令和２年度

内外一体の経済成長戦略に係る国際経済調査事業

（人生100年時代／ポストコロナ時代の個人の活動履歴の在り方に関する調査）

調査報告書（概要版）

2021年3月

一般財団法人日本情報経済社会推進協会

目次

■ **事業概要**

■ **機能面**

① 個人の特定と認証
② 個人データの連携方法
③ 個人データの認証方法

■ **非機能面**

④ 個人データの扱い方
⑤ UX向上

■ **未来の社会基盤イメージ（案）**

事業概要

- 事業概要
- 検討事項
- 個人データのDX化と検討事項のマッピング

事業概要

■ 課題意識

- 場所や時間にとらわれない多様な働き方や学び方・生き方が出現する中では、まさに『「個」のエンパワーメント時代』が近い将来、到来すると考えられ、学習過程から経済活動・社会貢献まで、より一層「個人」の活動履歴が重要になっている。
- しかしながら、「個人」を中心としたDX化については、情報銀行やパーソナルデータの観点で議論はされるものの未だ明確化されておらず、その基盤となるPersonal Data Store（PDS）やTrusted Web等の構想が提唱されるものの議論が必ずしも進んでいるとはいえない。

■ 目的

- 『「個」のエンパワーメント時代』に向けて、労働市場のより一層の透明性向上（安全性の確保）と活性化を実現するとともに、デジタル化の進展等に応じた「個人」の多様なスキル向上や学び直しの機会の拡大、またこれに伴う精緻で個人主体の人材に関する新規事業の創出や、社会保障の充実等へとつなげていくことを目的に、国際的にも通用する自己証明基盤として、「個人」が管理する「個人の活動履歴」のDX化に焦点をあてつつ、紙証明からの脱却や信頼性の向上、並びに自己実現のために必要な情報の整理とその情報の管理手法等の確立を目指す。
  - 労働市場のより一層の透明性向上（安全性の確保）と活性化の実現
  - デジタル化の進展等に応じた「個人」の多様なスキル向上や学び直しの機会の拡大
  - 精緻で個人主体の人材に関する新規事業の創出や、社会保障の充実等へとつなげていくこと

■ 目指す成果

- 機能面
  - ① 個人の特定と認証
  - ② 個人データの連携方法
  - ③ 個人データの認証方法　など
- 非機能面
  - ④ 個人データの扱い方（データの財産権、プライバシーの在り方等）
  - ⑤ UX向上　など

→ データ取り扱いに関する整理を行う

検討事項

■ 本事業では、マイナンバー制度をはじめとする政府全体の検討状況にも配慮しつつ、個人データのDX化にあたり求められうる機能面・非機能面のガバナンスの在り方について検討した。

検討事項		検討概要
機能面	①個人の特定と認証	• 個人データの連携における個人IDとeKYC • デジタルアイデンティティ（ID）の在り方
	②個人データの連携方法	• デジタルアイデンティティ • アイデンティティ管理の類型 • 個人データの証明可能な連携方法の類型
	③個人データの認証方法	• 個人の活動履歴の構成要素 • 活動履歴のライフサイクル • 証明書（Credential）のライフサイクル
非機能面	④個人データの扱い方	• プライバシーの在り方 • データ形式 • オントロジーの在り方
	⑤UX向上	• UX向上につながるニーズ • UX向上に必要な要素

個人データのDX化と検討事項のマッピング

JIPDEC

トラスト
アンカー
マイナンバーカード
パスポート
免許証
個人ID

eKYC
eKYC
eKYCなど
eKYC

民間
ID
など

①個人の特定と認証

Category I

必ず証明を求められる
業務遂行上保持が求められる

活動履歴
国家/公的資格 等

金融・決済情報
口座番号　等

健康・生活習慣情報
保険証　等

発行者

③個人データの認証方法

Category II

証明を求められることがある

活動履歴
学位・成績・資格　等

金融・決済情報
口座残高、資産
融資・ローン履歴　等

健康・生活習慣情報
民間保険　等

発行者

Category III

証明が前提になっていない
リファレンス等でしか証明できない

<客観的/定量的データ>

活動履歴

学び・経験
課外活動、学習履歴、リカレント等

仕事
職歴（役職、期間）、
参加プロジェクト等

健康・生活習慣情報
健康管理データ、
睡眠時間・運動履歴、ゲーム履歴　等

<主観的/定性的データ>
性格、対人関係
勤務態度、評価　等

発行者

API
API
API
API
API
API

②個人データの連携方法

個人（保有者）

能力、実績を評価した転職等

検証者
人材ビジネス主体／人材関連部署

検証者
人起点のプラットフォーム

⑤UX向上

④個人データの扱い方

機能面

①個人の特定と認証

- 個人データの連携における個人IDとeKYC
- デジタルアイデンティティ（ID）の在り方

個人データの連携における個人IDとeKYC

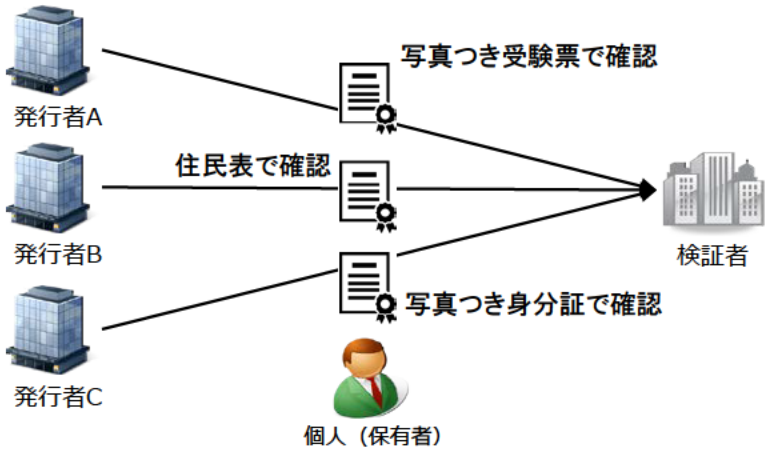
- 活動履歴（個人データ）として、発行者（資格発行団体・企業等）から、個人に対して様々な証明書等が紙媒体で発行されている。発行者は、個人を特定するため身分証明書等（例えばマイナンバーカードなど）を用いて身元確認を行っている。
- そこで、代表的な発行者（資格発行団体）における身元確認方法について調査したところ、資格発行団体において身元確認の基準がなく、その方法も様々であることが判明した。また、発行者・検証者の双方において以下に示す課題も明らかとなった。

発行者の課題

- 活動履歴の証明を発行するにあたり、本人（保有者）の身元確認（KYC）の基準がない。
- 本人（保有者）の身元確認（KYC）に、すでにコストをかけて実施している。
- 本人（保有者）の身元確認（KYC）を厳格にするとコスト増となる。

打ち手

- KYCのコストを下げる。



検証者の課題

- 提出された活動履歴の証明の信頼性がバラバラで、一律に扱うことができない。
- 提出された活動履歴の証明が、提出した本人（保有者）のものであるか保証がない。
- 確認がコスト（負担）である。

打ち手

- 確認するコストを下げる。

- 発行者における本人（保有者）の**身元確認を電子化（eKYCを導入）する**ことによって、身元確認のコストを下げることができると考えられる。
- 発行者から**基準に準拠した身元確認を行ったことが保証**されることによって、検証者における活動履歴の証明の確認コストが下がり、活動履歴の活用が進むのではないか。

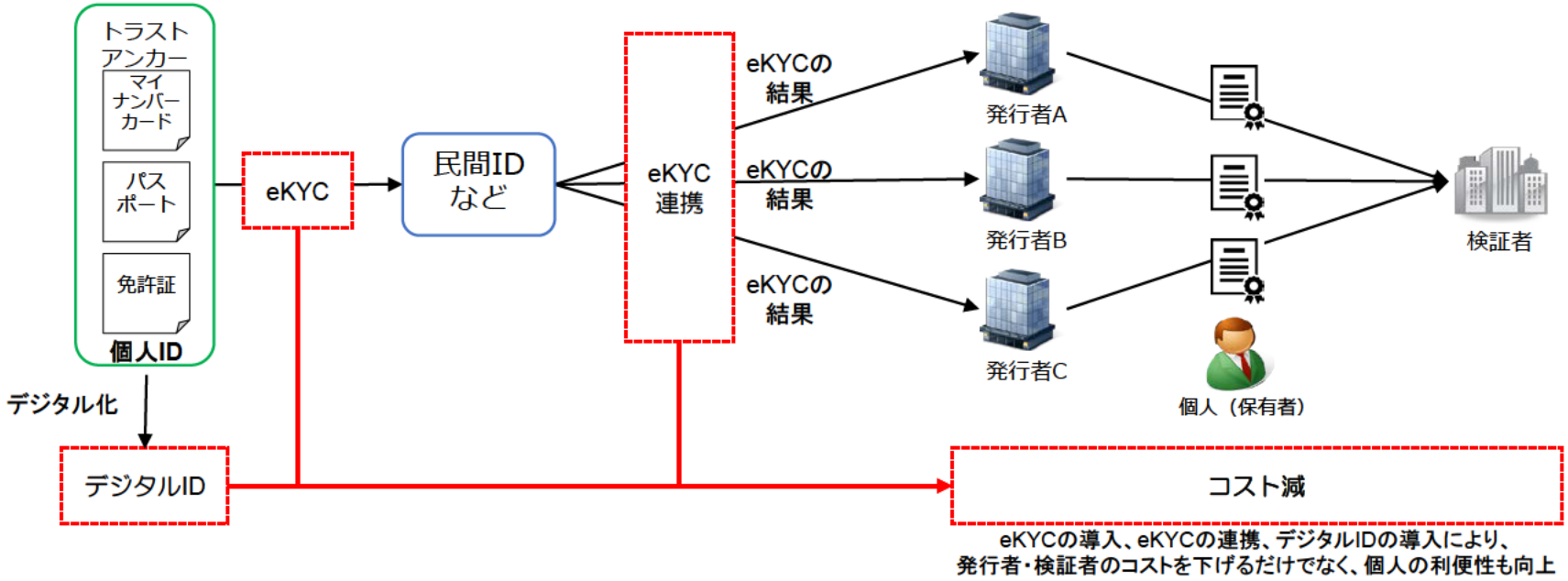
（参考）発行側における身元確認の現状

資格の分類		試験の名称	実施主体	身元確認方法		
				申込時	試験時	発行時
業務独占資格	弁護士、公認会計士、司法書士のように、有資格者以外が携わることを禁じられている業務を独占的に行うことができる資格。	教育職員（教育職員免許法）	国	住民票	試験票	住民票又は戸籍抄本
		医師（医師法）	国	写真（卒業校で本人確認を行い、卒業校が割印）	申込時の写真と照らし合わせ、試験実施機関が確認、受験票	住民票又は戸籍抄本
名称独占資格	栄養士、保育士など、有資格者以外はその名称を名乗ることを認められていない資格。	中小企業診断士	団体	特になし	受験票・写真票・写真付本人確認書類	住民票の写し
		情報処理安全確保支援士（情報処理促進法）	国	特になし	受験票に貼り付けられた写真と本人の顔で確認	戸籍謄本・住民票等の公的書類の提出
必置資格（設置義務資格）	特定の事業を行う際に法律で設置が義務づけられている資格。	宅地建物取引主任者	団体	特になし	受験票	特になし
技能検定	業務知識や技能などを評価するもの	情報処理技術者試験（情報処理促進法）	国	特になし	受験票に貼り付けられた写真と本人の顔で確認	なし
民間資格	その資格を持つ者の知識や技能を、民間の団体が認定している資格	簿記検定、プログラミング検定	日本商工会議所	同じ資格試験でも、会議所によって異なる	試験会場にて、受験票と写真付本人確認書類で確認	なし
		個人情報管理士	日本個人情報管理協会	受験票を配達記録郵便で送り、本人に届いたかで確認	受験票での確認	なし
		TOEIC	国際ビジネスコミュニケーション協会	会員登録してもらうが、書類等の提出はない	試験会場にて、受験票と写真付本人確認書類で確認	なし

資格の分類は、文部科学省の整理による。尚、上記委では文部科学省の整理に該当しない資格を民間資格として整理。
参照：https://www.mext.go.jp/b_menu/shingi/chousa/shougai/014/shiryo/07012608/003.htm

デジタルアイデンティティ（ID）の在り方

- 日本においてeKYCが進んでいないことの要因の一つに、身分証明書のデジタルID化が進んでいないことがあげられる。
- 日本では、総務省の設置する「マイナンバーカードの機能のスマートフォン搭載等に関する検討会」において検討が進んでいる。一方で、国際的標準として、パスポート、免許証、身分証明書のデジタルID化の標準規格が策定されている。



- 日本においてデジタルIDのインフラ整備が求められる。
- その際、デジタルIDのインフラは、まずは国際標準に準拠したもので整備を進めるものの、プライバシー保護やセキュリティ確保の点で国際標準作りは未だ途上であり、日本としても積極的に提案していく。

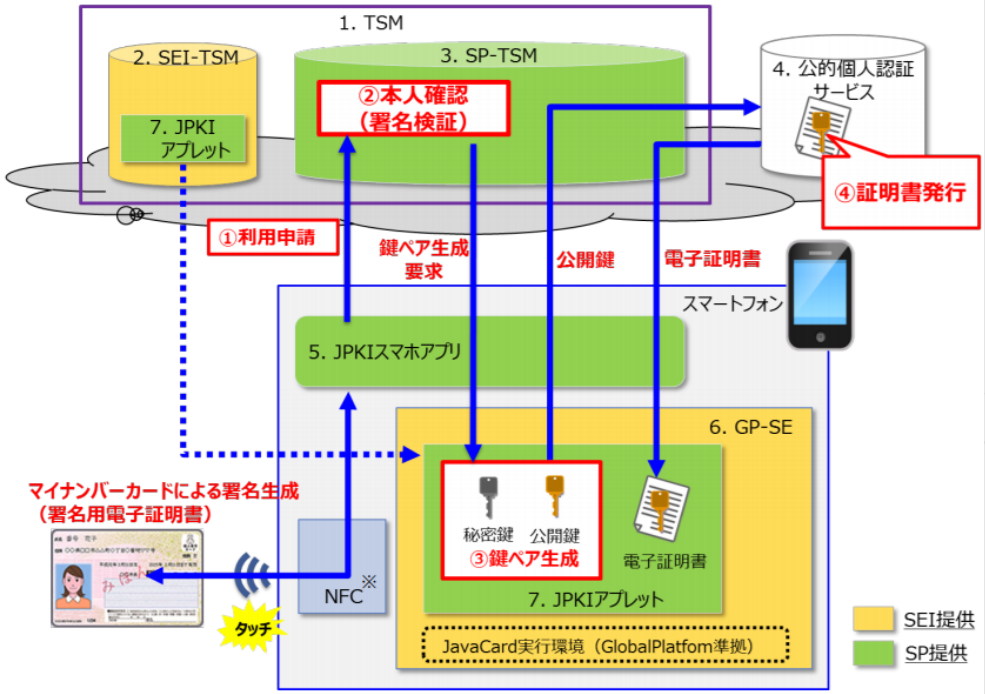
（参考）日本の検討状況

■ マイナンバーカードの機能のスマートフォン搭載等に関する検討会

➢ オンラインによる高度な本人確認を可能とするマイナンバーカードの機能（公的個人認証サービス）をスマートフォンに搭載することを基本方針として検討

スマホに電子証明書を搭載するためのシステム構成　10

スマホに電子証明書を搭載するためのシステム構成およびその用語解説



※「Type B」を使用。

（補足）上図ではJPKIスマホアプリは利用者によってGoogle Playからダウンロードされた状態を想定。

サーバ側

1. TSM: Trusted Service Manager
   - SEI-TSMとSP-TSMで構成される。スマートフォン上のSecure Element（SE）へのデータ配信をセキュアに実施する。

2. SEI-TSM
   - SEの発行者（SEI: Secure Element Issuer）が運営するTSM。
   - サービス提供者（SP: Service Provider）のアプレットを預かり、SEにアプレットを格納する役割を担う。

3. SP-TSM
   - SPが運営するTSM。
   - ユーザの利用申請を受け付け、SEのパーソナライズを行う役割を担う。

4. 公的個人認証サービス
   - J-LISが運営する認証サービス。

スマートフォン側

5. JPKIスマホアプリ
   - 利用申請やサービス利用時に使用するAndroidアプリ。
   - Google Playからダウンロードする。利用申請時やサービス利用時に使用する。

6. GP-SE
   - Androidスマートフォンに搭載されるSE。
   - GlobalPlatform仕様に準拠し、Javaアプレットをダウンロードできる。

7. JPKIアプレット
   - JPKI機能を実装するJavaアプレット。

出典：マイナンバーカードの機能のスマートフォン搭載等に関する検討会「第１次とりまとめ（案）」
https://www.soumu.go.jp/main_content/000725415.pdf

（参考）デジタルIDの国際標準

■ パスポート、運転免許証、個人識別用ID管理など、デジタルIDに関する標準化が進んでいる。

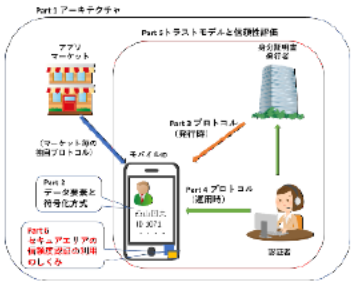
- ICAO TR DTC
  - **Digital Travel Credentials（デジタル旅行資格情報）**
  - 2021年の標準化を目指し、審議中
  - 欧州＆オーストラリア：積極的に実証実験や導入検討

参考：https://unitingaviation.com/news/security-facilitation/replacing-a-conventional-passport-with-digital-travel-credentials/

- ISO/IEC18013-5
  - **Mobile driver licenses（モバイル運転免許証）**
  - 2021年の標準化を目指し、審議中
  - アメリカ：2021年正式導入
  - 欧州＆オーストラリア：積極的に実証実験や導入検討

参考：https://medium.com/@dkelts.id/mobile-driver-licenses-mdl-how-to-use-iso-18013-5-5a1bbc1a37a3

- ISO/IEC 23220
  - **モバイルデバイスにおける個人識別用ID管理のための基礎的要素**
  - 2022年の標準化を目指し、審議中
  - ドイツで国民証IDのスマホ化、導入検討中



出典：https://www.meti.go.jp/press/2020/06/20200622003/20200622003.html

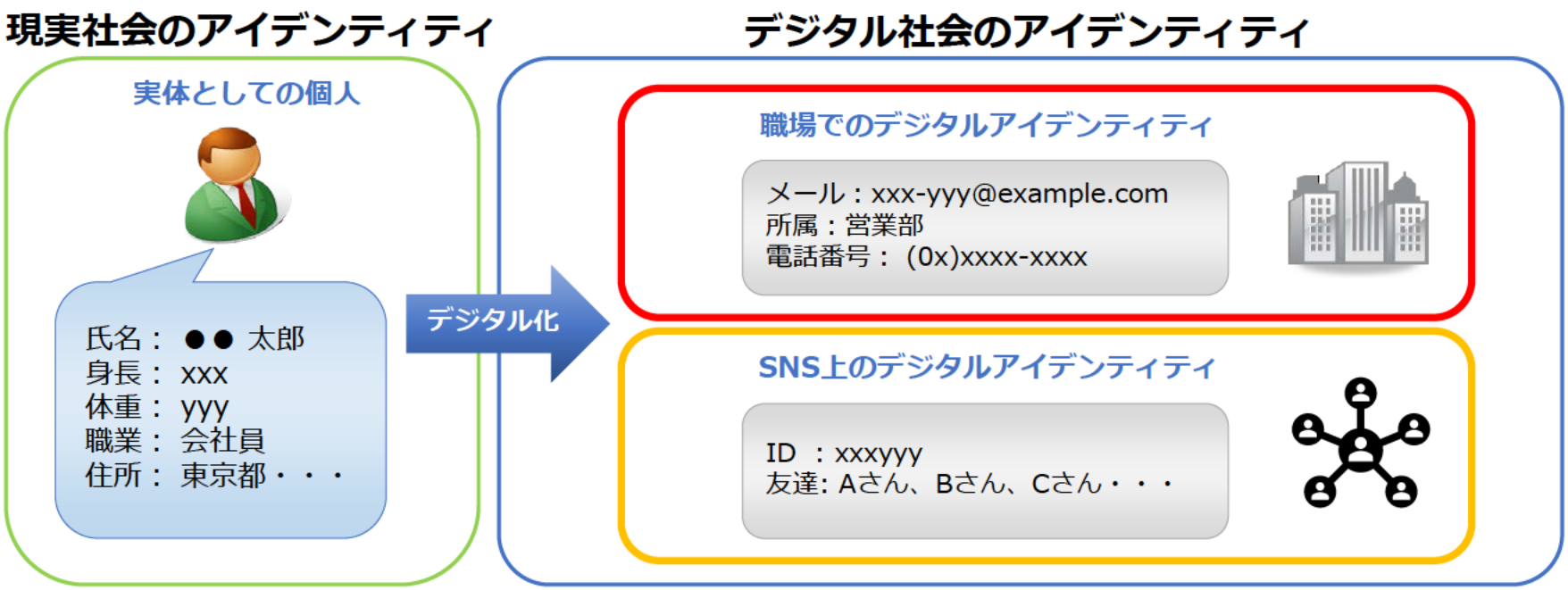
機能面

②個人データの連携方法

- デジタルアイデンティティ
- アイデンティティ管理の類型
- 個人データの証明可能な連携方法の類型

デジタルアイデンティティ

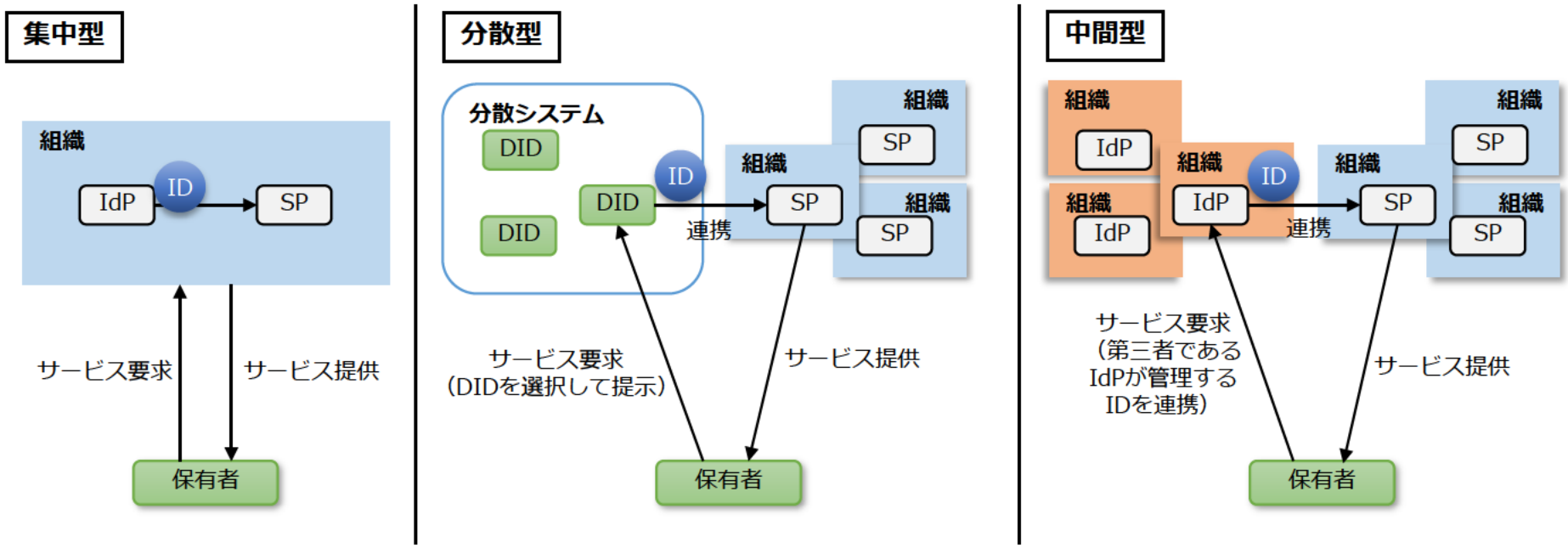
- **アイデンティティ（Identity）**
  - ISO/IEC 24760-1で「実体（Entity）に関する属性情報（Attribute）の集合」と定義される。
  - アイデンティティは、氏名、住所、電話番号、メールアドレス、職業などの様々な属性情報の組み合わせで成り立つ。
  - 資格、技能や職歴といった個人の活動履歴も属性情報のひとつである。
- **デジタルアイデンティティ**
  - アイデンティティを構成する属性情報がデジタル化され、デジタル社会におけるデータとしての個人である。



- 個人データの連携方法は、デジタルアイデンティティの一部である活動履歴に係る属性情報を証明可能な方法で連携することであると言える。

アイデンティティ管理の類型

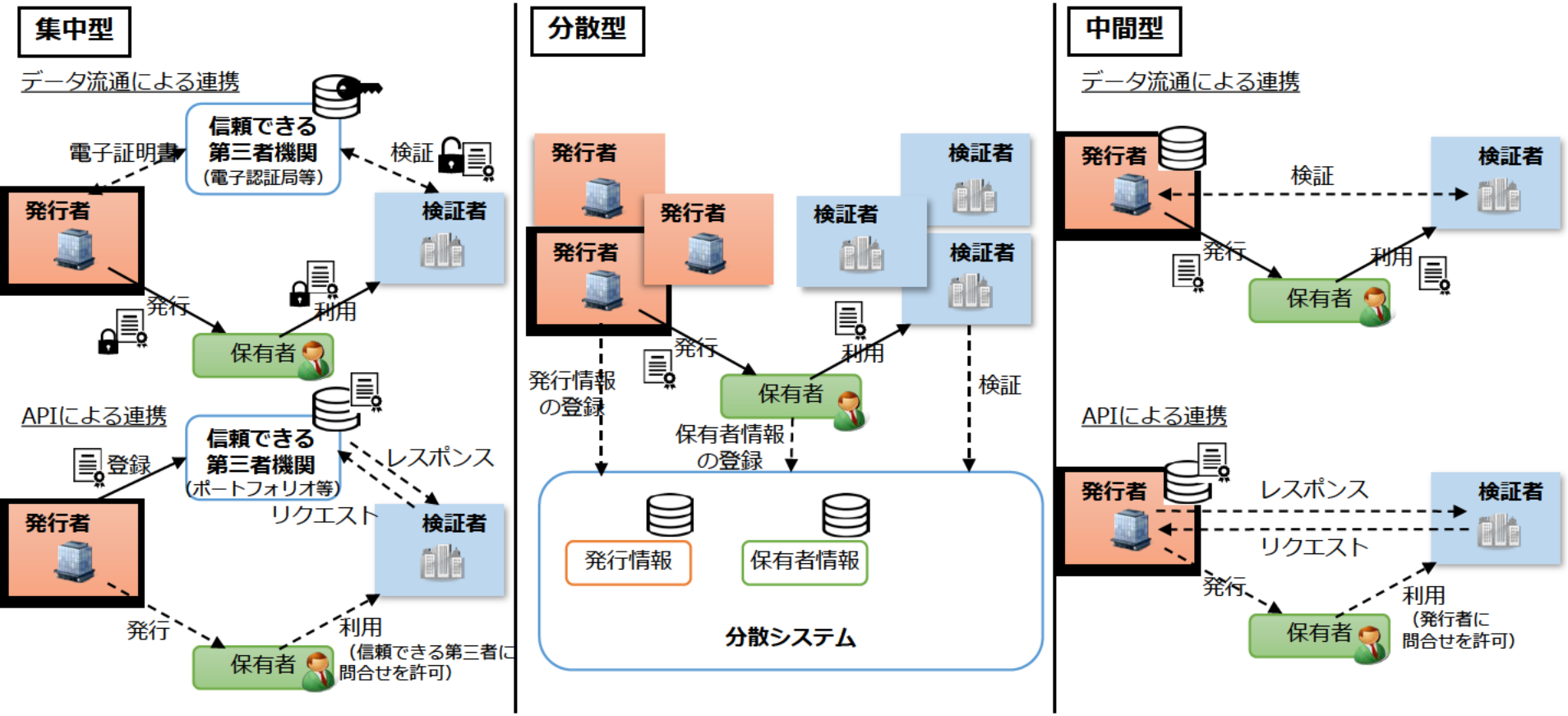
- デジタルアイデンティティの管理は、以下の3つに分類することができる。
  - 集中型のID管理
    - 保有者のアイデンティティを組織が管理する。
  - 分散型のID管理
    - 分散型アイデンティティ（Decentralized Identity：DID）は、保有者自身がアイデンティティに関する管理権限を持ち、保有者の許可した範囲で連携する。
  - 中間型（連携/Federation）のID管理
    - 保有者のアイデンティティを第三者であるIdP（Identity Provider）が管理し、保有者が許可した範囲で連携する。



- 分散型は、管理の権限をすべて保有者が持つことができることから、個人主体の活動履歴のDX化に適していると考えられる。
- ただし、**アイデンティティの利用における責任も保有者自身がすべて請け負うこととなる**ため、責任と権限のバランスを考慮する必要がある。

個人データの証明可能な連携方法の類型

- アイデンティティ管理の類型をもとに、個人データの証明可能な連携方法の３類型を整理した。
- 集中型及び中間型では、個人データを検証可能な形式で流通させて連携する方法と発行者が提供するAPIに検証者が問い合わせることで連携する方法に分けることができる。



- 個人の活動履歴のうち資格証明書のようにある時点の状態を証明するための情報についてはデータ流通による連携が適している。一方、現在の状態を示す情報を連携する場面においては、APIによる連携が良いという場合もある。
- 発行者や第三者機関の信頼度（将来にわたって存在し続けるかなど）の観点では、発行者の存在に依拠しない分散型が望ましいと考えられる。

（参考）個人データの連携方法に関連する国際標準

- デジタルアイデンティティのフレームワーク
  - NIST SP800-63-3 Digital Identity Guidelines
  - ISO/IEC 29115:2013 Entity authentication assurance framework
  - ISO/IEC TS 29003:2018 Identity proofing
- 身元確認（Identity Proofing）結果に係る連携方法
  - OpenID Connect for Identity Assurance1.0
- 当人認証（AuthenticationとAuthorization）に係る連携方法
  - OpenID Connect1.0
  - OAuth2.0
- 活動履歴に係る連携方法
  - APIによる連携方法
    - Financial-grade API（FAPI)
  - データ共有による連携方法
    - OpenBadge2.0（ https://openbadges.org/ ）
    - BlockCerts（ https://www.blockcerts.org/ ）

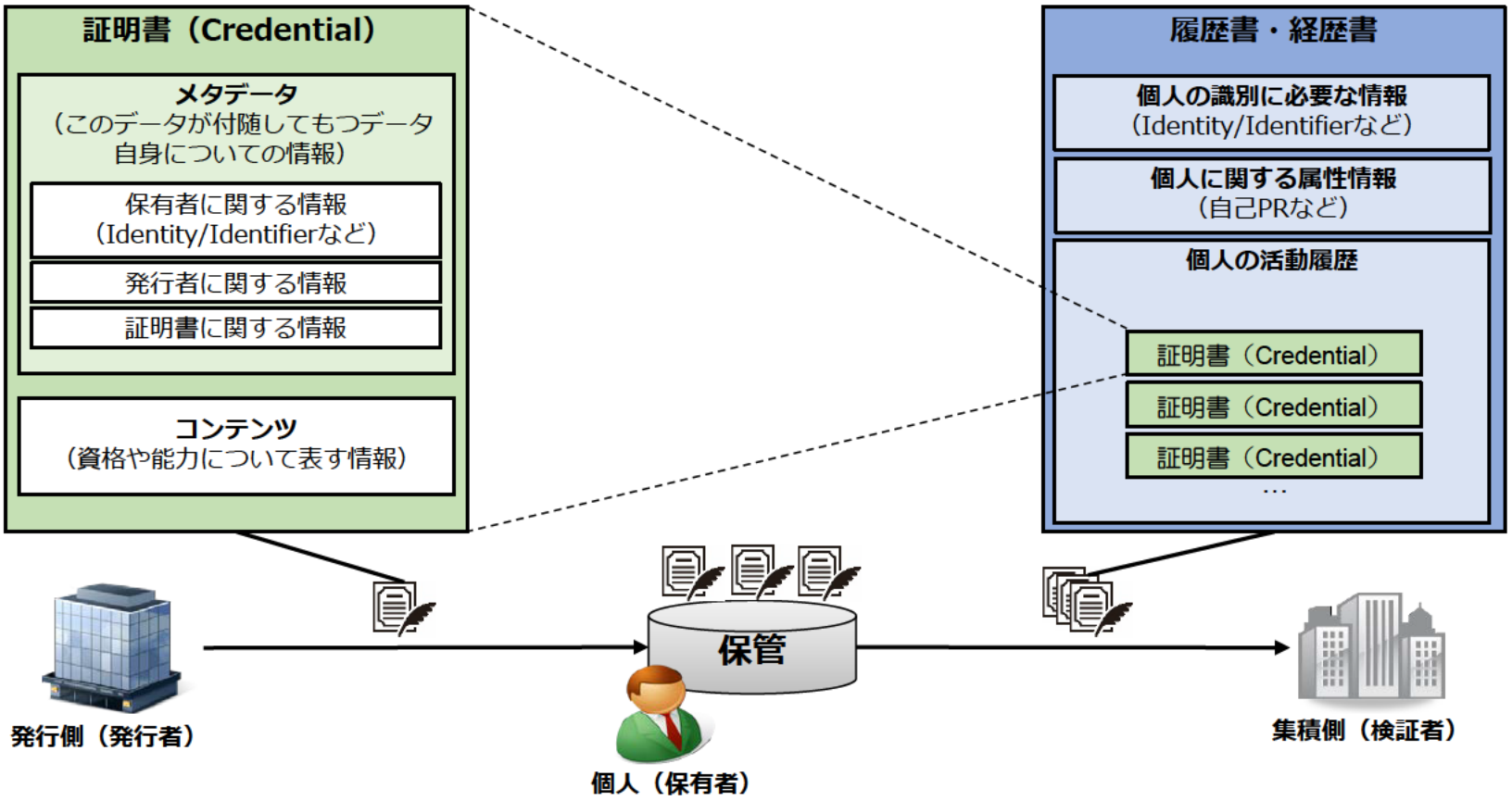
機能面

③個人データの認証方法

- 個人の活動履歴の構成要素
- 活動履歴のライフサイクル
- 証明書（Credential）のライフサイクル

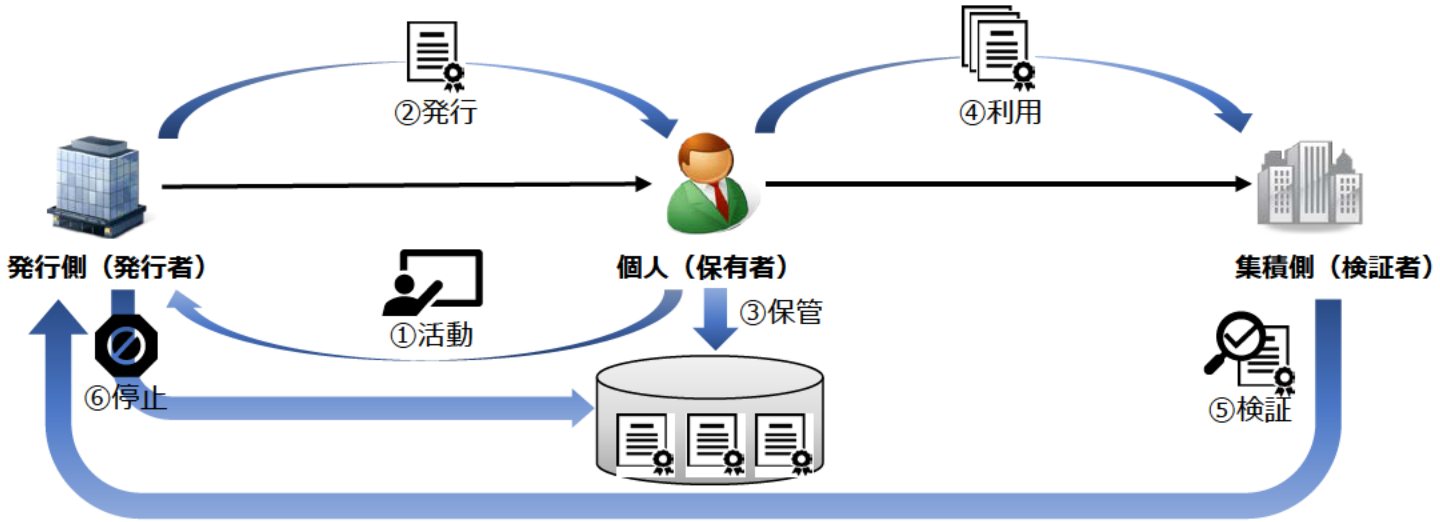
個人の活動履歴の構成要素

- デジタルアイデンティティとしての個人の活動履歴は、発行者により証明書（Credential）として発行される。
- 個人の活動履歴は、下図の履歴書・経歴書のように証明書（Credential）の集合体として利用されることが多い。
- 活動履歴の利用は、以下のような流れとなる。
  - ① 発行側（発行者）から個人（保有者）に、活動履歴が証明書（Credential）として発行される。
  - ② 個人（保有者）は、様々な活動履歴を保管する。
  - ③ 個人（保有者）は集積側（検証者）に、保管している活動履歴の中から、必要な活動履歴を選択して提示（共有）する。
  - ④ 検証者は、提供を受けた証明書（Credential）を検証することで**「個人データの認証」**を行う。



活動履歴のライフサイクル

■ デジタル化された活動履歴のライフサイクルは、下図のようになる。



活動履歴のライフサイクル	内容
①活動	発行者が、個人（保有者）に技能、経歴を持っているかを確認する。
②発行	発行者が、個人の身元情報を確認するとともに、実態との結びつきを確認する（Identity Proofing）。
	発行者が、データベース（Identity Register）に登録する。
	発行者が、登録情報をもとに活動履歴の証明（Credential）を個人に発行する。
③保管	個人が、活動履歴の証明を保管する。
④利用	個人が、活動履歴の証明を提示・共有する。
⑤検証	個人から提示を受けた活動履歴の証明を、検証者が確認（Verify）する。
	（AND/OR）検証者がリスクに応じて発行者に対して活動履歴の証明を検証（Validate）する。
⑥停止	発行者が、個人の活動履歴の証明を停止（失効）する。
	（OR）発行者が、個人に活動履歴の証明を再発行（再有効化）する。
	（OR）発行者が、事業を廃止する。

証明書（Credential）のライフサイクル（１／２）

サイクル	内容	要求事項	海外事例	あるべき姿
活動	発行者が、個人（保有者）に技能、経歴を持っているかを確認する。		• 発行者が、個人に技能、経歴を持っているかを確認する。 • （米国：LER）発行者である教育者や研修機関は、個人の現在のスキルセットを評価してギャップを特定し、追加の学習機会を推奨する。	• 個人が希望する職業と保有するスキル等とのギャップを特定し、必要なスキル等が提案されることが望ましい。
発行	発行者が、個人の身元情報を確認するとともに、実態との結びつきを確認する（Identity Proofing）。	• 個人が実在する人物であるかを確認 • 個人との紐づけを確認する仕組み。	• （米国：NIST）リスク評価を実施し、その結果に応じた身元確認の方法が、身元確認保証レベル（IAL（Identity Assurance Levels））として定義されている。（自己申告、公的証明書などをエビデンスとする確認、対面での確認） • （米国：NIST）発行者は名前, 住所, 誕生日, Email, 電話番号などのPII（Personally Identifiable Information）を個人から収集するとともに、そのIdentity Evidenceとなる運転免許証とパスポートなど２種類のIdentity Evidenceを収集し、それぞれがマッチすることを検証し、確認する。	• 標準化された身元確認方法によって、個人を特定し、実在の人物であることが確認され、肉体と紐づけられることが望ましい。
	発行者が、データベース（Identity Register）に登録する。		• （米国：NIST）CSP（Credential Service Provider）は登録コードを個人が提示した任意のAddress of Recordに送信し、個人が送信された登録コードを提示することで紐付けを行い、登録をする。 • （米国：NIST）（OR） CSPはProofingの通知を個人の住所に対して送信し、個人はその通知を提示することで紐付けを行い、登録を行う。	• オンラインを前提とした場合、個人が提示した任意のAddress of Record（e-mail除く）に送信し、個人が送信された登録コードを提示することで紐付けを行い、登録をすることが望ましい。
	発行者が、登録情報をもとに活動履歴の証明（Credential）を個人に発行する。	• 個人に対して発行されていることを確実にする仕組み。	• （米国：LER）証明書の発行には、発行者と個人の両方の同意が必要である。 • （米国：NIST）個人が自身の所有する1つ以上のAuthenticatorに紐づけられたIdentityレコード (すなわち、Credential) の正当な保有者であることをCSPに対して証明するプロセスに基づいて、Credentialが発行される。 • （米国：LER）発行者の機能は、記録システムに統合しやすく、発行の容易さ、取り消し、記録管理など、Credentialの発行に関与するすべてのプレーヤーが要求する機能をサポートするものでなければならない。 • （米国：LER）Credentialは、必要とされるスキルの定義に関する基準に準拠した形で、かつ、人間や機械で読み取り可能な形である必要がある。。 • （米国：LER）職業と仕事の説明・スキル等についての理解と相互比較を向上させるために標準化されたオントロジーを使用する。 • （欧州）個人・発行者を識別するためにeIDAS準拠のPKIインフラに依存し、e-Sealで署名され、発行される。 • （欧州）Credentialは、発行者やベンダーに継続的に依存してはならない。開放性（オープンソース、オープンアクセス、ボーダレス、中立）は、このような発行者やベンダーによるロックインを防ぐのに大いに役立つ。	• Credentialの発行にあたっては、発行者・個人・検証者がデジタル上で利用可能な形式で発行されることが望ましい。 • 加えて、標準化されたオントロジー等に基づいた言語で記載されていることが望ましい。
保管	個人が、活動履歴の証明を保管する。		• （米国：LER）オープンスタンダードに基づいて構築されたシステム上に保管される。 • （米国：LER）個人が自身の個人情報を提示・共有することを望むまで、個人情報が安全かつ非公開であることが保証される。 • （米国：LER）システムは、個人がCredentialを生涯を通じて利用できるようにすべきである。 • （米国：LER）特定のプロバイダやソリューションに縛られないことが特に重要である。 • （米国：LER）プライバシーとセキュリティの要件が満たされていることを確認するために監視が必要な場合もある。 • （欧州）個人は、ユーロパスのeポートフォリオまたはその他のプラットフォームやウォレットに証明書を保存することができるものとする。	• 保管用システムは、ベンダーロックインを回避できるようにオープンスタンダードに基づくものが望ましく、かつ、長期的に利用できるものが望ましい。 • 個人が提供・共有を望むまで、個人情報が安全かつ非公開で、セキュアな環境で保管されることが望ましい。

証明書（Credential）のライフサイクル（２／２）

サイクル	内容	要求事項	海外事例	あるべき姿
利用	個人が、活動履歴の証明を提示・共有する。	• 個人以外が証明書を利用するケースも考えられるが、本事業では個人が直接使用する場合に限る。 • リクエストとレスポンスをセットが検討すべき。（年齢が20歳以上かを聞かれているときに、身分証を見せるのではなくYesかNoかを答えるだけでよいなど。）	• （米国：LER）Credentialの提示・共有は、特に個人を特定する情報（PII）については、必要な開示量に応じて最適化されるべきである。 • （米国：LER）個人は発行者を関与させることなく、あるいは発行者に通知することなくCredentialを提示・共有することができる。 • （欧州）個人は、共有する内容（たとえば、Webリンクを送信するか、直接情報を送信するか）と期間（たとえば、Webリンクがアクティブである期間を決定できる）を制御できる。	• Credentialの提示・共有においては、個人情報だけでなく、活動履歴に関しても、個人のコントロールによって必要最小限な情報量に調整可能であることが望ましい。 • 個人が意図しない発行者への通知・関与は制限されるべきである。
検証	個人から提示を受けた活動履歴の証明を、検証者が確認（Verify）する。	• 証明書の内容が正しいことを確認できる仕組み。 • 証明書を提示している人が、確かに個人であることを確認できる仕組み。	• （米国：LER）多くの異なる発行者から発行されるCredentialは、標準的な仕様が提供され、様々なタイプのCredential（およびCredentialデータ標準）が検証可能でなければならない。 • （米国：NIST）証明書を提示している本人が確かに本人であるかどうかに関して、リスク評価を実施し、そのリスク評価結果に応じた認証の方法を、当人認証保証レベル（AAL（Authenticator Assurance Level））に応じた方法で実施し、個人が保有者として認識された上でCredentialの提示・共有を行う。 • （欧州）資格情報等のCredentialに記載されている名前と生年月日を、個人の国民eIDに保存されている名前と生年月日と比較する。	• 様々なタイプのCredentialが検証できるように、Credentialは標準的な仕様であることが望ましい。 • デジタル上において、非常に高い強度（AAL3）で、個人が認証されることが望ましい。 • Credentialに記載されている個人情報と認証された個人の個人情報を比較して検証することが望ましい。
	（AND/OR）検証者がリスクに応じて発行者に対して活動履歴の証明を検証（Validate）する。	• 証明書が本物であることを確認できる仕組み。	• （欧州）発行者が高等教育機関などの特定の資格について特定のCredentialを発行する権限を有しているか、指定された標準に従ってCredentialが発行されているか、発行者が本当にCredentialを発行したか(e-Sealのチェック)、有効期間内か(証明書に埋め込まれた有効期限情報との照合)、証明書は取り消されていないか(失効リストとの照合)を検証する。	• Viewerなどによって、署名・有効期限等の確認が自動的に行われることが望ましい。
停止	発行者が、個人の活動履歴の証明を停止（失効）する。		• （米国：NIST）CSPは，オンラインアイデンティティが存在しなくなった(例えば，本人の死亡や詐称であることが判明した)とき、個人に要求されたとき，またはCSPが個人の加入要件を満たさなくなったと判断したとき，速やかにCredentialを停止（失効）する。 • （欧州）Credentialを発行する際、授与機関は、将来必要になった場合に失効証明書を発行することを約束する失効リストのURLもCredentialに示さなければならない。	• 個人が、保有者としての要件を満たされない状態（死亡、詐称等）になった場合に停止（失効）されることが望ましい。 • 有効期限のあるものに関しては、予め失効に関する情報もCredentialに含めることが望ましい。
	（OR）発行者が、個人に活動履歴の証明を再発行（再有効化）する。		• （米国：NIST）（身元確認がIAL2またはIAL3で実施されていた場合）個人に対して、身元確認のプロセスを再び実施する。	• Credential発行に至るまでの身元確認および登録プロセスを再度実施する事が望ましい。
	（OR）発行者が、事業を廃止する。	• 発行者が不在であっても証明書が有効であることを保証する仕組みが必要。	• （米国：LER）発行者が存在しなくなるなど、Credentialへのアクセスが失われた場合には、正当に発行されたCredentialの信頼できる記録を直接入手して、他の手段でCredentialを回復したり、アクセスできるようにできなければならない。	• 分散台帳やブロックチェーン技術を活用するなどし、記録が残るように整備されることが望ましい。

（参考）個人の活動履歴を巡る欧米の事例

JIPDEC

- 米国
  - NIST SP 800-63-3
    https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
  - NIST SP 800-63A
    https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf
  - NIST SP 800-63B
    https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
  - NIST SP 800-63C
    https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf
  - White Paper on Interoperable Learning Records
    https://www.commerce.gov/sites/default/files/2019-09/ILR_White_Paper_FINAL_EBOOK.pdf
  - Learning and Employment Records : Progress and the path forward
    https://www.commerce.gov/sites/default/files/2020-09/LERwhitepaper09222020.pdf
- 欧州
  - Europass Digital Credentials Infrastructure (EDCI)
    https://europa.eu/europass/en/europass-digital-credentials-interoperability
  - Europass framework for digitallysigned credentials
    https://ec.europa.eu/futurium/en/system/files/ged/europass_background-info_framework-digitally-signed-credentials.pdf

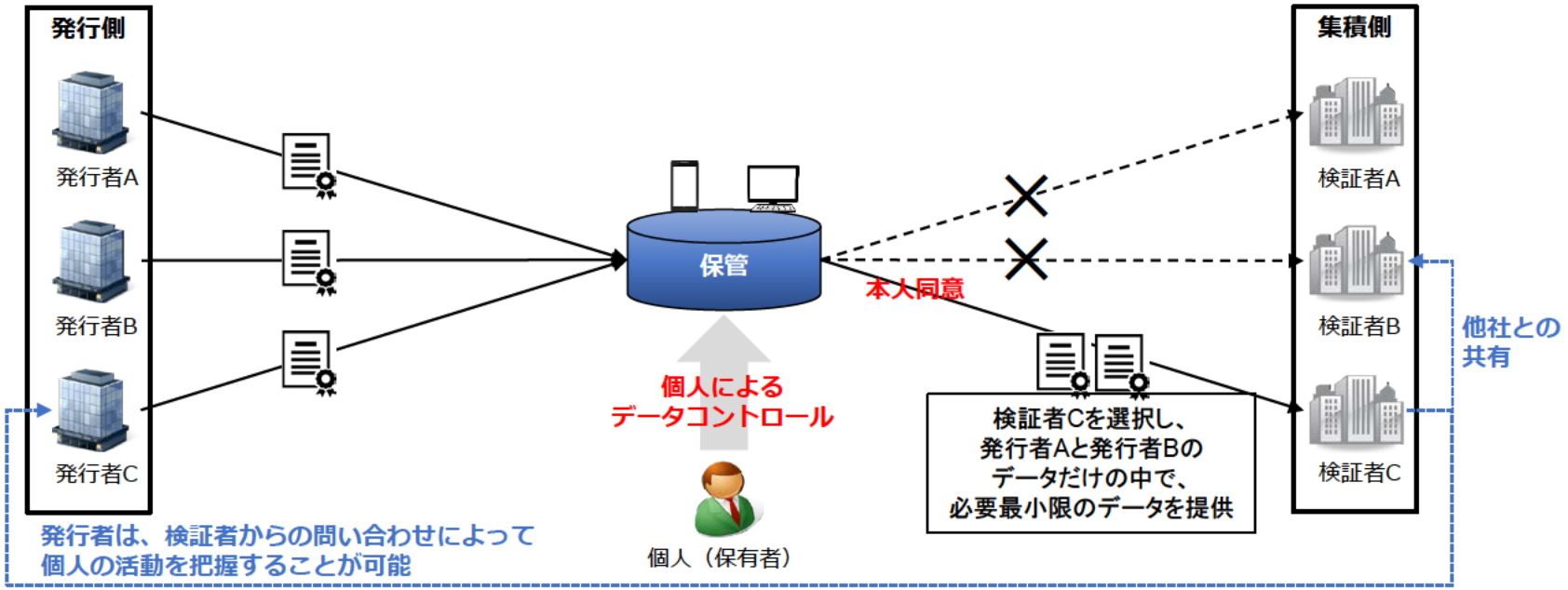
非機能面

④個人データの扱い方

- プライバシーの在り方
- データ形式
- オントロジーの在り方

プライバシーの在り方

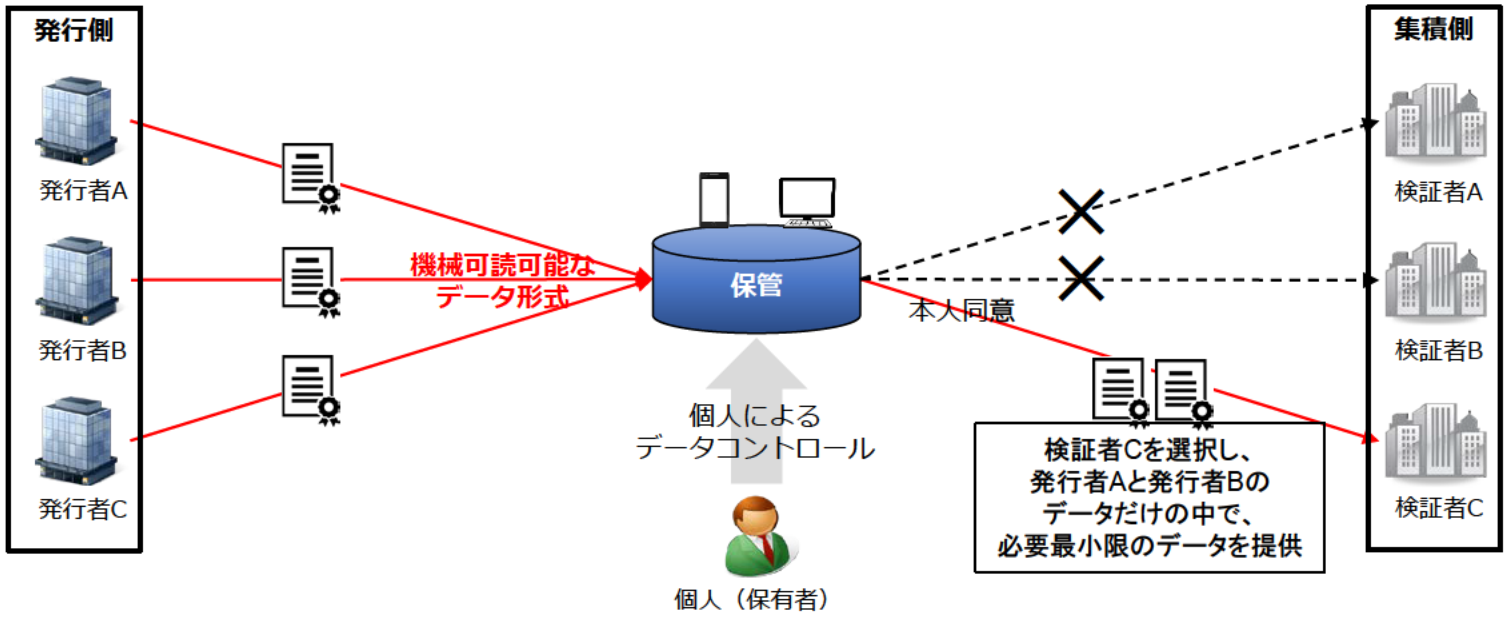
- 個人が検証者に提供するデータは、必要最小限であること（ex.検証者に成人かと問われた場合に、YES／NOだけが提供できれば足り、生年月日まで教える必要はない）が好ましい。
- また、検証者が個人の活動履歴データを他社と共有したり、検証者が発行者へ問い合わせた際に、発行者によって、個人の活動が把握されてしまうというようなプライバシーリスクも考えられる。



- プライバシー保護の観点からも、保有者はいつでもデータにアクセスし、保有者の同意の下で、個人の活動履歴データを「いつ、誰に、何を、どこまで」提示するか、また、一度提供したデータの利用停止など、保有者自らがコントロールできる範囲を整理し、保有者がコントロールできる機能を実装する必要があるのではないか。
- また、検証者の行動（発行者への問合せや他社との共有）によるプライバシーリスクを避けるための仕組みが求められる。

データ形式

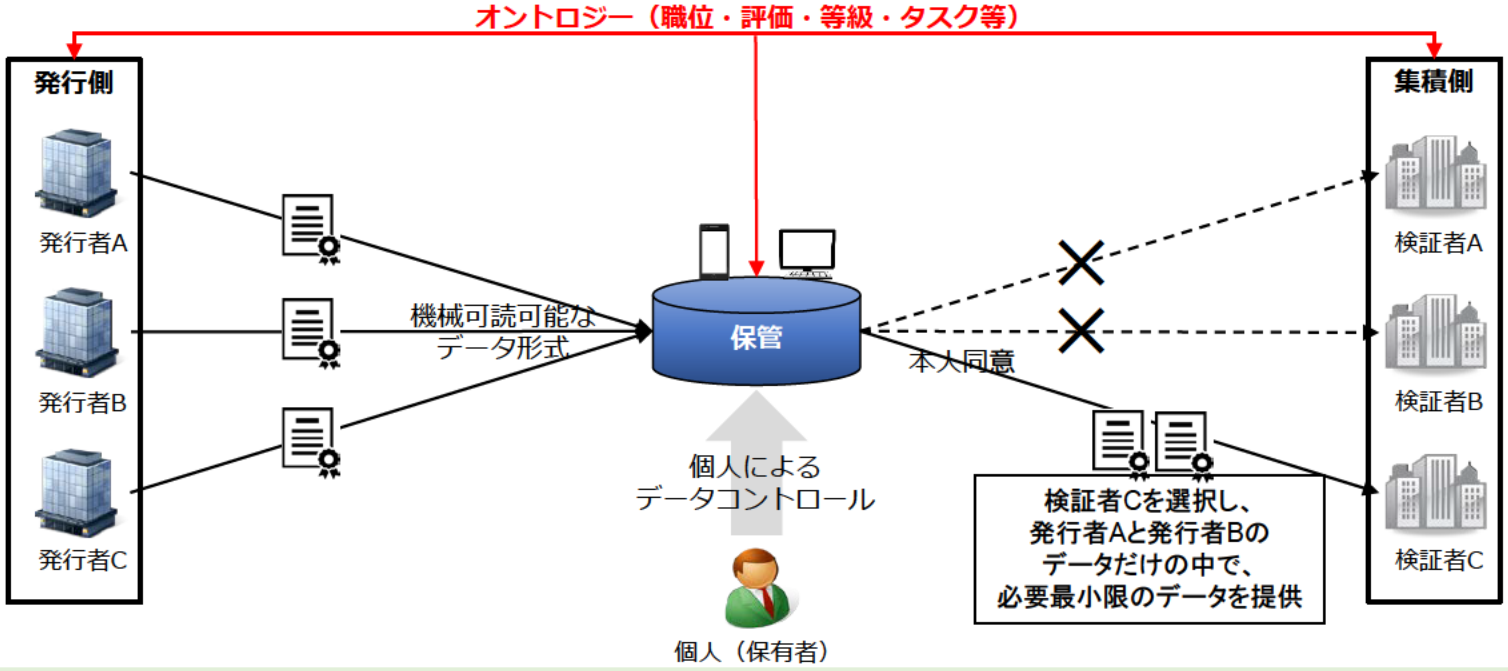
- 日本では、個人の活動履歴を連携することを前提にデータとして管理されていない。そのため、個人の活動履歴をデータで提供する取り組みも進んでいない。
- その理由として、個人の活動履歴データの形式や構造、および実装する機能等が定まっていないことが挙げられる。



- 円滑な個人の活動履歴データの流通のために、構造化され、一般的に利用される機械可読可能な形のデータ形式や構造、実装する機能等の整理が必要ではないか。
- その際、海外の取組（OpenBadges、Blackcerts、W3CのVerifiable Credentialsなど）ではJSON形式を採用しているが、グローバルな人材交流が想定される未来において、海外で採用されているデータ形式の採用を検討するべきではないか。

オントロジーの在り方

- 例えば、転職を想定し、在籍していた企業が発行者となり、職務等に関する個人の活動履歴データが提供された場合、転職先となる企業（検証者）が転職希望者よりデータを受け取ったとする。
- この際、保有者・発行者・検証者の間において、職位・評価・等級・タスク等についての共通理解がなければ、保有者は発行者が記載した内容について誤解をする可能性があり、システム間でのデータ利用が難しいと考えられる。



- 職位・評価・等級・タスク等について、保有者・発行者・検証者が共通理解を持つための標準的な基準策定が求められる。
- そのために、日本版O*netや日本標準職業分類などをより精緻化し、職位・評価・等級・タスク等の標準的な基準策定を進めるべきではないか。

（参考）海外からの人材獲得のために

海外まで視野に入れたオントロジーや職業分類の在り方を整理することで、海外人材の獲得が進むことが考えられる。

その例を、以下に示す。

■ 個人の活動履歴の国際標準化

- 欧州では、各国で発行される資格・学位等の標準化に取り組んでいる。（右図参照）
- その基準は、「知識」「技能」「能力」の３つの指標に大別され、それぞれレベル分けが行われており、各国はこの基準に沿うように、自国の資格・学位を整理している。
- 欧州では、欧州全体での資格・学位等の比較が容易になることが期待されている。

■ 職務・資格の関係性の整理

- アメリカでは、O*netやSOC（Standard Occupational Classification）などのオントロジーやフレームワークが精緻化されており、各職種で求められるスキルが明確になっている。
- このため、職種に応じた資格や学習講座などが整備されており、希望する就職・転職先で求められるスキルを事前に獲得することができる。
- 個人は、希望する職種に必要なスキルを事前に獲得できるので、就職・転職の際に、必要なスキルを持っていることをアピールすることが可能になっている。

水準	知識	技能	能力
	EQF と関連して，理論的知識及び／又は事実的知識としての知識が記述される。	EQF と関連して，（論理的，直感的，創造的な思考を用いながら）認知的な技能としての技能が記述される。	EQF と関連して，責任感と自律という意味で能力が記述される。
1	基礎的な一般知識を持っている	簡単な課題を遂行するのに必要な基礎的な技能を持っている	体系的な背景において直接的な指導を受けながら仕事又は学習できる
2	仕事又は学習の分野における基礎的な事実的知識を持っている	課題を実行し，かつ簡単なルールや道具を用いながら日常の問題を解決する上で，重要な情報を利用するのに不可欠となる基礎的な認知的技能及び実践的技能を持っている	監督を受けながら，ある程度の責任感を持って仕事又は学習できる
3	仕事又は学習の分野における事実，原則，方法，一般的概念に関する知識を持っている	基礎的な方法，道具，材料，情報を選別して用いる場合に，課題を片付け，かつ問題を解決するための認知的技能及び実践的技能を一通り持っている	仕事上の課題又は学習上の課題を責任を持って片付けることができる
4	仕事又は学習の分野における理論的知識や事実的知識を幅広く多様に持っている	仕事又は学習の分野における特殊な問題を解決するための認知的技能及び実践的技能を一通り持っている	通常は予測可能だが変化する可能性のある，仕事又は学習背景を規定する行動要因の中で，自主的に行動管理をすることができる 仕事又は学習の活動の評価及び改善に対して一定の責任を引き受け，他者の日常の作業を監督することができる
5	仕事又は学習の分野における包括的で特殊な理論的知識及び事実的知識，並びにこれらの知識の境界に対する意識を持っている	抽象的な問題を創造的に解決する上で必要となる，包括的な認知的技能及び実践的技能を持っている	予測できない変化が起こるような仕事又は学習背景の中で，指導し監督することができる 自らの成果と他者の成果を吟味し発展させることができる
6	理論や原則に対する批判的な理解を伴った，仕事又は学習の分野における進歩的な知識を持っている	専門的技能や技術革新的能力を自在に使いこなせることを証明し，かつ特殊な仕事及び学習の分野における複雑で予測不可能な問題を解決するのに必要となる進歩的な技能を持っている	複雑な専門的あるいは職業的な活動又はプロジェクトを監督し，予測不可能な仕事又は学習背景において決定責任を引き受けることができる 個人及び集団の職業上の発展に対する責任を引き受けることができる
7	部分的には仕事又は学習の分野における最先端の知識と結び付き，かつ技術革新的な思考的試み及び／又は研究の基盤となる，極めて特殊化された知識を持っている ある仕事又は学習の分野の問題に対する，また様々な分野に共通する事項への批判的な意識を持っている	新たな知識を獲得し，新たな方法を開発し，様々な分野の知識を統合する上で，研究及び／又は技術革新の分野における特殊化された問題解決技能を持っている	新たな戦略的アプローチを必要とする複雑で予測不可能な仕事又は学習背景を監督し，形成することができる。 専門的知識及び職業実践への寄与及び／又はチームの戦略的なパフォーマンスの反省に対する責任を引き受けることができる
8	ある仕事又は学習の分野における，また様々な分野に共通する先端的知識を持っている	統合や評価を含め，研究及び／又は技術革新の分野における中心的な問題提起を解消し，また手元にある知識又は職業的実践を拡大又は再定義するための最も先端的で特殊化された技能及び方法を身に付けている	仕事を含め，指導的な仕事又は学習背景における新たなアイディアや手法を開発するにあたり，相当の権威，技術革新能力，自律性，学術と職業の不可侵性，継続的な参加が認められる

非機能面

⑤UX向上

- UX向上につながるニーズ
- UX向上に必要な要素

UX向上につながるニーズ

■ アンケート調査から分かったニーズ

➢ 企業が把握したい個人の活動履歴について

- **「担当業務で取得した知識・スキルの内容やレベル」「社外の研修やセミナーの受講履歴」**を把握したいという強いニーズが存在することが分かった。
  - 資格・スキル・経験等の個人の活動履歴の把握が進んだ企業においては、自社の人材マネジメントの向上を通して、企業が成長するという大きな経済効果があることも明らかになった。

➢ 標準化について

- 個人の能力等を形成する業務上での経験（**職歴・プロジェクト等**）については、その活用のために、**標準的指標や具体的な内容を可視化してレベル・水準を把握できる仕組みが必要**であることが分かった。

■ 検討会・ヒアリング調査から分かったニーズ

➢ ニーズのある個人の活動履歴

- **犯歴**のデータを紐づけることで、**企業のセキュリティ向上**を図れるのではないか。
  - 但し、二重処罰に該当しないか、更生の機会を奪わないかというバランスが大事であり、再チャレンジの余地を残すことに最大限の配慮が必要

➢ 個人の活動履歴の利用方法

- フリーランスや個人経営者は、独立した時点で信用度がリセットされるため、融資を受ける事が困難であることから、個人の活動履歴データを**与信のために利用**したい。

➢ 個人によるデータ管理

- 副業・兼業が当たり前になると、A社の立場とB社の立場、労働者の立場と事業者の立場など、複数の立場や帰属先を持つことになる。これまでは個人と組織が１対１で、帰属先ごとに職務経歴や税を徴収するための情報を管理してきたが、これからは**個人の帰属先が増えていくので、個人を軸に一元管理することが必要**になっている。

➢ 海外人材獲得

- 海外人材獲得のためには、海外のプラットフォームとのインターオペラビリティを意識しておくことが必要。

➢ その他

- 未経験者の場合、企業は経験者を欲しいと考えているので、なかなか採用に結び付かない。そこで、職業訓練を受けたり、資格を取得した後に、**実習訓練を行うなどのサポートが必要**ではないか。

UX向上に必要な要素

■ プライバシーの在り方、データ形式・構造、オントロジーの在り方、アンケート／ヒアリング調査、および検討会での議論を踏まえ、人生100年時代に継続して利用される**個人中心の社会基盤に求められる要素**を整理すると、以下のように整理される。

要素	説明
透明性（Transparent）	オントロジー／フレームワークに基づき、明確に定義され、比較が可能で、共有され、共通の言語/記述で記載された情報を提供することで、個人の活動履歴の透明性が担保される。
平等（Equitable）	様々な資格・スキル等を持つ人々が、資格・スキル等を等しく提示できるようになることで、縁故等によらず、等しく機会を得ることが可能になる。
制御（Controllable）	保有者が指定した関係者、目的、期間に対してのみ、必要な個人の活動履歴が提供する権限を持つ。また、提供される個人の活動履歴は、保有者の同意の下、限定された範囲・目的の中で利用される。
アクセス（access）	保有者は、いつでも自身の活動履歴にアクセスできる。 例えば、発行者が存在しなくなった場合のようにアクセスが失われた場合には、正当に発行された活動履歴の信頼できる記録を直接入手して、他の手段でクレデンシャルを回復したり、アクセスしたりすることができなければならない。
安全（Secure）	不正な編集やアクセスからデータを保護するために、関連するセキュリティ基準に準拠する。
ポータブル（Portable）	構造化され、一般的に利用される機械可読可能な形のデータ形式や構造、実装する機能等の整理され、保有者は、自分の利用目的のために、個人の活動履歴を持ち運べるようになる。
相互運用性（Interoperable）	共通のオントロジー/フレームワークに基づき、システム間で、データを機械で読み取り、交換し、実行できる。また、複数の発行者からのデータの組み合わせを可能にする。
共有可能（Shareable）	保有者が就職・転職等に応募する際に共有できるようにする。
検証可能（Verifiable）	発行者によって発行された個人の活動履歴データが、真正であることをデジタル的に確認することができる。

未来の社会基盤イメージ（案）

- 未来の社会基盤イメージについて
- 長期的な視点による未来の社会基盤イメージ（案）
- 短・中期的な視点による未来の社会基盤イメージ（案）
- 政府に求められること、民間で推進すべきこと

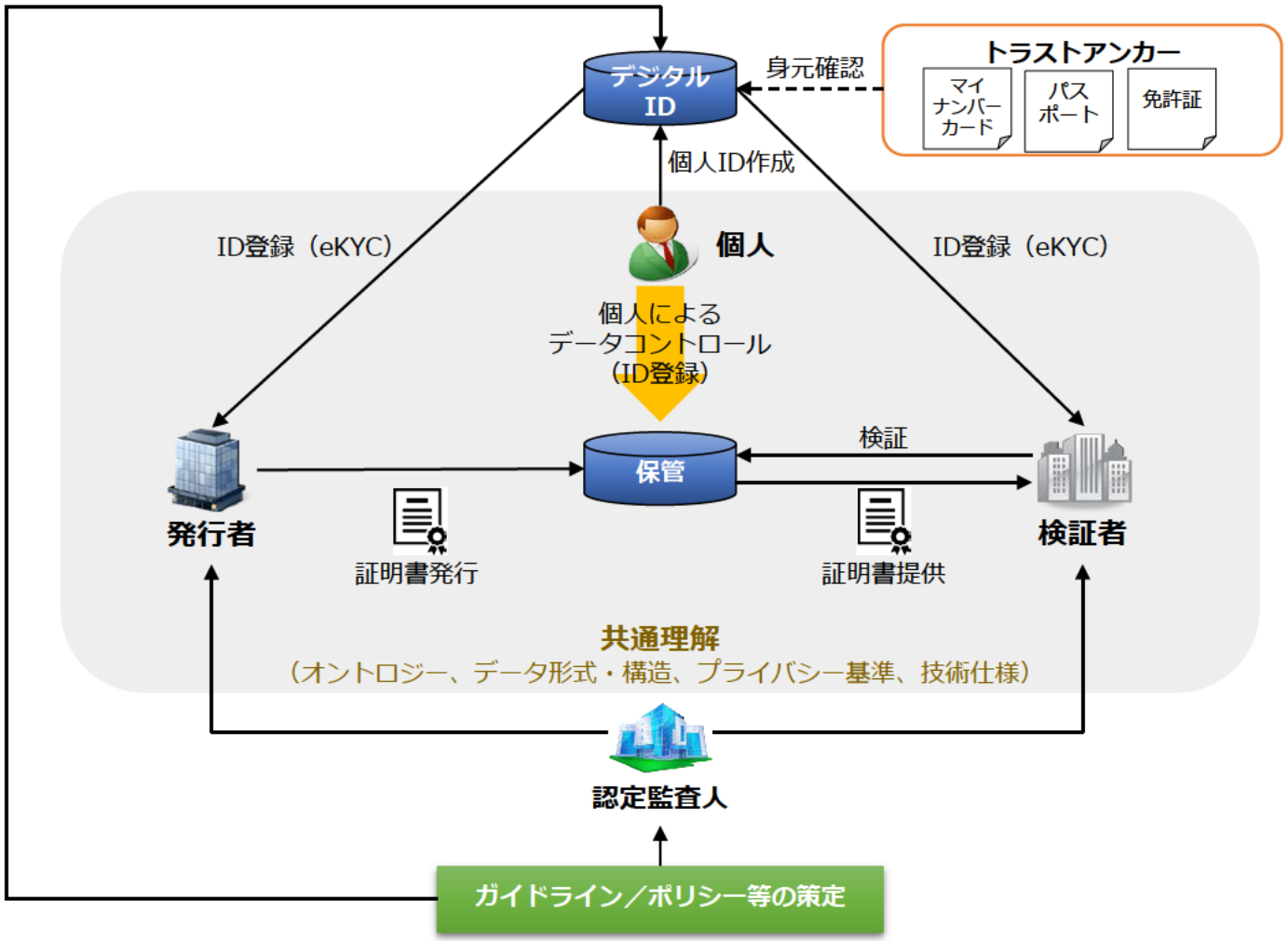
未来の社会基盤イメージについて

- これまでの調査において、以下の内容を確認してきた。
  - 機能面
    - ① 個人の特定と認証
      - eKYCとデジタルIDインフラの構築
    - ② 個人データの連携方法
      - アイデンティティ管理の累計と個人データの証明可能な連携方法の類型
    - ③ 個人データの認証方法
      - 活動履歴のライフサイクルにおける個人データの認証方法
  - 非機能面
    - ④ 個人データの扱い方
      - プライバシー、オントロジーの在り方とデータ形式・構造
    - ⑤ UX向上
      - UX向上につながる様々なニーズと求められる要件

- 上記を踏まえ、次ページ以降に、長期的な視点で目指すべき未来の社会基盤イメージ（案）を示すとともに、その社会基盤イメージに至る過程として、短・中期的な視点で実現すべき社会基盤イメージ（案）を示す。

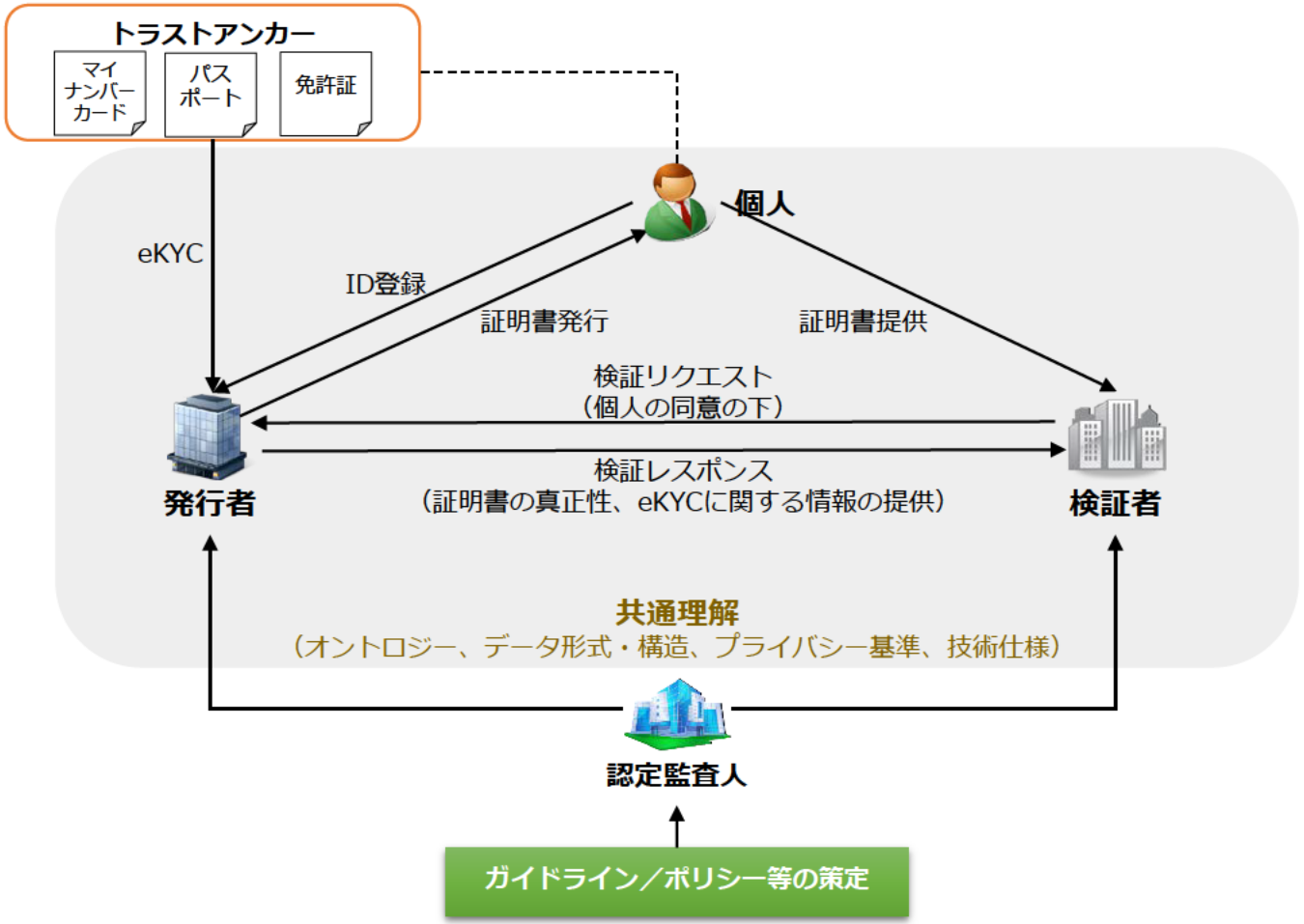
長期的な視点による未来の社会基盤イメージ（案）

- 個人中心の社会基盤として、個人が自らのデジタルIDを作成し、個人の活動履歴データのコントロールを行う。
- 但し、現状では、デジタルIDの仕組みや、アイデンティティの利用における責任も個人がすべて請け負うことになることへの対応など、未整備な部分も多い。



短・中期的な視点による未来の社会基盤イメージ（案）

- 長期的な視点での社会基盤イメージでは、未整備な課題が状況である。
- そこで、長期的な視点での社会基盤イメージを目指しつつ、まずは、既に活用可能な技術を用いて、eKYCとID連携を進めるとともに、発行・保管・共有・検証されるデジタル証明書に関するオントロジー・データ形式・プライバシー基準等の整備を進めることがよいのではないかと考えられる。
- 上記の点を踏まえ、長期的な視点の社会基盤イメージに至る前段として、短・中期的な視点による未来の社会基盤イメージを以下に示す。



政府に求められること、民間で推進すべきこと

- 短・中期的な視点による未来の社会基盤イメージの実現を進めつつ、長期的な視点による未来の社会基盤イメージを前提とした継続的な取組として、「政府に求められること」と「民間で推進すべきこと」には、以下のようなことが考えられる。
- なお、大前提として、各種証明書のデジタル化が進んでいないことが、こうした個人の活動履歴のプラットフォームを構築していく上でのボトルネックともなっており、官民共にデジタル化を一層推進していくことが望まれる。

事務局整理（案）	
政府に求められること	• 資格・証明書のデジタル化推進 • ガイドライン／ポリシー等のルールや技術仕様の検討 • マイナンバーカード等を用いたeKYC／デジタルIDの仕組み・ルールの検討 • 資格等の活動履歴データの質を保証する仕組み・ルールの検討 • 個人の活動履歴データの国際連携の橋渡し
民間で推進すべきこと	• 資格・証明書のデジタル化促進 • 発行資格の正しさを証明する機能の開発と社会実装 • eKYCを念頭に置いた身元確認の基準策定 • eKYC／デジタルIDの開発と社会実装 • 民間企業・団体が求める人材情報の整理と標準化 • オントロジーや職業分類に関する整理と共通理解に向けた調整 • 国際連携を阻害しない、相互運用可能な社会基盤の開発と社会実装 • プライバシーに配慮した個人情報の取扱いの徹底

検討会概要

■ 人生100年時代／ポストコロナ時代の個人の活動履歴の在り方検討会

➢ 労働市場のより一層の透明性向上（安全性の確保）と活性化を実現するとともに、デジタル化の進展等に応じた「個人」の多様なスキル向上や学び直しの機会の拡大、またこれに伴う精緻で個人主体の人材に関する新規事業の創出や社会保障の充実等へとつなげていくことを目的に、有識者・発行者・集積者からなる検討委員会を設置した。

委員一覧

（※五十音順･敬称略）

氏名	所属	立場
板倉 陽一郎	ひかり総合法律事務所 弁護士	有識者
海老沼 貴明	日本電気株式会社　人材組織開発部　主任	集積者
加藤 茂博	株式会社リクルートキャリア ビジネスプロデューサー	有識者・集積者
川口 かおり	ウォンテッドリー株式会社 執行役員	集積者
岸上 順一	慶応義塾大学大学院政策・メディア研究科 特任教授、W3C/Keio Deputy Director	有識者
楠 正憲（座長）	Japan Digital Design株式会社 CTO	有識者
倉持 和宏	独立行政法人情報処理推進機構　IT人材育成センター　国家資格・試験部長	発行者
黒坂 達也	慶応義塾大学大学院政策・メディア研究科 特任准教授	有識者
崎村 夏彦	NATコンサルティング合同会社　代表社員	有識者
田渕 仁志	一般財団法人国際ビジネスコミュニケーション協会 管理本部 本部長	発行者
中村 素典	京都大学　情報環境機構 教授	有識者
平田 麻莉	一般社団法人プロフェッショナル&パラレルキャリア・フリーランス協会　代表理事	集積者
宮澤 賀津雄	一般社団法人人材育成と教育サービス協議会　ISO/TC232国内審議委員会　委員長	有識者
村上 臣	リンクトイン・ジャパン株式会社　日本代表	集積者

検討会開催概要

回数	日程	議事
第１回	2020年12月25日（金）9時～11時	1．事業の説明（経済産業省） 2．個人の「活動履歴」の範囲・種類の特定（事務局） 3．アンケート／ヒアリング調査の実施案（事務局）
第２回	2021年1月29日（金）9時～11時	1．海外調査報告（事務局） 2．アンケート／ヒアリングの中間報告（事務局）
第３回	2021年3月3日（水）16時～18時	1．活動履歴データのガバナンスイノベーション（事務局） 2．未来の社会基盤イメージ（案）（事務局）