資料4

Verifiable Credential (VC/VDC) の活用におけるガバナンスに関する有識者会議

VCに関連する各種制度等について

令和7年3月10日　　デジタル庁　デジタル社会共通機能グループ　トラスト担当

デジタル庁
Digital Agency

目次

1. 議論対象の整理

1-1. 議論対象のスコープ：Verifiable Credentialの概要

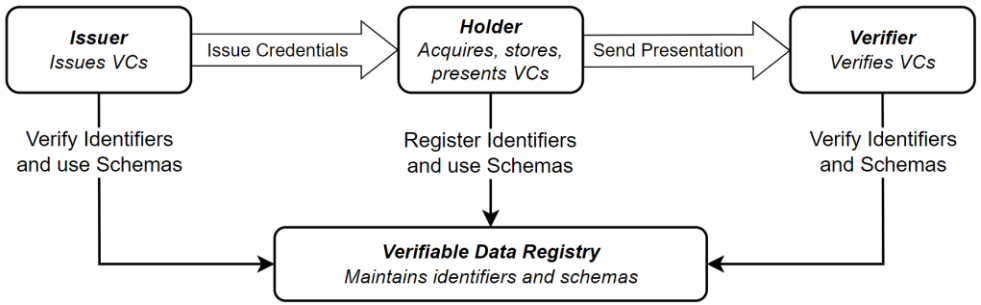
- **Verifiable（Digital）Credential（VC/VDC。以下「VC」とする。）※1はデジタル署名による真正性・改ざん防止等の機能を実現することができる機械可読かつ汎用的なデータ形式（デジタル証明書）及びデータ流通の形態**として、その標準化・実装が進みつつある。

※１：VCという用語は、W3Cにおいて標準化されたVerifiable Credentials Data Modelを指す場合、デジタル署名が付されたデータの真正性・改ざん防止等が検証可能なデータ形式全般（W3C VCDM以外を含む。）を指す場合がある。

- VCは、自己主権型アイデンティティ（SSI：Self-Sovereign Identity）と呼ばれる**「分散型」のアイデンティティ管理を実現する考えを元に発展したコンセプトである Issuer-Holder-Verifierモデル※2 におけるデータ形式として利用することができる。**

※２：下図。頭文字を取りIHVモデル、またはthree party modelと呼ばれる。
また、VCはあくまでデータ形式であるため、IHVモデル以外、分散型ではないデータ流通においても利用することができる。

- VCにDID（Decentralized Identifier、分散型識別子）を組み合わせる、また、検証用の公開鍵（署名検証鍵）の保管場所としてブロックチェーンを用いる例もあるが、これらはいずれも必須ではなく、メリット／デメリットを踏まえ、ユースケースに応じて選択される。



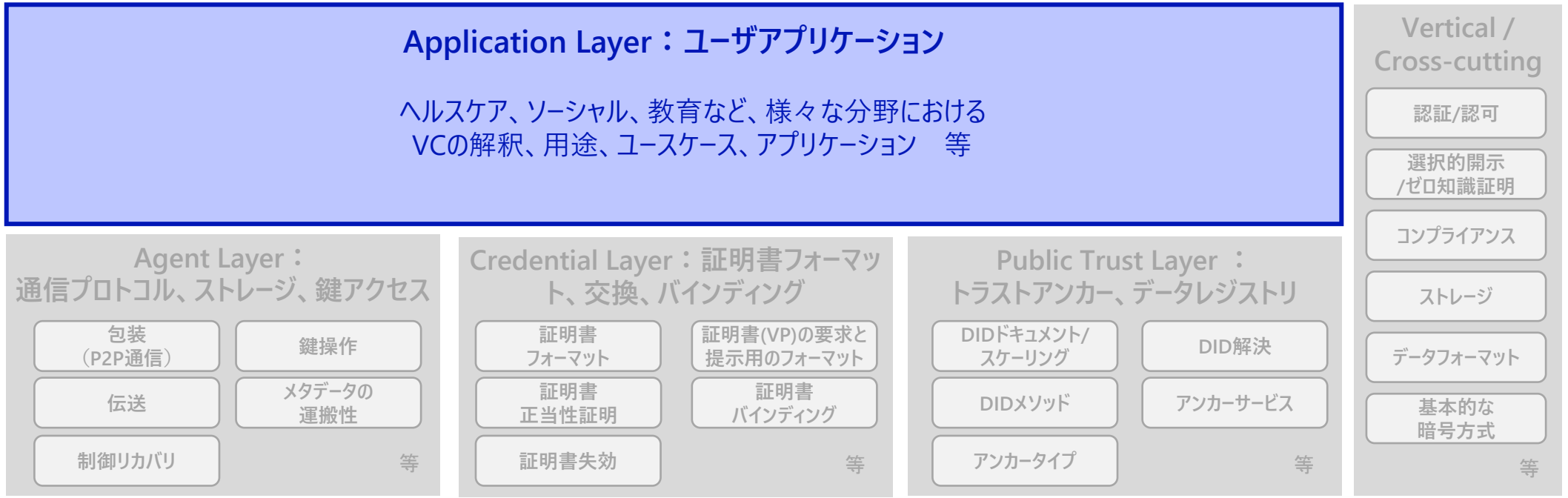
https://www.w3.org/TR/vc-data-model-2.0/

1-2. 議論対象のスコープ：レイヤ

本会議では、VCに関する通信プロトコルや証明書フォーマット等に関して、代表的な技術や仕様を利用することを前提としたうえで、現時点で一般化された解釈や用途が確立されていない状況にある、**ユースケースにより異なるVCの利用プロセス（発行・管理・検証等）について、各種法令の遵守・プライバシー・セキュリティ等の観点から留意すべき点を整理する。なお、本会議では、W3Cにおいて標準化が行われている狭義のVC※1に限定せず、mDL（ISO/IEC 18013-5におけるmdoc Data Model）などを含む広義のVCについて取り扱う。**

※1 W3C Verifiable Credentials Data Model

- 下記はTrusted WebによるVC規格概観整理図を基にした参考であり、グレーで例示した技術仕様に関する議論は本会議で行わない。
- 既に一定の扱い方の標準がある点に関しては論点としない（例：VCにおいてIssuerとVerifierが別主体であること）

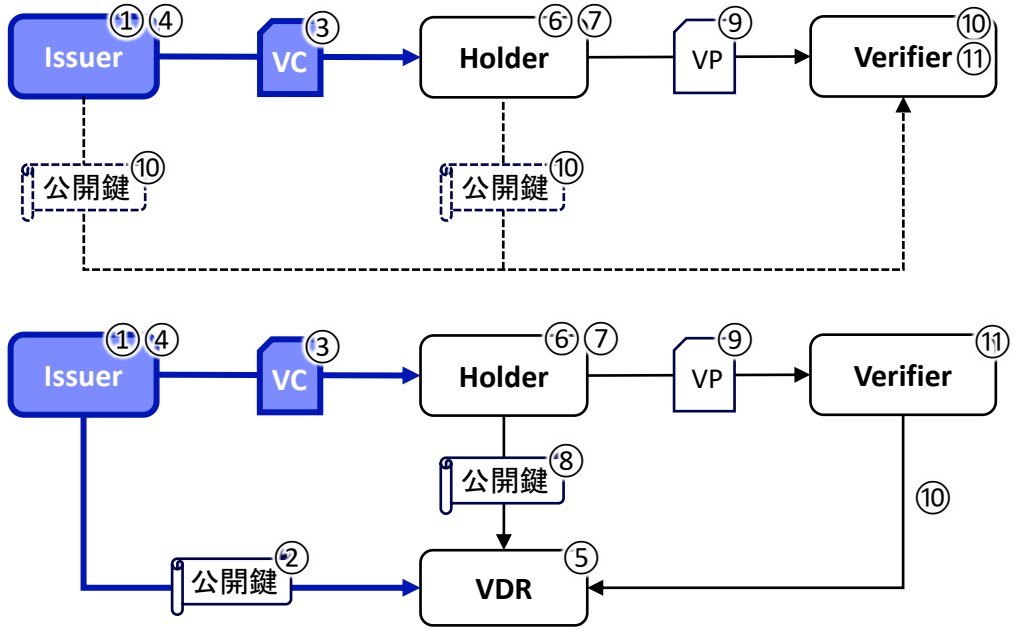


[1] https://github.com/decentralized-identity/interoperability/blob/master/assets/interoperability-mapping-exercise-10-12-20.pdf

1-3. 議論対象のスコープ：VCの利用プロセス

本会議においては、下図に示されるVCの発行・流通・利用プロセスのうち、主に**クレデンシャルの発行に着目し、Issuerのアクションに関する法令・制度を中心に整理を行う**。

VC利用プロセス例



VC利用プロセスの各アクション例

① **Issuerが、適切な情報源に基づき、VCを作成**
② **Issuerが、VDRに公開鍵を登録**
③ **Issuerが、Holderに対し、VCを発行**
④ **Issuerが、発行済のVCに対し、更新・失効等の管理を実施**
⑤ VDRが、登録された鍵を保管・管理
⑥ Holderが、発行されたVCを保管・管理
⑦ Holderが、VCに署名しVPを作成
⑧ Holderが、VDRに公開鍵を登録
⑨ Holderが、VerifierにVP/VCを提示
⑩ Verifierが、受け取ったVP/VCをIssuer/Holderの公開鍵で検証
（PKIの場合、公開鍵や証明書の有効性は認証局が担保する）
⑪ Verifierが、受け取ったVP/VCを保管・破棄

補足
- Issuerが発行するクレデンシャルのデジタル署名について、検証可能であることを前提とする。
- 前ページの通り、本検討会の議論対象はW3C Verifiable Credentials Data Model以外の広義のVCを含み、個々の仕様における各種用語・定義が異なる可能性がある。本図・本説明はあくまで参考として利用されたい。

1-4. 議論対象のスコープ：利用用途

下表に示すように、VCはさまざまな利用用途が期待されるが、**本年度は「本人確認」に関する用途を主眼**とし、現行の法令・制度との関連性や留意点を整理したうえで、VCの利活用が今後見込まれるユースケースに関する議論を行う。

これは、VCの活用が見込まれるユースケースの中でも「本人確認」については、偽造・不正利用等が行われた際のリスクが高く、適切な利活用を促進するための先行的な整理を行う緊要性が高いためである。

VCの利用用途		考えられるユースケースの例
本人確認		**本人確認書類（マイナンバーカード等）**
資格証明	**学歴・職歴**	学歴（学生証、卒業証書、成績証明書等）/ 職歴（社員証、在職証明、給与明細等）
	資格・スキル	公的資格（医師、弁護士、運転免許、教員免許等）/ 民間資格（日商簿記、TOEIC等）
	その他	チケット（コンサート、スポーツ観戦チケット等）/ 渡航関連（パスポート、ビザ、搭乗券等）
属性証明	**権利・所有**	財産所有（不動産、車両等）/ 知的財産権（特許、著作権等）
	取引・契約	金融取引（残高証明、信用スコア等）/ 法人間取引（契約証明、取引証明等）
	その他	医療・ヘルスケア（ワクチン接種証明、診察券等）/ 小売・サービス（会員証、クーポン等）

※証明書類の発行主体が本来想定した利用目的と、社会通念上の使用実態には乖離が生じる場合がある。一例として、自動車運転免許証は事実上、広範な本人確認手段として機能しているが、ここでは各証明書類の第一義的な利用目的に基づき区分し、記載している。

2. デジタルにおける本人確認

2-1. はじめに：デジタルにおける本人確認の課題

- 「誰かの身元」を確認する本人確認行為自体は、デジタル技術やネットワークの発達以前から存在した行為であるが、サイバー空間・デジタル社会においては、現実世界と比較したその特徴から、さらにこの重要性が増している。
  - ✓ データの複製・改変の容易性
  - ✓ 扱うことができるデータに対する制限
  - ✓ ネットワークの先の相手の匿名性・接続する相手の拡大
  - ✓ ディープフェイク、多数の攻撃を試行すること等の攻撃の容易性

- デジタルにおいてサービスを提供する際に「正しい利用者であるか否か」を区別すること、また、これを区別する基準・定義を設定することは、依然として困難かつ重要な課題であるものの、VCの利活用において信頼性を確保するためにも、各種のリスク・脅威を踏まえた整理を行う必要がある。
  - フィッシング、認証情報の不正利用、偽造身分証、詐欺、etc.

Digital identity is hard. Proving someone is who they say they are — especially remotely, via a digital service — is fraught with opportunities for an attacker to successfully impersonate someone. As correctly captured by Peter Steiner in The New Yorker, "On the internet, nobody knows you're a dog."

デジタルアイデンティティは難しいものです。誰かがその本人であることを証明することは―とくにデジタルサービスを介し、遠隔の場合において―攻撃者が誰かに成り済ます機会を多く含んでいます。ピーター・スタイナーが『ニューヨーカー』誌で正しく指摘しているように、「インターネット上では、誰もあなたが犬であることを知らない」のです。

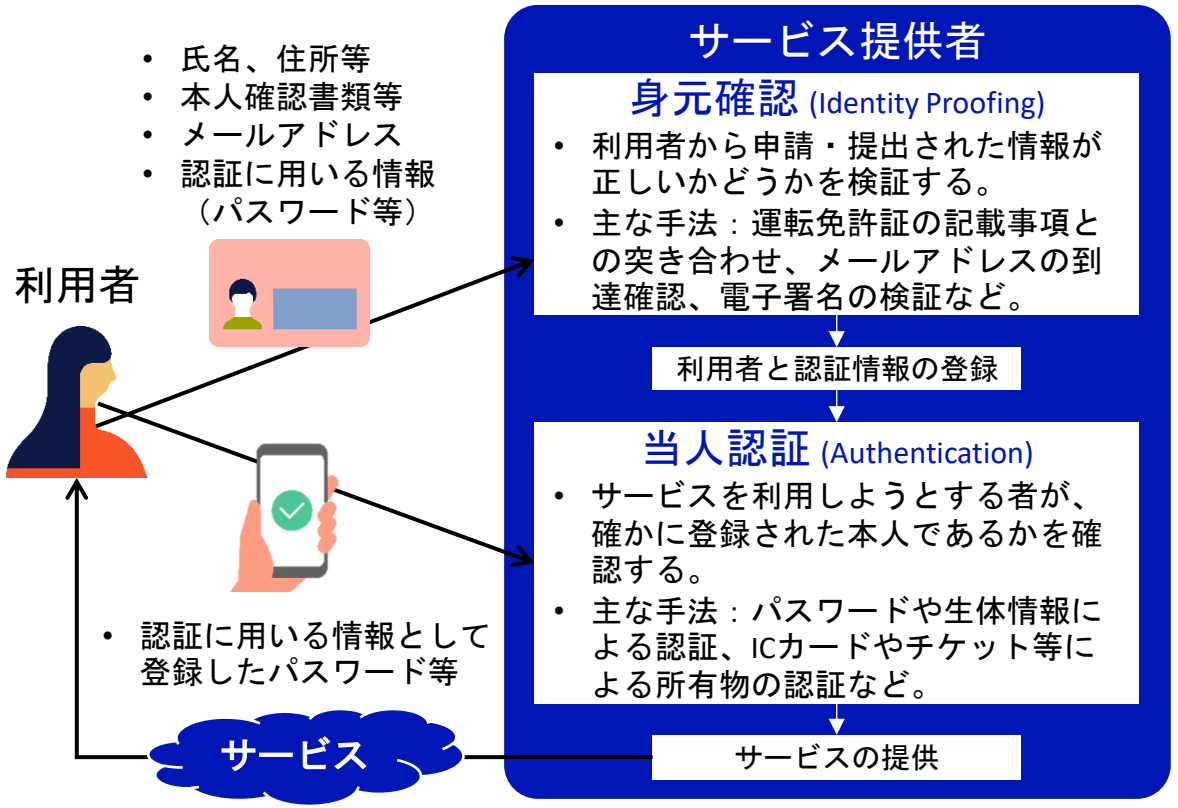
（National Institute of Standards and Technology Special Publication 800-63-3 Executive Summaryより。事務局仮訳）

2-2. 本人確認（身元確認・当人認証）

本人確認の主な構成要素として、利用者の身元を特定して利用者として登録する「**身元確認 (Identity Proofing)**」と、既に登録された本人であることを確認する「**当人認証 (Authentication)**」の2つ*がある。

※それぞれの要素単体（とくに身元確認）について「本人確認」と呼ぶ場合もあるが、本スライドにおいては、**これら２つの要素を総称したものを「本人確認」、個々の要素を指す際には「身元確認」「当人認証」と区別する**。

身元確認・当人認証のレベルは、プライバシーやユーザビリティの観点も踏まえると、いずれも「高ければよい」ものではなく、サービスの特性やリスクに応じて選択される。



①「身元確認 (Identity Proofing)」

サービス提供に必要な**利用者情報を収集・検証する**行為（利用者情報：氏名、住所、メールアドレス等）

- サービス利用申請、ユーザ登録など、サービスの初回利用時に行われることが一般的
- 収集する情報や検証内容（改ざん有無の確認等）は、サービスによって異なる

②「当人認証 (Authentication)」

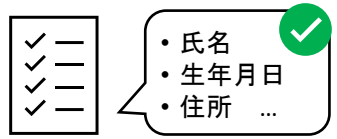
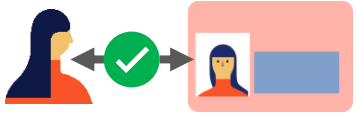
サービスを利用しようとする者が**「あらかじめ登録された本人」であること**を確認する行為

- Webサイトへのログイン時のパスワード、パスキー等による認証、マイナンバーカードを利用した認証など
- なりすまし時のリスク等に応じて、認証強度が選択される（多要素認証など）

本人確認ガイドライン改定に向けた有識者会議
令和６年度（２０２４年度）第４回資料（改変）

（概要）本人確認（身元確認・当人認証） - 身元確認プロセスの全体像（概観）

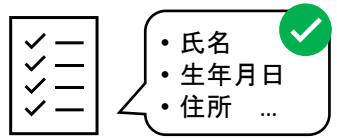
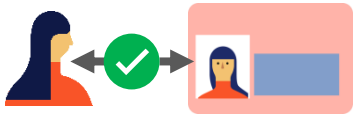
身元確認における脅威の議論においては、身元確認に含まれる一連のプロセス・ステップごとに想定される脅威を踏まえ、その対策が、本人確認を行う目的・手続におけるリスクを考慮して十分であるか留意する必要がある。

身元確認プロセス	プロセスの概要	主な手法
属性情報の収集 	• 申請者から氏名、生年月日、住所等の属性情報を収集し、申請者を一意に識別できる状態とする。 （SP 800-63A-4の ”Resolution” に相当）	a) 本人確認書類から電子データを読み取る b) 本人確認書類の券面から機械的に読み取る c) 申請者自身に記入・入力を求める d) IDプロバイダから取得する
本人確認書類の検証 	• 申請者から提示された本人確認書類が偽造・改ざんされたものでないことを物理的又は電子的に検証する。これにより、収集した申請者の属性情報が正確かつ真正なものであることを確認する。 （SP 800-63A-4の ”Validation” に相当）	a) デジタル署名の検証 b) 対面での券面の検査 c) 非対面での券面の検査
申請者の検証 	• 本人確認書類が備える顔写真や暗証番号等を用いて、提示された本人確認書類が確かに申請者自身のものであることを検証する。 （SP 800-63A-4の ”Verification” に相当）	a) 対面での容貌確認 b) 非対面での容貌確認 c) 暗証番号等による検証 d) 確認コードの送付による検証

本人確認ガイドライン改定に向けた有識者会議
令和６年度（２０２４年度）第４回資料（改変）

（概要）本人確認（身元確認・当人認証） - 身元確認における脅威の整理

身元確認における脅威の議論においては、身元確認に含まれる一連のプロセス・ステップごとに想定される脅威を踏まえ、その対策が、本人確認を行う目的・手続におけるリスクを考慮して十分であるか留意する必要がある。

身元確認プロセス	想定される主な脅威		
属性情報の収集 	**❶ 重複登録** • 属性情報の不足や誤り等により、申請者が既に登録済みの人物であると検知できず、重複申請を受け付けてしまう	**❷ 別人との誤紐づけ** • 属性情報の不足や誤り等により、申請者を別の人物と区別できず、別人の情報と紐づけてしまう	
本人確認書類の検証 	**❸ 本人確認書類の偽造・改ざん** • 偽造又は改ざんされた本人確認書類によって、実在する別の人物や架空の人物になりすまされる	**❹ 本人確認書類の複製** • 複製された本人確認書類によって、実在する別の人物になりすまされる	**❺ 本人確認書類の不正な発行** • 不正な手続によって発行された本人確認書類により、実在する別の人物や架空の人物になりすまされる
申請者の検証 	**❻ 本人確認書類の盗用** • 盗まれた本人確認書類によって、実在する別の人物になりすまされる	**❼ 本人確認書類の貸し借り** • 貸し借りされた本人確認書類によって、実在する別の人物になりすまされる	**❽ カメラ映像の偽造・改ざん** • カメラの映像を不正に加工されたり、差し替えられたりすることで、別の人物になりすまされる

本人確認ガイドライン改定に向けた有識者会議
令和６年度（２０２４年度）第４回資料（改変）

（参考）本人確認（身元確認・当人認証）- 脅威に対する対策手法の大まかな強度

身元確認における脅威の議論においては、身元確認に含まれる一連のプロセス・ステップごとに想定される脅威を踏まえ、その対策が、本人確認を行う目的・手続におけるリスクを考慮して十分であるか留意する必要がある。

想定される主な脅威	対策手法の大まかな強度 弱 → 強 注：ここで示す強弱関係はあくまで大まかな基準であり、実際の強度は様々な条件によって変化する。			
❶ 重複登録 ❷ 別人との誤紐づけ	申請者自身に記入・入力を求める	本人確認書類の券面からOCR等で機械的に読み取る	本人確認書類から電子データを読み取る	
❸ 本人確認書類の偽造・改ざん	非対面での券面の検査	対面での券面検査	デジタル署名の検証	
❹ 本人確認書類の複製	複製対策なし	本人確認書類の複製対策 （複製検知印刷技術等）	本人確認書類の複製対策 （耐タンパー技術等）	
❺ 本人確認書類の不正な発行	**信頼できる機関から発行された本人確認書類の利用** **（信頼できる機関：本人確認書類の発行プロセスが明らかであり、かつ対象手続に十分な水準で実施されていると信頼できる機関。）**			
❻ 本人確認書類の盗用	確認コードの送付	暗証番号等による検証	非対面での容貌確認	対面での容貌確認
❼ 本人確認書類の貸し借り	耐性なし			
❽ カメラ映像の偽造・改ざん	対策なし	ライブネスチェック等の不正検知技術の採用	統制環境下でのリモート身元確認	対面での身元確認

本人確認ガイドライン改定に向けた有識者会議
令和６年度（２０２４年度）第２回資料（改変）

（参考） 米国NIST SP 800-63-4 2pdにおけるEvidence Requirementsの概要

身元確認を受ける者が提出する本人確認書類（Identity Evidence）の強度に関するレベル分け要件
（米国NISTにより策定が行われている本人確認等に関する基準であるSP-800-63 第4版ドラフト第2版におけるもの。）

要件の項目	SUPERIOR	STRONG	FAIR
①発行プロセス	• 発行元は、その人物の実在性を確実に把握できるよう設計されたプロセスにより身元確認を行っていること。その発行プロセスは州や連邦政府等による監督対象となっていること • このような手順にはIAL2以上の身元確認が含まれるが、これに限らない	SUPERIORと同じ	• 発行元は、その人物の実生活上の身元を把握しているという確信を形成できるように設計されたプロセスによる身元確認を行っていること
	• 発行元は、 その人物が物理的に実在することを有人の（Attended）プロセスによって確認していること	要件なし	要件なし
	• 郵便による送達など、本人に届けられた可能性が高いとみなせる	SUPERIORと同じ	SUPERIORと同じ
②含まれる情報	• 氏名 • 参照番号 • 顔写真	SUPERIORと同じ	• 氏名 • 参照番号又は顔写真のいずれか
③暗号学的な保護とデジタル署名	• 属性は暗号学的に保護されており、発行元のデジタル署名によりvalidateできること	要件なし	要件なし
④含まれる情報を権威あるソースにより検証できること	要件なし ※②のデジタル署名の検証により Attribute Validationが可能	必須	必須
⑤物理的なコピー・複製への対策（物理エビデンスの場合）	必須	必須	必須

※上記の要件はNIST SP 800-63A-4 2pd の内容をもとに要点を抽出・要約したものであるため、各要件は厳密な記載とはなっていない点に留意されたい。

本人確認ガイドライン改定に向けた有識者会議
令和６年度（２０２４年度）第５回資料（改変）

（参考）本人確認（身元確認・当人認証） – 当人認証における脅威の整理

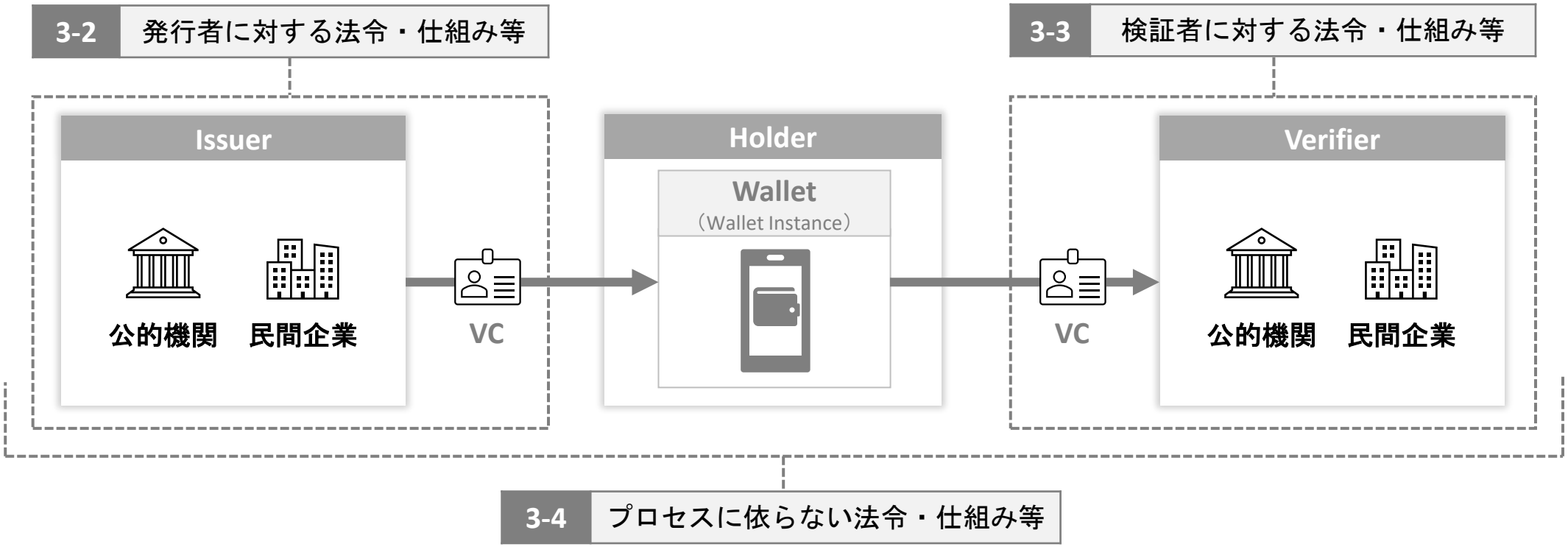
当人確認についても、脅威を踏まえ、適切な利用形態となるように留意する必要がある。

No.	主な脅威	脅威の概要	対策例
1	オンライン上でのパスワードの推測	総当たりやパスワードリスト等により繰り返しログインを試行することで、なりすましを行う	パスワードの複雑性の確保、一定時間あたりの認証回数の制限、多要素要素の採用
2	盗聴・リプレイ攻撃	通信を盗聴し、パスワード等の認証情報を窃取することでなりすましを試みる、同じ内容を再送信することでなりすましを行う	通信の暗号化、チャレンジレスポンス方式の採用、nonceの導入、ワンタイムパスワードの採用
3	パスワードや認証器の盗用	他サービスから漏えいしたパスワード、盗難したICカード等を用いてなりすましを行う	多要素要素の採用
4	フィッシング攻撃	利用者を偽のサイトに誘導し、入力されたパスワード等を攻撃者が窃取したり、正規のサイトにリアルタイムに中継したりすることで、なりすましを行う	フィッシング耐性を有する認証技術の採用 ※ ワンタイムパスワードはリアルタイム中継型のフィッシング攻撃への耐性を有さない点に留意
5	暗号鍵の不正な取り出し・複製	秘密鍵が格納されたデバイスに対し、物理的な解析やサイドチャネル攻撃等を行うことにより、秘密鍵を不正に取り出そうとする	耐タンパ性を有するハードウェアの利用等

3. 各種法令・制度・仕組みとの関連及び留意点

3-1. IHV（Issuer-Holder-Verifier）モデル

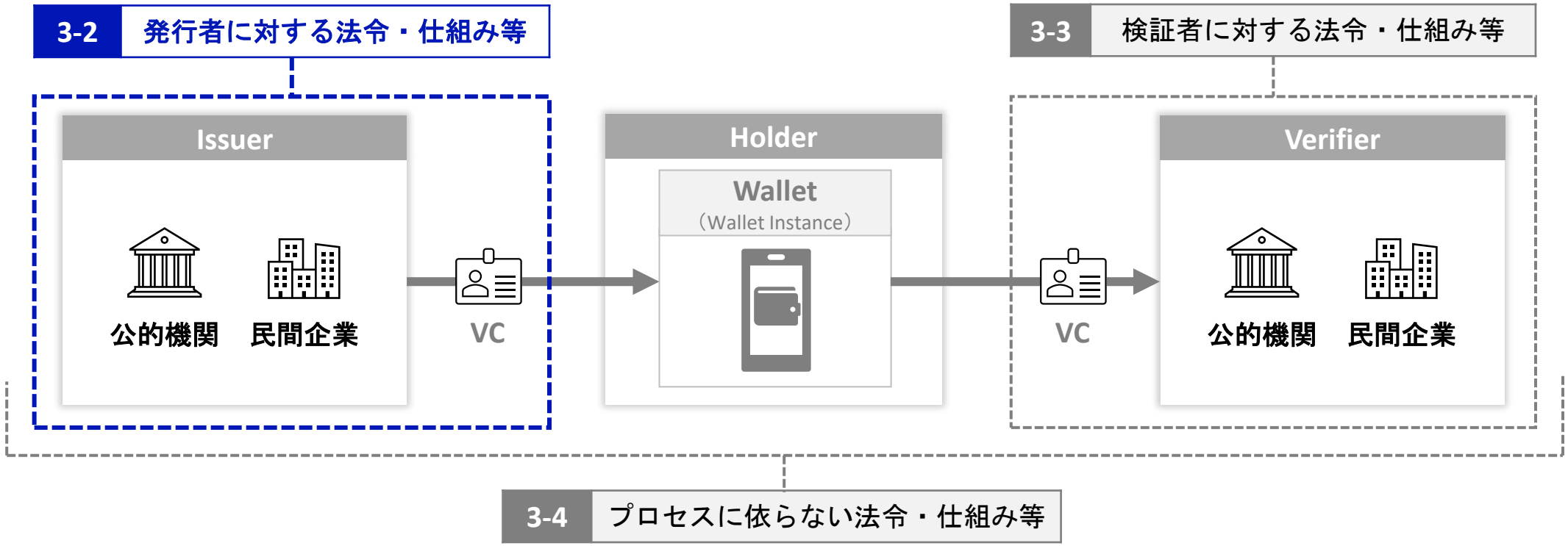
「本人確認」用途にVCを活用する場合の留意事項に関する議論の参考として、証明書の発行に関する各アクター（Issuer, Holder, Verifier）やデータ（Verifiable Credential）に関する各種法令・制度・仕組みを、IHV（Issuer-Holder-Verifier）モデル※1を踏まえ整理・分類。



※1：three-party-modelとも。本検討会においては、IHV（Issuer-Holder-Verifier）モデルそのものや基本的なアクターに関する解説は省略する。

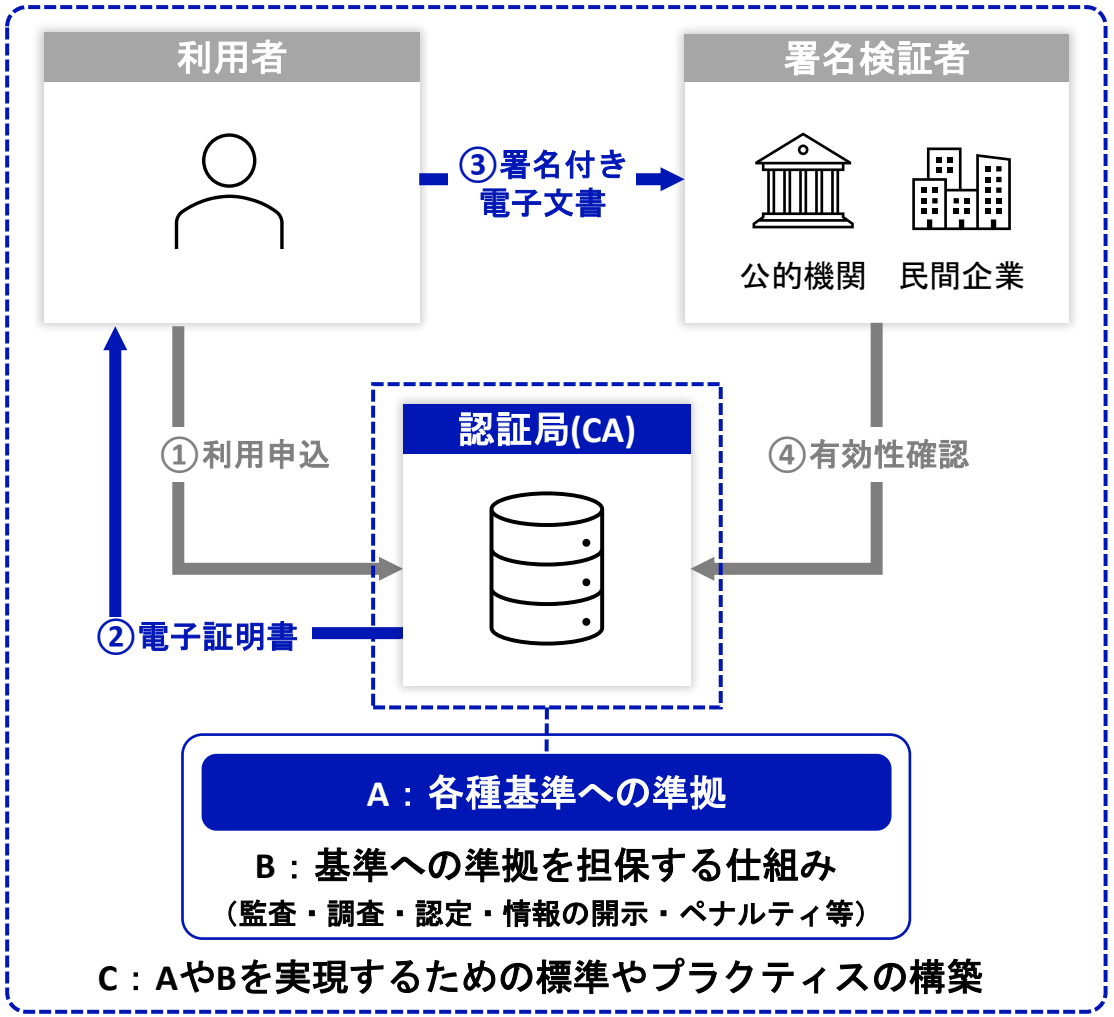
3-2. 発行者に対する法令・仕組み等

「本人確認」用途にVCを活用する場合の留意事項に関する議論の参考として、証明書の発行に関する各アクター（Issuer, Holder, Verifier）やデータ（Verifiable Credential）に関する各種法令・制度・仕組みを、IHV（Issuer-Holder-Verifier）モデル※1を踏まえ整理・分類。



※1：three-party-modelとも。本検討会においては、IHV（Issuer-Holder-Verifier）モデルそのものや基本的なアクターに関する解説は省略する。

3-2. 発行者に対する法令・仕組み等 – 公開鍵基盤（PKI）の事例



公開鍵基盤（PKI）においては、認証局（CA）が発行する電子証明書に対する信頼性と安全性を担保するため、様々なルールや仕組みが積み上げられてきた。

A：基準・ルール

- 電子署名法による認定基準
- CA/Browser Forumが策定するBaseline Requirements

B：基準への準拠を担保する仕組み

- 監査、調査、認定制度など
- 情報の開示
- 信頼性を損なう主体に対するペナルティなど

C：その他標準・プラクティス等

標準化技術

- 証明書失効リスト（CRL）
- オンライン証明書状態プロトコル（OCSP）

プラクティス

- CP/CPS（証明書ポリシー、認証局運用規定）の公開
- 証明書の有効期限の設定

以上の通り、**PKIでは認証局が「信頼に足る主体」であること、また、この利用における信頼性を担保するため、長年にわたり積み上げられた仕組みが存在するが、VCについては、まだ未成熟である点が多いのではないか。**

3-2. 発行者に対する法令・仕組み等 – 発行者(Issuer)に対する規律

前スライドのPKIの事例を踏まえると、本人確認書類等の発行者（Issuer）に対する規律としては、主に、**書類発行時の本人確認、業務プロセスや技術的基準に関し、「①発行の(業務)プロセス自体を定めるもの」、また、監査・調査・認定の仕組みや罰則等を定める「②発行者の性質や発行プロセスを担保するもの」の２つが考えられる。**

PKIにおける実例：電子署名法第４条による特定認証業務の認定（一部のみ概要）

①発行の(業務)プロセス自体を定める規定

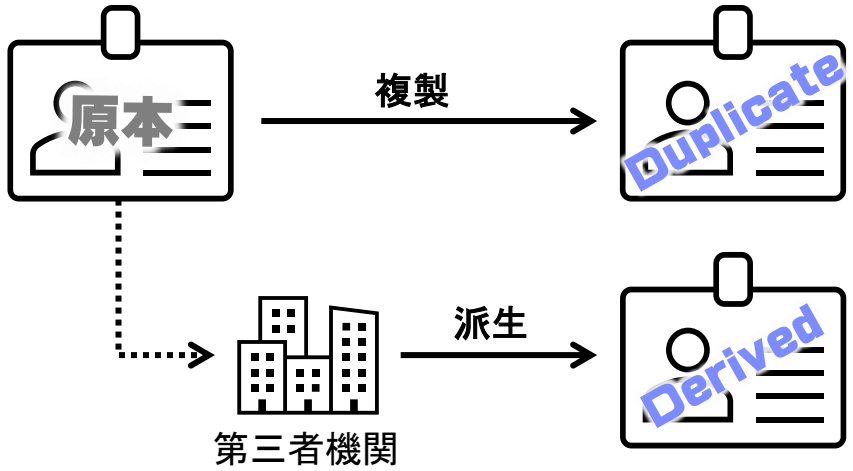
- **業務の用に供する設備に関する基準**
  - 建物・部屋のセキュリティ
  - 設備のアクセス制御等
  - 暗号装置（HSM）の安全性
- **利用者の真偽の確認（身元確認）の方法に関する基準**
  - 本人確認書類及び身元確認の方法に関する基準
- **その他の業務の方法に関する基準**
  - 利用者に対する重要事項説明
  - 電子証明書の記載事項
  - 公開鍵・CRL等の公開
  - 認定業務との誤認を防止する措置
  - CP/CPSの設定
  - その他業務手順・責任及び指揮系統等の設定

②発行者の性質や発行プロセスを担保する規定

- **主務大臣による認定（及び認定の取消）**
- **主務大臣又は指定調査機関による調査**
- **主務大臣による報告徴収及び立入検査を行う権限**
- **欠格事項**
- **罰則規定**

3-2. 発行者に対する法令・仕組み等 – 発行者(Issuer)が発行するデータについて

行政手続や保有個人情報の開示請求等の手続に際し、本人確認書類として、本人に対し一に限り発行される書類※１を求める法令等は多数存在するが、これは、本人確認書類の貸与等のリスクを踏まえ、「本人」以外が当該書類を所持しているリスクを低減させ、身元確認の確実性を高める役割があると考えられる。**VCの発行に際しても、正当な権限を有さない第三者（発行権者以外）による書類の複製・派生行為※２は、この一意性を喪失させるものであるため、原本と同等の性質を持つ書類として利用・流通することは困難であると考えられる。**



	現実世界	デジタル
	―	• 原本を電子的に複製したもの（原本と明確な差異はない）
	• コピー機等で複写したもの（例：パスポートのコピー） • 原本の発行者以外の第三者が原本を元に別途発行したもの（例：「本人確認済み」のスタンプが押された書類）	• 原本の発行者以外の第三者が原本を元に別途発行したもの

※１）「一に限り発行された書類」とは、特定の個人に対して、原則として１枚だけ発行が行われる、有効な書類が同時に２枚以上存在しない書類のことを指し、例としてマイナンバーカード、運転免許証などが該当する。

※２）ここでいう「複製」は同一性が確保されたもの（Duplicate）、「派生」は同一性が必ずしも確保されていないもの（Derived）として分類する。また本分類は「デジタルクレデンシャルの利用用途に応じた管理要件に関する考察」[1]を参考にしている。

[1] デジタルクレデンシャルの利用用途に応じた管理要件に関する考察 https://dal.sfc.keio.ac.jp/ja/TR/management-requirements-for-digital-credentials/

（参考）発行者に対する法令・仕組み等 – 発行者(Issuer)が発行するデータについて

- 各種証明書の持つ法的証拠力については、**公的機関が発行する書類、民間が発行する書類で前提の違いがある点に留意する必要があると考えられる。**公正な第三者たる公務員が職務上作成する公文書は、民事訴訟法第228条第２項により、民事裁判において、真正に成立している（その文書が作成名義人の意思に基づいて作成されたものである：形式的証拠力がある）ものとして取り扱われる※1一方、民間が発行するVCを含む電磁的な私文書については、電子署名法第３条の推定規定の適用を受けるないしその他の方法により、これを立証する必要がある。

※１：また、公文書については、民事訴訟法第228条第３項の規定により、裁判所が当該文書を作成した公務所に照会を行うことが可能である。

- これら規定は、実質的証拠力（その文書が事実の証明にどこまで役立つのか（＝作成名義人によってその文書に示された内容が信用できるものであるか）といった中身の問題）について規定しているものではなく、いずれにしても、円滑な取引のためには、利用形態ごとのリスクに応じて、前述の「基準・ルール」「基準への準拠を担保する仕組み」などにより、その信頼性を向上させることも重要である。

公文書の形式的証拠力

公正な第三者たる公務員が職務上作成する公文書は、民事訴訟法第228条第２項により、真正に成立しているものとして取り扱われる。

※これは、公務の公益性・公共性を担保する様々な仕組み（守秘義務、公正な試験による採用、虚偽公文書作成罪等の刑事罰等）などが前提に存在すると考えられる。

私文書の形式的証拠力

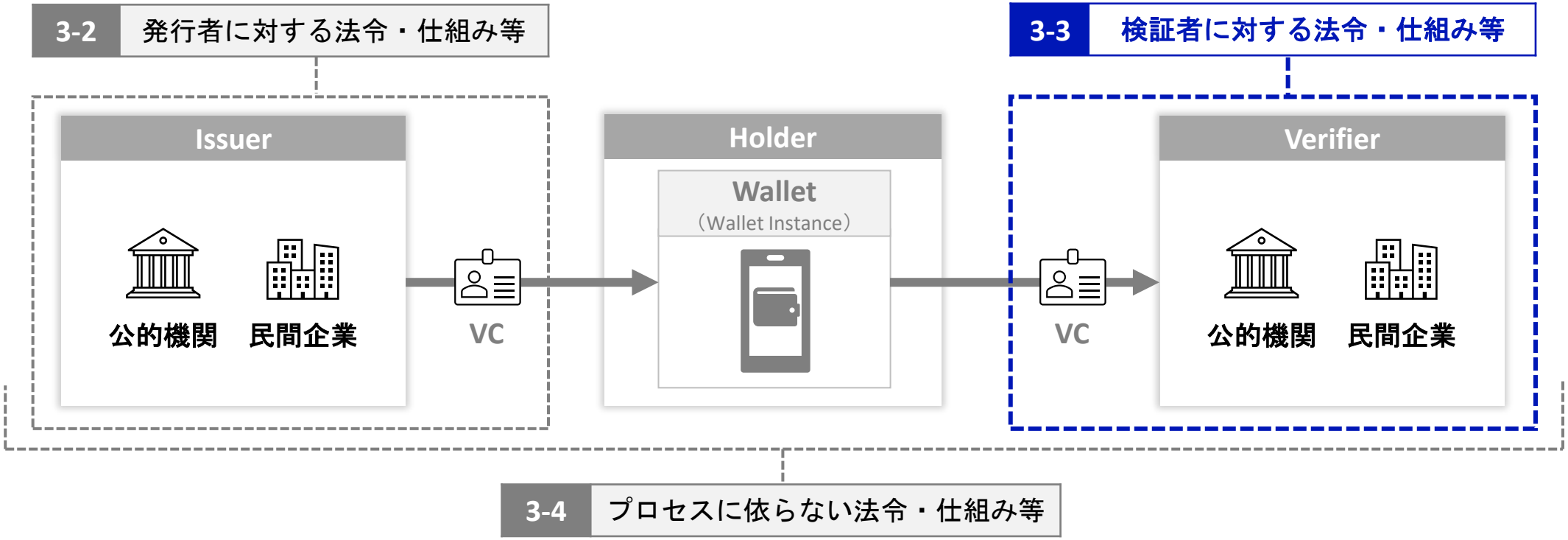
民間により発行される証明書（学生証、口座残高証明書等）を含む私文書については、民事訴訟法第228条第４項や電子署名法第３条による推定規定を受けるないしその他の方法により形式的証拠力を担保する必要がある。

内閣府、法務省、経済産業省「押印についてのQ&A」https://www.moj.go.jp/content/001322410.pdf

デジタル庁、法務省「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するＱ＆Ａ（電子署名法第３条関係）」
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/517ca59b-6ea4-4179-a338-8d1b51a4d40b/4ae659c2/20240109_digitalsign_qa_01.pdf

3-3. 検証者に対する法令・仕組み等

「本人確認」用途にVCを活用する場合の留意事項に関する議論の参考として、証明書の発行に関する各アクター（Issuer, Holder, Verifier）やデータ（Verifiable Credential）に関する各種法令・制度・仕組みを、IHV（Issuer-Holder-Verifier）モデル※1を踏まえ整理・分類。



3-3. 検証者に対する法令・仕組み等 – 検証者(Verifier)に本人確認を要求する法令について

本人確認行為自体は、法令に依らない形で民間においても多く行われている（会員証の作成時の身元確認等）ものの、とくにリスクが高い手続・確実な本人確認が行われる必要がある手続等については、法令により検証者に本人確認を要求するものもある。

ひとくちに「本人確認」といっても、手続ごとのリスクは様々であり、VCを利用した本人確認についても、その手続ごとのリスクプロファイルを踏まえ、この対策として十分な水準を満たす手続から、徐々に利用が拡大するものと考えられる。

検証者に本人確認（身元確認）を求める法令の例

- **業法として、規制対象となる業界における不正の防止・健全な発展などの目的を踏まえて事業者等に本人確認の義務等を課すないし方法を定めるもの**

電子署名及び認証業務に関する法律（電子署名法）、犯罪による収益の移転防止に関する法律（犯収法）、携帯電話不正防止利用法、たばこ事業法、古物営業法 など

- **行政手続等において行政機関が行う本人確認の方法を定めるもの**

行政手続における特定の個人を識別するための番号の利用等に関する法律（マイナンバー法）など

電子署名法施行規則 第五条第一項
*認証業務の利用の申込みをする者（以下「利用申込者」という。）に対し、住民基本台帳法（昭和四十二年法律第八十一号）第十二条第一項に規定する**住民票の写し若しくは住民票記載事項証明書、戸籍の謄本若しくは抄本**（現住所の記載がある証明書の提示又は提出を求める場合に限る。）若しくは領事官（領事官の職務を行う大使館若しくは公使館の長又はその事務を代理する者を含む。）の**在留証明**又はこれらに準ずるものとして**主務大臣が告示で定める書類の提出を求め**、（以下略）*

（参考）犯罪収益移転防止法における自然人の本人確認手法の概要

※令和７年２月末時点版

非対面での取引

類型		方法	該当条項
個人顧客向け	本人確認書類を用いた方法	「写真付き本人確認書類の画像」＋「容貌の画像」を用いた方法	１号ホ
		「写真付き本人確認書類のＩＣチップ情報」＋「容貌の画像」を用いた方法	１号ヘ
		「本人確認書類の画像又はＩＣチップ情報」＋「銀行等への顧客情報の照会」を用いた方法	１号ト（１）
		「本人確認書類の画像又はＩＣチップ情報」＋「顧客名義口座への振込み」を用いた方法	１号ト（２）
	電子証明書を用いた方法	「公的個人認証サービスの署名用電子証明書（マイナンバーカードに記録された署名用電子証明書）」を用いた方法	１号ワ
		「民間事業者発行の電子証明書」を用いた方法	１号ヲ・カ
法人顧客向け		「法人の本人確認書類」又はその写しの送付を受ける方法	３号ニ
		「電子認証登記所発行の電子証明書」を用いた方法	３号ホ

対面での取引

類型	方法	該当条項
個人顧客向け	「写真付き本人確認書類①」の提示を受ける方法	１号イ
	「本人確認書類②」の提示を受け、下記のいずれかを組み合わせた方法 i)　「本人に取引関係文書を送付」する方法 ii)　異なる「本人確認書類」OR「補完書類」の提示を受ける方法 iii)　ii) の書類又はその写しの送付を受ける方法	１号ロ １号ハ １号ニ
	「本人確認書類③」の提示を受け、「本人に取引関係文書を送付」する方法	１号ロ
法人顧客向け	「法人の本人確認書類」の提示を受ける方法	３号イ
	申告を受け、登記情報提供サービスから登記情報の送信を受ける方法（非対面でも利用可能）	３号ロ
	申告を受け、国税庁・法人番号公表サイトと照合する方法（非対面での利用可能）	３号ハ

※外国の自然人・外国の法人を除く

自然人（外国人を除く）の本人確認書類

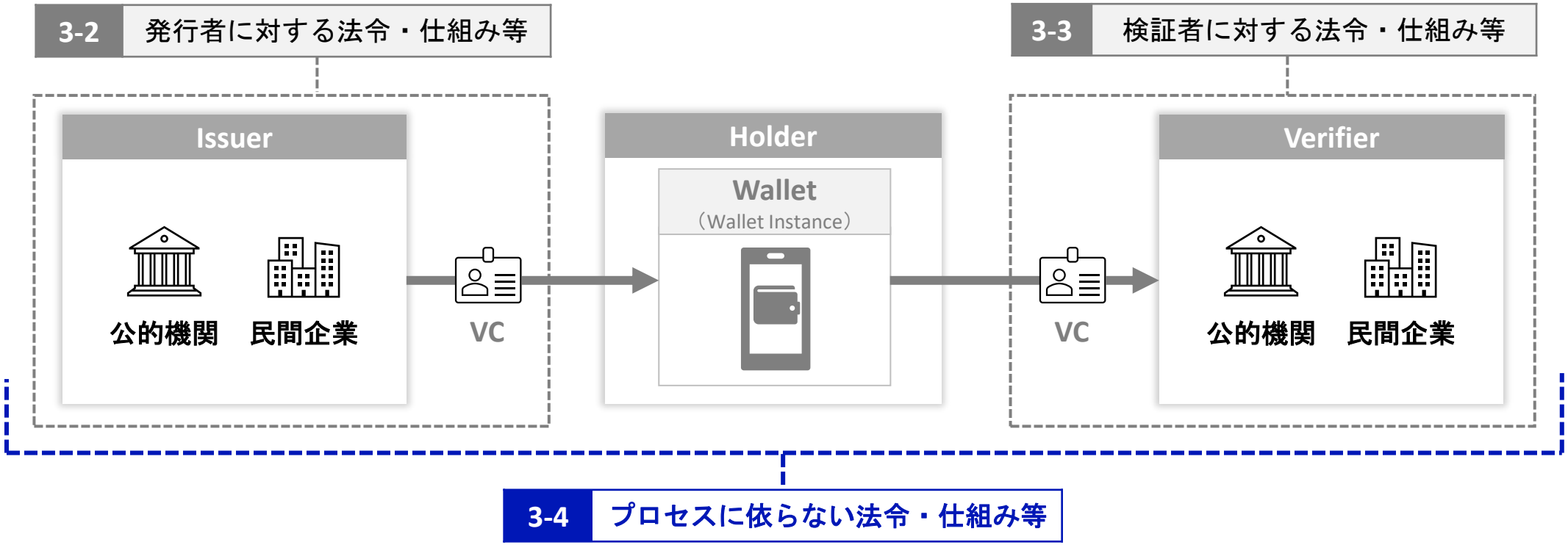
① ア：運転免許証、運転経歴証明書、在留カード（顔写真のあるもの）、特別永住者証明書（顔写真のあるもの）、マイナンバーカード（顔写真のあるもの）、旅券（パスポート）等
　イ：上記のほか、官公庁発行書類等で氏名、住居、生年月日の記載があり、顔写真のあるもの
② ア：在留カード（顔写真のないもの）、特別永住者証明書（顔写真のないもの）、マイナンバーカード（顔写真のないもの）、各種健康保険証、各種資格確認書、国民年金手帳、母子健康手帳、特定取引等に使用している印鑑に係る印鑑登録証明書 等
③ ア：②以外の印鑑登録証明書、戸籍の附票の写し、住民票の写し・住民票記載事項証明書
　イ：上記のほか、官公庁発行書類等で氏名、住居、生年月日の記載があり、顔写真のないもの（マイナンバーカードの通知カードを除く。）

3-3. 検証者に対する法令・仕組み等 – 公的個人認証サービスの事例

公的個人認証サービス（JPKI）署名用電子証明書又は利用者証明用電子証明書による電子署名又は電子利用者証明の検証は、主務大臣による認定を受けた民間事業者を含む法定された署名検証者や利用者証明検証者が行う。また、主務大臣による認定を受けた民間の署名検証者は、業務の設備・電子署名及び電子利用者証明の検証の方法等が基準に適合している者であり、さらに、その署名検証等を適切に行う義務が設けられているなど、適正な利用を担保する仕組みが設定されている。

3-4. プロセスに依らない法令・仕組み等

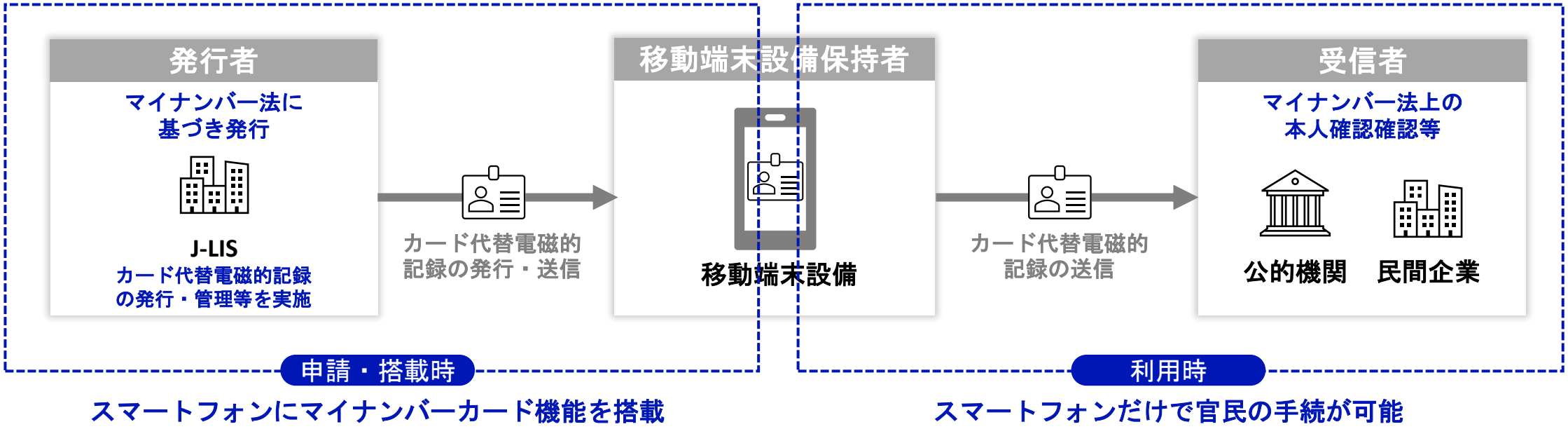
VCの利活用に限ったものではないが、プロセスに依らない法令・仕組み等として、情報の取扱い等の規律を求める法令（個人情報保護法、マイナンバー法など）、事業者に規律を求める法令（電気通信事業法、各業界の業法など）、刑法（公文書・私文書の偽造など）、アプリストア運営事業者の規約、その他消費者に対する配慮が必要となる点等が考えられ、**VCの利活用においても、そのユースケースや利用形態によって、未整理の論点が存在する可能性があり、個別の整理等を要する可能性があることに留意。**



参考. マイナンバー法におけるカード代替電磁的記録

カード代替電磁的記録について

カード代替電磁的記録は、マイナンバーカードの機能をスマートフォンに搭載することを目的として、デジタル社会形成基本法等の一部改正法によるマイナンバー法の改正により新たに規定された。**カード代替電磁的記録及びVerifiable Credentialは、いずれもスマートフォンにおいて活用できるデジタル証明書の一種であるが、カード代替電磁的記録は物理マイナンバーカードの「代替」たる電磁的記録として、法令によりその発行手法、利用手法が厳格に規定されている。**

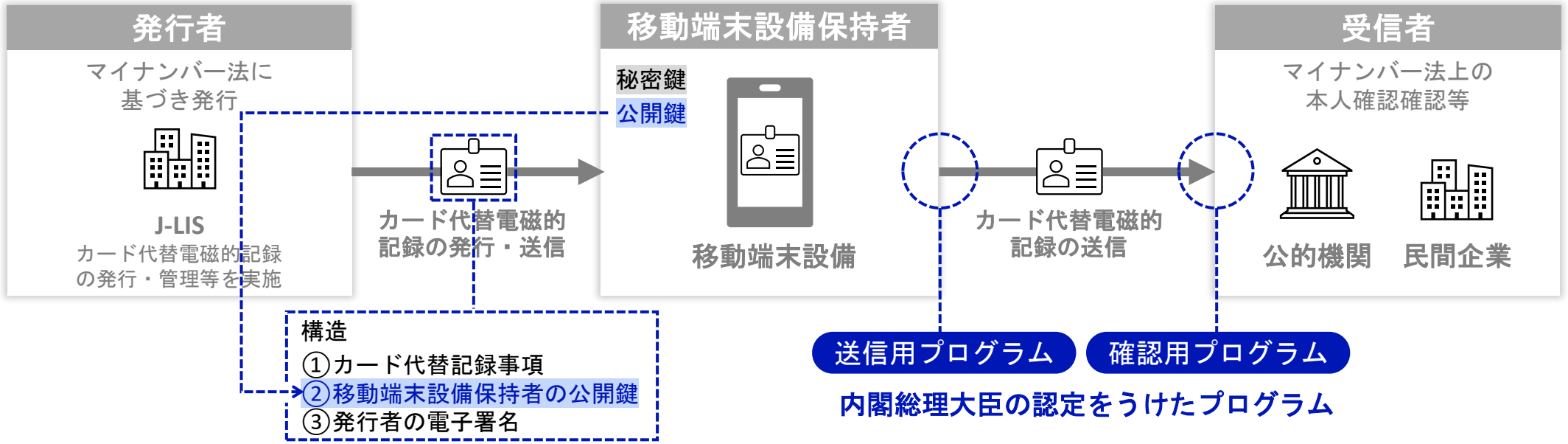


参考. マイナンバー法におけるカード代替電磁的記録

カード代替電磁的記録の真正性や安全性

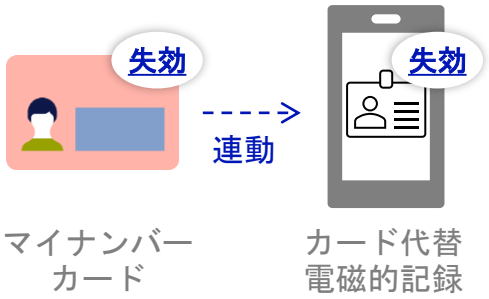
カード代替電磁的記録の発行者である地方公共団体情報システム機構（J-LIS）は、申請者の移動端末設備の公開鍵に機構の秘密鍵を用いて電子署名することが義務付けられており、これにより受信側は、発行者と送信者双方の署名を検証することで、**記録の真正性と送信者の同一性を確認できる**。

また、カード代替電磁的記録の利用に係る安全性を担保するため、カード代替電磁的記録の**送信用/確認用プログラムに対し、内閣総理大臣による認定制度が設けられている**。



参考. カード代替電磁的記録との相違点

カード代替電磁的記録における不正利用の防止対策



個人番号カード（マイナンバーカード）は、信頼性の高い身分証として、不正利用を防ぐため、各種の脅威に対処するための基準や対策が定め・講じられている。

例えば、カード代替電磁的記録はあくまでも物理マイナンバーカードの代替としての位置付けであるため、その有効性は原本たる個人番号カードの有効性に依拠しており、個人番号カードが失効した場合、それに紐付くカード代替電磁的記録も自動的に失効する仕組みを講じている。

さらに、マイナンバーカードの特徴として、その発行及び管理が住民基本台帳の情報に基づいて行われている点が挙げられる。住民票の記載事項に変更が生じた場合、その旨を届け出ることがマイナンバー法上義務付けられている。

マイナンバーカードの派生、もしくは類似したデジタル証明書の扱い

マイナンバーカードを利用して本人確認等を行った情報を用いて、派生クレデンシャルを作成・活用する場合、その証明権者は派生クレデンシャルの作成者となり、信頼を確保するための仕組みが別途必要となることに加え、前述のような、**記載事項の変更、紛失等による失効が派生クレデンシャルに反映されず、情報の最新性に関する信用性は低下する。**

マイナンバー制度においては、本人の同意により、事業者等が利用者の最新の利用者情報について、地方公共団体情報システム機構（J-LIS）に照会を行うことができるサービス（最新の利用者情報（４情報）提供サービス）が提供されており、金融機関等において、顧客の住所変更等の情報を取得し、顧客情報の更新を行っているケース場合がある。派生的なクレデンシャルであっても、このような仕組みの活用により、その信用度を向上させることは可能である。

ただし、**デジタル証明書に記録される情報自体の信用度向上は、発行機関自体の信用度を含む発行プロセスの信頼性向上のいち要素に過ぎず、その他の「基準・ルール」「基準への準拠を担保する仕組み」などについても、依然、重要であることに変わりはない。**

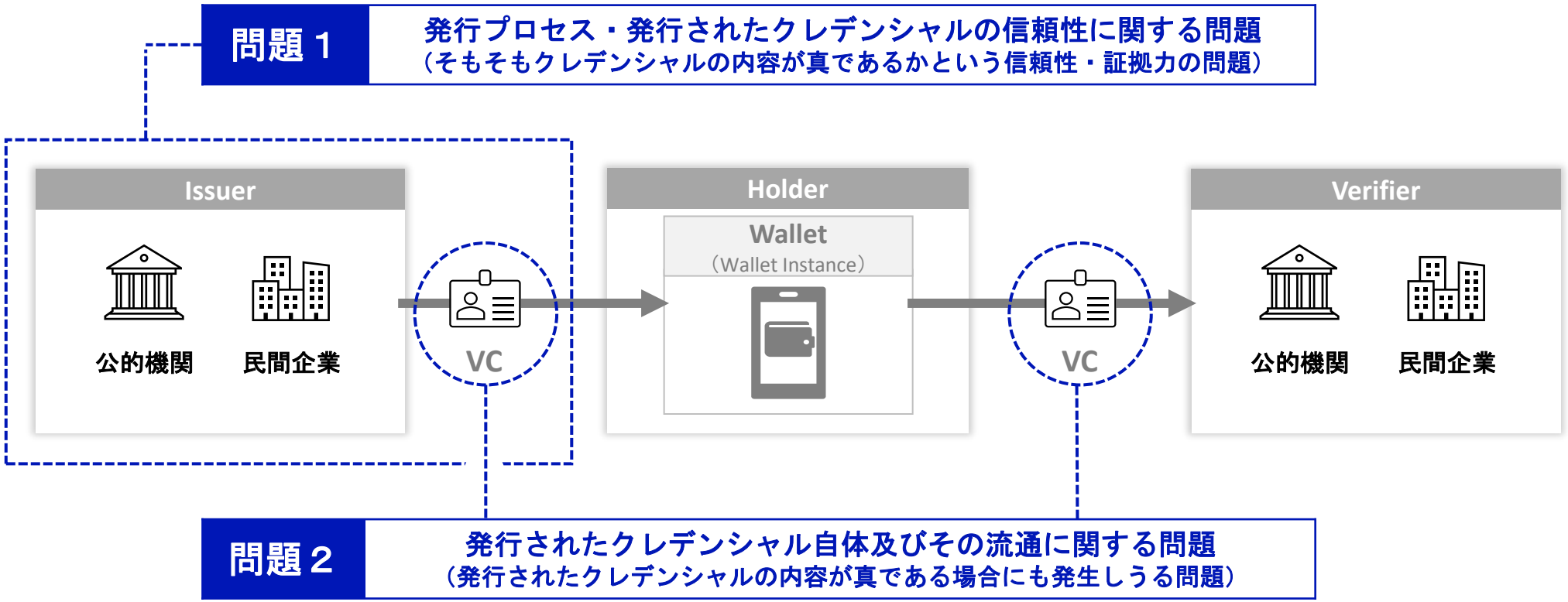
3-5. 各種法令・制度・仕組みとの関連性及び留意点のまとめ

3-1 IHVモデル	-
3-2 発行者に対する法令・仕組み等	• 公開鍵基盤（PKI）は、認証局（CA）が発行する電子証明書に対する信頼性と安全性を担保するための仕組みや議論の積み重ねがあるが、**VCは未成熟な点が多く整理が必要**なのではないか。 • デジタル証明書の発行者に対する規律として、身元確認方法などの「**発行の(業務)プロセス自体を定めるもの**」と、これへの準拠を担保するための監査や罰則等を定める「**発行者の性質や発行プロセスを担保するもの**」が存在するのではないか。 • VCの発行に際して、正当な権限を有さない第三者による書類の複製・派生行為は、この一意性を喪失させるものであるため、**原本と同等の性質を持つ書類として利用・流通することは困難**ではないか。
3-3 検証者に対する法令・仕組み等	• デジタル証明書の検証者に対する法令として、とくにリスクが高い手続・確実な本人確認が行われる必要がある手続等において、**検証者が本人確認を行うこと及びこの方法を規定するものがある**。 • 手続ごとのリスクは様々であり、VCを利用した本人確認についても、その**手続ごとのリスクプロファイルを踏まえ**、この対策として十分な水準を満たす手続から、徐々に利用が拡大するものと考えられるのではないか。
3-4 プロセスに依らずに規律を求める法令等	• 本人確認等のプロセスについて直接規定する法令以外でも、プロセスに依らずに規律を求める法令や規約等の順守、その他消費者に対する配慮が必要となる点が考えられ、**VCの利活用においても、そのユースケースや利用形態によって、未整理の論点が存在する可能性がある**ことに留意するべきでないか。
参考 カード代替電磁的記録との相違点	• カード代替電磁的記録及びVerifiable Credentialは、いずれもスマートフォンにおいて活用できるデジタル証明書の一種であるが、カード代替電磁的記録は物理マイナンバーカードの「代替」たる電磁的記録として、法令によりその発行手法、利用手法が厳格に規定されている。 • 第三者機関がマイナンバーカードを利用した派生的なクレデンシャルを作成・活用した場合も情報の最新性や信用性を担保する仕組みを講じることは可能だが、**発行プロセス全体の信頼性向上には、基準・ルールの遵守などについても依然重要である**のではないか。

4. 各種法令・制度・仕組みを踏まえたVCの利用

4-1. VC利用時の考慮事項のイメージ

各種法令・制度・仕組みにおいて取られている対策等も踏まえ、VCの利用に際し事故及び不正に繋がる問題例として下記が考えられるのではないか。また、不正利用時のリスクが大きい本人確認における利用においては、これらにとくに留意するべきではないか。



4-1. VC利用時の考慮事項のイメージ

問題１

発行プロセス・発行されたクレデンシャルの信頼性に関する問題（そもそもクレデンシャルの内容が真であるかという信頼性・証拠力の問題）

3-2章整理

クレデンシャルに格納された内容に関する信頼性

- クレデンシャル発行時の確認プロセス等の不備、不正確・古い情報に基づくクレデンシャルの発行　など

クレデンシャルのライフサイクル（ステータスの変化・失効管理等）管理に関する信頼性

- 失効メカニズムの不備、有効期限の管理不足 など

クレデンシャルの発行者自体の信頼性

- 正当な証明権者であるか（Authoritative source（権威ある情報元）へのアクセスを持つ者か）、管理体制、発行プロセスの透明性　など

問題２

発行されたクレデンシャル自体とこの流通に関する問題（発行されたクレデンシャルの内容が真である場合にも発生しうる問題）

3-2章整理

IssuerとVerifier間における認識の不一致（クレデンシャルの機能等に関する誤解・誤認）

- クレデンシャルの使用目的に関する認識の相違（本人確認と属性証明の誤解・誤認等）
- クレデンシャルに記載された内容の機能に関する誤解（情報の最新性等）

3-3章整理

Verifierにおける確認の不足

- Walletから提示されたVCは正当な保有者から提示されたものか（Holder（人）とWalletのバインディング（結びつき））　など
- クレデンシャルの発行者の確認、クレデンシャルの失効の確認　など

3-4章整理

プライバシー、セキュリティ、その他利活用に関する問題

- 名寄せリスク、過剰なデータの開示、Holderのウォレットのセキュリティ、QRコードやリダイレクトによる攻撃、相互運用性の欠如、運用者の移行・永続性　など

4-2. VC利用時の考慮事項を踏まえた対応の考え方

「4-1. VC利用時の考慮事項のイメージ」に挙げた考慮事項を踏まえた、Issuer、Verifierにおける対策の原則となる考え方としては、以下のように整理できるのではないか。

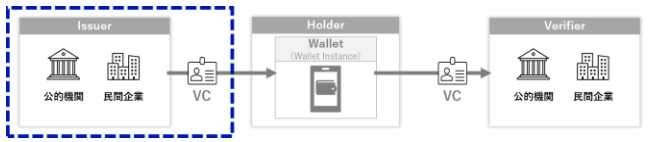
問題１　発行プロセス・発行されたクレデンシャルの信頼性に関する問題（そもそもクレデンシャルの内容が真であるかという信頼性・証拠力の問題）

- クレデンシャルに格納された内容に関する信頼性
- クレデンシャルのライフサイクル（ステータスの変化・失効管理等）管理に関する信頼性
- クレデンシャルの発行者自体の信頼性

問題２　発行されたクレデンシャル自体とこの流通に関する問題（発行されたクレデンシャルの内容が真である場合にも発生しうる問題）

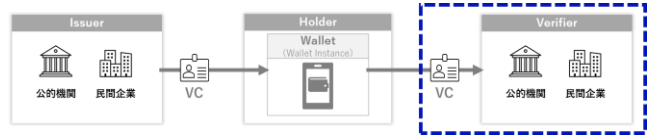
- IssuerとVerifier間における認識の不一致（クレデンシャルの機能等に関する誤解・誤認）
- Verifierにおける確認の不足
- プライバシー、セキュリティ、その他利活用に関する問題

対応１



Issuerにおいて、一次情報源や発行プロセス等を踏まえ、発行するVCが何を証明するクレデンシャルかを正確に把握し、伝達する。

対応２



Verifierにおいて、検証の目的上求められる証明の要件・リスクを正確に把握した上で、必要十分な証明が可能なVCのみを受け入れる。

4-3. VC利用時の要件（Issuer関係）

対応１ Issuerにおいて、一次情報源や発行プロセス等を踏まえ、発行するVCが何を証明するクレデンシャルかを正確に把握し、伝達する。

考慮すべき観点の例※１

証明内容の性質・一次情報源との関係

情報源・証明権限の所在

- 一次情報源はIssuerが所持・管理するものか（Authoritative source（権威ある情報元）を管理する者か）
- Issuerは当該情報の正当な証明権者か
- 派生クレデンシャルの場合、関係するすべての検証プロセスが担保されているか

※次頁で詳細補足する

情報の時間的有効性と更新性

- VCに記載する内容（属性等）は将来の更新や変更が生じうるものか
- 有効期限や失効メカニズムは適切に管理しているか

発行プロセスの信頼性

発行プロセス

- 本人確認・身元確認の厳格性
- 発行時の身元確認はどのレベルで行うか
- なりすまし防止対策（クレデンシャルとHolder, Walletのバインディング等）は十分か

プロセスの規定根拠

- 発行プロセスの根拠（法令・業界ルール等）は何か
- そのプロセスは外部から透明か

Issuer自体の信頼性

- Issuerの実在性や真正性はどう保証しているか
- Issuerの変更・廃止時の対応計画はあるか

情報の開示と透明性

利用条件と制限・責任の明示

- Issuerの責任範囲は明確か
- VCの想定利用範囲や制限は明示しているか
- VerifierやHolderの証明書の性質や実現できる内容に関する誤認を防止する措置が取られているか

ただし、当該事項の実施に関しては、Issuerによるリスク評価及び検討結果に基づき、低リスクと判断される場合において、適切な情報開示を前提として、一部の要件を緩和することも可能だと考える。また、Verifierにおいても、適切にリスク評価を行い、リスクに応じた適切な対応を実施する必要がある。

※１：必ずしも観点のすべてを網羅しているわけではない

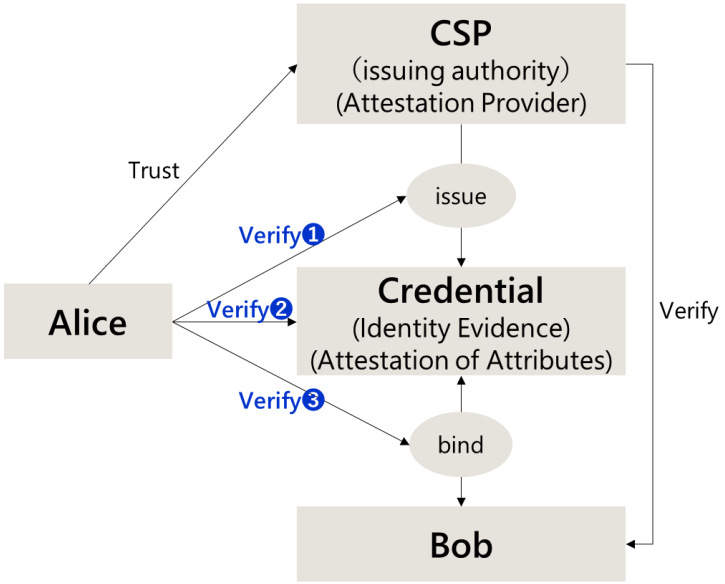
4-3. VC利用時の要件（Issuer関係）

対応１ Issuerにおいて、一次情報源や発行プロセス等を踏まえ、発行するVCが何を証明するクレデンシャルかを正確に把握し、伝達する。

参考：「情報源・証明権限の所在」補足

事務局イメージとして、一次情報源から発行したVCと、第三者機関の情報源から発行したVCの検証プロセスの差異を下記に示す。
後者の場合、前者に比べて検証プロセスの多層化・複雑化を招き、相応のリスク対策や信頼性を担保するための仕組みが必要となる。

一次情報源から発行したVCの検証プロセス

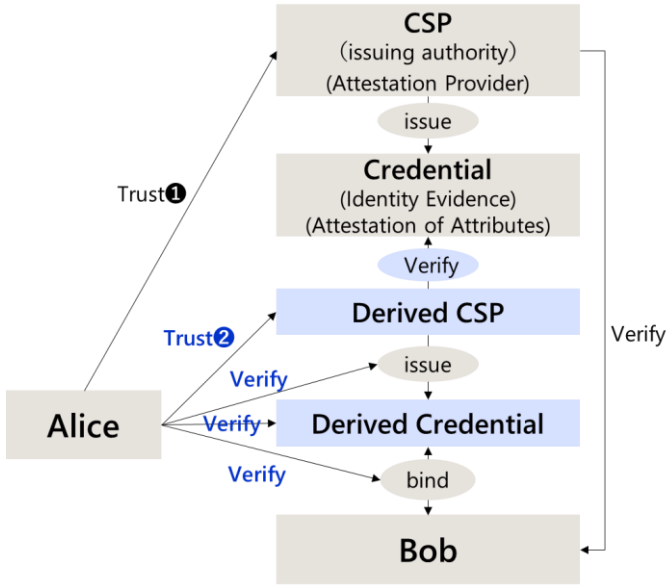


基本的なトラストモデル
AliceはBobを直接Verifyせず、代わりに信頼するCSPによるVerifyの結果（Credential/Evidence/Attestation）をもって、Bobを間接的にVerifyする。

間接的なVerify
Bobを直接Verifyする代わりに以下の3点をVerifyする。

❶Credentialが信頼するCSPによって発行されたものであること
❷Credentialが真正であり、偽造や改ざんがされていないこと
❸CredentialがBobに紐づいているものであり、他人にものでないこと

第三者機関の情報源から発行したVCの検証プロセス



4-3. VC利用時の要件（Verifier関連）

対応２　**Verifierにおいて、検証の目的上求められる証明の要件・リスクを正確に把握した上で、必要十分な証明が可能なVCのみを受け入れる。**

考慮すべき観点の例※1

VerifierはVCの利用形態に応じた適切なリスク評価を行うべきである。また、ある主体に関する情報は広義に「属性情報」と捉えられるが、**その検証目的や不正利用のリスク等に応じて、本人性の厳密さやリアルタイム性等の要件・対策は異なる**こと（※）に留意すべきである。※例えば、飲食店における学生割引の適用と、法令により厳格な本人確認が要求される場合とでは、求められるリスク対応のレベルが異なる。

属性情報（attributes）　VCで証明される内容

例）氏名、生年月日、住所、性別、所属組織、能力・技能の評価、収入、支払い履歴、学修歴　等

属性証明　検証できる属性情報として（事実の確認）

属性証明の確認（事実の確認）を踏まえて資格の保有を確認するといった目的があることが想定される。

資格証明　属性情報を何等かの権利・許可を得るための資格として検証

本人確認（身元確認・当人認証）の結果、資格証明や属性証明を行う場合や、本人確認を目的としたクレデンシャルにより属性や資格の確認を行うことも考えられる。

例）年齢の検証　→　酒類の購入資格の確認　等
　　納税証明書の検証　→　非課税世帯を対象とした給付を得るため　等

本人確認　識別可能・実在性などを確認できる属性情報による身元確認（＋登録済みのクレデンシャルを用いた当人認証）

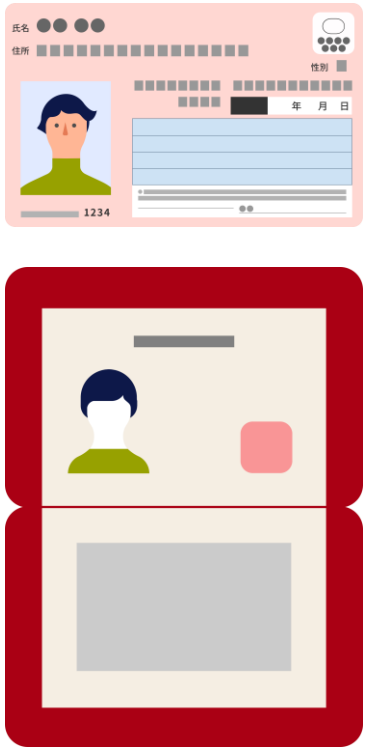
不正利用のリスクを踏まえ、複製の防止、偽造防止の対策の実施や、明示的な有効期限が設けられる場合が多い。

例）定期的な実在性の確認、時間経過による容貌の変化への対応　等

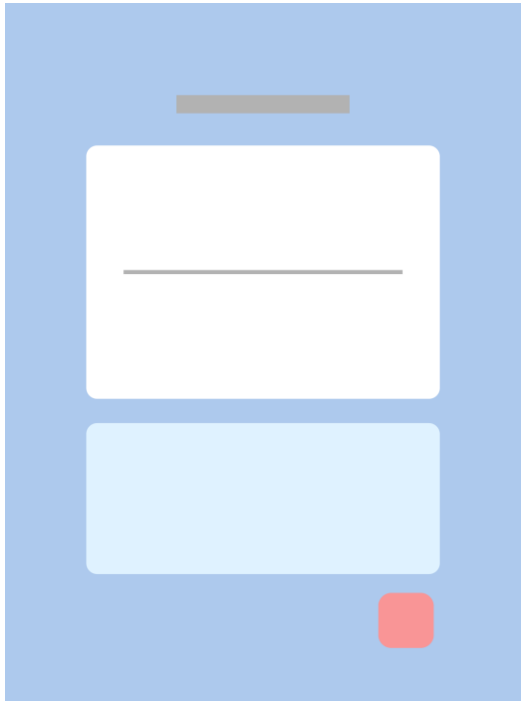
※１：必ずしも観点のすべてを網羅しているわけではない

参考：属性確認と身元確認との関係について

- 属性に関する証明書・資格に関する証明書は、原則として、これ単体では身元確認を行う要素とはなり得ない※。
- VCについても、複製を防止する機能、利用時の当人認証等の対策が無い限り、単に属性を証明するものに過ぎない。身元確認（予め身元確認が行われたアカウントにおいては当人認証）を行うなどして、提示した者の身元を確認しない限り保有者の属性証明にはならない。
- 身元確認には本人と保有者との紐付けを行うことができる写真付き身分証や公的個人認証サービス等を利用することが一般的。



本人確認書類
による本人確認
（身元確認）



属性に関する証明書
（卒業証明書等）
による属性確認

※最初から本人確認を行うことを目的として発行された、適切な対策が施されている本人確認書類を除く。

4-3. VC利用時の要件（Verifier関連）

対応２ Verifierにおいて、検証の目的上求められる証明の要件・リスクを正確に把握した上で、必要十分な証明が可能なVCのみを受け入れる。

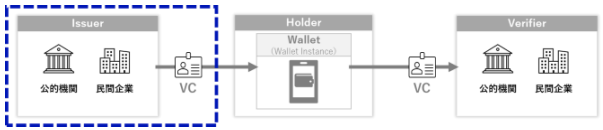
VCの例とその検証用途の組み合わせ（事務局イメージ）

例	発行者 / 証明権者	一次情報源	発行先 / 名宛人	利用用途	リスクを踏まえ想定されない用途	リスクを踏まえ利用時に検証すべき要素の代表例
卒業証明書	学校（学長・学部長等）	学籍簿等	特定の卒業生	• 対象人物が学校を卒業した事実、対象人物が学位取得の事実　など	• 本人確認（身元確認・当人認証） ※発行者が想定していない用途	• **「発行者」が正しい発行者（学校）であること、その他フォーマット等真正な書類**であることの検証 • **「申請者」が「発行先・名宛人」本人**であることの検証（証明書と申請者の結びつき（バインディング）の確認）
学生証	学校（学長・学部長等）	学籍簿等	特定の学生	• 身元確認（低リスクであるもの） • 学内サービス・連携サービスのための当人認証の要素として（出席確認、証明書発行機等） • 対象人物が現在学生である事実（属性証明）、ひいては学割資格を持つ者であることの確認　など	• 身元確認（高リスクであるもの） ※入学時等の身元確認等を踏まえて作成される学籍簿等は、人物の実在性を一定程度保証するが、実在する特定の人物であることを証明することは主目的ではなく、住所の確実性、同姓同名との取り違え等のリスクへの考慮が十分でない。	• **「発行者」が正しい発行者（学校）であること、その他フォーマット等真正な書類**であることの検証 ※物理的な身分証においては、有効期限・利用期限を設定する等してリアルタイムで失効できないリスクを低減。デジタルにおいても、定期的な実在性の確認等の観点からリスクの低減に役立つ。 • **真正であると確認された書類上の人物と手続を行っている「申請者」が同一人物で**あることの確認
委任状	委任者（またはこの委託を受けた者等）	委任者	特定の受任者	• 受任者が契約・手続等を行う権限・資格を有していることの確認	• 受任者の身元確認	• **証明書のフォーマット等真正な書類**であることの検証 • **「委任者」が契約・手続等を行う正当な権限・権利**を有していること • **真正であると確認された書類上の受任者と手続を行っている「受任者（申請者）」が同一人物**であることの確認

4-4. まとめ：推奨されるVCの利用形態とは？

これら議論を踏まえ、VCの社会一般への普及のためには、利用者やVerifierにとって安心・安全な利用形態であることが重要であると考えられる。例えば、プライバシーに配慮したユースケースを実現できる技術であっても、正しく利用せず事故等が発生すると、普及の妨げになる可能性がある。これら観点から、**検討事項が少なくメリットが大きい事例を初期ユースケースとして推奨すべきではないか。**

対応１



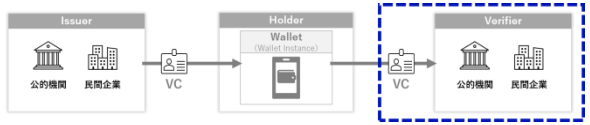
Issuerにおいて、一次情報源や発行プロセス等を踏まえ、発行するVCが何を証明するクレデンシャルかを正確に把握し、伝達する。

考慮すべき観点の例

Issuerは下記を正しく把握・実施

- 証明内容の性質と一次情報源との関係
- 発行プロセスの信頼性
- 情報の開示と透明性

対応２



Verifierにおいて、検証の目的上求められる証明の要件・リスクを正確に把握した上で、必要十分な証明が可能なVCのみを受け入れる。

考慮すべき観点の例

Verifierは下記を正しく把握・実施

- VCの利用形態に応じた適切なリスク評価を行う
- 検証の目的や不正利用のリスク等に応じて、本人性の厳密さやリアルタイム性等の要件や対策は異なることに留意する

考慮すべき観点を踏まえ推奨されるVCの初期ユースケースの性質（イメージ）

- **発行者が情報源を管理する（証明権者となる）属性に関するもの**
- **不正利用のリスクが高い手続に用いる書類・証跡・属性であって、<u>現在機械可読ではない・デジタル署名が伴っていない</u>もの**

今後ユースケースを拡大するためには、議論の積み上げが必要ではないか。

5. 議論のポイント

5-1. ご議論いただきたいポイント（1/2）

これまでの事務局の整理を踏まえて、下記についてご議論・コメントいただきたい。

本日ご議論いただきたいポイント

①現行法令・制度との関連性と留意点について

本人確認（とくに身元確認）用途にVCを利用する場合に留意すべき点、VC一般において留意するべき点全般について、適切な整理となっているか。

A) **「3. 各種法令・制度・仕組みとの関連及び留意点」について** 20分程度

- 事務局整理を踏まえ、とくにVCを本人確認の用途に利用するうえで、安心・安全なVCの利活用を進めるためには、どのような点に留意するべきか。
- 安心・安全に利用できる環境の構築に向けてどのような対応（個々の事業者・業界・国）が望まれるか。

B) **「4. 各種法令・制度・仕組みを踏まえたVCの利用」について（4-1節～4-3節）** 25分程度

- 留意点・考慮事項に対する適切な対応となっているか。また、より適切な対応が考えられないか。
- とくに優先順位が高い留意点・考慮事項はどの点か。
- 他に考慮すべき事項・課題があるか。

5-1. ご議論いただきたいポイント（2/2）

これまでの事務局の整理を踏まえて、下記についてご議論・コメントいただきたい。

本日ご議論いただきたいポイント

②推奨されるVCの利用用途について　15分程度

C)　①の議論や「4-4. まとめ：推奨されるVCの利用形態とは？」を踏まえた推奨されるVCの利用用途やユースケースについて

- 事務局の整理（考慮すべき観点を踏まえ推奨されるVCの初期ユースケースの性質）が適切か。
- 上記を踏まえ、具体的なユースケースとしてどのようなものが考えられるか。（官・民それぞれ）

デジタル庁

Digital Agency