

システム開発実習

確認画面付きフォームの実装

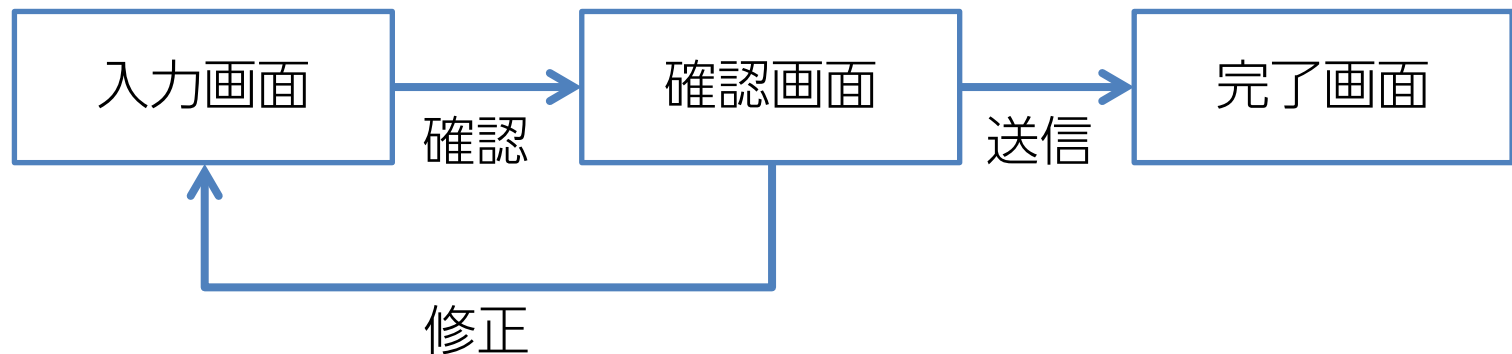
株式会社ジードライブ

この講義で学ぶこと

- 確認画面を持つフォームの画面遷移とその実装方法

確認画面を含む画面遷移

- 入力画面：入力フォーム
- 確認画面：入力内容の表示、修正ボタンと送信ボタン
- 完了画面：送信完了のメッセージ

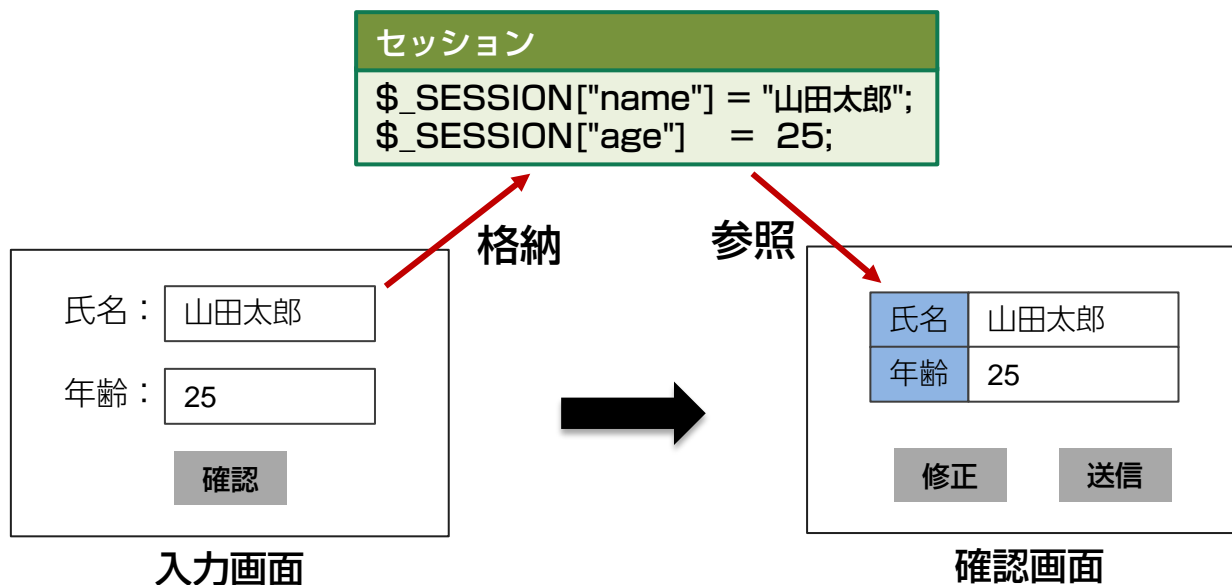


確認画面が入る場合の問題

- ユーザが入力画面でフォームに入力したデータをどのようにして確認画面へ渡すか



セッションにデータを格納する



各画面で行う処理

入力画面で行う処理

GET で呼び出された場合

- 入力フォームを表示する
 - 送信ボタンのラベルは「確認する」など
 - 自分自身にPOST送信する



The screenshot shows a web form with a light gray background. On the left, there is a label 'お問い合わせ内容' (Inquiry Content) in black text, followed by a red bracketed label '[必須]' (Required). To the right of the label is a large, empty rectangular input field. Below the input field, centered, is a button with a light gray background and a thin black border, containing the text '確認する' (Confirm) in black.

入力画面で行う処理

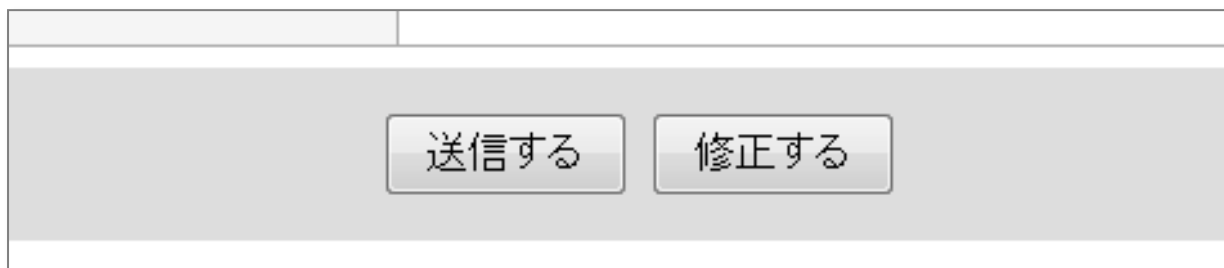
POST で呼び出された場合

- 送信された値のバリデーションを行う
- バリデーションでエラーが無かった場合：
 - ① 入力データをセッション変数に格納する
 - ② 確認画面へ移動する
- バリデーションでエラーがあった場合は、エラーメッセージと共に再びフォームを表示する

確認画面で行う処理

GET で呼び出された場合

- 入力データをセッション変数から読み出す
 - 入力データのセッション変数が存在しない場合は不正なアクセスとみなし、入力画面に移動させる
- 入力内容と共に「送信」ボタンと「修正」ボタンを備えたフォームを表示する



確認画面で行う処理

POST で呼び出された場合

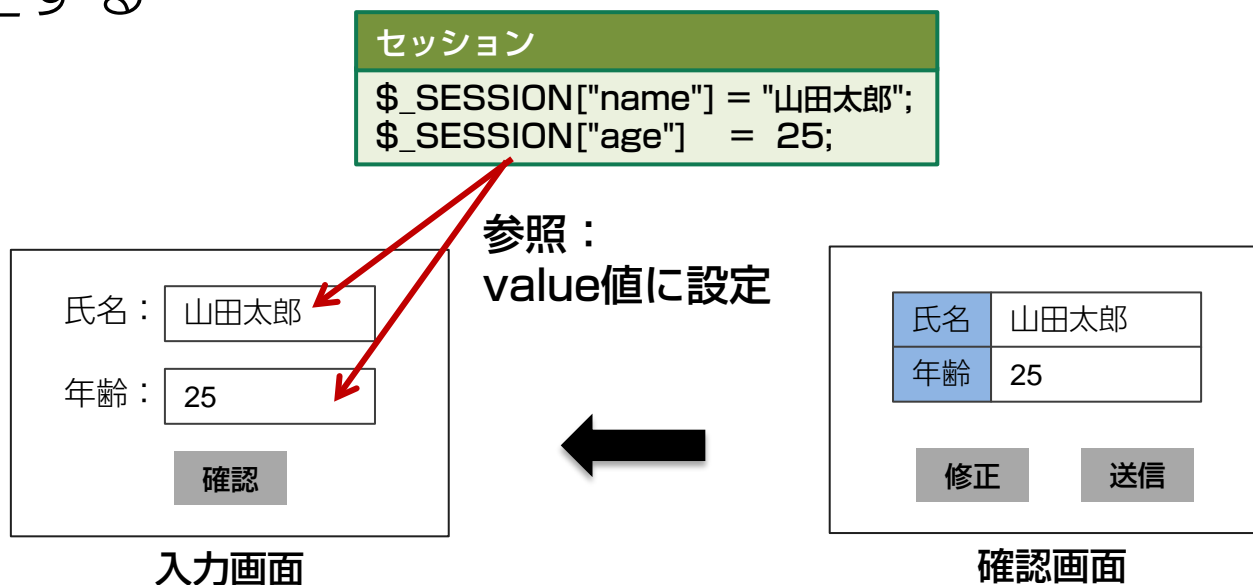
- 「送信」 ボタンで送信された場合
 - セッション変数に格納された値を元に何らかの処理を行う
 - データベースにデータを追加する（データ追加）
 - メールを作成し管理者へ送信する（問い合わせ）
 - 入力内容を保持するセッション変数を破棄する
 - 完了画面へ移動する
- 「修正」 ボタンで送信された場合
 - 入力画面へ移動する

確認画面で行う処理

- 確認画面から入力画面へ戻る場合、フォームにはユーザが入力した値が残っている必要がある



- セッション変数に格納されている値を、value値として設定する



完了画面で行う処理

- 完了メッセージを表示する
 - 「お問い合わせいただき、ありがとうございました」等のメッセージ
 - トップページ等へのリンク

練習

- input.php
 - List 05A-1-1
- input_conf.php
 - List 05A-2-1
- input_done.php
 - List 05A-3-1

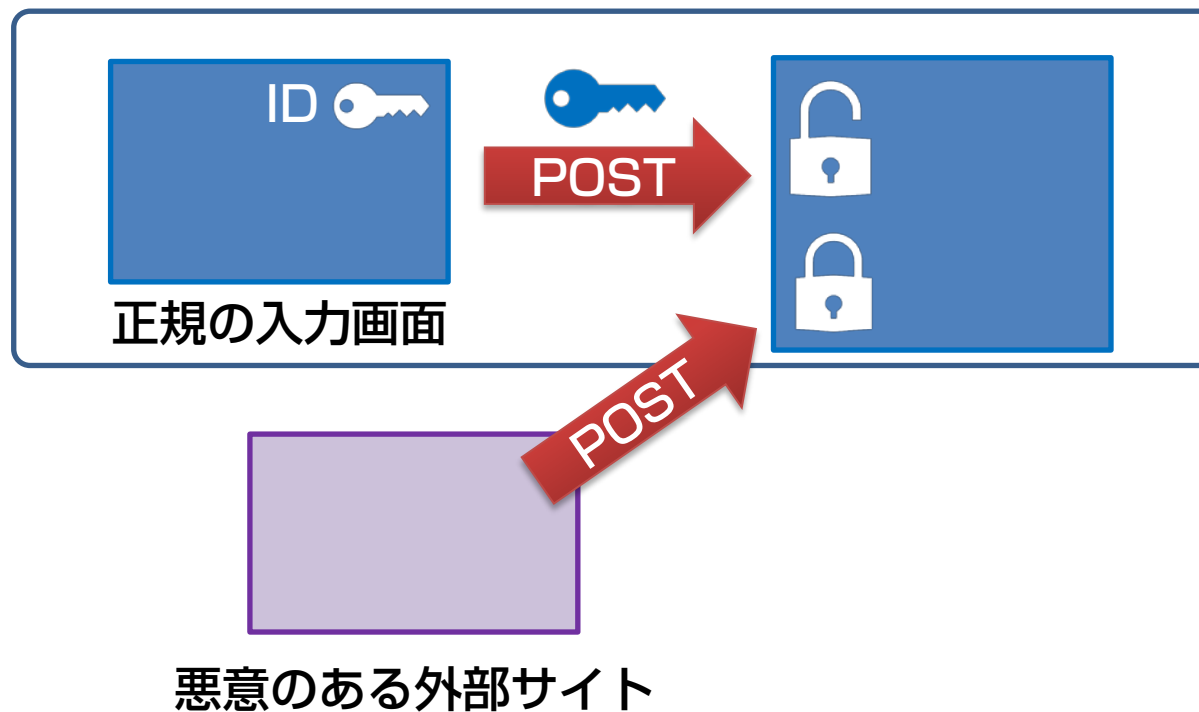
セキュリティ対策

CSRF

- CSRF : **C**ross **S**ite **R**equ~~e~~**s**t **F**orge~~r~~**i**es
クロスサイト リクエスト フォージェリ
- Webサーバ上に罠となるページを作り、意図しないショッピング決済や掲示板への書き込みといった処理を呼び出す攻撃
 - ショッピングや掲示板などでは、通常POSTリクエストで値を送る
 - 悪意のある者が勝手にPOSTリクエストを作って送ることができてしまう

CSRF対策

- 正規のユーザが、ページを訪れた際にIDを発行し、次のページに秘密の情報(セッション)として送る



練習

- 練習05B-1
 - cart.php
 - purchase.php
- 練習05B-2
 - dummy.php
- 練習05B-3
 - cart.php
 - purchase.php

実習

- 実習課題05-1 を行う