報道各位

2018年8月27日
株式会社インプレスR&D
https://nextpublishing.jp/

クラウド認証プラットフォームを使って、セキュアなSPAを作る！

# 『「Auth0」で作る！認証付きシングルページアプリケーション』発行

技術書典シリーズ、8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、『「Auth0」で作る！認証付きシングルページアプリケーション』(著者:土屋 貴裕)を発行いたします。

**『「Auth0」で作る！認証付きシングルページアプリケーション』**
https://nextpublishing.jp/isbn/9784844398417


著者:土屋 貴裕
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102ページ
ISBN:978-4-8443-9841-7
発行:インプレスR&D

**＜＜発行主旨・内容紹介＞＞**

【Auth0を使って、セキュアなシングルページアプリケーションを体験しよう！】

本書はクラウド認証プラットフォーム「Auth0」を使ってユーザー認証付きのSPA(シングルページアプリケーション)作るためのチュートリアルです。

Auth0はOpenID Connect、JsonWebToken(JWT)ベースの認証方法を採用しており、本書を通じてJWTがどんなものか、どのようにJWTを発行して、どのように認証を行うかを知って、実際に体験することができます。

〈本書の対象読者〉

Vue.jsがちょっと分かる程度のフロントエンドの知識がある人
Rails Tutorialを終わらせた程度のサーバーサイドの知識がある人
(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。)

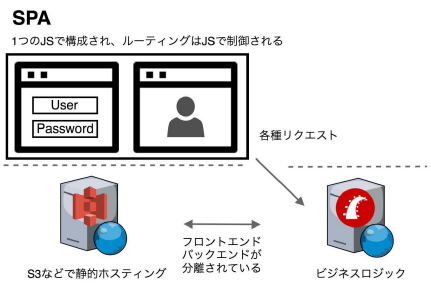
# SPA と認証について図解付きで詳しく解説

度結合した状態になります。

### 1.4.2　SPA とトークン認証

モバイルアプリのように、フロントエンドSPAとバックエンドを完全に分離させる場合はトークン認証を使います。枠組みはモバイルアプリと同じで、トークンをブラウザ側のローカルストレージやクッキーに保存して利用します。

図 1.5: SPA とトークン認証



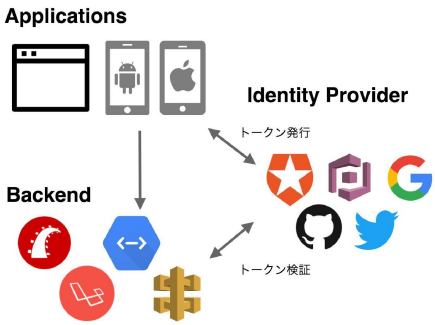

SPA は S3 などの静的ホスティングを用いて表示し、認証を含めたロジックは別の API サーバーに置きます。認証に関するルーティングは SPA で考慮する必要があるので、セッション認証よりも SPA の実装は複雑になります。ただし、フロントエンドとバックエンドが疎結合になりますので、ウェブ版からのモバイルアプリ展開が行いやすくなりますし、スケールも容易です。

モバイルファーストで開発を進めた場合は、すでに API 側にトークン認証の仕組みが存在するはずなので、ウェブ専用にセッション認証を用意するよりも、トークン認証を利用するほうがシステム全体の構成はすっきりします。

## 1.5　モダンなアプリケーションの構成と IdP

長々とアプリケーションのアーキテクチャーと認証について解説しましたが、モダンなアプリケーションの場合、アプリを含めたフロントエンドの選択肢として、Web（SPA）・Android・iOS の 3 種類のプラットフォームが存在し、バックエンドはモノリシックなフレームワークとサーバーレスの 2 種類が存在します。これらを相互に繋ぎ、拡張することを念頭におくのであればトークン認証は悪くない選択です。また、認証サービス自体も分離することによって、よりすっきりした構成になります。

図 1.6: IdP を分離したアーキテクチャー




このように分離した認証サービスは IdP（Identity Provider）と呼ばれます。Google・Twitter・Facebook なども IdP として認証機能を提供しており、色々なサービスで「Google でログイン」「Twitter でログイン」を使った方も多いのではないでしょうか。

大手 SNS 兼 IdP のサービスを認証基盤として活用するのをリスクであると判断する場合は、認証サービスを自身で構築することになります。自身で構築する場合は AWS Cognito や Auth0 などのサービスを使うとよいでしょう。もちろん Rails を使うことも可能です。

登場人物は多くなりましたが、認証の仕組みはひとつのパターンしかありません。各要素がどのように繋がるかの観点でみると、非常にすっきりしているのではないでしょうか。次章からは、主にトークン認証を扱って次のような構成でアプリの開発を行います。

・App: SPA（Vue.js + Nuxt.js）
・API: Rails API Mode
・Identity Provider: Auth0

本書ではこのような構成で話を進めますが、たとえば SPA をモバイルに置き換えたり、API




# 認証プラットフォーム「Auth0（オースゼロ）」についてその詳細を丁寧に解説

# 第4章　Auth0

ここまでは OIDC とその周辺技術について説明してきました。本章では、本書で扱うクラウド認証プラットフォームの「Auth0」を紹介します。Auth0 の良さを知ってもらえたらと思います。

## 4.1　Auth0 とは

Auth0[1]（オースゼロ）は、ウェブサービス、モバイルアプリなどに認証・認可の仕組みを提供する IDaaS（Identity as a Service）と呼ばれているサービスです。

図 4.1: Auth0 のロゴ


多くの IDaaS はこれまで主に社内向けのサービスで、1 つの ID を使って自社で契約しているさまざまなシステムへのログインを可能とするサービスとして使われてきました。業務でさまざまなクラウドサービスを扱う場合、いくつもあるサービスの ID・パスワードを管理するのはリスクであり、社内インフラの管理者にとって頭を悩ませる問題のひとつでした。これを解決する機能を提供するのが IDaaS で、Okta[2] や OneLogin[3] が有名どころです。

もちろん Auth0 も前述したような社内インフラ用の ID マネジメントも可能なのですが、BtoC サービスのような一般ユーザー向けの認証にも力を入れています。アプリケーションに認証機能を付けることは、必須でありながらサービスの本質とは離れているので、意外と面倒なものです。Auth0 を使えば、アプリケーションに認証機能を独自実装することなく、さまざま認証を簡単に組み込むことができます。

Auth0 は OIDC を標準プロトコルとして採用しており、各種プラットフォーム向けに SDK や組み込みフォームを提供しているので、簡単に組み込みを行うことができます。とにかく簡単に色々なことが行えるようになっています。

### 4.1.1　機能と料金

フリープランでカバーできる範囲はざっくり次のとおりです。

・7000 人までのアクティブユーザー
・2 種類までのソーシャルログイン（Google や GitHub など）
・パスワードレス対応
・TouchID 対応
・組み込み UI「Lock」の使用（Web、iOS、Android）
・Auth0 Database の使用（Auth0 内で LoginID/Password を管理する）
・ユーザーに対する JavaScript ベースのルールの適用（特定の IP 禁止など）
・ユーザーへのメタデータ追加

フリープランでだいたいのことができるので、数十人、数百人規模のアプリケーションで、安定性やサポートを重要視しないのであればフリープランで十分かもしれません。ソーシャルログイン数の制限を緩和して欲しいところではありますが、エンジニア向けサービスであれば Google と Github などで良さそうです。このようなログインサービスの選定は、提供サービスの内容次第でしょう。トライアルもしやすいので、まずは気軽に触ってみるのがお勧めです。

### 4.1.2　制限を超える場合

開発者向け、Pro 開発者向けに、もう一歩踏み込んだ機能を使える有料プランも用意されています。OSS プロジェクトの場合は、無償で全機能を制限なしに利用することができます企業ユーザーで 7000 人のアクティブユーザーを超える場合は、Developer, Developer Pro プランをクレジットカード決済で利用することもできます。SLA やオンラインサポートが必要な方は、Auth0 もしくは代理店経由で Enterprise プランの問い合わせが必要となります。

各プランで提供される機能と料金に関しては、詳しくは公式の Pricing[4] を参照してください。ログイン後の設定画面でも詳細なプラン比較ができます。

## 4.2　Auth0 のよい点

筆者が使って感じたのは次の 3 点です。

1.https://auth0.com/jp/
2.https://www.okta.com/
3.https://www.onelogin.com/
4.https://auth0.com/pricing

## JavaScript のフレームワーク「Nuxt.js」に Auth0 を組み込むためのチュートリアルを掲載

第6章　NuxtにAuth0を組み込む

本章ではNuxtにAuth0の組み込み、フォームLockを実装し、Googleアカウントでのソーシャルログイン後にJWTを発行してブラウザに保存するところまでを作ります。
Railsとの連携はここでは実装しません。

図6.1: 連携図（JWT発行時）



Auth0のアカウントを登録してない場合は、先にAuth0の章を読んで、事前準備をしてください。

54 | 第6章　Nuxtに Auth0を組み込む

### 6.1　2種類のライブラリ

JavaScriptでのAuth0の組み込み方法は、次の2種類が候補に挙がります。

・auth0-js: https://github.com/auth0/auth0.js
・auth0-lock: https://github.com/auth0/lock

auth0-jsはJavaScript向けの汎用的なSDKで、auth0-lock（以下Lock）はauth0-jsを利用して、サインイン、サインアップ用のフォームを組み込んだラッパーライブラリです。Auth0の章でも紹介しました。

自分でフォームを組んでみても楽しいのですが、手軽に組み込めるのでLockを使用するのがよいでしょう。auth0-jsについては、Auth0のVue向けチュートリアルにauth0-jsを使った組み込み方法が掲載されているので参考にしてみてください。

LockおよびAuth0.jsについては、古いバージョンが設定されていると正常に動作しない場合があります。（稀にサンプルソース中のpackage.jsonで古いバージョンを指定している場合があります）その場合にはLock 11.xおよびauth0.js 9.xにアップグレードしましょう。

### 6.2　Lockを組み込む

#### 6.2.1　ライブラリの追加

Lockを組み込んでいきましょう。パッケージ名はauth0-lockになります。yarnで追加してください。

リスト6.1: auth0-lockを追加する

```
$ yarn add auth0-lock
```

Lockを利用するために、plugins/auth0.jsにAuth0Utilクラスを実装していきます。Nuxtのプラグインとして実装します。

リスト6.2: plugins/auth0.js

```
import Auth0Lock from 'auth0-lock'
import nuxtConfig from '~/nuxt.config'
const config = nuxtConfig.auth0

class Auth0Util {
  showLock(container) {
    const lock = new Auth0Lock(
      config.clientID,
      config.domain,
      {
```

第6章　Nuxtに Auth0を組み込む | 55

## ＜＜目次＞＞

**＜＜著者紹介＞＞**

土屋 貴裕

情報系の大学で音声認識を専攻し、大学院卒業後は大手自動車部品メーカーにてカーナビゲーションシステムの音声認識機能の開発に携わる。その後 Web 系 SIer にて、小規模 Web システムの開発でフロントエンド、バックエン

ド、インフラまで 1 人で担当。2017 年からはクラウド請求書の Web サービスの開発に携わっている。フロントエンドからインフラまで幅広く興味があるが、最近は基盤環境を改善したり、エンジニアリングを下支えするような技術が好き。2018/04 に開催された技術書典 4 で頒布された本書の底本「Auth0 でつくる！認証付き SPA」の功績が認められ、Auth0 Ambassadors of the Month の April 2018 Winners を受賞する。

**＜＜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 iBookstore、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。

**【株式会社インプレス 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