TOPPAN

令和 4 年度補正
Trusted Web 開発等推進事業に係る調査研究

【報告書】

（OpenID for Verifiable Credentials
コンフォーマンステスト支援）

2024 年 3 月

TOPPAN 株式会社

本書の位置づけ

Trusted Web の取り組みと同様に諸外国においてもデータや相手方、メッセージのやり取りに関する検証可能性の実現に関する要求の声は高まっている。例えば米国カリフォルニア州におけるモバイル運転免許証や EU における European Digital Identity Wallet の大規模パイロット検証など既に社会実装に向けた具体的な歩みを始めている事例も存在する。

しかしながら、Verifiable Credentials に代表される必要となる要素技術自体およびその利用方法（プロファイル）に関する国際的なコンセンサスが取れている状態には至っていないのが現状であり、各種標準化団体に加えて実際に社会実装を行う主体（政府や業界団体など）が積極的に歩み寄り安全かつ相互運用が可能な状況に向けて共に歩むことが Trusted Web の理念を実現するために最も重要なことの一つである。

上記を背景として、本調査研究事業においては Trusted Web 実証事業に参画した事業者の協力を得て、現在 OpenID Foundation が開発している相互運用性を担保するためのコンフォーマンステストを利用した各事業者のウォレット実装のプロトコル対応状況の検証を行った。この検証を通じて各事業者のウォレット実装の精緻化のみならず今後グローバルで利用されるコンフォーマンステスト自体の改善に繋げ、グローバルで相互運用性のある検証可能なデータ、相手方の認識、メッセージのやり取りといった Trusted Web の理念の実現へ寄与することを目指す。

本報告書は 2024 年 1 月〜3 月にかけて実行された上記事業者によるコンフォーマンステストを利用した検証結果を取りまとめたものである。

目次

1.コンフォーマンステストの概要

OpenID Foundation では同団体が策定する OpenID や OAuth に関連する技術仕様やプロファイルの認定プログラムを提供している。同プログラムは実装者が仕様の適用を行うのを支援し、高品質な実装を提供することを目的としたものである。実装者は認定を受けることにより仕様に準拠した実装であることを外部に表明することが可能となり、実装者のビジネス拡大に繋げることが可能となる。実装者は認定を受けるために自己診断を行う必要があり、当該の診断を行うために利用するのがコンフォーマンステストである。

本調査研究事業においては Trusted Web の開発を推進する上で鍵となる技術仕様の一つである OpenID for Verifiable Credentials に関する認定プログラムの立ち上げに向けて同団体が開発を進めている新たなコンフォーマンステストを利用して Trusted Web 実証事業参加事業者のウォレットの実装を検証することを通じ、実装の品質向上に繋げるだけでなく、同団体の認定プログラムの開発の推進についても支援を行うものである。

1.1. OpenID Foundation における認定プログラムの概要と歴史

先に述べた通り、OpenID Foundation は実装者に向けて仕様適用の推進と実装の品質向上を支援することを目的とした認定プログラムを提供している。

同プログラムは以下の歴史を持つ。

- 2015 年：OpenID Provider 向け認定プログラムを開始
- 2016 年：Relying Party 向け認定プログラムを開始
- 2019 年：FAPI プロファイル実装者向け認定プログラムを開始

なお、本報告書記載時点（2024 年 3 月）における認定実装は下表の通りである。

表 1　認定実装のリスト

対象仕様・プロファイル		概要	認定実装数
OpenID Providers & Profiles	基本プロファイル	OpenID Provider の基本的な実装に関する認定	209
	ログアウトプロファイル	OpenID Provider のログアウトに関する認定	23
OpenID Relying Parties & Profiles	基本プロファイル	Relying Party の基本的な実装に関する認定	53
	ログアウトプロファイル	Relying Party のログアウトに関する認定	6
FAPI OpenID Providers & Profiles	基本プロファイル	FAPI 1.0 対応の OpenID Provider に関する認定	47
	UK オープンバンキング	UK オープンバンキングに関する認定	7

対象仕様・プロファイル		概要	認定実装数
	オーストラリア CDR	オーストラリア CDR に関する認定	10
	ブラジルオープンバンキング	ブラジルオープンバンキングに関する認定	312
	ブラジルオープンファイナンス	ブラジルオープンファイナンス（FAPI-BR v2）に関する認定	128
	ブラジルオープンイシュランス	ブラジルオープンイシュランスに関する認定	86
	KSA（サウジアラビア）オープンバンキング	KSA（サウジアラビア）オープンバンキングに関する認定	22
	FAPI 2nd Implementors Draft	2018 年に発行された FAPI の実装者向けドラフトの第２版に関する認定	74
FAPI CIBA OpenID Providers & Profiles	基本プロファイル	CIBA 対応の OpenID Provider に関する認定	14
FAPI Relying Parties & Profiles	基本プロファイル	FAPI1.0 対応の Relying Party に関する認定	4
	ブラジルオープンバンキング	ブラジルオープンバンキングに関する認定	84
	ブラジルオープンファイナンス	ブラジルオープンファイナンス（FAPI-BR v2）に関する認定	46
	ブラジルオープンイシュランス	ブラジルオープンイシュランスに関する認定	74
	KSA（サウジアラビア）オープンバンキング	KSA（サウジアラビア）オープンバンキングに関する認定	17
	FAPI 2nd Implementors Draft	2018 年に発行された FAPI の実装者向けドラフトの第２版に関する認定	3
FAPI2 Providers & Profiles	FAPI2.0 Security Profile 2nd Implementers Draft & Message Signing 1st	FAPI2.0 のセキュリティプロファイル（実装者向けドラフト第２版）およびメッセージ署名（実装者向けドラフト第１版）に関する認定	7

対象仕様・プロファイル		概要	認定実装数
	Implementers Draft		
	オーストラリア FAPI2.0 ConnectID Implementers Draft	オーストラリアの FAPI2.0 ConnectID 実装者向けドラフトに関する認定	6
FAPI2 Relying Parties & Profiles	FAPI2.0 Security Profile 2nd Implementers Draft & Message Signing 1st Implementers Draft	FAPI2.0 のセキュリティプロファイル（実装者向けドラフト第２版）およびメッセージ署名（実装者向けドラフト第１版）に関する認定	2
	オーストラリア FAPI2.0 ConnectID Implementers Draft	オーストラリアの FAPI2.0 ConnectID 実装者向けドラフトに関する認定	21

１.２. 認定に向けた一般的な流れ

実装者が OpenID Foundation の認定プログラムによる認定を受けるための流れは一般に下記の通りである。

1. 実装者自身でテストを実施（コンフォーマンステストを利用）
2. テストログを OpenID Foundation へ提出
3. 認定費用の支払い
4. OpenID Foundation によりログの確認を行い問題がなければ認定し公表
5. 認定マークを事業者へ付与

なお、本調査研究事業時点においては OpenID for Verifiable Credentials に関する認定プログラムは開発中であり、開発中のコンフォーマンステストを利用して実装の確認を行ったとしても正式な認定の対象とはならない。（ただし、OpenID Foundation 関連の Web サイト等で本調査研究事業によりコンフォーマンステスト開発を支援したことを公表する予定である。）

１.３. OpenID for Verifiable Credentials に関するテスト開発状況

本調査研究事業時点における OpenID for Verifiable Credentials 関連のコンフォーマンステストの開発状況は下表の通りである。

表 2　コンフォーマンステストの開発状況

仕様	開発状況	備考
OpenID for Verifiable Presentations	Implementer's Draft 2 に対応したテストを開発中	シナリオ - No-state - With-state-and-redirect - Response_uri-not-client_id 以下のパラメータに対応 - Presentation_defition = request_uri - Response_mode = direct_post - 対応クレデンシャルフォーマットは sd-jwt-vc ならびに ISO mDoc
OpenID for Verifiable Credential Issuance	未着手	

1.4. OpenID for Verifiable Credentials に関するテストツールの概要

本調査研究事業時点におけるテストツールの概要は下記の通りである。

ツール URL：

https://openid.net/certification/conformance-testing-for-openid-for-verifiable-presentations/

利用イメージ：

1. ログイン

   テストを開始するためにはツールへログインする必要がある。Google アカウント、Gitlab アカウント、もしくは WebFinger で発見できる OpenID Provider でログインを行う。

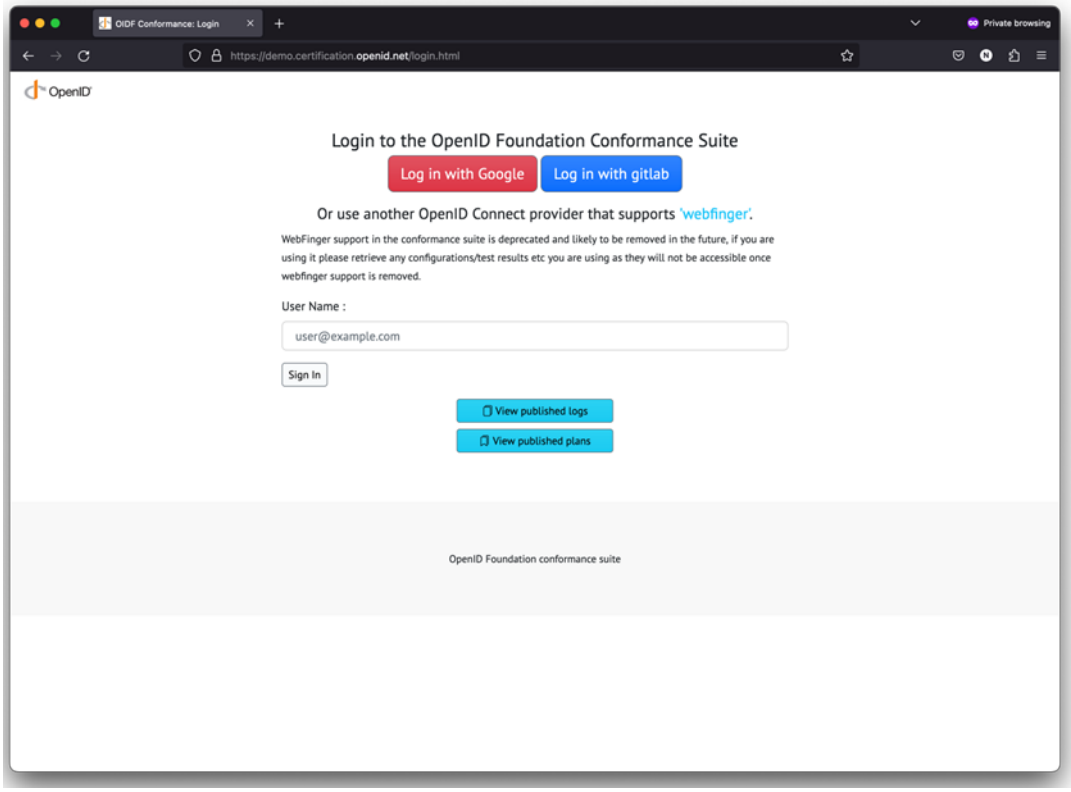

図 1　ログイン画面

2. テストラン・ログの管理
   ログインするとテストプランやログを管理する画面が表示される。初回はテストプランの作成を行う必要がある。

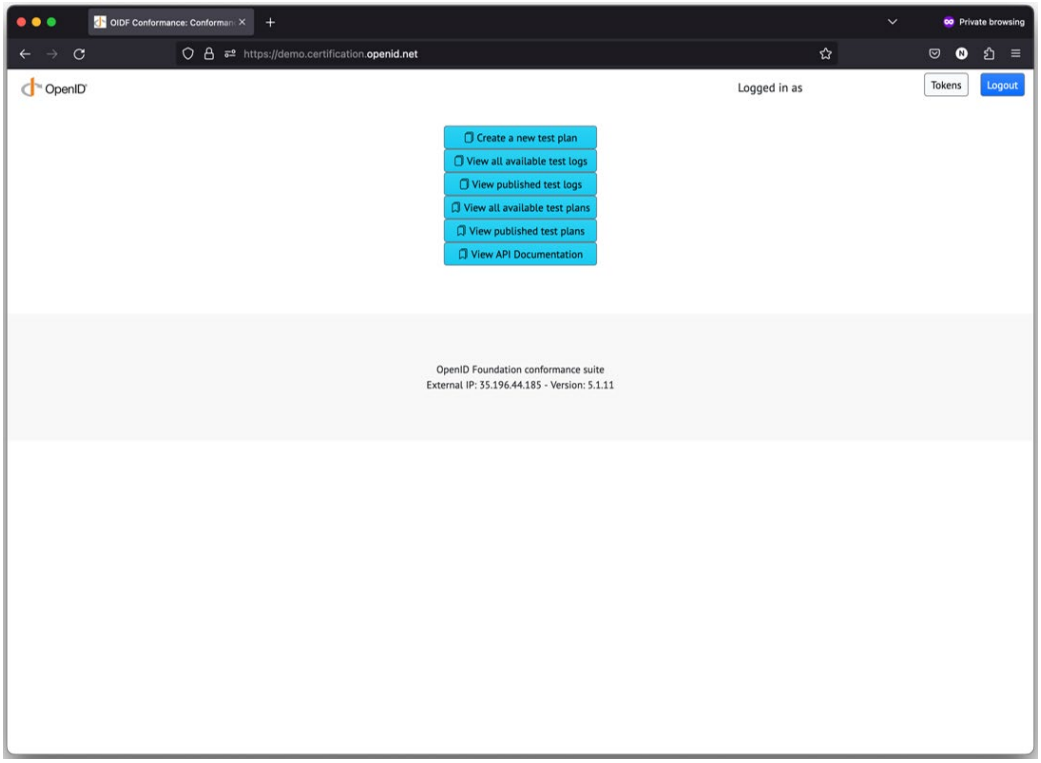

図 2　テストプラン・ログの管理画面

3. テストプランの作成

OpenID for Verifiable Presentations のテストプランを作成する際は以下の通りパラメータを設定する。

- Test Plan : OpenID for Verifiable Presentations ID2 を指定する
- Server – authorization_endpoint : Wallet の認可エンドポイントを指定する
- Client – presentation_definition : Verifier が指定する presentation_definition を指定する

なお、Test Information の Publish を Yes にするとテストログが公開されるため注意が必要である。

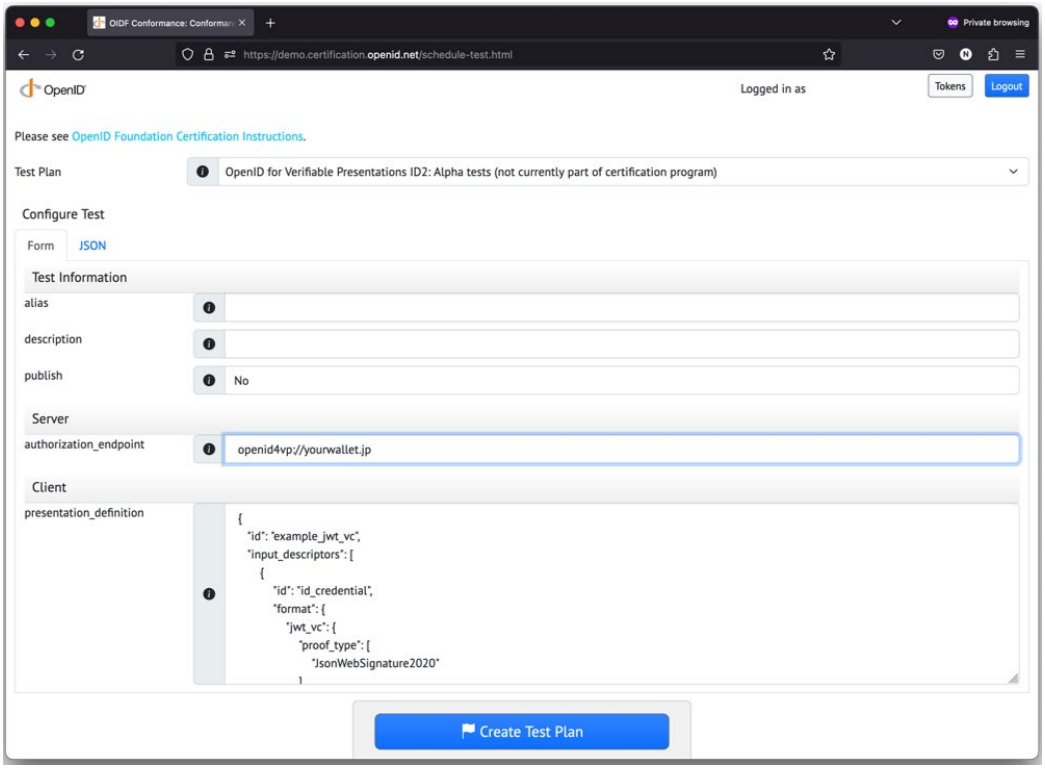

図 3　テストプランの作成画面

4. テストシナリオの選択

テストプランの作成が完了したらテストシナリオを選択する。プリセットされているテストシナリオは以下の通り。

- oid4vp-happy-flow-no-state（正常系）
- oid4vp-happy-flow-with-state-and-redirect（正常系）
- oid4vp-happy-flow-response-uri-not-client-id（異常系）

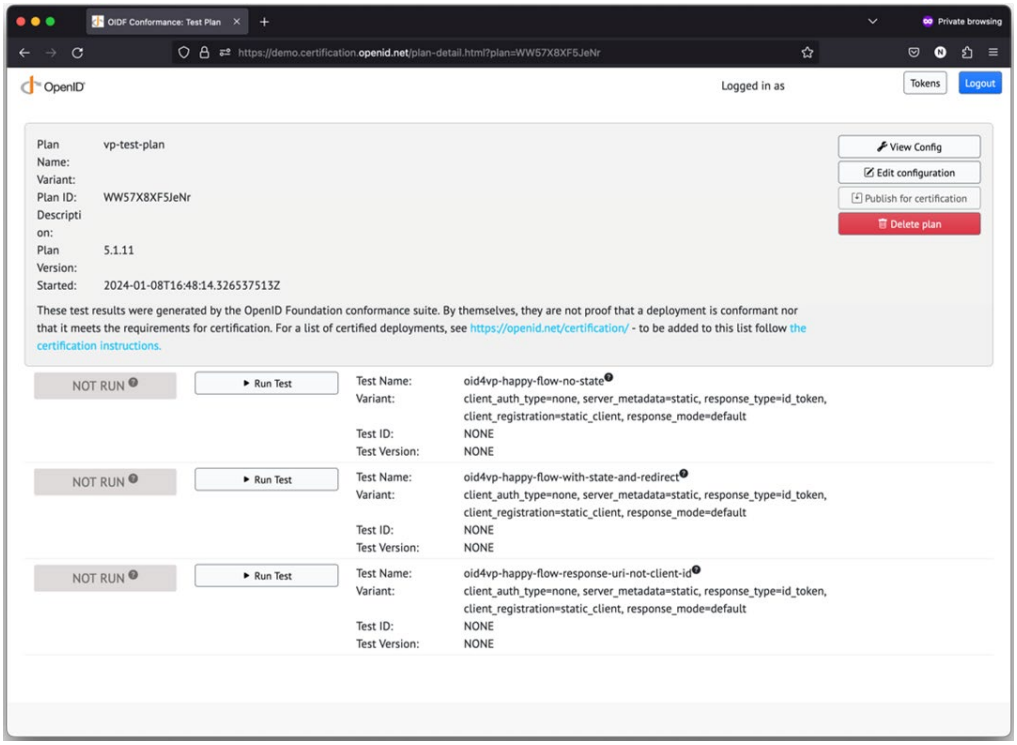

図 4　テストシナリオ選択画面

5.　テストの実行

テストシナリオを選択し、テストを実行する。画面に表示されるステップに従い Wallet で QR コードを読み込む等、OpenID for Verifiable Presentations の実行に必要なアクションを実行する。

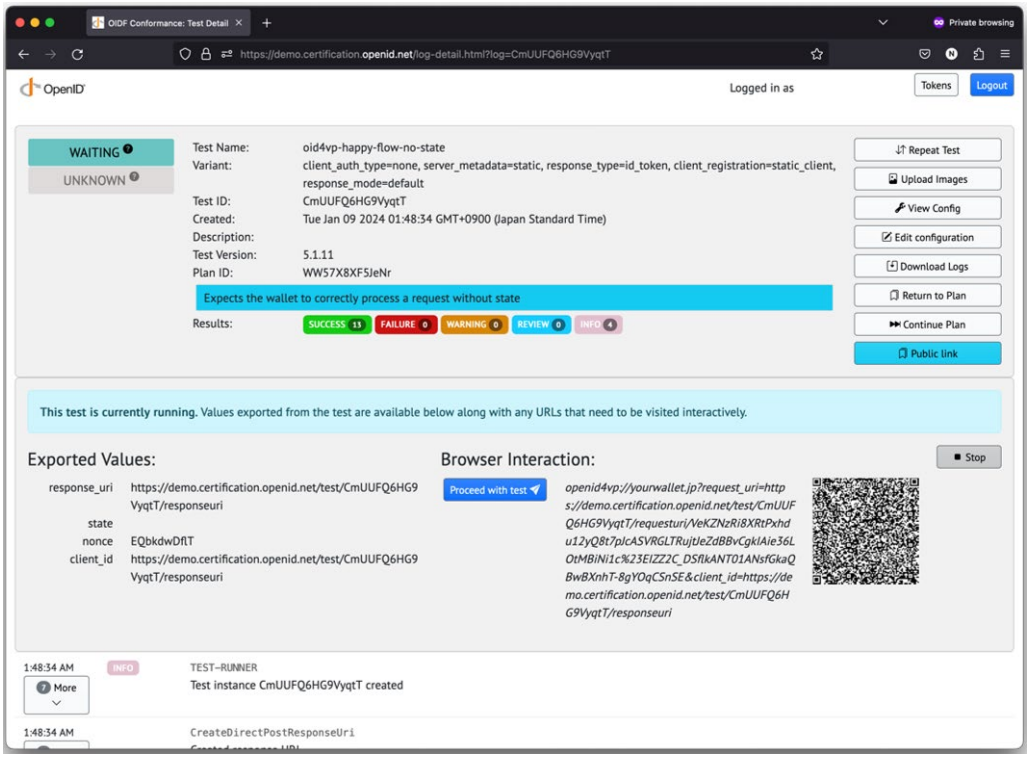

図 5　テスト実行画面

2.本調査研究事業におけるコンフォーマンステスト実施概要

2.1. コンフォーマンステスト開発支援の目的

本調査研究事業において OpenID Foundation のコンフォーマンステスト開発を支援する目的は以下の通りである。

- 開発中とは言え、仕様策定団体の提供するテストを利用することで Trusted Web 実証事業参加事業者の実装品質を向上する
- 今後の相互運用性の実現に向けて実装者が標準仕様への対応を行うための勘所についての理解を促進する
- 国際的な仕様策定団体である OpenID Foundation のプログラム開発を支援することを公表することにより Trusted Web 関連事業の国際的なプレゼンスを向上する

2.2. 参加事業者一覧

コンフォーマンステストを利用した実装テストに参加した Trusted Web 実証事業参加事業者は下表の通りである。

表 3　参加事業者一覧

事業者名	ユースケース名	実装に関する補足
株式会社 DataSign	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	同社開発の OWND Wallet を利用
大日本印刷株式会社	共助アプリにおけるプラットフォームを超えたユーザートラストの共有	Meeco 社の実装を利用
株式会社 ORPHE	下肢運動器疾患患者と医師、研究者間の信用できる歩行データ認証・流通システム	Data Gateway 社の実装を利用
一般社団法人情報サービス産業協会（JISA）	補助金事業を題材として法人向け行政手続 DX 社会基盤化のプレ検討	B 類型のため実装なし（机上検討のみ）

2.3. コンフォーマンステスト実施までの流れ

下図のスケジュールで本調査研究事業を進めた。

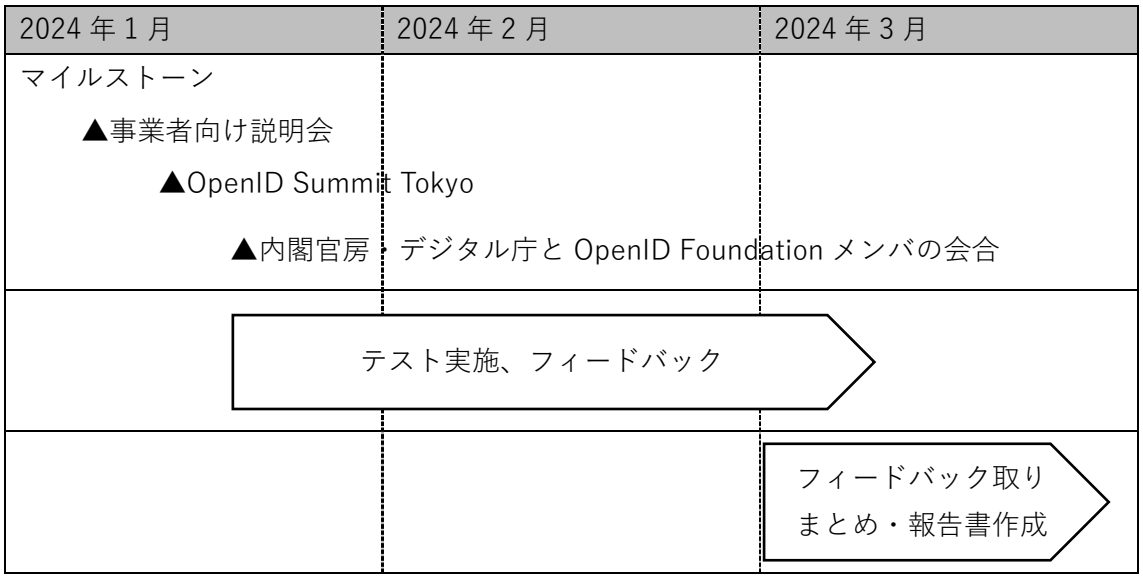
2024 年 1 月
2024 年 2 月
2024 年 3 月
マイルストーン
▲事業者向け説明会
▲OpenID Summit Tokyo
▲内閣官房・デジタル庁と OpenID Foundation メンバの会合
テスト実施、フィードバック
フィードバック取り
まとめ・報告書作成

図 6　実施スケジュール

3.コンフォーマンステスト実施の結果

前述の通り、各事業者によりコンフォーマンステストの実施を行い、以下の通りの結果が得られた。なお、株式会社 DataSign および大日本印刷株式会社の 2 社が実際にテストを行い、フィードバックを得ることができた。

3.1. 株式会社 DataSign

（1） テストに利用した環境

以下の通り実装したウォレットを利用してテストを実施した。

表 4　テスト環境

区分		実装	備考
プロトコル	発行	OpenID for Verifiable Credential Issuance ※pre-auth-flow、credential endpoint のみ	Draft 12
	提示	OpenID for Verifiable Presentations ※cross device flow のみ、jwt_vc_json は direct_post のみ	Draft 18
クレデンシャル フォーマット		SD-JWT（draft-ietf-oauth-sd-jwt-vc-01） JWT_VC_JSON（VC signed as JWT）	

（2） ユースケース概要

1. マイナンバーカードから読み取った情報を VC として発行、年齢確認が必要なサービスへのサインアップに 13 歳以上、15 歳以上、などの情報を選択開示して提示する。
2. 社員証を VC として発行し、メッセージサービス（Matix 拡張）上で利用者の属性として開示し、利用者同士が互いに所属を明らかにした上で相互にコミュニケーションを開始するために利用する。（この際、メッセージサービスが VCI / VP に対応しており利用者のクレデンシャルの受け取りと検証を実施する。）
3. イベントの参加証を VC として発行、上記のメッセージサービスにて同様に利用者の属性情報として VC を登録することで、イベントへの参加実績の確認に利用する。

（3） コンフォーマンステスト実施結果

以下の通りテストを実施した。

表 5　テスト結果

テスト日	結果	結果詳細
2/19	失敗	request_uri_signed のテストで登録した jwk に d プロパティを指定し忘れた（登録時点でエラーになる挙動が望ましい）

テスト日	結果	結果詳細
2/19	失敗	request_uri_signed のテストで登録した jwk に alg プロパティを指定し忘れた
2/19	失敗	request_uri_signed のテストを試みたが、署名の検証にあたり公開鍵を取得する手段が無く、実施を見送った（client_metada を介しての取得を想定）
2/19	失敗	VP トークンを送信した際に state パラメータの返却漏れで NG（その後修正して OK）
2/19	失敗	VP トークンを送信した際にレスポンスボディの redirect_uri へアクセスしていなかったため（その後修正して OK）
2/19	成功	request_uri_unsigned のテストで、上記 2 件の NG に対応した結果、oid4vp-happy-flow-no-state と oid4vp-happy-flow-with-state-and-redirect のテストを Pass

（4） コンフォーマンステストに関するフィードバック・コメント

コンフォーマンステストを通じて以下のコメントを得た。

テストツール自体について

表 6　テストツール自体に関するフィードバック・コメント

項番	フィードバック・コメント	補足
1	個別の Plan の画面の「Edit Configulation」が実際には新しいプランを作成する挙動なので文言は変えた方が良い	
2	alias の役割が解りにくい	redirect_uri などに影響があって重要な入力内容なので、アイコンのマウスオーバー不要で説明が表示された方が良いと感じる
3	セッションが切れるまでの時間が短い	テスト中に何度か再ログインを求められた
4	vp-test-plan を作成するとテストケースが 3 つ生成されますが、どのような基準でこのケースが選ばれているのかが不明瞭なので選択の基準などがわかるようにしてほしい	
5	個別の Plan 画面でも失敗したテストの Failure summary が表示できると良い	
6	テストが失敗した際に、根拠となる仕様へのリンクが表示される点はとても便利	

テストシナリオについて

表 7　テストシナリオに関するフィードバック・コメント

区分	シナリオ	コメント
プリセット	oid4vp-happy-flow-no-state	特になし
	oid4vp-happy-flow-with-state-and-redirect	特になし
	oid4vp-happy-flow-response-uri-not-client-id	異常系のシナリオは各種考えられると思うが、なぜこのシナリオが選ばれたのか不明
追加希望	jwks_uri による verifyer の公開鍵の取得と signed_request の検証	現状、signed_request の検証ができないため追加を希望

その他のコメント

表 8　その他のコメント

区分	シナリオ	コメント
クレデンシャルフォーマット	素の JWT-VC への対応	選択開示が必要ないシナリオは様々発生すると考えらえる
シナリオ	クライアントの動的登録のシナリオの対応 （client_metadata/client_metadata_uri パラメータに連動したウォレットの挙動の確認）	まずウォレットに対して verifier が静的登録するシナリオはあまり現実的ではない。 また、configuration で client_metadata の任意のパラメータに値をセットできると、ウォレット上で表示するクライアント情報が登録した通りか確認可能となるため。 （例えば今回実装したウォレットでは提供同意画面でクライアントの名前、ドメイン、プライバシーポリシー URL、利用規約 URL などを client_metadata から取得して表示している）
その他	仕様へのコメント	動的クライアントの場合、公開鍵を jwks で公開しても任意の URL になってしまうため signed_request の検証の重要性があまり高くないのかもしれな

区分	シナリオ	コメント
		いが、例えば/.well-known 配下に設置するルールなどがあれば少なくともドメインの持ち主であることは保証ができるので、その様な仕様となれば一定の意味を持たせられるのではないか。

3.2. 大日本印刷株式会社

（1） テストに利用した環境

以下の通り実装したウォレットを利用してテストを実施した。

表 9　テスト環境

区分		実装	備考
プロトコル	発行	OpenID for Verifiable Credential Issuance	Draft 13
	提示	OpenID for Verifiable Presentations	Draft 10, 20
クレデンシャル フォーマット		SD-JWT-VC JWT_VC_JSON（VC signed as JWT）	

（2） ユースケース概要

共助アプリが共助実績をユーザに発行し、別の共助アプリや第三者企業による検証を行うことができる。

（3） コンフォーマンステスト実施結果

以下の通りテストを実施した。

表 10　テスト結果

テスト日	結果	結果詳細
1/25	失敗	リクエスト URI に追加されたフラグメントが原因でテストが失敗した ※テスト側の不具合。フィードバックを行い後に修正された
2/13	失敗	kb-jwt に正しい iss と iat の値がない問題を発見
2/14	成功	全てのシナリオで成功
3/6	失敗	Configuration request_uri_signed を使用する際、JWKS に use=sig を持つ複数の JWK を提供すると、テストがエラーとなる事象を発見（テスト側の想定が JWK は一つである前提だったため）

（4） コンフォーマンステストに関するフィードバック・コメント

コンフォーマンステストを通じて以下のコメントを得た。

テストツール自体について

表 11　テストツール自体に関するフィードバック・コメント

項番	フィードバック・コメント	補足
1	初めてツールを使用した際に、エンティティ“Plan”、“Log”“Configuration”、“Test”といった用語が直観的に分かりにくい。	これらが何であるか、また互いにどのように関連しているかを説明するセクションがあるとよい。
2	“Browser Interaction”が何なのか初見では分かりにくいため、解説を追加すべき。	Same device flow ではボタンが使用され、QR コードが Cross device flow に使用されることを説明することで Browser Interaction の用途が分かりやすくなる。 また QR コードはデバッグや API ベースのウォレットに役立つ。
3	一部の設定オプションについてエラーが起きている。	Client Id Scheme redirect_uri & Request Method request_uri_signed を選択すると、無効なシナリオになってしまう。
4	OpenID4VP で規定されているクレデンシャル形式の識別子をラベルとして使用する。	sd_jwt_vc を vc+sd-jwt に変更する。 （ラベルを仕様に合わせる）
5	テストログの表示が常に 10 にリセットされるので、100 件表示に変更する。	テストログを表示 > 「100 件表示」に変更 > ログを表示 > 戻る > 10 件表示

テストシナリオについて

表 12　テストシナリオに関するフィードバック

区分	シナリオ	コメント
プリセット	oid4vp-happy-flow-no-state	特になし
	oid4vp-happy-flow-with-state-and-redirect	特になし
	oid4vp-happy-flow-response-uri-not-client-id	特になし
追加希望	Flow with client_id_scheme = did	他の client_id_scheme をテストする方法があるとよい。
	Flow where response_type = vp_token id_token	SIOPv2 についてもテストできると良い

その他のコメント

表 13　その他のコメント

区分	シナリオ	コメント
クレデンシャルフォーマット	素の JWT-VC への対応	典型的なシナリオではまだ Selective Disclosure は不要なため、SD-JWT-VC 以外に JWT-VC もサポートすべきである

4.今後の展望

現状の認定プログラムにおいては例えば UK オープンバンキング向けプロファイル認定など、基本的な技術仕様のみならず具体的なユースケースに特化した認定が数多く存在する。今後 Trusted Web の社会実装を行い、諸外国とも相互運用を目指す上では Trusted Web 対応プロファイルの策定および認定のスキームの確立が重要になることは明白である。

Trusted Web 事業においてはガバナンスモデルの策定を行い、実装に繋げるために本認定プログラムを有効に活用していくことが望ましい。

また、テストツールに関して現状は Wallet のみを対象としているが、Issuer/Verifier についてもテストを実行できるようにすることで安全で相互運用性がある環境の実現に寄与できるものと考えられる。

以上