

はじめてのWeb認証

新卒エンジニア向け基礎講座

React + Hono デモアプリで体験しながら学ぼう

今日覚えること

1. 認証って何？ 身近な例で理解
2. なぜ必要？ Webアプリの課題
3. どうやって実現？ 4つの方法
4. 気をつけることは？ セキュリティ対策
5. 実際に触ってみよう デモアプリ体験

認証って何？

身近な例で考えてみよう

認証 = 本人確認

- スマホの指紋認証
- 銀行ATMの暗証番号
- 会社の入館カード

認可 = 権限確認

- 管理者だけがアクセスできるページ
- 自分の口座しか見れない
- 部長しか承認できない機能

なぜWebで認証が必要？

問題：誰でもアクセスできてしまう

`http://example.com/mypage`

↓

誰でも他人のマイページが見れる！

解決：ログインした人だけ

ログイン画面 → 本人確認 → マイページ表示

つまり：「この人は確かに〇〇さんです」を証明する仕組み

Webの困った性質

HTTPは「忘れっぽい」

あなた：「ログインしました！」

サーバー：「はい、どうぞ」

5秒後...

あなた：「マイページ見せて」

サーバー：「あなた誰でしたっけ？」

毎回「誰ですか？」と聞かれる！

解決方法：覚えておいてもらう

お店の例

1. 入店時：「整理券22番です」
2. 買い物中：「22番の方ですね」
3. 退店時：「22番の方、ありがとうございました」

Webでも同じ

1. ログイン時：「セッションID ABC123」
2. ページ閲覧時：「ABC123の方ですね」
3. ログアウト時：「ABC123さん、お疲れさまでした」



2つの考え方



お店型（ステートフル）

- 店員が覚えている
- お客さんは整理券だけ持つ
- 店員「22番の方は田中さんですね」



スマホ型（ステートレス）

- お客さんが全部持っている
- 身分証明書を毎回見せる
- 店員「身分証確認しました、田中さんですね」

方法1：基本認証

一番シンプルな方法

ユーザー名: tanaka
パスワード: password123

良いところ・悪いところ

😊 簡単に実装できる

😓 パスワードが丸見え（Base64のみ）

😓 毎回入力が必要

いつ使う？




開発中のテスト、社内ツールなど

方法2：セッション認証

お店型の実装

1. ログイン成功 → 「整理券」 発行
2. 整理券をクッキーに保存
3. ページ見るとき → 整理券を見せる

良いところ・悪いところ

-  サーバーが全部管理（安全）
-  すぐにログアウトできる
-  ユーザーが増えると重くなる

いつ使う？




普通のWebサイト、社内システム

方法3：JWT認証

スマホ型の実装

```
{  
  "ユーザー": "田中",  
  "権限": "一般",  
  "期限": "2025-01-01"  
}
```

良いところ・悪いところ

-  サーバーが軽い
-  大きなシステムに向いている
-  一度発行すると止められない

⚠ JWT認証の落とし穴

ログアウトできない？

普通の認証（セッション）

ログアウト → サーバー「はい、削除しました」
→ 本当にログアウト完了

JWT認証

ログアウト → ブラウザから削除
→ でもサーバーは「まだ有効」と思ってる
→ 見た目だけのログアウト

重要：盗まれたトークンは期限まで使われる可能性

方法4：AWS Cognito

Amazon が提供するサービス

- ユーザー登録・ログイン機能
- SMS認証、顔認証なども簡単
- トークンを無効化できる（JWTの問題を解決）

良いところ

- 😊 自分で作らなくていい
- 😊 セキュリティ機能が充実
- 😊 ユーザーが増えても大丈夫

