目次

改訂情報

変更年月日	変更内容
2014-12-01	初版

はじめに

本書の目的

本書では intra-mart Accel Platform で提供するOAuth認証機能の仕様について述べます。

対象読者

本書は、以下の条件を満たす人を対象としています。

- intra-mart Accel Platform を理解している
- OAuth認証を利用したアプリケーションの利用者
- 以下のいずれかの条件を満たす、OAuth認証を利用したアプリケーションの開発者
  Java を理解している開発者
  サーバサイドJavaScript を理解している開発者

本書の構成

本書は、以下のような内容で構成されています。

- *概要*

  OAuth 2.0について説明しています。
- *intra-mart Accel Platform で提供している認証フロー*

  intra-mart Accel Platform で提供している認証フローについて説明しています。
- *intra-mart Accel Platform で提供しているエンドポイント*

  intra-mart Accel Platform で提供しているエンドポイントについて説明しています。
- *アクセストークンの有効期限と更新方法*

  アクセストークンの有効期限と更新方法について説明しています。

概要

OAuthとは

OAuth (Open Authorization)は、シンプルで標準的な方法でデスクトップやWebアプリケーションからセキュアにAPIへアクセスする認可を与えるオープンなプロトコルです。
ユーザは、アプリケーションがリソースを参照する際にパスワードやその他の認証情報をそれらのアプリケーションにさらすことなくアクセスを許可することができます。

intra-mart Accel Platform ではOAuth2.0の仕様に準拠した以下の認証フローを提供します。

- *認可コードによる認可*
- *インプリシットグラント*
- *アクセストークンの更新*

OAuth2.0の仕様や用語については、以下を参照してください。

[RFC 6749 - The OAuth 2.0 Authorization Framework]

intra-mart Accel Platform で提供している認証フロー

intra-mart Accel Platform では以下の認証フローを提供しています。

- *認可コードによる認可*
- *インプリシットグラント*
- *アクセストークンの更新*

それぞれの認証フローは、以下の場合に使用します。

- *認可コードによる認可*

  WebアプリケーションからOAuth認証を利用する場合に使用します。

- *インプリシットグラント*

  ネイティブなモバイルやデスクトッププリケーションのようなクライアントアプリケーションからOAuth認証を利用する場合に使用します。

- *アクセストークンの更新*

  発行されたアクセストークンの有効期限が切れ、新しいアクセストークンを取得する場合に使用します。

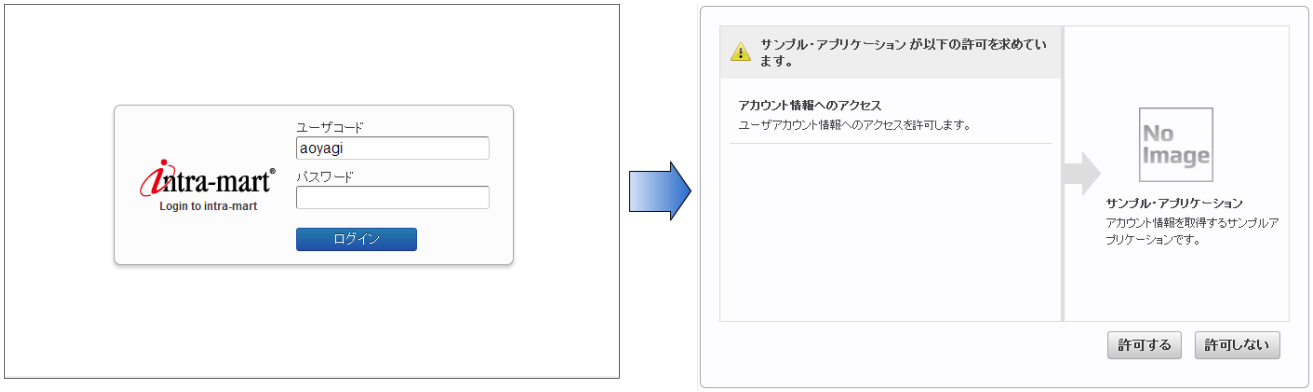
認可コードによる認可

認可コードによる認可は、クライアントアプリケーションがユーザに直接認可を要求する代わりに、ユーザを認可サーバ（ intra-mart Accel Platform ）へリダイレクトさせ、ユーザがリダイレクトして戻ってきた際に認可コードを取得します。

認可コードは認可サーバで作成され、クライアントアプリケーションにブラウザ経由で渡される、ユーザのアクセス許可を表す短期間のトークンです。
クライアントアプリケーションは認可コードとクライアントの認証情報を認可サーバに送りアクセストークンを取得します。

認可コードによる認可フロー

1. ユーザがブラウザより、クライアントアプリケーションを実行します。
2. クライアントアプリケーションはユーザのブラウザに認可エンドポイントへリダイレクトするレスポンスを返します。
3. 認可サーバはユーザ認証を行い、クライアントアプリケーションのアクセス許可をたずねます。



4. ユーザがアクセスを許可した場合、指定されたリダイレクトURIを用いて認可コードをクライアントアプリケーションに受け渡します。

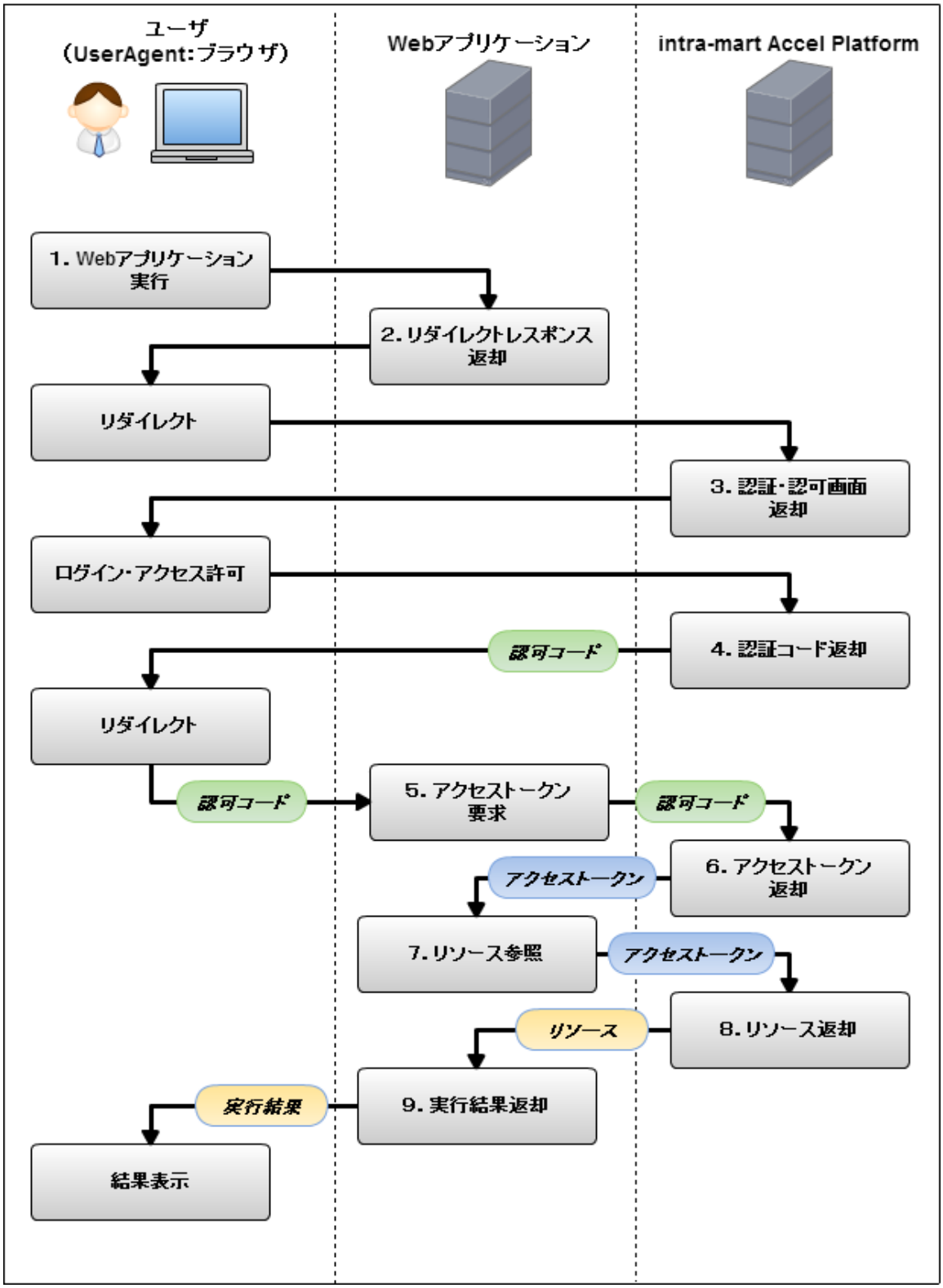
5. クライアントアプリケーションは受け渡された認可コードを用いて、トークンリクエストを送信します。

6. 認可サーバは、認可コードおよびクライアントアプリケーションの認証情報（クライアントシークレット）を検証し、クライアントアプリケーションへアクセストークンおよびリフレッシュトークンを返却します。

7. クライアントアプリケーションは取得したアクセストークンを用いて intra-mart Accel Platform 上のリソースへアクセスします。

8. intra-mart Accel Platform はアクセストークンを検証してリソースを返却します。

9. クライアントアプリケーションは取得したリソースを用いて処理を行い、結果をユーザへ返却します。

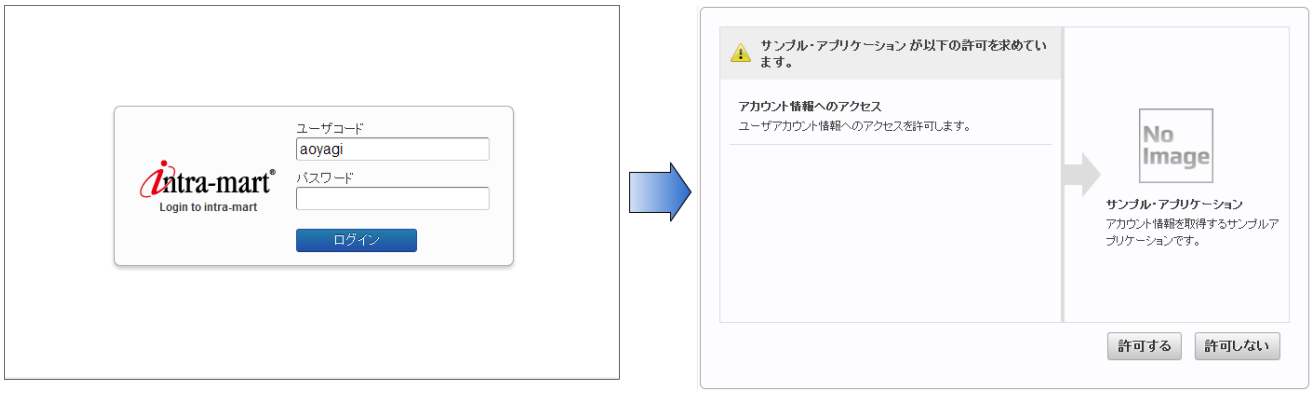


インプリシットグラント

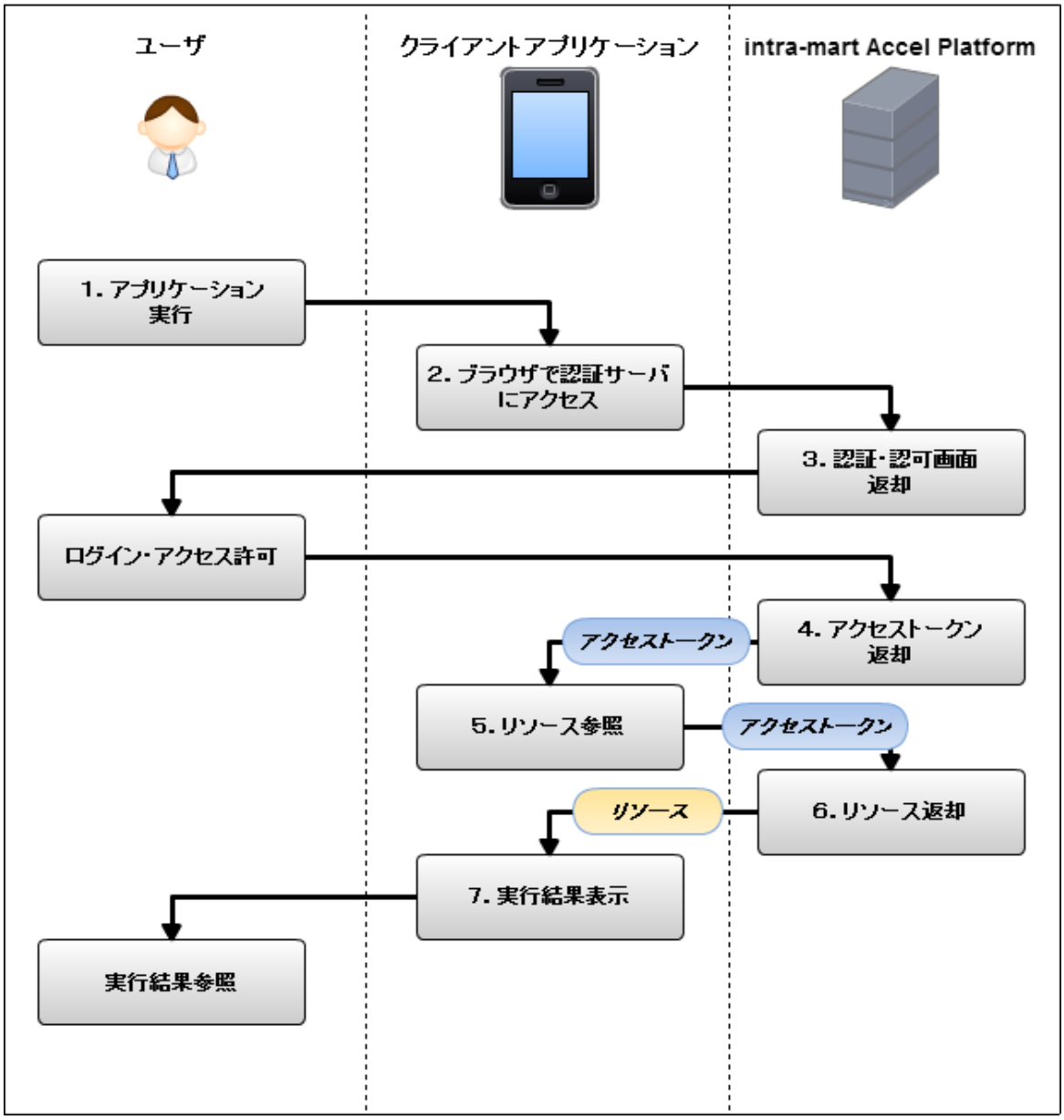
インプリシットグラントフローは、モバイルやデスクトップ上で動作するクライアントアプリケーションでOAuth認証を利用する場合に使用します。
ユーザのコンピュータ、または、デバイスで実行されるアプリケーションではアプリケーション毎の共通の機密情報を安全に保護することができない可能性があります。
そのため、インプリシットグラントフローではクライアントを認証せずにアクセストークンを発行します。（ただし、クライアントにアクセストークンを渡す際に使用されるリダイレクトURIをもとに、クライアントの身元が検証可能なこともあります。）

インプリシットグラントフロー

1. ユーザがクライアントアプリケーションを実行します。
2. クライアントアプリケーションはユーザのブラウザを起動して認可エンドポイントへリクエストを送信します。
3. 認可サーバはユーザ認証を行い、クライアントアプリケーションのアクセス許可をたずねます。



4. ユーザがアクセスを許可した場合、指定されたリダイレクトURIを用いてアクセストークンをクライアントアプリケーションに受け渡します。
5. クライアントアプリケーションは取得したアクセストークンを用いて intra-mart Accel Platform 上のリソースへアクセスします。
6. intra-mart Accel Platform はアクセストークンを検証してリソースを返却します。
7. クライアントアプリケーションは取得したリソースを用いて処理を行い、結果をユーザへ返却します。



コラム

- インプリシットグラントフローでは、リフレッシュトークンは発行されません。
  アクセストークンの有効期限が過ぎた場合、再度上記の手順でアクセストークンを取得する必要があります。

アクセストークンの更新

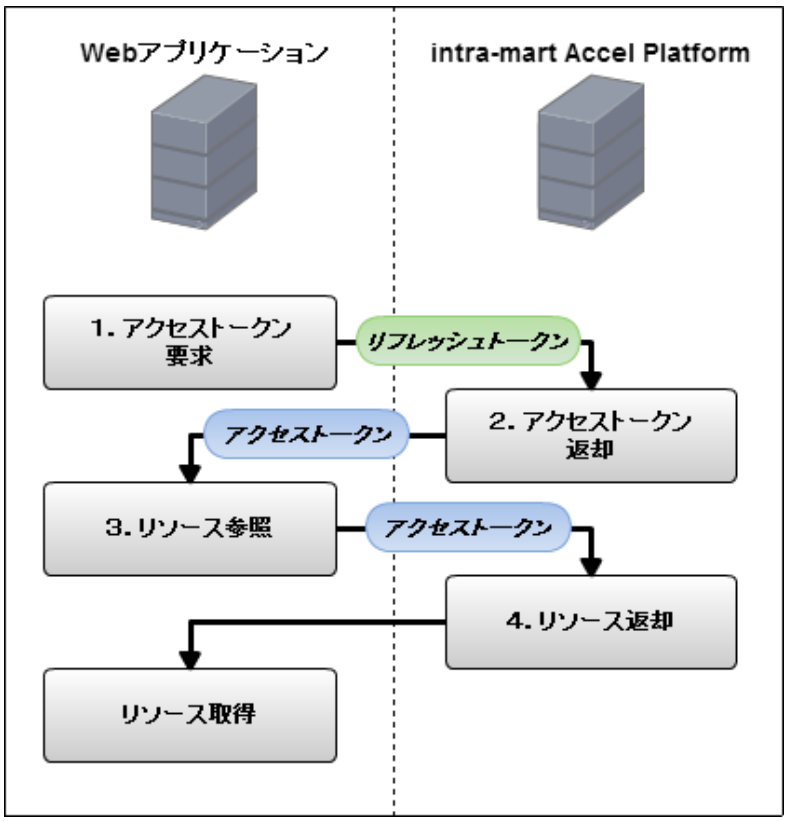
認可サーバがクライアントアプリケーションにリフレッシュトークンを発行している場合、クライアントアプリケーションはアクセストークンの有効期限が過ぎた際に、リフレッシュトークンを用いてトークンの更新リクエストを送ることができます。

アクセストークンの更新フロー

1. クライアントアプリケーションは認可サーバにアクセストークンの更新リクエストを送信します。
2. 認可サーバは、リフレッシュトークンおよびクライアントアプリケーションの認証情報（クライアントシークレット）を検証して新しいアクセストークンおよびリフレッシュトークンを返却します。古いアクセストークンおよびリフレッシュトークンは破棄されます。

3. クライアントアプリケーションは取得した新しいアクセストークンを用いて intra-mart Accel Platform 上のリソースへアクセスします。

4. intra-mart Accel Platform はアクセストークンを検証してリソースを返却します。



intra-mart Accel Platform で提供しているエンドポイント

intra-mart Accel Platform では、以下のエンドポイントを OAuth クライアントに提供します。

- 認可エンドポイント

  リソース所有者が、保護リソースへのアクセスを OAuth クライアントに許可するための許可 URL です。

  ```
  https://<HOST>:<PORT>/<CONTEXT_PATH>/oauth/authorize
  ```

- トークンエンドポイント

  OAuth クライアントが、アクセス・トークンとユーザ許可の付与を交換するトークン要求 URL です。

  ```
  https://<HOST>:<PORT>/<CONTEXT_PATH>/oauth/token
  ```

- トークン確認エンドポイント

  OAuth クライアントが、受け取ったアクセストークンが自分自身に発行されたトークンか確認するための確認 URL です。

  ```
  https://<HOST>:<PORT>/<CONTEXT_PATH>/oauth/token/verify
  ```

各エンドポイントの利用方法は「 OAuth プログラミングガイド 」 - 「 クライアントアプリケーションからOAuth認証機能を利用する方法 」を参照してください。

アクセストークンの有効期限と更新方法

アクセストークンの有効期限はトークンを発行してから 1 時間になります。
有効期限が切れた場合はアクセストークンを更新して新しいトークンを取得する必要があります。

アクセストークンの更新方法は以下の通りです。

1. 認可コードによる認可フローの場合
   リフレッシュトークンを利用して新しいトークンを取得します。
   詳しくは「 *アクセストークンの更新* 」を参照してください。

2. インプリシットグラントフローの場合
   アクセストークンを取得した際と同様の方法で新しいトークンを取得します。
   詳しくは「 *インプリシットグラント* 」を参照してください。

アクセストークンの有効期限の設定方法

OAuth認証モジュールでは、アクセストークンの有効期限をクライアント毎に設定できるようになっています。
アクセストークンの有効期限を変更する場合は、以下の設定ファイルを編集します。

- ファイル名

  oauth-client-details-config.xml

- 設定項目

  <client-details> - <client-detail access-token-validity-seconds>

詳しい設定については 「 設定ファイルリファレンス 」 - 「 クライアント詳細設定 」を参照してください。

注意

アクセストークンの有効期限を長くした場合、トークンが漏洩した際のセキュリティリスクが高くなります。
必要以上にアクセストークンの有効期限を長くしないようにしてください。