要件定義書

2024年3月15日

Version 1.0

**目次**

[1. プロトタイプシステムの概要 2](#_Toc143767608)

[1.1. 目的 2](#_Toc143767609)

[1.2. 課題 2](#_Toc143767610)

[1.3. 用語定義 3](#_Toc143767611)

[2. スキーム 4](#_Toc143767612)

[2.1. 事業スキーム 4](#_Toc143767613)

[2.2. アクター 4](#_Toc143767614)

[2.3. ユースケース図 5](#_Toc143767615)

[3. 機能要件 6](#_Toc143767634)

[3.1. ウォレット 6](#_Toc143767635)

[3.2. 証明書発行 7](#_Toc143767636)

[3.3. 属性情報取得 7](#_Toc143767637)

[4. 非機能要件 8](#_Toc143767638)

[4.1. ウォレット 8](#_Toc143767639)

[4.2. 証明書発行 8](#_Toc143767640)

[4.3. 属性情報取得 8](#_Toc143767641)

# プロトタイプシステムの概要

## 目的

本システムでは、ユーザ自身が自らのアイデンティティを管理し、属性情報を他者と相互検証できるようにした上で、特定のサービスに依存しないよう、相互運用性を確保したデータのやりとりや安全なメッセージングを行うことができるようにすることで、オンラインコミュニケーションのトラストおよびUI/UXを向上させることを目指す。

また、属性情報のやりとりのプロトコルとして、OpenID for Verifiable Credential Issuance（以降「OID4VCI」）、OpenID for Verifiable Presentations（以降「OID4VP」）、 Self-Issued OpenID Provider v2（以降「SIOPv2」）に対応することを想定しており、これらの標準技術を用いてIssuerが証明書を発行するためのコード、およびVerifierが属性情報の検証を行うためのコードを含めてオープンソースとして公開を行うことで、それぞれのステークホルダーが特定の事業者に依存することなく、これらの実装が行えるようにする。

## 課題

* 昨年度のユースケース分析レポートでは、13事業者中11事業者がDecentralized Identifiers（DID）やVerifiable Credentials（VC）の組み合わせを属性情報の検証の仕組みとして採用している一方、他の手法と比較評価をした上で採用しているケースはなく、また、その11事業者すべてが別々のウォレット実装を行っている。当社の昨年度実証でもウォレット実装を行ったが、汎用的なウォレットにはなっておらず、UI/UXの課題が残った。
* エンティティ（人や法人）間のデータのやりとりにおいて、アイデンティティウォレットを基点にユーザ自身のコントロールのもとに検証可能な属性情報のやりとりを行ったとしても、エンティティ間でメールやメッセンジャー、ＳＮＳ等でのメッセージングを行う際に、それらの連絡先情報を共有することにより、Trusted Webの外側でデータのやりとりが発生してしまうこととなる。当社の昨年度実証においても、メールアドレスの提供を一部実証したが、結局メールアドレスやその他の連絡先情報を共有することにより、連絡先情報に紐づく自身の属性情報のコントロールはできず、特定のサービスへの依存や、メッセージのやりとりの相手先やメッセージ自体の検証、安全性の担保ができなくなってしまうことが課題となった。
* 現在利用されている、メールやSNS、法人向けコラボレーションツール等のオンラインでのメッセージングや属性データのやりとりは、マーケティング分野に限らず、CtoC、BtoC、BtoB、それぞれのケースで多くの課題があることが分かった。(報告書参照)

## 用語定義

**表 1-1：用語定義**

|  |  |
| --- | --- |
| 用語 | 定義 |
| エンティティ | 実体として認識できるものの総称。例えば、自然人、法人、製品、サービスなどをエンティティと現すことが多い。 |
| アイデンティティ | エンティティに関する属性情報の集合。（ISO/IEC 24765-1） |
| デジタルアイデンティティ | デジタル空間上のアイデンティティ。 |
| 属性情報 | 氏名、生年月日、住所などのアイデンティティを構成する情報。 |
| デジタルアイデンティティウォレット (DIW) | デジタルアイデンティティを安全に保存、管理、共有するためのツールやアプリケーション。本書では単純にウォレットと表記する場合もある。 |
| オンラインコミュニケーション | オンラインにおける属性情報やメッセージのやりとりのこと。 |
| メッセージングサービス | メッセージやその他の情報のやりとりができるツールやアプリケーション。 |
| メッセージングプロトコル | メッセージングサービスの基盤技術となるプロトコル。 |
| アクター | ユースケースにおけるエンティティ。本書でのユースケースとしてはウォレットを扱うエンドユーザー (Holder)、証明書を発行するIssuer、証明書を検証するVerifierを想定している。 |
| 証明書 | 然るべき発行機関からエンティティへ発行されたアイデンティティの一部または全部を証明するもの。本書では電子署名技術を用いて証明可能なデジタル証明書の意味で用いる。 |
| 証明書署名要求 (CSR: Certificate Signing Request) | 証明書への署名を要求するためのドキュメント。 |
| キーペア（鍵ペア） | 電子署名に用いられる秘密鍵（署名鍵）、公開鍵（検証鍵）のペア。 |
| 選択的属性開示 | 属性情報の一部もしくは属性情報から導き出される情報のみを選択的に提示でき、  かつ前記の情報のみでも検証可能となる仕組み。 |
| Decentralized Identifiers（DID） | 分散的に管理されたグローバルに一意な識別子。 |
| Verifiable Credentials (VC) | 改ざん検出が容 易なクレデンシャルであり、誰が発行したかを暗号学的に検証 できるもの。 |
| Selective Disclosure for JWTs (SD-JWT) | 選択的属性開示をJSON Web Toke (JWT)nをベース技術として実現する標準仕様。 |
| OpenID for Verifiable Credential Issuance（OID4VCI） | IssuerからHolderに証明書を発行する標準仕様。 |
| OpenID for Verifiable Presentations（OID4VP） | HolderからVerifierに証明書を提示する標準仕様。 |
| Self-Issued OpenID Provider v2（SIOPv2） | エンドユーザー (Holder) 自信がOpenID Provider (OP) となり認証連携を行う標準仕様。 |
| Decentralized Identifiers（DID） | 分散的に管理されたグローバルに一意な識別子。 |
| 階層型決定性 (HD: Hierarchical Deterministic) ウォレット | 1つのシードからマスターキーとなる秘密鍵を生成し、そこから木構造のような階層的に複数の派生秘密鍵と派生公開鍵(アドレス)を生成する鍵管理方法をとるウォレット。 |
| Matrix | オープンソースの分散型メッセージングプロトコル。 |
| Synapse | Matrixホームサーバーのオープンソースソフトウェア。 |
| Element | Matrixクライアントのオープンソースソフトウェア。 |

# スキーム

## 事業スキーム

グラフィカル ユーザー インターフェイス が含まれている画像

自動的に生成された説明

**図 2-1：事業スキーム図**

## アクター

### アクタータイプ

**表 2-1：アクタータイプ**

|  |  |  |
| --- | --- | --- |
| No | アクタータイプ | 説明 |
| 1 | エンドユーザー | ウォレットを利用して各種便益を受ける個人。 |
| 2 | Issuer | クレデンシャル発行体。 |
| 3 | Verifier | クレデンシャル提供先。 |

### アクター

それぞれのユースケースによってアクターが異なるため、詳細は[別紙\_ユースケース設計書.pdf](https://drive.google.com/file/d/1p-DWLv6Jke5osqD2dlKrt94PDyNJ8oKv/view?usp=drive_link)を参照ください。

## ユースケース図

詳細は[別紙\_ユースケース設計書.pdf](https://drive.google.com/file/d/1p-DWLv6Jke5osqD2dlKrt94PDyNJ8oKv/view?usp=drive_link)を参照ください。

# 機能要件

## ウォレット

**表 3-1：機能要件一覧（ウォレット）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | 大分類 | 中分類 | 要件 | 備考 |
| 1 | セットアップ | ウォレット初期設定 | 簡易かつ安全にウォレットの利用を開始できること | HDウォレットにて実装する |
|  |  | ウォレットロック解除 | 生体認証など簡易かつ安全にウォレットを利用できること |  |
| 2 | 証明書取得 | マイナンバーカード情報取得 | OID4VCIのCredentialOfferのプロトコル上で基本４属性を持つVC発行を要求できること |  |
| 3 | 属性情報提供 | サインアップ(属性情報提供) | OID4VPのプロトコル上でのクレデンシャル提供要求を受け付けられること |  |
|  |  | 提供属性情報選択 | 提供要求のメタデータに従って対象の属性を明示できること |  |
|  |  | 提供履歴表示 | 提供済みの属性情報の履歴を表示できること |  |
| 4 | メッセージング | サインイン | SIOPv2プロトコルでサインアップできること |  |
|  |  | 企業認証 | 所属企業の真偽を証できること | 検証者の正当性検査 |
| 5 | リカバリ | ウォレット | リカバリーフレーズにてマスターアカウントが復旧できること |  |
|  |  | SNSアカウント | HDウォレットの機能により過去生成したRP事のペアワイズアカウントのログインIDを復旧できること |  |

## 証明書発行

**表 3-2：機能要件一覧（証明書発行）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | 大分類 | 中分類 | 要件 | 備考 |
| 1 | 鍵(キーペア)管理 | キーペア生成 | 指定されたキーIDと暗号曲線で新しいキーペアを生成し、データベースに保存できること  暗号曲線名は指定されたリストから選択される必要がある | 暗号曲線 : P-256, secp256k1, Ed25519 |
|  |  | キーペア取得 | 指定されたキーIDに対応するキーペアの公開部分を取得できること |  |
|  |  | キーペア失効 | 指定されたキーIDに対応するキーペアを失効させることができること |  |
|  |  | CSRの生成 | 指定されたキーIDからCSRを生成できること |  |
|  |  | 自己署名証明書の生成 | 指定されたキーIDとCSRを使用して自己署名証明書を生成できること |  |
|  |  | 証明書の登録 | 指定されたキーIDに対して一つ以上の証明書を登録できること |  |
| 2 | クレデンシャル発行 | xID連携 | マイナンバーカード情報発行する際にxIDと連携して証明書情報を提供できること |  |
|  |  | 証明書発行 | 特定の形式でクレデンシャルを発行する（JWT VC JSON, vc+sd-jwtなど） | sd-jwt : マイナンバー(4情報+13歳以上)、社員証  jwt\_vc\_json : イベント参加証 |

## 属性情報取得

**表 3-3：機能要件一覧（属性情報取得）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | 大分類 | 中分類 | 要件 | 備考 |
| 1 | アカウント | サインアップ | QRコードを表示してWalletからのサインアップを提供できること  Walletでのサインアップが完了するとブラウザもサインアップが完了し、画面が遷移する |  |
|  |  | サインイン | QRコードを表示してWalletからのサインインを提供できること  Walletでのサインアップが完了するとブラウザもサインアップが完了し、画面が遷移する |  |
|  |  | 属性情報提供 | QRコードを表示してWalletから属性情報を提供ができること(OID4VP) | 提供できる情報 : 年齢証明(13歳以上)、所属証明(社員情報)、イベント参加証(PbDL) |
|  |  | バックアップ | 暗号鍵を再生成するためのセキュリティーキーをダウンロードできること | 12個の4文字毎のランダムな文字列 |
|  |  | リストア | 取得したセキュリティーキーを入力することで、アカウントのリストアができること |  |
|  |  | 無効化 | ユーザーの希望に応じてアカウント無効化ができること |  |
| 2 | メッセージング | 1on1 | ダイレクトメッセージを送信する際に、送信先の公開されている所属組織情報から身元を検証が可能であること |  |
|  |  | メッセージ送信 | 身元を検証した結果、送信先に対して暗号化されたメッセージを送信が可能であること |  |

# 非機能要件

## ウォレット

**表 4-1：ウォレット**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | 大分類 | 中分類 | 要件 | 備考 |
| 1 | 性能要件 | レスポンスタイム | ユーザーの操作に対して即座に反応し、遅延なく情報を提供する |  |
|  |  | 効率的なデータ処理 | 暗号・復号化など重たい処理も効率的に処理してユーザビリティを低下させない |  |
| 2 | 安全性要件 | データの暗号化 | 保存される個人情報やデジタル証明書は、適切に暗号化して保護される |  |
|  |  | 生体認証 | 必要な部分には生体認証による認証を要求してセキュリティーを担保する |  |
| 3 | 互換性要件 | 標準プロトコルのサポート | 標準プロトコルのサポートにより、ほかのWalletとのデータ互換性を担保する |  |
|  |  | クロスプラットフォーム対応 | androidとiosを提供することで、複数のプラットフォームで一貫した機能とユーザー体験を提供する |  |
| 4 | ユーザビリティ要件 | UI/UX | ユーザーが簡単に理解し、効率的に操作できるユーザーインターフェースを提供 |  |

## 証明書発行

**表 4-2：証明書発行**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | 大分類 | 中分類 | 要件 | 備考 |
| 1 | 性能要件 | レスポンスタイム | リクエストに対してユーザビリティーを損なわない応答時間でリクエストに返信する |  |
|  |  | スケーラビリティ | 負荷の増加に応じたリソースの提供をおこなう |  |
| 2 | 安全性要件 | データ暗号化 | データの重要性に応じ、適切に暗号化を行う |  |
|  |  | 通信のセキュリティ | すべての通信は、TLS/SSLを使用して暗号化される |  |
|  |  | 脆弱性 | アプリケーションは脆弱性から適切に保護されている |  |
| 3 | 可用性要件 | アップタイム | ユーザビリティーを毀損しない稼働率を保証する |  |
| 4 | 保守性要件 | ロギング | デバッグや監査のために適切なレベルのログを生成し、保存する |  |
|  |  | ドキュメント | システムのアーキテクチャ、APIエンドポイント、使用方法に関する十分なドキュメントを提供 |  |

## 属性情報取得

**表 4-3：属性情報取得**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | 大分類 | 中分類 | 要件 | 備考 |
| 1 | 性能要件 | レスポンスタイム | リクエストに対してユーザビリティーを損なわない応答時間でリクエストに返信する |  |
|  |  | スケーラビリティ | 負荷の増加に応じたリソースの提供をおこなう |  |
| 2 | 安全性要件 | データ暗号化 | データの重要性に応じ、適切に暗号化を行う |  |
|  |  | 通信のセキュリティ | すべての通信は、TLS/SSLを使用して暗号化される |  |
|  |  | 脆弱性 | アプリケーションは脆弱性から適切に保護されている |  |
| 3 | 可用性要件 | アップタイム | ユーザビリティーを毀損しない稼働率を保証する |  |
| 4 | 保守性要件 | ロギング | デバッグや監査のために適切なレベルのログを生成し、保存する |  |
|  |  | ドキュメント | システムのアーキテクチャ、APIエンドポイント、使用方法に関する十分なドキュメントを提供 |  |