公的個人認証サービスと海外ｅＩＤの相互利用環境に係る調査研究

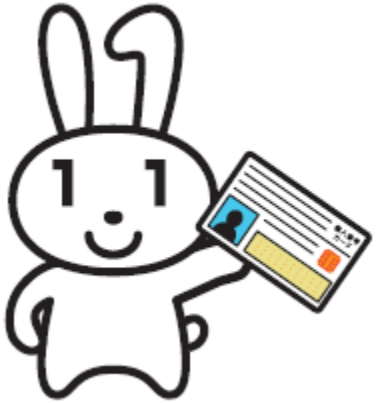
東京工業大学　科学技術創成研究院

小尾高史

一般財団法人 ニューメディア開発協会

KEIRIN 競輪の補助事業

みなさん
マイナンバーカード
お持ちですか？



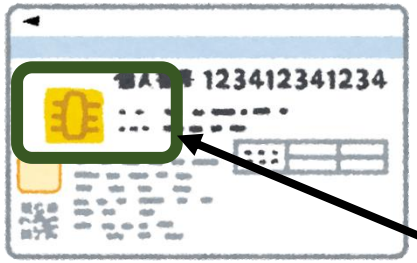
この犬は？

マイナンバーカード

発行	市区町村 （地方公共団体情報システム機構（J-LIS)による一括発行）
券面	顔写真、基本４情報は必須、個人番号を裏面に記載
交付手数料	無料
有効期限	10回目の誕生日まで（20歳未満は5年）
交付枚数	約5815万枚 (人口の約45.9%）(2022年7月現在）
ICチップ搭載AP	公的個人認証AP（JPKI-AP)、券面AP、券面入力補助AP、住基AP

電子空間での本人確認

- 電子空間（インターネットなど）では、オンラインで利用者を確認する方法が必要
  - マイナンバーカードは、電子空間での公的身分証明書？



PCの前に座っているのは犬？

オリジナルのイラストは
On the Internet, nobody knows you're a dog,
Peter Steiner,
The New Yorker 1993

- 電子空間での身分証明書は、チップの中に
  - マイナンバーカードは入れ物
  - 電子空間での公的身分証明書は、公的個人認証サービス（JPKI）
  - マイナンバーは使っていません

JPKIのキャラクター
マイキーくん

公的個人認証サービス

- **公的個人認証サービス**
  （The Public Certification Service for Individuals, JPKI）
  - 2004年1月29日より提供開始（開始時は電子署名のみ）
  - インターネットを通じて安全・確実な行政手続き等を行うために、他人によるなりすまし申請や電子データが通信途中で改ざんされていないことを確認するために必要な機能を提供
  - 個人番号制度の導入（整備法）により、2016年1月より「利用者証明（いわゆる電子認証）」の仕組みを導入
  - 主務大臣が認定した民間事業者も証明書の有効性確認を実施可能（2022年8月現在民間事業者160社(大臣認定事業者18社、同事業者を利用している事業者142社)）

JPKIのキャラクター　マイキーくん

利用者証明（電子認証）

- ネットワーク等を介して、サービス提供側が、サービス利用者を認証する仕組み
- 利用者証明は、マイナポータルへログインするために利用されることとなるが、実際の利用範囲は、従来の電子署名と同様であり、公的機関等であれば従来と同様に利用可能
- 電子署名用証明書には４情報が記載（情報の変更があると失効）されるが、利用者用証明書には個人情報の記載はなし（証明書のシリアル番号で管理）
- 電子署名用証明書のシリアルと利用者用証明書のシリアルの紐づけ情報は、J-LISから入手することが可能
- コンビニでの住民票の写し、保険資格確認、印鑑登録証明書等の交付に利用
- PINの入力なしで利用する仕組みを用意（特定利用者証明）

eIDとは

- Electronic identification (eID) （電子的本人確認）は、電子的に住民の身元を保証するための仕組み
- eIDは、様々な情報へアクセスするための鍵として利用
- EUを含む様々な国で、公的なeIDカード及びeIDを発行
- マイナンバーカードは、eIDカード、JPKI（利用者証明）は、eID
- EUでは、
  - 2016年7月施行の“Regulation on electronic identification and trust services for electronic transactions in the internal market（eIDAS規制）”により、域内での共通的なeIDフレームワーク確立を目指す
  - eIDASに準拠するeIDの相互承認制度を導入
  - 2018年9月以降は、Substantial及びHighレベル（3段階の中、高）のLoAを要求する公共サービスでは、原則、他国のeIDを受け入れ

eIDの保証レベル（EUの例）

保証レベル	
Low（低）	本人確認書類での本人確認、対面での本人確認を実施。 なりすまし、盗聴、リプレイ攻撃、改ざんに耐性を持つ認証方法を利用。 （例：施設予約サイトなどへログインするためのID、パスワード）
Substantial （中）	上記の要件に加えて 真正であることが確認された本人確認書類により本人確認を実施 （但し、対面での本人確認は行わない）。 動的認証、2つ以上の要素（知識、所有物、生体情報）を利用した多要素認証を利用。 （例：運転免許証を用いてネット上で本人確認を行い発行されたオンライン バンキング用のID、パスワードに加えてログイン時にはSMSによるワン タイムパスワードを利用）
High（高）	上記の要件に加えて 有効な本人確認書類を用いた対面での本人確認が実施。 （もしくは、事前に対面での本人確認を行った認証手法による本人確認を実施） 複製や改ざんに対する**保護機能を有したデバイス**を利用 マイナンバーカード → 公的個人認証サービスはここに相当

公共手続きには、このレベルのeIDが必要

EU各国のeIDカード

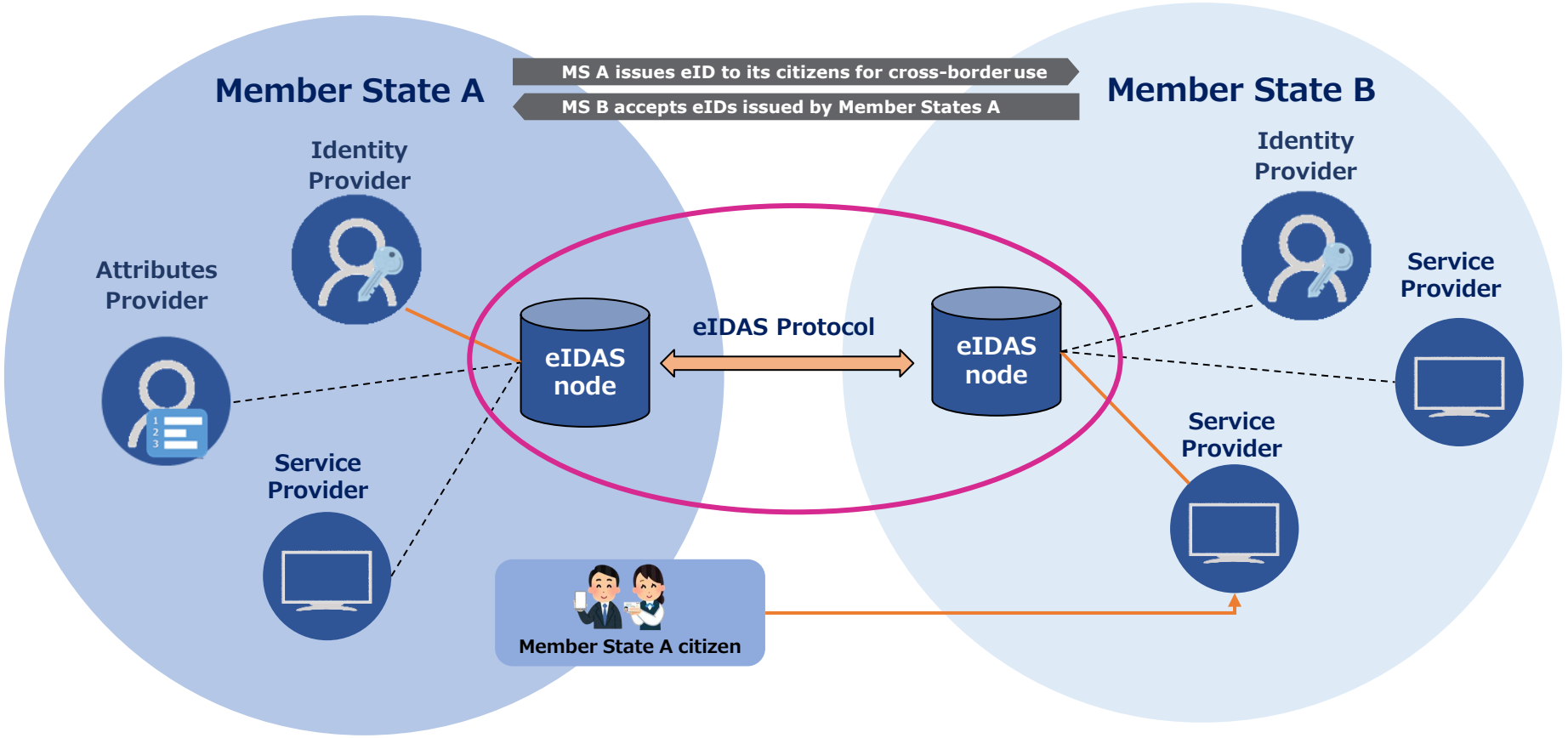
- EU各国のeIDカードは、EU圏内のパスポート（電子パスポートと同様の機能を搭載）
- EUの多くの国で所持・携帯義務有り
- 申請時もしくは受け取り時の対面での本人確認は必須
- カード発行手数料（10-30ユーロ程度）が必要
- 緊急発行スキーム（5営業日程度で発行）を持つ国が多い
- 未成年の有効期限は短く、一定年齢以上の住民のカード有効期限を長く設定することもある
- カード券面には、出生地の記載はあるが、必ずしも現住所の記載はない
- カード表面には、住民識別番号、カード番号等の記載がある
- チップ内には、生体情報（顔画像、指紋情報）が格納されるが、電子認証等での利用ではなく、オフラインでの本人確認時での利用
- 多くが電子認証（利用者証明）、電子署名を標準でサポート
- 証明書には、氏名を含む国が多い
- eIDAS準拠のeIDカードを用いたeIDの保証レベルは、high

NMDAのホームページにより詳細なデータがあります

EU内のeID相互運用への取り組み

- 2008年から2015年にかけて、Secure Identity Across Borders Linked (STORK, 2012年よりSTORK2.0)において、eIDの相互運用を推進
- eIDAS規則の発行により、STORKによる相互運用からeIDASの連携の下でのeID連携の仕組みに移行
- 2018年9月29日以降は、Substantial及びHighレベル（3段階の中、高）のLoAを要求する公共サービスにおいては、原則、他国のeIDを受け入れ
- eID連携には、eIDAS nodeを各国が用意。ベースとなるeIDAS nodeのソフトウエアは、Connecting Europe Facilityが開発し、無償公開
- eID導入国の多くはすでにeIDAS nodeの運用を開始

EU間でeID連携を行う仕組み



JPKIとEU eIDの相互運用

- JPKIは、EUのeIDASに準拠したeIDと同等の機能を有するため、EUとの相互運用性を確保できる可能性

→ **EUの取り組みを参考に、JPKIの海外（EU)との相互運用の可能性を調査・検討**

2020-2021年度

ニューメディア開発協会において

公的個人認証サービスと

海外eIDの相互利用環境に係る調査研究

を実施

調査の背景と目的

1. eIDAS規則を参考として、公的個人認証サービスが提供する利用者証明用機能（国内eID）とこれと同様な機能を有する海外eIDとの連携のための技術的な調査と比較検討を行い、相互利用の実現可能性を見極める
2. 国内eIDと海外eIDを相互利用するアプローチとして、デジタルチケットの実現を目標に、デジタルチケットの現状を調査し、各管理プロセス（予約、購入、譲渡等、および入場）における課題を抽出して、eID連携をフル活用した安全、便利、かつ確実な運用スキームを実現することを目指す

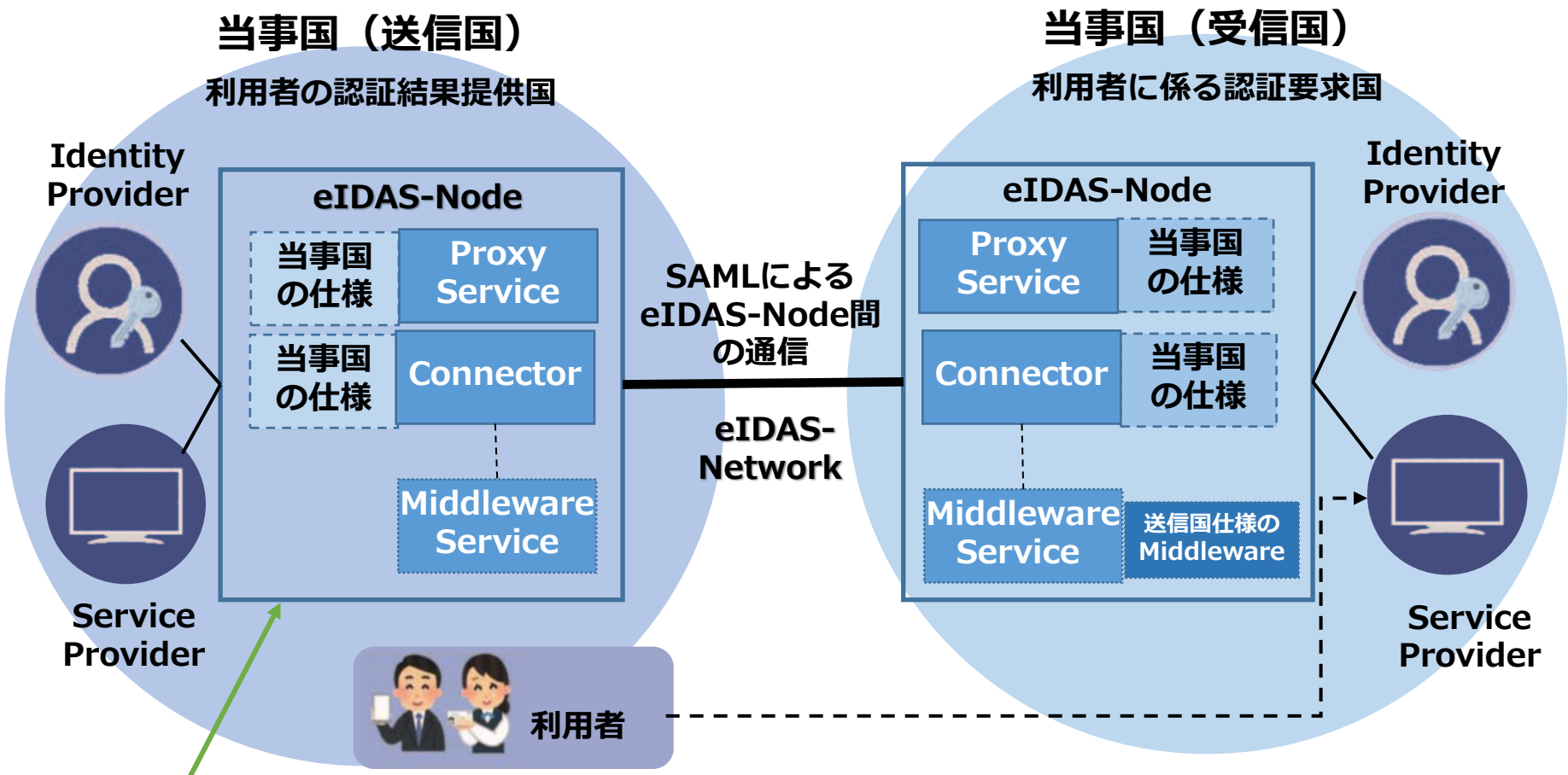
eID国際連携のユースケース例

- **外国人が日本のオンラインサービスを受ける例**
  - 日本で働いていた外国人が母国に戻ったのちにも、自国のeIDでマイナポータルへのログインを可能とし、日本居住時の情報を取得する
    - 日本での年金受給資格（10年間納付）を保持したまま母国へ戻った外国人が年金記録を確認
    - 薬剤情報、検診情報の確認
  - マイナンバーカード発行前に自国のeIDを利用して各種公的オンラインサービスを受ける
- **逆にＥＵ各国で提供されるオンラインサービスをマイナンバーカードを利用して受けることも**

eID国際連携のユースケース例

- **eID（JPKI）を使用したデジタルチケット**
  - 不正購入・不正転売を効率的に防止
  - 外国人によるチケット購入の容易化（海外携帯電話番号でSMS認証を利用できない場合あるが、eID利用により回避）
  - 不正入場の防止等（eIDによる入場の場合）
    - ✓電子的手段による本人確認の効率化
    - ✓テロ容疑者等、監視が必要な入場者の識別の容易化
- **日本人による外国金融機関及び外国人による国内金融機関のオンライン口座開設や、インターネットバンキング**

eIDAS-Nodeの構成要素

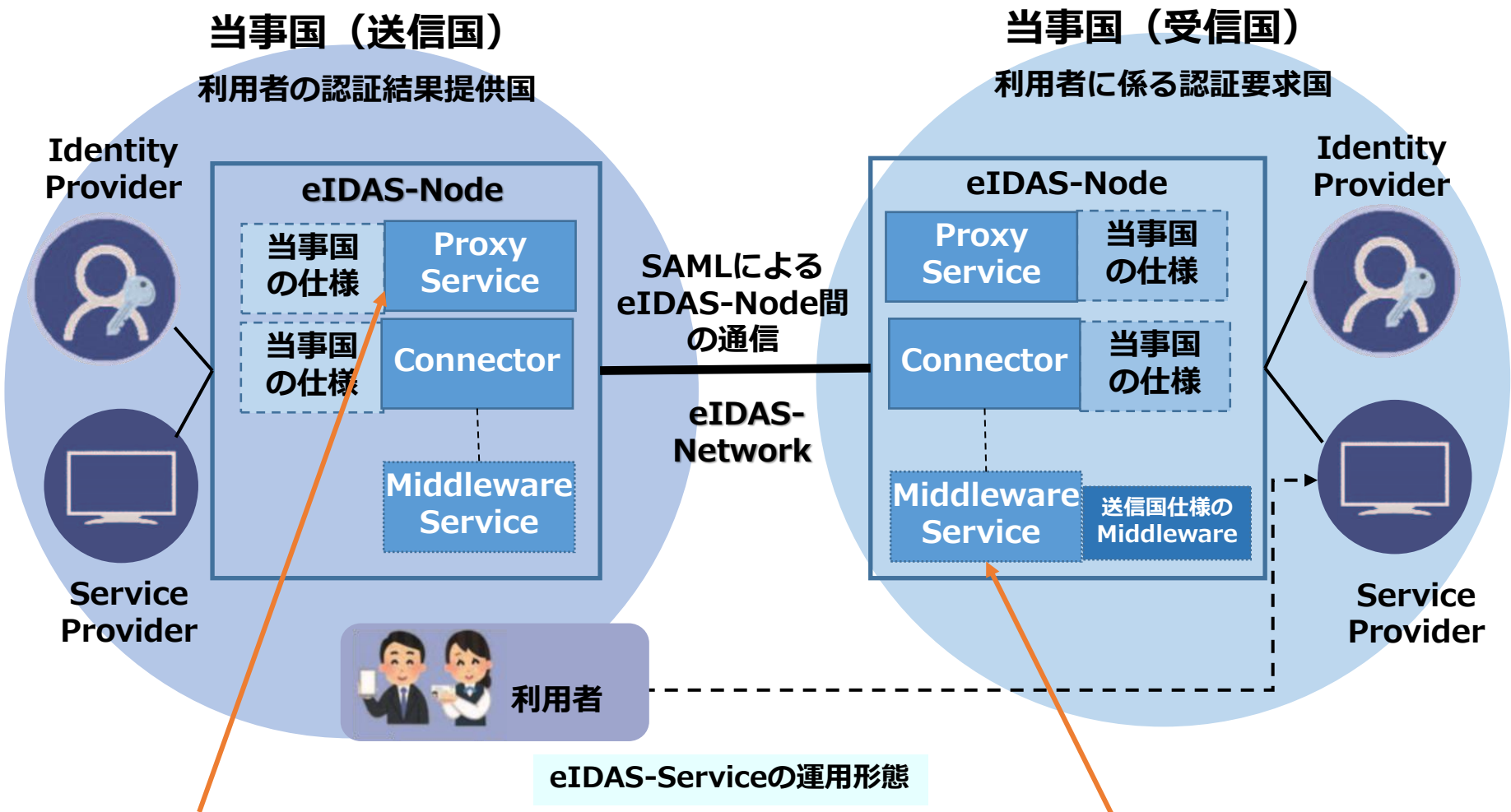


eIDAS-Node

EU加盟国間における越境認証を行うためにeIDAS準拠の技術仕様に基づき実装
eIDAS-Networkに繋がる他国のeIDAS-Nodeとの通信を行う枠組

- 越境認証を要求： eIDAS-Connector
- 越境認証の結果を提供： eIDAS-Service

eIDAS-Nodeの構成要素

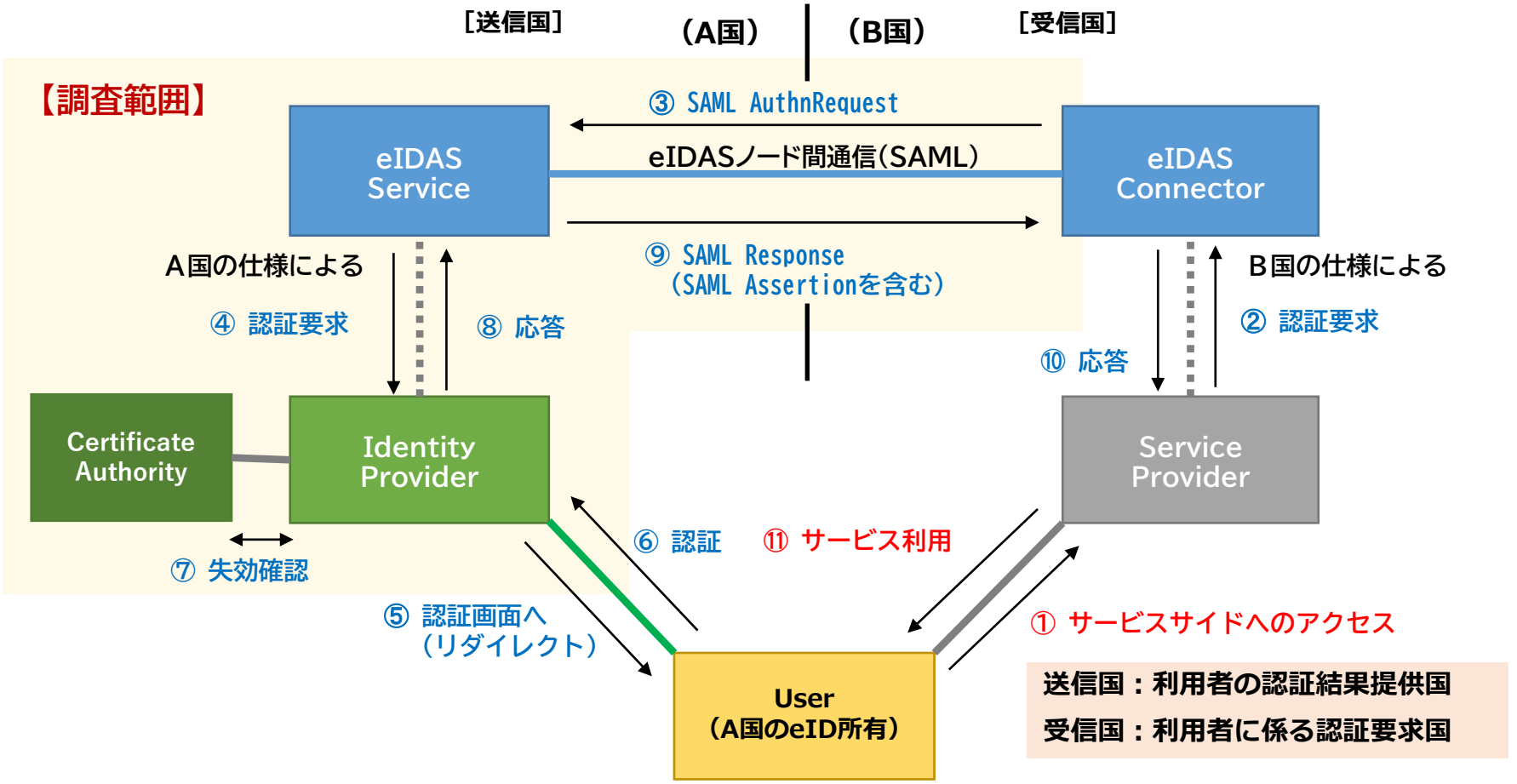


eIDAS-Serviceの運用形態

<Proxy-based> 【推奨形】
送信国がeIDAS-Proxy-Serviceを操作し、受信国のeIDAS-Connectorと送信国の電子識別スキームとの間の通信を中継する。

<Middleware-based>
受信国がeIDAS-Middleware-Serviceを操作して送信国から提供されたMiddlewareを実行することで、送信国の電子識別スキームとの間の通信を中継する。

サービス利用時における処理シーケンス



※SAML:Security Assertion Markup Language

連携時に提供される項目

- **自然人**
  - 必須項目
    - 姓
    - 名
    - 生年月日
    - ユニークID
      （固有の識別子を使用しないことを推奨）
  - オプション項目
    - 旧姓・旧名
    - 現住所
    - 出生地
    - 性別
- **法人**
  - 必須項目
    - 法人名
    - ユニークID
  - オプション項目
    - 住所
    - 付加価値税登録番号
    - 税照会番号
    - 法人登記番号
    - 取引主体識別子
    - 事業者登録・識別（EORI）
    - 物品税番号

提供するサービスに応じてオプション項目を必須項目とすることは可能

eID連携のためのJPKI利用に係る課題

1.日本語文字からラテン文字への翻字

✓ SAML Assertionに含める氏名、住所などの文字コードの扱い

- eIDAS-Node間で使用する文字コードは、理論上、XML仕様に基づき、UTF-8, UTF-16のいずれも使用可能
- ラテン文字への翻字が一意でないものは、ラテン文字に翻字したものを送る必要がある（日本語は、これに該当することを確認）

（1）仕様準拠に基づく要求事項

- eIDAS-ServiceからeIDAS-Connectorに対して非ラテン文字（日本語文字）を送る場合には、当該非ラテン文字と一緒に、ラテン文字に翻字したものを送る必要がある。
- 非ラテン文字（日本語文字）からラテン文字への翻字情報は、権威ある情報源から提供する必要がある。

eID連携のためのJPKI利用に係る課題

1.日本語文字からラテン文字への翻字

（2）公的個人認証サービス(JPKI)仕様の適合性

1. 利用者の認証は、利用者証明用電子証明書を使用することで可能
2. SAML Assertionに含めて SAML Responseで返す４種（姓、名、誕生日、個人識別子）の属性情報のうち、個人識別子を除き、公的個人認証サービス(JPKI)の署名用電子証明書に含まれている
3. 但し、公的個人認証サービス(JPKI)で扱う氏名や住所等のデータは、現在「漢字」や「かな」である また、厳密には氏名を構成する「姓」と「名」のデータが分離されておらず、読み仮名やローマ字（ラテン文字）表記に該当するデータが定義されていないという問題が存在

Attribute name	M/O	eIDAS MDS Attribute	利用者証明用電子証明書	署名用電子証明書
FamilyName	M	姓	×	△(未分離)
FirstName	M	名	×	△(未分離)
DateOfBirth	M	生年月日	×	○
PersonIdentifier	M	ユニークID	○※	○※
BirthName	O	旧姓･旧名	×	×
PlaceOfBirth	O	出生地	×	×
CurrentAddress	O	現住所	×	○
Gender	O	性別	×	○

M:Mandatory, O:Option　　※ 実際のPersonIdenrifierは、eIDAS-Nodeで生成する。

eID連携のためのJPKI利用に係る課題

1.日本語文字からラテン文字への翻字

（3）非ラテン文字からラテン文字への翻字情報の取得方法［対処案］

〔案１〕住民基本台帳の姓と名の区別を明確にして、ローマ字表記の情報を追加する

【処理例】

前提：ローマ字表記の情報が住民基本台帳のデータベースに登録されている

処理：利用者を利用者証明用電子証明書で認証する際に取得した利用者証明用電子証明書の発行番号を使って住民基本台帳のデータベースからローマ字表記の情報を取得する

〔案２〕利用者がeID連携を行うためにeIDAS-Nodeを使用する際に、その利用申請として氏名等のローマ字表記の情報を登録する処理を追加する
（この場合、なりすまし防止のため利用者情報の登録に署名用電子証明書を利用する）

【処理例】

前提：利用者証明用電子証明書と署名用電子証明書を紐付けた情報データベースの他に、利用者証明用電子証明書に紐付くローマ字表記のデータベースフィールドが存在する（又は設ける）

処理：署名用電子証明書を利用して利用者情報を初期登録する際に、利用者証明用電子証明書と署名用電子証明書を紐付けた情報データベースを使って、署名用電子証明書の発行番号から利用者証明用電子証明書の発行番号を取得して、利用者証明用電子証明書に紐付くローマ字表記のデータとなる利用者情報を追加登録する

利用者を利用者証明用電子証明書で認証する際に、取得した証明書の発行番号を使って問合せ、利用者証明用電子証明書に紐付くローマ字表記のデータベースからローマ字表記の情報を取得する

eID連携のためのJPKI利用に係る課題

2. 保証レベル「High(高)」の要件への適合

保証レベル「High(高)」を実現するためには、eIDAS規則等（Regulation (EU) 2015/1502）に照らして、次のような項目について要件に適合させる必要

- 登録（Enrolment）：電子識別手段（eIDカード）の申請から発行まで
- 電子識別手段の管理（Electronic identification means management）
- 認証（Authentication）
- 管理運営及び組織（Management and organization）
  - プロバイダとしての資格、義務と責任、法的要件の順守、事業継続
  - 利用者へのサービスに関する情報提供
  - 情報セキュリティ管理（記録保持、技術上の管理策、施設管理及び人的管理）
  - 法令順守及び監査

実際にEU内でJPKIを利用する場合には、
eIDスキームの通知と相互承認に準じた取り扱いが必要

eID連携のためのJPKI利用に係る課題

3. 相互運用性及び信頼性を確保するための運用環境の整備

（１）eID連携の通信において、

1. SAML AuthnRequestで利用され個人を特定するPerson IdentifierのFormat Typeには、“persistent (永続的)”, “transient (一時的)”, “unspecified (未設定)”の３種がある。
2. 運用上、これらをすべてサポートする必要があるが、主には“transient”が使用されている

（２）eIDAS-ServiceとIdP［公的個人認証サービス(JPKI)を含む］との間及び eIDAS-Connector / SP間における運用ルールやセキュリティの確保については定められておらず、当事国に委ねられている。

eIDAS-Nodeを構築し運用するために、

- Person Identifierの生成方法及び当該情報の処理上必要な期間の維持方法を含めた相互運用性や信頼性を確保するための手続や運用ルールを明確化することが必要
- IdP及びSPを構成し運用するために、その相互運用性や信頼性を確保するための手続や運用ルールを明確にするなど、運用環境の整備が求められる

eID連携のためのJPKI利用に係る課題

4. eIDAS規則は、EU加盟国間の連携が前提

日本がEU加盟国とeIDAS規則に準拠したeID連携を実現するためには、国際的にEUと協業するための体制を確立して、この障壁を取り除く必要

5. 国内におけるeID連携を推進するための支援活動

EUにおけるCEF(Connecting Europe Facility) のように、日本国内におけるeID連携を推進するために基幹となるインフラ整備を行うことが必要

Service Providerを生み育てるための資金援助制度の創設や、Service Providerが容易に利用可能なOpen Source Software Libraryを展開することによって、連携利用可能なサービス生み出す環境を育成することが求められる

本日お話ししたeID関係の内容は、NMDAのホームページから参照いただけます

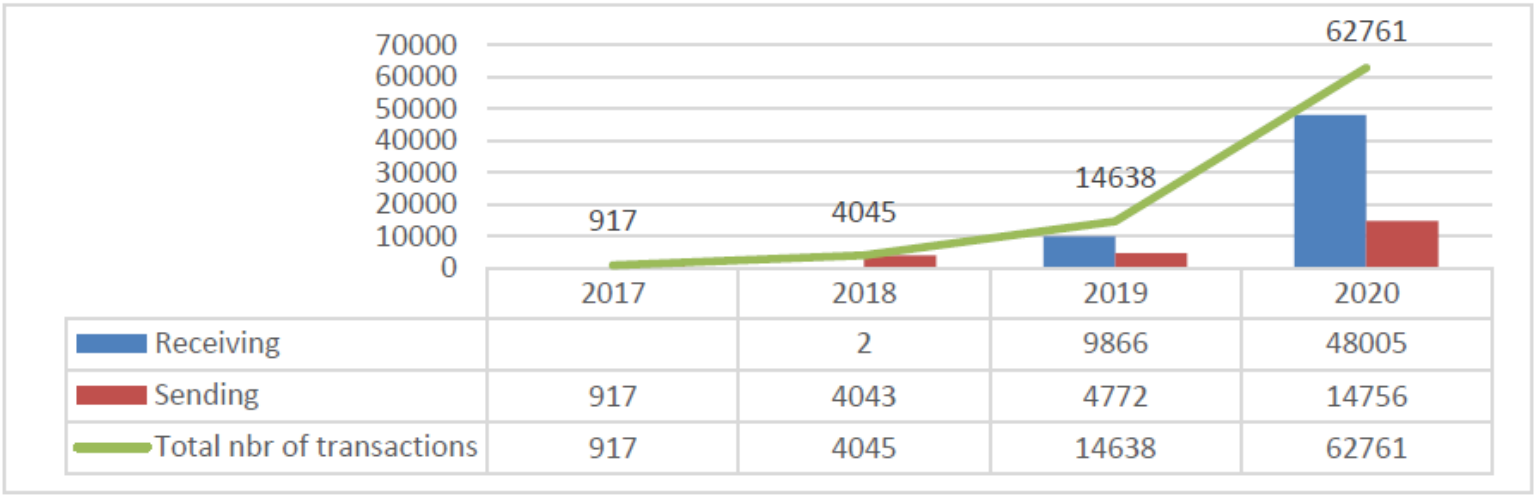
２０２０年度ＪＫＡ機械振興補助事業
「公的個人認証サービスと
海外ｅＩＤの相互利用環境に係る調査研究」の調査報告書
https://www2.nmda.or.jp/archives/1671/

EUにおけるeIDの現状

- 1,835人のEU市民に対する調査（2021年12月）

Understanding the European identity experience, THALES より

eIDのクロスボーダー利用の推移



	2017	2018	2019	2020
Receiving		2	9866	48005
Sending	917	4043	4772	14756
Total nbr of transactions	917	4045	14638	62761

クロスボーダー利用数の推移

民間にeIDを開放している国

eID schemes open to private relying parties: AT, BE (itsme), CZ, DK, EE, ES, FI, DE, HU, IT (SPID), IT (eID), LV, LI, LU, NL, PL, PT (eID), PT (CDM), SE (Freja), SE (BankID)

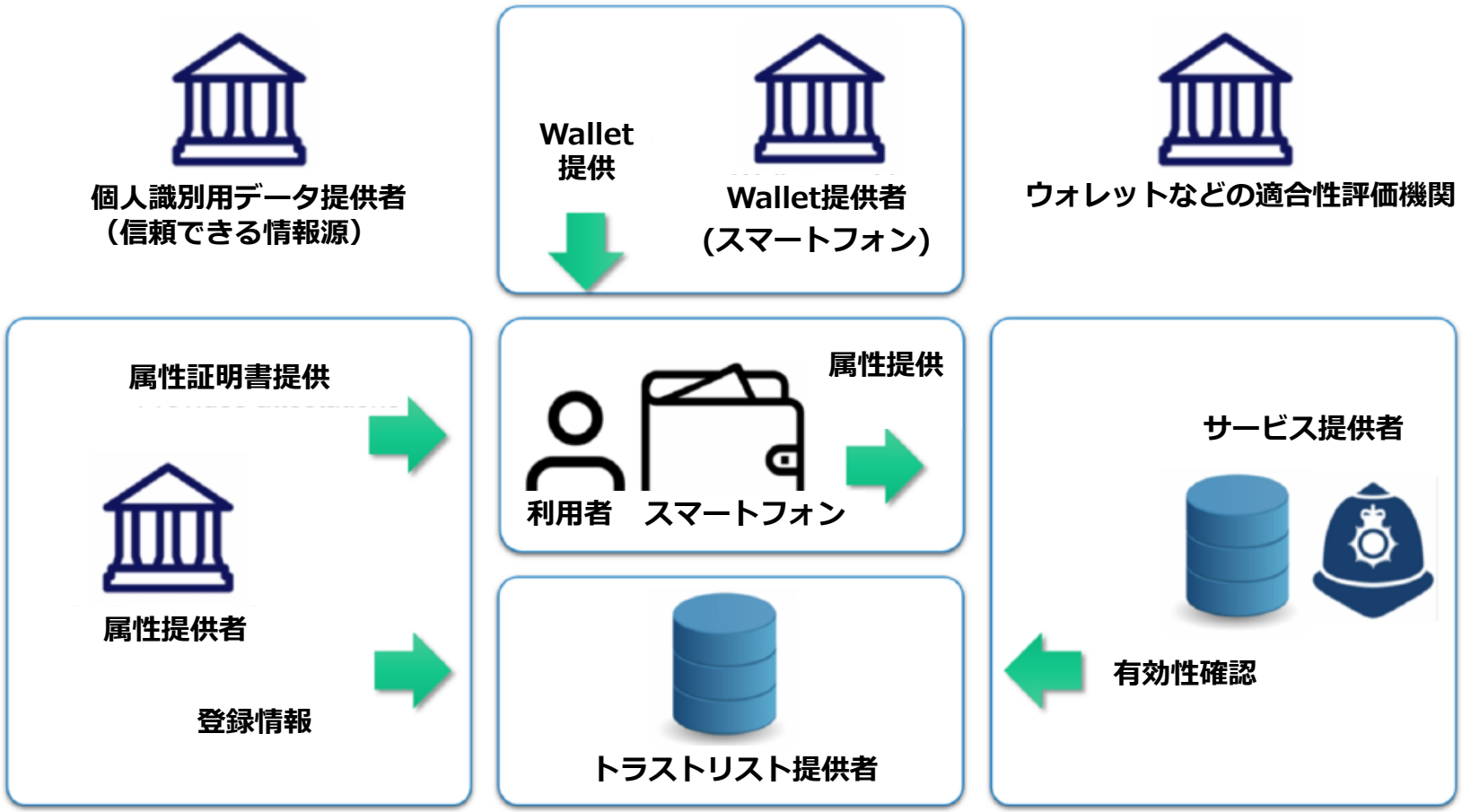
eID schemes not open to private relying parties: BE(eID), EL, HR, SK, SI, UK

COMMISSION STAFF WORKING DOCUMENT 130 (2021)

European Digital Identity Wallet

- 国のデジタルID（eID）や個人の属性証明書や運転免許証、卒業証書などを電子的にスマートフォン等に保管、使用可能な「EUデジタルIDウォレット」を提供
- EUデジタルIDウォレットは、各加盟国の公的機関、または民間団体・企業（加盟国の承認が必要）が発行
- ウォレットを用いてユーザーが自らの身元を証明（認証）したり、特定の個人属性（年齢など）を証明
- ユーザーは自分のアイデンティティ、データ、証明書のどの項目を第三者と共有するかを選択し、誰とどのような共有を行ったかを追跡可能
- EU内の公的サービスや一定の民間サービス（公共性の高い民間サービスや、大規模プラットフォーマーなど）は欧州デジタルIDウォレットの利用を受け入れることを義務化
- 但し、各加盟国の既存の国内制度に基づいて構築

EU Digital Identity Wallet ecosystem



The impact of EU Digital Identity Wallets on NRENs (2021) より

マイナンバーカード機能のスマートフォン搭載

（現在）
マイナンバーカード用
電子証明書の利用
には、毎回カードの
読み取りが必要

**スマートフォンひとつで、いつでもどこでも、
様々な手続・サービスが利用可能に**

生体認証等の活用によって
スマートフォンならではの利便性を実現

子育て支援　TAX　確定申告

オンライン行政手続

薬剤・健診情報　母子健康手帳

自己情報取得（マイナポータル）

健康保険証　コンビニ交付

資格確認

銀行・証券
口座開設　住宅ローン
契約

携帯電話申込　キャッシュレス
決済申込

各種民間サービス

マイナンバーカードの機能（電子証明書）のスマートフォン搭載行政機関・民間事業者等向け説明資料（デジタル庁）より

スマホJPKIの機能

これまで

マイナポータルへのログイン時には毎回マイナンバーカードの読み取りが必要

スマートフォン用電子証明書を利用

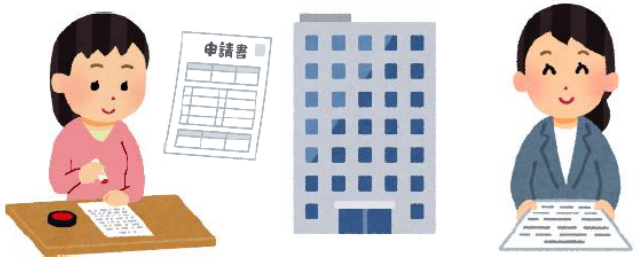
マイナンバーカードを読み取る必要がなく、生体認証等を使って簡単にログインが可能

→通勤中でも、外出先でも、いつでもどこでもサービスを利用可能

マイナポータルで利用できる主なサービス	
行政手続の検索・電子申請	自治体の各種手続の検索及び電子申請が可能。対象手続拡大中。 【例】保育施設利用申込み、給付金申請、児童手当申請
自己情報の確認・提供	行政機関等が保有する自分の情報を確認したり、第三者に提供することが可能。 【例】税・所得情報（金融機関や自治体における手続等に利用） 予防接種履歴・薬剤情報（民間の健康管理アプリ・お薬手帳アプリ等と連携が可能）
お知らせ	行政機関等から情報配信を受けることが可能。 【例】税金の納付依頼、児童手当の手続等の利用者の状況に応じた行政手続の案内

これまで（役所窓口）

書類作成、役所訪問・提出 → 本人確認・申請完了



スマートフォン用電子証明書を利用（電子申請）

マイナポータルで手続を検索・申込内容を入力 → 電子証明書を使って電子署名・電子申請

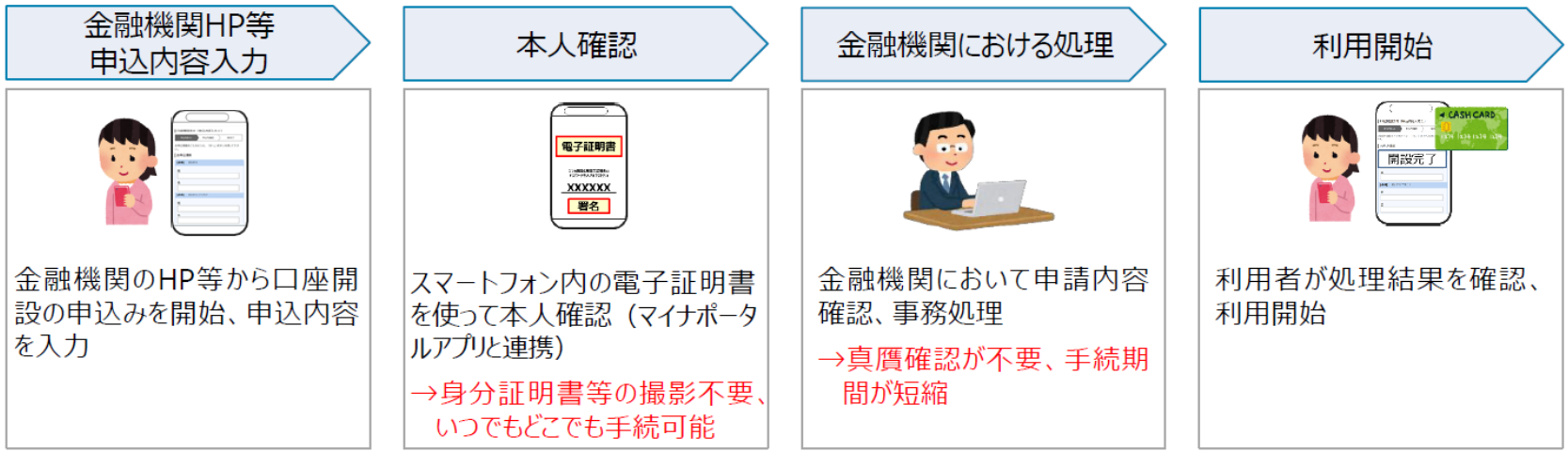
- 入力支援機能を使って、氏名・住所や過去の申請情報等を簡単に入力
- 役所窓口に出向くことなく、いつでもどこでも、スマートフォンひとつで手続可能

マイナンバーカードの機能（電子証明書）のスマートフォン搭載行政機関・民間事業者等向け説明資料（デジタル庁）より

金融機関での利用イメージ

金融機関の口座開設の流れ（窓口・eKYC）

スマートフォン用電子証明書を活用した流れ



※現時点におけるイメージであり、今後変更となる可能性がある。

※遅くとも令和4年9月には民間サービス等との連携に必要なAPI情報を公開予定。また、民間サービスにおける更なる利用拡大を促進する観点から、海外事例（シンガポール等）も参考としつつ、開発者目線の利便性向上にも取り組む。

マイナンバーカードの機能（電子証明書）のスマートフォン搭載行政機関・民間事業者等向け説明資料（デジタル庁）より

国際的eID連携に向けて

- JPKIとEU eID等との相互認証
- eID連携のための仕組みを構築・運営する組織
- ローマ字表記の氏名データの登録・提供方法
- 国籍の登録・提供方法
- EU Identity Walletとの連携の可能性

Tokyo Tech

Thank you