OAuth & OpenID Connect 勉強会 by Authlete - OAuth/OIDC 機能の組み込みかた

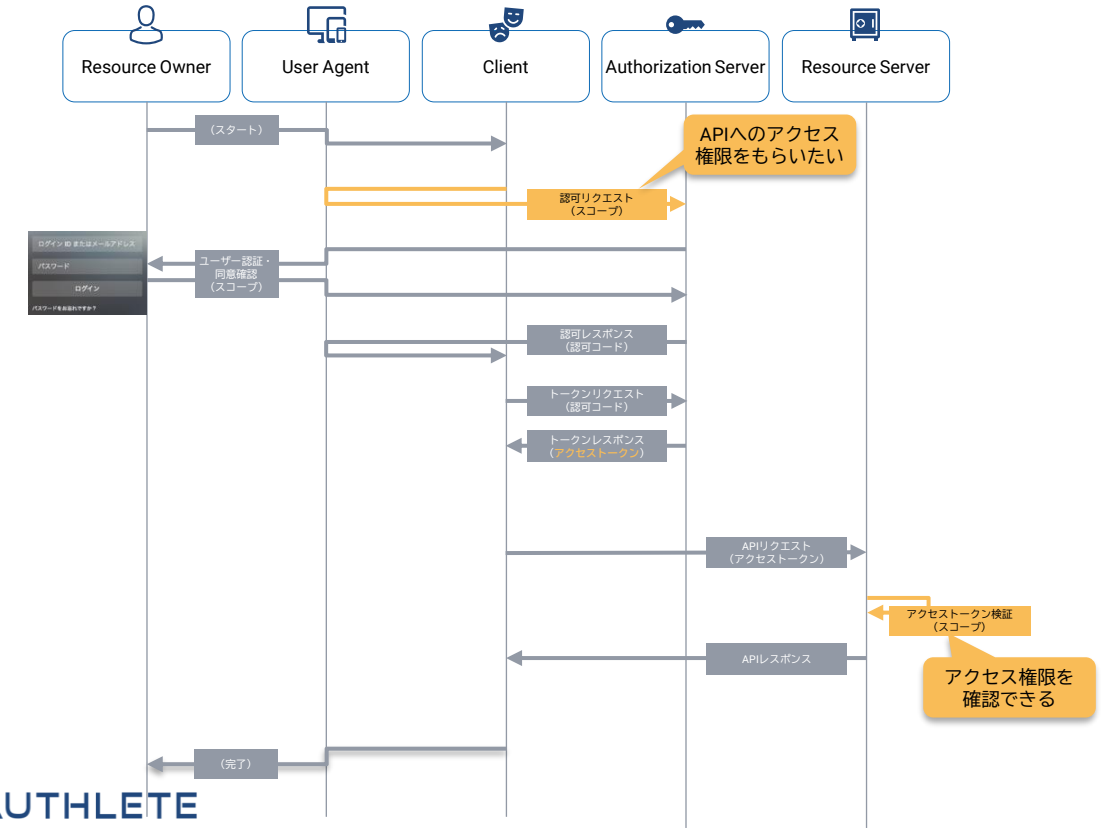
「OAuth/OIDC 化」の考えかた

工藤達雄
Authlete

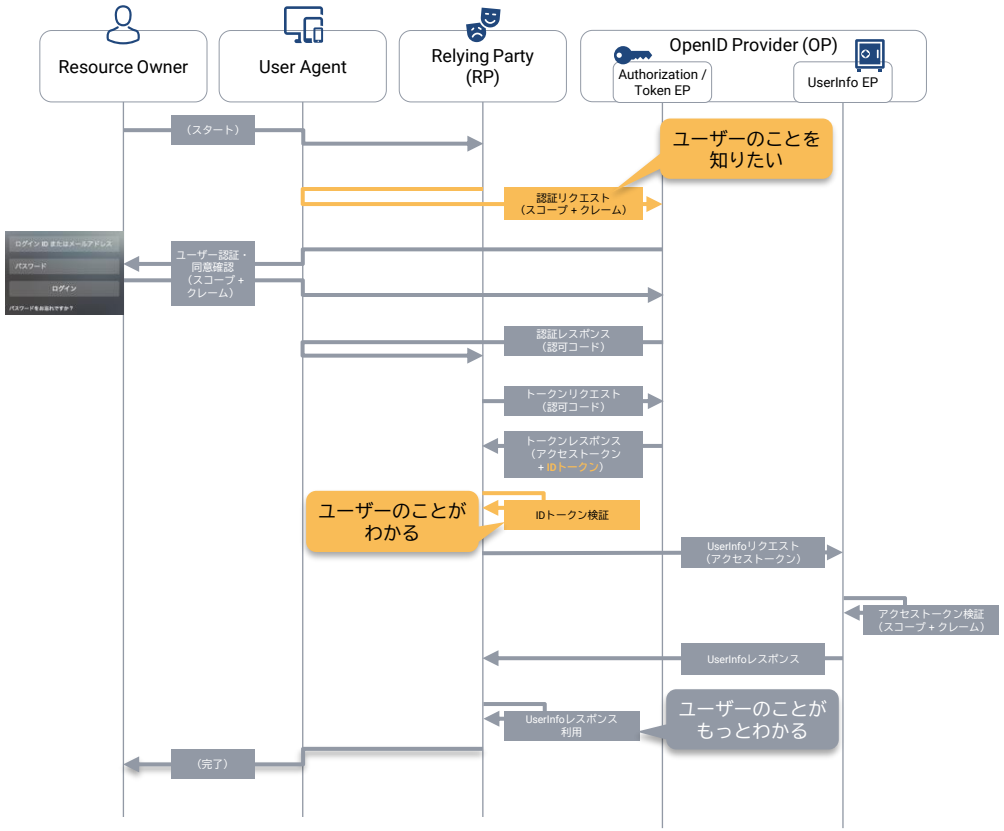
OAuth/OIDCのおさらい

- **OAuth 2.0**: 「アクセストークン」を用いた「API認可フレームワーク」
- **OpenID Connect**: 「IDトークン」を用いた「ID連携プロトコル」

Authorization Code Grant Flow / Bearer Token の例

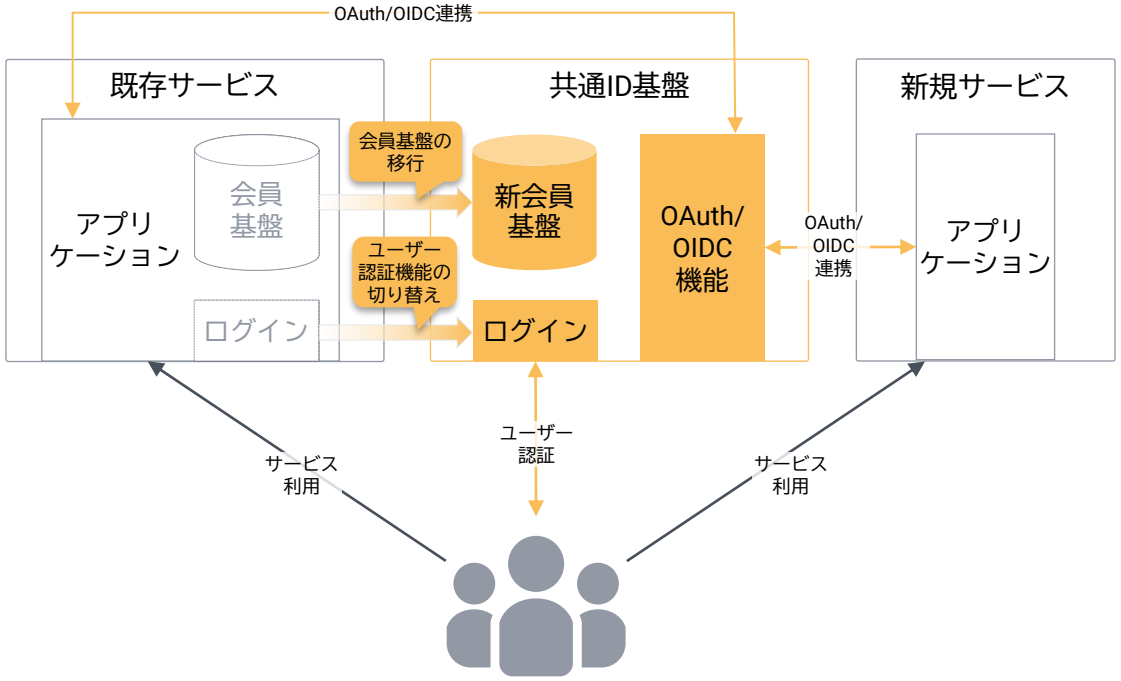


Authorization Code Flow w/ Userinfo の例



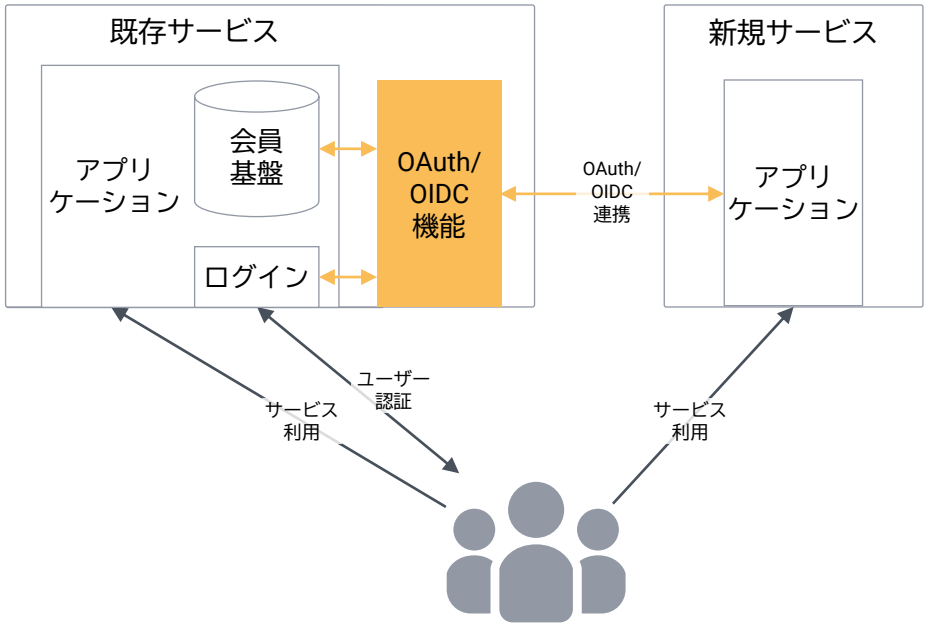
既存サービスにOAuth/OIDC機能をどう追加するか

- 既存の情報・機能をどう活かすかによって取るべきアプローチは異なる
- 王道は独立した「共通ID基盤」の構築
- ポイント
  - 会員基盤の移行やユーザー認証機能の切り替えなどが可能であること
  - かつ投資対効果が見込めること
  - CIAMソリューション、IDaaS、…



OAuth/OIDC化 – もうひとつの王道

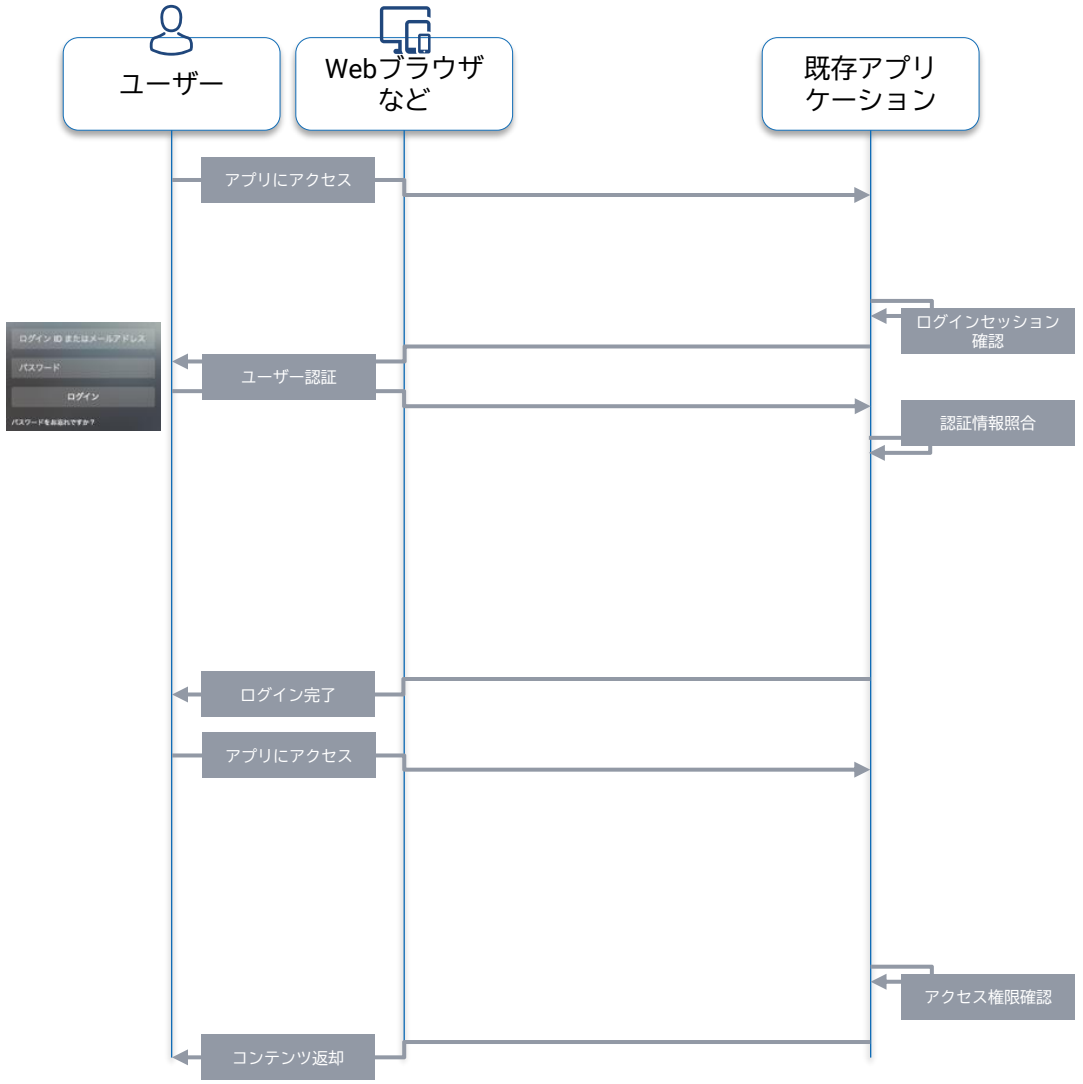
- 既存サービスにOAuth/OIDC機能を組み込む
- 既存の会員基盤やユーザー認証機能などをそのまま使う
- ユースケース例
  - 複数サービスのIDをどれかひとつに寄せたい
  - 自社の独自SSO/API認可機構を改善したい
  - 自社サービスに外部SaaSを連携させたい



既存アプリケーションの利用シーケンス

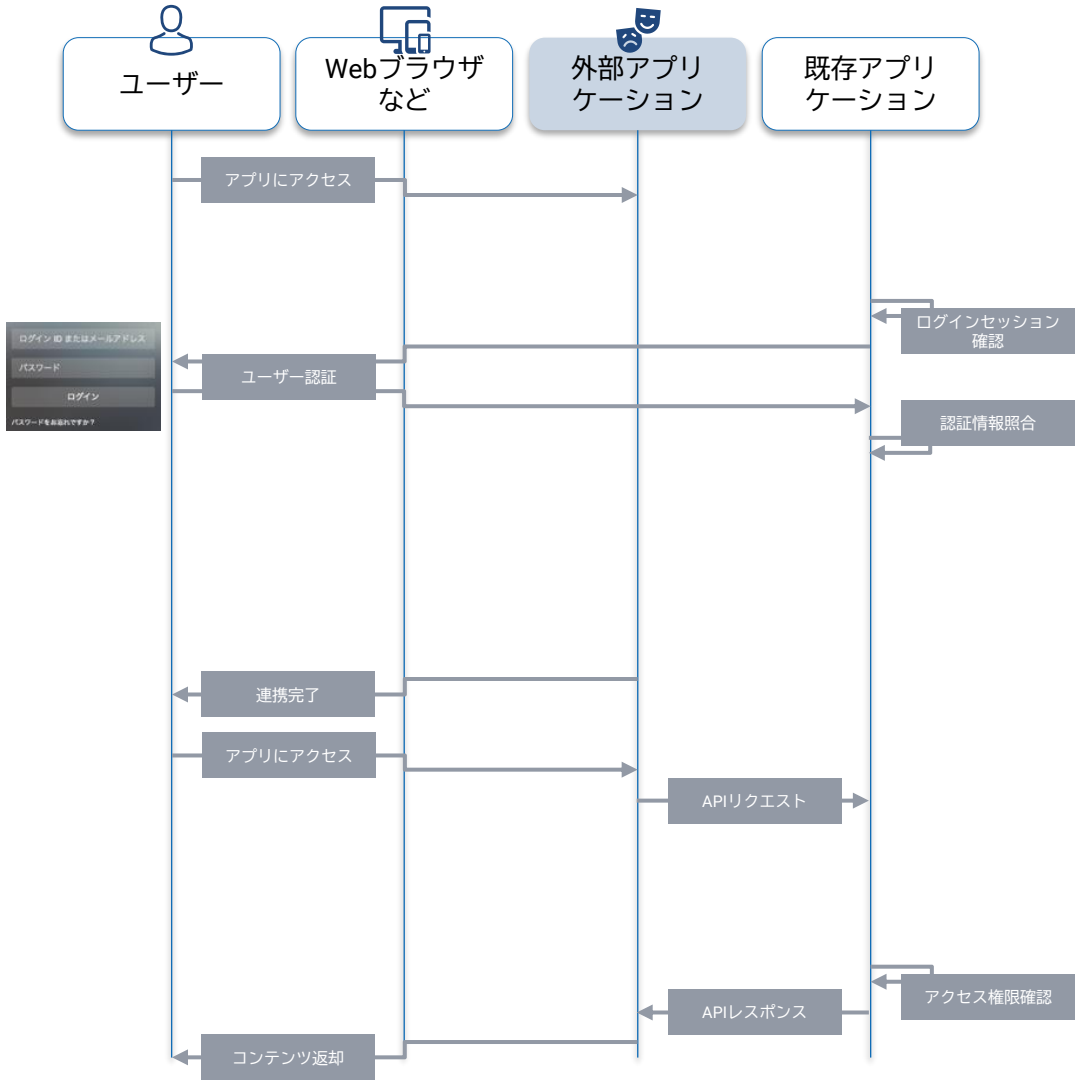
- ユーザーが既存アプリにアクセス
- 未ログインの場合、既存アプリがユーザー認証
- 既存アプリにログイン完了
- ユーザーが、ログイン済み状態で既存アプリにアクセス

- 既存アプリが、ユーザーのアクセス権限を確認し、コンテンツを返却



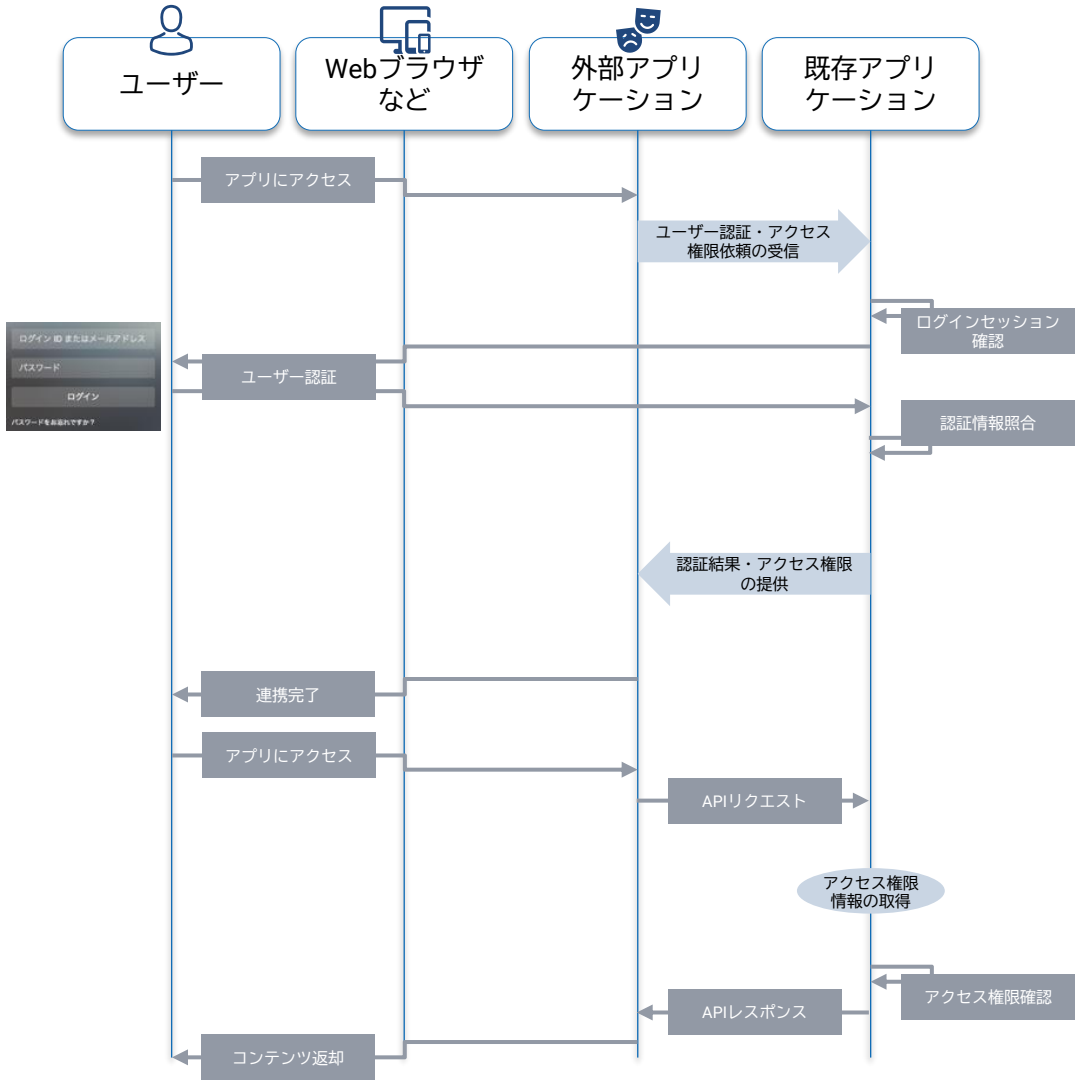
そこに別のアプリケーションが加わる

- ユーザーが外部アプリにアクセス
- 未ログインの場合、既存アプリがユーザー認証
- 既存アプリと外部アプリが連携
- ユーザーが、連携済み状態で外部アプリにアクセス
- 外部アプリがAPIにアクセス
- 既存アプリが、ユーザーのアクセス権限を確認し、APIレスポンスを返却
- 外部アプリがコンテンツを返却



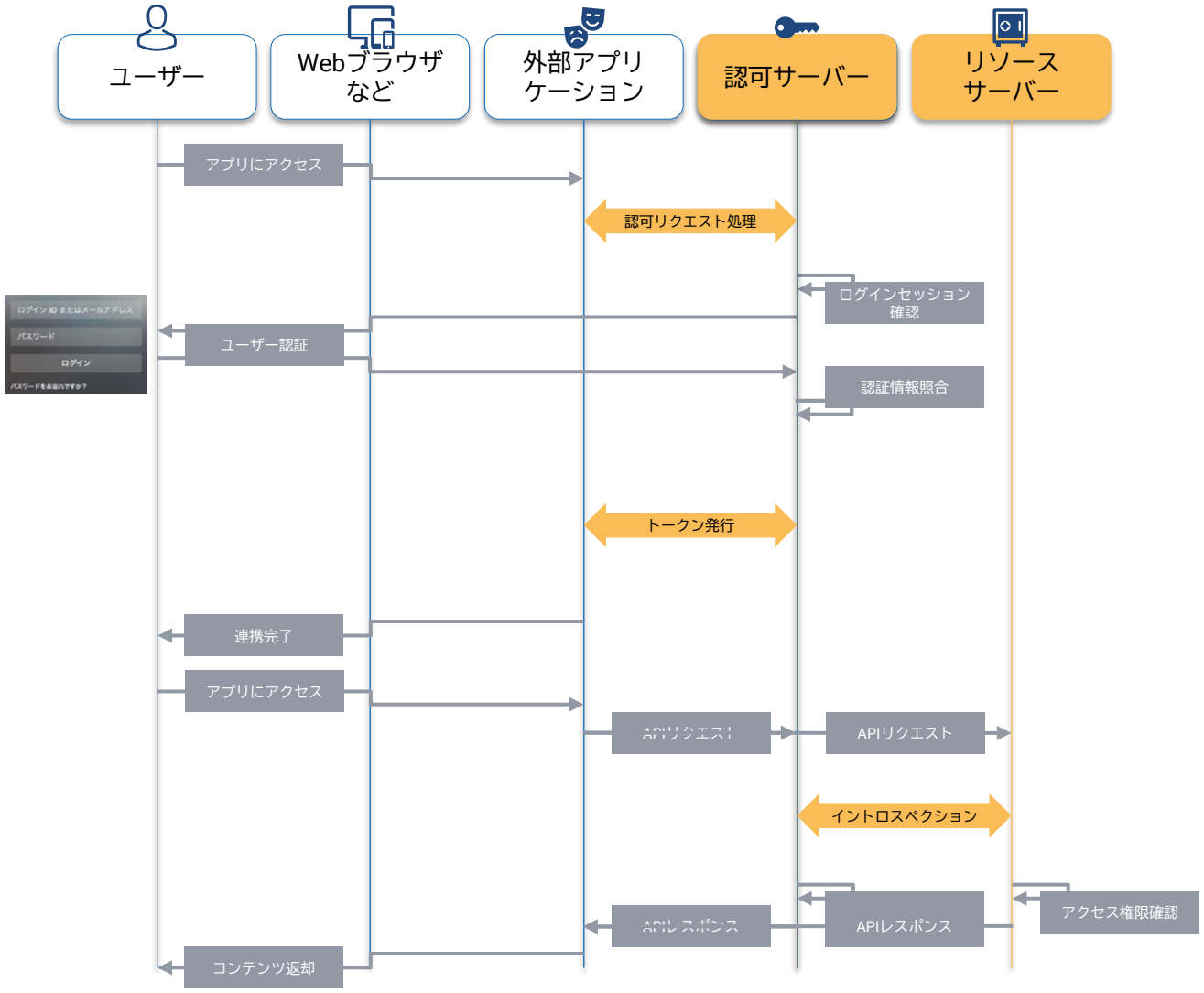
既存アプリケーション側の対応

- ユーザー認証・アクセス権限依頼の受信
  - どのようなユーザー認証・アクセス権限が求められているか? どのアプリに?
- 認証結果・アクセス権限の提供
  - どのような形式で返却する?
- APIリクエストに関するアクセス権限情報の取得
  - どうやって取得する?



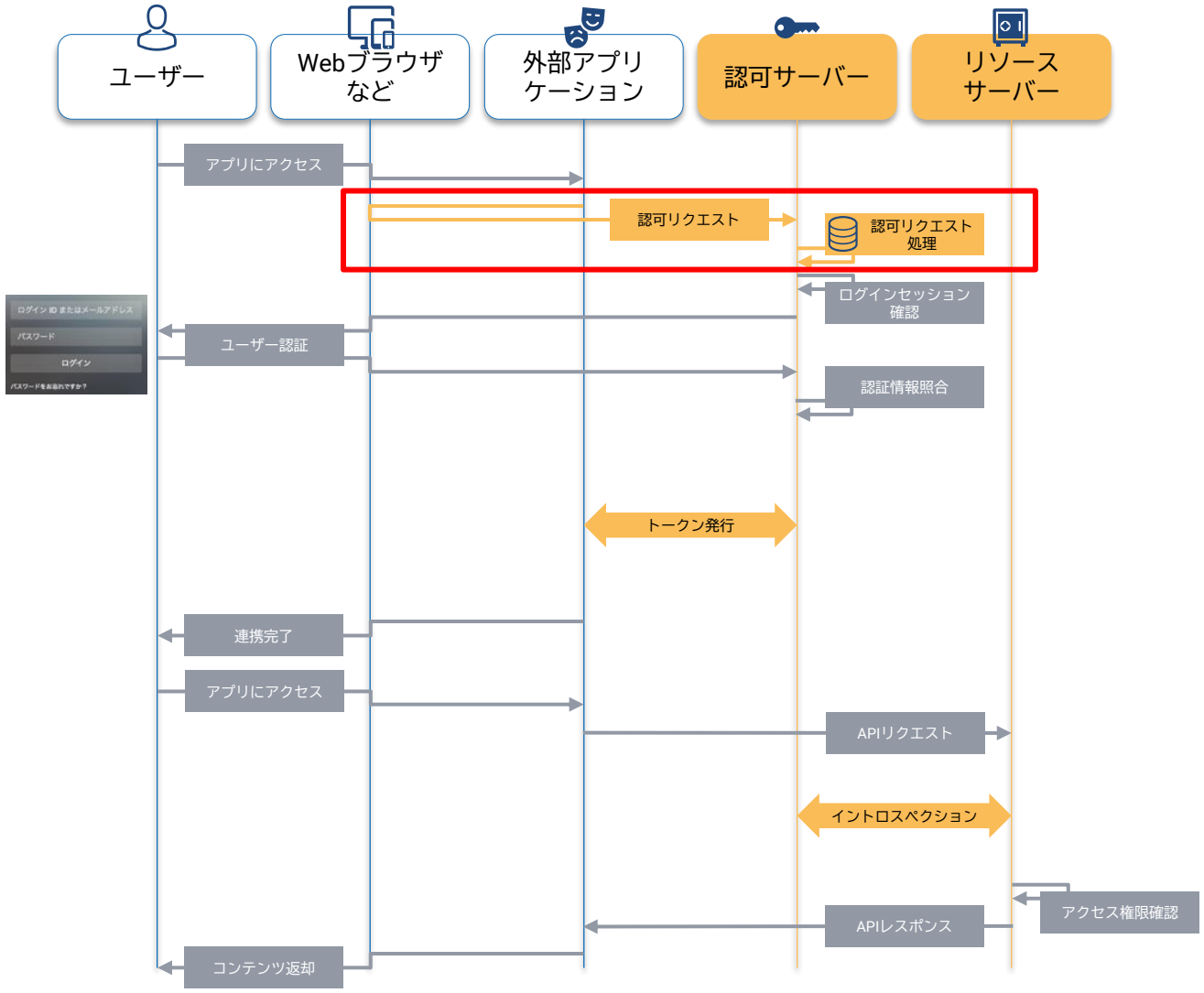
既存アプリケーションを「OAuth/OIDC化」

- アプリケーションから2つの機能を分解
  - 認可サーバー（and/or OpenIDプロバイダー）
  - リソースサーバー
- OAuth/OIDCエンドポイントを認可サーバーに実装
  - 認可リクエスト処理
  - トークン発行
  - イントロスペクション（オプション）
  - その他



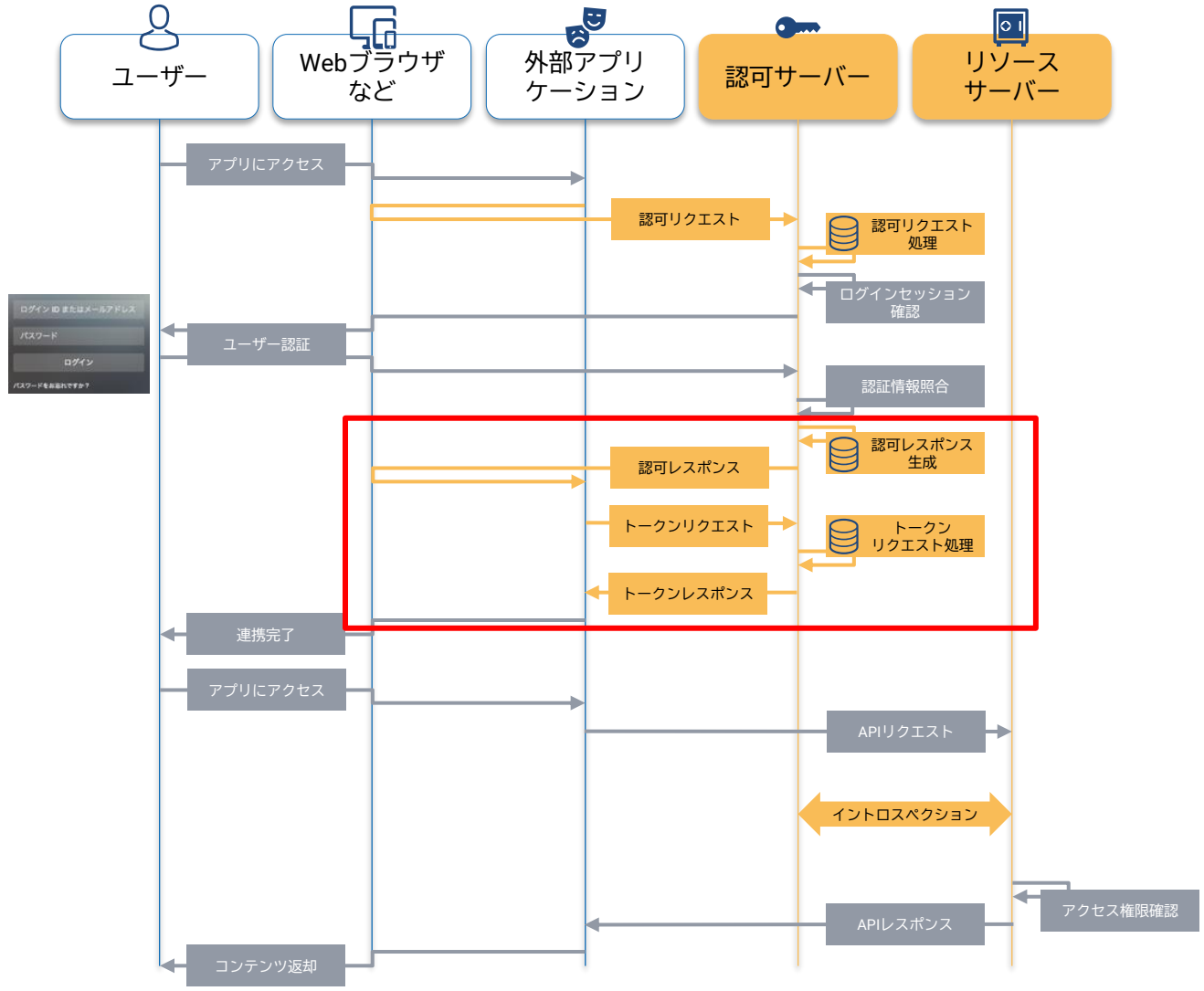
認可リクエスト処理

- 「認可エンドポイント」
  - 認可リクエストの内容を解析
  - 後続のOAuth/OIDC処理に引き継ぎ



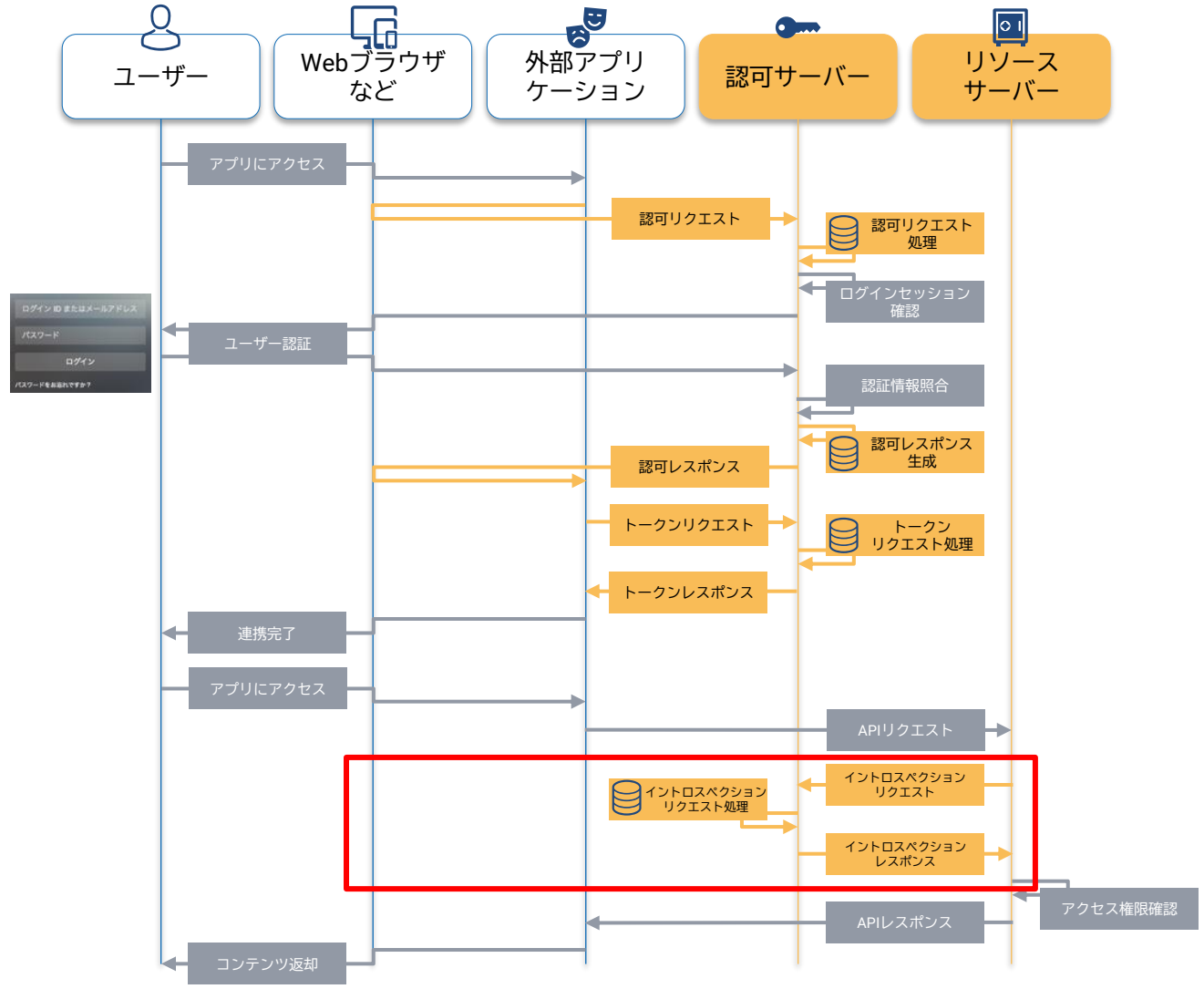
トークン発行

- 「認可レスポンス生成機能」と「トークンエンドポイント」
  - 認可リクエストと、ユーザーとのやり取りに基づき、認可レスポンスを生成
  - トークンリクエストの内容を解析
  - 認可リクエストと、ユーザーとのやり取りと、トークンリクエストに基づき、トークンレスポンスを生成
  - その後、発行したトークンのライフサイクルを管理



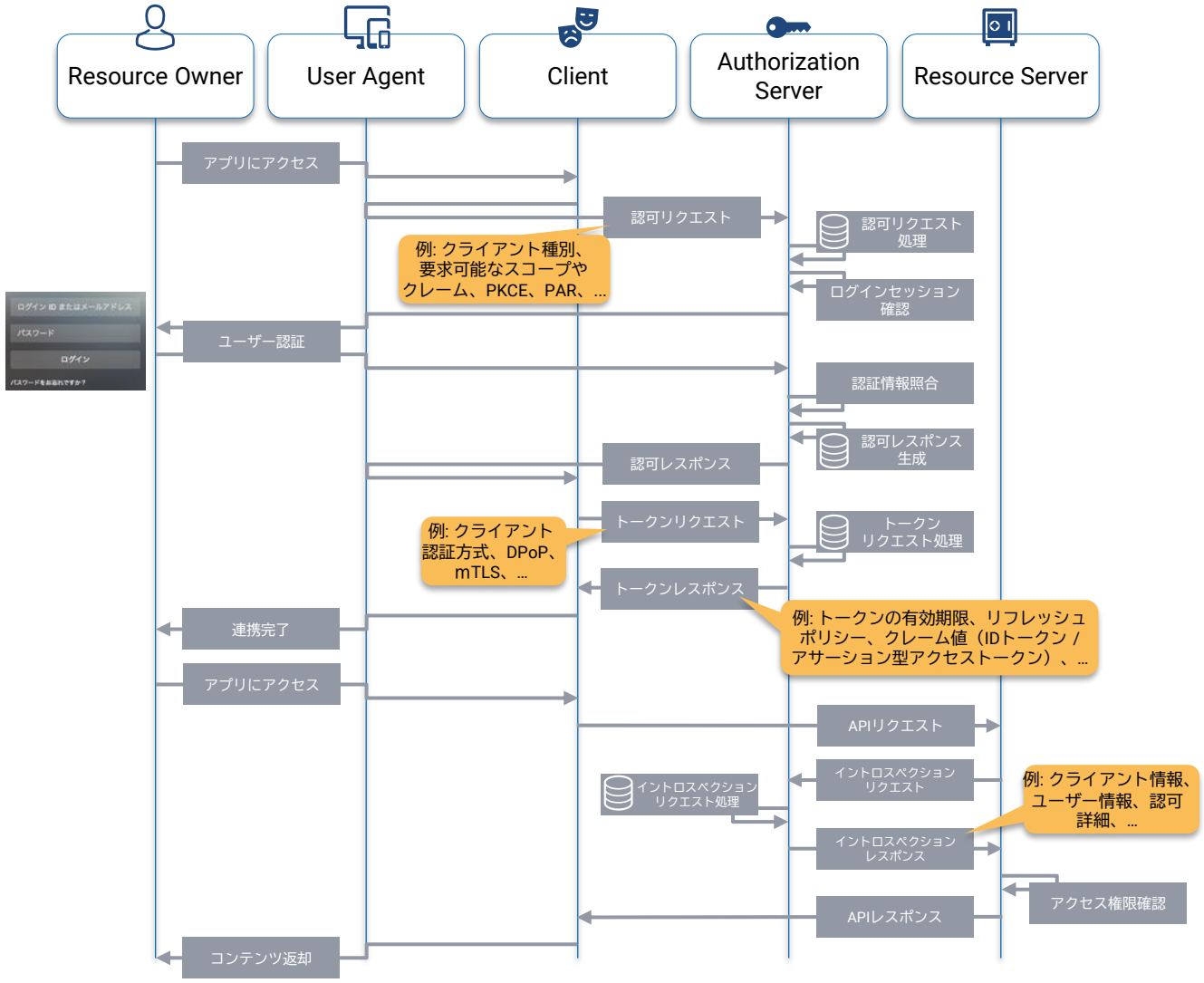
イントロスペクション（オプション）

- 「イントロスペクション エンドポイント」
  - イントロスペクション リクエストの内容を解析
  - イントロスペクション リクエストと、トークンの状態と、トークン発行のコンテクストに基づき、イントロスペクション レスポンスを生成



プロファイリング（OAuth/OIDCの詳細仕様化）

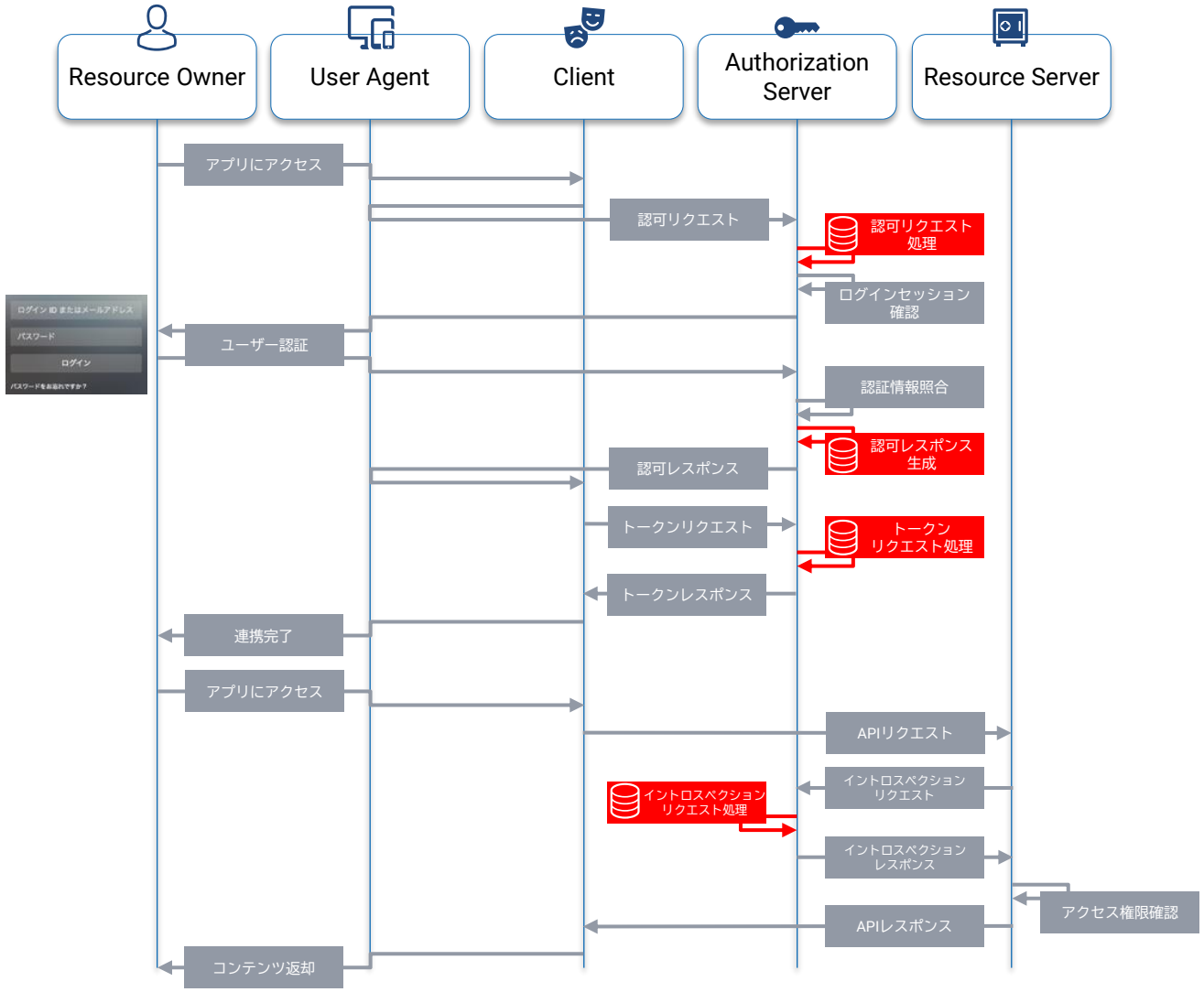
- くわしくは前回の勉強会をどうぞ
  - https://www.authlete.com/ja/resources/videos/20240618/
- ユースケース例
  - 複数サービスのIDをどれかひとつに寄せたい
    - 親サービスと、子となる複数サービスとのすり合わせ
  - 自社の独自SSO/API認可機構を改善したい
    - 既存のSSO/API認可ポリシーとOAuth/OIDC仕様とのすり合わせ
  - 自社サービスに外部SaaSを連携させたい
    - SaaSが定めるプロファイルに準拠



まとめ

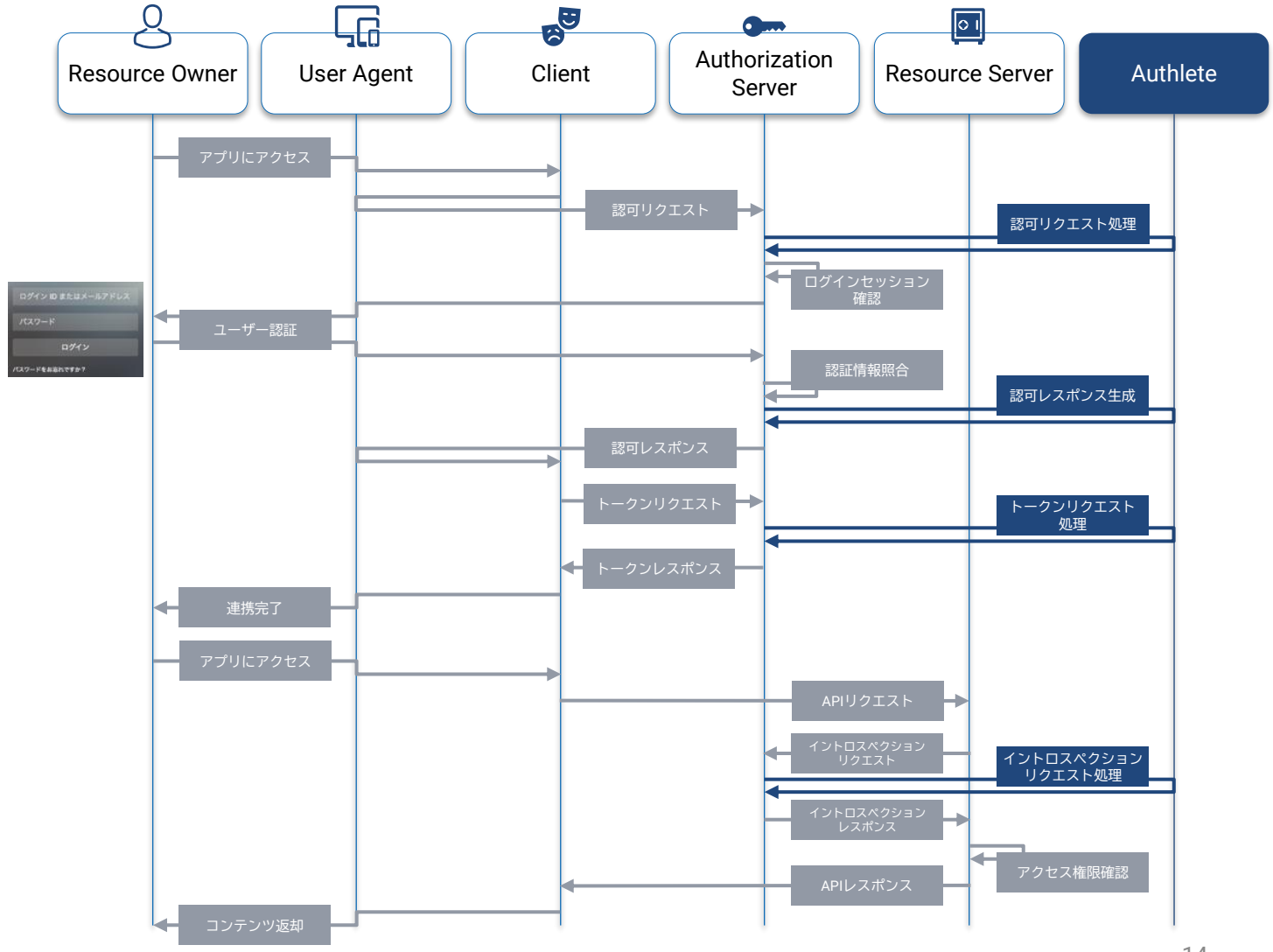
- 追加する機能
  - OAuth/OIDC共通
    - 認可リクエスト処理
    - トークンリクエスト処理
  - OAuth
    - イントロスペクションリクエスト処理
    - リボケーション、PAR、RAR、DPoP、mTLS、…
  - OIDC
    - IDトークン発行処理
    - ディスカバリー、UserInfo、…
- 必要な実装
  - OAuth/OIDCプロトコル処理
  - トークンライフサイクル管理
  - クライアント/サーバー設定管理

…大変なのでは!?



Authlete: OAuth/OIDC化に必要な実装を提供

- OAuth/OIDCリクエスト処理を代行するAPI
- トークン管理のための永続的ストレージ
- 鍵管理やクライアント設定の一元化
- ユーザー向けセルフサービスや運用者向け機能を実装するための管理API



Thank You

www.authlete.com

info@authlete.com

Palo Alto, Tokyo, Dubai

AUTHLETE

AUTHLETE

We Are Hiring!!

https://www.authlete.com/ja/careers/