ウォレットによるアイデンティティ管理とオンラインコミュニケーション（DataSign）

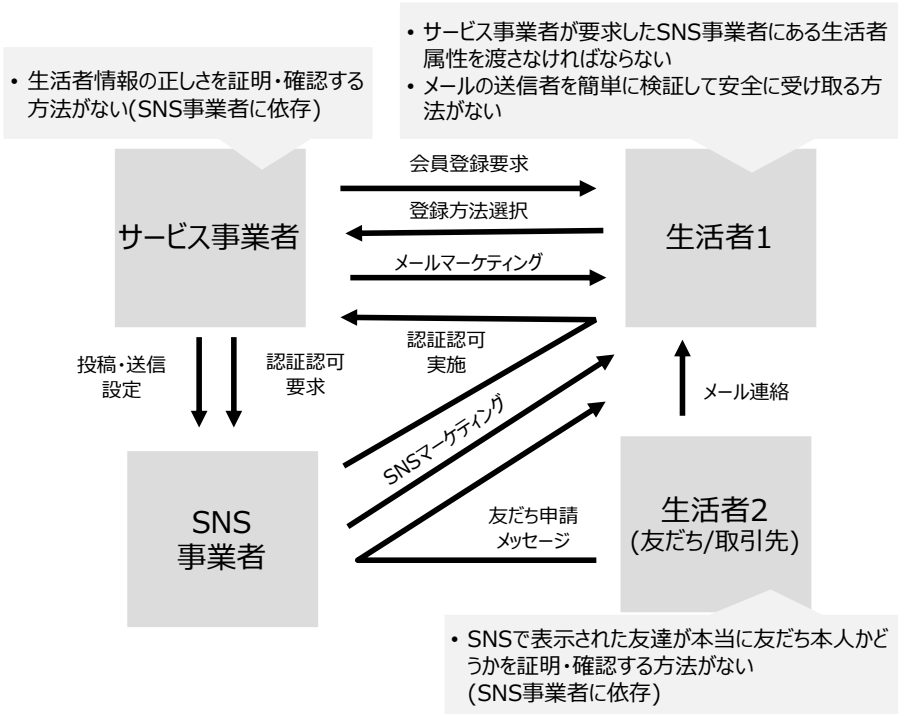
現在の課題（ペインポイント）

- 生活者1はSNS事業者のログイン機能を使うと便利だが、よく知らないサービス事業者にSNS事業者が管理する属性情報を渡したくない
- 生活者1は特定のSNSを用いてメッセージを送ろうとすると、生活者2(友だちや取引先)もその特定のSNSを利用していないとメッセージが送信できない。メールは送信者の検証ができず安全ではない
- サービス事業者は利用者の属性の確認・検証を行いたいが、本人確認はコストが高く、利用者のUXを阻害してしまう
- サービス事業者は生活者に簡便な会員登録方法を提供したいが、複数のSNSに対応すると、逆にUXを阻害してしまう

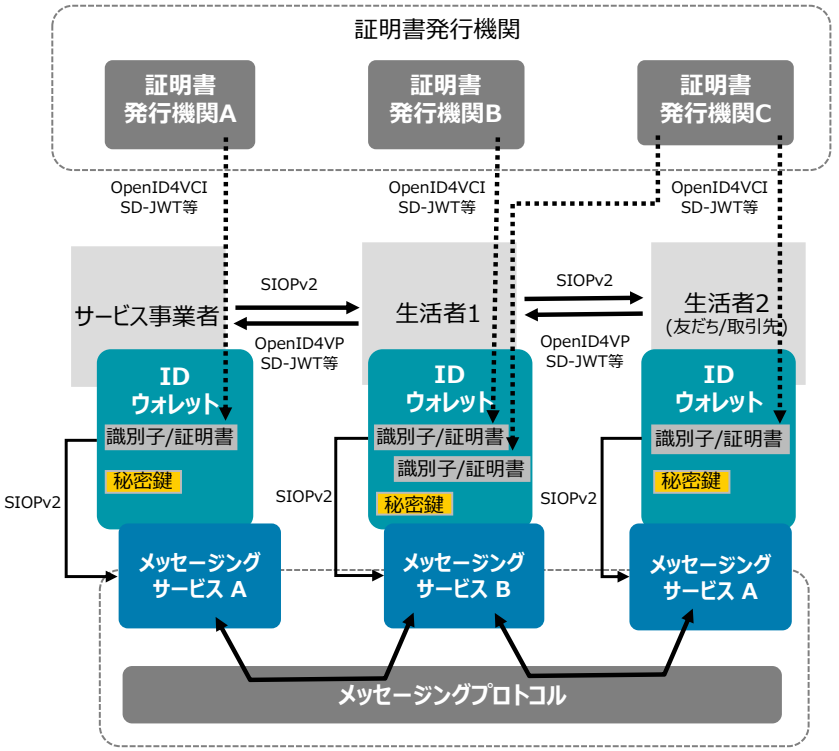
Trusted Webの実現により解決する内容

- 生活者1は特定の事業者に依存せず、サービス事業者や生活者2(友だち/取引先)に自分の意思で必要最小限の属性情報を渡すことができる
- 生活者1は特定の事業者に依存せず、サービス事業者や生活者2(友だち/取引先)と相互に属性情報を検証し、合意した範囲で安全なオンラインコミュニケーションができる
- サービス事業者は特定の事業者に依存せず、簡便に利用者の属性の確認・検証を行い、適切なサービス提供を行うことができる

課題解決前の事業スキーム図（As-Is）



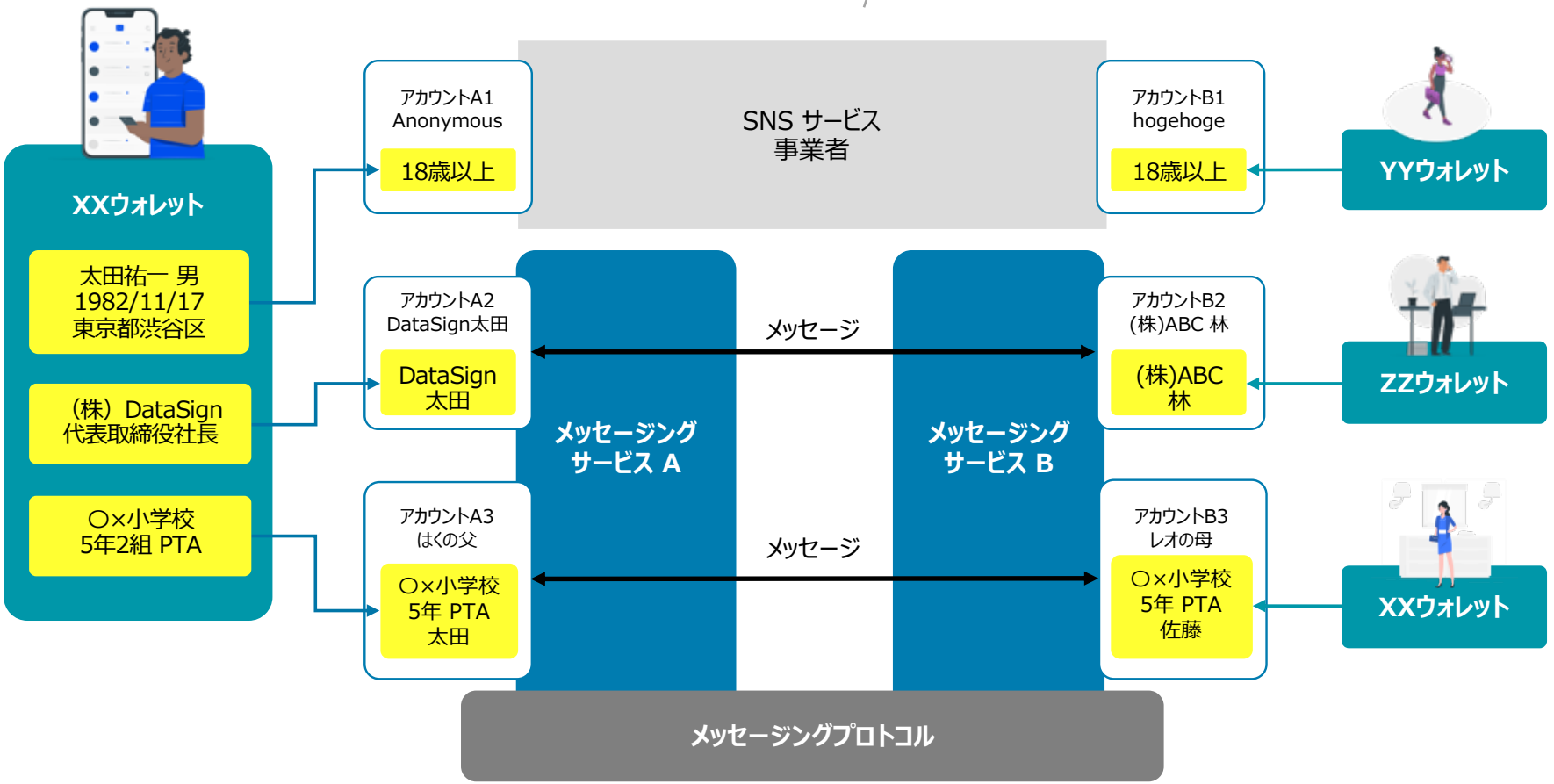
創出するユースケースの事業スキーム図（To-Be）



ウォレットによるアイデンティティ管理とオンラインコミュニケーション（DataSign）

- ウォレットによるアイデンティティ管理
- 選択的開示による必要最小限の情報の共有

- 利用者自身で管理するアイデンティティを用いたサービスの利用（登録・ログイン）およびメッセージングサービスの利用



事業内容、社会的・経済的な価値

事業内容

- 国際標準やデファクトスタンダートとなり得る技術をベースにユーザが自身のアイデンティティを管理でき、汎用的に利用できるアイデンティティウォレットをUI/UXを重視して開発
- 相互に検証可能で安全なメッセージングプロトコルを検討し、誰でも参加可能なメッセージングサービスの開発
- アイデンティティウォレットをベースとしたさまざまなユースケースで利用でき、かつ相互運用可能なデータのやりとりの実現を検討
- オープンソースプロジェクトとしてコミュニティと連携し、社会実装/普及を検討

社会的・経済的な価値

- 試算①
  - 現在の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）の市場規模は、これらのビジネスモデルがパーソナルデータを用いた広告によって成り立っていることを鑑みると世界で約６３兆円程度となる[1]
  - オンラインコミュニケーションの10%がTrusted Webに移行すると仮定すると、6.3兆円程度の市場規模となる
- 試算②
  - BtoCサービスにおける広告型フリーミアムモデル（課金すると広告が出ない、YouTubeプレミアム等）や広告型割引モデル（広告を視聴すると割引がある、Netflix等）の採用例を参考にすると、BtoCサービスにおける一人当たりの売上はおよそ月額200円～1000円程度である[2]
  - これはヒアリングにおいて生活者が支払ってよいと考える金額と同程度であり、現在のSNS利用者の10%が移行すると仮定すると、46億人×10%×1000円×12ヵ月 = 5.5兆円程度の市場規模となる

これらの試算を鑑みると、オンラインコミュニケーション市場において10%がTrusted Webに移行すると仮定すると、世界で５～６兆円の市場規模が見込まれる。（世界における日本のGDP割合から日本における市場規模は3500億円が見込まれる） [3]

[1] statista, https://www.statista.com/topics/2498/programmatic-advertising/#topicOverview
[2] DATAREPORTAL, https://datareportal.com/reports/digital-2022-global-overview-report
[3] 内閣府, https://www.esri.cao.go.jp/jp/sna/data/data_list/kakuhou/files/2020/sankou/pdf/kokusaihikaku_20211224.pdf

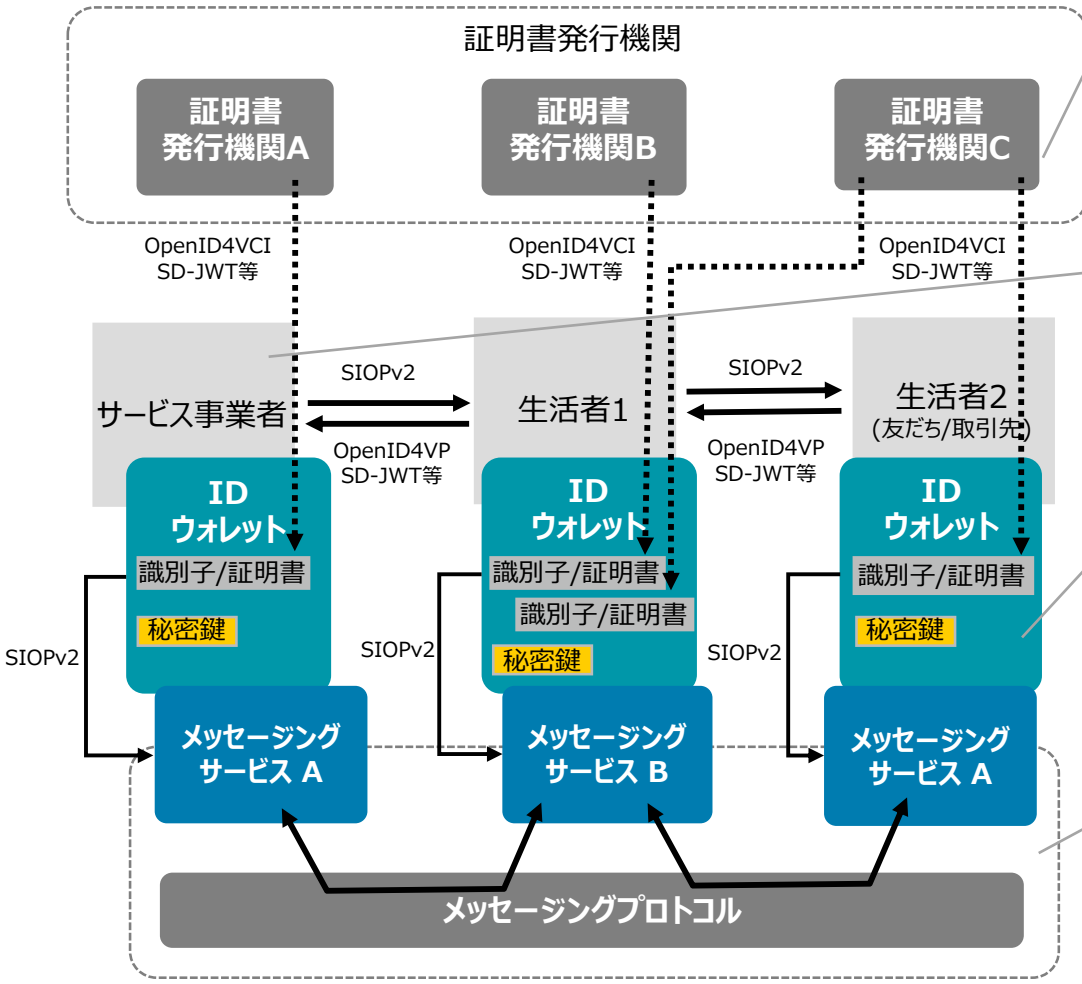
本実証事業における検証ポイント

No.	検証する課題・論点	初期仮説	論点解決に向けて検証・実施する内容
①	証明書発行機関は生活者、サービス事業者にどのように証明書を発行すべきか	・ 証明書発行には安全性と相互運用性を確保するためOpenID Foundation（OIDF）が標準化を進めているOpenID for Verifiable Credential Issuance (OpenID4VCI) を利用する ・ 発行先で柔軟な利用ができるようにSelective Disclosure for JWTs (SD-JWT)等の選択的開示に対応する ・ 証明書発行の際に証明する属性の内容に応じて身元確認を行う	・ 初期仮説の技術のみでなく、従来の公開鍵基盤で利用されている技術の検討も幅広く実施する ・ 実装した際の技術的に困難な点を確認し、必要に応じて標準化団体にフィードバックする ・ NIST SP 800-63等を参考に安全性の向上や身元確認レベルの検討を図る ・ 発行機関や発行時の審査方法のトラストをどのように担保するか検討を行う ・ 本人確認については現状ではX.509証明書を発行しているが、選択的開示の概念等を鑑み、その方法やプロトコルは委託先事業者と協議を行い、実施方法を検討する
②	生活者、サービス事業者は識別子/証明書をどのように管理して自身を証明すべきか	・ 識別子や証明書の管理のため専用のウォレットアプリを利用する (OpenID4VCI対応) ・ 安全性と相互運用性を確保するためSelf-Issued OpenID Provider v2（SIOPv2）やSD-JWT、OpenID4VPに対応したアイデンティティウォレットでサービス事業者に対し会員登録を行う ・ 秘密鍵を管理し、必要に応じて秘密鍵を復元する	・ 初期仮説の技術のみでなく、また識別子/証明書に関してもDIDやVCのみでなくその他の技術利用 (X.509証明書等) も広く検討する ・ ウォレットの実装や利用する技術に関してOWFやEUDIWの動向を踏まえて決定し実証を行う ・ 秘密鍵のバックアップ・復元方法の検証を行う
③	生活者、サービス事業者はどのように証明書を検証すべきか	・ サービス事業者はOpenID for Verifiable Presentations (OpenID4VP) に準じて生活者が提示した証明書を検証する ・ 生活者はアイデンティティウォレットの機能を利用してVCの検証を行う ・ 生活者、サービス事業者は Originator Profile（OP）やBrand Indicators for Message Identification (BIMI) 等の技術を利用してメッセージ送信者を検証する	・ 初期仮説の技術のみでなく、その他の技術 (X.509証明書等)が利用された場合の検証方法を広く検討する ・ ウォレットアプリを利用したVCの検証のみでなく、その他の技術 (X.509証明書等)が利用された場合の検証方法を広く検討する ・ OPやBIMIが分散型メッセージングプロトコル上で利用可能かどうか、またこれら以外の送信者の検証技術についても検討する

本実証事業における検証ポイント

No.	検証する課題・論点	初期仮説	論点解決に向けて検証・実施する内容
④	生活者、サービス事業者はどのように特定の事業者に依存せず、簡単かつ安全にメッセージをやりとりできるか	・ ウォレットでログインできる分散型メッセージングプロトコルを利用したメッセージサービスをOSSベースで実装し、End to End暗号化を実施しつつ簡単かつ安全にメッセージをやりとりする	・ 分散型メッセージプロトコル (Matrix, AT Protocol, Tox等)の比較検討を行い、アーキテクチャとの相性を検証する ・ また分散型メッセージングプロトコルに限らず、従来のプロトコルとも比較検討を実施し、ユースケースやアーキテクチャを実現する最適な技術を検討する
⑤	システムの全体でどのようなUXを実現すべきか	・ ウォレットを基点とし、OpenID4VCIに準じた証明書発行、OpenID4VPに準じた証明書提示、SIOPv2に準じた認証・認可、分散型メッセージングプロトコルに準じたメッセージ送受信に関するUXリサーチ・UXデザインを行う	・ 各標準仕様で考えられているUXのフローを参考としつつ、実際にデザインプロトタイプを用いたUXリサーチを実施して、利用者にとって扱いやすくかつ意味を理解しやすいUXとなるように検証を行う
⑥	プライバシーバイデザインをどのように取り入れたアーキテクチャを実現するか	・ 要求を満たす証明書を選択的に開示する ・ 誰にどの証明書を開示したかを管理する ・ メールアドレスや電話番号、SNSの識別子など、容易に変更ができない識別子を利用せずにメッセージのやりとりを行う ・ メッセージのやりとりがEnd to End暗号化されている	・ OpenID4VPやSD-JWTなどの標準仕様を利用した場合に、従来の方法よりプライバシーバイデザインの考え方に従ったアーキテクチャとなっているか検証を行う
⑦	提案するシステムアーキテクチャーを広く普及させるためには、どのような進め方がよいか	・ 業界団体、国際標準化団体での標準仕様や、仕様策定が進められている技術を広く採用し、証明書発行機関、サービス事業者、ウォレットのコアとなる部分はオープンソースとして公開する ・ サービス事業者、生活者は国内外どちらの存在でも可とし、グローバルな環境を前提としてアーキテクチャの普及を目指す	・ 各業界団体やコミュニティと連携して実装・公開するオープンソースのグローバルな普及を目指し、新たなルール・ガバナンスおよびコミュニティ形成を検討する ・ グローバルでのデータのやりとりを前提として、本ユースケースにおけるデータの越境移転に対するトラスト関連のルールや論点等についてコミュニティを通じて専門家へヒアリングを実施する

実装するシステムアーキテクチャ・アプリ概要



- 証明書発行機関がOpenID4VCIに準拠して証明書を発行するオープンソースコードを開発
- 証明書はウォレットアプリで比較検討し決定した証明書形式に準拠した証明書を発行する

- サービス事業者がOpenID4VP/SIOPv2に準拠して、認証・認可および証明書の検証を実施できるオープンソースコードを開発

- ISO/IEC 23220を参考にし、EUDIWのARFのユースケースへの適合性を検討しながら、国際標準規格や非独占的なOSSをベースとしたウォレットアプリケーションを構築しオープンソースとして公開

- メッセージングサービスはSIOPv2に準拠して、アイデンティティウォレットでログインする想定
- メッセージングプロトコルは標準技術/オープンソースのプロトコルを比較検討し、本ユースケースに沿ったものを選定、または改変して用いる

実装するシステムアーキテクチャ・アプリ概要 (新規性・相互運用性)

技術的な新規性

- 証明書発行プロセス、証明書提示プロセスに国際標準技術であるOpenID4VCI、OpenID4VPを採用予定である。また、認証・認可プロセスにおいても国際標準技術であるSIOPv2を採用予定である
- 昨年度実証事業の報告では、1つの企業がSIOPを採用しており、さらに1つの企業がOpenID4VCI、OpenID4VPに準拠したウォレットを作成しているが、本実証では、認証・認可プロセスにSIOPv2、証明書発行および証明書提示に対応した証明書形式の採用、選択的開示の実証を予定しており、OpenID4VCI、OpenID4VP、SIOPv2、選択的開示(SD-JWT等)に対応したウォレットは現時点では存在せず、これらの標準技術を組み合わせ、実際にシステムを開発することは技術的に新規性が高いといえる
- また、分散型メッセージングプロトコルを利用したサードパーティアプリケーション実装、およびウォレットをつかったメッセージサービスへの認証連携はこれまでになく、技術的に新規性が高いといえる

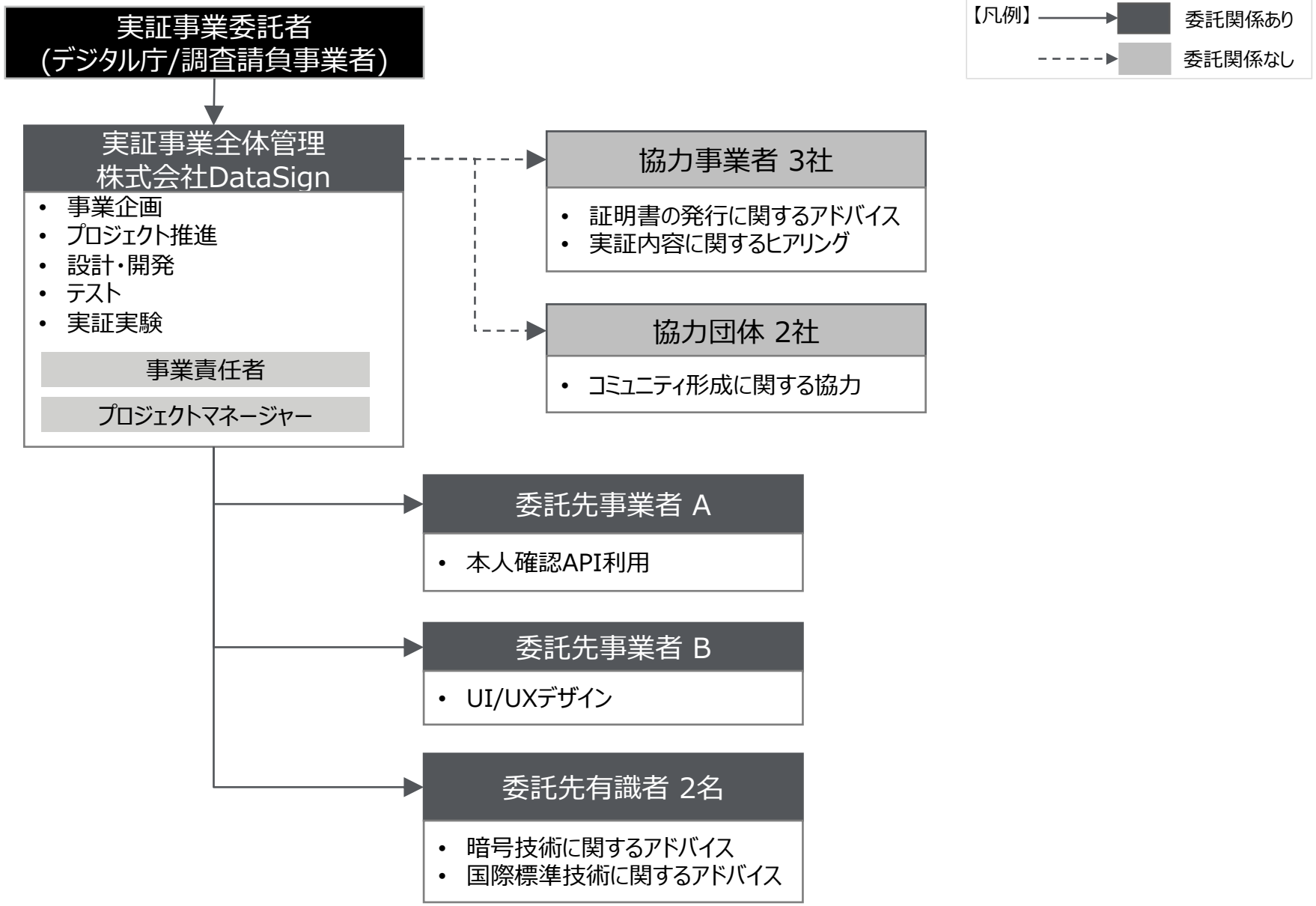
現社会インフラとの相互運用性

- 本実証で作成する証明書発行機関はOpenID4VCI、選択的開示(SD-JWT等)に対応する。ウォレットはOpenID4VCI、OpenID4VP、SIOPv2、選択的開示(SD-JWT等)に対応する。標準仕様をベースとして実装することで、特定の証明書発行機関、ウォレットに依存することなく、現在同様の取り組みを進めているOWFやEUDIWとの連携も将来的に視野に入れ、グローバルに相互運用性が高い仕組みを実現できる可能性が高い
- また、OpenID Connectは現社会インフラとして広く利用されている技術であり、これをベースとしたSIOPv2等の技術にサービス事業者が対応することは難しくない
- メッセージングサービスに関しては、オープンソースのメッセージングプロトコルであれば異なるサービスであってもメッセージのやりとりが可能であり相互運用性が高い仕組みといえる
- さらに現行のメッセージングサービス（Slack等）とのブリッジ接続が可能な方式など、現行インフラとの相互接続も視野に入れた検討を行う

実装するシステムアーキテクチャ・アプリ概要 (機能一覧)

アプリ(システム)	機能	概要
アイデンティティウォレット	秘密鍵・公開鍵生成機能	・ 秘密鍵・公開鍵を生成し、秘密鍵はウォレットに保存、公開鍵はデバイスの提供する安全性の確保された領域に保存する機能
	識別子生成機能	・ 生活者もしくはサービス事業者が利用する識別子を生成する機能（ペアワイズ識別子を想定）
	証明書申請機能	・ 証明書発行機関に対して証明書の発行を申請する機能
	証明書保存機能	・ 証明書発行機関から発行された証明書を保存する機能
	証明書提示機能	・ 生活者もしくはサービス事業者へ証明書を提示する機能
	証明書検証機能	・ 提示された証明書を検証する機能
	履歴機能	・ 証明書を提示した相手や種類の履歴を保存・閲覧する機能
メッセージングプロトコル/サービス	認証・認可機能	・ ウォレットからの認証・認可要求に対して認証・認可を行う機能
	メッセージ検証機能	・ メッセージの送信者・メッセージそのものを検証する機能
	メッセージ暗号化送受信機能	・ メッセージを暗号化した上で送信および受信を行う機能
	メッセージ表示機能	・ メッセージを復号し表示する機能
	メッセージ送信要求機能	・ 特定の相手に対してメッセージの送信を要求する機能
	メッセージ許諾機能	・ 誰からメッセージ送信の要求が来ているか、誰に対してメッセージの送受信を許可したか、を管理する機能
証明書発行機関用システム	認証・証明書発行機能	・ サービス事業者もしくは生活者の認証を行い、審査を実施し、証明書発行機関の秘密鍵で署名された証明書を発行する機能（本実証において証明書は委託先事業者が発行する想定だが、選択的開示に対応した証明書を発行するために必要な機能を開発する想定）
サービス事業者用システム	認証・認可機能	・ 生活者のウォレットに対して認証・認可を行う機能
	証明書検証機能	・ 生活者が提示する証明書を検証する機能

実施体制


【凡例】
委託関係あり
委託関係なし
実証事業委託者
(デジタル庁/調査請負事業者)
実証事業全体管理
株式会社DataSign
• 事業企画
• プロジェクト推進
• 設計・開発
• テスト
• 実証実験
事業責任者
プロジェクトマネージャー
協力事業者 3社
• 証明書の発行に関するアドバイス
• 実証内容に関するヒアリング
協力団体 2社
• コミュニティ形成に関する協力
委託先事業者 A
• 本人確認API利用
委託先事業者 B
• UI/UXデザイン
委託先有識者 2名
• 暗号技術に関するアドバイス
• 国際標準技術に関するアドバイス