本資料は配布事業者様・団体様内までの範囲でお取扱いください

大阪広域データ連携基盤(ORDEN)
ID 連携仕様書

大阪府スマートシティ戦略部

第 2.3 版

令和 7 年 03 月 21 日

目次

1．はじめに

1．1．本紙の目的

本紙は事業者向けに、ORDEN の ID 連携基盤との連携を検討する為に必要な情報を提供します。ID 連携基盤との連携は標準仕様である OAuth2.0(RFC 6749[1])/OpenID Connect(OpenID Connect Core 1.0[2])のプロトコルに準拠しており、本紙では連携仕様の詳細な内容ではなく、概要を説明します。

本紙では ID 連携基盤との連携について、下記の 2 点について記載します。

1. ID フェデレーション

   ID 連携基盤利用者の認証を行うことで連携サービスのログインを可能にする。

2. 属性情報取得

   本人同意の下、ID 連携基盤利用者の属性情報を連携サービスが ID 連携基盤から取得する。

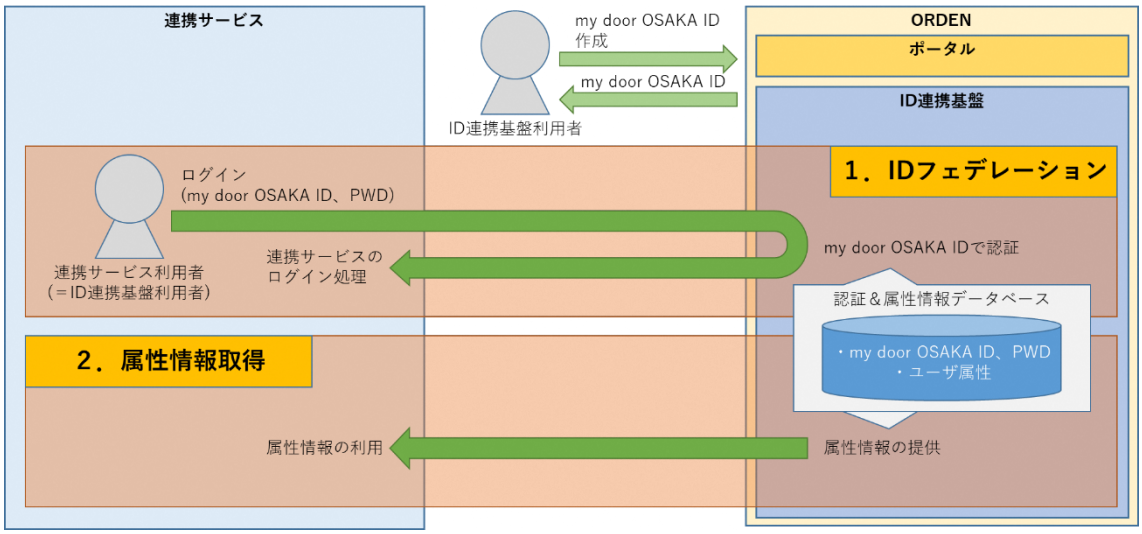

図 1．ID 連携基盤との連携イメージ

1．2．用語集

表 1 に、本紙で使用する用語の一覧を記載します。

表 1．用語一覧

#	名称	説明
1	ORDEN	府民や来街者の利便性向上につながるサービスを創出する為のプラット

[1] https://www.rfc-editor.org/rfc/rfc6749

[2] https://openid.net/specs/openid-connect-core-1_0.html

		フォームで、ポータルと ID 連携基盤により構成される
2	ID 連携基盤利用者	ID 連携基盤を利用する府民や来街者
3	ポータル	府民や来街者に対して様々な情報を提供するポータルサイト
4	OP (OpenID Provider)	ID 連携基盤として OpenID による認証機能を提供する
5	my door OSAKA ID	ID 連携基盤利用者が ID 連携基盤で認証する際に利用する利用者自身のメールアドレス
6	共通 ID	OP が ID 連携基盤利用者に対して発行する ID で、ID 連携基盤利用者を一意に識別する為の ID
7	RP (Relying Party)	OP に対して認証要求を行う Web アプリケーション
8	UA (User Agent)	ID 連携基盤利用者が操作する Web ブラウザ及びスマホアプリ
9	ID トークン	ID 連携基盤利用者の認証情報を含むトークンで、OP から RP に発行される
１０	アクセストークン	属性情報の取得権限を持つトークンで、OP から RP に発行される
１１	属性情報	ID 連携基盤利用者の氏名や住所等の情報
１２	連携事業者	ID 連携基盤との連携サービスを提供する事業者
１３	連携サービス	ID 連携基盤の認証機能や属性情報提供機能を利用するサービス
１４	クライアント ID	OP が連携サービスに対して発行する ID で、連携サービスを一意に識別する為の ID
１５	クライアントシークレット	クライアント ID と対の、OP にアクセスする為に必要となる資格情報

１．３．参考資料

ID 連携基盤との連携仕様に関する詳細な内容として、表２に記載の資料を用意しています。表２の各資料は大阪府(以下、本府)と事業者との協議に際し提供します。

表２．連携仕様に関する資料

#	名称	説明	フォーマット
1	【ORDEN】ID 基盤開発ガイド-アプリ連携編	連携サービスが ID 連携基盤と連携する為に必要な具体的な情報と API の仕様を記載	.pptx
2	【ORDEN】ID 基盤開発ガイド_別紙 1.トークン仕様と検証方法	トークンの仕様と検証方法の詳細を記載	.pptx
3	【ORDEN】ID 基盤開発ガイド_別紙 2.ORDEN ID 基盤で	属性の詳細を記載	.xlsx

	保持する属性		

1．4．ID 連携基盤との連携に向けた事前準備

ID 連携基盤との連携には ID 連携基盤が発行するクライアント ID とクライアントシークレットが必要です。クライアント ID/シークレットは本府と事業者との協議により発行するものとします。図 2 にクライアント ID/シークレットを取得するまでの基本的な流れを示します。

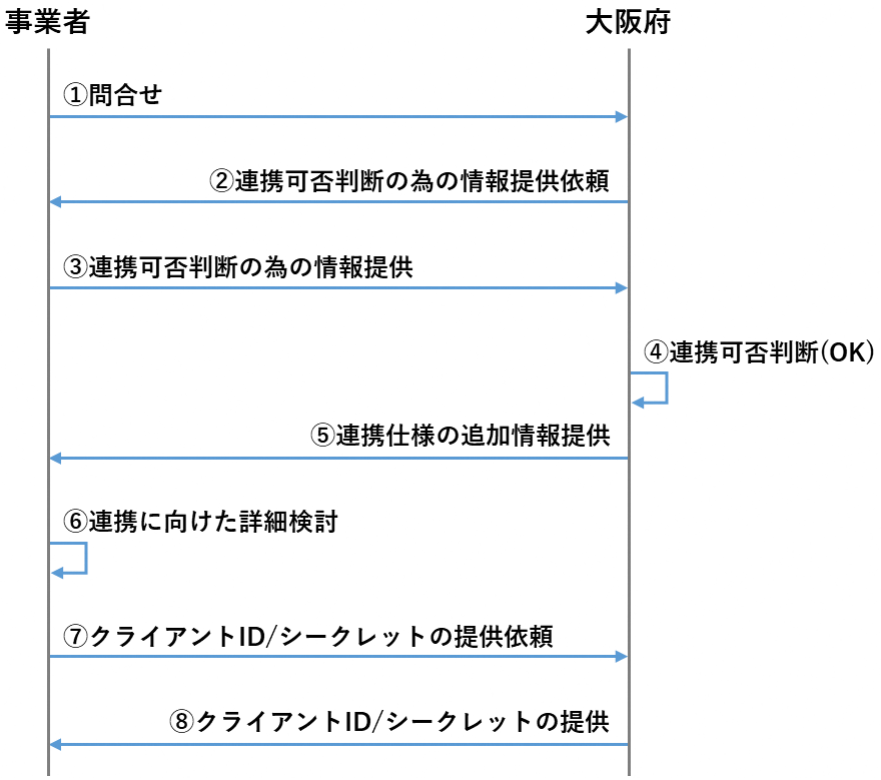

図 2．クライアント ID/シークレット取得までの流れ

#	実施事項	実施者	実施内容
①	問合せ	事業者	ID 連携基盤との連携を希望する事業者は、8 章に記載の問合せ先に下記の事項を記載の上ご連絡ください。 ・事業者名 ・担当者氏名と連絡先(メール、TEL) ・連携を希望するサービスの名称と概要、ID 連携基盤との連携イメージの概要
②	連携可否判断の為の情報提	大阪府	本府では ID 連携基盤との連携可否を判断する為に、「事業性」、「ORDEN 規約ポリシーの遵守」、「セキュリティ」、「個人情報保護」の観点で基準を

	供依頼		定めており、ID 連携基盤との連携を希望する事業者は連携にあたり本基準をクリアする必要があります。各観点に対する対応状況を確認する為のチェックシートを用意しています。下記に各基準の概要を示します。 ・事業性チェック 連携を希望する事業者のサービスが ORDEN の目的と合致しているか、サービスの需要、事業者の信用を確認します。 ・ORDEN 規約ポリシーの遵守チェック 本府より ORDEN のサービス利用規約とポリシーを提示し、連携事業者にて遵守可能か確認します。 ・セキュリティチェック 本府にて作成したセキュリティチェックシート(総務省セキュリティガイドライン参考)を、連携を希望する事業者にて記載し、本府にてチェックシートを確認して連携可否を判断します。 ・個人情報保護チェック 本府にて作成した個人情報保護チェックシートを連携事業者にて記載し、本府にてチェックシートから個人情報保護において問題がないか確認して連携可否を判断します。
③	連携可否判断の為の情報提供	事業者	「事業性」、「ORDEN 規約ポリシーの遵守」、「セキュリティ」、「個人情報保護」の各観点に対する対応状況をチェックシートに記入して提供します。
④	連携可否判断	大阪府	事業者から提供されたチェックシートを基に、ID 連携基盤と事業者との連携可否を判断します。
⑤	連携仕様の追加情報提供	大阪府	ID 連携基盤との連携仕様に関する詳細な内容として、1．3 に記載の資料を提供します。
⑥	連携に向けた詳細検討	事業者	ID 連携基盤との連携仕様に関する詳細な内容を基に、ID 連携基盤との連携に向けて具体的な検討を行います。
⑦	クライアント ID/シークレットの提供依頼	事業者	ID 連携基盤と連携する為のクライアント ID/シークレットの提供を依頼します。
⑧	クライアント ID/シークレットの提供	大阪府	事業者からの求めに応じ、クライアント ID/シークレットを提供します。

2．ID 連携基盤との連携モデル

本章では、連携サービスが ID 連携基盤と連携する際の連携モデルについて概説します。

ID 連携基盤との連携モデルには ID 連携に関するモデル(**＃１：ID フェデレーション**)とデータ連携に関するモデル(**＃２：属性情報取得**)があります。

２．１．モデル＃１：ID フェデレーション

本モデルは、ID 連携基盤が連携サービスに代わり連携サービスの利用者の認証を行うことで連携サービスへのログインが可能になるモデルです。この時、連携サービスの利用者の認証には共通 ID を利用します。

本モデルには、連携サービスが連携サービスの利用者をログイン処理する際に、連携サービスの利用者を識別する方法として表３に記載の a ～ c の３つのパターンがあり、連携サービスの実態に合わせて選択します。

表３．連携サービスの利用者を識別する方法

#	ログイン処理のパターン	識別方法
a	認証のみ(利用者を個別に識別しない)	連携サービスは連携サービス独自の ID を持たず、連携サービスの利用者を個別に識別しない状態で連携サービスにログインすることを想定しています。連携サービスの利用者を個別に識別し、各利用者に異なるサービス内容を提供する場合は b もしくは c のパターンを選択します。
b	共通 ID で識別	連携サービスは共通 ID を連携サービスの ID とする ID テーブルを持ち、連携サービスの利用者を個別に識別できる状態で連携サービスにログインすることを想定しています。
c	連携サービスの ID で識別	連携サービスは連携サービスの ID と共通 ID の ID 紐付けテーブルを持ち、連携サービスの利用者を個別に識別できる状態で連携サービスにログインすることを想定しています。

２．２．モデル＃２：属性情報取得

本モデルは、本人同意の下、連携サービスが ID 連携基盤から ID 連携基盤利用者の属性情報を取得することが可能になるモデルです。

３．ID フェデレーション

本章では、ID フェデレーションモデルの処理の流れを説明します。

図３に、本モデルの、連携サービスにログインする際の処理フローを示します。

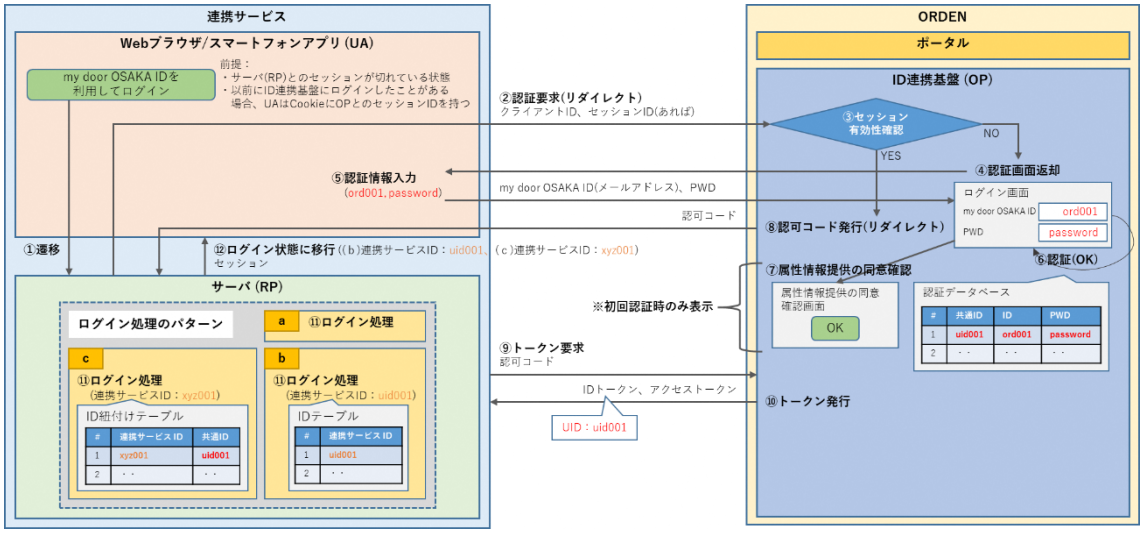

図３．連携サービスにログインする際の処理フロー

処理の前提：

・認証には OpenID Connect の認可コードフローを利用する。
・連携サービスは OP からクライアント ID とクライアントシークレットを取得している。
・OP には ID 連携基盤利用者のアカウントが作成されている。
・UA と RP とのセッションは切れている。
・以前に UA が ID 連携基盤にログインしたことがある場合、UA は Cookie に OP とのセッション ID を持つ。
・ログイン処理(⑪)のパターンが b の場合、RP には共通 ID を連携サービスの ID とする ID テーブルが作成されている。
・ログイン処理(⑪)のパターンが c の場合、RP には連携サービスの ID と共通 ID の ID 紐付けテーブルが作成されている。

処理の流れ：

① 遷移

連携サービスの利用者は UA に用意されているボタン等を押下し、OP に対して認証要求を開始する。

② 認証要求

RP は UA からの認証要求を OP にリダイレクトする。この時、OP から取得しているクライアント ID をリクエストに含める。また、UA が Cookie に OP とのセッション ID を持つ場合は、セッション ID もリクエストに含める。

③ セッション有効性確認

OP は UA からのリクエストにセッション ID が含まれている場合、当該のセッション ID が有効かどうか確認し、有効な場合は⑦の認可コード発行を実施する。当該のセッシ

ョン ID が有効でない場合、もしくはセッション ID 自体が含まれていない場合は④の認証画面返却を実施する。

④ 認証画面返却

OP は UA に認証画面を返却する。

⑤ 認証情報入力

連携サービスの利用者は認証情報として、認証画面に my door OSAKA ID(メールアドレス)と PWD を入力する。

⑥ 認証

OP は連携サービスの利用者に入力された認証情報と認証データベースに格納している情報とを照合する。

⑦ 属性情報提供の同意確認

当該の連携サービスの利用者において ID 連携基盤が連携サービスに代わり連携サービスの利用者の認証を行ったことがない場合、OP は連携サービスの利用者に対し、連携サービスに対する属性情報提供の同意確認画面を表示する。

⑧ 認可コード発行

OP は認証が完了した場合には、リダイレクト先の RP に認可コードを発行する。

連携サービスが連携サービスの利用者をログイン処理する際のパターンが a の場合、連携サービスは連携サービス独自の ID を持たず、連携サービスの利用者を個別に識別しないため、⑧〜⑩の処理を実施せずに⑪以降の処理を実施することが出来ます。

⑨ トークン要求

RP は OP から取得した認可コードを利用し、OP に対してトークンを要求する。

⑩ トークン発行

OP は認可コードが正当であると検証できた場合には、RP に ID トークンとアクセストークンを発行する。

⑪ ログイン処理

パターンが a の場合は、RP は認可コードの取得により認証の完了を把握し、連携サービスのログイン処理を行う(※場合によっては認可コードの発行元の確認や、⑨〜⑩の処理を実施して取得したトークンを検証する等、連携サービスの実態に合わせて選択します)。

パターンが b の場合は、RP は ID トークンに含まれる ID 連携基盤利用者の識別子(UID)と ID テーブルに格納している連携サービスの ID を照合し、連携サービスの利用者を個別に識別できる状態で連携サービスのログイン処理を行う。

パターンが c の場合は、RP は ID トークンに含まれる ID 連携基盤利用者の識別子(UID)をキーに、ID 紐付けテーブルに格納している連携サービスの ID を参照し、連携サービスの利用者を個別に識別できる状態で連携サービスのログイン処理を行う。

⑫　ログイン状態に移行

連携サービスはログイン状態となる。

上記の処理フローは、連携サービスを起点として連携サービスにログインする際に、ID 連携基盤が連携サービスに代わり連携サービスの利用者の認証を行います。上記の他、ポータルを起点として連携サービスを利用する場合の処理の流れを説明します。

図 4 に、ポータルから連携サービスに遷移する際の処理フローを示します。

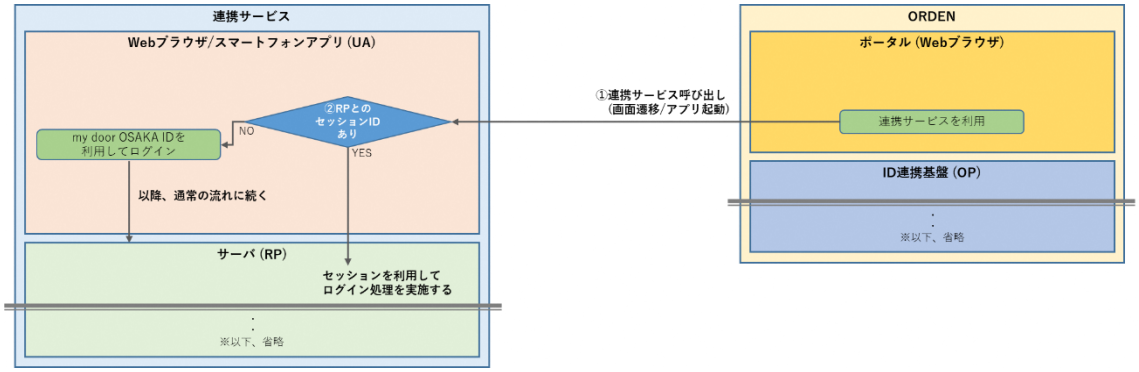

図 4．ポータルを起点とする連携サービスの利用

処理の前提：

・認証には OpenID Connect の認可コードフローを利用する。

・連携サービスは OP からクライアント ID とクライアントシークレットを取得している。

・OP には ID 連携基盤利用者のアカウントが作成されている。

・ID 連携基盤利用者は ID 連携基盤にログインしている。

処理の流れ：

①　連携サービス呼び出し

連携サービスの利用者はポータルに用意されているボタン等を押下し、連携サービスに遷移する。

②　セッション ID 有無確認

UA は RP とのセッション ID を保持しているか確認し、保持している場合は RP にセッション ID を送付する。RP はセッション ID を利用してログイン処理を実施する。結果として、連携サービスをログイン状態から開始することが可能となる。UA が RP とのセッション ID を保持していない場合は、通常の流れと同様に、連携サービスの利用者は UA に用意されているボタン等を押下し、OP に対して認証要求を開始する。

４．属性情報取得

本章では、属性情報取得モデルの処理の流れを説明します。

図５に、本モデルの、連携サービスが ID 連携基盤から属性情報を取得する際の処理フローを示します。

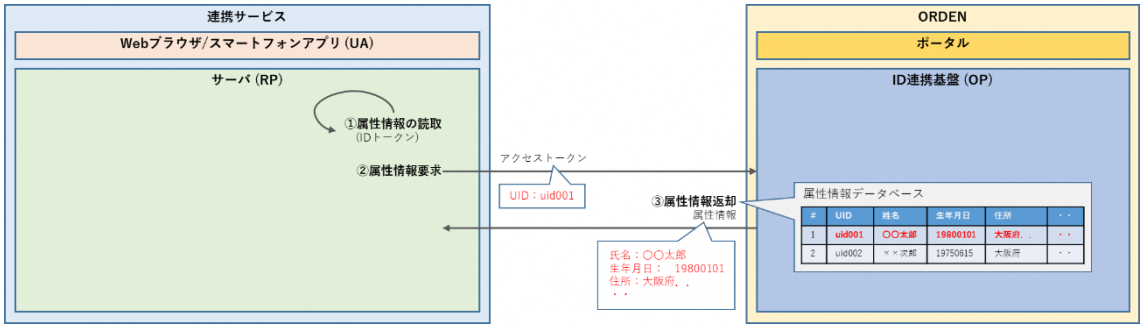

図５．連携サービスが ID 連携基盤から属性情報を取得する際の処理フロー

処理の前提：

・属性情報の読取(①)を実施する前に、RP は OP から ID トークンとアクセストークンを取得している。

処理の流れ：

① 属性情報の読取

RP は OP から取得した ID トークンに含まれる属性情報を読み取る。

ID トークンに属性情報が含まれるため、アクセストークンを利用して属性情報を別途取得する必要はありません。ただし、認証時以降に任意のタイミングで最新の属性情報を確認したい場合は、アクセストークンを利用して②～③の処理を実施することにより属性情報を取得します。

② 属性情報要求

RP は OP から取得したアクセストークンを利用し、OP に対して属性情報を要求する。

③ 属性情報返却

OP は属性情報データベースを参照し、アクセストークンに対応する ID 連携基盤利用者の属性情報を RP に返却する。

表４に、ID 連携基盤から取得可能な主な属性情報を記載します。属性情報の詳細は１．３に挙げている資料に記載しています。

表４．属性情報一覧

#	項目	備考
1	共通 ID	OP が ID 連携基盤利用者に対して発行する ID で、ID 連携基盤利用者を一意に識別する為の ID
2	メールアドレス	
3	連携済み外部 IdP	連携済みの外部 IdP(現在は xID のみが対象)
4	姓	
5	名	
6	姓(カナ)	
7	名(カナ)	
8	電話番号	
9	性別	
10	生年月日	形式：yyyy-MM-dd
11	都道府県	
12	市区町村	政令市の場合、「○○市(区を含まない)」、「○○市○○区(区を含む)」の２パターンを取得可能
13	町名・番地・建物名・部屋番号	政令市の場合、「○○区○○町・・(区を含む)」、「○○町・・(区を含まない)」の２パターンを取得可能
14	鉄道会社名	自宅から利用する鉄道会社名
15	駅名	自宅から利用する駅名
16	通勤・通学先市町村	
17	子供の情報(生年月日)	最大 10 名
18	子供の情報(性別)	同上
19	備考 1	
20	備考 2	
21	備考 3	

５．ID 連携基盤利用者のライフサイクル

本章では、ID 連携基盤利用者のライフサイクルを説明します。

アカウントの作成

基本的に、ID 連携基盤利用者はポータルを起点としてアカウントを作成します。アカウントを作成する際に、ID 連携基盤利用者は氏名や住所等の属性情報を入力します。

属性情報の修正

アカウントを作成する際に入力した属性情報は、ID 連携基盤が用意する画面上で、ID 連携基盤利用者自身で修正することが出来ます。連携サービスは ID 連携基盤から属性情報を再度取得することで、修正された属性情報を確認することが出来ます。

アカウントの削除

アカウントはポータルを起点として削除されます。ID 連携基盤利用者はポータルの画面上でアカウントを削除するための操作を実施します。アカウントが削除されると、ID 連携基盤利用者は当該アカウントを利用して連携サービスにログインできなくなります。

6．補足事項

表 5 に、ID 連携仕様に関する補足事項の一覧を記載します。

表 5．補足事項

#	項目	説明
1	アクセストークンの有効期限	アクセストークンの有効期限は 1 時間です。リフレッシュトークンで延長可能です。リフレッシュトークンの有効期限は 90 日です。
2	属性情報の修正内容が反映されるタイミング	属性情報が修正された際は、ID 連携基盤から取得可能な属性情報に修正内容が直ぐに反映されます。

7．本紙の利用条件

・本紙の著作権は本府に帰属します。
・本紙の内容は予告なしに変更することがあります。
・本府は、本紙に掲載する情報について、その内容の完全性、正確性、有用性、安全性等の、いかなる保証も行いません。
・本紙に掲載されている情報に基づいて利用者が下した判断及び起こした行動により起因又は関連していかなる結果が発生した場合においても、本府はその責任を負いません。

8．問い合わせ先

本紙に関するお問い合わせ先は下記のとおりです。

・大阪府スマートシティ戦略部戦略推進室戦略企画課

・メール：senryaku-js@gbox.pref.osaka.lg.jp
・電話番号：06-6945-9067

変更履歴

#	版	該当箇所	変更内容	変更者	確認日	備考
1	1.0	−	新規作成	NTT-BS	2023/03/31	
2	2.0	1.3 参考資料 4 表 4	参考資料を MAB 版に更新 表 4 属性情報を R5 版に更新	NTT-BS	2023/12/18	
3	2.1	4 表 4	表 4 属性情報を更新	NTT-BS	2024/01/15	
4	2.2	1.1 1.2 1.3 1.4 2 2.1 2.2 3 4 5	ORDEN を ORDEN の ID 連携基盤、または ID 連携基盤に修正 ORDEN ID を共通 ID に修正 図 1 の修正 表 1 の修正 ORDEN を ID 連携基盤に修正 表 2 の修正 ORDEN を ID 連携基盤に修正 ORDEN を ID 連携基盤に修正 ORDEN を ID 連携基盤に修正 ORDEN ID を共通 ID に修正 表 3 の修正 ORDEN を ID 連携基盤に修正 ORDEN ユーザを ID 連携基盤利用者に修正 図 3 の修正 ORDEN を ID 連携基盤に修正 ORDEN ID を共通 ID に修正 図 4 の修正 ORDEN ユーザを ID 連携基盤利用者に修正 ORDEN を ID 連携基盤に修正 表 4 の修正 図 5 の修正 ORDEN ユーザを ID 連携基盤利用者に修正 ORDEN ID を ID 連携基盤利用者に修正 ORDEN ID をアカウントに修正	NTT-BS	2024/10/27	

			ORDEN を ID 連携基盤に修正 表 5 の修正			
5	2.3	xx	表 4 の#12、13 を修正	NTT-BS	2025/03/21	
6						
7						
8						
9						
10						