回本人確認）	• 金融機関口座開設時の本人確認 • 携帯電話契約時の本人確認 • アカウント開設時の初期登録	• 当該ユーザーが実在することを確認する • 当該ユーザーの身元情報（本人特定事項・基本4情報など）を取得し、その正確性を確認する • 当該ユーザーを重複なく、唯一の自然人に帰着させ、事業者の台帳に登録する
当人認証 （ログイン認証）	• ネットサービスへのログイン • コンビニ端末での住民票請求 • クレジットカードによる決済	• 操作者と事業者の台帳記載の情報を確実に対応付ける • 操作者が、まちがいなく期待される当人であることを確認する
電子署名 （電子契約）	• 電子契約への署名 • 住宅ローンの申込 • 携帯電話回線の契約 • 不動産売買契約	• 署名文書が、署名者の意思に基づいて作成されたことを検証可能な形式で証明する • 署名文書が、改ざんされていないことを検証可能な形式で証明する
リンクの制限 （意図しない名寄せの抑止）	• サービスごとに異なる識別子を発行 • 保険証提示の際の被保険者番号黒塗り	• ユーザーの意図しないトラッキングやプロファイリング（パーソナルデータの目的外利用）を防ぐ

本人確認の2つのプロセス

本人確認のプロセスは、通常は「身元確認」と「当人認証」の2つの異なるプロセスに分けられる。これらのプロセスはその目的が異なっており、その概念と違いを区別しておくことが重要である。

	目的	プロセス
身元確認  	• 当該ユーザーが実在することを確認する • 当該ユーザーの本人特定事項（基本4情報等）と、その正確性を確認する • 当該ユーザーを重複無く、唯一の自然人に帰着させて登録する	1. 本人特定事項とエビデンス（身分証）を提示・収集する 2. 提示されたエビデンスが本物であるかを確認する（Validation） 3. 提示されたエビデンスが登録しようとしている当人のものかを確認する（Verification） 4. 身元確認完了後、クレデンシャルを登録する
当人認証  	• ある行為の作業者が、まちがいなく期待される当人によってなされていることを確認する • 操作者と事業者の保持するアイデンティティ情報を確実に対応付ける	• クレデンシャル＝認証の３要素（知識・所持・生体）のいずれか（１つもしくは複数）を照合する

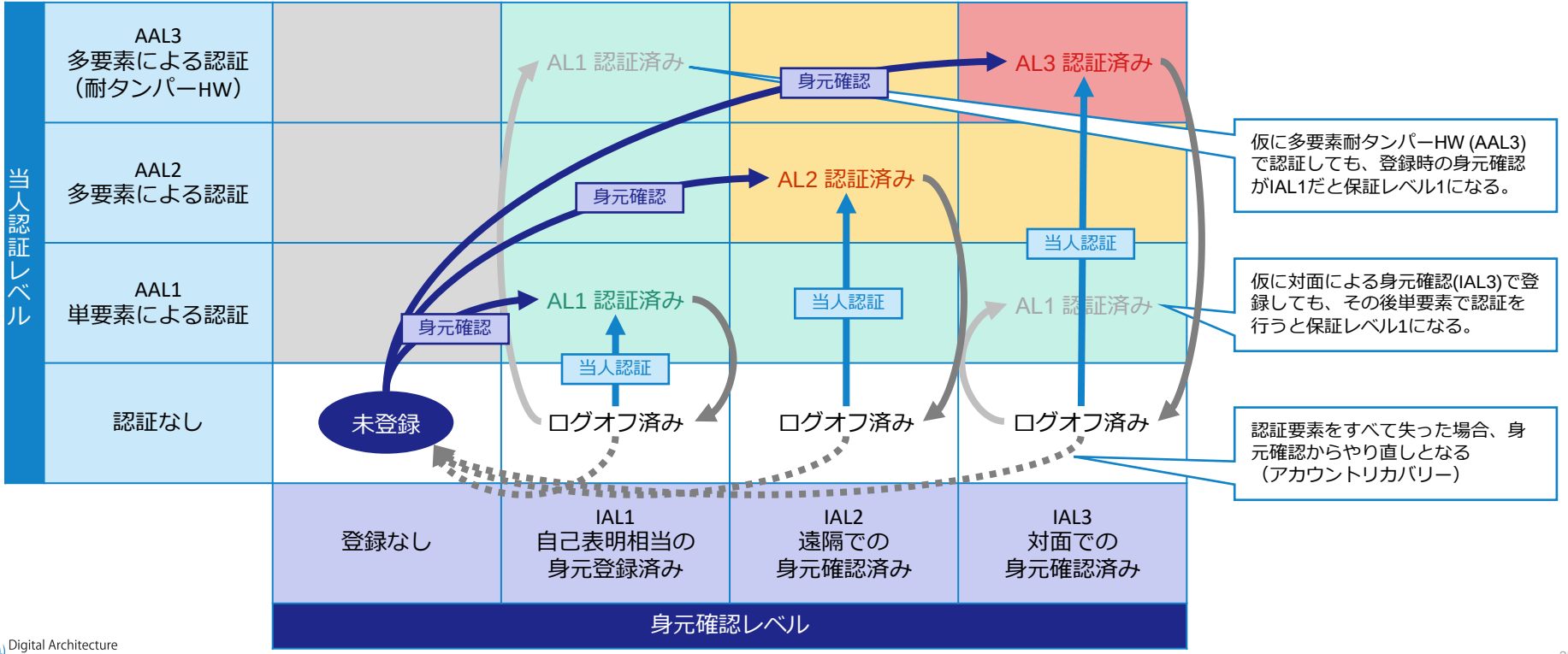
本人確認の保証レベル（Assurance Level）

行政手続におけるオンラインによる本人確認の手法に関するガイドライン（内閣官房 情報通信技術(IT)総合戦略室）によると、身元確認、当人認証、双方ともにその信頼性を3つのレベルに分けて評価し、低く評価されたほうのレベルを本人確認の保証レベルとみなす。

保証レベル	身元確認レベル （Identity Assurance Level / IAL）	当人認証レベル （Authenticator Assurance Level / AAL）
レベル3 身元が対面で確認され 信用度が非常に高い	• 写真付き身分証明書の**対面での確認** • 公的な台帳との照合 • 重複登録ではないことの確認 	• 複数の認証要素による認証（多要素認証） • 暗号プロトコル • 耐タンパー性のあるハードウェア 
レベル2 身元が遠隔又は対面で確認され 信用度が相当程度ある	• 公的な台帳との照合、もしくは公的証明書の添付 • 電子署名もしくは署名捺印 	• 複数の認証要素による認証 （多要素認証）  パスワード＋SMS認証等
レベル1 信用度ほとんどなし 自己表明相当	• 電子メールの到達確認 • ICチップを使用しない画像解析型eKYC	• 単要素による認証 

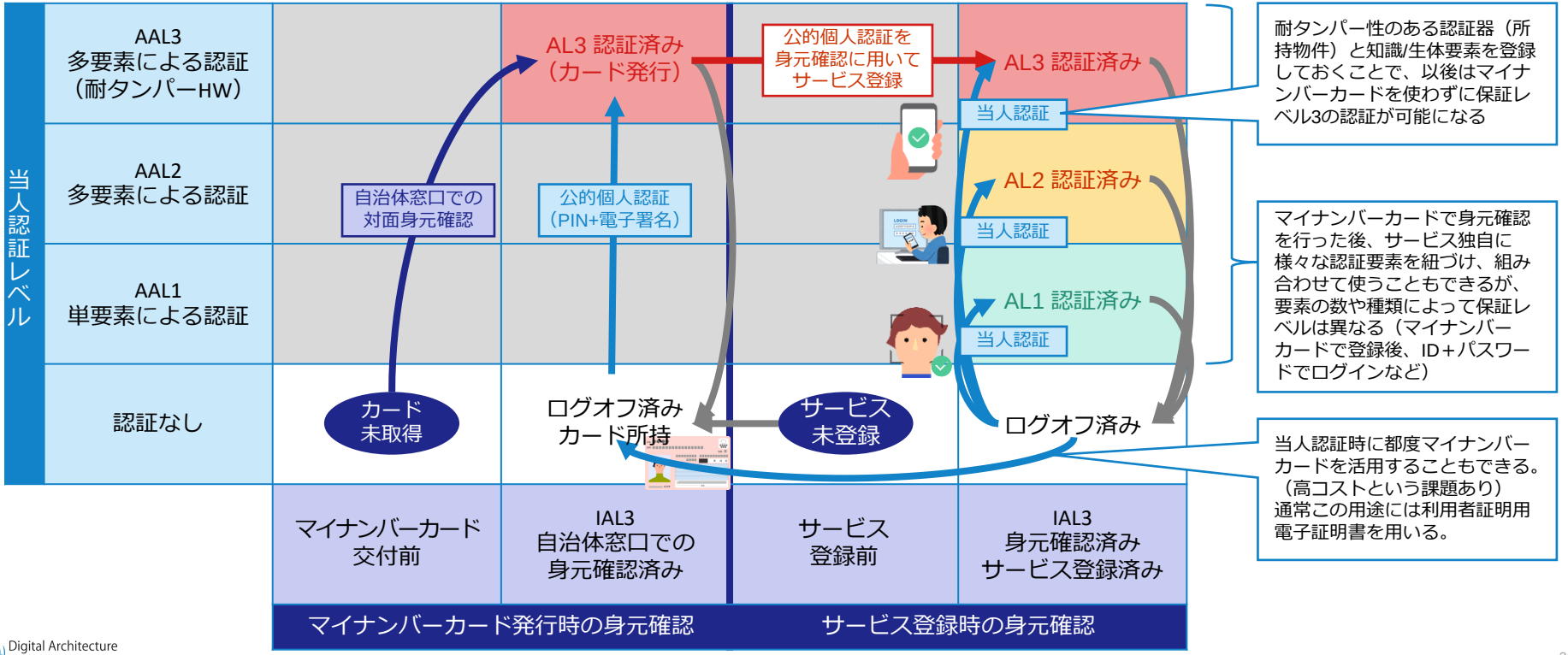
本人確認における状態遷移

認証済みの状態で認証要素（知識・物件・生体）を登録しておくことで、ログオフ後に再度当人認証を行うことができるようになる。
利便性を保ちつつ保証レベルが高い状態を作り出すためには、複数の認証要素を登録しておくことも重要である。



公的個人認証を身元確認に使う場合

マイナンバーカードの公的個人認証をサービス登録時（例えば銀行の口座開設等）に使うと、遠隔でありながら対面と同等のIAL3相当の身元確認が可能になる。各サービスでは継続的に用いる当人認証に都度マイナンバーカードを使うこともできるが、独自の認証要素を登録して以後はカードを使わないような設計も可能である。



（3）識別子によるプライバシーを保護する仕組み

識別子とは

- 識別子とは、エンティティの集合から、あるエンティティを1つに識別するために用いられる一意の属性情報。社員番号、会員番号など。
- 個人を特定できる識別子はトラッキングやプロファイリング等に利用できることから、**プライバシーを保護するためには識別子を適切に保護することが重要**である。

識別子に対するプライバシーリスクの構成要素

個人を特定する性質の強さ

悉皆性

残すところなく全員を識別できる性質

例）社員番号は当該会社内では悉皆性があるが、市民全体の集合においては悉皆性はない。

唯一無二性

重複なく一意に識別できる性質

例）ソーシャルネットワークのアカウントや携帯電話番号等は同一人物が複数作成・契約することが可能であり、唯一無二性を持つとは言えない。

ユースケースの広さ

ライフサイクル

識別子が利用される期間（ライフサイクル）が長ければ長いほど、プライバシー侵害のリスクは増大する。逆に毎回利用都度に使い捨てることで、リスクを極小化することもできる。

利用用途と範囲

ひとつの識別子を複数の事業者間で広く使いまわすことで、それぞれの事業者がもつパーソナルデータからプロファイリングが行われたり、トラッキングされたりするリスクが増大する。

識別子の変換

同じ識別子をあらゆる用途で際限なく使いまわすのではなく、用途やライフサイクルに応じて異なる識別子を振り直したり変換したりすることで、識別子の利用範囲を限定しプライバシーのリスクを軽減することができる。一方で、異なる識別子に変換したとしても、付随する様々な属性情報を組み合わせて絞り込むことで、識別子単体では特定できない個人であっても名寄せ可能になることもある。例えば、識別子が異っていたとしても、氏名やメールアドレスが同じならばそれで名寄せ・識別ができてしまうケース等が考えられる。

識別子を制限するための規制

全国民に個人を特定する性質が強い唯一無二の番号を政府が付番すると国民の情報監視につながりかねない懸念から、限られた行政手続き（税・社会保障・防災）のみで利用できるマイナンバー（個人番号）と、民間も含めて利活用できるマイナンバーカード（JPKI電子証明書）が、それぞれ異なるものとして規制も含めて法制度化された。

	個人番号（マイナンバー）	JPKI電子証明書（マイナンバーカード）
根拠法	番号法	公的個人認証法
識別子	12桁の数値	電子証明書の発行時シリアル番号 ※発行者署名や公開鍵も識別子としての性質ももつ
対象	全住民に対して付番される（悉皆性あり・唯一無二）	希望者のみ（悉皆性が高い*・唯一無二） ※署名用電子証明書は15歳以上のみ
ライフサイクル	原則一生涯同じ番号 （ただし、漏洩時等には再発行することもできる）	最長5年間 シリアル番号は電子証明書再発行時に新たに採番される
利用範囲	行政機関（税・社会保障・防災分野のみ）	行政機関および主務大臣認定をうけた民間事業者
規制	個人番号利用事務・関係事務を除き 一切の提供、保管、収集が禁止じられている	電子証明書の認定設備外での保管や 目的外の外部送信が禁じられている

官民含め、異なる事業者間での識別子による名寄せを規制する措置が講じられている。

※ JPKI電子証明書の発行は任意となっているが、国民のマイナンバーカード保有率は約71%（令和5年7月31日現在）であり、悉皆性は高いと考えられる。

参考：マイナンバーとマイナンバーカードの違い

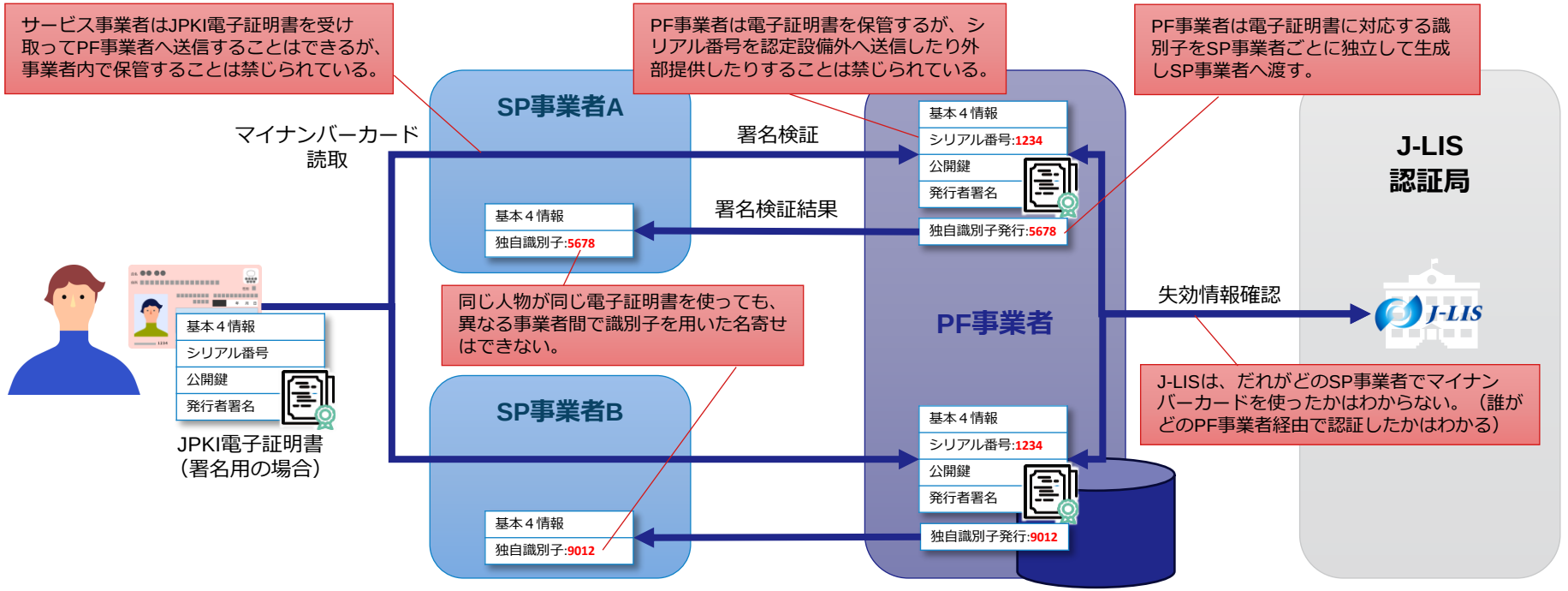
マイナンバーとマイナンバーカードの違い

マイナンバー	マイナンバーカード
	
○ 全住民1人に一つ、本人の意思にかかわらず、強制的に付番・利用される。引越・転職・結婚でも不変の番号で、個人を特定する機能が極めて強い。	○ マイナンバー使用時の本人確認（「番号確認」と「身元確認」）を1枚で行えるようにした、顔写真付きのカード。
住基ネット違憲訴訟最高裁判決を踏まえ、以下の措置を講じて制度化	本人の申請に基づき、市区町村長が厳格な本人確認を行ったうえで交付
○ 利用主体や利用範囲を法律で限定（税・社会保障・災害対策の3分野で個別に規定）。	○ 官民・分野を問わず、また、マイナンバーの利用事務であるか否かを問わず、対面でもオンラインでも本人確認手段として幅広く利用可能。
○ 情報を一元管理する仕組みとしない。漏洩防止、法定されていない収集・名寄せの禁止など、厳格に管理	○ ICチップ内に搭載された電子証明書により、マイナンバーを使わずに、オンラインで本人確認が可能。
○ なりすまし防止のため、本人確認（「番号確認」と「身元確認」）を義務付け。	○ 電子証明書やICチップの空き領域は民間活用も可能。
※ 現在、5地裁においてマイナンバー違憲訴訟が係争中（横浜、名古屋、東京地裁は国側の勝訴判決）	

出所）マイナンバーカードを活用したオンライン取引等の可能性について（令和2年4月総務省自治行政局住民制度課）

JPKIにおける識別子の取り扱い

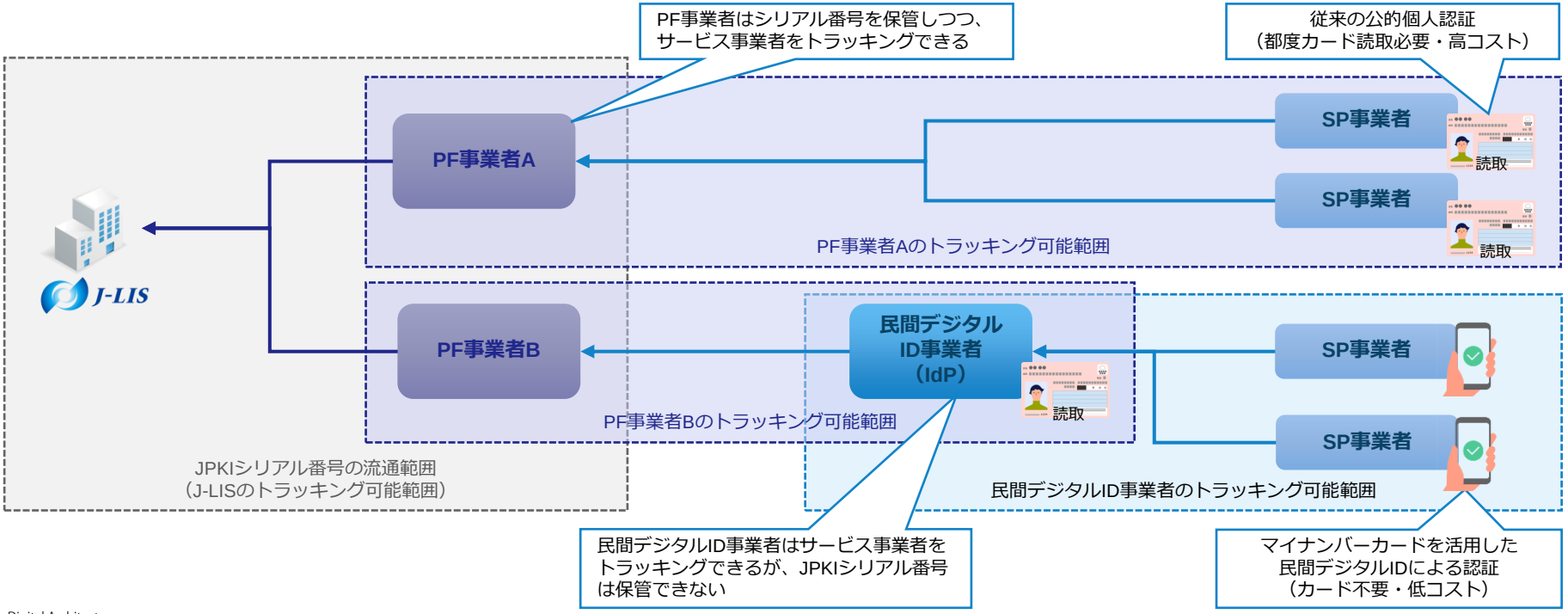
JPKI電子証明書およびそのシリアル番号は、認定を受けたPF事業者の設備内でのみ保管が認められており、異なる民間事業者間で照合できないようになっている。



※ PF事業者であれば、同一人物に対して過去に発番されたJPKI電子証明書のシリアル番号の履歴をJ-LISから取得することができる。この仕組みによって、PF事業者はJPKI電子証明書が再発行されても、同一人物を識別（トラッキング）することが可能である。

政府による国民監視を制限するPF事業者・民間デジタルID事業者の役割

サービス事業者と政府の運用する認証局との間に、PF事業者や民間デジタルID事業者等が介在することで、**識別子の流通範囲を限定し、政府による国民の民間サービス利用状況のトラッキング可能性を制限**することができる。



現状の仕組みのまとめ

- デジタルIDは、サイバー空間とフィジカル空間の間における、「身元確認」「当人認証」「電子署名」という３つの基本機能を提供する。

- デジタルIDにおいてプライバシーを保護するには「リンク不可能性（Unlinkability）」が重要である。そのためには、識別子の利用を制限し、保護する必要がある。

- マイナンバーカードは、法令と認定制度によって規制されたPF事業者を、信頼できる第三者としてJ-LISとサービス事業者の間に仲介させることで、識別子のリンク不可能性を担保している。

3章　課題の構造化

識別子を流通させない仕組みによる課題

- JPKIによる署名（認証含む）検証の証跡（電子証明書含む）データ保管には、識別子の流出を防ぐために厳しい基準と監査が義務付けられており、高コストの要因となっている。
- 電子証明書がPF事業者の設備外に送信できないことから、署名の事実を署名者や第三者が検証したり、タイムスタンプ認証局が長期署名を付したりすることができない。

コスト面の課題	**サービス利用都度の当人認証はコスト許容性が極めて低い**	初回利用時の身元確認と異なり、サービス利用都度の認証においてトランザクションごとに数十円～数百円のコストは一般的に許容されない。
	電子証明書保管コストの課題	署名検証のみならず、電子証明書を保管するための設備の運営維持および監査に少なくないコストがかかっている。
	永久保管のコスト	犯収法に対応した本人確認を行った場合、証跡データは契約完了後7年間の保存が義務付けられているが、多くの事業者にとって事実上の永久保管義務となっている。永久保管を前提とした委託業務には事業継続性のリスクもコストとして織り込む必要がある。
	ベンダーロックインの課題	電子証明書を含む証跡データの保存先が法で規制されていることから、PF事業者の乗換えは容易ではなく、ベンダーロックインや価格競争阻害の要因になっている。
電子署名文書流通の課題	**署名文書の真正性を直接に検証できるのは認定事業者のみ**	電子証明書が認定事業者の設備外に送信できないことは、当該認定事業者でなければ署名文書の真正性を直接に検証ができないことを意味する。署名者本人であっても、認定設備内の署名データを確認することはできない。
	長期署名の課題	認定設備外への電子証明書の送信規制が、契約事実を長期にわたって証明する必要がある場合に必要なタイムスタンプ事業者による追加署名を行う際の課題となっている。
	複数（三者以上）者間署名の課題	契約当事者が3者以上となるケースでは、署名文書を流通させることができなくなる。

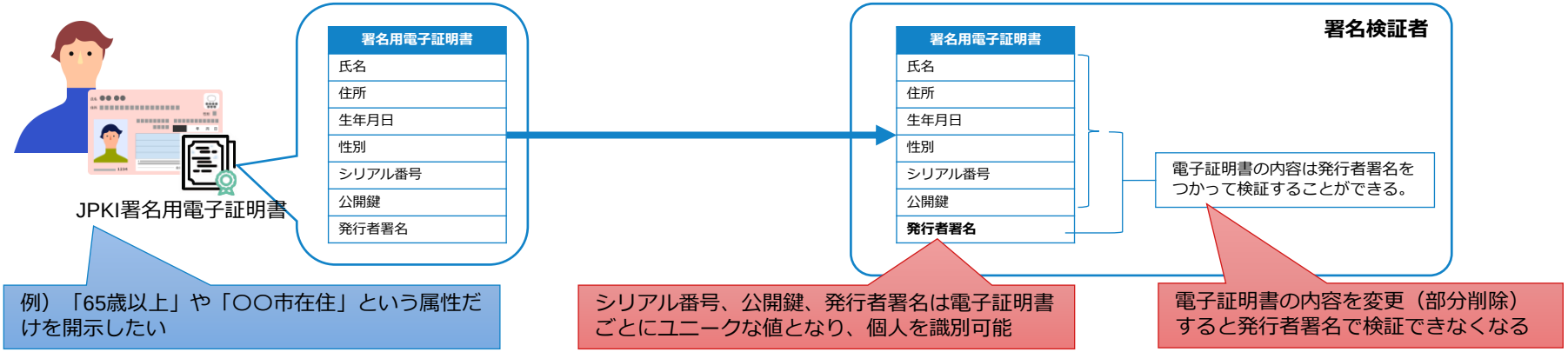
認証を信頼できる第三者に依存することの課題

IDの発行や認証を行うIDプロバイダ（IdP）として、J-LISやPF事業者等の「信頼できる第三者（Trusted Third Party / TTP）」に依存することは、コストや利便性の面でメリットがあるものの、プライバシーの侵害や市場寡占による弊害を招きやすいといった課題がある。

プライバシーや公平性の課題	**IdP (TTP)によるトラッキング可能性**	サービスが利用される都度IdPへ問い合わせを行うことから、IdP側ではユーザー個人がどのサービスをどの程度の頻度で利用しているのかをトラッキングできる。
	IdP (TTP)による利益誘導	IdPの運営主体が、異なるサービスを運営していた場合、自社サービスへの誘導や利用者の囲い込みに利用される場合がある。
	IdP (TTP)による情報管理のリスク	IdP内で個人情報が適切に管理されているとは限らず、またそれを利用者が認知できない恐れがある。規約への一方的な同意が求められたり、利用者がその内容を十分に理解できない場合もある。
寡占による課題	**単一障害点の課題**	サービスが一つのIdPに依存していると、IdPが障害により可用性を失ったり、IdPそのものが廃止されたり、また、IdP側の一存で遮断や排除がなされると、サービス利用者には甚大な影響が及ぶ。
	イノベーションや競争の阻害	利用者の選択肢が減り、潜在的な問題が改善されなかったり、イノベーションを阻害する要因になる。

属性情報開示のコントロールに関する課題

プライバシーを保護するためには、不必要な情報を秘匿しつつ、本当に必要な情報のみを選択的に開示することが望ましいが、現状のマイナンバーカードでは信頼できる第三者を仲介させない限り、情報を選択的に開示することは難しい。



x.509電子証明書に関する課題	**現状の電子証明書では選択的開示ができない**	JPKI署名用電子証明書には基本4情報に加えてシリアル番号が含まれているが、住所のみや生年のみ等、これらの属性情報を選択的に開示することはできない。 シリアル値や電子証明書を法令で保護しても、基本4情報で名寄せが行われる可能性がある。
	電子証明書による個人識別の課題	電子証明書には公開鍵や発行者署名など、個人を識別できるユニークな値を含まざるを得ない。ゼロ知識証明等の技術を用いない限り、現状の電子証明書を受け手が検証するモデルでは、匿名性と検証可能性を両立しながら属性情報を選択的に開示することはできない。
IdPを仲介した際の課題	**TTPに依存することの課題**	属性情報の開示先であるSP事業者との間に、PF事業者やデジタルID事業者等を信頼できる第三者（TTP）として仲介させることで開示情報をコントロールすることは可能であるが、TTPに自身の情報を開示せざるを得ず、前述のTTPに依存することの課題がある。

課題のまとめ

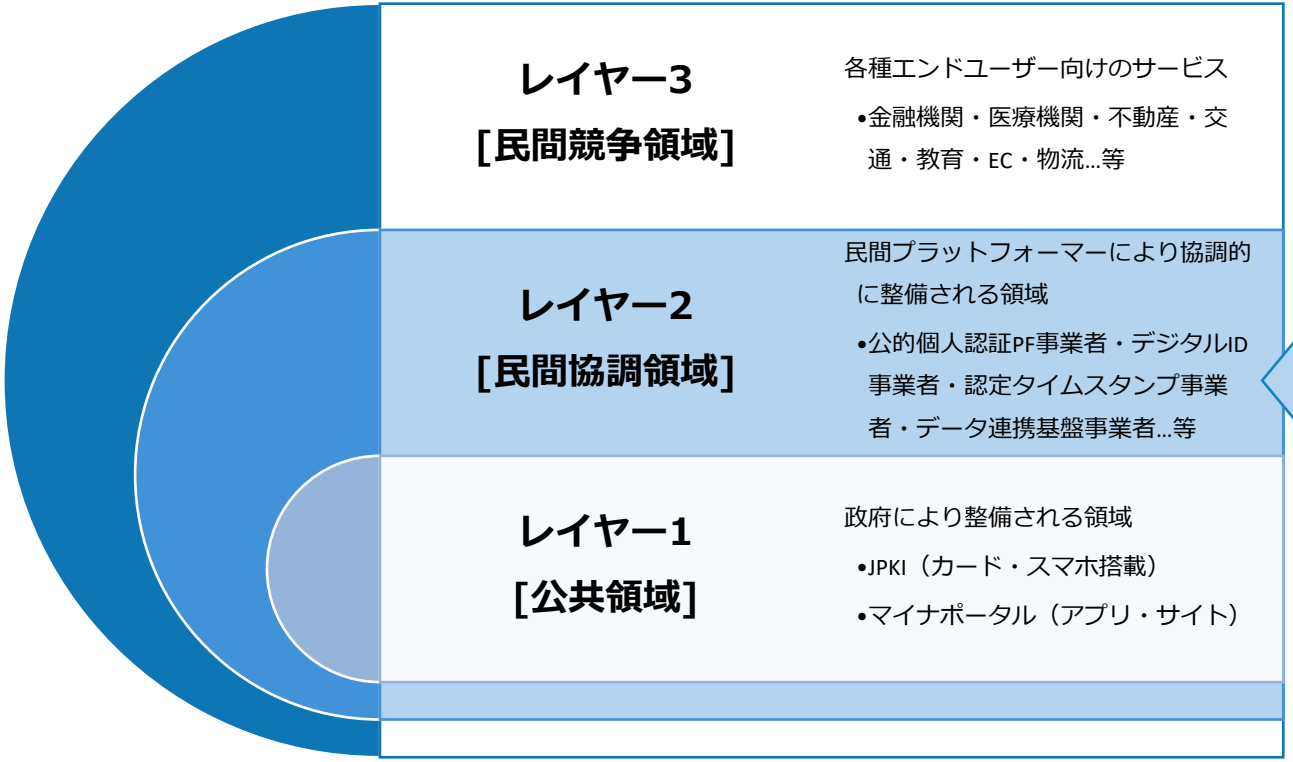
- 現行のマイナンバーカード／JPKIは、PF事業者を信頼できる第三者（TTP）として想定。電子証明書の取り扱いを法令でPF事業者に限定して規制し、主務省庁が監査を行うことで、TTPであるPF事業者の信頼性を担保している。

- 一方で、プライバシーをTTPと法規制に依存して保護するのは**高コスト**であり、**寡占による情報管理等の課題**も多い。**分散型IDやゼロ知識証明などの技術を活用し、低コスト・オープンかつ安全性の高い次世代型ID基盤の整備**が求められる。

4章　アーキテクチャ設計によるゴール・目的の明確化

民間協調領域を中心としたアーキテクチャ設計

官民の事業領域の間に民間協調領域を加えた3層のレイヤーを想定し、レイヤー２を中心とした全体最適アーキテクチャの設計を行う



ガバナンス
- JPKI民間利活用にむけたガイドライン策定
- アシュアランスレベルの民間認定制度

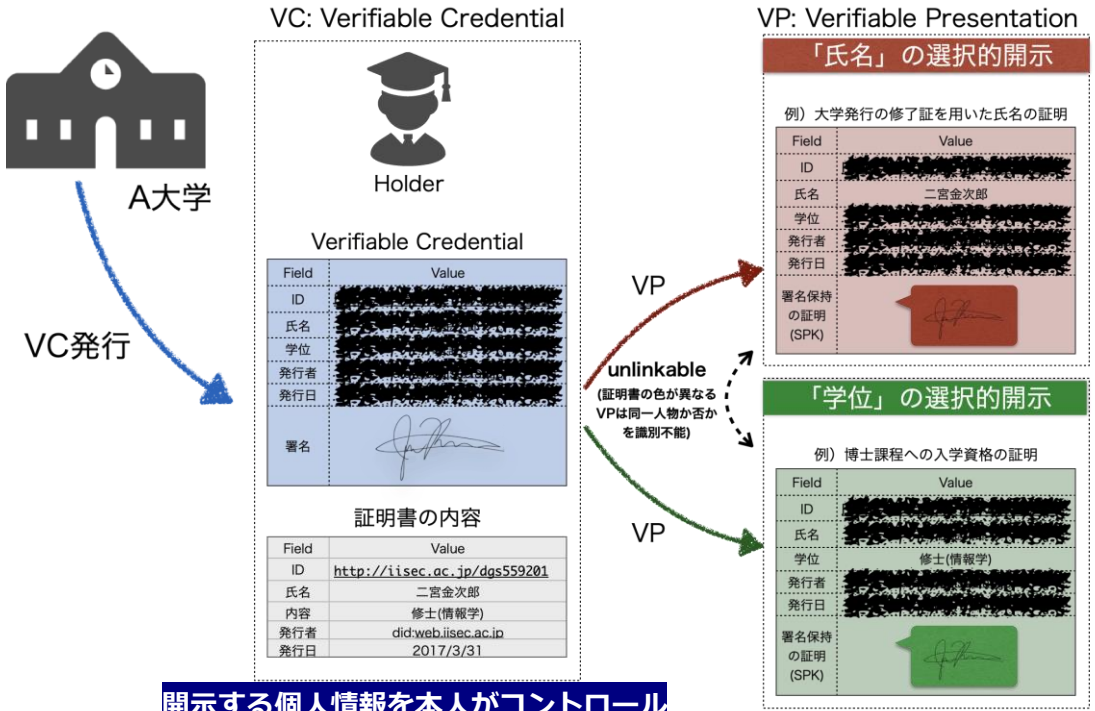
技術実装
- VC/DID技術による自己主権型デジタルIDの技術開発・社会実装

国際標準化
- 国際動向の調査、標準化における貢献

目指すべき　次世代型ID基盤（自己主権型アイデンティティ）

本プロジェクトでは、プライバシー侵害のリスクを排除しながら、パーソナルデータの高度利活用を行う『自己主権型アイデンティティ』の民間ID適用の社会実装を目指す。

※参考解説　佐古和恵「分散型デジタルアイデンティティとは？～概念、仕組み、実現に資する技術と課題～」
日本銀行金融研究所ディスカッションペーパー：https://www.imes.boj.or.jp/research/abstracts/japanese/23-J-08.html



開示する個人情報を本人がコントロール

ショッピングサイトでの口座開設

B大学院入試

Digital Architecture Design Center

国際標準化動向調査

欧州でもeIDAS規則が改正され、eIDAS2.0がDigital ID Walletという名称でスマートフォンに拡張され、スマホJPKIと同じ機能のデジタル署名基盤の標準化が進みつつあり、相互運用性の確保が喫緊の課題。

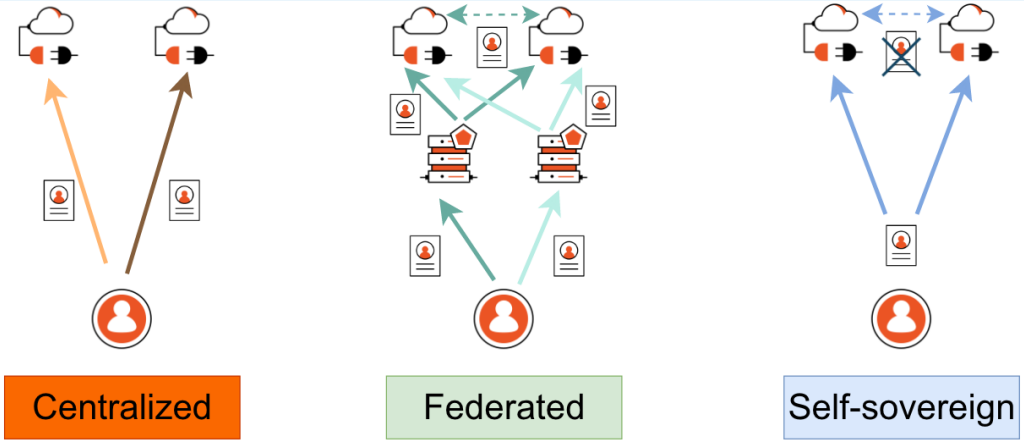
●Digital ID Wallet

ISO/IEC 23220で進んでいる国際規格とJPKIの相違を詳細なレベルで確認する必要がある．さらに、今後の方向性として以下の論点がある。

・論点1
ID Walletのディストリビューテッドモデルをフランスとドイツが中心となってSC17で進めており、日本は独仏に追従すれば良いか？
(Distributed= Federated ∪ SSI?)

・論点2
OpenID ConnectとW3C Verifiable Credentialsの2方式が有力視されており、日本の立ち位置を見極める必要がある。

参考) Sharif, A. *et al.* The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. *Applied Sciences* 12, 12679 (2022).



Centralized Identities： 管理者などのエンティティが、システムレベル（アクティブディレクトリなど）の集中型アイデンティティを管理する。その結果、ユーザーのアイデンティティはこれらのエンティティによって決定され、エンティティを通じてのみ削除することができます。集中管理されたエンティティへの依存は、しばしば相互運用性の欠如につながる。その主な理由は、ユーザーのIDをそのまま転送することができず、別のサービスプロバイダーのために再作成しなければならないためである；
Federated Identities：中央ログインソリューション（IdP）を提供することで、単一の権威に基づく階層を破壊することを目的とし、ユーザーはIdPに登録された1つのクレデンシャルのみを使用して、異なるSPでアイデンティティを共有できるようにする。このソリューションは、シングルサインオンの体験と相互運用性を提供することで、パスワード疲労の問題を解決することができますが、それでも、複数のSP間でユーザーを追跡する問題は未解決のままです。実際、IdPが多数のSPから情報を集約してユーザープロファイルを作成することは可能であり、これはいくつかのプライバシー問題を引き起こす可能性がある[68]；
自己主権型 ID：デジタル ID 管理の次の最も新しい段階であり、ユーザに自分自身のデータの制御を取り戻すことによって、前のモデルのプライバシー問題を解決することを目的としている。主なアイデアは、制御をネットワークの中心からネットワークの端に移し、直接的な相互作用を可能にすることである[69]。

ISO/IEC JT1/SC 17/WG 4との連携の必要性

ISO/IEC JTC1は、ISO(国際標準化機構)とIEC(国際電気標準会議)合同の技術委員会であり、SC17（Sub Committee）は、カードおよび個人識別に関する標準化を担当する副委員会である。うちWG4は「端子付きICカード」について標準化を行っているグループで、ISO23220をはじめ、eIDについて議論されている。

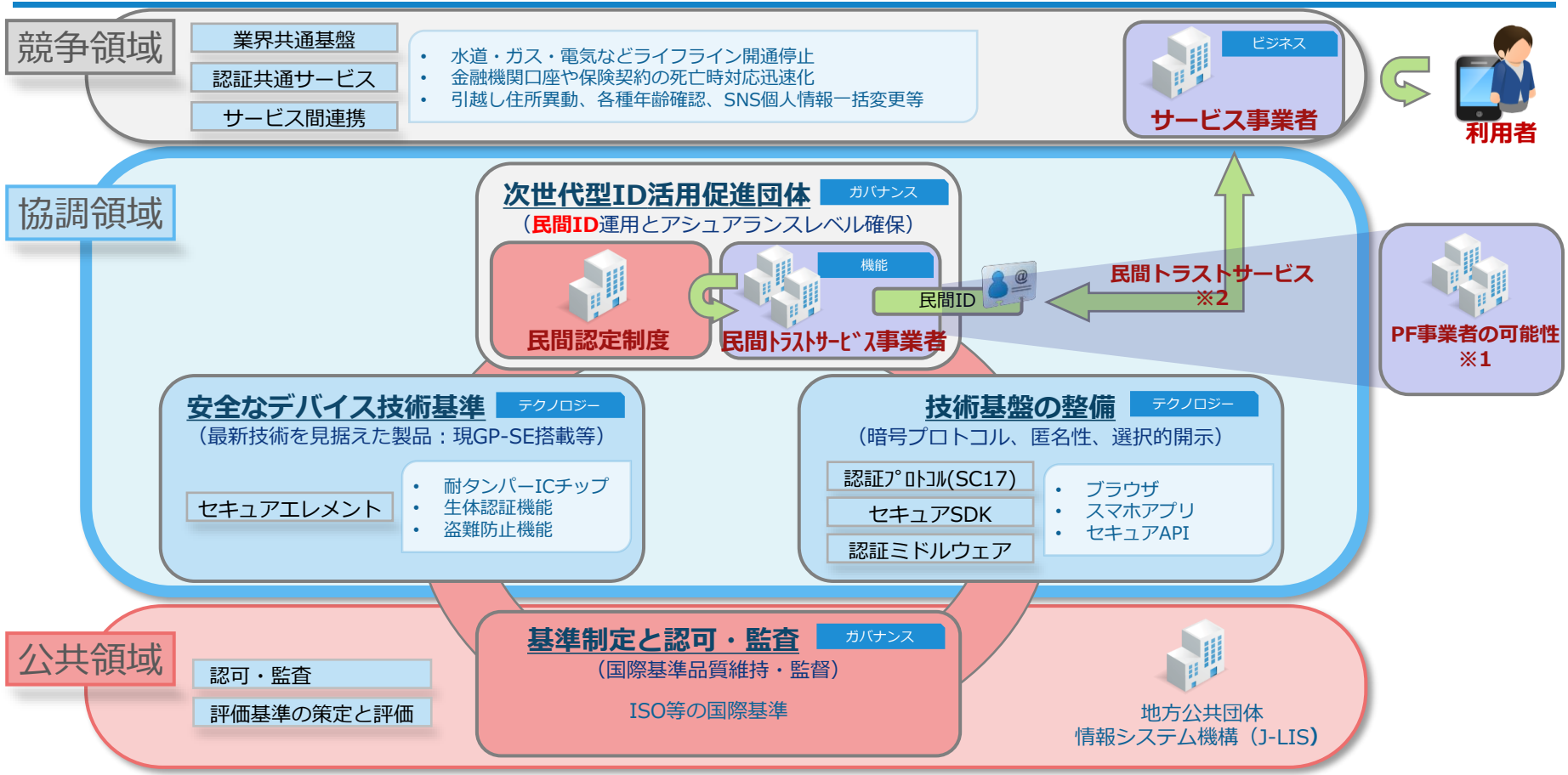
- 7月のWG4へオブザーバ参加した際に、ISO23220シリーズについての議論がされていた。ISO23220は、各国の政府や民間等の発行機関が発行するモバイル身分証明書（モバイルeID）の相互運用を可能にすることを目的とした規定群である。23220-1（part1）については2023年初頭にリリースされているが、part2以降はドラフトの段階であり、この内容を知ることおよび貢献できるポイントを探すことは本活動としても有意義である
- 注目すべきは我々のラボ活動でもテーマとしているVerifiable Credentialであったり、eIDとプライバシーの両立といった内容については重要なテーマととらえ集中的な議論が行われていることである。これは我々の議論の方向性が国際標準化動向と整合が取れていることでもあり、また相互にフィードバック可能であると考えた。
- 特に、第三者機関（公的機関）による生年月日や住所等の属性証明（claim）について、個人情報保護の観点から公開鍵証明書（credential）に検証可能な形式で秘匿して記載する方針が合意されているが、現時点では以下について連携できると考えている

  (1)ハッシュ方式のみが議論されており、我々が本格プロジェクトで提案する

  (2)ゼロ知識証明方式は先送りされており貢献の余地があることを確認した

※ ハッシュ方式は，ハッシュ関数を利用した選択的開示方式であり、ゼロ知識証明方式は「開示した属性がIdPより署名を受けている」ことをゼロ知識証明により示す選択的開示方式である。
ただし、ハッシュ方式は複数の選択的開示が連結可能であるため、集約して個人情報を復元できるリスクがある一方、ゼロ知識証明方式は連結不能性が達成されており、複数のSP事業者に選択的開示した属性を集約できないことが技術的に保証されるため、高度な自己主権性を達成するより優れた方式である。

JPKIをトラストアンカーとした次世代型ID基盤 そのために必要な協調領域



※1 PF事業者の可能性：民間トラストサービス事業者はPF事業者相当の統制・実務・設備・監査要件が求められると想定され現PF事業者の参入協力が期待される。
※2 民間トラストサービス：事例としてのサービスは、VC発行、民間証明書発行、電子契約、法人証明、タイムスタンプなど。

5章　ステークホルダーの分析・特定

（1）着目するユースケース
（2）ヒアリング調査

（1）着目するユースケース

デジタルIDのライフサイクル

時　　間　　軸

Reference: ISO/IEC 15288 Life Cycle Definition

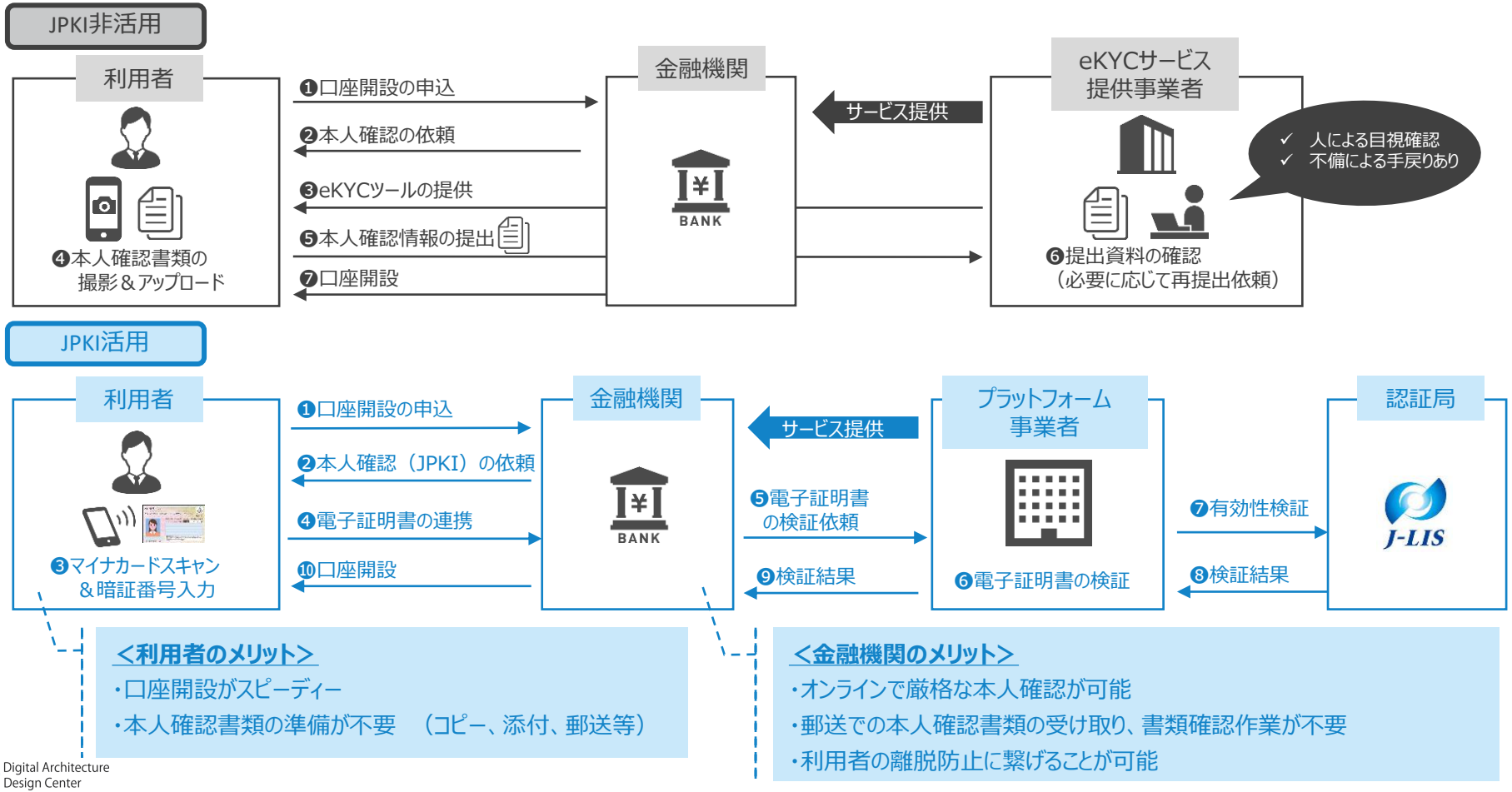
Concept Stage	Development Stage	Production Stage	Utilization Stage	Retirement Stage
			Support Stage	

主務大臣認定プロセス	デジタルID活用プロセス	廃棄プロセス
	①銀行口座開設のユースケース ★JPKI活用の場合 ★JPKI非活用の場合（現状eKYC) ②引越しワンストップサービス ★官民協調を目指した先進取り組み	

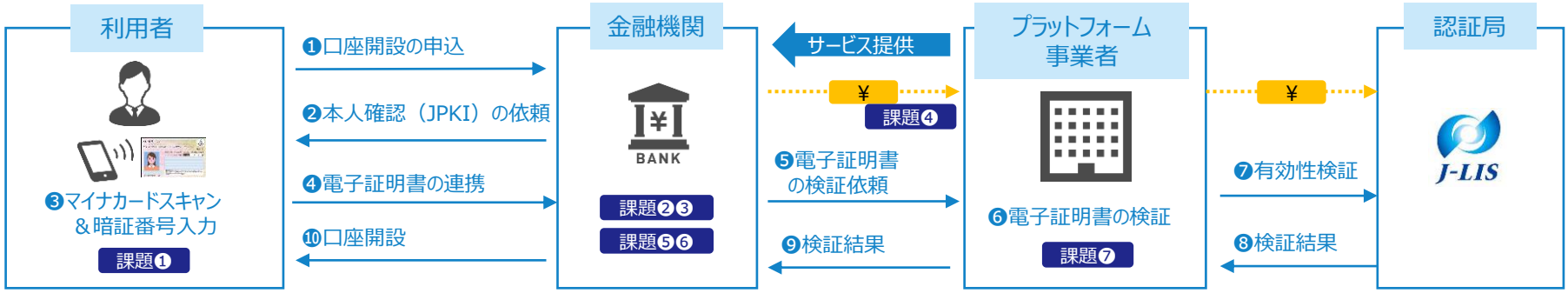
意味軸

（1）身元確認
（2）当人確認
（3）識　　別　⇒（属性証明）
（4）電子署名

パーソナルデジタルID活用プロセス例（金融機関における口座開設ユースケース）



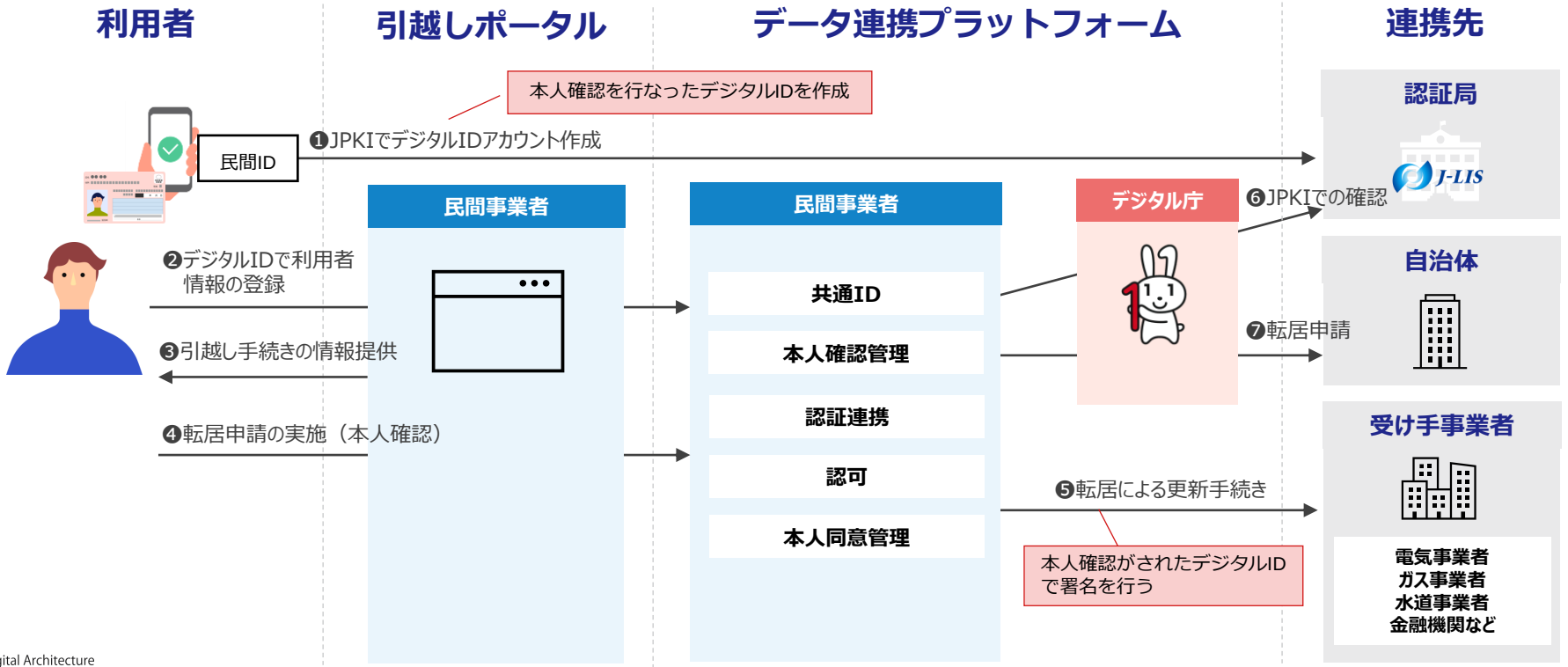
JPKI利用時の課題（金融機関における口座開設ユースケース）



課題No	分類１	分類２	課題概要
❶	利用者	UX	マイナンバーカード所持とパスワード記憶が必須
❷	金融機関	顧客獲得	マイナンバーカード未所持者もいるため、JPKI以外の本人確認手法も残す必要あり
❸		業務	既存の本人確認手法による業務も残しつつ、JPKIの新たな業務を追加する必要あり
❹		コスト	・署名用電子証明書の利用（本人確認）はトランザクションが少なく、コストの影響はないが、 利用者証明用電子証明書の利用（ログイン）はトランザクションが多くなり、コスト増となる
❺		導入準備	・フロント（モバイル側）にカード読み取り機能を実装する必要がある 既存eKYCの方法に応じて対応方法を変える必要あり（ブラウザorアプリ）
❻		導入検討	・JPKIは機能としては完全ではなく（スマホ化など）、導入時期を静観している状況
❼	PF事業者	提供	・金融機関側の採用観点でもある、サービスレベルの情報が少ない

パーソナルデジタルID活用プロセス例（官民協調を目指した先進取組 引越しワンストップサービス）

民間事業者が運営する「引越しポータル」を通じ住民が転居情報を自治体や民間事業者に提供することで、引越し手続きの一元化を実現します。



パーソナルデジタルIDの4つの機能（意味軸）とユースケース（再掲）

パーソナルデジタルIDが用いられるユースケースは、以下の4つに分類される。

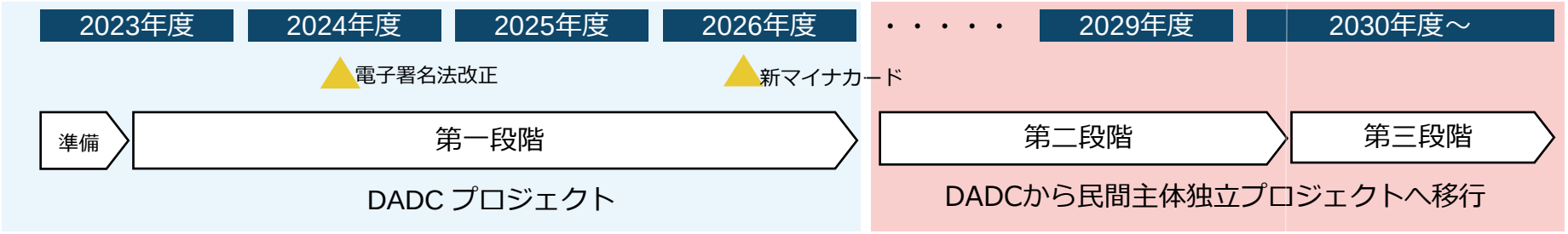
機能	例	目的
身元確認 （初回本人確認）	• 金融機関口座開設時の本人確認 • 携帯電話契約時の本人確認 • アカウント開設時の初期登録	• 当該ユーザーが実在することを確認する • 当該ユーザーの身元情報（本人特定事項・基本4情報など）を取得し、その正確性を確認する • 当該ユーザーを重複なく、唯一の自然人に帰着させ、事業者の台帳に登録する
当人認証 （ログイン認証）	• ネットサービスへのログイン • コンビニ端末での住民票請求 • クレジットカードによる決済	• 操作者と事業者の台帳記載の情報を確実に対応付ける • 操作者が、まちがいなく期待される当人であることを確認する
電子署名 （電子契約）	• 電子契約への署名 • 住宅ローンの申込 • 携帯電話回線の契約 • 不動産売買契約	• 署名文書が、署名者の意思に基づいて作成されたことを検証可能な形式で証明する • 署名文書が、改ざんされていないことを検証可能な形式で証明する
リンクの制限 （意図しない名寄せの抑止）	• サービスごとに異なる識別子を発行 • 保険証提示の際の被保険者番号黒塗り	• ユーザーの意図しないトラッキングやプロファイリング（パーソナルデータの目的外利用）を防ぐ

主なステークホルダー

レイヤ	ステークホルダー	実施
公共	官庁	● デジタル庁　デジタル社会形成の司令塔（マイナンバー含む） ● 関連省庁　総務省、金融庁、厚労省、他
	地方公共団体情報システム機構（J-LIS）	● 公的個人認証法（電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律）に基づく認証局として、署名用電子証明書及び利用者証明用電子証明書の発行及び失効並びに失効情報の作成等に係る認証事務を担当している
民間	主務大臣認定事業者（PF事業者）	● 主務大臣認定（以下、本認定）により、マイナンバーカードに格納された電子証明書（署名用電子証明書および利用者証明用電子証明書）を用いて電子署名等を行う「公的個人認証サービス」に伴う署名検証業務を行う事業者
	SP事業者	● 公的個人認証サービスの利用にあたり、自社で署名検証設備を整備せず、電子証明書の有効性確認をPF事業者に委託することでサービス提供する事業者をサービスプロバイダー事業者
	SI事業者	● 公的個人認証サービスを利用したサービスを地方自治体や民間企業向けに提供する事業者 ● SI事業者自身が、SP事業者の資格を有することもある
	民間事業者	● 金融機関など、公的個人認証サービスを利用したサービスを顧客に提供する事業者 ● 民間事業者自身がが、SP事業者の資格を有することもある

6章　今後のアクションプラン

あるべき姿実現までのステップ

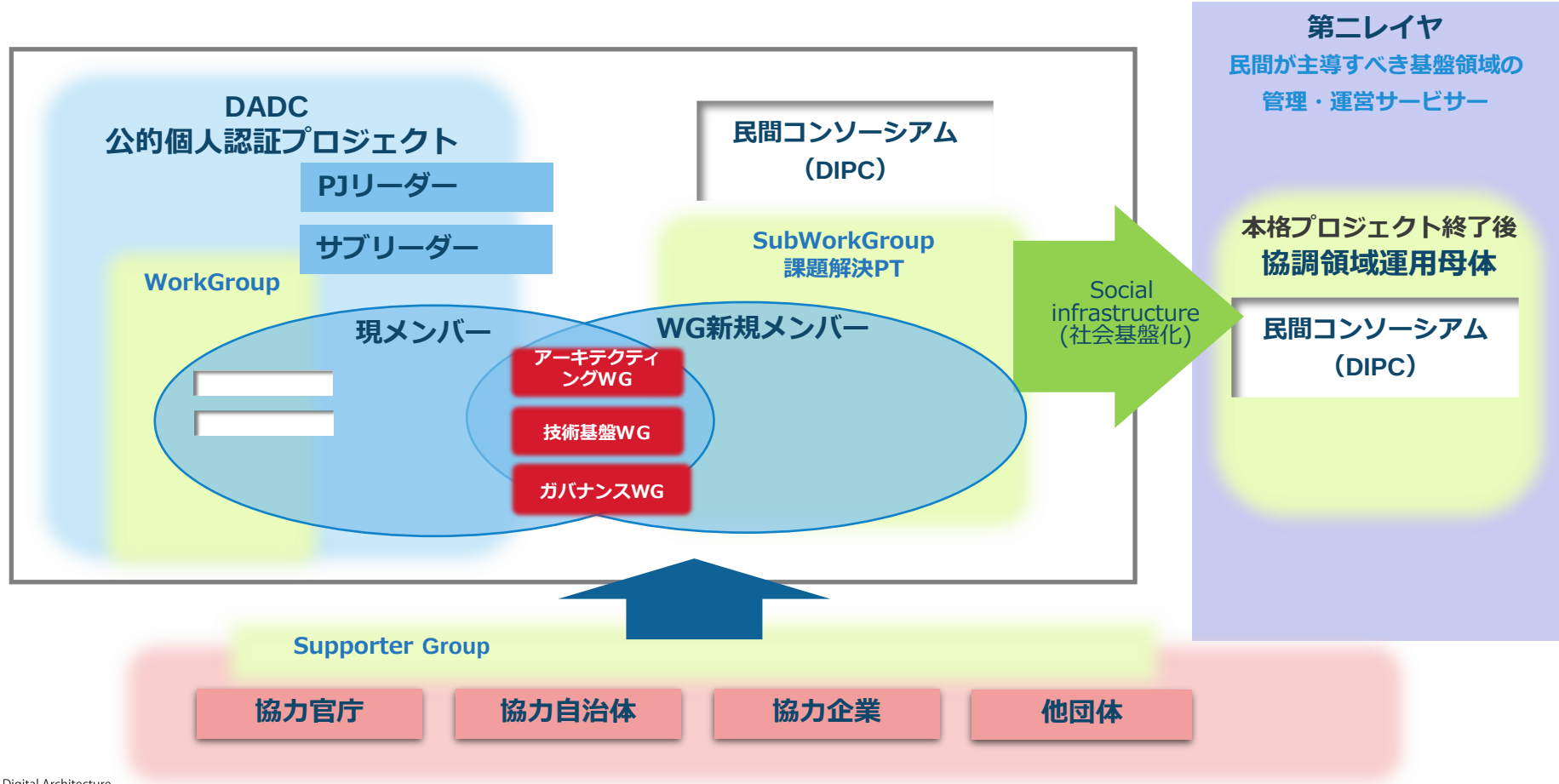


▲グローバル展開

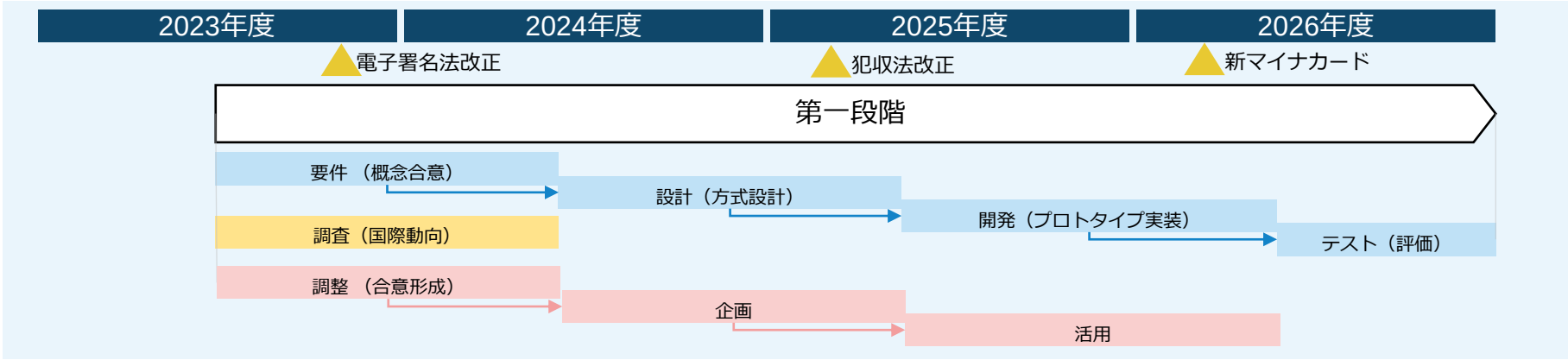
▲国際標準化団体加盟（SC17）　▲次世代型ID基盤　▲東南アジア諸国との連携　▲欧州との相互運用性確保

フェーズ	基盤（協調領域）整備	実証（競争領域スタート）	Society5.0実現
アーキテクティングWG	• 全体最適アーキテクチャ設計		国際ビジネス進展
技術基盤WG	• 全体最適アーキテクチャ設計 • 技術基盤整備 • 匿名クレデンシャル&選択的開示機能	• 次世代型ID基盤（自己主権型アイデンティティ）の普及促進 • 官民データ連携基盤におけるパーソナルデータの安全かつ有効な社会実装（出生、就学、結婚、引越、事故、病気、介護、死亡等）	• 次世代型ID基盤の本格グローバル展開
ガバナンスWG	• 次世代型ID基盤の制度設計 1. 民間ID活用ガイドラインの策定 2. アシュアランスレベル民間認定制度		

体制計画


DADC
公的個人認証プロジェクト
PJリーダー
サブリーダー
WorkGroup
現メンバー
WG新規メンバー
民間コンソーシアム
（DIPC）
SubWorkGroup
課題解決PT
アーキテクティングWG
技術基盤WG
ガバナンスWG
Social infrastructure (社会基盤化)
第二レイヤ
民間が主導すべき基盤領域の
管理・運営サービサー
本格プロジェクト終了後
協調領域運用母体
民間コンソーシアム
（DIPC）
Supporter Group
協力官庁
協力自治体
協力企業
他団体

DADCプロジェクトロードマップ（案）



アーキテクティングWG

- 全体最適アーキテクチャ設計（全工程）

技術基盤WG

- 要件（目標設定・概念合意・要件定義）
  - 想定期間：10ヶ月
- 調査（国際動向調査と要件フィードバック）
  - 想定期間：10ヶ月
- 設計（方式設計）
  - 匿名クレデンシャル・選択的開示機能
  - 想定期間：6～12ヶ月
- 開発（プロトタイプ実装）
  - 技術仕様書
  - 想定期間：12ヶ月
- テスト（評価）
  - 想定期間：6ヶ月

ガバナンスWG

- 調整（合意形成）
  - ヒアリング実施
  - 想定期間：10ヶ月
- 企画
  - 民間IDアシュアランスレベルを認定する民間制度の企画書やガイドライン
  - 想定期間：6～12ヶ月
- 活用
  - 匿名クレデンシャル・民間IDの活用ガイドライン
  - 想定期間：12ヶ月

DADCプロジェクト活動の想定成果物（案）

アーキテクティングWG　技術基盤WG

- 匿名クレデンシャル&選択的開示機能の技術基盤整備
  - 調査レポート
    - 国際標準化動向の調査と相互運用性　検討・企画
  - 技術仕様書
    - 技術仕様の検討・企画
  - 基盤整備事業（予算化、体制構築、実施）

ガバナンスWG

- 民間IDアシュアランスレベルを認定する民間制度の企画書
  - 認定基準の設定、認定機関の設定、認定制度の権威付け
- 匿名クレデンシャル・民間IDの活用ガイドライン（金融機関、Sier、キャリア）
  - 本人確認手段としての匿名クレデンシャル・民間ID活用ユースケース企画・促進

参考）実施施策2（案）

■ 第二段階（2027年度～2029年度）

- 民間IDによる匿名クレデンシャル&選択的開示機能による、次世代民間ID基盤（自己主権型）の普及促進
  - ➢ 民間の競争による技術開発を後押し
    - 民間主体の自己主権型アイデンティティの範囲、制度、規定などの整備
    - 普及策の検討・企画

- ワーキンググループの拡張（金融保険、Sier、キャリア、医療他）
  - ➢ 官民データ連携基盤におけるパーソナルデータの安全かつ有効な社会実装（出生、就学、結婚、引越、事故、病気、介護、死亡等）

デジタルアーキテクチャデザインセンター
https://www.ipa.go.jp/dadc