仕様書別紙２

共通ID基盤接続仕様書

この仕様書は、本システムと共通 ID 基盤の OIDC 連携の構築に係る業務内容を示すものである。

１　業務名

令和８年度　観文文委第 16 号　文化施設貸館システム構築業務

２　業務の目的

本システムについて、静岡市の共通 ID 基盤との OIDC 連携によるログインを実装し、本システムの共通 ID によるログインを可能とするとともに、静岡市ワンストップポータルサイトから本システムへの共通 ID によるシングルサインオンを実現することにより、利用者の利便性向上および職員の業務効率化を図ることを目的とし、システムの機能改修を行うものとする。

３　業務内容

３．１　プロジェクト管理

（１）プロジェクト管理

本業務を円滑に進めるために、計画策定、進捗管理、品質管理、リソース管理、情報セキュリティ管理、リスク管理、会議体運営等必要な作業を行うこと。また、共通 ID 基盤の構築事業者との連携を図ること。

（２）要件定義

契約締結後、本仕様書を踏まえて実装する機能要件などについて、本市DX推進課及び本市対象業務所管課と対面もしくはＷＥＢ会議形式で協議を行い、システムの内容が把握できるように要件定義書を作成した上で報告会を開催し、本市の承認を得ること。また、既存利用者のアカウントと共通IDの紐付け等、機能構築後の業務フローを作成すること。

（３）本システムと共通 ID 基盤の ID 連携機能の構築

本市が承認した要件定義書に基づき、本システムの既存IDと共通IDの紐付けによる、共通IDによるログインおよび、静岡市ワンストップポータルサイトから本システムへの共通IDによるシングルサインオンを可能とする。また、構築において、共通ID基盤との接続テストの計画書（想定テスト項目等を含む）を作成し、接続テストを実施した上で、テスト結果報告書を作成すること。

４　技術要件

４．１　必須技術要件

（１）プロトコルおよびフロー

・OpenID Connect Core 1.0 に準拠すること。

・Authorization Code Flow(認可コードフロー)をサポートすること。

（2）エンドポイント

以下のエンドポイントは共通 ID 基盤より提供されるものとする。

また、すべてのエンドポイントとの通信は HTTPS により通信が暗号化済である。

・Authorization Endpoint

：利用者の認証を開始するためのエンドポイント

・Token Endpoint

：ID トークンおよびアクセストークンを取得するためのエンドポイント

・UserInfo Endpoint

：ユーザ情報を取得するためのエンドポイント

・JWK Set URI（JSON Web Key Set URI ）

：ID トークンの電子署名の検証用公開鍵のリストを JSON 形式で提供する URL

（3）ID トークン

ID トークンは共通 ID 基盤より以下の形式で提供されるものとする。

・JWT（JSON Web Token）形式。

・後述の「ID トークンのクレーム情報」に記載されたクレーム（利用者に関する情報）。

・署名アルゴリズム RS256（RSA Signature with SHA-256）。

（4）ID トークンのクレーム情報

ID トークンのクレームは下記を含むこと。

・iss（Issuer Identifier）

：共通 ID 基盤（IdP：Identity Provider）の一意な識別子（URL 形式）。

・sub（Subject Identifier）

：利用者の一意な識別子。この値は永続的で、再割り当てなし。

・aud（Audience）

：本システム（RP:Relying Party）のクライアント ID。

・exp（Expiration Time）

：ID トークンの有効期限（Unix タイムスタンプ形式）。

・iat（Issued At Time）

：ID トークンの発行時刻（Unix タイムスタンプ形式）。

・nonce（Nonce）

：認証リクエスト時に本システム（RP）が指定した nonce の値。
（リプレイアタック防止用）

（5）Openid （必須）

その他、標準で定義されている profile や email などのスコープと追加で定義されるカスタムスコープについては共通 ID 基盤の定義を確認後、本システムとの連携に追加で必要なスコープが発生した場合別途協議する。

（6）セキュリティ

① 通信の暗号化

・すべてのエンドポイント（Authorization Endpoint, Token Endpoint, および推奨される UserInfo Endpoint 等）との通信は、HTTPS（TLS による暗号化）で行うこと。

TLS のバージョンは、TLS 1.2 以上を必須とする。可能であれば、より安全な TLS 1.3 の利用が望ましい。

・既知の脆弱性が存在する古いプロトコルバージョン（例: SSLv3、TLS 1.0、TLS 1.1）はサポートしないこと。

② 認証リクエストおよびトークンリクエスト

・認証リクエストおよびトークンリクエストにおいて、state パラメータおよび nonce パラメータをサポートし、CSRF（クロスサイトリクエストフォージェリ）攻撃やリプレイ攻撃への対策を講じること。

５．２ 推奨技術要件

共通 ID 基盤が下記の技術要件を満たしていることが望まれる

（１）PKCE(Proof Key for Code Exchange)

共通 ID 基盤は、PKCE（Proof Key for Code Exchange by OAuth Public Clients / RFC 7636)をサポートしていること。

（２）OAuth 2.0 および OpenID Connect の仕様に準拠したエラーレスポンスを返すこと。

５．３ 提供情報

共通 ID 基盤との連携に必要な情報は以下の通り。

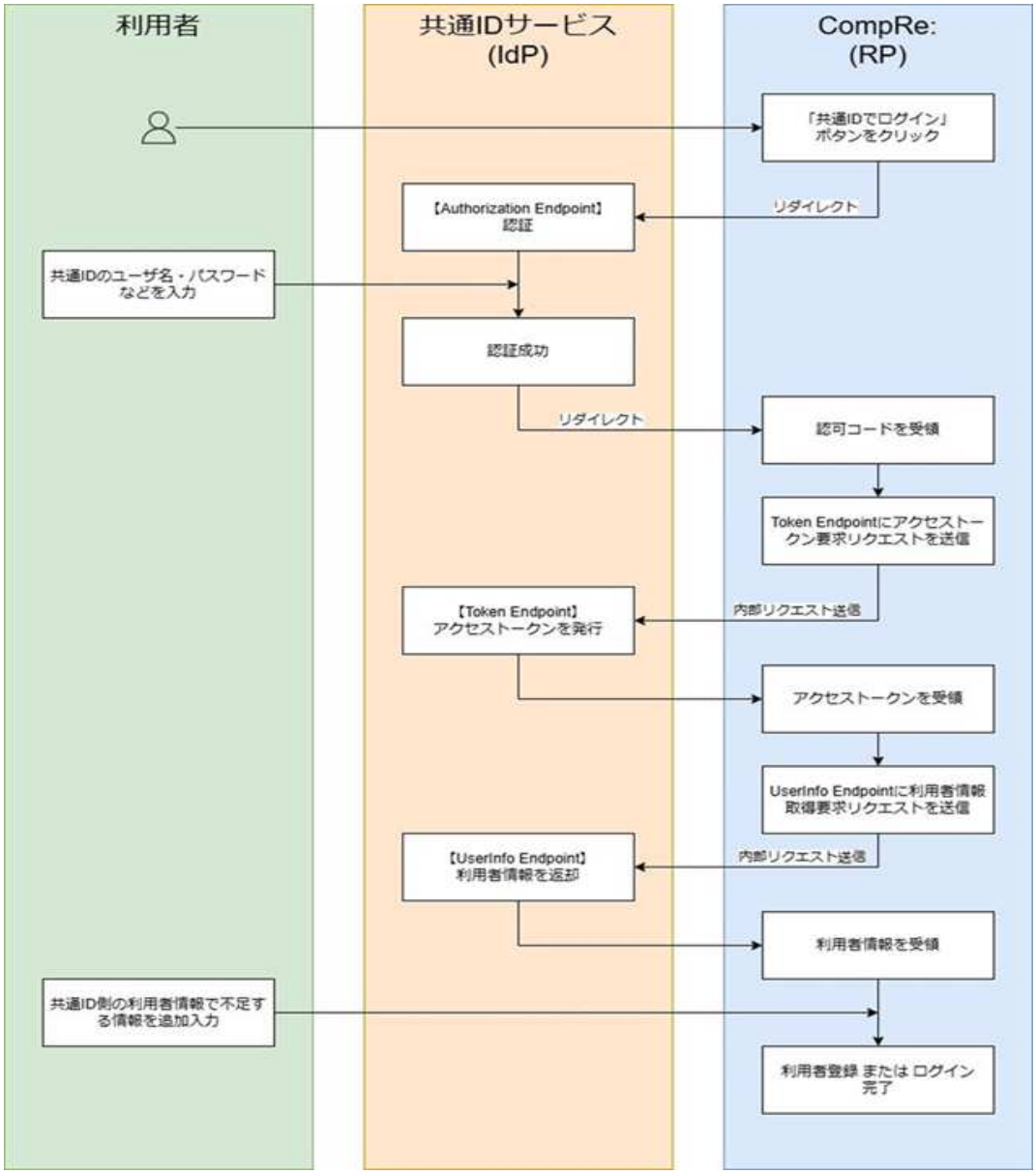
・各エンドポイントの URL

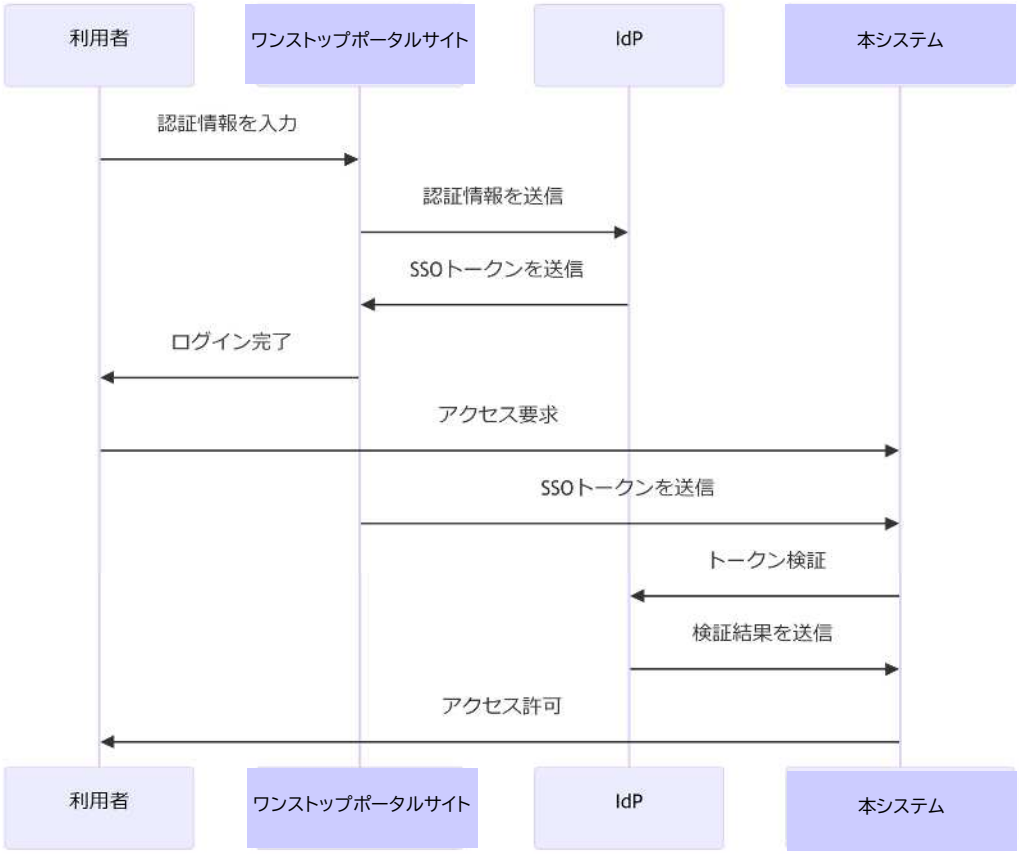
・クライアント登録方法（クライアントとして登録する際の手順（静的登録、または可能であれば動的クライアント登録）

・共通 ID 基盤の技術仕様に関するドキュメント（API 仕様書、IF 仕様書など）

・利用可能なスコープと、それによって取得可能なクレーム（利用者情報）の一覧

（参考）連携イメージ


利用者
共通IDサービス
(IdP)
CompRe:
(RP)
「共通IDでログイン」
ボタンをクリック
リダイレクト
【Authorization Endpoint】
認証
共通IDのユーザ名・パスワード
などを入力
認証成功
リダイレクト
認可コードを受領
Token Endpointにアクセストー
クン要求リクエストを送信
内部リクエスト送信
【Token Endpoint】
アクセストークンを発行
アクセストークンを受領
UserInfo Endpointに利用者情報
取得要求リクエストを送信
内部リクエスト送信
【UserInfo Endpoint】
利用者情報を返却
利用者情報を受領
共通ID側の利用者情報で不足す
る情報を追加入力
利用者登録 または ログイン
完了


利用者
ワンストップポータルサイト
IdP
本システム
認証情報を入力
認証情報を送信
SSOトークンを送信
ログイン完了
アクセス要求
SSOトークンを送信
トークン検証
検証結果を送信
アクセス許可
利用者
ワンストップポータルサイト
IdP
本システム