

お問い合わせフォーム

ECサイトなどでよく使われる
「お問い合わせフォーム」です。

下記の仕様を満たすようにします。

- 入力内容のチェック
- XSS対策
- CSRF対策

localhost

お問い合わせ

お問い合わせは下記のフォームよりお願いいたします。
必須 マークは必須入力項目です。

お名前	必須	<input type="text"/> (50文字以内)
住所	必須	郵便番号： (半角数字と半角ハイフンのみ) <input type="text"/> 都道府県： --選択してください-- 市区町村： (50文字以内) <input type="text"/> 町名番地等： (50文字以内) <input type="text"/>
メールアドレス	必須	<input type="text"/>
電話番号		<input type="text"/> (半角数字と半角ハイフンのみ)
お問い合わせ内容		<input type="text"/> (1,000文字以内)

確認

お問い合わせフォーム

入力フォーム

入力項目に入力を行い、「確認」ボタンをクリックすると、フォームの内容を「確認ページ」へPOSTで送信します。

お問い合わせ

お問い合わせは下記のフォームよりお願いいたします。
必須 マークは必須入力項目です。

お名前	必須	未来 太郎 (50文字以内)
住所	必須	郵便番号： (半角数字と半角ハイフンのみ) 550-0005 都道府県： 大阪府 市区町村： (50文字以内) 大阪市西区 町名番地等： (50文字以内) 西本町1丁目7番7号CE西本町ビル901
メールアドレス	必須	contact@miraino-katachih2.co.jp
電話番号		0120-111-557 (半角数字と半角ハイフンのみ)
お問い合わせ内容		お弁当はどんな種類がありますか？ お肉系が好きです。 (1,000文字以内)

確認

お問い合わせフォーム

確認ページ

「入力フォーム」で入力した内容を確認します。

入力内容に誤りがあったときは、「入力フォーム」のページにリダイレクトし、エラー内容を表示します。入力内容は保持したままにします。

「送信」ボタンをクリックすると、「お問い合わせ完了」ページにリダイレクトします。

「戻る」ボタンをクリックすると「入力フォーム」に戻ります。入力内容は保持したままにします。



localhost

お問い合わせ内容確認

下記の内容でよろしければ「送信」ボタンを押してください。

お名前	未来 太郎
住所	〒550-0005 大阪府 大阪市西区 西本町1丁目7番7号CE西本町ビル901
メールアドレス	contact@miraino-katachih2.co.jp
電話番号	0120-111-557
お問い合わせ内容	お弁当はどんな種類がありますか？ お肉系が好きです。

送信 戻る

お問い合わせフォーム

確認ページ

「確認ページ」の「戻る」ボタンで「入力フォーム」に戻ったとき、または、入力内容に誤りがあって「入力フォーム」にリダイレクトしたとき、右のように、入力した内容が保持されたままになっているようにします。

localhost

お問い合わせ

お問い合わせは下記のフォームよりお願いいたします。
必須 マークは必須入力項目です。

お名前	必須	<input type="text" value="未来 太郎"/> (50文字以内)
住所	必須	<div>郵便番号： (半角数字と半角ハイフンのみ) <input type="text" value="550-0005"/></div> <div>都道府県：<input type="text" value="大阪府"/> </div> <div>市区町村： (50文字以内) <input type="text" value="大阪市西区"/></div> <div>町名番地等： (50文字以内) <input type="text" value="西本町1丁目7番7号CE西本町ビル901"/></div>
メールアドレス	必須	<input type="text" value="contact@miraino-katachih2.co.jp"/>
電話番号		<input type="text" value="0120-111-557"/> (半角数字と半角ハイフンのみ)
お問い合わせ内容		<div><input type="text" value="お弁当はどんな種類がありますか？"/> <input type="text" value="お肉系が好きです。"/></div> <div>(1,000文字以内)</div>

確認

お問い合わせフォーム

完了ページ

本来であれば、このページで

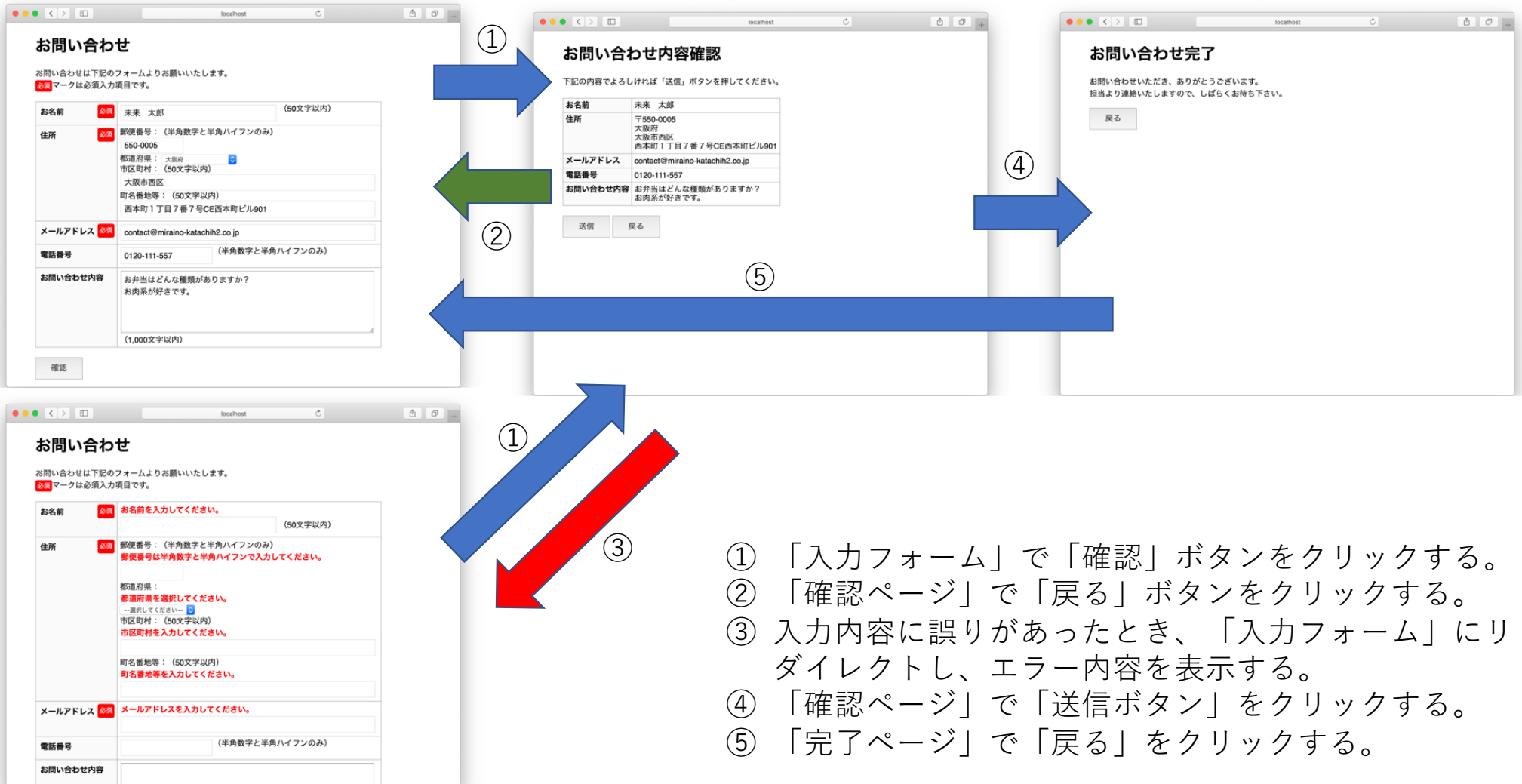
- 確認メールの送信処理
- データベースへの登録処理

などを行いますが、今回は右の表示のみができればOKです。

「戻る」ボタンをクリックすると、「入力フォーム」に戻ります。入力内容はすべて削除されているようにします。



お問い合わせフォーム 画面遷移



- ① 「入力フォーム」で「確認」ボタンをクリックする。
- ② 「確認ページ」で「戻る」ボタンをクリックする。
- ③ 入力内容に誤りがあったとき、「入力フォーム」にリダイレクトし、エラー内容を表示する。
- ④ 「確認ページ」で「送信ボタン」をクリックする。
- ⑤ 「完了ページ」で「戻る」をクリックする。

お問い合わせフォーム

入力項目

- お名前 必須入力、50文字以内
- 住所
 - 郵便番号 必須入力、半角数字のみ7桁、もしくは、(半角数字3桁)-(半角数字4桁)
 - 都道府県 必須入力、セレクトボックスから選択
 - 市区町村 必須入力、50文字以内
 - 町名番地等 必須入力、50文字以内
- メールアドレス 必須入力、256文字以内*
- 電話番号 任意入力、半角数字と半角ハイフンのみ
- お問い合わせ内容 任意入力、1,000文字以内

*インターネットの規約で、メールアドレスの長さは256文字までと決められています。

お問い合わせフォーム

入力した値は**バリデーション**（値の妥当性チェック）を行います。
値に妥当性がない場合（入力規則に則っていない場合）はエラー表示を行い、次の処理に進むことができないようにします。

- お名前

- 未入力するとき

- ✓ お名前を入力してください。

- 50文字を超えるととき

- ✓ 恐れ入りますが、お名前は50文字以内でご入力ください。

- 郵便番号

- 未入力するとき

- ✓ 郵便番号を入力してください。

- 半角数字のみ7桁、もしくは、(半角数字3桁)-(半角数字4桁)の形式でないとき

- ✓ 郵便番号は半角数字と半角ハイフンで入力してください。

お問い合わせフォーム

- 都道府県
 - ・ 未選択のとき
 - ✓ 都道府県を選択してください。
- 市区町村
 - ・ 未入力ของとき
 - ✓ 市区町村を入力してください。
 - ・ 50文字を超えるとき
 - ✓ 恐れ入りますが、市区町村は50文字以内で入力してください。
- 町名番地等
 - ・ 未入力的时候
 - ✓ 町名番地等を入力してください。
 - ・ 50文字を超えるとき
 - ✓ 恐れ入りますが、町名番地等は50文字以内で入力してください。

お問い合わせフォーム

- メールアドレス

- 未入力するとき

- ✓ メールアドレスを入力してください。

- メールアドレスの形式が正しくないとき

- ✓ メールアドレスを正しく入力してください。

- メールアドレスの長さが256文字を超えると

- ✓ 恐れ入りますが、メールアドレスは256文字以内で入力してください。

- 電話番号

- 電話番号の形式が正しくないとき

- ✓ 電話番号を正しく入力してください。

- 任意入力なので、未入力は許可します。

- お問い合わせ内容

- 文字数が1,000文字を超えると

- ✓ 恐れ入りますが、お問い合わせ内容は1,000文字以内で入力してください。

- 任意入力なので、未入力は許可します。

お問い合わせフォーム

フォームをsubmitし、バリデーションエラーがあるときは、右のように表示します。

お問い合わせ

お問い合わせは下記のフォームよりお願いいたします。
必須 マークは必須入力項目です。

お名前	必須	<input type="text"/> (50文字以内)
住所	必須	郵便番号：(半角数字と半角ハイフンのみ) <input type="text"/> 都道府県： 都道府県を選択してください。 --選択してください-- 市区町村：(50文字以内) <input type="text"/> 町名番地等：(50文字以内) <input type="text"/>
メールアドレス	必須	<input type="text"/>
電話番号		<input type="text"/> (半角数字と半角ハイフンのみ)
お問い合わせ内容		<input type="text"/> (1,000文字以内)

確認

お問い合わせ

お問い合わせは下記のフォームよりお願いいたします。
必須 マークは必須入力項目です。

お名前	必須	お名前を入力してください。 <input type="text"/> (50文字以内)
住所	必須	郵便番号：(半角数字と半角ハイフンのみ) 郵便番号は半角数字と半角ハイフンで入力してください。 <input type="text"/> 都道府県： 都道府県を選択してください。 --選択してください-- 市区町村：(50文字以内) 市区町村を入力してください。 <input type="text"/> 町名番地等：(50文字以内) 町名番地等を入力してください。 <input type="text"/>
メールアドレス	必須	メールアドレスを入力してください。 <input type="text"/>
電話番号		<input type="text"/> (半角数字と半角ハイフンのみ)
お問い合わせ内容		<input type="text"/>

お問い合わせフォーム

XSS対策

POSTされてきた値を**サニタイズ**します。

`htmlspecialchars()`関数を使います。

<https://www.php.net/manual/ja/function htmlspecialchars.php>

```
// サニタイズ
foreach ($_POST as $k => $v) {
    $post[$k] = htmlspecialchars($v, ENT_QUOTES, 'UTF-8');
}
```

お問い合わせフォーム

CSRF対策

ワンタイムトークンを生成し、別のサイト、別のセッションからPOSTされるのを防ぎます。

送信フォーム側

```
// ワンタイムトークンを生成してセッションに保存 (XSRF対策)
$token = bin2hex(openssl_random_pseudo_bytes(2048));
$_SESSION['token'] = $token;
```

...

```
<input type="hidden" name="token" value="<?= $token ?>">
```

`openssl_random_pseudo_bytes()` 関数

<https://www.php.net/manual/ja/function.openssl-random-pseudo-bytes.php>

`bin2hex()` 関数

<https://www.php.net/manual/ja/function.bin2hex.php>

お問い合わせフォーム

CSRF対策

受信側

```
// フォームで送信されてきたトークンが正しいかどうか確認（CSRF対策）
if (!isset($_SESSION['token']) || $_SESSION['token'] !== $_POST['token']) {
    $_SESSION['err_msg']['err'] = "不正な処理が行われました。";
    header('Location: ./');
    exit;
}
```

セッションに保存されたトークンがないとき、または、セッションに保存されたトークンとPOSTされてきたトークンの内容が異なるとき、次ページのように「不正な処理が行われました。」と表示し、「確認ページ」へ遷移できないようにします。

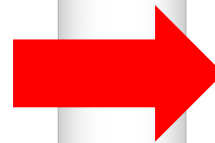
お問い合わせフォーム

CSRF対策

ローカルに保存したHTMLファイルからサーバーにPOSTしてみました。



A screenshot of a web browser window showing a contact form titled "お問い合わせ". The browser's address bar shows the file path "file:///Users/tadashi/Documents/index.html". The form includes fields for "お名前" (Name), "住所" (Address), "メールアドレス" (Email), "電話番号" (Phone Number), and "お問い合わせ内容" (Message). Each field has a red "必須" (Required) label. The "住所" field includes a dropdown for "都道府県" (Prefecture) and a text input for "市区町村" (City/Town/Village). The "お問い合わせ内容" field has a character count "(1,000文字以内)". A "確認" (Confirm) button is at the bottom.



A screenshot of a web browser window showing the same contact form, but now running on "localhost". A red box highlights the message "不正な処理が行われました。" (Invalid processing was performed.) with a red arrow pointing to it. The form fields and layout are identical to the local file version, but the "確認" button is now disabled.

お問い合わせフォーム

ヒント(1)

- 変数が空かどうかを調べる
empty()
<https://www.php.net/manual/ja/function.empty.php>
- 文字の長さを調べる
strlen()
<https://www.php.net/manual/ja/function.strlen.php>
- 複雑なバリデーションを行うには、**正規表現**を使う
<https://www.php.net/manual/ja/function.preg-match.php>
 - ✓ 正規表現について調べてみましょう
 - ✓ 正規表現が正しいかどうかを、下記のサイトで調べることができます。
<http://okumocchi.jp/php/re.php>

お問い合わせフォーム

正規表現の例

```
// 郵便番号のバリデーション
if (empty($post['postal_code'])) {
    $_SESSION['err_msg']['postal_code'] = "郵便番号を入力してください。";
    $validityCheck = false;
}
if (!preg_match('/^[0-9]{3}-?[0-9]{4}$/', $post['postal_code'])) {
    $_SESSION['err_msg']['postal_code'] = "郵便番号は半角数字と半角ハイフンで入力してください。";
    $validityCheck = false;
}
```

お問い合わせフォーム

ヒント(2) セッション (\$_SESSION) をうまく使います。

- バリデーションエラーの表示にはセッション (\$_SESSION) を使います。

```
<!-- エラーメッセージの表示 -->
<?php if (isset($_SESSION['err_msg']['name'])): ?>
<p class="warning"><?= $_SESSION['err_msg']['name'] ?></p>
<?php endif ?>
```

```
// バリデーションチェック
$validityCheck = true;

// 名前のバリデーション
if (empty($post['name'])) {
    $_SESSION['err_msg']['name'] = "お名前を入力してください。";
    $validityCheck = false;
}
```

お問い合わせフォーム

ヒント(2) セッション (\$_SESSION) をうまく使います。

- POSTされた値をセッションに保存して、入力フォームで表示します。

```
// サニタイズ
foreach ($_POST as $k => $v) {
    $post[$k] = htmlspecialchars($v, ENT_QUOTES, 'UTF-8');
}
```

```
// POSTされてきた値をセッションに代入する
$_SESSION['post'] = $post;
```

```
<!-- テキストボックスに表示する -->
<input type="text" value="<?php if(isset($_SESSION['post']['name'])) echo $_SESSION['post']['name'] ?>">
```