産業用データ連携基盤
基本設計書
認証・認可

第1.0版

変更来歴

#	版数	発行年月日	変更内容
1	0.9	2023/11/14	・CADDEを活用して、産業データ連携基盤を開発するにあたり版数0.9として作成 ・CADDEからDATA-EXに文言を修正 ・クライアント認証方式をクライアントID、シークレットから、クライアントID、クライアント証明書に変更 ・運用管理者を運営事業者に修正 ・外部IdP連携については、連携概要としては記載しているが非対応
2	1.0	2024/3/21	・基盤名称「DATA-EX」を「産業用データ連携基盤」に変更 ・「利用者」(データ利用者/利用者コネクタ等)を「受領者」に変更

用語集

#	用語	略号	説明
1	認証・認可	__	産業用データ連携基盤における認証と認可に関する仕組みの総称
2	認証	__	DATA-EXユーザIDとパスワードを照合することによって、産業用データ連携基盤におけるDATA-EXユーザの真正性を確認すること
3	認証機能	__	産業用データ連携基盤が支援サービス群として保有する、認証のための機能
4	認証トークン	__	産業用データ連携基盤における、認証機能が発行するアクセストークンに対するラベル名
5	認可	__	データ提供者が自身の持つカタログやデータに対して、誰にアクセスを許可するかを設定すること
6	認可機能	__	各データ提供者が保有する、認可のための機能
7	認可トークン	__	産業用データ連携基盤における、認可機能が発行するアクセストークンに対するラベル名
8	認可情報	__	認可をするために必要な情報のこと（カタログやデータの識別子、条件など）
9	認可確認	__	カタログやデータにアクセス要求があった際に、認可を確認して提供可否を決定すること
10	DATA-EXユーザID	__	産業用データ連携基盤を利用する際に必要となるDATA-EXのユーザID
11	DATA-EXユーザID(受領者)	__	本設計書上でユーザがデータ受領者としてふるまっていることを強調するときのDATA-EXユーザIDの表記
12	DATA-EXユーザID(提供者)	__	本設計書上でユーザがデータ提供者としてふるまっていることを強調するときのDATA-EXユーザIDの表記
13	認可コード	__	OAuth2.0認可コードグラントを用いてトークンを取得する際に、内部的に用いられる短命トークンのこと

用語集(一般)

#	用語	略号	説明
1	ユーザ	—	システムを利用する主体のこと
2	ID	—	ユーザなどを一意に特定するための識別子
3	アクター	—	ユーザがシステムに対して果たす役割のこと
4	クライアント	—	サーバに要求を送信するアプリケーションのこと 本書では、アプリケーションは認証機能で認証される必要があるため、クライアントは認証機能に登録されているアプリケーションという意味合いを含んでいる
5	認証	—	人やアプリケーションなどの真正性を確認すること 人を認証することはユーザ認証、アプリケーションを認証することはクライアント認証と表現することがある
6	認可	—	アクセス制御のためのアクセスポリシーを定義すること
7	JSON Web Token	JWT	RFC7519で定められたトークンの仕様。読み方はジョット JWTの例としては、アクセストークン(OAuth2.0)、IDトークン(OpenID Connect)などがある
8	クレーム	—	JWTが保持している情報のこと JWTをデコードすることやトークンイントロスペクションに成功することでクレームを確認できる。
9	Bearerトークン	—	Bearerとは持参者を意味し、切符のように所有しているだけでアクセス権限を持つトークン
10	Proof of possessionトークン	—	Bearerトークンとは異なり、持参と同時に所持証明も必要とするトークン Bearerトークンとの対比のため本説明を記載するが、未使用
11	アイデンティティプロバイダ	IdP	認証情報を提供するもの Googleなどのソーシャルネットワークサービスで提供されていることが多い
12	OAuth2.0	—	RFC6749で定められている認可のプロトコル Resource OwnerがResource Serverにある自身のリソースにアクセスするための方法を定めている OAuth1.0とOAuth2.0では仕様に乖離があるため、OAuth2.0とバージョンを明記することが多い アクセストークンを定義している
13	OpenID Connect	OIDC	認証と認可のプロトコル 認可のプロトコルであるOAuth2.0に認証の要素を追加し拡張したプロトコル IDトークンを定義している
14	User-Managed Access	UMA	OAtuth2.0を基にしたプロトコル OAuth2.0に対して、Resource Ownerが第三者へリソースへのアクセスを許可するユースケースに関する拡張が行われている
15	Attribute-Based Access Control	ABAC	属性によってアクセス制御を行う方式
16	Keycloak	—	認証と認可に関するオープンソースソフトウェア アイデンティティプロバイダとしてや、認可サーバとしての機能を提供する
17	Identity Assurance Level	IAL	身元確認の厳密さや強度を示すレベル
18	Authenticator Assurance Level	AAL	当人認証プロセスの強度を示すレベル
19	Trusted Platform Module	TPM	ハードウェア耐タンパー性を持つセキュリティチップ

用語集(OAuth2.0)

#	用語	略号	説明
1	アクセストークン (Access Token)	—	OAuth2.0で定義されたトークン
2	認可コード (Authorization Code)	—	認可コードグラントの処理過程で内部的に利用される短命のトークン
3	リソースオーナー (Resource Owner)	—	OAuth2.0で定義された4つのロールのうちのひとつ リソースサーバに自身のリソースを持っている
4	クライアント (Client)	—	OAuth2.0で定義された4つのロールのうちのひとつ 認可機能からアクセストークンを取得し、リソースサーバにアクセスするサードパーティーアプリケーション
5	リソースサーバ (Resource Server)	—	OAuth2.0で定義された4つのロールのうちのひとつ リソースオーナーのリソースを保持しているサーバ
6	認可サーバ (Authorization Server)	—	OAuth2.0で定義された4つのロールのうちのひとつ アクセストークンの発行や検証を提供する
7	クライアントID	—	認可サーバに対してリクエストするアプリケーションのID クライアント認証に必要となるときがある 認可サーバに登録されたクライアントやリソースサーバといったアプリケーションを一意に識別する
8	認可コードグラント (Authorization Code Grant)	—	OAuth2.0で定義されたアクセストークンを発行するための4つのグラントタイプのうちのひとつ
9	認可コード	—	認可コードグラントで利用される、アクセストークンを取得するために必要な短命のトークン
10	インプリシットグラント (Implicit Grant)	—	OAuth2.0で定義されたアクセストークンを発行するための4つのグラントタイプのうちのひとつ
11	リソースオーナーパスワードクレデンシャルズグラント (Resource Owner Password Credentials Grant)	—	OAuth2.0で定義されたアクセストークンを発行するための4つのグラントタイプのうちのひとつ
12	クライアントクレデンシャルズグラント (Client Credentials Grant)	—	OAuth2.0で定義されたアクセストークンを発行するための4つのグラントタイプのうちのひとつ
13	トークンエンドポイント	—	認可機能が具備するトークン発行を受け付けるためのエンドポイント
14	トークンイントロスペクションエンドポイント	—	認可機能が具備するトークンイントロスペクションを受け付けるためのエンドポイント
15	トークンイントロスペクション (Token Introspection)	—	クライアントからリソースサーバに送られてきたアクセストークンが有効かどうかを、リソースサーバが認可機能に確認すること アクセストークンが有効だった場合は、アクセストークンのデコードされたPayload部が得られる 本設計書では、トークン検証と表現することがある
16	トークンエクスチェンジ (Token Exchange)	—	RFC8693で定義された、なりすましや委任に関してOAuth2.0を拡張するための仕様 既存のアクセストークンをSubject Tokenとして認可機能に渡すことで新規のアクセストークンを得る 本設計書では、トークン交換と表現することがある

用語集(User-Managed Access)

#	用語	略号	説明
1	Protection API	__	UMAにおいて、Authorization Serverが具備するAPI
2	Protection API Token	PAT	Protection APIにアクセスするためのアクセストークン
3	Requesting Party	RP	UMAによって拡張された、リソースアクセスを行う、Resource Ownerではない第三者のこと
4	Requesting Party Token	RPT	UMAで定められているトークンの仕様 認可確認が成功した際に得られるトークンで、認可情報が入っている 認可情報以外のクレームについてはアクセストークンと同様

用語集(OpenID Connect)

OpenID ConnectはOAuth2.0を包含するため、用語集(OAuth2.0)も参照のこと。
以下はOpenID Connectに特有のものを示す。本書では、OpenID Connectといった場合、OpenID Connect 1.0のことを指す。

#	用語	略号	説明
1	IDトークン	__	OpenID Connectで定義されたトークン
2	UserInfoエンドポイント	__	OpenID Connectで定義されたエンドポイント ユーザの情報を取得する
3	End-User	__	OAuth2.0のResource Ownerに相当
4	Requesting Party	RP	OAuth2.0のClientに相当
5	OpenID Provider	OP	OAuth2.0のAuthorization Serverに相当

用語集(Keycloak)

#	用語	略号	説明
1	レルム	—	Keycloakの設定単位 ユーザやクライアントなど様々な設定を内包する
2	ユーザ	—	Keycloakが保管しているユーザの情報 Keycloakはユーザの情報を保持しているため、ユーザ認証をすることができる 例えば、ユーザ名、パスワード、属性などをユーザ情報として持つ
3	クライアント	—	Keycloakに対してリクエストするアプリケーションの情報 Keycloakはクライアントの情報を保持しているため、クライアント認証をすることができる 登録されたクライアントは、クライアント(OAuth2.0)やリソースサーバ(OAuth2.0)としての役割を持つ クライアントタイプとして、Confidentialクライアント、Publicクライアント、Bearer-onlyクライアントがある
4	Authorization Services	—	OAuth2.0やUMAをベースとした、リソース、ポリシー、パーミッションなどを設定することによって細やかなアクセス制御を提供するためのKeycloakの機能
5	リソース	—	Authorization Servicesの概念 アクセス制御の対象となるリソース
6	ポリシー	—	Authorization Servicesの概念 アクセス制御をする際のアクセスポリシー
7	パーミッション	—	Authorization Servicesの概念 リソースとポリシーの組で認可を表現するもの

目次

1. 概要

認証の目的

産業用データ連携基盤では、DATA-EXに登録されているユーザであるかの真正性の確認が必要であるため、その仕組み（認証）を具備する。
そして、認証済みのユーザに産業用データ連携基盤の利用およびデータアクセスを許可するためのアクセス制御の仕組みを具備する。

認可の目的

産業用データ連携基盤では、データ提供者が自身のカタログやデータを、特定のデータ受領者にのみ提供することが必要であり、その仕組み（認可）を具備する。

1. 概要 > 1.2. 要件 > 1.2.1. 認証・認可の要件

認証・認可の要件は以下の通り。

#	目的（ユースケース、業務要件）	システム要件	関連する業務
1	ユーザの身元確認や適格性評価をして、産業用データ連携基盤を利用するために、ユーザを登録することができる	産業用データ連携基盤を利用するユーザを一意に識別するためのDATA-EXユーザIDを発行することができる 認証機能にユーザ情報を保管することができる	利用準備
2	産業用データ連携基盤を利用するユーザの真正性を確認することができる	認証機能がユーザのクレデンシャルを照合することによって利用を要求しているユーザの真正性を確認することができる また、認証機能は外部IdP(*1)と連携して利用を要求しているユーザの真正性を確認することもできる	データ提供 データ発見 データ取得・連携
3	登録されたDATA-EXユーザだけに本システムの利用を制限することができる	各アプリケーションが認証機能に問い合わせることによって、アクセス可否を確認することができる	データ提供 データ発見
4	ユーザの属性に基づいたデータ提供可否を設定することができる	ユーザが自身の保有するカタログやデータのアクセスに対して認可を与えられる仕組みを持つ ここで、データ提供者としてのユーザは以下のような認可の与え方ができる ① ユーザを指定して認可を与えることができる ② 組織を指定して一度に多数のユーザ(組織・組織内個人)に認可を与えることができる ③ ユーザの当人認証レベルを指定して認可を与えることができる ④ 契約(*2)にもとづいた①～③を行うことができる	データ提供
5	ユーザの属性に基づいたデータ提供可否を決定することができる	ユーザがカタログやデータにアクセスした際に、認可を確認して提供可否を判断することができる	データ発見 データ取得・連携

*1: 外部IdPとは本システム外の一般のサービスで提供されている、ユーザの認証情報を提供するサービスである。
詳細については「2. 方式 > 2.1. 認証方式 > 2.1.3. 外部IdP」に記載。

*2: 契約とはデータ提供の公開範囲を限定できる仕組みであり、あらかじめ提供者・受領者間で行われる契約である。
詳細については「1. 概要 > 1.3. 業務フロー > 1.3.8. 認可情報登録（限定提供データ（契約有））」に記載。

認証の対象を以下に示す。

#	認証の対象	説明
1	ユーザ	産業用データ連携基盤を利用するためには、あらかじめ産業用データ連携基盤の利用申請をする必要がある 産業用データ連携基盤のユーザは、「DATA-EXユーザID」で識別される

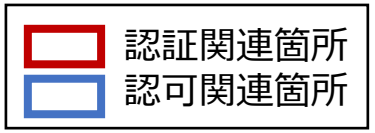
認可の対象（アクセス制御される対象）を以下に示す。

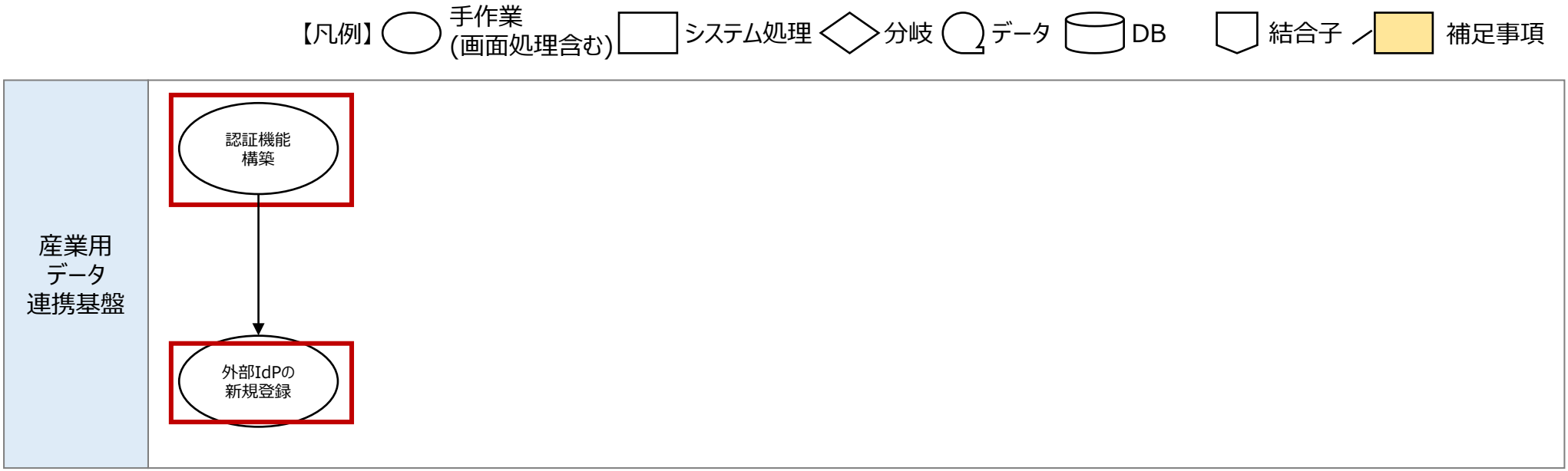
#	認可の対象（アクセス制御される対象）	説明
1	提供者内CKANのURL （データ提供者が保有するカタログ全体）	ユーザがデータ受領者としてデータ発見（提供者内カタログ検索）時に認可確認する
2	データ提供者が提供する各データのURL （データ提供者が提供する個々のデータ）	ユーザがデータ受領者としてデータ取得時に認可確認する

認証・認可に関連する業務フローの一覧を以下に示す。

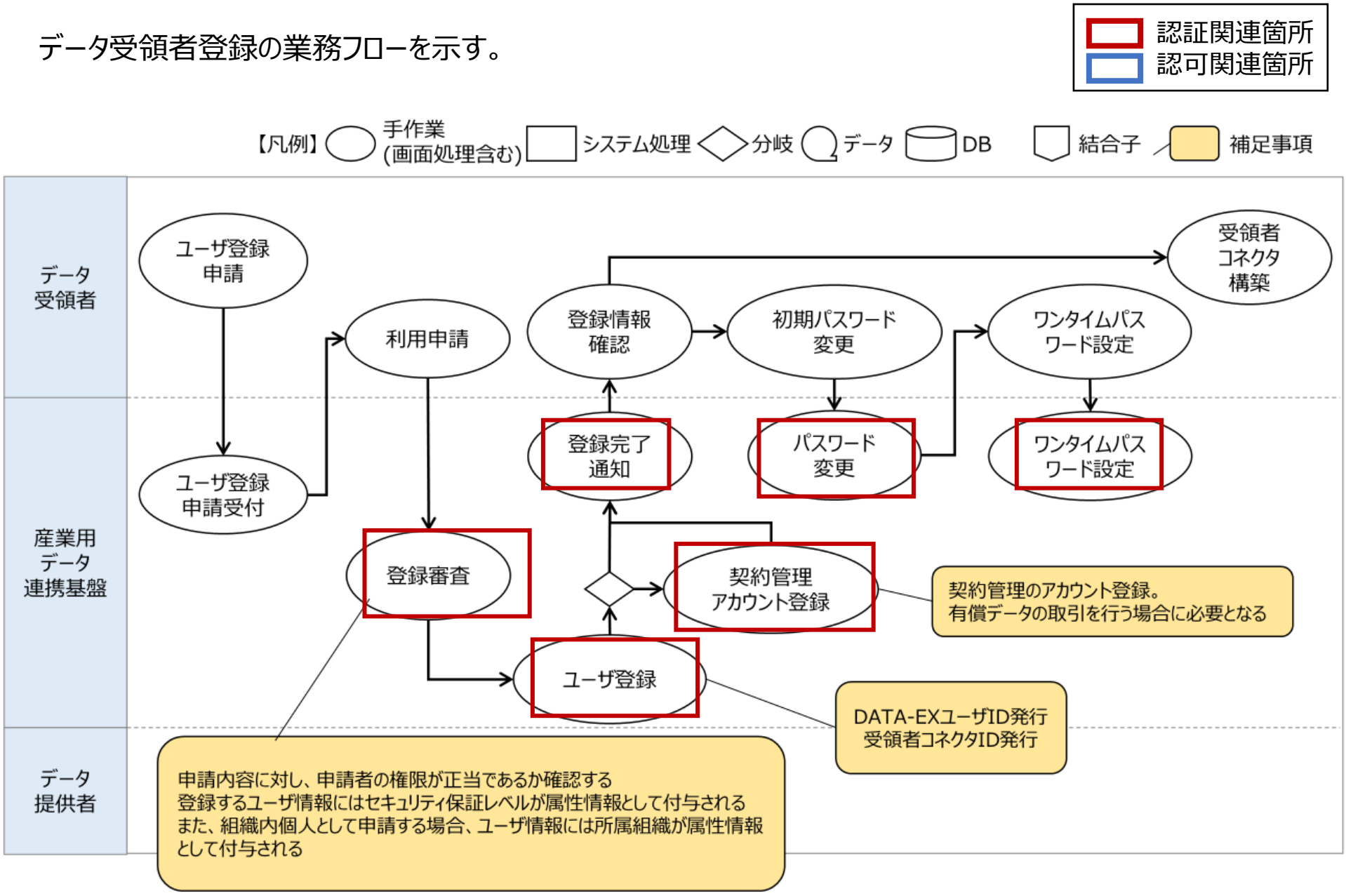
#	業務フロー	概要
1	認証機能運用開始	運営事業者が認証機能を運用開始する
2	認可機能運用開始	データ提供者が認可機能を運用開始する
3	データ受領者登録	申請を受けて運営事業者がデータ受領者を登録する
4	データ提供者登録	申請を受けて運営事業者がデータ提供者を登録する
5	ユーザ情報更新	申請を受けて運営事業者がユーザ情報を更新する
6	提供データの準備	データ提供者が提供データを準備する
7	認可情報登録（限定提供データ（契約無））	限定提供データ（契約無）に対して、データ提供者が認可情報登録する
8	認可情報登録（限定提供データ（契約有））	限定提供データ（契約有）に対して、データ取引市場が契約に基づいて認可情報登録する
9	データ発見時認可確認（限定提供データ（契約無））	限定提供データ（契約無）に対して、データ受領者がデータ発見時に認可確認する
10	データ取得時認可確認（限定提供データ（契約無））	限定提供データ（契約無）に対して、データ受領者がデータ取得時に認可確認する
11	データ取得時認可確認（限定提供データ（契約有））	限定提供データ（契約有）に対して、データ受領者がデータ取得時に認可確認する

認証機能運用開始の業務フローを示す。

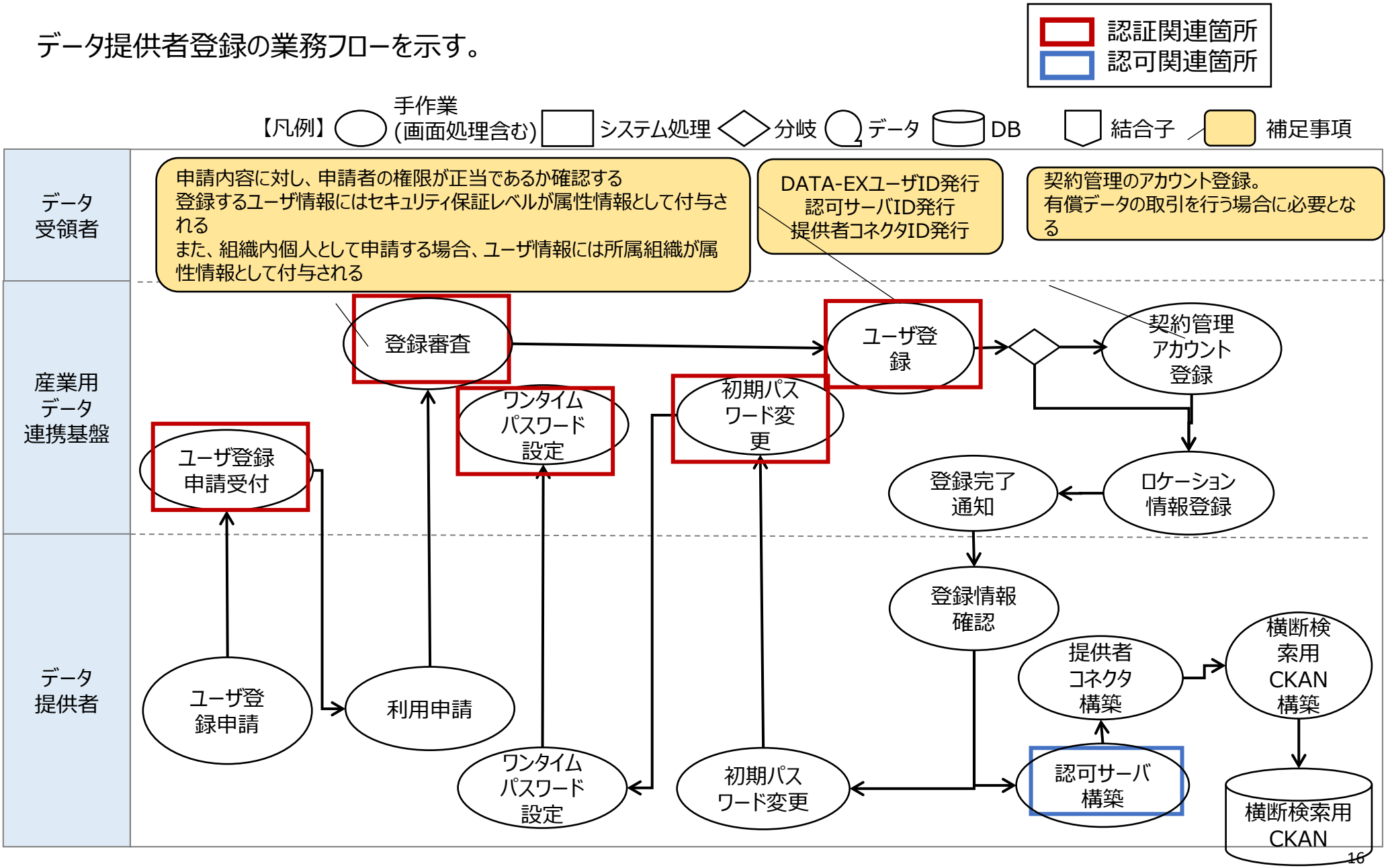




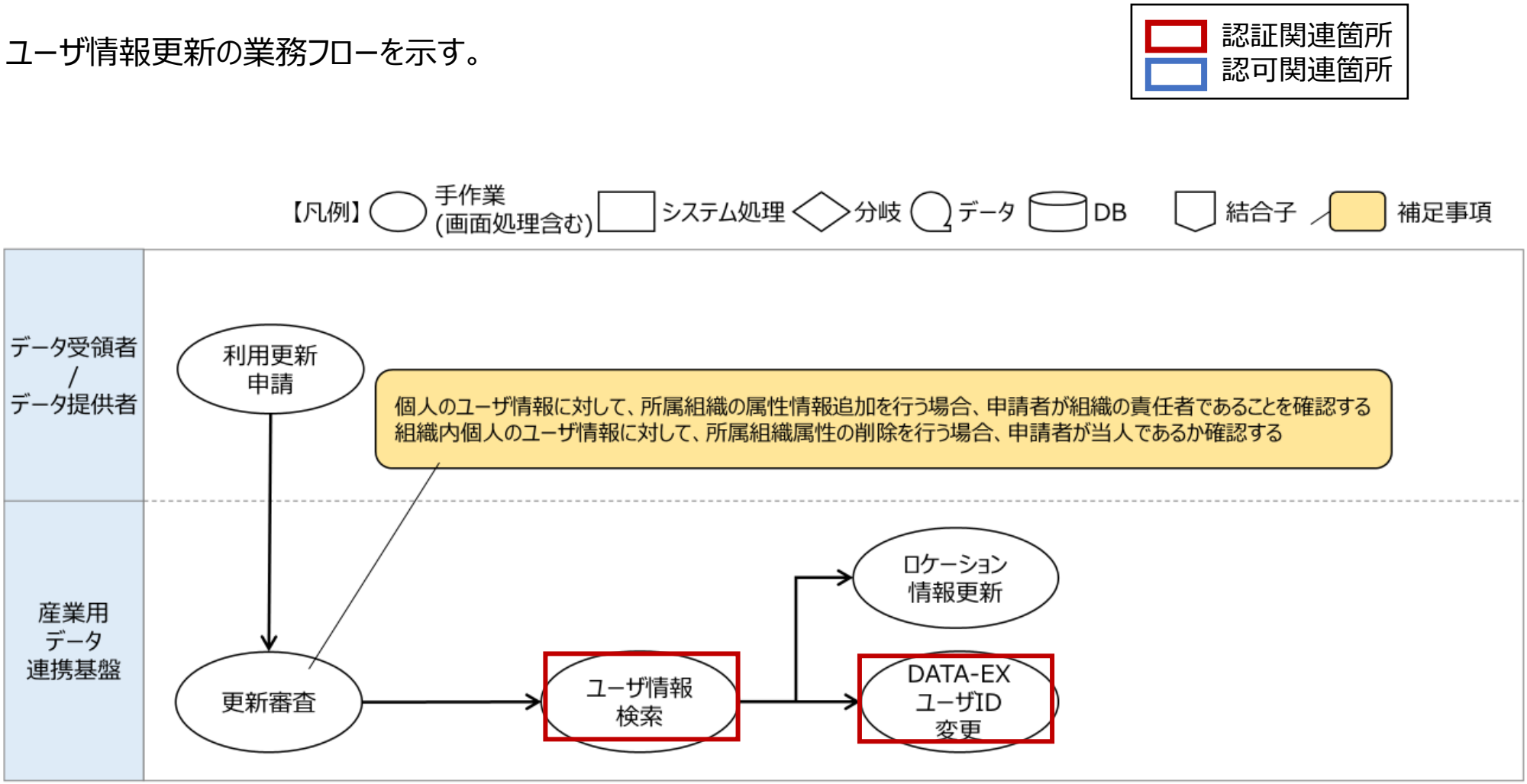
データ受領者登録の業務フローを示す。



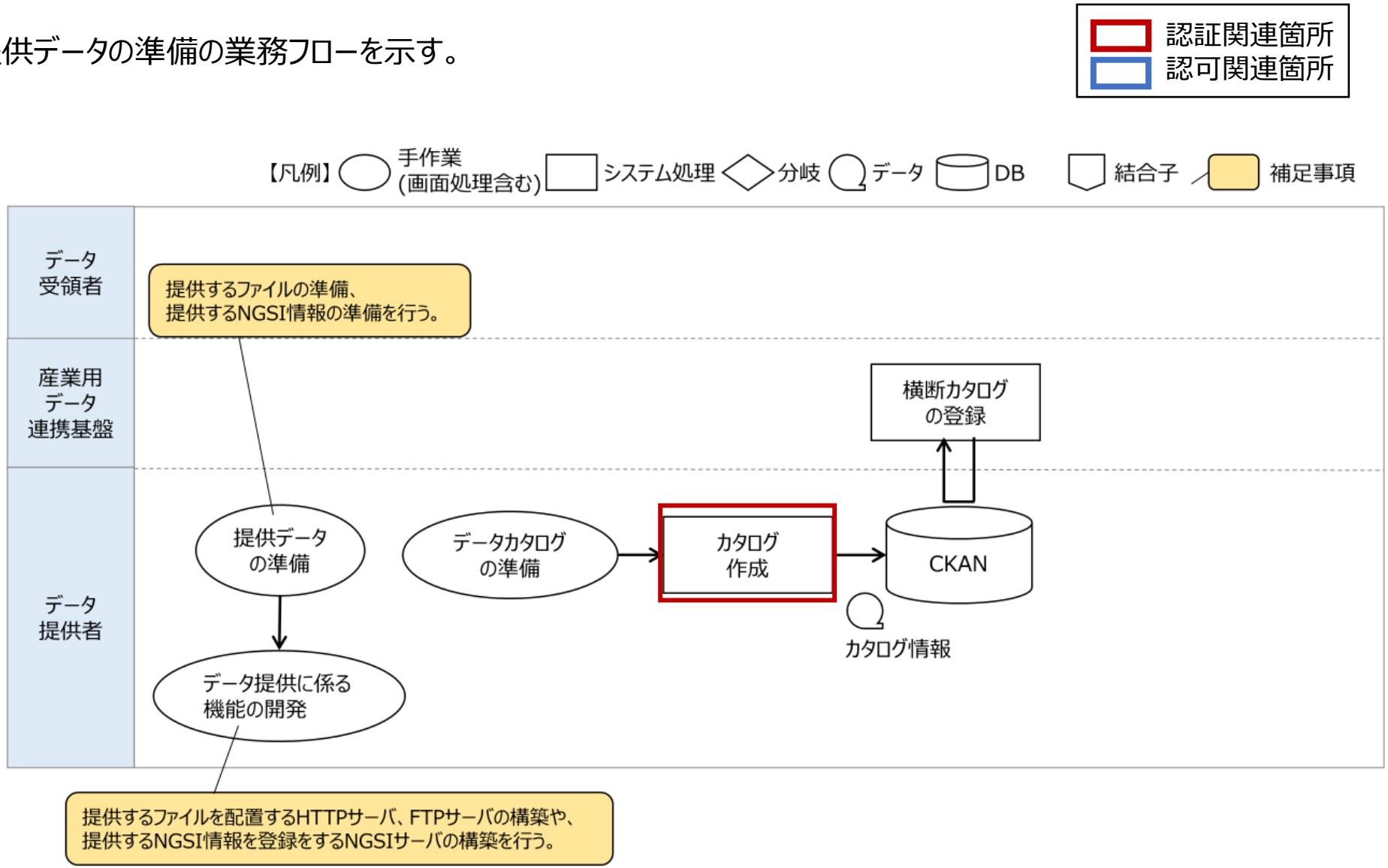
データ提供者登録の業務フローを示す。



ユーザ情報更新の業務フローを示す。

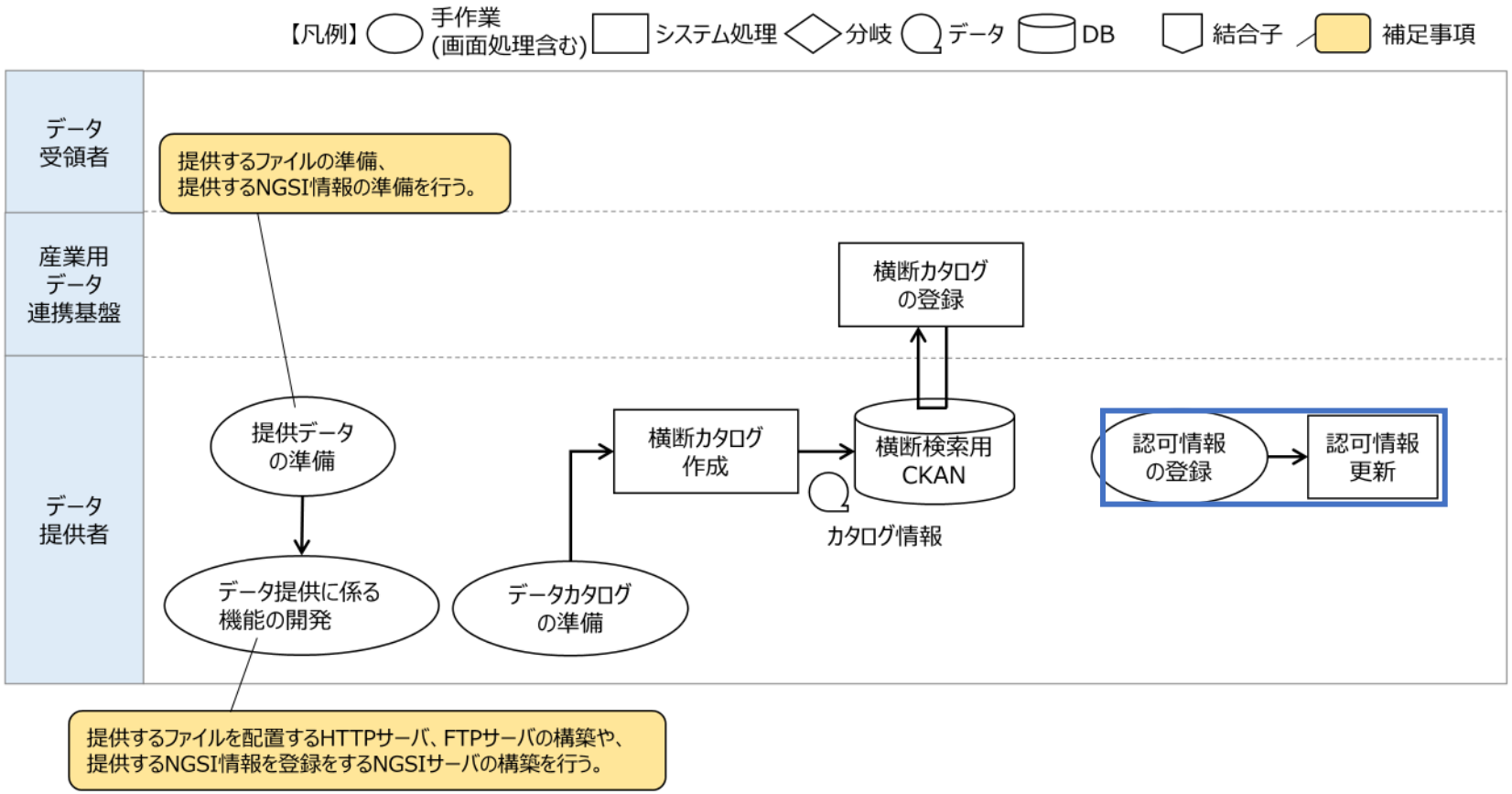


提供データの準備の業務フローを示す。

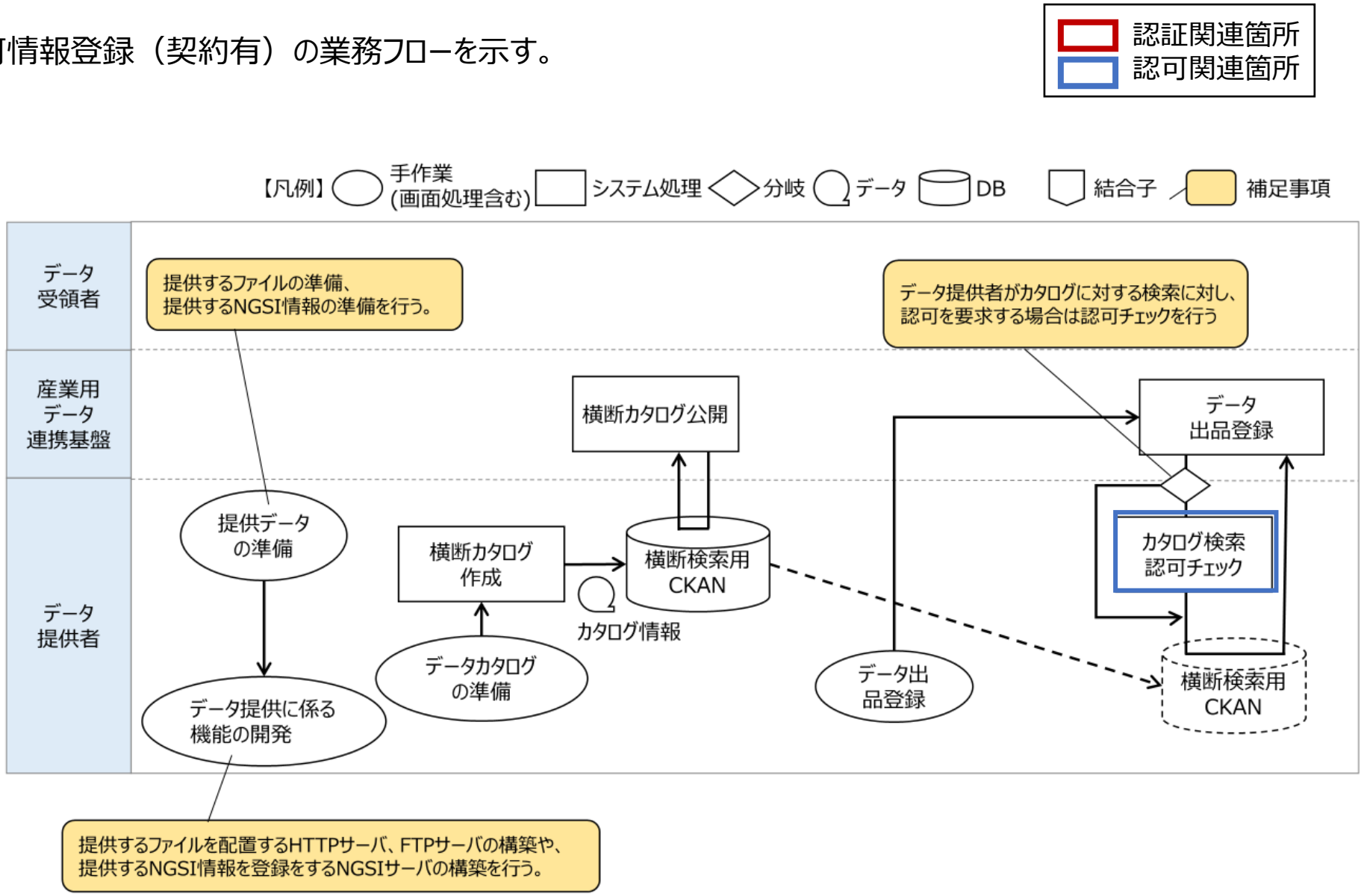


認可情報登録（契約無）の業務フローを示す。

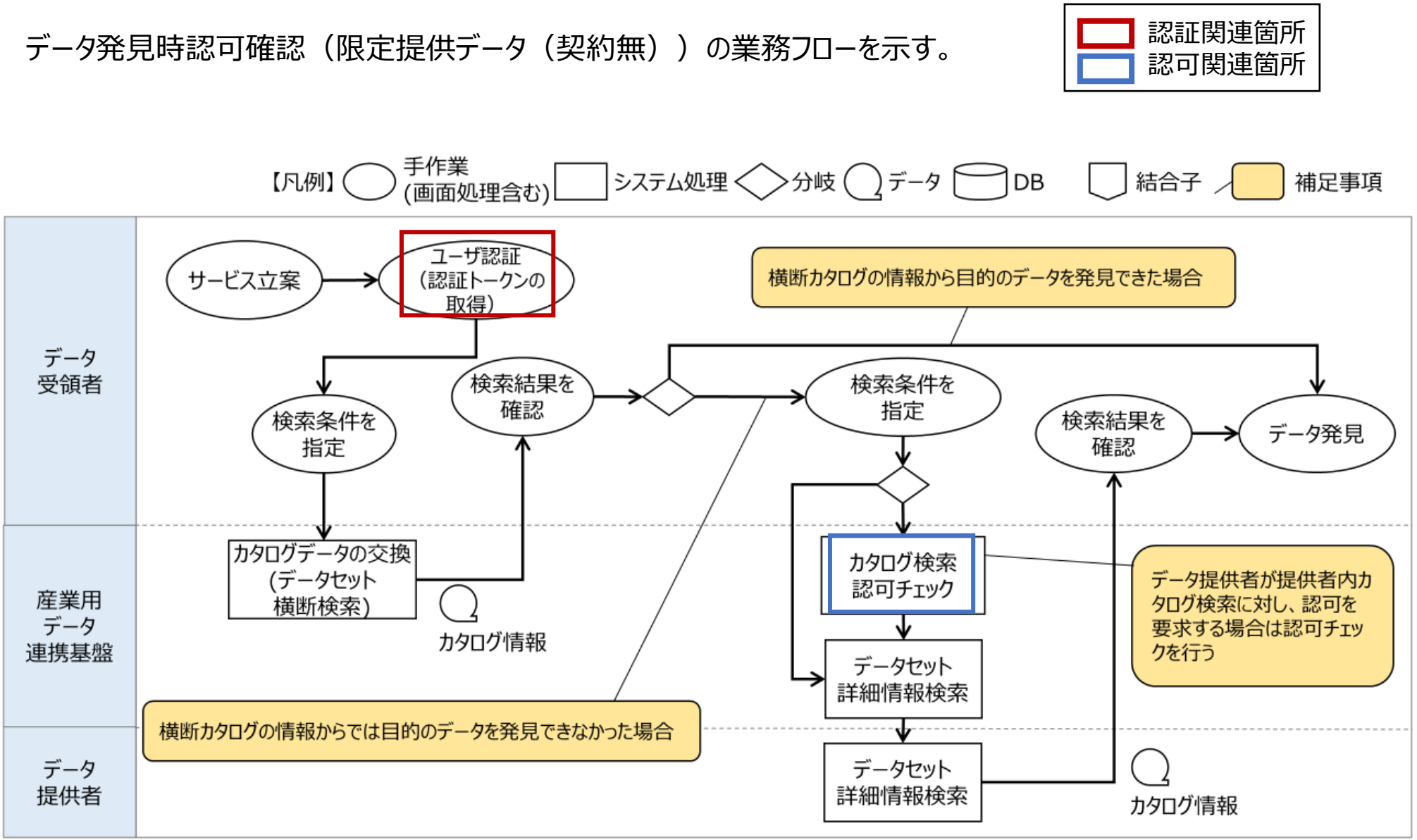
認証関連箇所
認可関連箇所



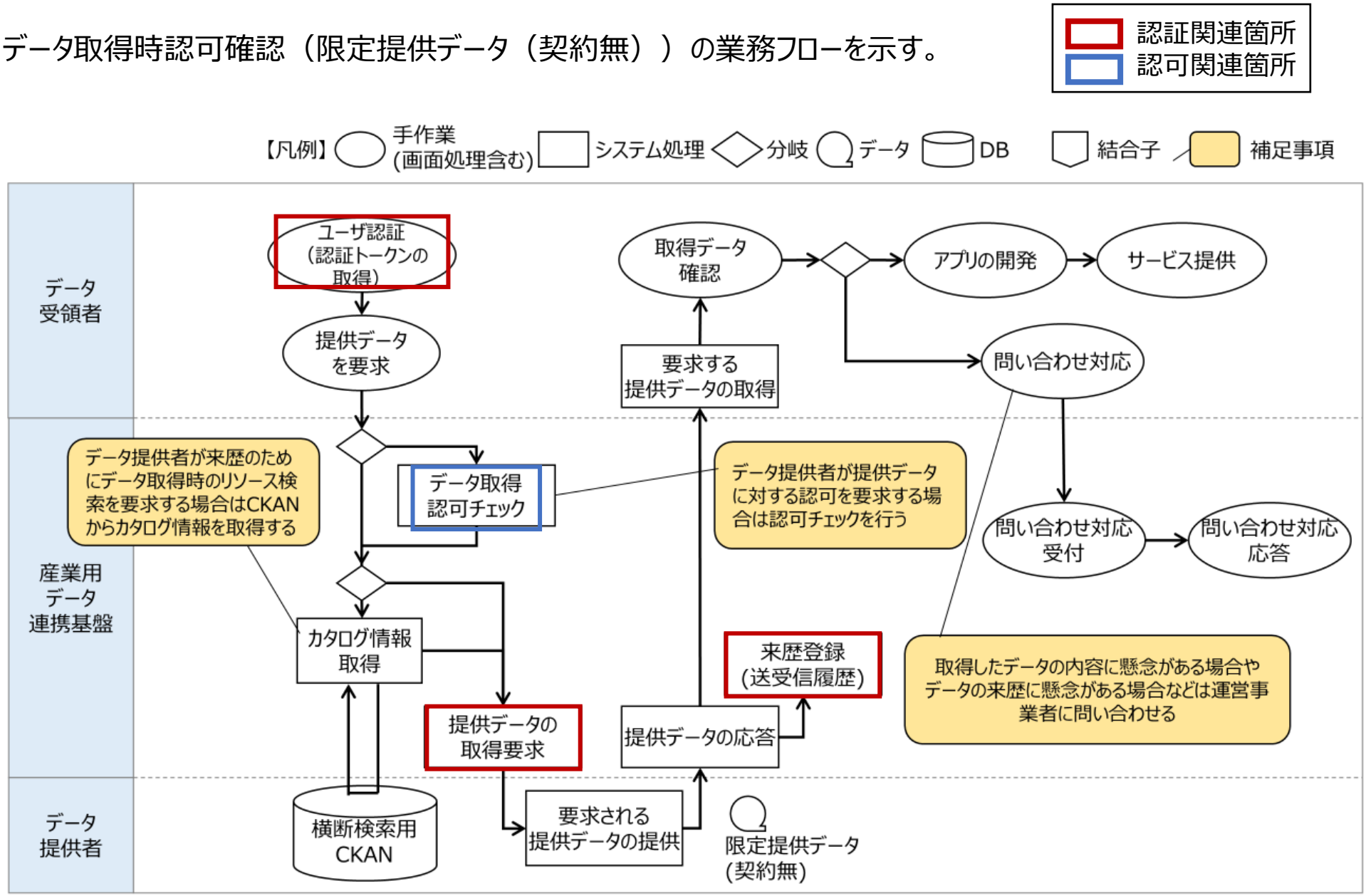
認可情報登録（契約有）の業務フローを示す。



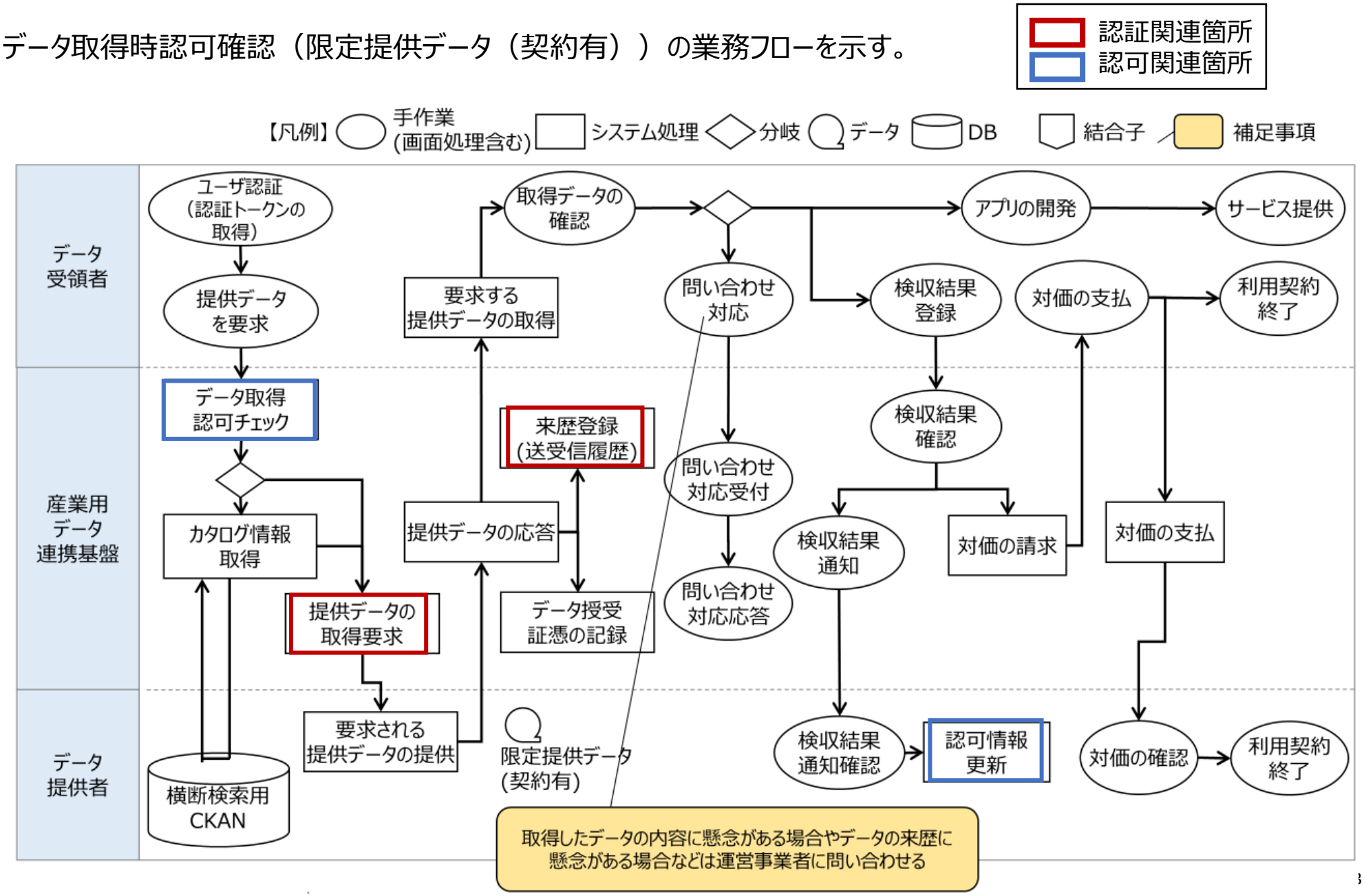
データ発見時認可確認（限定提供データ（契約無））の業務フローを示す。



データ取得時認可確認（限定提供データ（契約無））の業務フローを示す。



データ取得時認可確認（限定提供データ（契約有））の業務フローを示す。



2. 方式

2. 方式 > 2.1. 認証方式 > 2.1.1. 概要

産業用データ連携基盤では知識と所有による認証に対応している。

#	認証要素	産業用データ連携基盤の対応該否	説明
1	知識	DATA-EXユーザIDとパスワード	・初期パスワードはユーザ利用申請時に、産業用データ連携基盤から払い出される。 ・パスワード更新は各ユーザがそれぞれのタイミングで行う。
2	所有	・ワンタイムパスワード ・クライアント証明書	・ユーザは初回利用時にワンタイムパスワード利用のため、スマートフォン用アプリの設定をすることが必要である。対応しているスマートフォン用アプリは、FreeOTPとGoogle Authenticatorである。 ・クライアント証明書は耐タンパデバイス秘密鍵を利用する。
3	生体	非対応	__

産業用データ連携基盤ではアプリケーションの種類によって認証方法が異なる。各アプリケーションの認証方法は以下の通り。

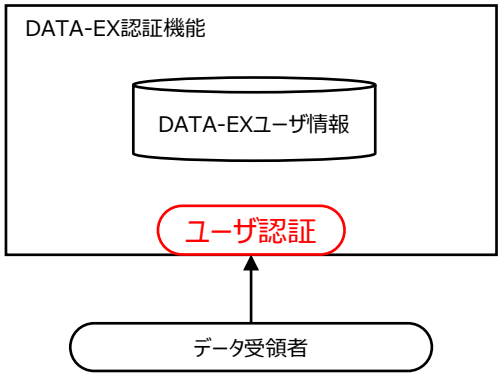
#	認証するアプリケーション	認証方法
1	ユーザ利用アプリケーション （WebApp、データカタログ作成ツール、認可機能）	以下の2要素によって認証する ・DATA-EXユーザIDとパスワード（知識要素） ・ワンタイムパスワード（所有要素）
2	自動処理用アプリケーション等	以下の1要素によって認証する 耐タンパデバイス秘密鍵を用いたクライアント証明書によって認証する（所有要素）

ユーザ利用アプリケーションについては以下の通り。

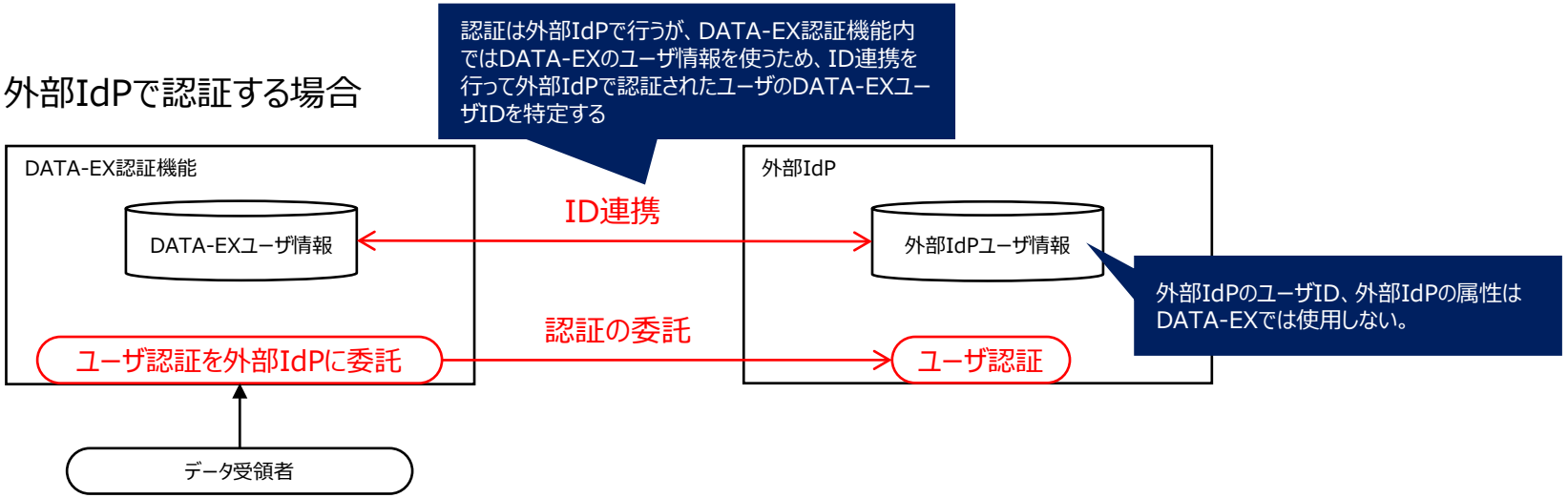
#	ユーザ利用アプリケーション	ユーザ	対応するIdP	関連する業務
1	WebApp	データ受領者	DATA-EX認証機能、外部IdP	データ発見、データ取得・連携、来歴確認
2	データカタログ作成ツール	データ提供者	DATA-EX認証機能	データ提供準備
3	認可機能	データ提供者	DATA-EX認証機能	データ提供準備

データ受領者は次の①、②から認証先を選択することができる
① DATA-EX認証機能
② 外部IdP

① DATA-EX認証機能で認証する場合

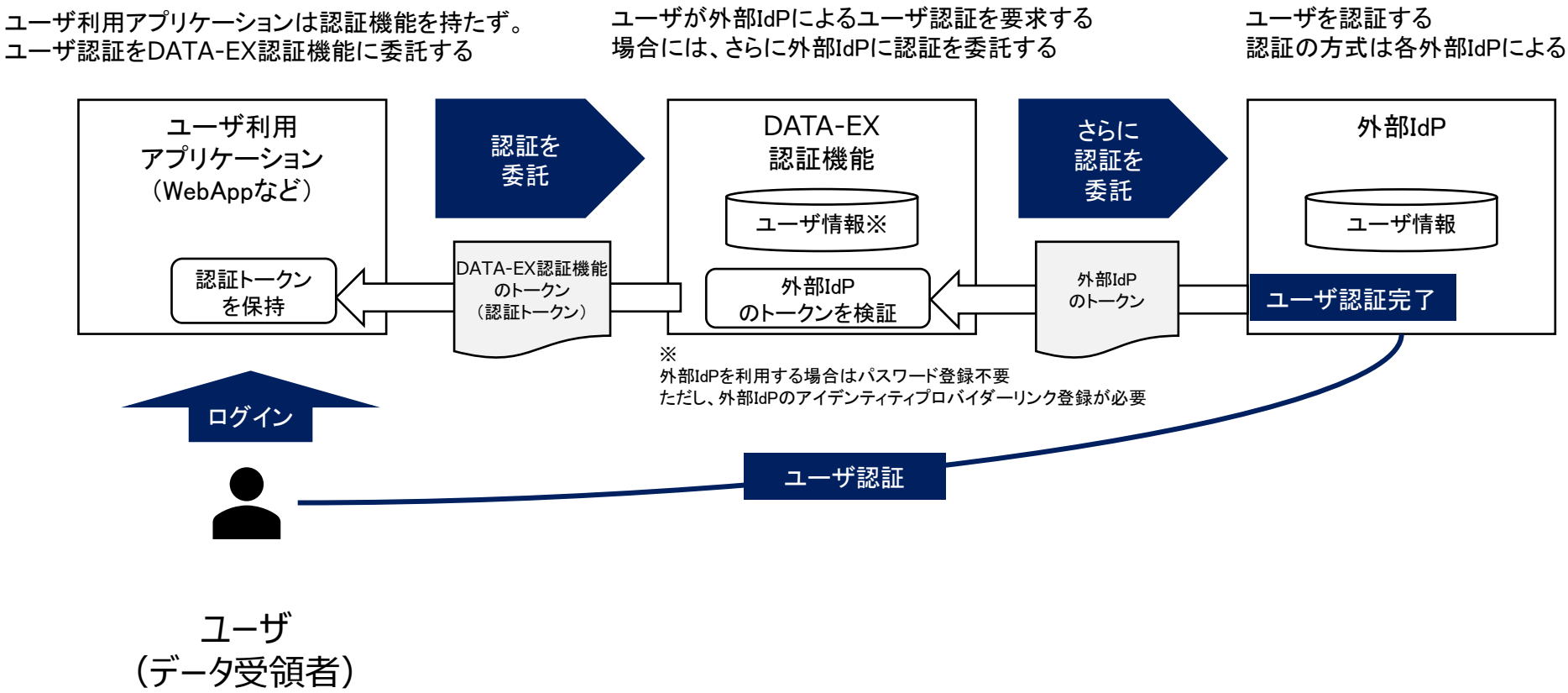


② 外部IdPで認証する場合



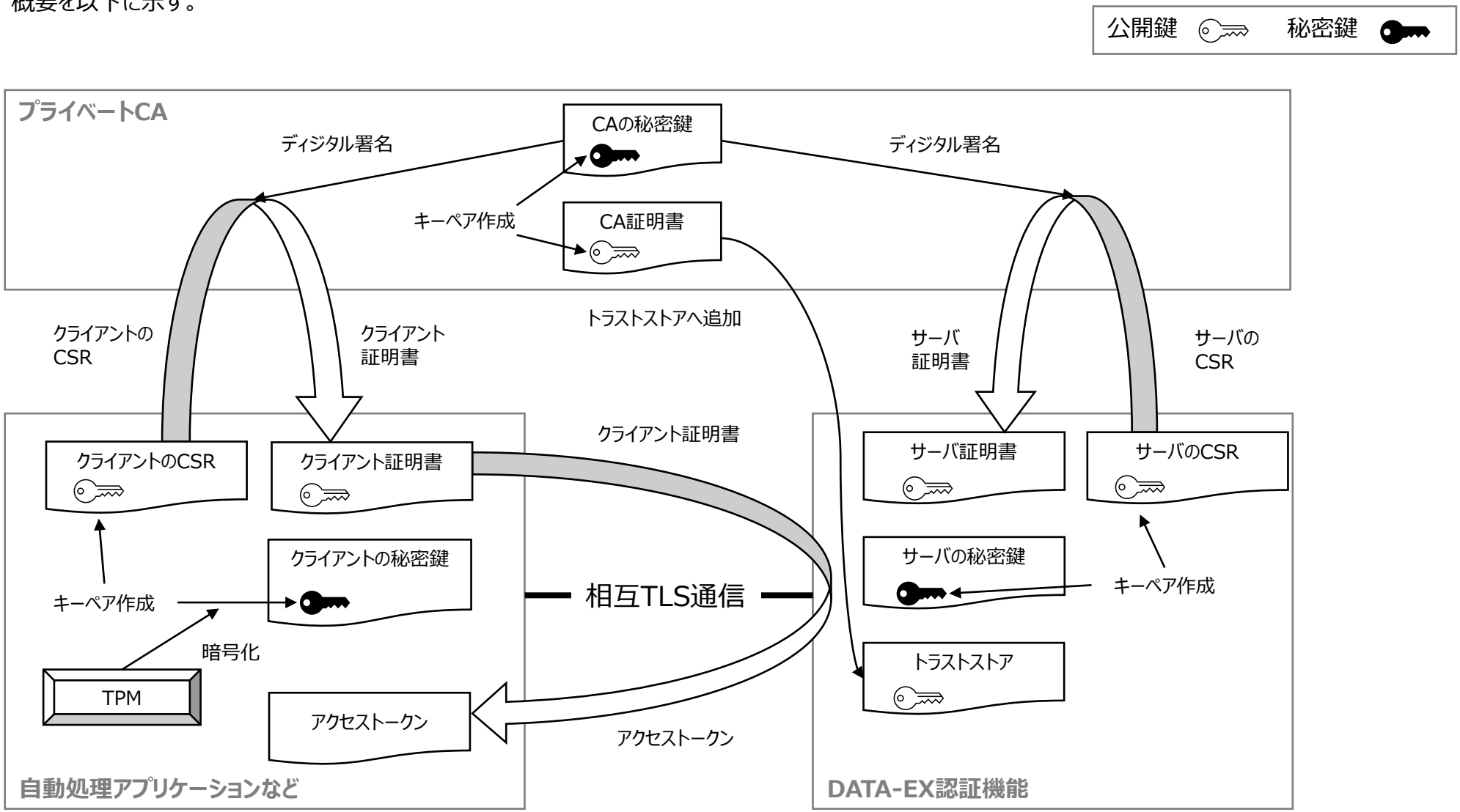
2. 方式 > 2.1. 認証方式 > 2.1.3. 外部IdP

IdPとは、Identity Providerの略称であり、ユーザの認証情報を提供するもののことであり、本システムの外部にある一般のサービスとして提供されているIdPを外部IdPとする。
データ受領者は外部IdPのユーザアカウントを所持していれば、 DATA-EX認証機能を用いて認証する代わりに、外部IdPで認証をすることもできる。
外部IdP認証時は各IdPのAALがユーザの属性(AAL)として設定される。



2. 方式 > 2.1. 認証方式 > 2.1.4. 人を介在しない認証

自動処理アプリケーションなどの人が介在しない状況においては、クライアント証明書でクライアント認証することによってアクセストークンを取得する。
クライアント証明書の作成においては、秘密鍵をセキュアに保管するためにTPMを利用する。
概要を以下に示す。



2. 方式 > 2.1. 認証方式 > 2.1.5. ユーザ情報

産業用データ連携基盤にて活用する、DATA-EX認証機能のユーザ情報は以下の通りである。
外部IdPのユーザ情報は各外部IdPによって異なるため割愛する。
DATA-EXユーザの属性であるDATA-EXユーザID、所属組織、AALは認可確認時に必要となる情報である。

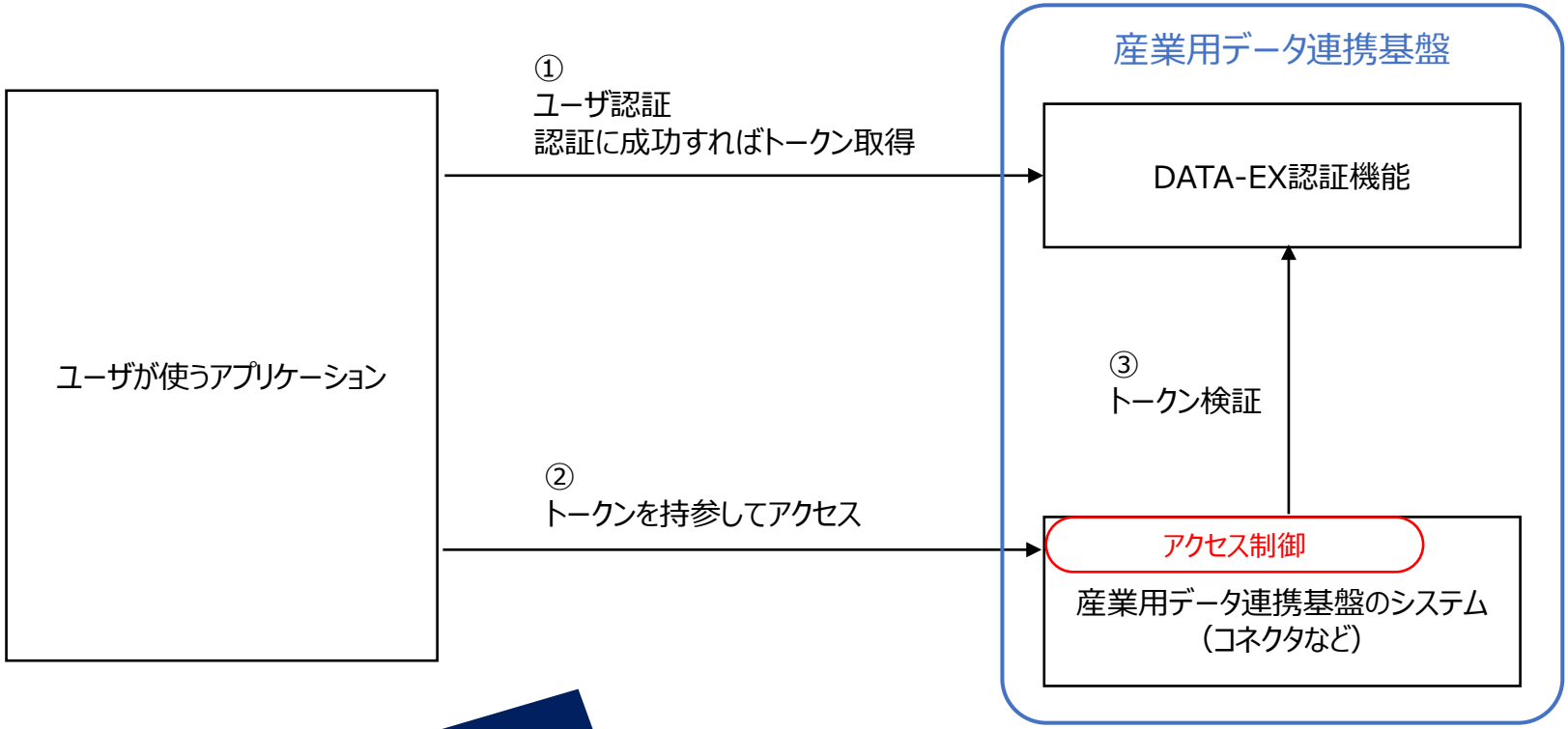
ユーザ情報

#	認証機能のユーザ情報	説明
1	DATA-EXユーザID	使用不可文字は、「<」「>」「/」「¥」の4文字。 文字数制限は、255文字まで。
2	DATA-EXユーザのパスワード	DATA-EX認証で用いるパスワード
3	DATA-EXユーザの基本情報	・メールアドレス ・性 ・名
4	DATA-EXユーザの属性	・住所 ・DATA-EXユーザID ・所属組織　※1 ・AAL (レベル1～3から選択され、ユーザ認証の際に何のIdPを用いたかによって都度更新される)　※2 ・その他の属性　※3

※1：　所属組織もDATA-EXユーザIDで表され、所属している組織が複数の場合はDATA-EXユーザIDが複数登録される。
※2：　付録 「身元確認、当人認証について」を参照のこと
※3：　拡張用。多数の属性を定義できる。DATA-EXでは認可定義に使用しない。

2. 方式 > 2.2. 産業用データ連携基盤へのアクセス制御方式 > 2.2.1. 概要

産業用データ連携基盤が活用するDATA-EXへのアクセス制御方式について説明する。DATA-EXでは認証されたユーザにのみ、DATA-EXのシステムへのアクセスを許可する。
アクセス制御の流れは以下の通り。
① ユーザ認証に成功すると、ユーザが使うアプリケーションはトークンを取得できる。
② ユーザが使うアプリケーションが産業用データ連携基盤のシステムにアクセスする際にはトークンを持参する。
③ 産業用データ連携基盤のシステムが持参されたトークンの検証をすることによってアクセス制御を行う。
産業用データ連携基盤では、OpenID Connect/OAuth2.0の仕様に基づいたトークンをベースとしたアクセス制御を行う。

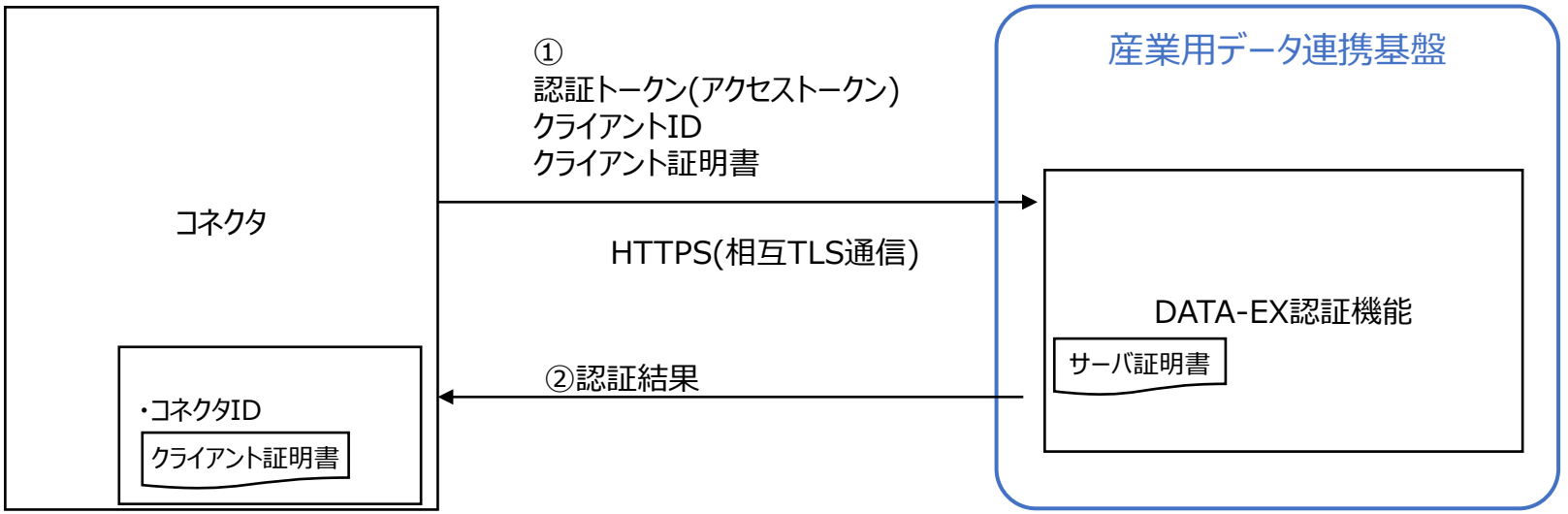


「ユーザが使うアプリケーション」、「 産業用データ連携基盤のシステム」が具体的に何かというのは、業務シーンによって異なる

2. 方式 > 2.2. 産業用データ連携基盤へのアクセス制御方式 > 2.2.2. クライアント認証

産業用データ連携基盤が活用するDATA-EX認証機能へのクライアント認証方式について以下に示す。
OAuth2.0の仕様に基づいた相互TLS認証を前提としたクライアント認証を行う。

DATA-EX認証機能は、クライアントID(コネクタID)発行時にクライアント証明書のSubject値を設定する。
コネクタは、コネクタ構築時に、 DATA-EX認証機能から発行されたクライアントID(コネクタID)とTTPにより発行されたクライアント証明書をコネクタに設定する。
コネクタから認証トークン検証時には、クライアント認証としてクライアントIDとクライアント証明書を用いて相互TLS通信をおこなった上で、認証トークンを認証機能で検証を行う。

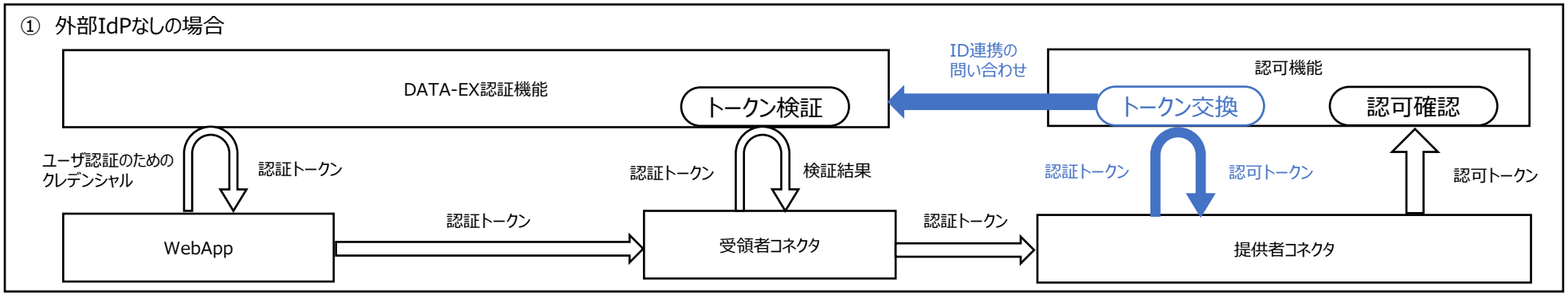


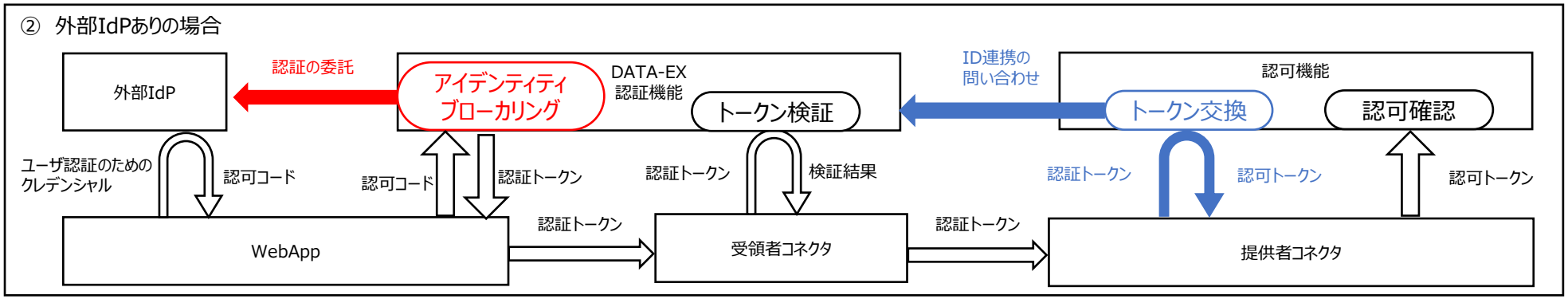
2. 方式 > 2.3. 認可確認のためのID連携方式 > 2.3.1. 概要

産業用データ連携基盤では、外部IdPで認証されたことをDATA-EX認証機能に引き継ぎ、また、認証されたユーザの属性情報を引き継いで、認可の確認ができるようにID連携を行う。ID連携はアイデンティティブローカリングやトークン交換によって行う。
アイデンティティブローカリングは、ユーザと外部IdPを認証機能が仲介し、外部IdPにユーザ認証を委託し、外部IdPでのユーザ認証成功を受けて、認証機能がトークンを発行することである。
トークン交換は、認証機能で発行済みのトークンの情報（ユーザ属性など）を引き継いで、認可機能のトークンを新たに発行する。
外部IdPなし／ありの場合は処理の流れが以下のように異なる。

① 外部IdPなしの場合
認証機能がユーザの認証および認証トークン発行を行う。

② 外部IdPありの場合
認証機能は外部IdPに認証を委託する。その後、アイデンティティブローカリングによって認証機能が認証トークン発行を行う。





2. 方式 > 2.3. 認可確認のためのID連携方式 > 2.3.2. トークン一覧

トークンの一覧は以下の通り。

#	産業用データ連携基盤におけるトークン名称	OIDC/OAuth2.0仕様におけるトークン種別	説明
1	認証トークン	アクセストークン	認証機能が発行するアクセストークンのこと 以下の状況で取得される ・ 運営事業者が認証されて、認証機能やユーザ登録申請機能が取得する ・ データ受領者が認証されて、来歴管理やWebAppが取得する ・ データ提供者が認証されて、来歴管理、データカタログ作成ツール、認可機能、契約管理が取得する
2	認可トークン	アクセストークン	認可機能が認証機能と連携した際に、認証トークンの情報を引き継いで認可機能が発行するアクセストークンのこと 以下の状況で取得される ・ 提供者コネクタが認証トークンと交換して取得する

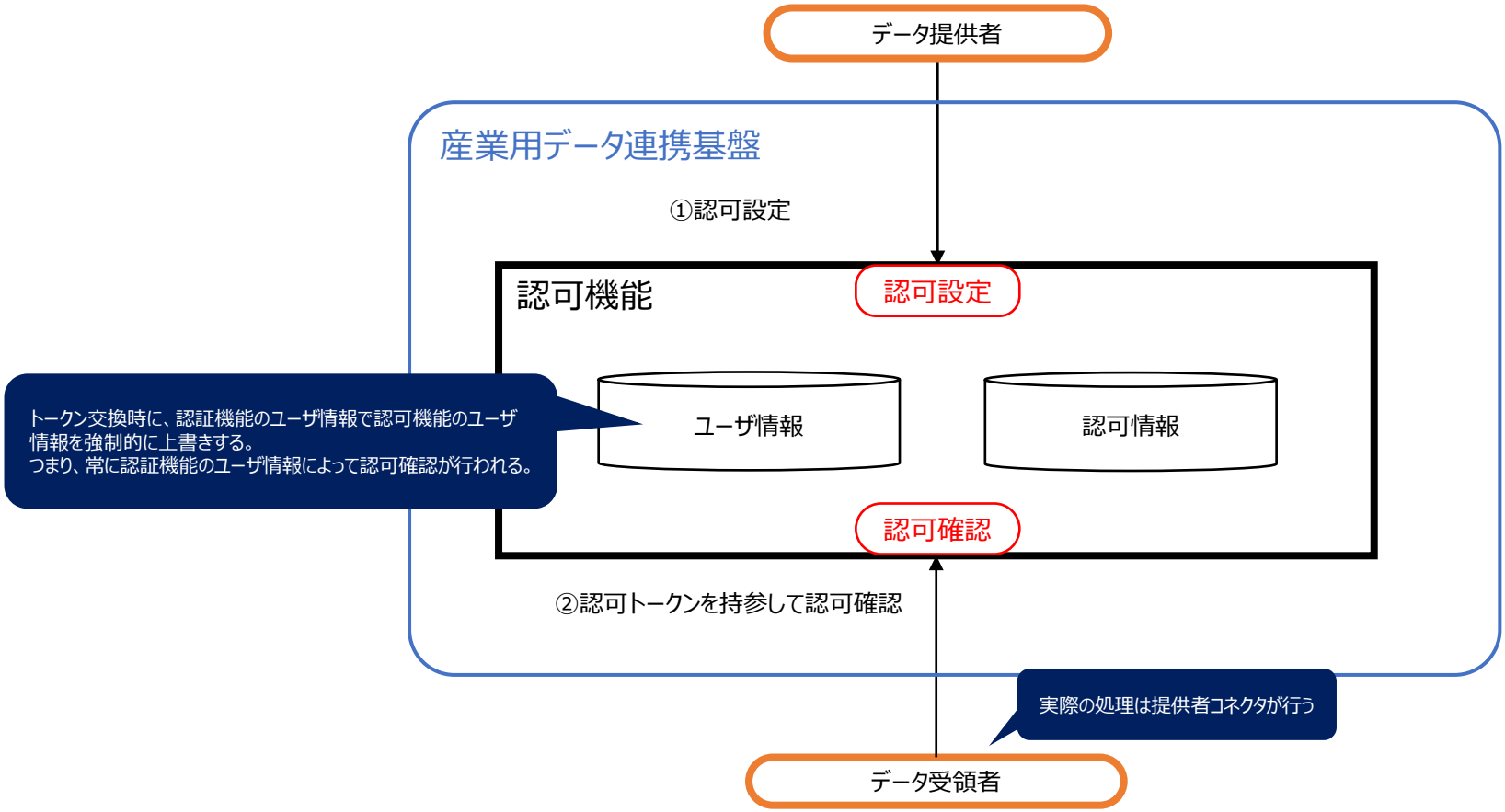
2. 方式 > 2.3. 認可確認のためのID連携方式 > 2.3.3. トークン内容

外部IdPが発行するトークンは、外部IdPごとに異なるため、各外部IdPの仕様を参照のこと。
産業用データ連携基盤で用いる認証トークンおよび認可トークンのクレームは以下表の通り。
トークンはユーザ属性を特定する情報を持っている。これらの情報によって認可確認をすることができる。

#	クレーム名	説明	クレーム値の例	備考
1	exp	トークンの有効期限(UNIX時間)	1654660700	JWT標準クレーム
2	iat	トークンが発行された時刻(UNIX時間)	1654660400	JWT標準クレーム
3	jti	トークンごとに一意な識別子	12ff3f47-f64f-4666-bda3-4e0984d9d4e7	JWT標準クレーム
4	iss	トークン発行者の識別子（トークン発行サーバの識別子）	https://example_domain/auth/realms/realm_name	JWT標準クレーム
5	sub	トークンの主題の識別子（ユーザの識別子）	be974a5a-b2f7-44bc-a9c3-2dbefa7a062a	JWT標準クレーム
6	typ	トークンの形式	Bearer	__
7	azp	認可された対象者のクライアントID	example_client	__
8	session_state	セッション状態	c0d02a92-4d79-4456-aa6b-623b162fe2dc	__
9	scope	スコープ	email profile	__
10	sid	セッションID	f67baba1-8b3c-430f-8815-f37470df0af3	__
11	address	住所	Tokyo-to, Chiyoda-ku 1-2-3	独自ユーザ属性
12	user	DATA-EXユーザID	XYZ	独自ユーザ属性 認可に利用
13	org	所属組織	XXXXXXX	独自ユーザ属性 認可に利用
14	aal	当人認証レベル	2	独自ユーザ属性 認可に利用
15	extras	その他の属性	"field1":"value1", "field2":"value2"	独自ユーザ属性

2. 方式 > 2.4. 認可方式 > 2.4.1. 概要

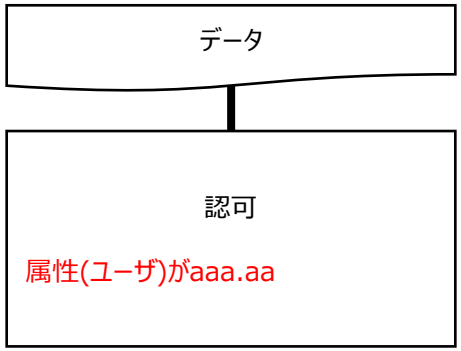
認可方式の概要について説明する。
カタログやデータに対するアクセス制御処理は2段階に分けられる。まず認可設定（認可情報の登録）が行われ、その後、認可確認が行われる。
認可に関する流れは以下の通り。
① データ提供者は、認可機能に対して認可設定をする。
② データ受領者は、認可トークンを認可機能に持参して認可確認（カタログやデータにアクセスする権限があるかの確認）する。認可トークンには認可を判断するための属性が含まれているため、認可確認をすることができる。



2. 方式 > 2.4. 認可方式 > 2.4.2. 認可の与え方

ユーザの実態としては、個人や組織がいると考えられる。
ユーザにはDATA-EXユーザIDが付与されているため、 DATA-EXユーザIDを指定して認可することで、特定のユーザにデータへのアクセスを許可することができる。一方で、ある組織に属する個人全員(組織自体も含む)に認可を与えたい場合は、まず、個人の属性に組織のDATA-EXユーザIDを付与する。次に、データに対して、属性に組織のDATA-EXユーザIDを持つユーザへの認可を与える。これによって、ある組織に属する個人全員にデータに対するアクセスを許可することができる。

例①

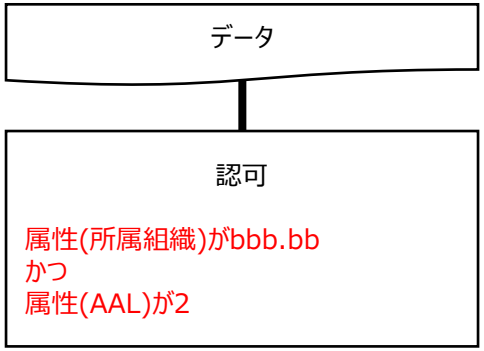


アクセス可能

個人

属性（ユーザ）	aaa.aa
属性（所属組織）	xxx.xx
属性（AAL）	2

例②



アクセス可能

組織

属性（ユーザ）	bbb.bb
属性（所属組織）	bbb.Bb
属性（AAL）	2

アクセス可能

個人（組織に属する）

属性（ユーザ）	ccc.cc
属性（所属組織）	bbb.bb
属性（AAL）	2

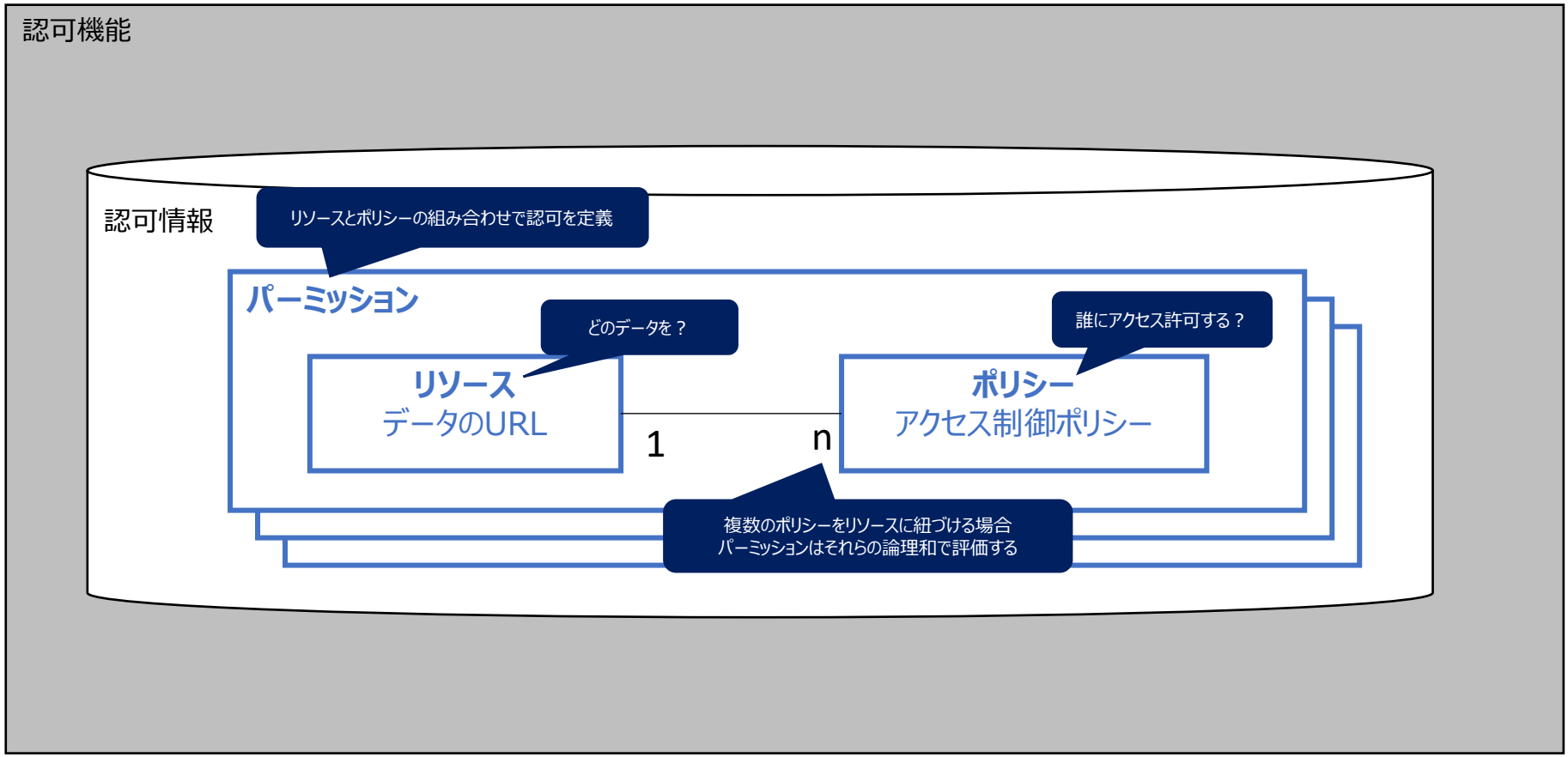
(AALが1のため)
アクセス不可

個人（組織に属する）

属性（ユーザ）	ddd.dd
属性（所属組織）	bbb.bb
属性（AAL）	1

2. 方式 > 2.4. 認可方式 > 2.4.3. 認可情報の内部処理

認可の設定は、内部処理でいくつかの認可情報を用いることで登録できる。
認可情報には、パーミッション、リソース、ポリシーがある。これらの概念はKeycloakの実装にもとづく。
パーミッションはリソースとポリシーの組み合わせであり、リソースはデータのURL、ポリシーはアクセス制御ポリシーのことを指す。
つまり、パーミッションを評価することで、「どのデータ」を「誰に」提供してよいかの可否を判断することができる。
リソースとポリシーの関係は、1対多であり、複数のポリシーをリソースに紐づける場合には、それらの論理和によってパーミッションを評価する。
また、パーミッションとリソースの関係は1対1とする。



2. 方式 > 2.4. 認可方式 > 2.4.4. 認可情報(リソース)

リソースとは、アクセスに制限をかける対象のことである。例えば、保護されたAPIのURL、データのURLなどがある。
ここで、アスタリスクをワイルドカードとして使用することができず、ディレクトリ単位でデータを指定することはできない。
産業用データ連携基盤では、HTTP(S)、FTP、NGSIのプロトコルに対応している。以下にURLの例を示す。
255文字までを制限とし、使用可能文字は半角英数、ハイフン、アンダーバーのみとする。

#	プロトコル	URLの例
1	HTTP(S)	https://example.com/data.pptx
2	FTP	ftp://example.com/data.pptx
3	NGSI	https://t1072680.dev-necjfiware.jp/orion/v2.0/entities?type=Test_CareService11,Fiware-Service=AAA,Fiware-ServicePath=/#

2. 方式 > 2.4. 認可方式 > 2.4.5. 認可情報(ポリシー)

ポリシーとは、誰にデータを提供してよいか、という条件のことである。
産業用データ連携基盤では、ユーザが持つ属性を条件としてRegExポリシーに設定する。また、複数のRegExポリシーの論理積をとるために、RegExポリシーをAggregatedポリシーによってグループ化する。

#	条件として設定する属性	説明
1	ユーザ	ユーザのDATA-EXユーザIDを設定する
2	ユーザの所属組織	ユーザの所属組織のIDを設定する
3	ユーザの当人認証レベル（AAL）	ユーザの当人認証レベルを1～3の数値で設定する

Regexポリシーの詳細を以下に示す。

#	Regexポリシーの項目	説明
1	ID	Regexポリシーを一意に識別するUUID
2	名前	このポリシーの名前
3	説明	このポリシーの説明
4	ターゲットクレーム	トークンのクレームを指定
5	正規表現のパターン	トークンのクレームの値とマッチする正規表現
6	ロジック	産業用データ連携基盤における認可設定では、「Positive」を固定として設定する

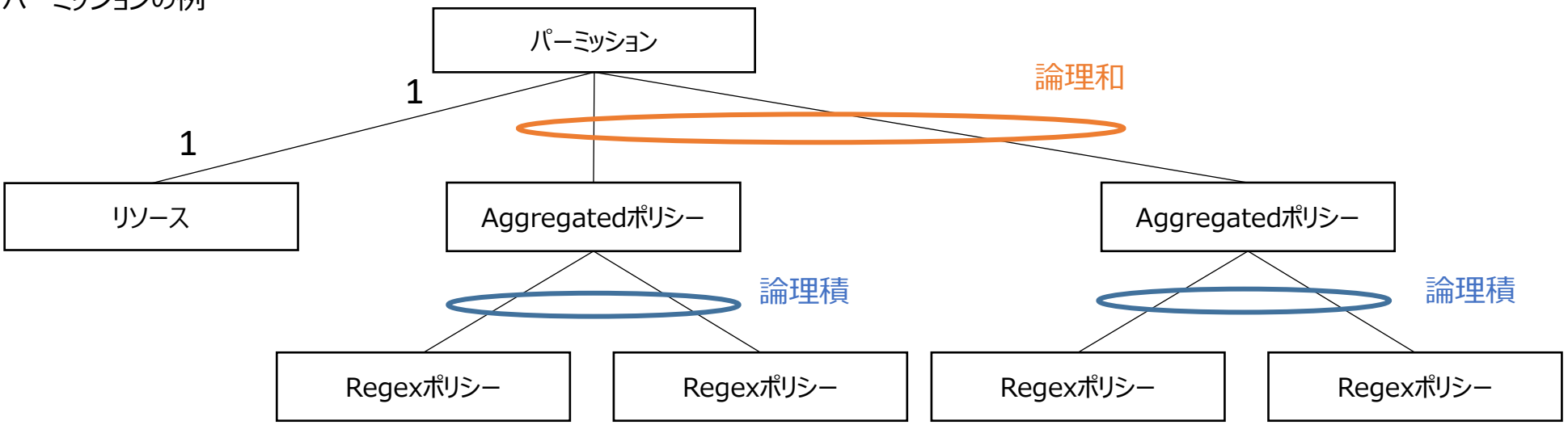
Aggregatedポリシーの詳細を以下に示す。

#	Aggregatedポリシーの項目	説明
1	ID	Aggregatedポリシーを一意に識別するUUID
2	名前	このポリシーの名前
3	説明	このポリシーの説明 契約にもとづく認可の場合、取引ID、契約形態、契約管理サービスURLを記入する
4	ポリシー	RegExポリシーの一覧
5	決定戦略	産業用データ連携基盤における認可設定では、「Unanimous」（RegExポリシーの論理積）を固定として設定する
6	ロジック	産業用データ連携基盤における認可設定では、「Positive」を固定として設定する

2. 方式 > 2.4. 認可方式 > 2.4.6. 認可情報(パーミッション)

パーミッションはリソースとAggregatedポリシーによって認可を表現する。
パーミッションはリソースを必ずひとつ持ち、Aggregatedポリシーを1～n個持つ（以下の例では2つ）
ユーザが持つ属性を指定するためには、Regexポリシーによって正規表現で記述する。複数のRegexポリシーの論理積をとるために、Aggregatedポリシーによって複数のRegexポリシーを指定する。

パーミッションの例



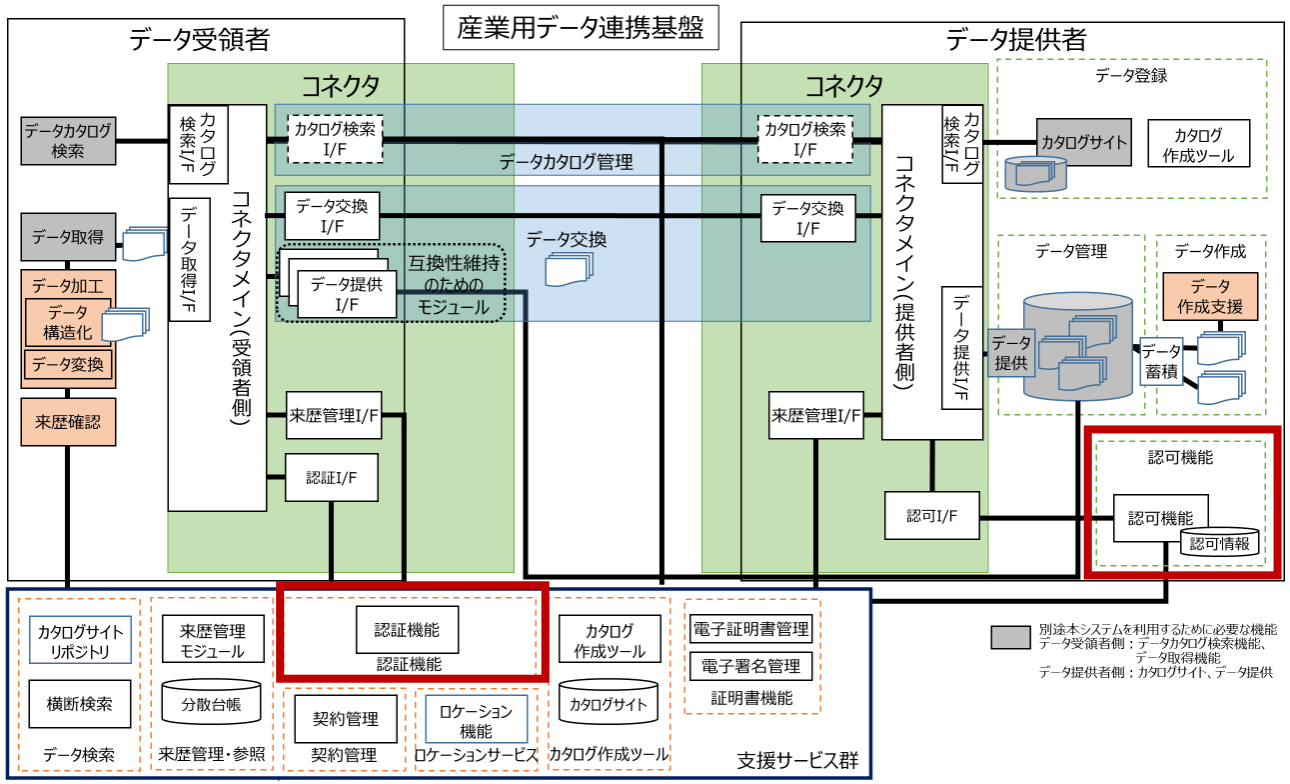
パーミッションの詳細を以下に示す。

#	パーミッションの項目	説明
1	ID	パーミッションを一意に識別するUUID
2	名前	このパーミッションの名前
3	説明	このパーミッションの説明
4	リソース	リソースを指定。産業用データ連携基盤における認可設定では、パーミッション名とリソース名は同一とする。
5	ポリシー	産業用データ連携基盤における認可設定では、Aggregatedポリシーの一覧を指定する
6	決定戦略	産業用データ連携基盤における認可設定では、「Affirmative」（論理和）を固定として設定する

2. 方式 > 2.5. 産業用データ連携基盤における認証・認可

産業用データ連携基盤における、認証機能と認可機能を下図の赤枠部分に示す。

#	機能	産業用データ連携基盤の枠組み上の位置	説明
1	認証機能	支援サービス群	ユーザ認証をする。 認証トークンの発行やその検証をする。
2	認可機能	データ提供者	データ提供者や契約管理からの要求を受け、認可の設定をする。 データ受領者からの要求を受け、認可の確認をする。 認可トークンの発行やその検証をする。



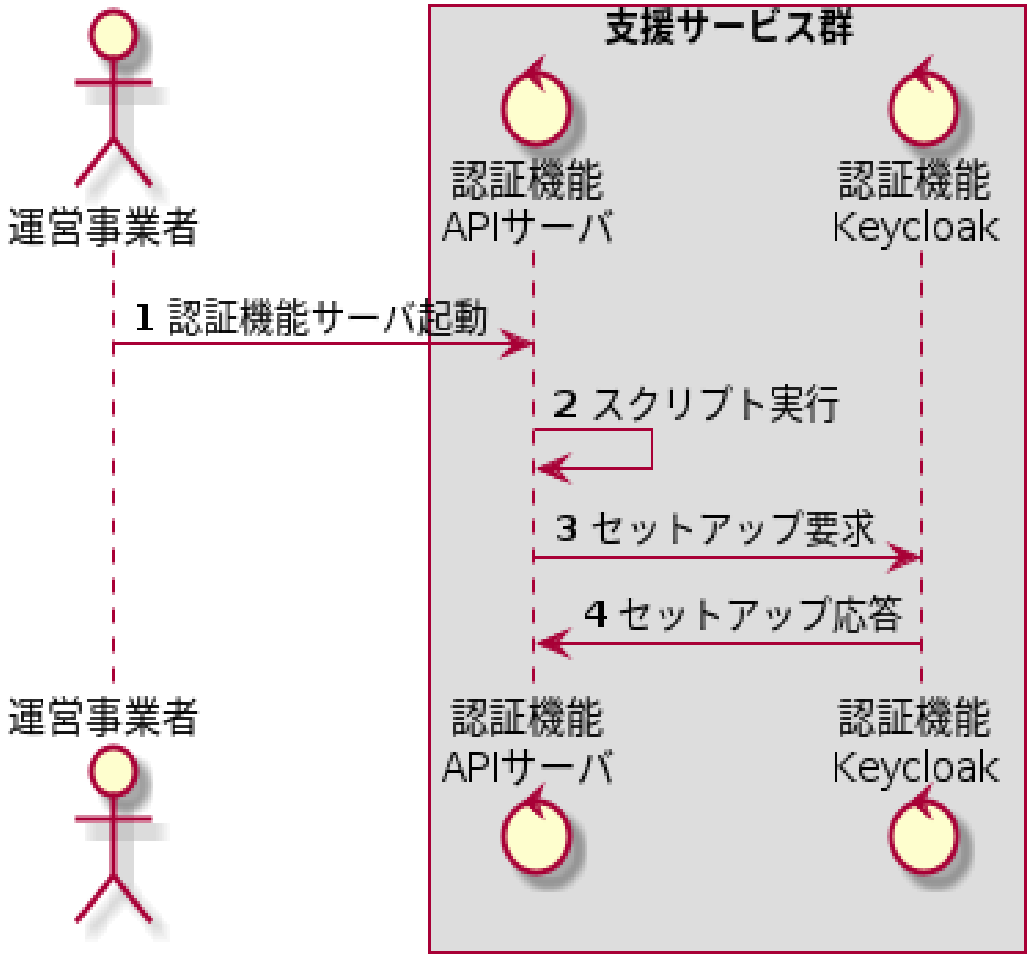
3. シーケンス

3. シーケンス > 3.1. 運営事業者の業務に関わるシーケンス

主に運営事業者の業務に関わるシーケンス一覧を示す。
コネクタに関連するシーケンスはコネクタの基本設計書を参照のこと。

#	シーケンス	説明	該当する業務フロー
1	認証機能構築	認証機能を構築する	認証機能運用開始
2	認証機能のログイン	各業務を行うために認証機能にログインする	データ受領者登録 データ提供者登録
3	ユーザ登録	ユーザを登録する	データ受領者登録 データ提供者登録
4	クライアント登録	クライアントを登録する	データ受領者登録 データ提供者登録
5	外部IdP登録	新規に外部IdPを登録する	認証機能運用開始

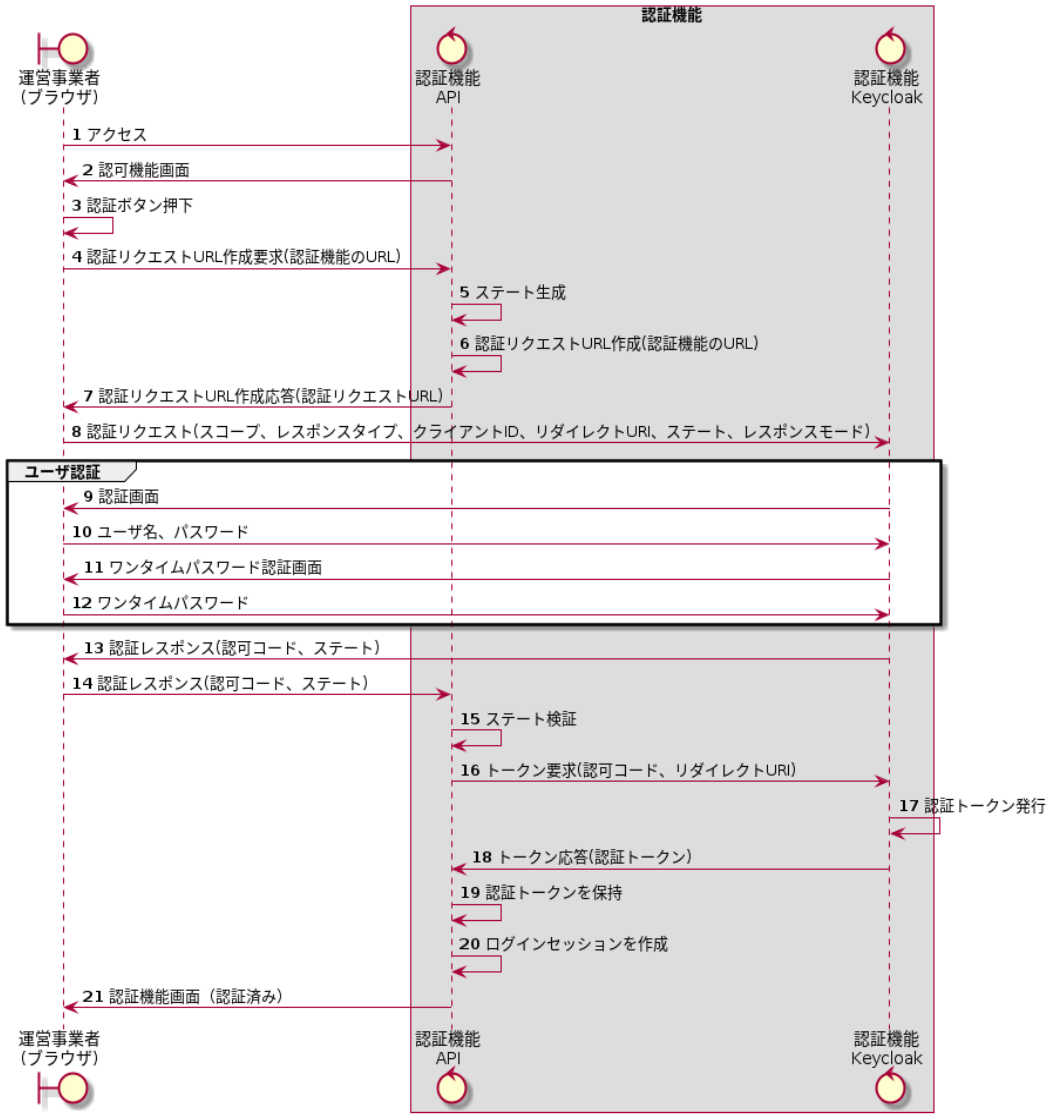
認証機能構築のシーケンスを以下に示す。
認証機能の初回立ち上げ時にスクリプトが自動で起動され、必要なセットアップが行われる。



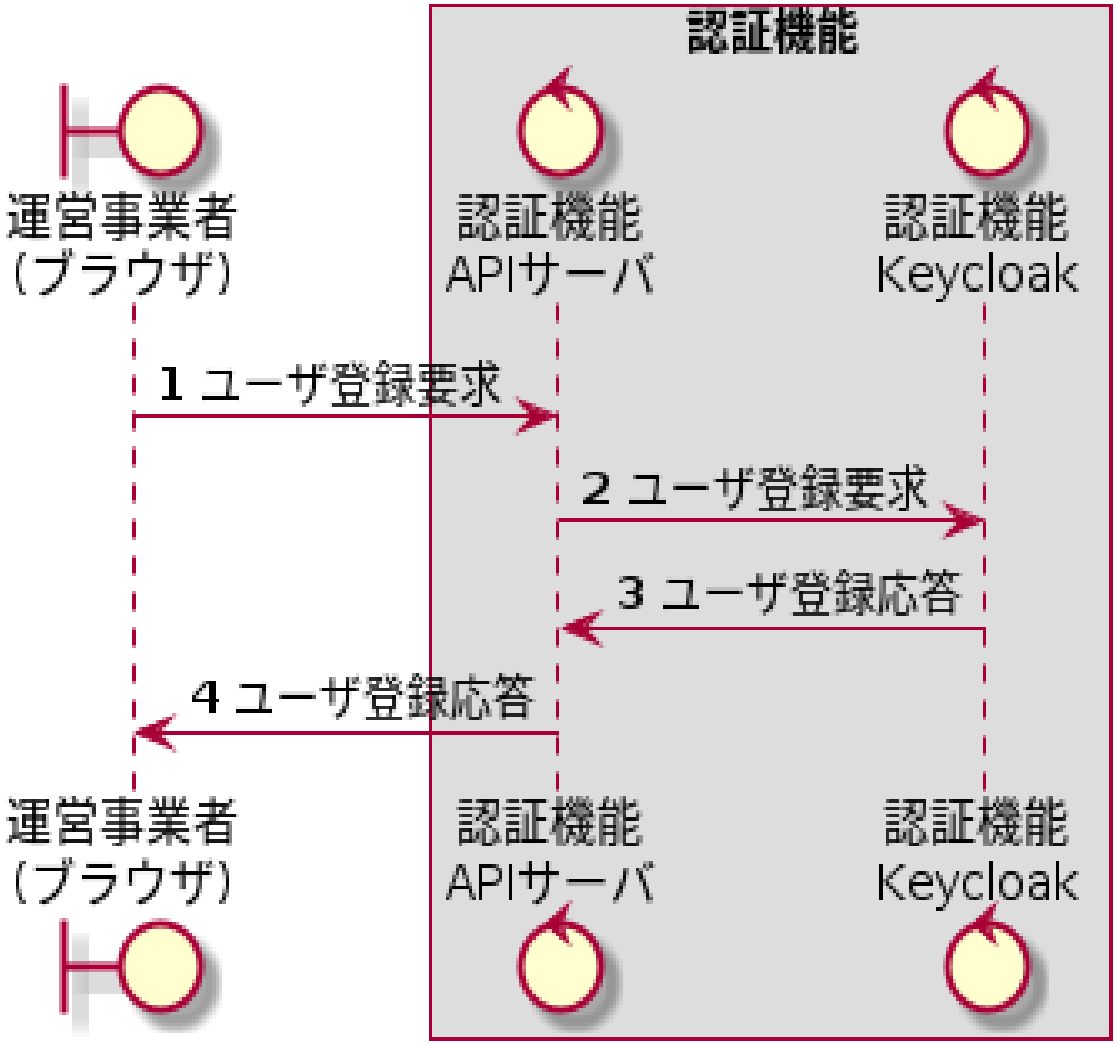
認証機能のログインのシーケンスを示す。

運営事業者が認証機能にログインする。認証リクエストをすることによってユーザ認証を開始することができる。
ユーザ認証に成功すると認証レスポンスによって認可コードが得られ、それと引き換えに認証トークンを得ることができる。

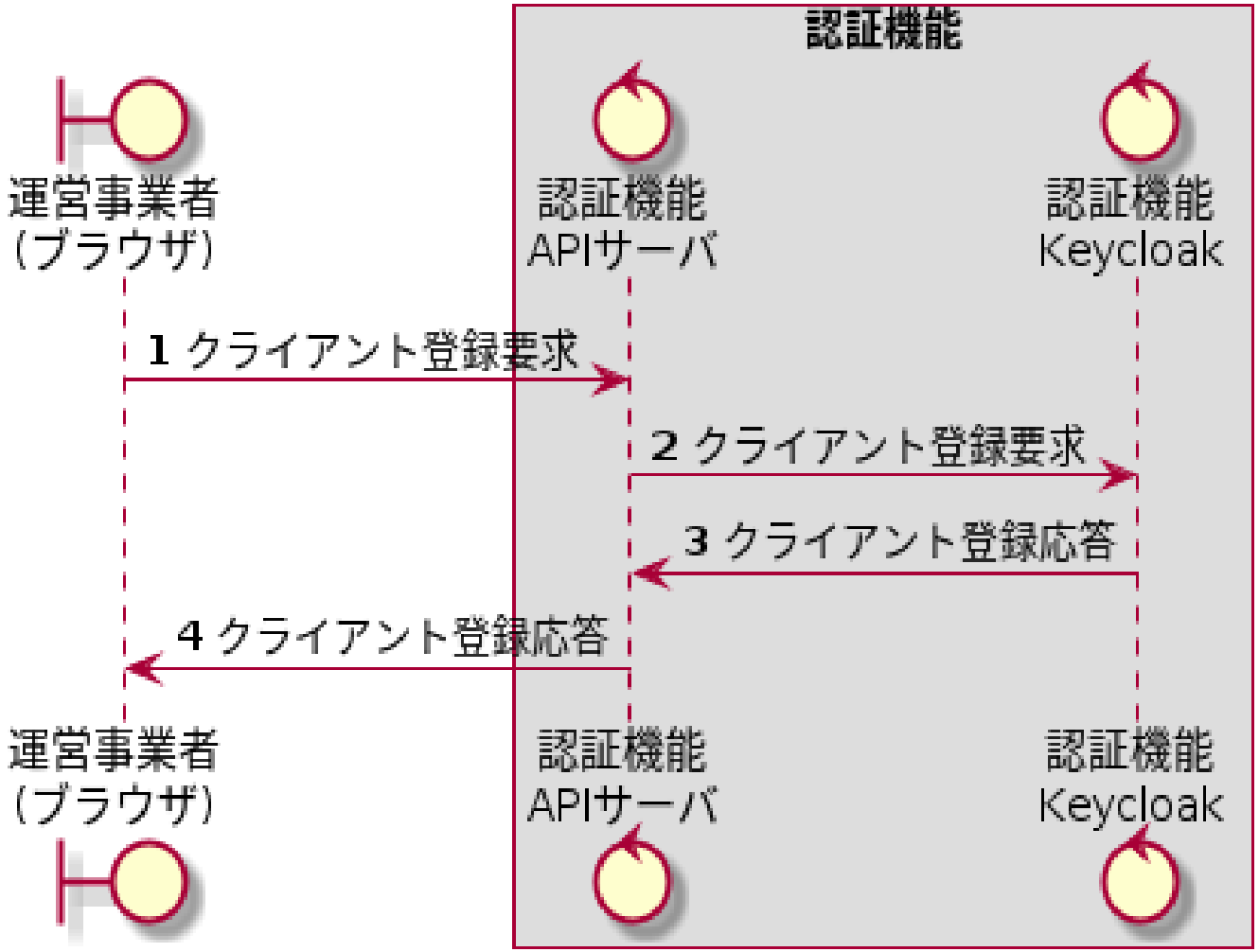
認証リクエストと認証レスポンスはOpenID Connect/OAuth2.0で規定されている。
シーケンス中のパラメータについて以下に補足する。
スコープとは、トークンを取得する際に権限の範囲を指定するものである。
レスポンスタイプとは、グラントタイプを指定するものである。ここでは認可コードグラントを指定している。
クライアントIDとは、認証機能がクライアントを識別するためのものである。
リダイレクトURIとは、認証機能画面からWebApp画面に戻るときのためのURIのことである。
ステートとは、認可コードのすり替え（クロスサイトリクエストフォージェリ）を防ぐために必要なランダム値である。
レスポンスモードとは、パラメータの受け渡し方法を指定するものである。
認可コードとは、 OpenID Connect/OAuth2.0で規定されている、認可コードグラントにおいてアクセストークンを取得するために必要な短命のトークンである。例えば、以下のようなランダム値である。
db377803-9bd7-401e-8f25-d7c8a0ddb0e9.cc6ccf64-1bed-4775-8a1d-2fd85c222d63.2163ff50-0e4e-4527-a52f-2aef468b9b4a
認証トークンはDATA-EX認証機能が発行するアクセストークンである。



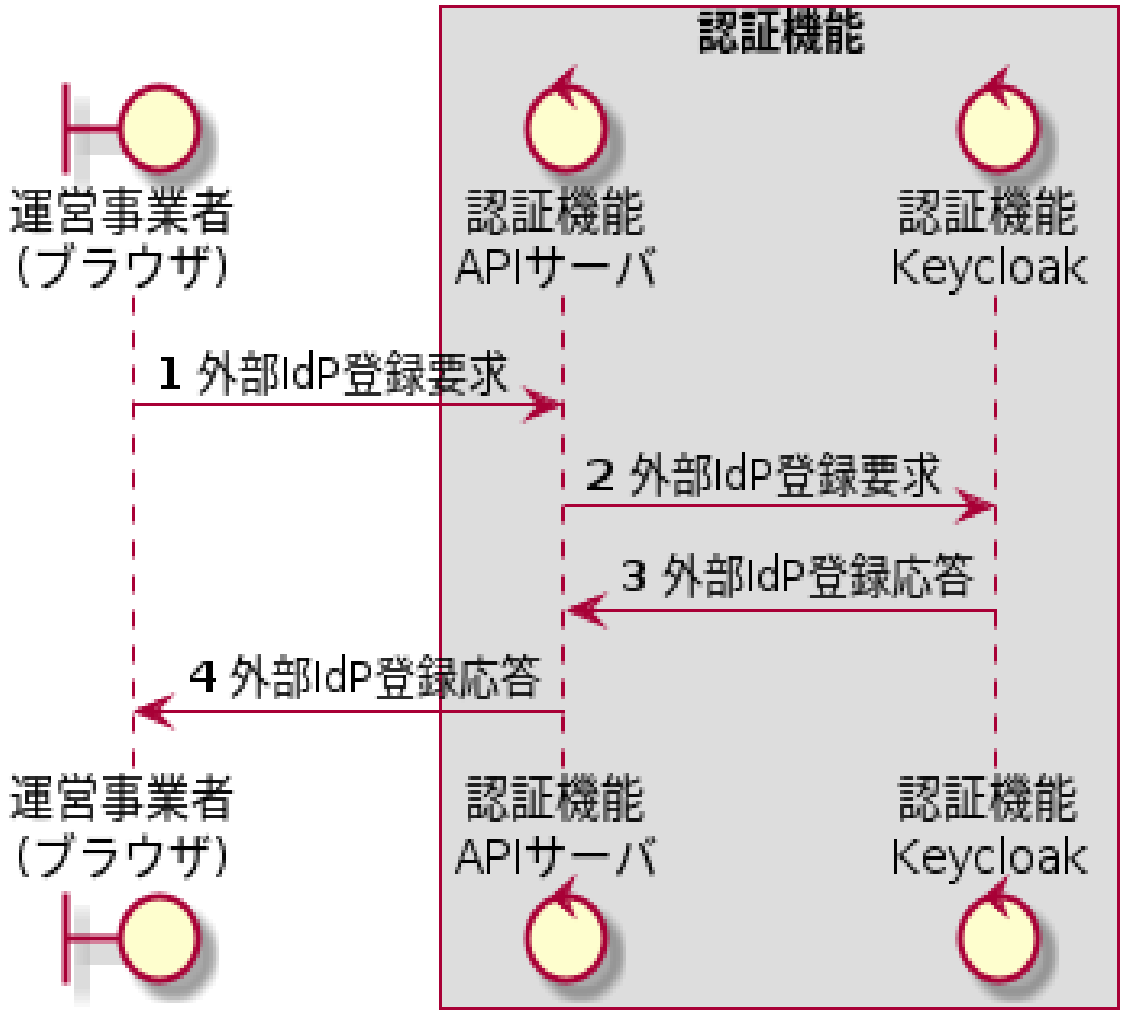
ユーザ登録のシーケンスを以下に示す。
ユーザの基本情報や属性など、ユーザの情報を登録する。



クライアント登録のシーケンスを以下に示す。
クライアントIDなど、ユーザが保有するクライアントに関する情報を登録する。



外部IdP登録のシーケンスを以下に示す。
産業用データ連携基盤が対応する外部IdPを新規に追加する際に本業務を行う。



3. シーケンス > 3.2. データ提供者の業務に関わるシーケンス

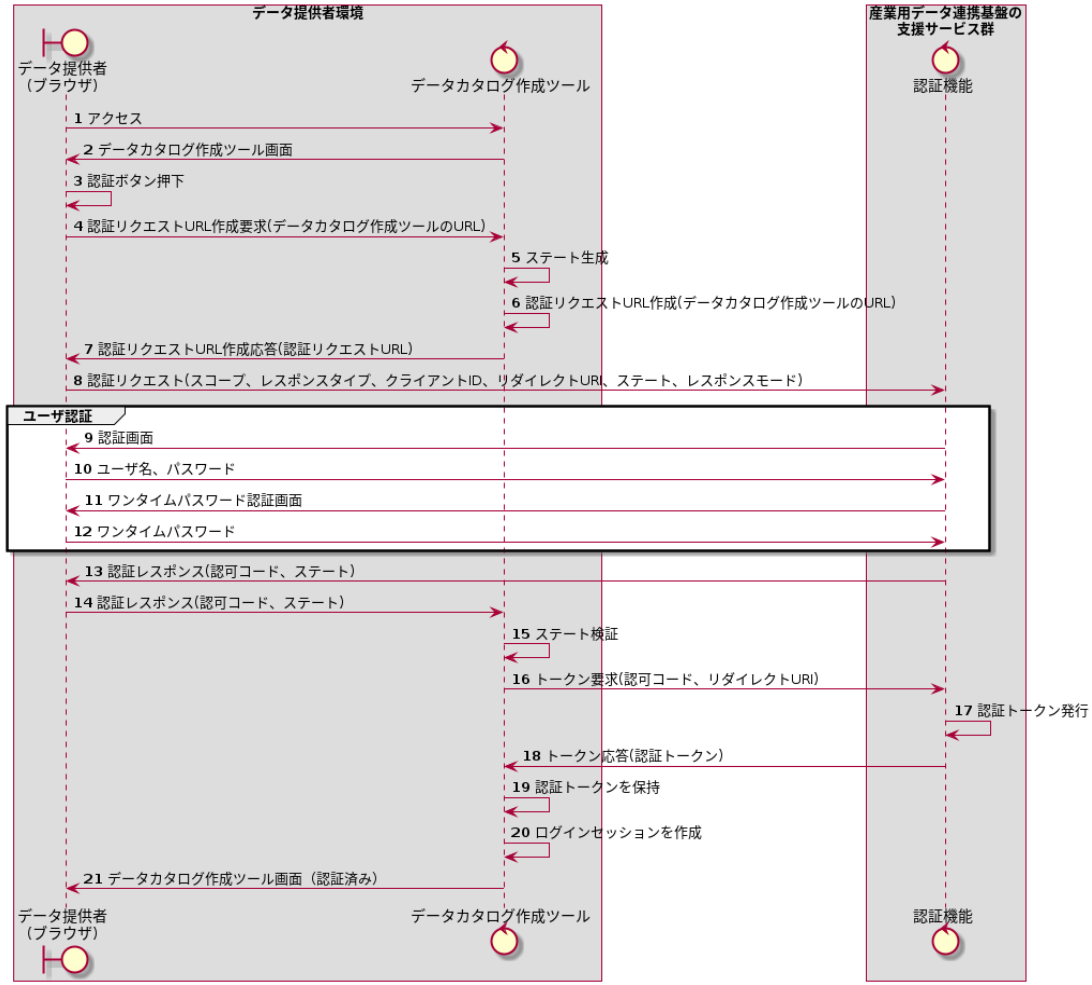
主にデータ提供者の業務に関わるシーケンス一覧を示す。

#	シーケンス	説明	該当する業務フロー
1	データカタログ作成ツールのログイン	データ提供者がデータカタログ作成ツールにログインする	提供データの準備
2	認可機能のログイン	データ提供者が認可機能にログインする	認可情報登録（限定提供データ（契約無）） 認可情報登録（限定提供データ（契約有））
3	認可情報登録	認可情報登録をする	認可情報登録（限定提供データ（契約無）） 認可情報登録（限定提供データ（契約有）
4	認可情報登録共通処理詳細	認可情報登録の共通処理の詳細	認可情報登録（限定提供データ（契約無）） 認可情報登録（限定提供データ（契約有））

データカタログ作成ツールのログインのシーケンスを示す。

データ提供者がデータカタログ作成ツールにログインする。
認証リクエストをすることによってユーザ認証を開始することができる。
ユーザ認証に成功すると認証レスポンスによって認可コードが得られ、それと引き換えに認証トークンを得ることができる。

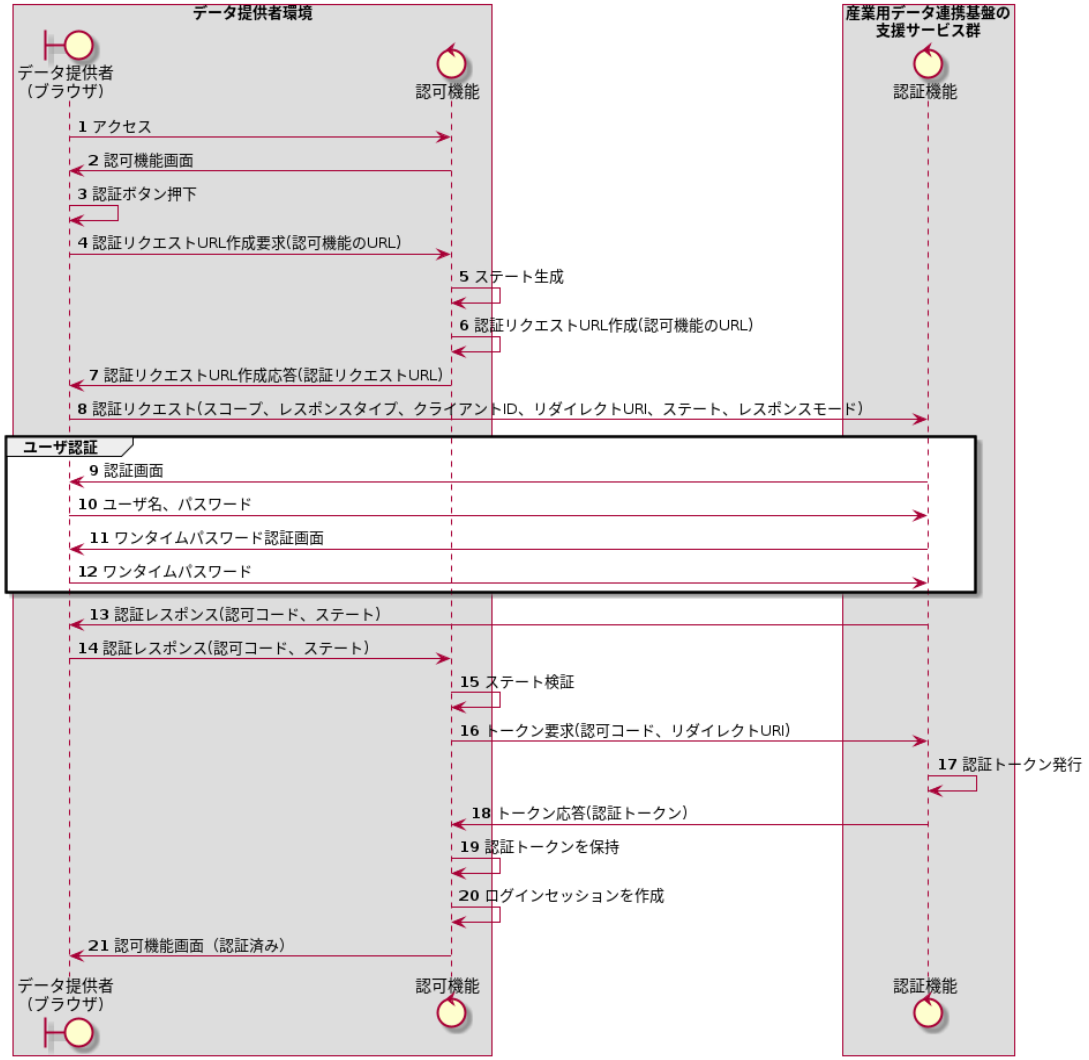
シーケンス中のパラメータについて以下に補足する。なお、認証リクエストと認証レスポンスはOpenID Connect/OAuth2.0で規定されている。
スコープとは、トークンを取得する際に権限の範囲を指定するものである。
レスポンスタイプとは、グラントタイプを指定するものである。ここでは認可コードグラントを指定している。
クライアントIDとは、認証機能がクライアントを識別するためのものである。
リダイレクトURIとは、認証機能画面からWebApp画面に戻るときのためのURIのことである。
ステートとは、認可コードのすり替え（クロスサイトリクエストフォージェリ）を防ぐために必要なランダム値である。
レスポンスモードとは、パラメータの受け渡し方法を指定するものである。
認可コードとは、 OpenID Connect/OAuth2.0で規定されている、認可コードグラントにおいてアクセストークンを取得するために必要な短命のトークンである。例えば、以下のようなランダム値である。
db377803-9bd7-401e-8f25-d7c8a0ddb0e9.cc6ccf64-1bed-4775-8a1d-2fd85c222d63.2163ff50-0e4e-4527-a52f-2aef468b9b4a
認証トークンはDATA-EX認証機能が発行するアクセストークンである。



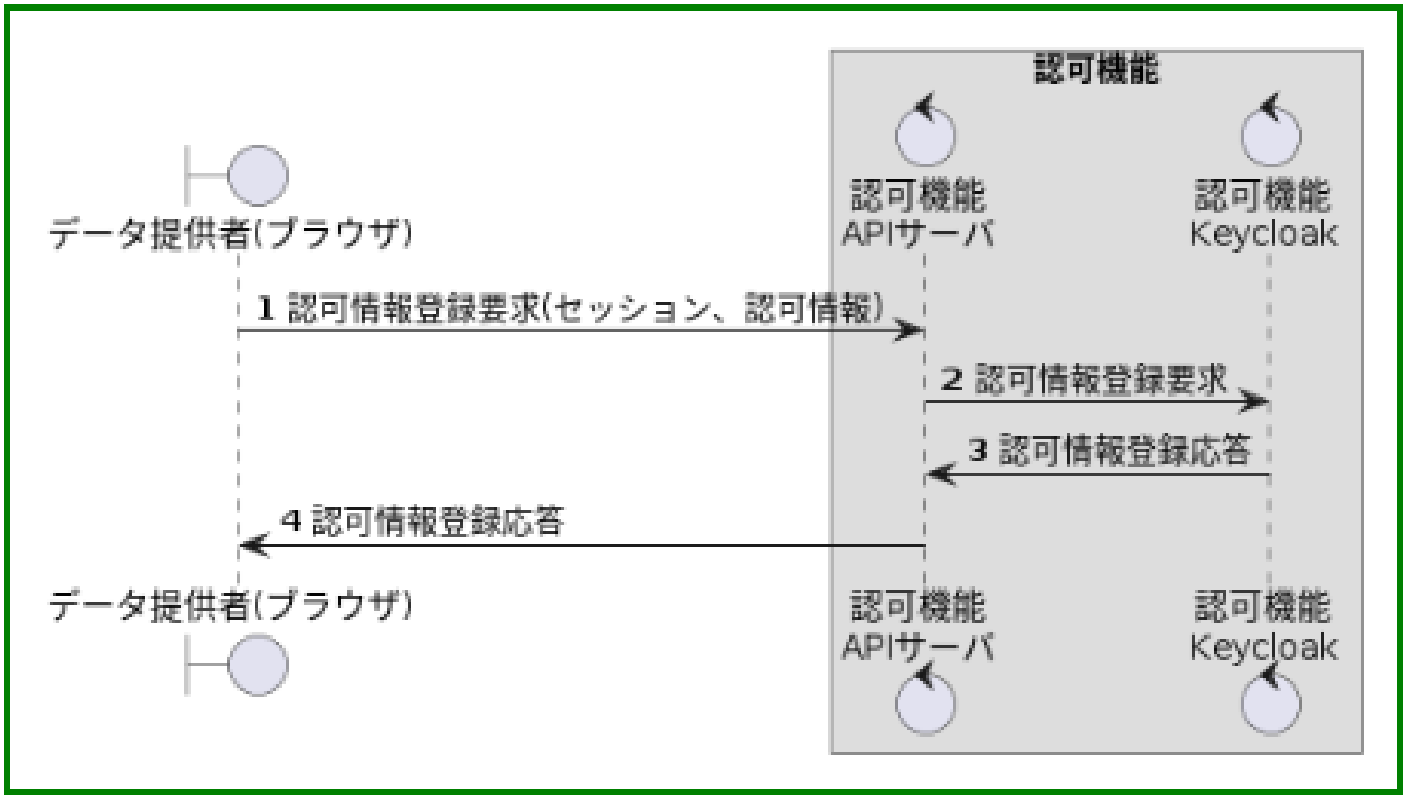
認可機能のログインのシーケンスを示す。

データ提供者が認可機能にログインする。
認証リクエストをすることによってユーザ認証を開始することができる。
ユーザ認証に成功すると認証レスポンスによって認可コードが得られ、それと引き換えに認証トークンを得ることができる。

シーケンス中のパラメータについて以下に補足する。なお、認証リクエストと認証レスポンスはOpenID Connect/OAuth2.0で規定されている。
スコープとは、トークンを取得する際に権限の範囲を指定するものである。
レスポンスタイプとは、グラントタイプを指定するものである。ここでは認可コードグラントを指定している。
クライアントIDとは、認証機能がクライアントを識別するためのものである。
リダイレクトURIとは、認証機能画面からWebApp画面に戻るときのためのURIのことである。
ステートとは、認可コードのすり替え（クロスサイトリクエストフォージェリ）を防ぐために必要なランダム値である。
レスポンスモードとは、パラメータの受け渡し方法を指定するものである。
認可コードとは、 OpenID Connect/OAuth2.0で規定されている、認可コードグラントにおいてアクセストークンを取得するために必要な短命のトークンである。例えば、以下のようなランダム値である。
db377803-9bd7-401e-8f25-d7c8a0ddb0e9.cc6ccf64-1bed-4775-8a1d-2fd85c222d63.2163ff50-0e4e-4527-a52f-2aef468b9b4a
認証トークンはDATA-EX認証機能が発行するアクセストークンである。



認可情報登録のシーケンスを以下に示す。



認可情報登録共通処理詳細のシーケンスを以下に示す。

本シーケンスはリソース、RegExポリシーAggregatedポリシー、パーミッションが新規作成時のシーケンスである。
上記それぞれの要素は作成前にKeycloakに検索要求がされ、存在しない場合に新規登録となる。

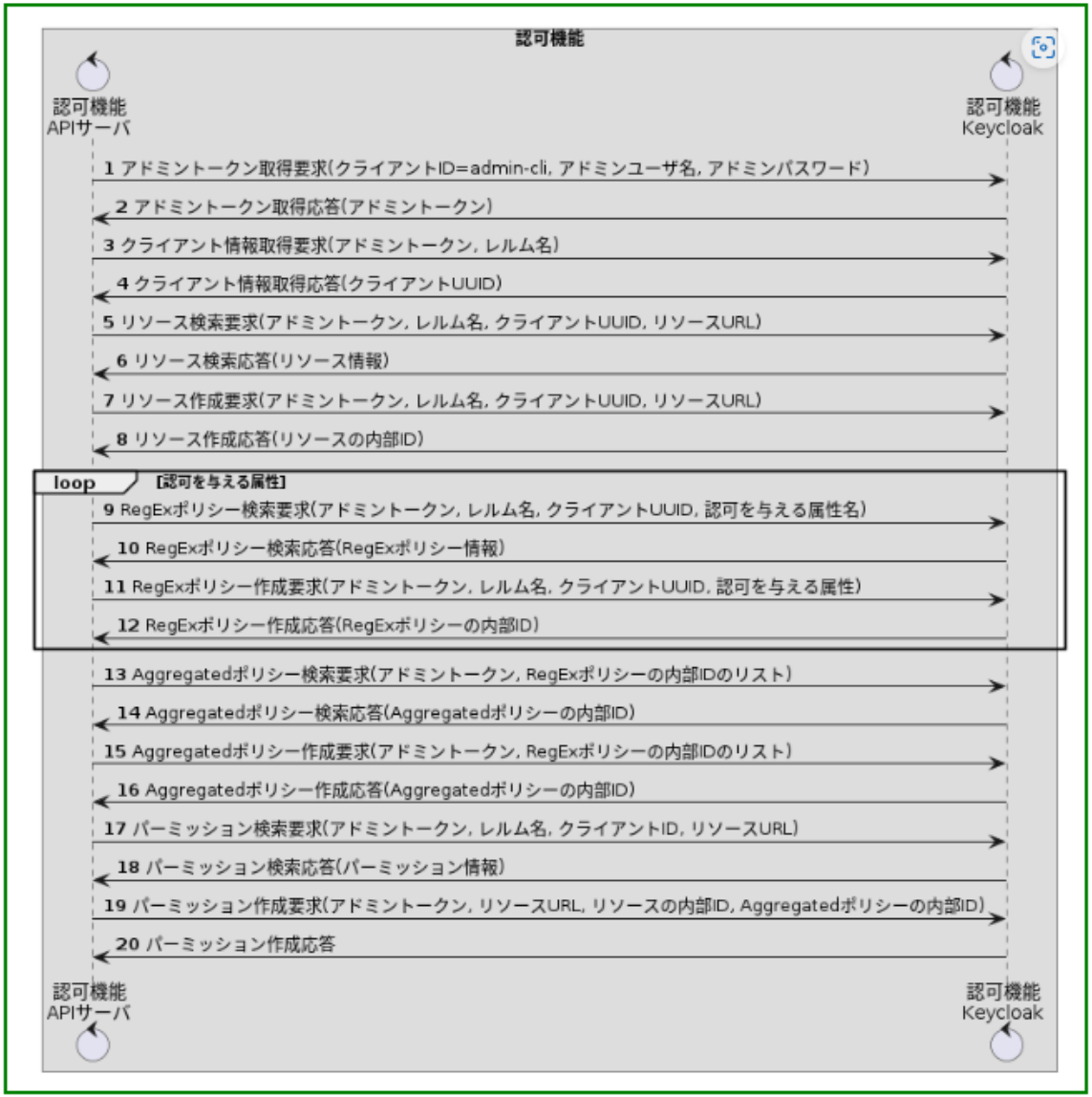
検索した結果存在する場合、それぞれ以下の処理となる。

・6番 リソース検索応答でリソース存在の場合：
7、8番は実行されず、存在しているリソースUUIDを取得し9番の処理へ移行

・10番 RegExポリシー検索応答でRegExポリシー与える属性が存在する場合:
11、12番は実行されず、RegExポリシーUUIDを取得しloop処理継続もしくは13番の処理へ移行

・14番 Aggregatedポリシー検索応答でAggregatedポリシーが存在の場合：
15、16番は実行されず、AggregatedポリシーUUIDを取得し17番の処理へ移行

・18番 パーミッション検索応答でパーミッションが存在の場合：
19、20番は実行されず、パーミッションを更新する処理が実行される



3. シーケンス > 3.3. データ受領者の業務に関わるシーケンス

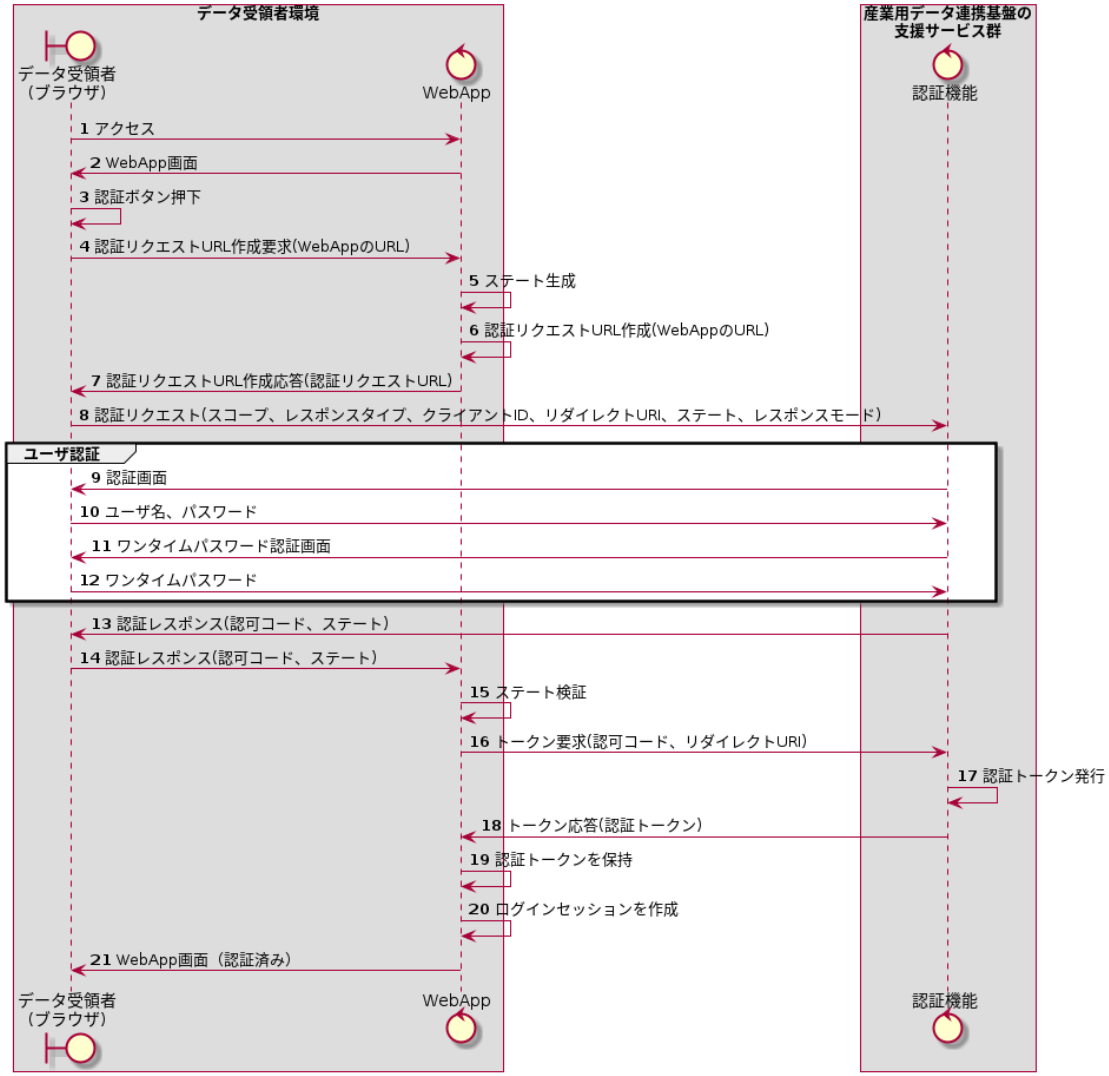
主にデータ受領者の業務に関わるシーケンス一覧を示す。

#	シーケンス	説明	該当する業務フロー
1	認証トークン取得（DATA-EXによる認証）	データ受領者がWebAppを利用して産業用データ連携基盤が活用するDATA-EXによって認証し、認証トークンを取得する	データ発見時認可確認（限定提供データ（契約無）） データ取得時認可確認（限定提供データ（契約無）） データ取得時認可確認（限定提供データ（契約有））
2	認証トークン検証	受領者コネクタがWebAppから受け取った認証トークンを認証機能に問い合わせて検証する	データ発見時認可確認（限定提供データ（契約無）） データ取得時認可確認（限定提供データ（契約無）） データ取得時認可確認（限定提供データ（契約有））
3	認可トークン取得	認可機能が認証トークンを認証機能に問い合わせて認可トークンに交換する	データ発見時認可確認（限定提供データ（契約無）） データ取得時認可確認（限定提供データ（契約無）） データ取得時認可確認（限定提供データ（契約有））
4	認可確認	提供者コネクタが認可トークンを認可機能に渡して認可を確認する	データ発見時認可確認（限定提供データ（契約無）） データ取得時認可確認（限定提供データ（契約無）） データ取得時認可確認（限定提供データ（契約有））

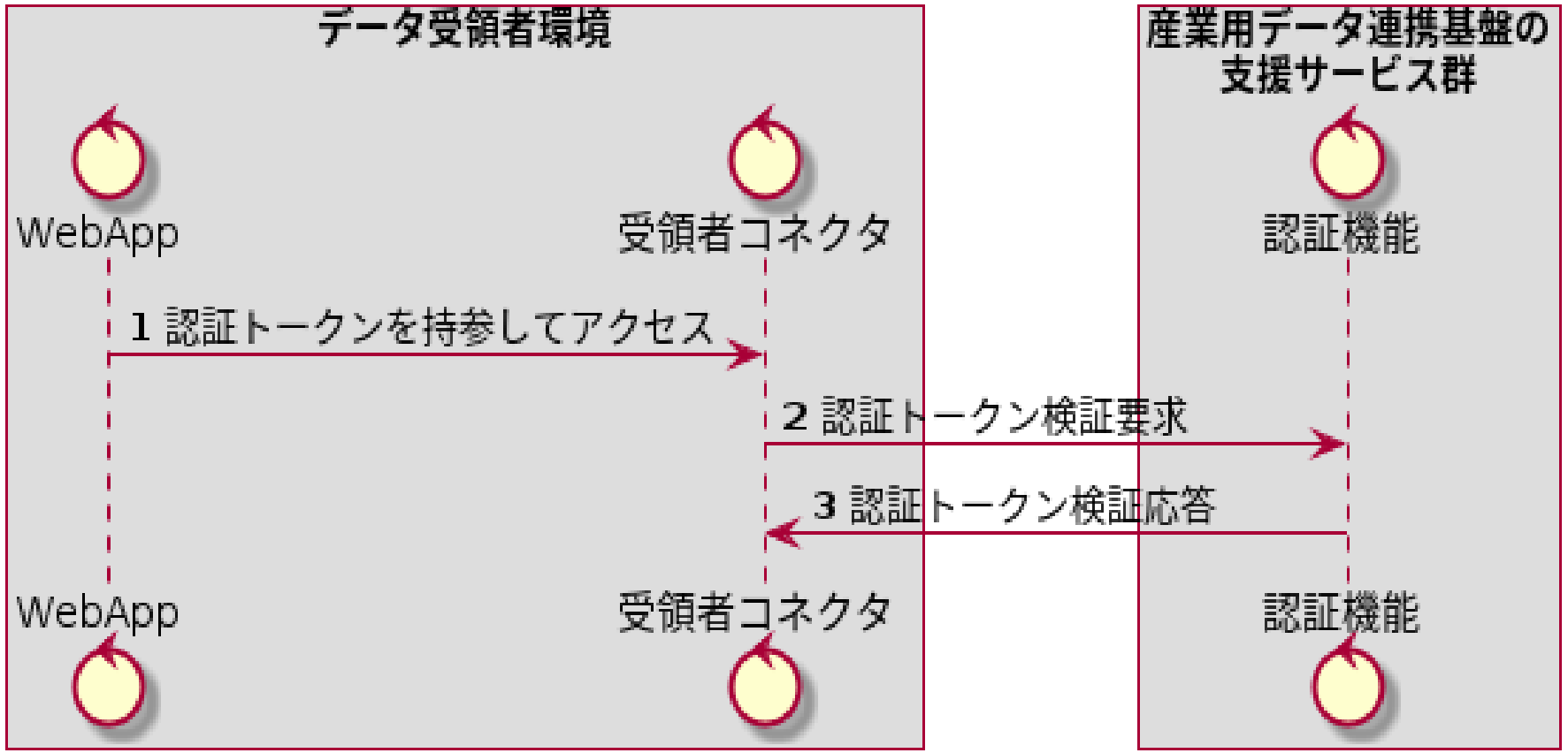
認証トークン取得（ DATA-EXによる認証）のシーケンスを示す。

データ受領者がWebAppにログインする。認証リクエストをすることによってユーザ認証を開始することができる。
ユーザ認証に成功すると認証レスポンスによって認可コードが得られ、それと引き換えに認証トークンを得ることができる。

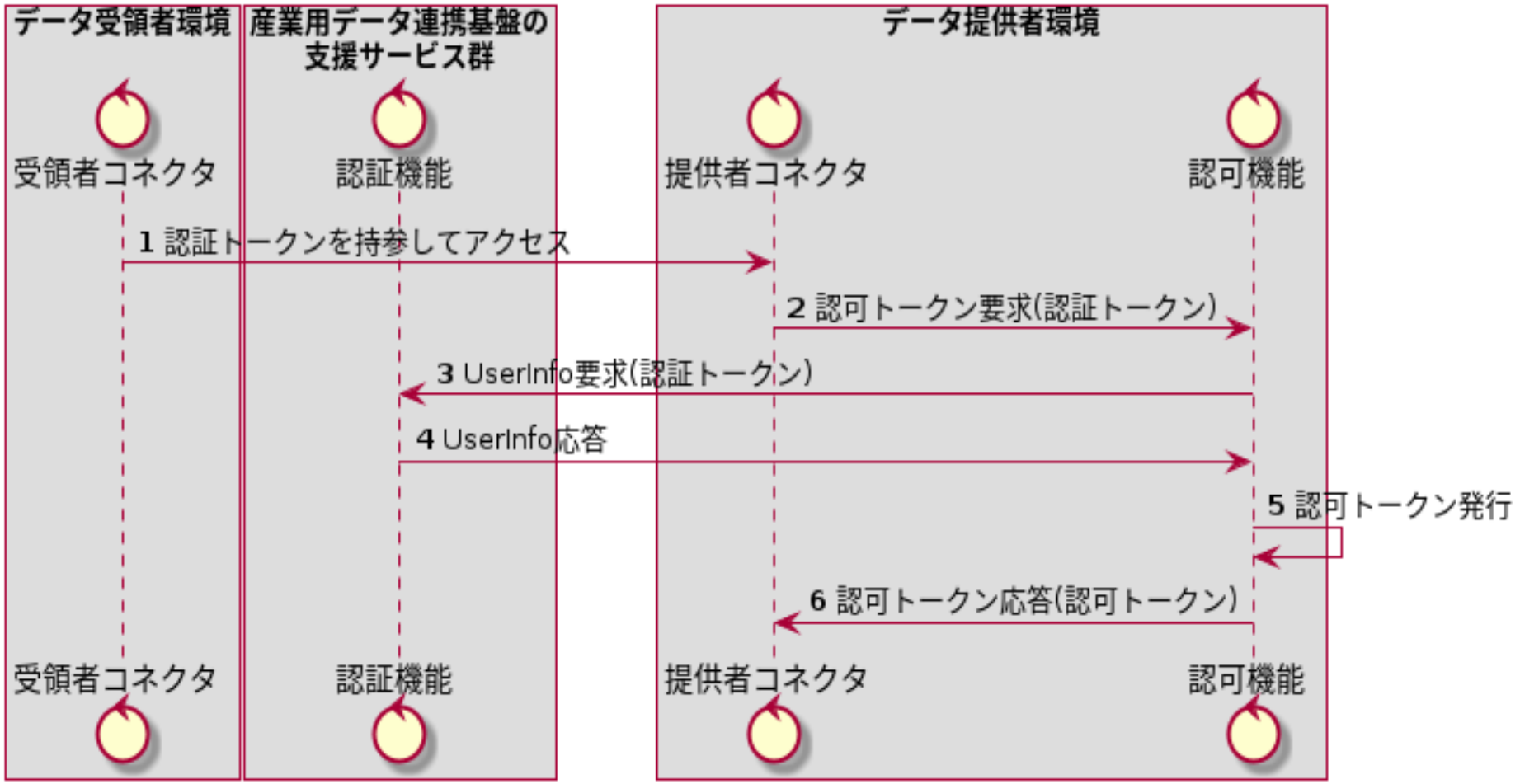
シーケンス中のパラメータについて以下に補足する。なお、認証リクエストと認証レスポンスはOpenID Connect/OAuth2.0で規定されている。
スコープとは、トークンを取得する際に権限の範囲を指定するものである。
レスポンスタイプとは、グラントタイプを指定するものである。ここでは認可コードグラントを指定している。
クライアントIDとは、認証機能がクライアントを識別するためのものである。
リダイレクトURIとは、認証機能画面からWebApp画面に戻るときのためのURIのことである。
ステートとは、認可コードのすり替え（クロスサイトリクエストフォージェリ）を防ぐために必要なランダム値である。
レスポンスモードとは、パラメータの受け渡し方法を指定するものである。
認可コードとは、 OpenID Connect/OAuth2.0で規定されている、認可コードグラントにおいてアクセストークンを取得するために必要な短命のトークンである。例えば、以下のようなランダム値である。
db377803-9bd7-401e-8f25-d7c8a0ddb0e9.cc6ccf64-1bed-4775-8a1d-2fd85c222d63.2163ff50-0e4e-4527-a52f-2aef468b9b4a
認証トークンはDATA-EX認証機能が発行するアクセストークンである。



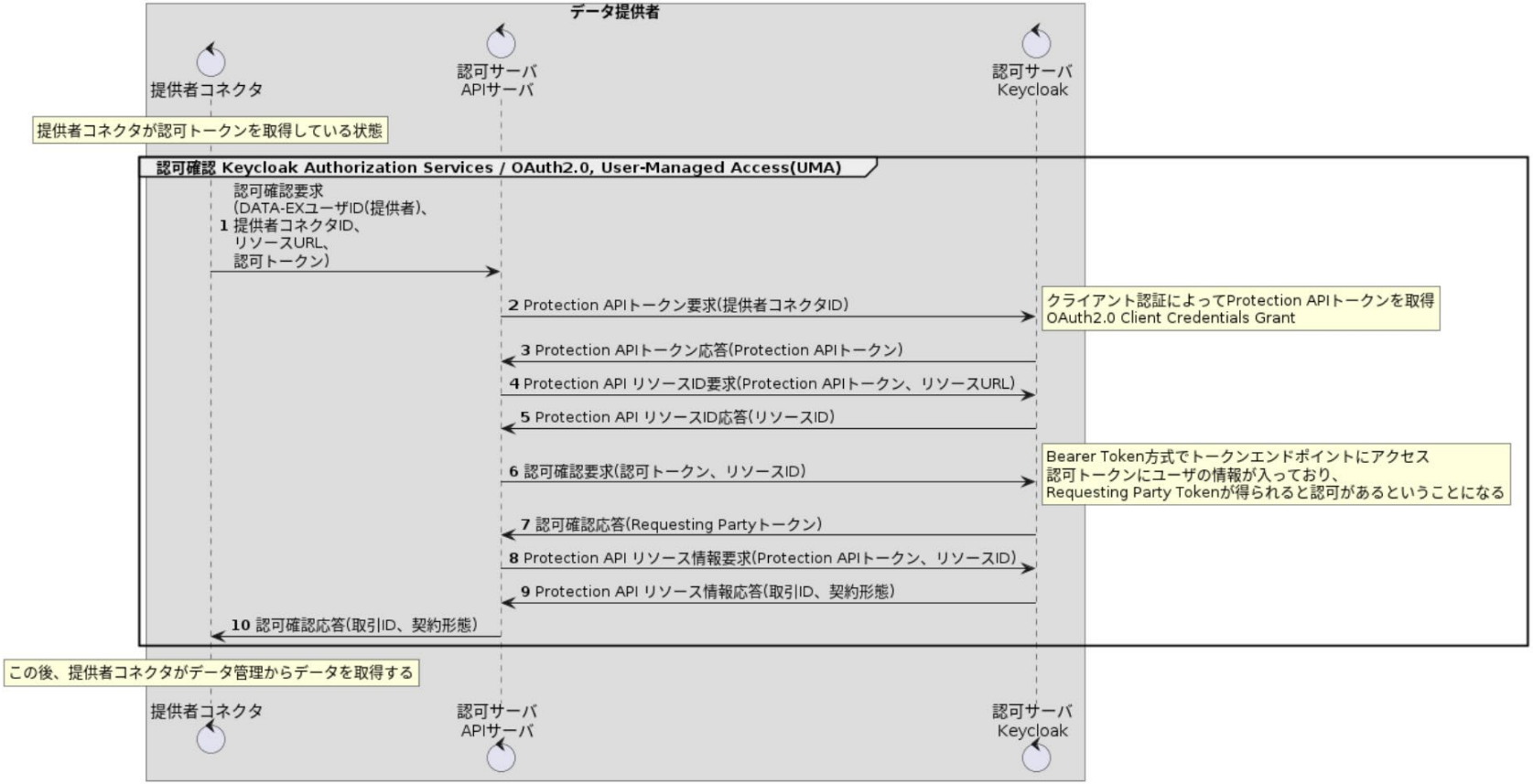
認証トークン検証のシーケンスを以下に示す。



認可トークン取得のシーケンスを以下に示す。

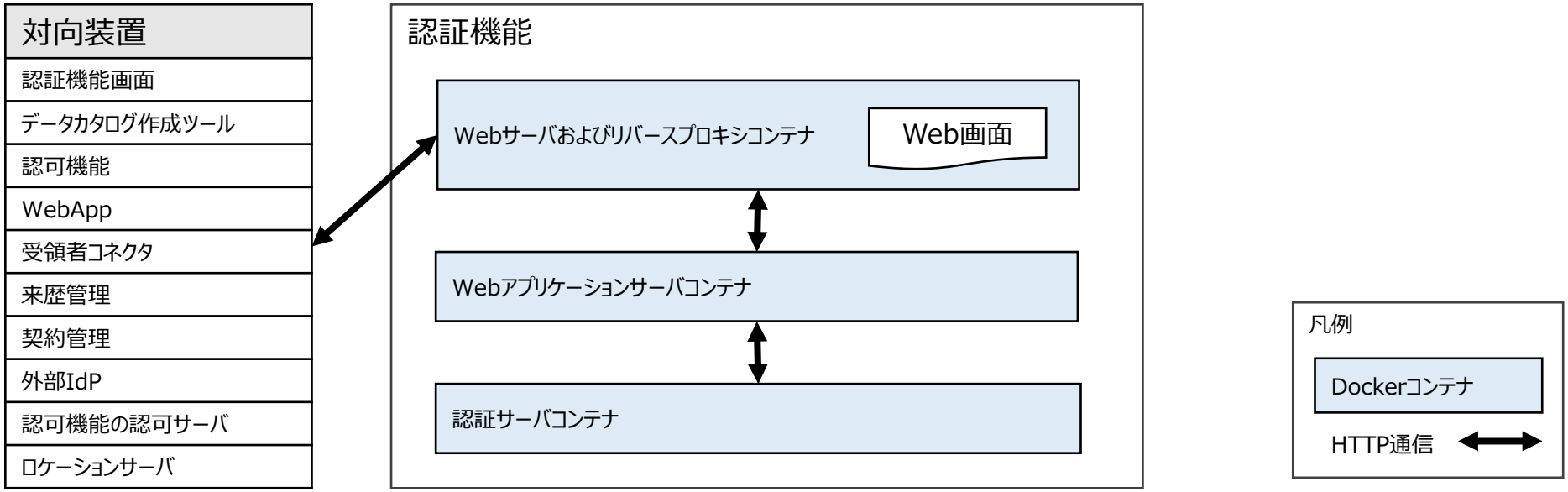


認可確認のシーケンスを以下に示す。
KeycloakのAuthorization Servicesのリソース、ポリシー、パーミッションにアクセスするにはProtection APIを利用する。
Protection APIを利用するためには、UMAに準拠したアクセストークンであるProtection APIトークンが必要となる。
https://www.keycloak.org/docs/latest/authorization_services/#querying-resources
認可確認を行うには、Bearer Token方式でトークンエンドポイントにアクセスする。
https://www.keycloak.org/docs/latest/authorization_services/#_authentication_methods



4. 認証機能

認証機能のシステム構成を以下に示す。
認証機能は内部でいくつかのコンテナが連携して機能を実現する。
運営事業者が操作するためのWeb画面を提供する。



#	OSS名	概要	バージョン	ライセンス
1	Docker	コンテナ仮想化を提供するソフトウェア	24.0.7	Apache License 2.0
2	Nginx	Webサーバおよびリバースプロキシの機能を提供するソフトウェア	1.23.1	BSD
3	FastAPI	Webアプリケーションサーバの機能を提供するソフトウェア	0.82.0	MIT
4	Keycloak	認証サーバの機能を提供するソフトウェア	19.0.2	Apache License 2.0

認証機能が提供する機能は以下の通りである。

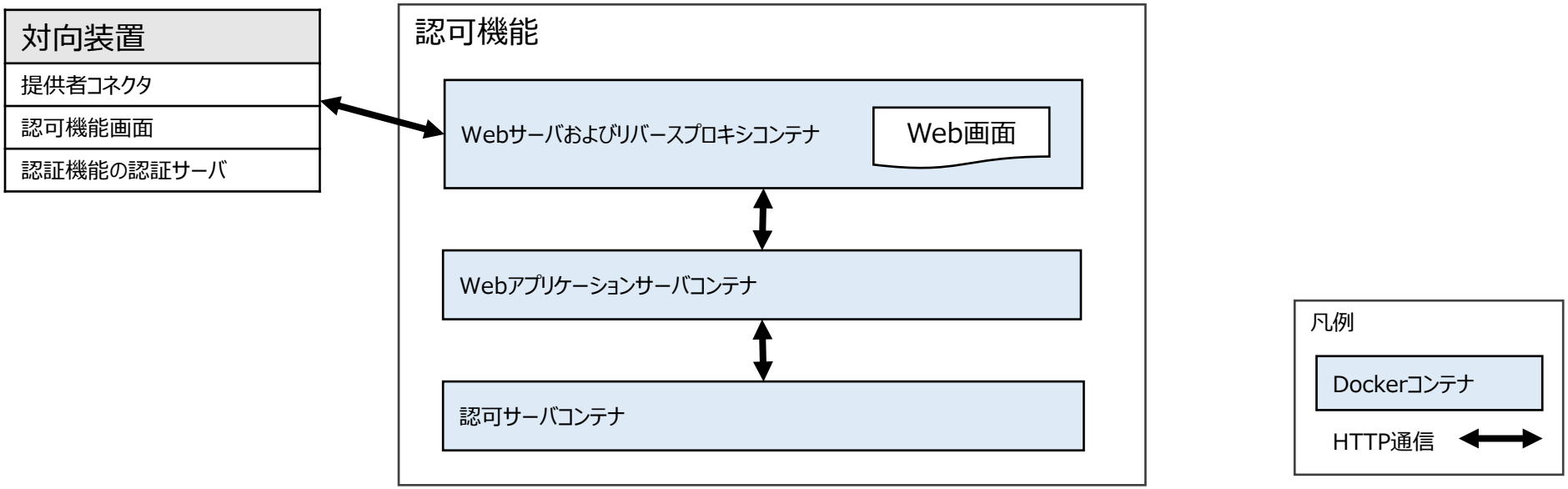
#	機能	概要
1	ユーザ管理機能	運営事業者がユーザを管理するための機能 ・ユーザの情報やクライアントの情報などを認証機能に登録する ・ユーザの情報を更新する ・ユーザの情報を削除する
2	外部IdP管理機能	運営事業者が外部IdPを管理するための機能 ・外部IdP情報を閲覧する ・外部IdP情報を登録する ・外部IdP情報を削除する
3	認証トークン管理機能	認証トークンを管理する機能 ・認証トークンを発行する ・認証トークンを検証する
4	外部IdP連携機能	外部IdPと連携する機能 アイデンティティブローカリングによって、ユーザが外部IdPで認証に成功すると認証機能のトークンを発行する
5	認可機能連携機能	認可機能と連携する機能 認可機能が認証トークンを認可トークンに交換する際の問い合わせを受け付ける
6	参加機関管理機能	参加機関管理機能については「基本設計書_認証・認可_別紙4_参加機関管理機能.pptx」を参照のこと。

画面仕様については「基本設計書_認証・認可_別紙1_画面仕様.pptx」を参照のこと。

API仕様については「基本設計書_認証・認可_別紙2_認証機能API仕様.html」を参照のこと。

5. 認可機能

認可機能のシステム構成を以下に示す。
認可機能は内部でいくつかのコンテナが連携して機能を実現する。
データ提供者が操作するためのWeb画面を提供する。



#	OSS名	概要	バージョン	ライセンス
1	Docker	コンテナ仮想化を提供するソフトウェア	20.10.7	Apache License 2.0
2	Nginx	Webサーバおよびリバースプロキシの機能を提供するソフトウェア	1.23.1	BSD
3	FastAPI	Webアプリケーションサーバの機能を提供するソフトウェア	0.82.0	MIT
4	Keycloak	認可サーバの機能を提供するソフトウェア	19.0.2	Apache License 2.0

認可機能が提供する機能は以下の通りである。

#	機能	概要
1	認証機能連携機能 （トークン交換機能）	認証機能と連携し、認証トークンを認可トークンに交換する機能 認証トークンの有する属性を引き継いで認可機能が新しくトークンを発行する また、以下のユーザ属性が引き継がれたユーザが自動作成される ・user ・org ・aal ・extras
2	認可情報管理機能	データ提供者や契約管理（提供者コネクタが中継）が認可情報を管理する機能 ・認可情報を閲覧する ・認可情報を登録する ・認可情報を削除する

画面仕様については「基本設計書_認証・認可_別紙1_画面仕様.pptx」を参照のこと。

API仕様については「基本設計書_認証・認可_別紙3_認可機能API仕様.html」を参照のこと。

付録

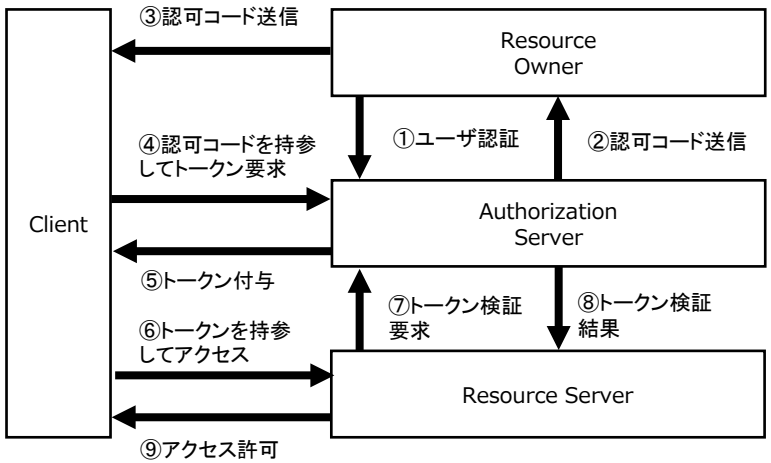
OpenID Connect/OAuth2.0のアクセス制御について

DATA-EXのトークンをベースとしたアクセス制御はOpenID Connect/OAuth2.0の仕様に基づいている。
OpenID ConnectはOAuth2.0をもとにしたプロトコルである。以下ではOAuth2.0の用語をもとに説明をする。
OAuth2.0ではいくつかのロールが定義されており、ロール間のフローがグラントタイプとしていくつか定義されている。（ロールとグラントタイプの一覧は下表）
DATA-EXでは、グラントタイプとしてAuthorization CodeとResource Owner Password Credentialsを採用する。（それぞれのフローは下図）

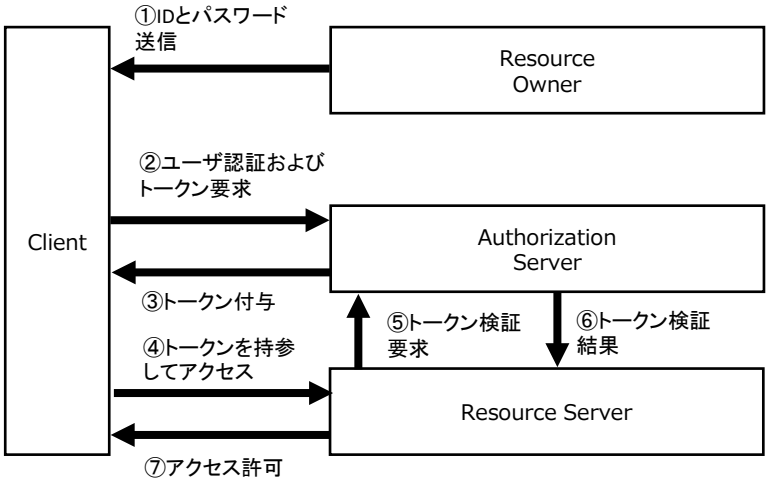
#	OAuth2.0のロール	説明
1	Resource Owner	ユーザ
2	Client	Resource Serverにアクセスするアプリケーション
3	Resource Server	Clientからアクセスされるサーバ
4	Authorization Server	トークンの発行と検証を行うサーバ

#	OAuth2.0のグラントタイプ	説明
1	Authorization Code	フロー中で認可コードを用いる方式
2	Resource Owner Password Credentials	ClientがResource OwnerのIDとパスワードを受け取る方式

グラントタイプがAuthorization Codeの場合



グラントタイプがResource Owner Password Credentialsの場合



JWTの標準的なクレーム

JWTの仕様として登録されているクレーム(Registered Claim Names)を以下に示す。
必須とされているクレームはなく、どのようなクレームを用いるかは個々のアプリケーションで定めてよいとされている。
https://tex2e.github.io/rfc-translater/html/rfc7519.html

#	クレーム名	簡易説明	説明
1	iss	Issuer	"iss"（発行者）クレームは、JWTを発行したプリンシパルを識別します。このクレームの処理は、一般にアプリケーション固有です。「iss」値は、StringOrURI値を含む大文字と小文字が区別される文字列です。このクレームの使用はオプションです。
2	sub	Subject	"sub"（サブジェクト）クレームは、JWTのサブジェクトであるプリンシパルを識別します。 JWTのクレームは通常、主題に関する記述です。サブジェクトの値は、発行者のコンテキストでローカルに一意であるか、グローバルに一意である必要があります。このクレームの処理は、一般にアプリケーション固有です。「sub」の値は、StringOrURI値を含む大文字と小文字が区別される文字列です。このクレームの使用はオプションです。
3	aud	Audience	"aud"（audience）クレームは、JWTの対象となる受信者を識別します。 JWTを処理することを目的とした各プリンシパルは、オーディエンスクレームの値で自身を識別しなければなりません。このクレームが存在するときに、クレームを処理するプリンシパルが「aud」クレームの値で自分自身を識別しない場合、JWTは拒否される必要があります。一般的なケースでは、「aud」値は、それぞれがStringOrURI値を含む、大文字と小文字を区別する文字列の配列です。 JWTが1つのオーディエンスを持つ特殊なケースでは、「aud」値は、StringOrURI値を含む単一の大文字と小文字を区別する文字列である場合があります。オーディエンス値の解釈は、一般にアプリケーション固有です。このクレームの使用はオプションです。
4	exp	Expiration Time	「exp」（有効期限）クレームは、JWTが処理のために受け入れられてはならない有効期限を識別します。「exp」クレームの処理では、現在の日付/時刻が「exp」クレームにリストされている有効期限の日付/時刻より前でなければならない（MUST）。実装者は、クロックスキューを考慮するために、通常は数分以内の多少の余裕を提供できます（MAY）。その値は、NumericDate値を含む数値でなければなりません。このクレームの使用はオプションです。
5	nbf	Not Before	「前」ではなく「nbf」クレームは、JWTが処理のために受け入れられてはならない時間を識別します。「nbf」クレームの処理では、現在の日付/時刻が、「nbf」クレームにリストされている前の日付/時刻以降である必要があります。実装者は、クロックスキューを考慮するために、通常は数分以内の多少の余裕を提供できます（MAY）。その値は、NumericDate値を含む数値でなければなりません。このクレームの使用はオプションです。
6	iat	Issued At	「発行」された「iat」クレームは、JWTが発行された時間を識別します。このクレームは、JWTの古さを判別するために使用できます。その値は、NumericDate値を含む数値でなければなりません。このクレームの使用はオプションです。
7	jti	JWT ID	「jti」（JWT ID）クレームは、JWTの一意の識別子を提供します。識別子の値は、同じ値が別のデータオブジェクトに誤って割り当てられる可能性が無視できる程度であることを保証する方法で割り当てる必要があります。アプリケーションが複数の発行者を使用する場合、異なる発行者によって生成された値間の衝突も防止する必要があります。「jti」クレームは、JWTが再生されないようにするために使用できます。「jti」値は、大文字と小文字が区別される文字列です。このクレームの使用はオプションです。

IDトークンのクレーム

OpenID Connect 1.0で定められたIDトークンのクレームを以下に示す。必須のクレームもいくつか定められている。
http://openid-foundation-japan.github.io/openid-connect-core-1_0.ja.html#IDToken

#	クレーム名	必須	説明
1	iss	○	REQUIRED. レスポンスを返した Issuer の Issuer Identifier. iss 値は, https スキーマで始まる大文字小文字を区別する URL であり, スキーマ, ホスト, そして任意でポート番号とパスを含む. クエリーとフラグメントは含まない.
2	sub	○	REQUIRED. Subject Identifier. Client に利用される前提で, Issuer のローカルでユニークであり再利用されない End-User の識別子. (例: 24400320 や AItOawmwtWwcT0k51BayewNvutrJUqsvl6qs7A4 等) この値は ASCII で255文字を超えてはならない (MUST NOT). sub 値は大文字小文字を区別する.
3	aud	○	REQUIRED. ID Token の想定されるオーディエンス (Audience). この値は Relying Party の OAuth 2.0 client_id を含まなければならない (MUST). 他のオーディエンスの識別子を含んでもよい (MAY). 一般的には aud は大文字小文字を区別した文字列の配列であるが, オーディエンスが単体の場合は aud 値を大文字小文字を区別した単一文字列としてもよい (MAY).
4	exp	○	REQUIRED. ID Token の有効期限. この有効期限以降に該当 ID Token を受け入れたり処理してはならない (MUST NOT). ある ID Token が有効期限内であるためには, この値が示す時刻より現在時刻が前でなければならない (MUST). 実装者は, 通常数分以内で, 時計のズレを考慮して多少の猶予期間を設けてもよい (MAY). この値は UTC 1970-01-01T0:0:0Z から該当時刻までの秒数を示す JSON 数値である. 詳細は RFC 3339 [RFC3339] を参照のこと.
5	iat	○	REQUIRED. JWT 発行時刻. この値は UTC 1970-01-01T0:0:0Z から該当時刻までの秒数を示す JSON 数値である.
6	auth_time	__	End-User の認証が発生した時刻. この値は UTC 1970-01-01T0:0:0Z から該当時刻までの秒数を示す JSON 数値である. リクエストに max_age が含まれていた場合, この Claim は必須である (REQUIRED). その他の場合は任意 (OPTIONAL). (auth_time Claim は, OpenID 2.0 PAPE [OpenID.PAPE] auth_time レスポンスパラメーターに相当する)
7	nonce	__	Client セッションと ID Token を紐づける文字列値. リプレイアタック防止のために用いられる. Authentication Request で指定されたままの値を ID Token に含める. ID Token に nonce が含まれる場合, Client は Authentication Request に含めた nonce 値が ID Token に含まれる nonce Claim Value と一致することを検証しなければならない (MUST). Authentication Request に nonce が含まれていた場合, Authorization Server は ID Token に Authentication Request で受け取ったそのままの Claim Value で nonce Claim を含めねばならない (MUST). Authorization Server は, 受け取った nonce に対して上記以外のなんらの処理も行うべきではない (SHOULD). nonce は大文字小文字を区別する文字列である.
8	acr	__	OPTIONAL. Authentication Context Class Reference. 実施された認証処理が満たす Authentication Context Class を表す Authentication Context Class Reference 値を示す文字列. "0" という値は End-User 認証が ISO/IEC 29115 [ISO29115] の定める level 1 を満たさないことを意味する. 長期間有効なブラウザクッキーを用いた認証などが, "level 0" の例として挙げられる. 金銭にかかわるリソースへのアクセス認可要求時には, level 0 の認証を受け入れるべきではない (SHOULD NOT). (OpenID 2.0 PAPE [OpenID.PAPE] nist_auth_level 0 に相当する) acr 値には, 絶対 URL か RFC 6711 [RFC6711] に登録された値を用いるべきである (SHOULD). RFC 6711 [RFC6711] 登録済の値を用いる場合, RFC 6711 [RFC6711] と異なる意味でそれを用いてはならない (MUST NOT). この値の意味するところはコンテキストによって異なる可能性があるため, この Claim を利用する場合は, 関係者間で値の意味するところについて合意しておくこと. acr は大文字小文字を区別する文字列である.
9	amr	__	OPTIONAL. Authentication Methods References. 認証時に用いられた認証方式を示す識別子文字列の JSON 配列. 例として, パスワードと OTP 認証が両方行われたことを示すといったケースが考えられる. amr Claim にどのような値を用いるかは本仕様の定めるところではない. この値の意味するところはコンテキストによって異なる可能性があるため, この Claim を利用する場合は, 関係者間で値の意味するところについて合意しておくこと. amr は大文字小文字を区別する文字列である.
10	azp	__	OPTIONAL. ID Token 発行対象である認可された関係者 (authorized party). この Claim が存在する場合, その値は受け取り手の OAuth 2.0 Client ID でなければならない. この Claim は, ID Token のオーディエンス値が単一文字列であり, かつその値が azp の値と異なる場合にのみ必要となる. オーディエンスと azp 値が同値である場合にも, この Claim を含んでもよい (MAY). azp は大文字小文字を区別する文字列である.

アクセストークンのクレーム

JWTとして標準とされているクレームはいくつかある（下表のJWTの仕様）が、アクセストークンとしては、IDトークンのように必須とされているクレームはない。
https://datatracker.ietf.org/doc/html/rfc6749#section-1.4
Keycloakのクライアント設定内の「スコープ」、「クライアントスコープ」の設定で外すことができるクレームがいくつか存在する。（外すことができないクレームを以下表のKeycloakの仕様で必須とした）
独自仕様としてクレームを追加したい場合はKeycloakのマッパー設定でクレームを追加することができる。

#	クレーム名	DATA-EXの仕様	JWTの仕様	Keycloakの仕様	説明	クレーム値の例
1	exp	必須	標準	必須	トークンの有効期限(UNIX時間)	1654660700
2	iat	必須	標準	必須	トークンが発行された時刻(UNIX時間)	1654660400
3	jti	必須	標準	必須	発行者ごとトークンごとに一意な識別子	“12ff3f47-f64f-4666-bda3-4e0984d9d4e7”
4	iss	必須	標準	必須	トークン発行者の識別子	“https://example_domain/auth/realms/realm_name”
5	aud	__	標準	オプション	トークンが意図している受信者の識別子	“account”
6	sub	必須	標準	必須	トークンの主題の識別子 トークン発行者におけるユーザのUUID	“be974a5a-b2f7-44bc-a9c3-2dbefa7a062a”
7	typ	必須	__	必須	トークンの形式	“Bearer”
8	azp	必須	__	必須	認可された対象者のクライアントID	“example_client”
9	session_state	必須	__	必須	セッション状態	“c0d02a92-4d79-4456-aa6b-623b162fe2dc”
10	preferred_username	__	__	オプション	ユーザ名	“example_user”
11	email_verified	__	__	オプション	メールアドレスの検証	false
12	acr	必須	__	必須	Authentication Context Class Reference	1
13	realm_access	__	__	オプション	レルムアクセス	{ "roles": ["offline_access", "uma_authorization"] }
14	resource_access	__	__	オプション	リソースアクセス	{ "account": { "roles": ["manage-account", "manage-account-links", "view-profile"] } }
15	scope	必須	__	必須	スコープ	“email profile”

身元確認のレベル、当人認証のレベルについて

定義内容	定義LoA	LoAの詳細	
ユーザ身元確認の確からしさ	IAL（Identity Assurance Level）SP 800-63A	IAL.1	身元確認不要、自己申告の登録でよい。メールアドレスの到達確認など
		IAL.2	識別に用いられる属性をリモートまたは対面で確認する必要あり
		IAL.3	識別属性を対面で確認する必要があり。検証担当者は有資格者
ユーザ認証の確からしさ	AAL（Authentication Assurance Level）SP 800-63B	AAL.1	1要素または2要素による認証
		AAL.2	2要素認証が必須。2要素目の認証手段はソフトウェアベースも可能
		AAL.3	2要素認証が必須。2要素目の認証手段はハードウェアベースが必須

引用元：
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/093e09a7-2ffe-4a41-971a-5c0dcfd3c0b3/20220125_meeting_trust_dx_01.pdf

ワンタイムパスワードについて

Keycloakが対応しているワンタイムパスワード方式として、以下表に示すように、TOTPとHOTPがある。
TOTP、HOTPいずれにしても、それぞれのユーザがスマートフォンのOTPアプリでQRコードを読み取り、OTP認証の初期設定をする必要がある。
Keycloakのデフォルト設定では、OTP初期設定したユーザのみがOTP認証が必須となる。このため、ユーザごとに必須となる認証要素が異なってくる。
Keycloakの設定により、ユーザ全員一律でOTP認証を必須とすることも可能である。

#	OTP方式	説明	対応アプリ
1	TOTP (Time-based OTP)	時刻とシードによりワンタイムパスワードを計算する	FreeOTP Google Authenticator
2	HOTP (HMAC-based OTP)	カウンター(認証回数)とシードによりワンタイムパスワードを計算する	FreeOTP

KeycloakのOTPの仕組み