日本総研
The Japan Research Institute, Limited

デジタルアイデンティティの動向と展望

~デジタル証明書技術の進展と個人・企業での活用見通し~

(株)日本総合研究所
先端技術ラボ

2025年8月28日

本資料に関するお問い合わせ 市原紘平 (ichihara.kohei@jri.co.jp)

本資料は作成日時点で一般に信頼できると思われる情報に基づき弊社が作成したものですが、情報の正確性・完全性を保証するものではありません。記載内容は経済情勢等の変化により変更されることがあります。
本資料の情報に起因してご閲覧者様及び第三者に損害が発生したとしても、執筆者、執筆にあたっての取材先及び弊社は一切責任を負わないものとします。本資料の著作権は株式会社日本総合研究所に帰属します(引用部分を除く)。

© 2025 The Japan Research Institute, Ltd. (except where indicated)

日本総研
The Japan Research Institute, Limited

サマリ -デジタルアイデンティティの動向と展望-

- 先行する欧州での議論
  - ✓ 欧州では、個人と法人を一体的、かつ様々なトラストサービスについて網羅的に検討が行われた上で規則として発効し、実現の期限も設ける形で社会実装を早期に進めようとしている。

- 日本でのトラストサービスに関する議論
  - ✓ トラストサービスのような公共～準公共のトピックについては、政府が早期に指針を打ち出すことが望まれる。新サービスの検討に取り組む民間企業は、政府がソリューションを用意する公共分野であるのか、各企業でサービスを検討する競争領域となるのかが判然としないと事業検討が難しい。取り組んだ分野が公共サービスで上書きされると投資が無駄となる。

- 進み始めた日本での社会実装
  - ✓ 日本では、デジタル庁主導で個人の身分証明の分野での社会実装が急速に進んでいる。
  - ✓ 今後「mdoc発行管理システム」(p.6)の提供が開始し、様々なデジタル証明書が発行されることが期待される。

- 技術動向
  - ✓ 証明書フォーマットにおいても、提示のプロトコルにおいても、選択的開示(p.10)が利用できる技術標準が採用されつつある。
  - ✓ しかしながら、アイデンティティウォレットアプリに提示する属性を選択するUIが無ければ利用することができない。デファクトスタンダードとなりうるスマホOSのアイデンティティウォレットに選択的開示を利用できるUIが実装されることが望まれる。

- 今後の展望
  - ✓ 今後、人に変わって様々な処理を行うAIエージェントや物理的なロボットが社会に増えてくると、それらの身元を確認するためのアイデンティティ証明書についての議論も深めていく必要が考えられる。EIC 2025(European Identity and Cloud Conference 2025)等で先行した議論がなされている。[1]

[1] https://tech.gmogshd.com/catchup-eic-arf-2025/

© 2025 The Japan Research Institute, Ltd. (except where indicated)

日本総研
The Japan Research Institute, Limited

目次・用語集 -デジタルアイデンティティの動向と展望-

© 2025 The Japan Research Institute, Ltd. (except where indicated)

1. デジタルアイデンティティに関する動向の概要

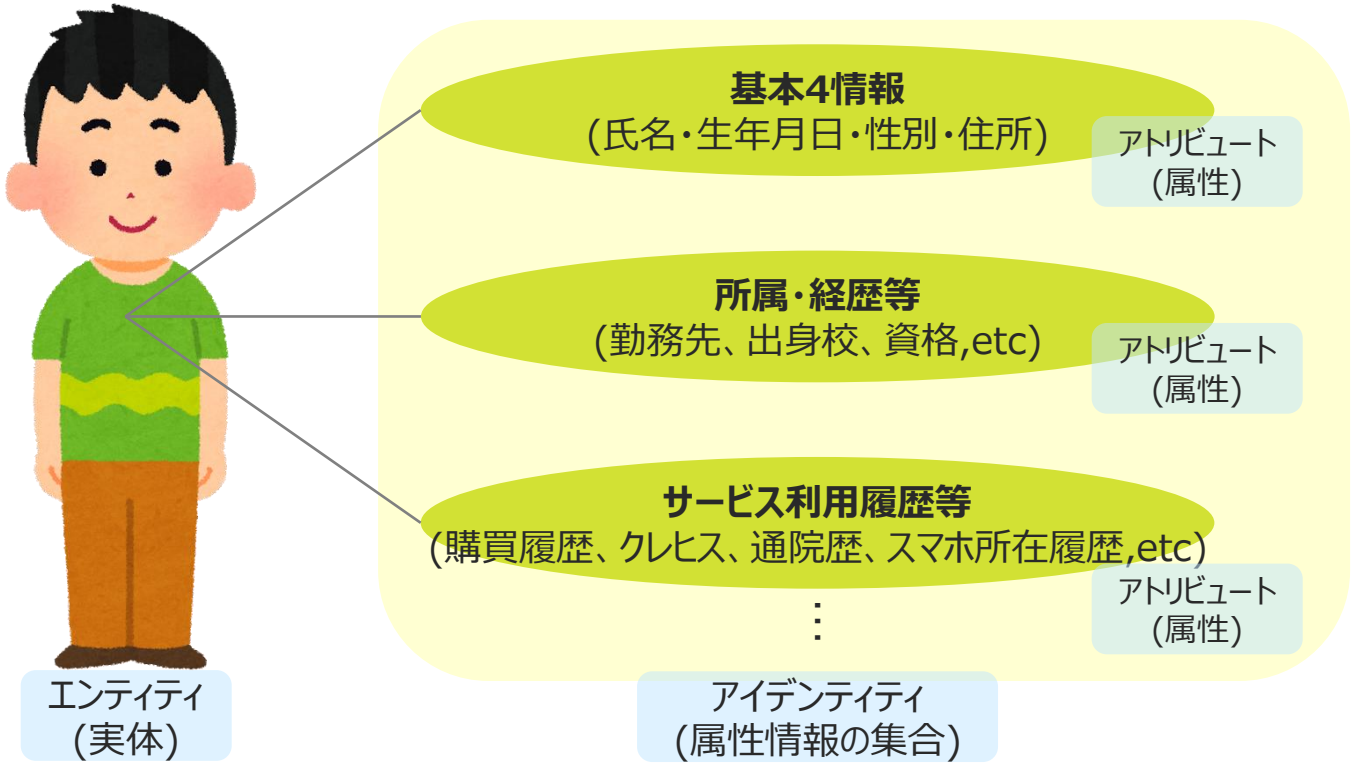
1.1 アイデンティティとは
1.2 社会実装が進むアイデンティティのデジタル証明書とIHVモデル
1.3 マイナンバーカードの属性情報のスマホ搭載
1.4 欧州で進む法人のデジタルアイデンティティ整備
1.5 デジタルデータの発出元法人を示すeシールの普及

© 2025 The Japan Research Institute, Ltd. (except where indicated)

日本総研
The Japan Research Institute, Limited

1.1 アイデンティティとは

- アイデンティティとは、『実体に関する属性情報の集合』(国際標準化機構(ISO)による定義)[1]
- 「ISO/IEC 24760-1:2019 Information security, cybersecurity and privacy protection」[1]では、関連用語が以下のように定義される。
  - エンティティ(entity)：明確に存在が区別されるドメインの運用目的に関連するアイテム
  - アトリビュート(attribute)：エンティティの特性または性質
  - アイデンティティ(identity)：エンティティに関連するアトリビュートの集合



[1] https://www.iso.org/standard/77582.html

© 2025 The Japan Research Institute, Ltd. (except where indicated)

日本総研 The Japan Research Institute, Limited

1.2 社会実装が進むアイデンティティのデジタル証明書とIHVモデル

- アイデンティティ(属性情報の集合)を他者に提示するためのデジタルデータとして、デジタル証明書やVerifiable Credentials(VC, 検証可能な資格証明)と呼ばれる技術が進展・普及してきている。
  - ➢ アイデンティティのデジタル証明書の活用では、IHVモデル(Issuer-Holder-Verifierモデル)が想定されている。
- IHVモデル(Issuer-Holder-Verifierモデル)とは、デジタル証明書の活用に関し、Issuer(発行者)、Holder(保有者)、Verifier(検証者)の3者を想定するモデルである。(three party modelとも呼ばれる)

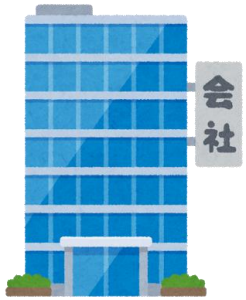
発行者(Issuer)
例：大学

発行
(Issue)

デジタル証明書(VC)
例：卒業証明書

保有者(Holder)
例：求職者

提示
(Presentation)



検証者(Verifier)
例：企業

- ✓ デジタル証明書では、各仕様で規定されるデータフォーマットに発行者の秘密鍵で署名がされる。
- ✓ 検証者は発行者の公開鍵で署名検証することで、発行者の証明書であると確認できる。(公開鍵の公開方法は様々)

- ✓ デジタル証明書(VC)として、標準化されたデータ形式やデジタル署名、検証プロトコルを用いることで、社会全体で効率的なシステムを構築できる。
  - ➢ なお、Verifiable Credentials(VC)という用語は、W3Cが策定する具体的な1つの技術仕様を指す場合もあるが、デジタル証明書全般(W3C VC以外の仕様も含む)を指す意味でも用いられている。
- ✓ 国際標準的なプロトコルに基づき共通的な形式のデータを発行することで、発行者と検証者が直接繋がることなく、アイデンティティを証明できる。
- ✓ 紙の証明書と違い、発行後に失効させることができるメリットも存在。(証明書失効リスト(CRL)に登録することで検証が失敗する)

© 2025 The Japan Research Institute, Ltd. (except where indicated)

日本総研 The Japan Research Institute, Limited

1.3 マイナンバーカードの属性情報のスマホ搭載

- 日本ではマイナンバーカードに記録された個人の属性情報をスマホに保存し、本人の意志で提示できるようになる。(オンライン送信含む)
  - スマホに保存される情報は基本4情報(氏名・住所・生年月日・性別)とマイナンバーと顔写真で「カード代替電磁的記録」と呼ばれる。
  - 「カード代替電磁的記録」は、デジタル証明書の国際標準規格の1つであるISO18013-5のmdoc data modelに準拠。[1]
  - 加えてデジタル庁は、mdoc形式のデジタル証明書を発行・管理できる「mdoc発行管理システム」を構築、運営することを公表。[1] 証明書の発行主体が共同で利用できるようにすることで、各主体の独自構築を不要にし社会のデジタル化を推進できるとしている。
- アイデンティティに関するデジタル証明書を保管するためのソフトウェアは、デジタルアイデンティティウォレット(DIW)と呼ばれる。
  - 個人のアイデンティティ証明書をスマホで管理する場合、決済やポイントプログラム利用等で既に普及しているスマホOS内蔵のウォレットソフトウェアが、機能を拡充する形でDIWとして利用されることが想定されている。(Apple Wallet, Google Wallet等)
  - マイナンバーカードの属性情報スマホ搭載では、Apple Walletが同情報を取り扱うための認定を取得済(2025/8/5現在)。[2]

✓ mdoc発行システムが提供されることで、様々な民間発行のデジタル証明書が簡単に発行できる。

✓ 個人がデジタル証明書を保管するのには、既存のスマホのウォレットソフトウェア等が使用される。

✓ 企業側から必要なデジタル証明書を照会(徴求)することができる。(p.12に記載)

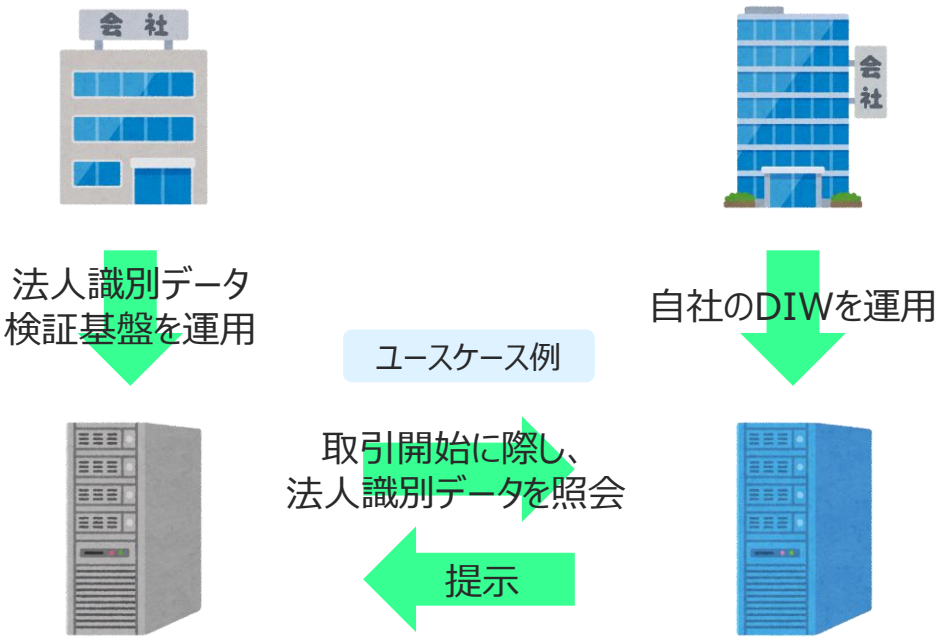
[1]デジタル庁 国民向けサービスグループ, "マイナンバーカード機能のスマホ搭載について", デジタル庁, 2024/7/22, https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/fcb737a4-07b9-4abd-bdca-34af9c4f71a5/f6f1ad84/20240913_meeting_smartphone_mynumbercard_outline_01.pdf (accessed on 2025/8/8)
[2]デジタル庁, "カード代替電磁的記録（属性証明機能）", デジタル庁, 2025/8/5, https://www.digital.go.jp/policies/mynumber/mynumbercard-mdoc (accessed on 2025/8/8)

© 2025 The Japan Research Institute, Ltd. (except where indicated)

1.4 欧州で進む法人のデジタルアイデンティティ整備

- 欧州等で企業(法人)についてもデジタルアイデンティティを活用する動きが活発化している。
  - 2024年に成立したeIDAS2.0*規則では、各国の個人のみならず、法人にも「EUデジタルアイデンティティウォレット(EUDI Wallet)を2026年までに提供することが各国に義務付けられた。[1]
  - 法人向けのデジタルアイデンティティウォレットは、サーバ型のウォレットが想定されている。(業務ITシステムとの連携の観点などから、証明書に紐付ける秘密鍵をサーバ上で保管する方式)
  - 個人識別データ(PID)同様、法人にも法人識別データ(LPID, Legal Person Identification Data)を整備することが制度化。新規顧客企業と商取引を開始する際、相手方の信頼性を確認しやすくなる等の活用が見込まれる。

*eIDAS, **E**lectronic **Id**entification, **A**uthentication, and Trust **S**ervices



政府主導で法人向けウォレットソフトウェアを整備(欧州)

- ✓ eIDAS2.0規則により、法人向けにもDIWを整備することが各国に義務付け。
- ✓ サーバ型ウォレットの要件等が規定されている。(用途に応じて段階的なセキュリティを要求。p.15で解説)
- ✓ 法人識別データ(LPID)を構成する「電子属性証明(EAAs, Electronic Attestation of Attributes)」は情報の信頼性が求められる。要件を満たすEAAが適格EAA(QEAA, Qualified EAA)と呼ばれる。

[1]European Commission, "Electronic identification and trust services including e-signatures (RP2025)", Interoperable Europe Portal, https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/electronic-identification-and-trust-services-including-e-signatures-rp2025 (accessed on 2025/8/8)

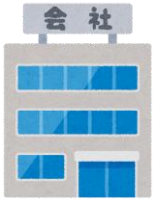
© 2025 The Japan Research Institute, Ltd. (except where indicated)

日本総研
The Japan Research Institute, Limited

1.5 デジタルデータの発出元法人を示すeシールの普及

- 法人が法人自身の秘密鍵によりデジタル署名(暗号学的署名)を行うことで、*
  デジタルデータの起源(発出元)と完全性(非改ざん性)を確認できるようにするための添付データやその措置をeシールという。
  - 日本では「電子社印」とも表現され[1]、eシールによりデジタルデータを用いた法人の取引を信頼性をもって行うことができる。
  - eIDAS2.0でも、法人のサーバ上でのリモート電子署名(remote eSig)やeシール作成に関し満たすべき要件等が整理されている。

*電子署名ともいうが、法的な意味での電子署名(意思表示)は自然人にのみ可能とされるためこのように記載。

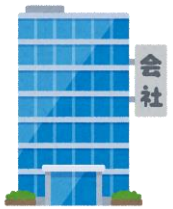


リモート署名・
eシール作成システムを運用

サーバ上でリモート署名
(eシール作成)

eシール済みのデジタルデータを送付

eシールの付与されたデジタルデータ
例：請求書



請求処理・
送金システムなどの運用

- ✓ eシールが付与されていることで、改ざんや発信元偽装の心配がない
- ✓ 標準化されたフォーマットのデジタルインボイスであれば自動処理が可能

[1]日本経済新聞社, “国認定「電子社印」、25年度運用開始　発行業者に8要件”, 日経電子版, 2025/1/30, https://www.nikkei.com/article/DGXZQOUA25AZN0V21C24A2000000/ (accessed on 2025/8/8)

© 2025 The Japan Research Institute, Ltd. (except where indicated)

2. デジタルアイデンティティ技術の概要

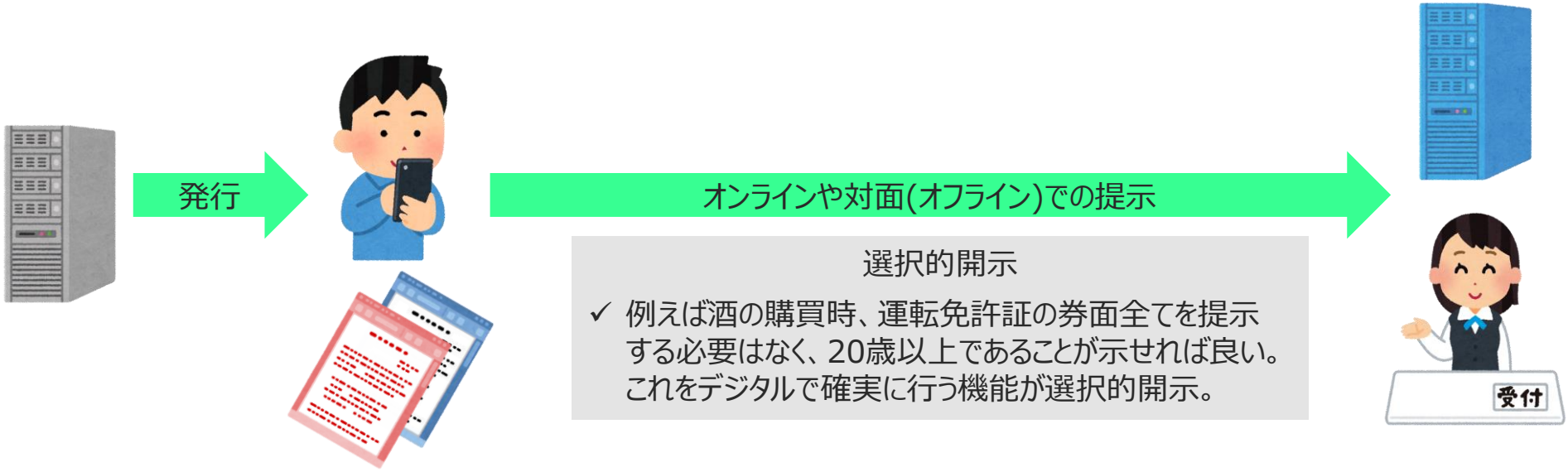
2.1 デジタルアイデンティティ関連技術の構成
2.2 代表的な証明書フォーマット -mdoc/mDLとSD JWT VC-
2.3 証明書の転送に関わる技術 -OID4VCIとOID4VP-

© 2025 The Japan Research Institute, Ltd. (except where indicated)

日本総研 The Japan Research Institute, Limited

2.1 デジタルアイデンティティ技術の構成

- デジタルアイデンティティに関する技術は大きく、
  ①デジタル証明書のフォーマットに関する技術と、②証明書の転送(発行・提示)に関する技術の2つに分けて考えることができる。
- デジタル証明書に特有の技術的トピックとして「選択的開示 (Selective Disclosure)」がある。
  - 「選択的開示 (Selective Disclosure)」とは、デジタル証明書に含まれる情報から保有者が指定したものだけを、暗号技術的に誤りや改ざんがないことを保証できる状態で提示できる機能を指す。



選択的開示

✓ 例えば酒の購買時、運転免許証の券面全てを提示する必要はなく、20歳以上であることが示せれば良い。これをデジタルで確実に行う機能が選択的開示。

①デジタル証明書のフォーマットに関する技術

✓ 次頁で代表的な証明書フォーマットである「mdoc/mDL」と「SD JWT VC」について解説する。

✓ 何れも、選択的開示を利用でき、eIDASで必須対応となっている仕様である。

②証明書の転送(発行・提示)に関する技術

✓ 証明書発行と提示の標準仕様を次々頁で解説する。(OID4VCIとOID4VP)

✓ 提示についてはオンラインの他、オフライン環境を想定しBluetoothやNFC等を用いる方式も想定されている。

© 2025 The Japan Research Institute, Ltd. (except where indicated)

日本総研 The Japan Research Institute, Limited

2.2 代表的な証明書フォーマット -mdoc/mDLとSD JWT VC-

- mdoc(mobile document, エムドック)は、
  運転免許証に関する国際技術標準であるISO/IEC18013 seriesの18013-5で規定されるフォーマット。
  - 運転免許証の証明書モデルmDLのフォーマットとして策定されたものを免許証以外にも活用している。
  - 処理フローから通信規格等まで明確に定義されており、特に免許証の代替としての用途が意識されていたことから、BluetoothやNFC等対面やオフライン環境でのプロトコルまで規格化されている。
- SD JWT VCは、JSONデータに署名や暗号化を施す方法を定めた標準であるJWT(JSON Web Token, ジョット)をベースに、SD(Selective Disclosure, 選択的開示)の機能を付与したフォーマット。インターネットに関する標準化団体IETFにより策定。
  - 対面やオフライン含め、提示のプロトコルは規格化されていないため、実装は別途行う必要がある。(後述するOID4VP等で可能)
- 一般に、mdocはスマホやオフライン用途、SD JWT VCはWeb標準技術との親和性からオンライン用途に向くとされる。
  しかしmdocにもサーバに格納する選択肢が存在し[1]、各用途で仕様の選択肢が限られるわけではない。

	mdoc	SD JWT VC
標準	ISO/IEC 18013-5	IETF / W3C VC
データ形式	バイナリ形式*のため軽量でIoT機器等にも向く *CBOR(Concise Binary Object Representation)	JSON
署名方式 (Secure Mechanism)	COSE (CBOR Object Signing/Encryption)	JOSE (JSON Object Signing/Encryption)
選択的開示	利用可能	利用可能
主な利用環境・ユースケース	スマホ、オフライン(NFC, QR, BLE)、対面での提示	オンライン提示、クラウド上での鍵管理
強み	高セキュリティ、オフライン対応	Web標準との統合、実装の容易さ

[1]TOPPAN株式会社, “令和4年度補正 Trusted Web 開発等推進事業に係る調査研究（規格・実装動向調査）”, 首相官邸ホームページ, 2024/3, https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/2023seika/files/002_report_technical_standard_agenda.pdf (accessed on 2025/8/8)

© 2025 The Japan Research Institute, Ltd. (except where indicated)

日本総研 The Japan Research Institute, Limited

2.3 証明書の転送に関わる技術 -OID4VCIとOID4VP-

- OID4VCI(OpenID for Verifiable Credential Issuance)は、VCの発行プロセスについての技術標準。
  - OpenID Foundation(OIDF)により策定。OIDFはOAuth2.0やOpenID Connect (OIDC)といったデジタルアイデンティティ関連技術やFAPI(Financial API)の標準化で知られる国際標準化団体。
  - 認可プロトコルのOAuth2.0やOIDCをベースとする。mdoc, SD JWT VCの両方を発行可能。
- OID4VP(OpenID for Verifiable Presentations)は、OIDFによるVCの提示プロセスについての技術標準。提示のフローは以下。

(1) 検証者が「この情報を提示せよ」というリクエスト(VP Token Request)を送る。
(2) VC保有者がDIW内のVCを選択、更に提示する属性情報も選択可能。(選択的開示を利用可能)
(3) Verifiable Presentation(VP Token)として保有者の署名をして検証者へ送る。(中身はVCを含むJWT/CBORオブジェクト)
(4) 検証者は発行者の署名を検証してVCの正当性を確認。

また、提示のユースケースに応じて3つのフローが定義されている。(下表)

OID4VPで定義される3つの提示フロー

	概要	内容
Same Device Flow (同一デバイスフロー)	✓ 単一のデバイスで完結するケースのためUXがシンプル	✓ OID4VPを実行するソフトウェアとDIWが同一デバイス上に存在する場合(同一スマホ上など)に、アプリ間でリダイレクトする方式。 ✓ ディープリンクやApp Linkを使用。
Cross Device Flow (クロスデバイスフロー)	✓ デバイスをまたいでVCを提示できる。 ✓ QRコードやone-time session IDを使ってセッションを紐付ける。	✓ OID4VPをPC上で実行し、スマホのDIWのVCを提示する場合など、リダイレクトの代わりにQRコードを使用して連携する。 ✓ PC上に表示されたQRコードをスマホでスキャンすることでURIを取得し、DIWアプリが起動する。
OpenID for Verifiable Presentations over BLE (BLEフロー)	✓ インターネット接続がないが、Bluetoothの近距離通信が使用できる状況で使用できる。	✓ BLE(Bluetooth Low Energy, 近距離無線通信)を活用することで、検証者と保有者のデバイスの片方または両方にインターネットアクセスがない場合でもVPの要求と受信が可能。

© 2025 The Japan Research Institute, Ltd. (except where indicated)

3. 法人のデジタルアイデンティティに関する議論

3.1 eIDASでの法人デジタルアイデンティティに関する議論

3.2 日本での法人デジタルアイデンティティに関する議論

© 2025 The Japan Research Institute, Ltd. (except where indicated)

日本総研 The Japan Research Institute, Limited

3.1 eIDASでの法人デジタルアイデンティティに関する議論

- トラストサービスとは「インターネット上における人・組織・データ等の正当性を確認し改ざんや送信元のなりすまし等を防止する仕組み」
  - eIDAS2.0では、トラストサービス事業者の認定のために国家監督機関(Supervisory Body)を設定し、適格トラストサービス事業者の適合性を評価する機関(Conformity Assessment Body)を指定することを定め監督する。
  - 適合性評価機関(CAB)から認定されたトラストサービス事業者が適格トラストサービスプロバイダ(QTSP)となる。QTSPによる適格電子署名(QES, Qualified Electronic Signature)は手書きの署名と同等の法的効力を持つ。
- eIDAS2.0では、「属性の電子証明」という新設セクション(§9)で、その法的効果、要件等が規定されており、今後詳細化されるであろう法人の属性証明(法人デジタルアイデンティティ)の内容についても注目される。
- また、リモート電子署名やリモートeシールといった法人のオンライン商取引でも重要なトピックについての規定も追加されている。(§4.5)

法人識別データ(LPID)の内容の考察

- ✓ 欧州デジタルIDウォレットアーキテクチャリファレンスフレームワーク(EUDIW ARF)では『信頼できる情報源 (Authentic Sources)』を『自然人または法人に関する属性を含む、法律で認められている、または法律で義務付けられている公的または私的なリポジトリまたはシステム』[1]と説明。
- ✓ 『公的許可および免許、財務および企業データなどの属性』が、『信頼できる情報源』の持つ法人に関わるデータとしては挙げられている。
- ✓ その他、法人識別データ(LPID)に含まれる属性情報については、現状具体的内容は未公表と見られるが、以下のようなものが考えられる。
  - 法人名
  - 所在地・登記住所
  - 法人の法的形態 (株式会社、有限会社等)
  - 法人の公式登録番号や識別子 (登記番号、VAT番号等)
  - 業の許認可・免許、マネジメント体制の認定 (ISO認証、Pマーク等)
  - 代表者情報 (法人を代表する自然人のPIDと紐付ける可能性)

適格電子署名リモート作成(QESRC)の構成

運用	✓ eIDAS2.0では、新たにリモートでの「適格署名・シール作成デバイス(QSCD, Qualified Signature and Seal Creation Devices)」の管理について規定され、QTSPにその運営が認められる。 ✓ キーバックアップは、オリジナル同等のセキュリティで管理し、サービス継続性に必要最小限の数でなければならない。
技術要素	✓ QTSPがリモート署名を実行する際、Signature Activation Module(SAM)が署名者の同意や認証をセキュアに処理。 ✓ 鍵管理はHardware Security Module(HSM)が担う。(Thales社などが機器を販売[2]) ✓ これらの機器はQSCDの認定を得ていなければならない。
認証有効期間	✓ リモート機器の認証有効期間は最大5年間とし、2年ごとに脆弱性評価を実施、未修復の場合は認証を取り消す規定。

[1] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.4.0/ [2] https://cpl.thalesgroup.com/blog/encryption/qualified-remote-signatures-luna-hsms

© 2025 The Japan Research Institute, Ltd. (except where indicated)

3.2 日本での法人デジタルアイデンティティに関する議論

- (一社)デジタルトラスト協議会(JDTF)は2024年に、
『公的法人認証実現に向けた検討～法人取引デジタル空間完結の実現案と普及施策～』[1]を発行した。
  - 『法人の本人特定事項確認をデジタル上で行う仕組みを、公的なトラストサービス「政府TaaS」として一元化する構想』を検討、解決方針として以下などが整理されている。
    - ✓『実印+印鑑証明書等に代わる、法人の証明(電子証明書)をデジタル上で付与できる仕組みの構築』
    - ✓『電子証明書の真正性、法人情報(登記情報、定款、決算情報等)、委任情報等の照会を、デジタル上で行う仕組みの構築』
    - ✓『個人が所属している法人情報をデジタル上で照会する仕組みの構築』
    - ✓『法人代表者から個人へ権限委任をデジタル上で登録・照会する仕組みの構築』
- 総務省は2024年に『eシールに係る指針(第2版)』[2]を発行。2025年度からeシール発行事業者の認定制度を開始する。[3]
  - 『eシールの付与対象となる電子文書等が求める信頼性の度合に応じて、異なる保証レベルのeシールを使い分けることが考えられ、一例として』[2]下図を公開している。

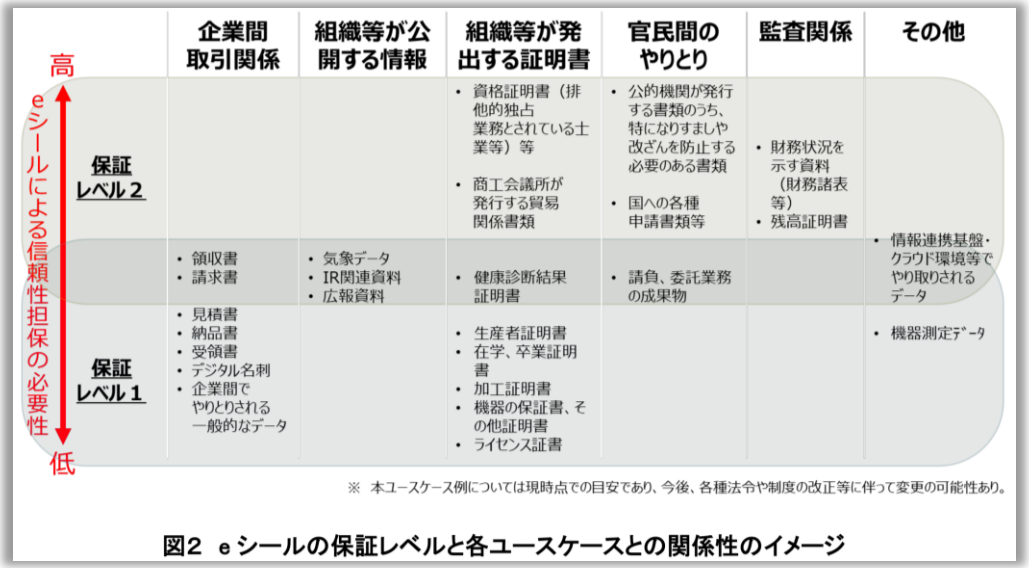


図2 e シールの保証レベルと各ユースケースとの関係性のイメージ [2]

e シールの保証レベル

レベル2

➢ 総務大臣による認定を受けたeシール用認証業務*によって保証され、eシールが付された電子データの起源や改変が行われていないことについて高い信頼が期待される保証レベル。(*認定eシール用認証業務)

レベル1

➢ 認定eシール用認証業務によって保証されてはいないが、より低コスト・簡易な手続で大量発行されるeシールに期待される保証レベル。

[1]https://jdtf.or.jp/report/whitepaper/file/%E5%85%AC%E7%9A%84%E6%B3%95%E4%BA%BA%E8%AA%8D%E8%A8%BC%E5%AE%9F%E7%8F%BE%E3%81%AB%E5%90%91%E3%81%91%E3%81%9F%E6%A4%9C%E8%A8%8E_Ver1.0.pdf
[2]https://www.soumu.go.jp/main_content/000942602.pdf [3]https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/electronic_seal.html

© 2025 The Japan Research Institute, Ltd. (except where indicated)

4. まとめ

4.1 まとめ

4.2 考察・今後の展望

© 2025 The Japan Research Institute, Ltd. (except where indicated)

4.1 まとめ

- 先行する欧州での議論
  - ✓ 欧州では、個人と法人を一体的、かつ様々なトラストサービスについて網羅的に検討が行われた上で規則として発効し、実現の期限も設ける形で社会実装を早期に進めようとしている。

- 日本でのトラストサービスに関する議論
  - ✓ 日本ではトラストサービス関する網羅的な検討の下、実現期限を設けて社会実装を進めるという動きは見られない。
  - ✓ 一方で個別のサービスについては欧州での議論も意識して同様の検討がなされているが、政府が指針を打ち出しているものと民間から提言されているものが混在している。
  - ✓ トラストサービスのような公共～準公共のトピックについては、政府が早期に指針を打ち出すことが望まれる。新サービスの検討に取り組む民間企業は、政府がソリューションを用意する公共分野であるのか、各企業でサービスを検討する競争領域となるのかが判然としないと事業検討が難しい。取り組んだ分野が公共サービスで上書きされると投資が無駄となる。

- 進み始めた日本での社会実装
  - ✓ 日本では、デジタル庁主導で個人の身分証明の分野での社会実装が急速に進んでいる。(iPhoneのAppleウォレットの身分証明書機能を米国外に展開するのは日本が初)[1]
  - ✓ 今後「mdoc発行管理システム」(p.6)の提供が開始し、様々なデジタル証明書が発行されることが期待される。

- 技術動向
  - ✓ 証明書フォーマットにおいても、提示のプロトコルにおいても、選択的開示(p.10)が利用できる技術標準が採用されつつある。
  - ✓ しかしながら、アイデンティティウォレットアプリに提示する属性を選択するUIが無ければ利用することができない。デファクトスタンダードとなりうるスマホOSのアイデンティティウォレットに選択的開示を利用できるUIが実装されることが望まれる。
  - ✓ Google Walletでは年齢確認の際、年齢の値自体は提示先へ秘匿しつつ、条件の値以上であることを暗号学的に証明するゼロ知識証明の技術が搭載され、オープンソース化もされている。[2]

[1] https://www.apple.com/jp/newsroom/2024/05/apple-announces-first-international-expansion-of-ids-in-apple-wallet-in-japan/ [2] https://eprint.iacr.org/2024/2010

© 2025 The Japan Research Institute, Ltd. (except where indicated)

日本総研 The Japan Research Institute, Limited

4.2 考察・今後の展望

- eシールの普及見通し

  安全・円滑な電子商取引を図るための認証スキームに関する取組は古くから存在するが*、
  以下の環境要因などから、今後普及が大きく進む可能性が考えられる。
  - ✓ 欧州でデジタルアイデンティティに関する包括的な議論が進んでおり、データ流通に相互承認したeシールが必要になる可能性がある。
  - ✓ 脱炭素への要請(欧州電池規則等)により、サプライチェーン全体でGHG排出量を把握しなければ、海外で製品の販売ができない可能性が出てきており[1]、製品の製造に関するデータを発出元を確実にした上で流通させる必要がある。
  - ✓ PeppolやJP PINTといった電子請求書の標準仕様策定され、普及してきている。

  *実に四半世紀近く前となる2001年には既に日米欧主要金融機関が出資・参加する電子認証プロジェクト・アイデントラス社の取組があった。[4]

- 日本における法人デジタルアイデンティティの展望
  - ✓ 日本では2025年度からeシール発行事業者の認定制度が開始、国税庁の法人番号を組織識別子として運用がなされる。[2]
  - ✓ 法人のデジタルアイデンティティ証明書発行を仮に民間主導で進めるとすれば、
    eシール発行事業者と信用調査会社や銀行などが協働することが一案として考えられるが、事業としての収益性は未知数である。
    (一社)デジタルトラスト協議会(JDTF)の報告書で指摘されている通り、政府主導の公的なトラストサービスとして提供されると、
    電子商取引や電子委任状のより一層の普及に資するのではないかと考えられる。

- Non-Human Identities(NHI)の議論
  - ✓ Non-Human Identities(NHI)とは、アプリケーションやサービスなど人間以外のエンティティについてのアイデンティティを指す。
  - ✓ 今後、人に変わって様々な処理を行うAIエージェントや物理的なロボットが社会に増えてくると、
    それらの身元を確認するためのアイデンティティ証明書についての議論も深めていく必要が考えられる。
    EIC 2025(European Identity and Cloud Conference 2025)等で先行した議論がなされている。[3]

[1] https://www.ipa.go.jp/digital/architecture/Individual-link/ps6vr7000001m4n6-att/guideline_for_datacooperation_in_BattCFPDD.pdf
[2] https://www.soumu.go.jp/main_content/000942602.pdf [3] https://tech.gmogshd.com/catchup-eic-arf-2025/ [4] https://www.secom.co.jp/corporate/release/2001/nr_20010724.html

© 2025 The Japan Research Institute, Ltd. (except where indicated)

執筆者・先端技術ラボのご紹介

執筆者

市原 紘平
Ichihara　Kohei

シニア・リサーチャー
Senior Researcher

Web3研究に取り組み、2018年からセキュリティトークン等をSMBCグループ内で啓蒙。現在、事業企画への生成AI活用に興味。

■ 執筆レポート

- AI駆動開発とSysEngへのAI適用研究の動向
- EAの活用動向とArchiMateの概説
- 自己主権型アイデンティティの動向と考察
- デジタル証券とRWAトークンの動向　他

■ 学術論文

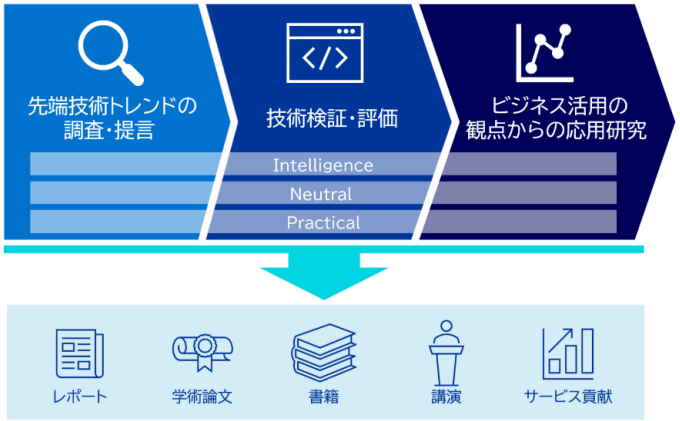
- Practices of Community Vitalization Using SBT (Soulbound Token) and FT (Fungible Token) on Blockchain. (IEEE ICCE 2024) 他

■ 専門委員活動 他

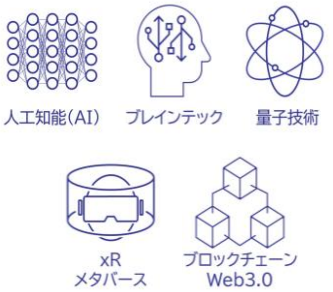
- ISO/TC 68委員会 委員、ISO/TC 68/JWG 1（デジタル通貨） エキスパート

先端技術ラボ

先端技術を活用したITサービスの創出に向けた技術の目利き役として、
「先端技術トレンドの調査・提言」、「技術検証・評価」、
「ビジネス活用の観点からの応用研究」に取り組んでいます。



主な研究・取り組み領域



弊社ホームページの **特集サイト** では、IT分野における先端技術の調査レポート、及び所属する部員のプロフィール詳細がご覧いただけますので、ぜひご参照ください。

本レポート執筆者へのメディア取材や講演などに関するご相談につきましては、当社ホームページの **問い合わせフォーム** よりご連絡ください。

株式会社日本総合研究所

日本総研は、シンクタンク・コンサルティング・ITソリューションの3つの機能を有するSMBCグループの総合情報サービス企業です。

東京本社　〒141-0022　東京都品川区東五反田2丁目18番1号　大崎フォレストビルディング
大阪本社　〒550-0001　大阪市西区土佐堀2丁目2番4号

© 2025 The Japan Research Institute, Ltd. (except where indicated)

日本総研

The Japan Research Institute, Limited