

本資料は「属性証明の課題整理に関する有識者会議」での議論を取りまとめることを目的としたものであり、何ら決定・確定されたものではない。また、現時点で準拠を求めるものではない。

## 別紙 3

### 行政機関における VC 及び DIW の活用にあたる検討事項リスト（案）

#### 本検討事項リストの概要・位置づけ

本検討事項リストは、最終的には各証明書制度の所管省庁等の行政機関が VC・DIW の導入判断時や導入判断後の検討の一助として、検討すべき事項を網羅的に把握できるチェックリストのような形で活用することを想定している。

今年度の段階では、デジタル庁の検討事項や証明書所管省庁等における検討事項を分離せず、委員の助言を基に、導入に必要な検討事項を洗い出した状態となっている。証明書等このため、現時点では精査前の段階であり、準拠を求めるものではない。また、本検討事項リストには今後策定予定の関連ガイドラインに記載しない事項も含まれ得る。本リストの洗い出し結果を踏まえて、次年度以降に検討主体を振り分けつつ、具体的な検討を進めることを予定している。

#### 本検討事項リストの使い方（判断の順序）

- (1) A 章：ユースケースを記述する
- (2) 要求保証レベルを定義する（発行・保持・提示・検証の観点に分解して整理する）※今後整理予定
- (3) B 章：アーキテクチャを比較・選定する（フォーマット・プロトコル・信頼モデル・状態確認）
- (4) C 章：ライフサイクル対策を整理する（ユースケースに応じて MUST・SHOULD・MAY を付与する）
- (5) D 章：ガバナンス設計を整理する（登録・認定、監査、インシデント対応、救済）

## 目次

A.	ユースケースに関する検討事項	4
A1.	対象とするユースケースの明確化	4
A2.	VC・DIWによる証明書のデジタル化に求められる業務的要件	4
A2-1.	VC・DIWによって解決を目指す現状の紙等の運用における課題やニーズの特定	4
A2-2.	手続や証明書が満たすべき業務要件の明確化	5
A3.	VC・DIWの導入の阻害要因となり得る制約	7
A3-1.	既存の法令・制度の改正の必要性の明確化	7
A3-2.	ステークホルダの意向や協調可否の明確化	7
A3-3.	現行システムやインフラの制約の明確化	7
A3-4.	業務環境や業務実態との適合性の明確化	7
B.	アーキテクチャに関する検討事項	8
B1.	プライバシー共通原則	8
B2.	ユースケースの業務的要件に適した標準仕様や実装	8
B2-1.	VCのフォーマットとプロトコルの選定	8
B2-2.	Walletの機能・形態の検討	9
B3.	各ステークホルダの信頼性を検証するための仕組み	9
B3-1.	Issuerの信頼性を検証する仕組みの検討	9
B3-2.	Holderの信頼性を検証する仕組みの検討	9
B3-3.	Walletの信頼性を検証する仕組みの検討	10
B3-4.	Verifierの信頼性を検証する仕組みの検討	10
B3-5.	その他の信頼性を担保する仕組みの検討	10
B4.	アーキテクチャに関するその他の検討事項	10
B4-1.	識別子のあり方の検討	10
B4-2.	失効・状態管理のあり方の検討	10
B4-3.	公開鍵基盤のモデルの検討	11
B4-4.	技術的相互運用性の確保の検討	11
B4-5.	その他の検討	11
C.	VCの各ライフサイクルにおける技術的対策	11
C1.	VCの発行時に求められる技術的対策	11
C1-1.	IssuerによるHolderの正当性の確認（本人確認等）のあり方の検討	11
C1-2.	発行時の攻撃対策の検討	12
C1-3.	VCとHolderの紐づけ方法の検討	12
C2.	VCの保持時に求められる技術的対策	12
C2-1.	スマートフォンの盗難対策の検討	12
C2-2.	Holderの暗号鍵の窃取・悪用対策の検討	12
C2-3.	VCの窃取・悪用対策の検討	12
C2-4.	その他の対策の検討	12
C2-5.	Wallet ProviderによるWallet内のデータの不正な閲覧対策の検討	13

C2-6.	Wallet ProviderによるWalletの利用履歴等の収集対策の検討 .....	13
C2-7.	スマートフォンの紛失、故障、機種変更、通信ができない場合を想定した対策の検討 .....	13
C3.	VCの提示時・検証時に求められる技術的対策 .....	13
C3-1.	提示時の中間者攻撃対策の検討 .....	13
C3-2.	第三者（偽のVerifier）によるHolderに対するフィッシング対策の検討 .....	13
C3-3.	偽造・改ざんされたVCや不適切なVCの提示に関する対策の検討 .....	13
C3-4.	第三者によるVCの盗用やVerifierによるVCの不正利用への対策の検討 .....	13
C3-5.	Verifierによる必要以上の情報の要求（同意の強制・形骸化等）に関する対策の検討 .....	13
C4.	Verifierでの保存・利活用時に求められる技術的対策 .....	14
C4-1.	Verifierにおける利活用・保存ポリシーの明確化 .....	14
C4-2.	VCの漏洩対策の検討 .....	14
C4-3.	別のVerifierやIssuerとの結託による名寄せ対策の検討 .....	14
C4-4.	その他のプライバシー面の対策の検討 .....	14
C5.	その他全般において求められる技術的対策 .....	14
C5-1.	偽造・改ざんされたVCや不適切に発行されたVCへの対策の検討 .....	14
C5-2.	Issuerの秘密鍵の漏洩等に関する対策の検討 .....	14
C5-3.	エコシステムの継続性に関する対策の検討 .....	14
D.	エコシステムとガバナンスのあり方 .....	15
D1.	エコシステムのあり方 .....	15
D1-1.	エコシステムにおいて必要な役割と責任の検討 .....	15
D1-2.	エコシステムの普及・維持のためのインセンティブの設計 .....	15
D1-3.	普及促進や理解醸成の方法の検討 .....	15
D1-4.	エコシステムに関するその他の検討 .....	15
D2.	ガバナンスのあり方 .....	16
D2-1.	ガバナンスの確立のために必要となる制度の検討 .....	16
D2-2.	VC化した証明書の実効性等の検討 .....	16
D2-3.	法的・制度的相互運用性の検討 .....	16
(付録)	用語定義 .....	17

## A. ユースケースに関する検討事項

ここでは、VC や DIW を導入する機関における、業務的な要件や制約事項に関する検討事項を記載する。

### A1. 対象とするユースケースの明確化

- ユースケース名：どの手続・どの証明書（属性）を対象とするか。
- 提示の目的：何を証明・検証するために、その証明書（属性）を提示するのか。
- 対象者と役割：Issuer・Holder・Verifier・Wallet Provider・ガバナンス主体・その他のステークホルダ（AI Provider 等）は誰か。それぞれどのような役割を担うのか。
- 提示シーン：対面・遠隔での提示のどちらを主とするのか。オンラインでの提示を可能とするのか、オフライン提示・検証は必要か。
- 提示相手の範囲：提示先（Verifier）は限定されるべきなのか、あるいは不特定多数に提示可能とするべきか。
- 提示頻度：提示頻度や提示先数はどの程度か（追跡・名寄せリスクの評価に用いる）。
- 発行根拠：原簿・台帳・資格付与の根拠は何か。
- 更新頻度：更新頻度はどの程度か。
- 有効期限・失効：有効期限の設定は必要か。失効・状態管理は必要か。
- 機微性・影響度：誤発行・盗用・名寄せ等が起きた場合の被害はどの程度か。
- 既存運用との関係：紙や PDF 等との並行運用は必要か。（完全にデジタルに移行することは可能か。）
- 例外運用：代理提示時・端末非保有時・災害時・通信断時などの例外時の取り扱いは必要か。
- 期待効果（KPI）：申請・発行・提示・検証の時間・コスト・事故率等で何を改善するか。
- AI エージェントの介在：利用者本人ではなく、AI（エージェントブラウザ等）が Wallet を操作して提示や申請を行うことを想定するか。

### A2. VC・DIW による証明書のデジタル化に求められる業務的要件

#### A2-1. VC・DIW によって解決を目指す現状の紙等の運用における課題やニーズの特定

- 利用者の課題・ニーズに対して VC・DIW で何を解決するか。
  - 利便性：発行申請・保管・提示における利便性の課題において VC や DIW で解決できる点は何か。  
（手動での手続が煩雑、紙の書類がなくなる、書類の紛失のリスクがある、再発行が困難、遠隔での申請手続きができない、窓口の空いている時間しか申請ができない 等）
  - プライバシー：プライバシーの課題において VC・DIW で解決できる点は何か。  
（不要な情報提示、提示先同士の結託による名寄せや、発行元に提示先が知られてしまう、提示後に開示情報の修正・取り消しができない 等のリスク）
  - コスト：証明書の申請・交付時に必要となる申請・郵送費用等の削減につながる点は何か。  
（窓口へ出向くコスト（交通費等）、手数料、待ち時間、郵送に係る費用 等）
  - 信頼性：悪意あるステークホルダによって不正に情報がやり取りされたり、意図しない手続が行われたりすることをどの程度防ぐべきか。（本人の同意のない情報提示、なりすまし 等）
  - その他：その他の VC や DIW で解決できる課題やニーズは何か。（申請書の入力ミス 等）
- 発行者の課題・ニーズに対して VC・DIW で何を解決するか。

- 事務負担：電子化・オンライン化による証明書発行事務において VC や DIW で解決できる負担は何か。（窓口対応工数・郵送対応工数 等）
- コスト：証明書の発行時において VC や DIW で削減できるコストは何か。（印刷費用・郵送費用 等）
- 当人性：手続において VC や DIW で解決できる当人性の課題は何か。（正しい VC の発行対象者（subject）に発行できること、当該本人以外が VC を利用できないこと 等）
- 信頼性：VC や DIW で解決できる信頼性の課題は何か。（発行した VC が改ざんされないこと、（発行者が意図した以上に）複製されないこと 等）
- 証明書の正当な発行主体：各法令・制度に基づくと、どの行政機関・民間企業等が証明書の発行主体たり得るか。
- 検証者の課題・ニーズは何か。
  - 信頼性：VC や DIW で解決できる信頼性の課題は何か。（改ざんの検知、本人以外からの提示の検知、証明書や署名の失効の検知、発行者の特定 等）
  - コスト（事務負担）及び投資対効果：VC や DIW で削減できるコストは何か。（受理した証明書の検証事務負担、社内システムへの転記作業等の負担等）VC の読取り機器等のコストが有人の作業コストを上回るか、新サービス展開時は新サービスでコストを吸収できるか。
  - データ利活用：VC や DIW で満たせるデータ利活用のニーズは何か。（機械可読化による検証データの AI 活用 等）
    - ◇ （参考情報）既存システムで VC を取り込み自動化処理するための雛形を提供することも考えうる。
  - データ管理負担の軽減：VC や DIW で削減できるデータ管理の負担は何か。（必要以上の個人情報を受領することによる管理負担、漏えい時の被害や対応負担 等）
- その他の関係者の課題・ニーズは何か。
  - 同意取得の手続の簡素化：本人同意取得の手続きの簡素化を求めるか。（バックエンドとの対比）
  - 利用シーンの拡大：将来的な相互運用性の向上や、それによる利用シーンの拡大を求めるか。
  - 外国における利用：大使館や領事館での手続・在外投票・外国における日本企業の手続等が必要か。
  - 国際的な相互運用性：国内だけでなく諸外国との相互運用性を求めるか。
  - 情報連携の拡張容易性：システムの疎結合による情報連携の拡張容易性や、それに伴う実現コストの削減を求めるか。
  - 新たな価値の提供：新たなサービスの創出の可能性があるか。（無人化や自動化 等）
  - データ定義の標準化：同種の情報を含む複数の証明書間で、意味の変換を伴わずに利用可能にする必要があるか。
  - API 等の標準化：同じ属性・資格の証明書であれば複数のステークホルダ間でシステム変更を伴わずに利用可能にする必要があるか。
  - 個人を介した情報連携：利用者を介した情報連携を求めるか。（マイナンバー法の制約等で行政機関間の情報連携が出来ない証明書をデジタル化する場合など）

## A2-2. 手続や証明書が満たすべき業務要件の明確化

- 証明書にはどのような要件が求められるのか。
  - 証明書の目的種別：証明書にどのような機能を求めるのか。（本人確認、資格証明、属性証明 等）
  - 証明書の有効期限：証明書に求められる有効期限の長さはどの程度か。
  - 署名の有効期限：署名に有効期限を設定する必要があるか。また、求められる期間はどの程度か。

- 失効管理：Issuer や Holder による手続によって有効期間内の証明書を失効する必要があるか。（その状態を Verifier が検知できる必要があるか。）手続から反映にどの程度リアルタイム性を求めるか。（手続後の即時反映、日次での反映 等）。
- 同時発行数の制御：複数の VC を同時に発行可能とするか。（1 枚に制限する必要があるか。）
- 提示回数の制御：1 つの VC を何度も提示可能とするか。（一度のみの提示に制限する必要があるか。）
- 機微な情報の保護：個人情報などの機微な情報についてプライバシー保護を特に考慮する必要があるか。（特に提示先が多い場合や、提示頻度が高い場合は留意が必要）
- 複数 VC の提示：他の VC と同時に提示できる必要があるか。
- 複数 VC の対象者の紐付け：複数の VC の対象者が同一人物であることを紐付け・証明しながらまとめて提示する必要があるか。
- 多言語対応：日本語以外の属性も含めるか。ふりがな・ローマ字・外字の扱いなどの考慮事項はあるか。
- 意味的相互運用性の確保：証明書に含まれる属性情報のうち、他の証明書などとの意味的な相互運用性（Semantic Interoperability）を確保する必要がある属性はどれか。
- 当人性：同一の Verifier に対して複数回同種類の VC を提示した際に、同一人物であることが特定できる必要があるか（例えば、氏名・生年月日等では唯一に特定できない場合がある他、改姓改名等で特定できない場合もある）。
- データ項目の互換性：VC 化に際して資格・属性証明書の統一化を図る必要があるか。
- 証明書の取扱いにどのような要件が求められるのか。
  - 情報のマスキング等の必要性：特定の情報に限って証明書を発行する、特定の情報のみをマスキングして提示するなどの運用上の情報のコントロールが求められるか。
  - 発行の場面：VC の発行は対面・非対面（オンライン）のいずれか（又は両方）で行う必要があるか。（従来は対面で発行していた証明書の場合、非対面での発行することは許容可能であるのか。）
  - 提示の場面：VC の提示は対面・非対面（オンライン）のいずれか又は両方で行う必要があるのか。
  - 提示環境の条件や制約：提示を行う環境に条件や制約はあるのか。（Wallet・Verifier がインターネットに接続できない環境での提示が必要 等）
  - 提示後の VC 取り扱い：検証した後の VC を Verifier 側で保管する必要があるか。その場合、保管期間やアクセス権、管理や破棄の手順はどうあるべきか。
  - 再提示：VC を受領した Verifier がさらに別の Verifier に VC を再提示する必要があるか。（例：年末調整に関する書類を従業員から受領した企業が税務署に提出する 等）
  - 人間の関与：提示の際、常に人間による生体認証を必須とするか。あるいは特定のリスクが低い属性証明（年齢確認のみ 等）については AI による自動提示を許容するか。
- 用途による要求事項の違い：同じ証明書でも用途によって大きく要件に差異がある点はあるか。また、要件が異なる場合、異なる証明書として発行すべきか。
- 本来用途以外の用途：本来の資格が意図しないが、広範に普及した用途をカバーするべきか。（例：運転免許証による本人確認、健康保険証でのビル入館手続 等）
- 代理・代行提示：未成年、成年後見、家族手続、法人代表等において、本人以外の提示（代理提示）を許容する必要があるか。許容する場合、どのように正当性（権限）を確認するべきか。
- 端末非保有・利用困難者への対応：想定利用者がスマートフォンを所持していない、利用が困難な場合の代替手段（紙・窓口・代理・委任等）をどのように設計するべきか。
- 災害・通信断時の例外運用：通信断・停電等によりオンライン照会ができない場合でも、提示・検証・業務継続

が必要か。必要な場合、どの範囲をオフラインで成立させるべきか。

### A3. VC・DIWの導入の阻害要因となり得る制約

#### A3-1. 既存の法令・制度の改正の必要性の明確化

- 法令・制度改正の必要性：既存の法令において電磁的記録の発行・受入を阻害する規定があり、法改正が必要か。（例：「書面による」、「対面による」、「携帯しなければならない」などの記載）
- 法令・制度改正の実現性：法改正・制度改正が必要な場合、改正に伴う影響を踏まえると実現は可能か。

#### A3-2. ステークホルダの意向や協調可否の明確化

- ステークホルダ：IssuerやVerifierやそのユースケースにおけるガバナンスを担う役割として、どのような組織やコミュニティが関係するか。
- ステークホルダのシステム調達の実現可否：各ステークホルダにおけるシステム改修やシステム調達が必要な場合、実現可能か。
- 関連する他の証明書：システムを共有したり、ガバナンスや運用の水準の整合性を取ったりする必要のある他の証明書はあるか。

#### A3-3. 現行システムやインフラの制約の明確化

- アプリケーション面の制約：VCの発行・提示を行うアプリケーションにはどのような条件や制約があるか。（例：スマートフォンの利用が必要、Webブラウザからの利用が必要等）。
- ネットワーク面の制約：VCの発行や提示に関係する企業や自治体の関係システムには、どのようなネットワーク面の条件や制約があるか。（例：VCの提示先となるシステムがインターネットから分離されている等）
- 関連システムとの関係：既存システムの改修や連携は必要か。必要だとすると、それはどのような要件で実現するべきなのか。もし連携ができない場合にどのような要件が求められるのか。

#### A3-4. 業務環境や業務実態との適合性の明確化

- 利用者環境：
  - デジタルリテラシー：想定利用者はスマートフォンの扱いなど一定のデジタルリテラシーを有しているか。
  - スマートフォンを保有していない場合の代替手段：印刷したQRコード等によるVCの発行は必要か。
  - スマートフォン対応機種：どの程度古いスマートフォンまで動作保証すべきか。必要な機能が充足されていないスマートフォンへの代替手段が必要か。（QRコード形式のVC、VCを全く使わない手段等）
  - 利用者の利用環境：スマートフォンなどの電子機器は提示現場に持ち込み可能か。通信環境はあるか。
  - VCの提示環境：窓口での提示を行う場合、どのような端末やネットワーク環境が窓口で利用可能であるか。スマートフォンを所持しない方向けの共用端末等は用意できるか。
- 発行業務の実現性：発行業務を担う者のスキルなどを踏まえて、VC発行業務を現実的に実施可能か。
- 発行システム構築・運用の実現性：システムの構築・運用コストも含めて対応が可能か。
- 既存の業務プロセスへのVCの適合性：検証者はVCによって証明書の何を確認するのか。（例えば、真正性だけでなく、他の証明書と突合してデータの妥当性も確認するなど）確認業務は現実的に実施可能か。確認した結果をどのように記録するのか。既存の業務プロセスに組み込み可能か。
- VCの外観：業務要件を満たすために、VCはユーザーにとってどのような見た目であるべきか。（レイアウトや表示・非表示項目はどうあるべきか。）

- VC の呼称：その証明書の VC について、類似の名称を他者に利用されないよう商標取得などを検討すべきか。（特に政府や公共機関の発行する VC の場合は、類似名称を民間事業者に使われてしまった場合に公共性が損なわれる可能性があり、留意する必要がある。）
- ユーザー体験：ユーザーがどのような状況に置かれており、VC や DIW によってどのようなユーザー体験を提供する必要があるのか。そのために求められるユーザーインターフェースのあり方は何か。

## B. アーキテクチャに関する検討事項

ここでは VC を扱うためのアーキテクチャとして、考慮すべきプライバシーや技術標準、信頼を確保するための仕組みなどの検討事項について記載する。

### B1. プライバシー共通原則

- データ最小化：Issuer・Wallet Provider・Verifier・その他のステークホルダ（AI Provider 等）それぞれが取得し得るデータ（ログ、テレメトリ、提示履歴、照会履歴 等）を棚卸しし、取得・保持を最小化するべきか。
  - 原則不保持：提示・検証に不要なログ、テレメトリ、提示履歴は原則として保持しない設計を優先するべきか。
  - 例外の管理：例外的に保持が必要な場合、目的、保持期間、アクセス制御、監査可能性、第三者提供制限をセットで定義するべきか。
- 相関（名寄せ）抑止：提示履歴や照会履歴により、提示先同士・発行元等との名寄せが起きない設計となっているか。（相関し得る識別子やメタデータを含まないか。）
- 参照：C2-6「ログとテレメトリの最小化」、C4-3「目的外利用等の防止、保持期間の最小化」と整合させるべきか。
- 利用制限：Wallet Provider やその他ステークホルダ（AI Provider 等）による目的外利用をどのように防止すべきか。

### B2. ユースケースの業務的要件に適した標準仕様や実装

#### B2-1. VC のフォーマットとプロトコルの選定

- 採用フォーマット：要求事項を踏まえ、どのようなフォーマットを採用すべきか。
  - オフライン提示・検証：当該ユースケースにおいて、オフライン提示・検証（近接提示を含む）が必須か。
  - 選択的開示：選択的開示（必要最小限開示）が必須か。必須の場合、どの粒度（属性単位等）で必要か。
  - Holder Binding：VC と Holder・Wallet の紐づけ（Holder Binding、Key Binding 等）の必要性はどの程度か。
  - 失効管理：失効・状態確認（Status）の方式と、照会によるプライバシー影響（追跡・名寄せ）の許容度はどの程度か。
  - 実装容易性：デベロッパーの実装容易性をどの程度求めるか。
  - 実装成熟度の評価：実装成熟度、相互運用試験（テストスイート等）の見通しをどう評価するか。
  - 拡張性：将来拡張（アルゴリズム更新、鍵更新、属性追加・版管理）への適合性はどうか。
  - 複数フォーマット対応の責任分界：相互変換やプロファイル差分の吸収を、どの主体がどこまで責任を負うか。

- 複数フォーマットへの対応要否：複数の VC フォーマットに対応する必要があるのか。（発行者、ホルダー、検証者 3 者それぞれにおいて）
- データ定義の標準化：VC の中に記載される属性情報のデータモデルやスキーマ等のデータ定義の標準化は必要か。また、その標準仕様はどのように公開・メンテナンスされるべきか。
- API の標準化：VC を取り扱うための API 等の標準化は必要か。また、その標準仕様はどのように公開・メンテナンスされるべきか。
- プロトコルの選定：どのようなプロトコルを採用すべきか。
  - ローカル提示・リモート提示のどちらが、あるいは両方が必要か。
  - 認定された Wallet Provider や Wallet Instance の健全性について発行・提示時の確認を必須とするか。
  - 発行・提示時における Holder のローカル認証を必須とするか。
  - 認定された Verifier を提示時に確認することを必須とするか。（フィッシング耐性が必要か。）

## B2-2. Wallet の機能・形態の検討

- Wallet の必要性：業務要件を満たすために、そもそも Wallet は必要か。
- Wallet の提供モデル：民間事業者の Wallet を使うのか、あるいは政府自身が Wallet を開発・提供するか。
  - 複数の提供モデルの併用：利用可能な Wallet は単一か。（複数のモデルを選択可能とするのか。）
- 重視する発行・提示モデル：対面での提示において、インターネットを経由せずに現場の通信のみで提示できる必要があるか。それとも対面においてもインターネット経由での提示ができればよいか。
- 提示インターフェース：どのようなインターフェースで提示する必要があるか。（NFC、BLE、QR コード、ブラウザ経由 等）
- 利用デバイス・環境：Wallet はスマートフォンアプリだけでよいか。（それとも、一般的な Web ブラウザからも利用可能である必要があるか。）また、複数のデバイスから同一の Wallet を利用できる必要があるか。

## B3. 各ステークホルダの信頼性を検証するための仕組み

### B3-1. Issuer の信頼性を検証する仕組みの検討

- Verifier→Issuer の信頼モデル：どのようなモデルによって、Issuer を Verifier が信頼できる仕組みとするのか。（従来型の PKI、Web PKI、Trusted List 等）
- 既存インフラの活用余地：既存の PKI 等のインフラや制度をそのまま活用、あるいは拡張して利用できる余地はあるか。（GPKI、LGPKI、認定 e シール 等）
  - （参考情報）過去にワクチン接種証明書（国内向け：SHC、海外向け：VDS-NC）が VC として発行されている。システム構築に際しては、これらの発行実績が参考になる。
- 公証人モデルの要否：信頼できる第三者機関が、本来の Issuer に代わって VC を発行するモデルは必要か。その際の第三者機関をどのように信頼する仕組みとするのか。
  - （参考情報）各自治体が VC 発行システムを開発するのはコストもかかるため、行政から委任された第三者機関が発行する事は考えられる。その際、紙の原本ではなく、真正なデータを管理する DB から提供されるか。（DB 管理できていない場合は、紙から起こすことになると思われる）

### B3-2. Holder の信頼性を検証する仕組みの検討

- Issuer→Holder の信頼モデル：Issuer が Holder を信頼できる仕組みとしてどのようなものを想定するか。
- Verifier→Holder の信頼モデル：Verifier が Holder を信頼できる仕組みとしてどのようなものを想定するか。

### B3-3. Wallet の信頼性を検証する仕組みの検討

- Issuer→Wallet の信頼モデル：Issuer が Wallet やスマートフォンを信頼できる仕組みは必要か。
  - （参考情報）スマートフォンがもつセキュリティ機能（例えば Secure Element 等）によっては、プラットフォームのシステムを介して発行（書き込みを行う）することが必要な場合も想定される。デュアルオフライン（提示側検証側共にオフライン）で使うのであれば Wallet と Verifier の両方でローカルのセキュリティ機能を具備する事が必要と思われる。また、セキュリティ機能のレベルは、国際的な動向をみながら要件を合わせていくことも必要と考える。デバイスセキュリティについては CC（Common Criteria）認証の是非の論点もあるが、毎年のように発売されるスマートフォンで取得するためのコストは非常に大きいと想定され、スマートフォンのライフサイクルに合った検証の方法を模索していく必要がある可能性がある。その他、プラットフォームとの関係性から一部のスマートフォンの扱いをどうするか考えることも必要。
- Verifier→Wallet の信頼モデル：Verifier が Wallet を信頼できる仕組みは必要か。（Holder binding の担保として）
- Wallet Provider の信頼モデル：Wallet の提供元の Wallet Provider を信頼できる仕組みは必要か。
- Wallet と Holder の紐づけ：Wallet と Holder のバインドはどのように確保するか。
- Wallet の信頼モデル：Holder の端末上で動作する Wallet インスタンスの信頼性をどのように担保するか。
- 複数 Wallet の信頼モデル：Holder が複数の Wallet を所有することを許容できるのか。その場合、Holder の持つそれぞれの Wallet をどのように信頼するのか。

### B3-4. Verifier の信頼性を検証する仕組みの検討

- Holder 及び Wallet→Verifier の信頼モデル：Holder や Wallet が Verifier を信頼したり認証したりすることのできる仕組みは必要か。（例：提示先 Verifier の信頼性を判断できる情報を Wallet に表示して判断を促す、登録済みの Verifier 以外には提示できないように Wallet で制御する等）
- Issuer→Verifier の信頼モデル：Issuer が(Wallet を経由して)Verifier を信頼できる仕組みは必要か。（Issuer が提示先の Verifier を制限する必要があるか）

### B3-5. その他の信頼性を担保する仕組みの検討

- トラストフレームワーク等への準拠をステークホルダに示す方法：Issuer や Wallet Provider が、特定のトラストフレームワーク、ガイドライン、技術仕様等に準拠していることを Holder などの関連するステークホルダにどのように示すべきか。

## B4. アーキテクチャに関するその他の検討事項

### B4-1. 識別子のあり方の検討

- エンティティの識別子：Issuer や Wallet などの各エンティティにおいて、VC の Holder をどのような体系の識別子で区別すべきか。
  - Holder の識別子：Holder を一意に特定する識別子が必要であるか。その識別子は、どのような文脈や範囲で一意に特定できる必要があるか。複数の VC や Wallet を跨いで一意に特定できる必要があるか。（法令等で定められた識別子を用いる場合、それら利用規約を考慮する必要がある。）

### B4-2. 失効・状態管理のあり方の検討

- 状態管理：失効・状態をどのように管理すべきか。（Status List など）

- Issuerの存続状態との関係：Issuerが存続しなくなった場合（組織の統廃合、廃業等）に、発行済VCは失効すべきか。失効しない場合、それ以降の状態管理をどう行うべきか。

#### B4-3. 公開鍵基盤のモデルの検討

- Issuerの公開鍵の参照・管理モデル：公開鍵はどのような形式とすべきか。
  - モデル：どのようなモデルで参照・管理できるようにすべきか。（中央レジストリ、直接配布 等）
  - フォーマット：どのようなフォーマットを用いるべきか。（JWKS（JSON Web Key Set）、X.509 等）
  - 公開鍵基盤等の方式：発行時にGPKIやLGPIを使うのか。それともTrusted List等を整備していくのか。
- その他の関係者の公開鍵の参照・管理モデル：Wallet・Wallet Provider・Verifierなどの検証を公開鍵証明書によって行う場合、どのような参照モデルの基盤とすべきか。（EUのTrusted Listに類する仕組み 等）
- Issuer撤退後の公開鍵管理：Issuerが存続しなくなった後も有効期限が継続するVCに関する公開鍵情報の管理は必要か。

#### B4-4. 技術的相互運用性の確保の検討

- 技術的相互運用性の確保対象：技術的に相互運用性を確保すべき点は何か。
- 技術的相互運用性確保の方法：技術的に相互運用性を確保する方法はどうあるべきか。（テストスイート、PKIのブリッジ 等）

#### B4-5. その他の検討

- メタ情報の公開方法：署名検証方法や鍵の格納場所などのメタ情報をどのように管理すべきか。
  - VC発行システムに接続可能な真正データのDBの必要性
- 属性項目：どの属性項目を含めるか。共通化は必要か。
  - 階層的な住所表記（市、区、番地、建物の表記方法の統一）
  - 主要な属性データ定義の統一（旧姓・別名・ミドルネームなども含む）
- エコシステムにおけるシステムの整備：身元確認、発行、Walletアプリ、検証アプリをどのように整備すべきか。
  - 証明書発行の際のWalletの登録管理をどうするか。
  - 真正データを発行するシステムの整備をどうするか。
  - 失効時等のライフサイクル管理をどうするか。

## C. VCの各ライフサイクルにおける技術的対策

ここでは、VCのライフサイクル単位で安全対策を中心とした技術的対策についての検討事項を記述する。

### C1. VCの発行時に求められる技術的対策

#### C1-1. IssuerによるHolderの正当性の確認（本人確認等）のあり方の検討

- 攻撃者の動機：証明書の性質などを踏まえ、攻撃者がHolderになりすまして証明書を不正取得する動機があるか。また実際に不正取得された場合にステークホルダが受ける被害を受容することは可能なのか。
- 申請者に対する本人確認や紐付きの確認：VC発行をリクエストする申請者に対し、身元確認や本人認証、HolderとWalletの紐付き確認などをどのような方法で行うべきか。

- Wallet Provider や Wallet Instance の正当性の確認：Wallet の提供元や端末で動作している Wallet の正当性をどのように確認すべきか。
  - （参考情報）互換性を検証するための仕組み（組織・コンソーシアム、適合性検証ツールの提供 等）が考えうる。

#### C1-2. 発行時の攻撃対策の検討

- リクエスト・レスポンスの改ざん対策：発行要求や応答の改ざんをどのように検知し、どのように対応すべきか。
- VC や認可情報の窃取対策：認可情報を窃取された場合にどのように検知し、どのように対応すべきか。
- 発行要求に関するリプレイ対策：VC の発行要求を使いまわされた場合にどのように検知し、どのように対応すべきか。

#### C1-3. VC と Holder の紐づけ方法の検討

- VC と Holder の紐づけ：VC と Holder、Wallet の紐づけは必要か。どのような方法によって VC、Holder、Wallet を紐づけるべきか。（暗号的な紐づけ、識別子による紐づけ、生体情報の紐づけ、属性情報の組み合わせによる紐づけ 等）
- Key Binding による VC と Holder の紐付けを行う場合、秘密鍵の複製防止対策をどのように行うかを Wallet にどのように要求するか。
- Key Binding による VC と Holder の紐付けを行う場合、VC を Verifier に提示する際の本人認証をどのように行うべきか。（暗証番号とする場合にその長さの制限をするか。生体認証とする場合には精度をどのように担保するか。）また、Wallet に対して本人認証方式をどのように指定し、要求するか。

## C2. VC の保持時に求められる技術的対策

#### C2-1. スマートフォンの盗難対策の検討

- ローカル認証：Wallet の起動時に生体認証、PIN 等を求めるべきか。VC の提示時にどのような認証を求めるべきか。

#### C2-2. Holder の暗号鍵の窃取・悪用対策の検討

- 鍵の漏洩対策：VC と Holder を紐づけるために用いられる鍵（通常 Wallet に格納され管理される秘密鍵）の窃取をどのように防止すべきか、漏洩が起きた場合にどのように検知・対応すべきか。（スマホ内のセキュアな領域などを利用すべき・できるか）
- 鍵の不正利用対策：スマートフォンの乗っ取りや鍵の外部共有などに対してどのような対策を講じるべきか。

#### C2-3. VC の窃取・悪用対策の検討

- VC の複製・持ち出し対策：VC の漏洩をどのように防ぐべきか。
- VC 漏洩後の盗用対策：VC の漏洩をどのように検知・対応・復旧すべきか。

#### C2-4. その他の対策の検討

- スマートフォンの侵害対策：スマートフォンに対してどのようなその他のセキュリティ対策を講じるべきか。
- Wallet への攻撃対策：Wallet に対してどのようなその他のセキュリティ対策を講じるべきか。
- バックアップへの攻撃対策：バックアップや復旧フレーズに対してどのようなその他の防御を講じるべきか。
- スマートフォンの侵害体制の確認：スマートフォンが備えるセキュリティ対策機能をどのように確認するか（Root 化、

Jailbreak などの有無、生体認証機能の精度、Wallet ソフトウェアの真正性、Key Attestation など）。

#### C2-5. Wallet Provider による Wallet 内のデータの不正な閲覧対策の検討

- 運用上の対策：どのような運用的な対策を行うべきか。（アクセス権の管理 等）

#### C2-6. Wallet Provider による Wallet の利用履歴等の収集対策の検討

- 利用履歴の保存の要否：Wallet の利用履歴を保持する必要があるか。
- ログとテレメトリの最小化：Wallet Provider に対して、ログとテレメトリの最小化に関する義務を課すべきか。

#### C2-7. スマートフォンの紛失、故障、機種変更、通信ができない場合を想定した対策の検討

- バックアップ・再発行：スマートフォンの紛失、故障などを見越してどのようにバックアップや復旧、再発行を行うべきか。
- データ移行：Wallet やスマートフォンを変更する際にどのようにデータを移行すべきか。（セキュリティ機能によっては Holder が自発的に削除しないとデータが残る場合もある。）
- 通信できない場合などの代替提示手段：一時的に提示ができない場合、どのような代替手段で提示を行うべきか。（通信環境がない場合 等）

### C3. VC の提示時・検証時に求められる技術的対策

#### C3-1. 提示時の中間者攻撃対策の検討

- リプレイ対策：提示要求を使いまわされた場合にどのように検知し、どのように対応すべきか。
- 中間者攻撃対策：提示時の中間者攻撃に対してどのように検知し、どのように対応すべきか。

#### C3-2. 第三者（偽の Verifier）による Holder に対するフィッシング対策の検討

- Verifier の真正性：Verifier の真正性の検証は必要か。必要な場合、どのような方法で行うべきか。
- Verifier の正当性：Verifier が本当に意図した機関に属するか検証が必要か。（例：〇〇病院、という Verifier は本当に医療法人として認可された「病院」であるか） 必要な場合、どのような方法で行うべきか。

#### C3-3. 偽造・改ざんされた VC や不適切な VC<sup>1</sup>の提示に関する対策の検討

- 署名検証：Verifier は Issuer の署名を必須で検証すべきか。必須である場合検証を促進する際に、どのような方法がとり得るか。（iPhone のマイナンバーカードのような確認プログラム等の提供やガイドライン 等）
- Issuer の機関としての正当性：Verifier は Issuer が本当に意図した機関に属するかの検証を必須で行うべきか。（例：〇〇大学、という Issuer は本当に学校法人として認可された「大学」であるか）
- プライバシー保護：VC の検証プロセスにおけるプライバシー面の考慮事項はないか。（VC が提示された事実やその提示先に関する情報を Issuer に知られ得る 等）

#### C3-4. 第三者による VC の盗用や Verifier による VC の不正利用への対策の検討

- VC と Holder の紐づき確認：VC の Holder Binding を確認するために、どのような対策を行うべきか。
- 提示先の限定：VC の提示先を特定の Verifier に限定すべきか、その場合にどのような対策を行うべきか。

#### C3-5. Verifier による必要以上の情報の要求（同意の強制・形骸化等）に関する対策の検討

- Verifier の制限：特定の（登録された）Verifier からのみ要求を受け付ける必要はあるか。

---

<sup>1</sup> 証明書の原課等が関知せず、発行プロセス等の正当性についても第三者的な認定がない中で、元の証明書と同等の効力を自称する VC など

- 利用目的の特定・通知方法：情報の利用目的を特定し、通知する方法はどうあるべきか。

## C4. Verifier での保存・利活用時に求められる技術的対策

### C4-1. Verifier における利活用・保存ポリシーの明確化

- データ利活用の目的：データ利活用の目的はなにか？
- データのライフサイクルの定義：データ保持が必要な場合、保持目的、保持期間、アクセス制御、監査、第三者提供制限、削除（破棄）手順はどうあるべきか。

### C4-2. VC の漏洩対策の検討

- VC の漏洩対策：VC に対してどのように持ち出しの対策を施すべきか。（暗号化やアクセス制御等）
- VC の適切な破棄：VC を保存しない設計や一定期間での破棄などによって VC の漏洩リスクを軽減すべきか。

### C4-3. 別の Verifier や Issuer との結託による名寄せ対策の検討

- メタデータによる名寄せ対策：メタデータで行われる名寄せに対してどのような対策を講じるべきか。（ペアワイズ ID、メタデータ最小化など）
- 属性による名寄せ対策：属性値で行われる名寄せに対してどのような対策を講じるべきか。（選択的開示など）
- 署名値による名寄せ対策：署名値で行われる名寄せに対してどのような対策を講じるべきか。（ゼロ知識証明、バッチ発行やそれに伴う Issuer 負荷をどうとらえるか 等）
- Verifier の制限：名寄せリスクの軽減のために、提示が可能な Verifier を限定するべきか。限定する場合はどのような方法がとり得るか。

### C4-4. その他のプライバシー面の対策の検討

- 目的外利用等の防止：提供後に目的外利用や第三者提供を行うことをどのように防止すべきか。
- 保持期間の最小化：リスクを踏まえると Verifier でのデータ保持ポリシーはどうあるべきか。
- 不当な差別への配慮：プロファイリングによって不当な差別が行われることをどのように防止すべきか。またそのような不当な扱いを暗黙的に取られていないか利用者に認識させる方法はあるか。

## C5. その他全般において求められる技術的対策

### C5-1. 偽造・改ざんされた VC や不適切に発行された VC への対策の検討

- Issuer の正当性の検証リストの構築：正当な Issuer のリストは必要か。必要だとすると既存の仕組みなどを使えるか。（例えば、実在する「行政機関」を網羅的に掲載したリストなど。）
- Issuer の正当性の検証リストへの登録：正当な Issuer のリストへの登録・公開を行うべきか。

### C5-2. Issuer の秘密鍵の漏洩等に関する対策の検討

- 鍵の保護：Issuer の署名鍵に対してどのような防御策を講じるべきか。
- 鍵の失効：万一 Issuer の署名鍵が漏洩した場合にどのように失効すべきか。

### C5-3. エコシステムの継続性に関する対策の検討

- エコシステムの継続リスク：Issuer や Wallet Provider などのステークホルダが撤退した場合にどのような影響が及ぶのか。

- 技術的互換性の担保：Wallet Provider の撤退などに対応するため、どのように互換性を担保すべきか。
- 再発行：Issuer が撤退した場合、端末の紛失や交換などで再発行が必要になった際にどのように行うべきか。
- 暗号アジリティの確保：PQC（対量子計算機暗号）への移行など、暗号技術が危殆化した場合に備えたアジリティ確保が必要か、どのように行うべきか。
- 脆弱性情報の共有コミュニティ形成：新規の脆弱性情報の共有等を頻度高く行える専門家コミュニティをどう形成するか。

## D. エコシステムとガバナンスのあり方

ここでは VC や DIW を継続的に扱うにあたって必要となるエコシステムの役割やインセンティブ、ガバナンスなどの検討事項を記載する。

### D1. エコシステムのあり方

#### D1-1. エコシステムにおいて必要な役割と責任の検討

- 基本的な役割：Issuer、Holder、Verifier、Wallet Provider の他に、どのような役割が必要か。
- ガバナンスを担う役割：EU における認定機関や適合性評価機関、インシデント報告体制など、どのようなガバナンスを受け持つ役割が必要か。
- AI エージェントに対する責任及びそのガバナンスを担う役割：AI エージェントの動作に対する責任を誰が負うべきか、及びそのガバナンスを受け持つ主体としてどのような役割が必要か。
- その他の役割：可用性担保に向けた仲介者など、その他どのような役割が必要か。

#### D1-2. エコシステムの普及・維持のためのインセンティブの設計

- 各ステークホルダのインセンティブ：エコシステムの普及・維持のために、Issuer、Wallet Provider、Verifier、一般消費者のインセンティブをどう確保すべきか。（例：Verifier のインセンティブ確保における、VC の普及率向上、発行リードタイムの短縮 など）

#### D1-3. 普及促進や理解醸成の方法の検討

- 普及促進：VC や DIW の普及促進にあたり、行政機関、民間企業、国民等に対してどのような活動を行うべきか。
  - （参考情報）Wallet と Verifier に関しては技術情報を共有して一定のレベルを維持できるようなコンソーシアムがあることが望ましい（特にセキュリティと互換性の面から）。

#### D1-4. エコシステムに関するその他の検討

- フィジビリティ：エコシステムを実現・持続可能なものとするために、人的リソースやコスト等を踏まえるとどのようなエコシステムの設計が必要か。
- システムの透明性・利便性の考え方：システムとして透明性や利便性の評価はどのように考えるのか。
- データ管理：エコシステム上のどの役割に、どのようなデータが蓄積され、どう管理するのか。またユーザーの安心・安全のため、エコシステムにおけるデータ管理の透明性をどう確保すべきか。

## D2. ガバナンスのあり方

### D2-1. ガバナンスの確立のために必要となる制度の検討

- 法令・制度のあり方：関連する現行法令（個人情報保護法等）、関連する制度（マイナンバーカード・JPKI等）との兼ね合いも踏まえ、新規の法令・制度や、既存の法令・制度の改正は必要か。
- 認定制度のあり方：Verifier、Wallet、Wallet Provider、Issuerの認定取得は必要か。あるいは独自に認定制度を作る必要があるか。
- 認定対象とする事実：WalletやAIなどの認定において、何を確認し担保すべきか。（例：収集したデータの二次利用防止、他WalletへVCのエクスポート、透明性レポートの公開等）
- ガイドラインのあり方：既存のガイドラインへの遵守方法、証明書制度の所管組織による独自のガイドラインの必要性、遵守を求めるのか、ガイドラインへの遵守を示す方法は何か、などはどうあるべきか。
- 適合性評価のあり方：試験、第三者評価、自己適合宣言等のうち、どの方式を採るべきか。対象（Issuer・Wallet・Wallet Provider・Verifier等）ごとに何を評価するべきか。
- 監査と是正のあり方：ログや運用を含め、どのような監査を行うべきか。違反・事故発生時の是正措置はどうあるべきか。
- インシデント報告体制：Issuer・Wallet Provider・Verifier等の間で、どのような報告・連絡・公表の体制が必要か。
- 利用者の救済：誤発行、盗用、目的外利用が疑われる場合の申立て、再発行、失効、相談窓口等をどのように設計するべきか。
- 競争政策上の措置：Walletプロバイダーの寡占・独占を防ぐための競争政策上の措置を講じる必要があるか。（スマホ新法の活用等）

### D2-2. VC化した証明書の実効性等の検討

- 法的効力：VC化した証明書を法的に紙の証明書と同様に扱うことは可能か。
  - （参考情報）電子署名法との関係性、法的効力などの整理が必要な場合があると想定される。
- セカンダリーユースでの取り扱い：その証明書制度を所管する行政機関が本来意図した場面以外でVCの提示が行われた場合、どのようなリスクが想定されるのか。そのリスクが顕在化した場合、証明書制度の所管組織としてどの程度責任を負う必要があるのか。

### D2-3. 法的・制度的相互運用性の検討

- 相互運用性の確保対象：法的・制度的に相互運用性を確保すべき点は何か。
- 相互運用性の方法：法的・制度的に相互運用性を確保する方法はどうあるべきか。

## (付録) 用語定義

### ● VC (Verifiable Credential)

- デジタル署名による真正性確保・改ざん防止等の機能を有する、「人、法人、モノ等」の属性情報に関する汎用的で機械可読なデータ形式・データ流通の形態。
- ここでは、より一般化された議論を行うため、W3C Verifiable Credentials Data Model のような特定の規格を指す意味ではなく、SD-JWT VC や mdoc などの複数の規格も含む抽象的な概念として「VC」という呼称を用いている。
- 本書の中では、以下のような性質を併せもつデータのフォーマットを想定している。
  - ◇ ①機械可読性
    - 一定のルールに基づいて情報が構造化データとして表現されているもの。
  - ◇ ②検証可能性
    - 発行者や利用者の署名を埋め込むことで、検証者が真正性や非改ざん性を検証できるもの。
  - ◇ ③選択的開示
    - ①②の性質によって証明書の一部のデータのみを提示した場合でも、真正性と非改ざん性を検証することができるもの。
- なお、W3C VCDM の「VP (Verifiable Presentation) 」に該当するもの（提示時に、Holder の鍵による署名等を付与した VC）についても、上記の理由により本資料では「VC」という呼称を用いている。

### ● DIW (Digital Identity Wallet) (又は単に「Wallet」)

- 個人・法人等が、自身の証明書 VC 等をスマートフォン等に保存・管理し、第三者に提示するための仕組み及びアプリケーション。
- 本書の中では以下の基本的な機能を備えるものとして想定している。
  - ◇ ①Holder を介した提示モデル (IHV モデル)
    - 利用者 (Holder) を介して証明書等の提示を行えること。
    - 発行元がオフラインでも証明書の提示や検証ができること。
    - 証明書が提示されたことを発行元に知られないこと。
  - ◇ ②検証可能なデータモデル (上記「VC」) の取扱い
    - 真正性と発行元を検証可能なデータモデルを取り扱うことができること。
    - 提示する情報とウォレットの紐づきを証明できること。
  - ◇ ③プライバシー保護に関する機能
    - 提示する情報を選択的に開示できること。
    - 提示情報の名寄せ対策 (リンク不可能性) を備えること。
  - ◇ ④証明書の発行・提示の相互運用性
    - 高い相互運用性を有する標準化された技術によって証明書の発行や提示ができること。