報道各位

2019 年 9 月 19 日
株式会社インプレスR&D
https://nextpublishing.jp/

整理して理解する！OAuth2.0 の解説書

『雰囲気で使わずきちんと理解する！整理して OAuth2.0 を使うためのチュートリアルガイド』発行

技術の泉シリーズ、9 月の新刊

インプレスグループで電子出版事業を手がける株式会社インプレス R&D は、『雰囲気で使わずきちんと理解する！整理して OAuth2.0 を使うためのチュートリアルガイド』(著者:Auth 屋)を発行いたします。

最新の知見を発信する『技術の泉シリーズ』は、「技術書典」をはじめとした各種即売会や、勉強会・LT 会などで頒布された技術同人誌を底本とした商業書籍を刊行し、技術同人誌の普及と発展に貢献することを目指します。

『雰囲気で使わずきちんと理解する！整理してOAuth2.0を使うためのチュートリアルガイド』
https://nextpublishing.jp/isbn/9784844378181

著者:Auth 屋
小売希望価格:電子書籍版　1600 円(税別)／印刷書籍版　1800 円(税別)
電子書籍版フォーマット:EPUB3／Kindle Format8
印刷書籍版仕様:B5 判／カラー／本文 94 ページ
ISBN:978-4-8443-7818-1
発行:インプレス R&D

＜＜発行主旨・内容紹介＞＞

深く考えずに OAuth2.0 を使っていませんか？　本書はそんなあなたのための OAuth2.0 入門書です。

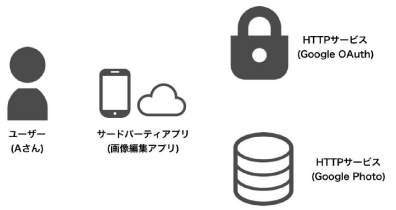
この1冊で、スコープや認可コードとは何かといった基本的な概念を整理して理解できます。

読み終わった時、利用したい API の OAuth2.0 関連資料や、OAuth2.0 の標準仕様を読みこなすための「地図」があなたの頭の中にできるでしょう。

(本書は、次世代出版メソッド「NextPublishing」を使用し、出版されています。)

OAuthとはなにか、なぜ必要かを丁寧に解説

図 1.1: 画像編集アプリの構成要素



4つの言葉をこの例にそって解説します。

サードパーティアプリ

画像編集アプリが「サードパーティーアプリ」に対応します。Google PhotoのAPIを提供するGoogleからみるとサードパーティだからです。

HTTPサービス

この例ではGoogle PhotoのAPIが「HTTPサービス」に当たります。

限定的なアクセス

画像編集アプリはGoogle PhotoのAさんのデータに対してどんな操作でも許されているわけではありません。許されるのは画像のダウンロードのみです。仮に画像編集アプリが画像のアップロードや、画像の削除をしようとした場合はGoogle Photoはそのアクセスを拒否しなければなりません。このようにサードパーティはHTTPサービスに対して一部の操作のみが許されます。

ところで、Google Photoは許可してよい操作をどのように知るのでしょうか。それはAさんの同意によります。OAuthでは「Google Photoにある写真やアルバムなどのデータはAさんのものである。Google Photoのものではない。」と考えます。したがって、画像編集アプリによるAさんのデータへの操作をGoogle Photoが勝手に許可してはいけません。

画像編集アプリが要求する権限一覧をAさんに提示した上で、Aさんから権限の委譲について同意を得る必要があります。その同意が完了してはじめて、Goole Photoは画像編集アプリに許可して良い操作を知ることができます。

認可フレームワーク

Google PhotoのAPIはインターネットに公開されているので悪意あるアクセスを前提としなければなりません。Google Photoはすべてのアクセスに対して、許可してよいアクセスかどうかを判断します。この判断に使われるのがアクセストークンです。認可フレームワークとは「アクセストークンの発行方法についてのルール」といえます。そして、このルールにそってアクセストークンを払い出すのが、GoogleのOAuthサービスになります。

各用語の説明が終わったので、もう一度定義に戻りましょう

> OAuth2.0はサードパーティアプリケーションによるHTTPサービスへの限定的なアクセスを可能にする認可フレームワークである。

これを例に沿って言い換えると次のとおりです。

> OAuth2.0は「画像編集アプリによるGoogle Photoへの限定的なアクセス(Aさんの領域へのアップロードのみ)」を可能にするための「アクセストークンの発行方法のルール」である。

1.2 OAuthはなぜ必要か

先程の定義には、触れられていないポイントがあります。それは「OAuthを使えば、ユーザーはサードパーティアプリにHTTPサービスのユーザー名、パスワードを教える必要がない」ということです。サードパーティアプリはユーザーのHTTPサービス上のユーザー名、パスワードを知らないにもかかわらず、限定的とはいえHTTPサービスへのアクセスが可能になります。それを可能にする方法は2章移行でじっくり解説するとして、まず、「サードパーティにユーザー名、パスワードを教えると発生する問題」について説明します。それは裏返すと「OAuthはなぜ必要か」という説明でもあります。

これも画像編集アプリの例で説明します。OAuthがなければ、Google Photoのユーザー名、パスワードを画像編集アプリに教えるしかありません。「画像編集アプリからGoogle Photoに継続的にアクセスする必要があること」、「ユーザーに何度もパスワードを入力させるのはわずらわしいこと」という理由から、パスワードは画像編集アプリに保存されるでしょう。その結果、「何が起こりうるか」、そして「OAuth2.0を利用することでそれがどのように解決するか」について説明します。

問題1

Aさんの Google Photoでのユーザー名、パスワードを画像編集アプリが保持している場合、画像編集アプリができることはGoogle Photoからの画像のダウンロードだけではありません。画像の削除、アップロードなどAさんができることは何でもできてしまいます。仮に画像編集アプリが悪意ある開発者によって作られたアプリだとします。その場合、画像編集アプリはGoogle PhotoのAさんのデータに対してあらゆる操作を勝手に行うことが可能になります[2]。

OAuth2.0を利用すれば画像編集アプリは、Aさんが委譲した権限のみを有しています。先の例では画像編集アプリはGoogle Photoからの画像のダウンロードだけを行えます。仮に、悪意あるアプリであっても、ダウンロードしかできないため影響は最低限に抑えられます。

また、Aさんは画像編集アプリに対する権限委譲についてGoogle Photoから同意を求められるので、そのときに権限が適切であるかどうかを確認することができます。

問題2

2.この例ではGoogle Photoだけでなく、Googleのすべてのサービスを利用可能になります。

OAuthのロール、トークン、エンドポイント、グランドタイプについてそれぞれ詳細に解説

第4章 OAuthのエンドポイント

OAuthのシーケンスを理解する際には、次の3つのエンドポイントの役割を理解することが大切です。認可エンドポイントとトークンエンドポイントは、認可サーバーが提供するURIです。リダイレクトエンドポイントは、クライアントが提供するURIです。

最も代表的なOAuthのグラントタイプである認可コードグラントでは、次の3つのエンドポイントが使われます[1]。次項では、認可コードグラントにおける各エンドポイントの役割を中心に説明します。

4.1 認可エンドポイント

認可エンドポイントは、認可サーバーによって提供されるエンドポイントで、認可コードの発行が主な役割です[2]。クライアントがアクセス権を持っていないリソースにアクセスする際には、まず認可エンドポイントにアクセスします。認可エンドポイントではユーザー名とパスワードの入力などによってリソースオーナーの認証が行われます。認証が完了すると、リソースオーナーは保護されたリソースへのアクセス権をクライアントに委譲することについて同意を求められます。リソースオーナーが同意すると、同意の証として認可コードがリダイレクトエンドポイントに送られます。

4.2 トークンエンドポイント

トークンエンドポイントは、認可サーバーによって提供されるエンドポイントです。

認可コードを受け取ったクライアントは、それと共に必要なパラメーターを指定してトークンエンドポイントにリクエストを投げることで、アクセストークンを取得できます。

トークンエンドポイントではBasic認証によって、クライアントのアイデンティティが確認されます。Basic認証としてAuhotization ヘッダーに設定されるのは、クライアントIDとクライアントシークレットです。ここでクライアントIDはクライアントの識別子、クライアントシークレットはパスワードに相当するものです。このクライアントIDとクライアントシークレットは認可サーバーにクライアントを事前登録[3]する際に発行されます。

4.3 リダイレクトエンドポイント(リダイレクトURI)

リダイレクトエンドポイントはクライアントが提供します。標準仕様では「リダイレクトエンドポイント」と表現されていますが、OAuthを利用したことがある人にとっては「リダイレクトURI」という表現のほうがなじみがあると思います。

リダイレクトURIは認可サーバーから認可コードを受け取るために使われます[4]。

認可サーバーは、リソースオーナーの権限委譲の同意がおこなわれると、ステータスコード302のレスポンスを返してリダイレクトURIにブラウザーをリダイレクトします。その際、クエリパラメーターとして認可コードの値が渡されます。リダイレクトURIを「https://client.example.com/callback」とすると、認可サーバーからのレスポンスは次のような形になります。

```
HTTP/1.1 302 Found
 Location: https://client.example.com/callback?code=SplxlOBeZQQYbYS6WxSbIA
```

1.それ以外のグラントタイプでは3つのうちの一部のエンドポイントが使われます
2.インプリシットグラントではトークンが発行されます。それ以外のグラントでは認可エンドポイントは利用しません。
3.事前登録については第5章で説明します。

4.インプリシットグラントではアクセストークンの受け渡しに利用されます。

クライアントがアクセストークンを取得する流れをチュートリアルで学ぶ

第6章　チュートリアル

この章ではクライアントがアクセストークンを取得する流れを、手を動かしながら学びます。認可サーバーとしては、画像編集アプリの例と同じくGoogleのOAuthサービスを利用します。リソースサーバーとして、GoogleのPhotos Library APIを利用します。

具体的には、次の3つのパターンでアクセストークンを取得します。

・認可コードグラント
・認可コードグラント + PKCE
・インプリシットグラント

ここでは、クライアントとして実際にアプリを作ることはしません。curlコマンドとブラウザーを利用して、クライアントが出すリクエストを投げることで実際のリクエスト、レスポンスを体験します。

curlコマンドはMacOS、Windows10[1]ともにデフォルトで利用できます。この章を読み進めるために、インストールや環境構築は必要ありません。

著者が確認のために利用した環境を次に記載しますが、特別なオプションは使っていないので、他のバージョンでも問題ないと思います。

表6.1: curlとブラウザーの検証バージョン

ツール	バージョン
curl	7.54.0
ブラウザー	Google Chorme バージョン: 74.0.3729.169（Official Build）（64 ビット）

6.1　クライアントの登録

まずは画像編集アプリをGoogleに登録し、クライアントIDとクライアントシークレットの発行を受けます。登録の流れは次のとおりです。

1．Google Cloud Platformの利用規約の同意
2．プロジェクトの作成
3．Photos Library APIの有効化
4．認証画面の作成
5．OAuthクライアントIDの作成

これらの登録はGoogle Developer Console(以降、デベロッパーコンソール)にて行います。

1. Google Cloud Platformの利用規約の同意

1.Windows 10 Ver.1803（RS4）のプレビュー版、Build 17063から標準コマンドとしてcurlコマンドが使えるようになっています。

デベロッパーコンソール(https://console.developers.google.com)にブラウザーでアクセスして下さい。デベロッパーコンソールに初めてアクセスすると図6.1のGoogle Cloud Platformの利用規約同意画面が表示されます。利用規約にチェックを入れ、居住国を選択して「同意して続行」を押して下さい。

なお、Google Cloud Platform(以降、GCP)とは、Googleがクラウド上で提供するサービス群の総称です。このチュートリアルでリソースサーバーとして利用するPhotos Library APIはGCPに含まれています。

図6.1: GDC初回アクセス

2. プロジェクトの作成

利用規約に同意するとデベロッパーコンソールのトップ画面図6.2が表示されますので「プロジェクトの選択」を押してください。

図6.2: デベロッパーコンソールのトップ画面

図6.3のプロジェクトの選択画面が表示されます。右上の「新しいプロジェクト」を押して下さい。

＜＜目次＞＞

＜＜著者紹介＞＞

Auth 屋
サウナと筋トレが趣味。好物は鴨汁つけ蕎麦。最近の楽しみは、技術同人誌サークル主さんとツイッターできゃふきゃふすることです。

＜＜販売ストア＞＞

電子書籍:
Amazon Kindle ストア、楽天 kobo イーブックストア、Apple Books、紀伊國屋書店 Kinoppy、Google Play Store、honto 電子書籍ストア、Sony Reader Store、BookLive!、BOOK☆WALKER
印刷書籍:
Amazon.co.jp、三省堂書店オンデマンド、honto ネットストア、楽天ブックス
※ 各ストアでの販売は準備が整いしだい開始されます。
※ 全国の一般書店からもご注文いただけます。

【インプレス R&D】 https://nextpublishing.jp/
株式会社インプレスR&D（本社:東京都千代田区、代表取締役社長:井芹昌信）は、デジタルファーストの次世代型電子出版プラットフォーム「NextPublishing」を運営する企業です。また自らも、NextPublishing を使った「インターネット白書」の出版など IT 関連メディア事業を展開しています。
※NextPublishing は、インプレス R&D が開発した電子出版プラットフォーム（またはメソッド）の名称です。電子書籍と印刷書籍の同時制作、プリント・オンデマンド（POD）による品切れ解消などの伝統的出版の課題を解決しています。これにより、伝統的出版では経済的に困難な多品種少部数の出版を可能にし、優秀な個人や組織が持つ多様な知の流通を目指しています。

【インプレスグループ】 https://www.impressholdings.com/
株式会社インプレスホールディングス（本社:東京都千代田区、代表取締役:唐島夏生、証券コード:東証1部9479）を持株会社とするメディアグループ。「IT」「音楽」「デザイン」「山岳・自然」「旅・鉄道」「学術・理工学」を主要テーマに専門性の高いメデイア&サービスおよびソリューション事業を展開しています。さらに、コンテンツビジネスのプラットフォーム開発・運営も手がけています。

【お問い合わせ先】
株式会社インプレス R&D NextPublishing センター

TEL 03-6837-4820
電子メール: np-info@impress.co.jp