

# 認証機能を分離した話

# 自己紹介

- ・名前: かるだん
- ・によわによわ高校生
- ・よく使う言語、フレームワーク:  
Node.js(NestJS)、 Dart(Flutter)
- ・



↑メインで使ってるカリンちゃん。  
かわいいね。

# 認証機能を分離した経緯

- ・タスク管理ツールの認証にFirebaseを使ってた
- ・新しくアプリを作るにあたって同じ認証情報を使いたい
- ・Firebaseでは何かと不便

# 認証機能を分離した経緯

- ・タスク管理ツールの認証にFirebaseを使ってた
- ・新しくアプリを作るにあたって同じ認証情報を使いたい
- ・Firebaseでは何かと不便

...そうだ、認証・認可サーバーを分離しよう

(勉強になるからヨシッ)

# 認証・認可のやり方

- ・認証サーバーでjwtを発行
- ・jwtをタスクサーバーで検証

やることはむちゃくちゃ簡単！

~~みんなもやってみよう！~~

# JWT(JWS)とは

- ・jsonのデータをbase64url形式でエンコードしたもの
- ・トークンの署名はJWSが担っている
- ・↑JWTに署名を加えてなりすまし防止・改ざん検出をしたもの

## JWTの中身



引用: [豆蔵デベロッパーサイト](#)

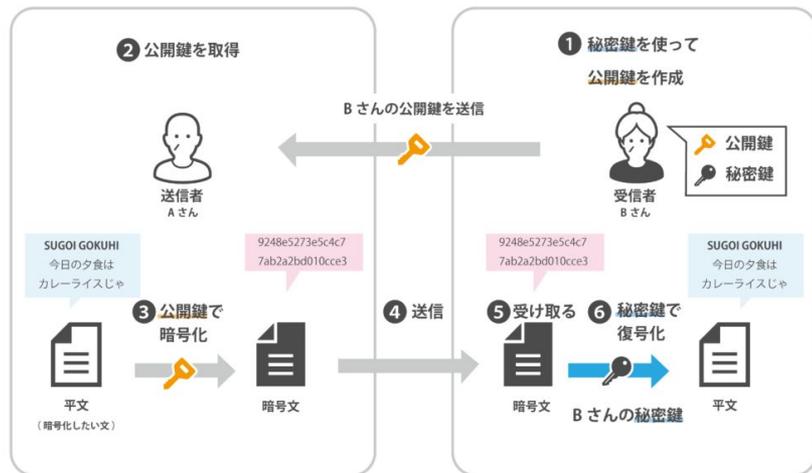
# 署名の仕組み

(認識曖昧だから間違ったらゴメンネ...)

- ・自分の秘密鍵を使って署名をする
- ・相手にメッセージ、署名、公開鍵を送る
- ・公開鍵を使って署名を検証する
- ・ハッシュ値を署名してなりすまし防止だけでなく改ざん検出を行うことも可能

※署名は公開鍵・共通鍵の両方で可能

## 公開鍵暗号方式



引用: [クミコミ](#)

# JWTのメリット・デメリット

## メリット

- ・サーバー側にトークンを保存する必要がない
- ・JWTのペイロードを使って情報を送れる
- ・なりすまし・改ざんのリスクが低い

## デメリット

- ・鍵の取り扱いの手間が増える
- ・
- ・

# 今回やったこと

- ・認証機能の実装
- ・セッションの管理
- ・jwtの生成、タスクサーバーのjwt認証

(これからやること)

- ・Firebaseからの移行
- ・クライアント側の実装

# 認証・認可サーバーは分離するべきか...?

目的無いならしないが吉

- ・分離した分管理の手間がかかる

- ・実装のコストが増える

- ・

勉強としてはむちゃくちゃ効果あるので分離した分のコストを受け入れられるならありかも

# 宣伝

Taskulesというタスク管理ツール作ってます！

Androidお持ちの方ぜひインストールしてみてください～

(絶賛金欠なので優しい方有料プラン入ってください ....)



←

Taskules (早期アクセス)

かるだん  
広告を含む・アプリ内課金あり

アンインストール 開く

① このアプリの早期アクセスに登録しました。デベロッパーにフィードバックを提供してアプリの改善にご協力ください。 [詳細を表示](#)

新機能 • →  
最終更新: 2024/07/10  
一部バグを修正

デベロッパーへの非公開のフィードバ...  
このフィードバックはデベロッパーにのみ表示されます

☆ ☆ ☆ ☆ ☆

フィードバックを入力

ゲーム アプリ 検索 書籍

以上！

ありがとうございました～