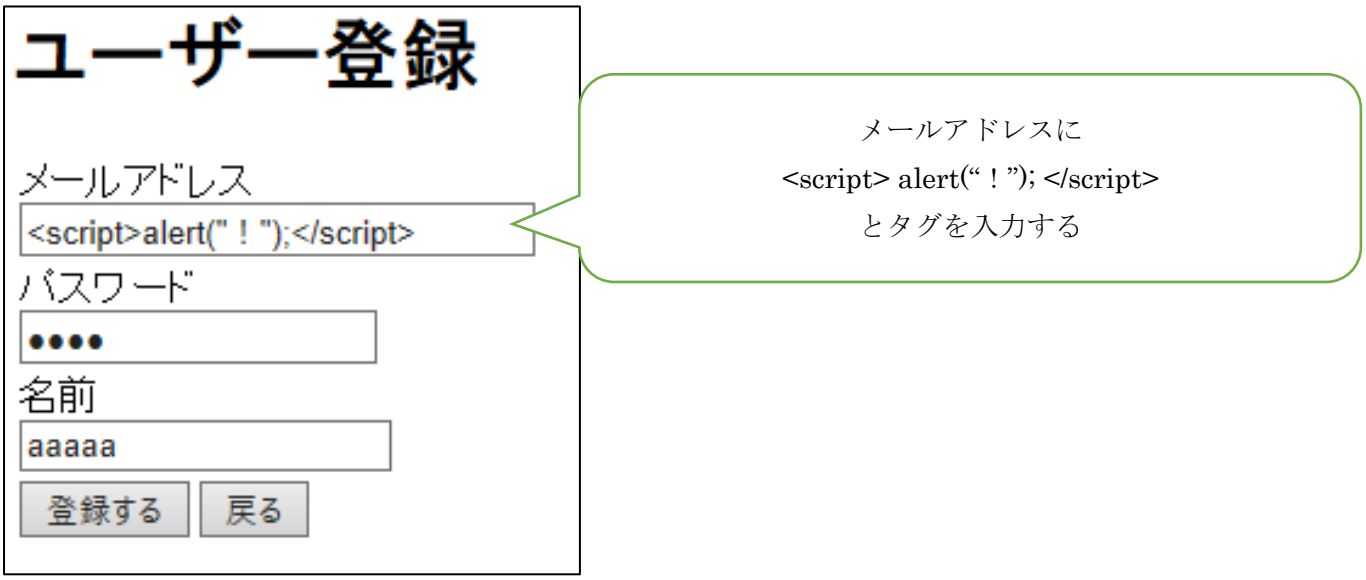
〇サニタイジング

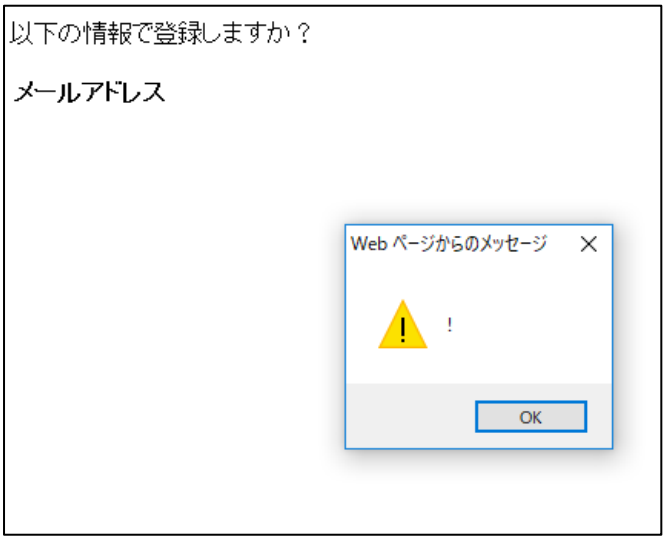
クロスサイト・スプリクティングの対策の１つ。入力データから HTML タグや JavaScript、SQL などの文字列を取り出し、置き換えを行い、入力データを無害化する処理のこと。入力フォームを持つ Web サイトでは重要なセキュリティ対策である。IPA では「サニタイジングのタイミングとしてはデータ入力時ではなく HTML 生成時を推奨」としている。

★実際にやってみた

サニタイジングされていないサイトに対して↓のように入力します。



この状態で次の画面へ行くと・・・・



JavaScript が実行され、alert（メッセージボックス）が出ました。

ソースコードを見てみると

```
<form action="insertuser" method="POST">
<table>
        <tr>
                <th>メールアドレス</th>
                <td><script>alert("！");</script></td>
        </tr>
        <tr>
                <th>名前</th>
                <td>aaaaa</td>
        </tr>
        <tr>
                <td>
                        <input type="submit" value="登録する">
                        <input type="button" value="戻る" onClic
                </td>
        </tr>
</table>
</form>
```

入力されたものが、そのまま HTML コードとして出力されています。
HTML の仕様では<script> </script>で囲まれた部分は JavaScript のコードとして認識されるため
alert が出てしまいます。

今回はアラートを出すだけですが、Javascript や HTML を埋め込めるということは、作成者側の意図しない動きをさせることができ、いろいろな悪いことができて今います。（XSS）

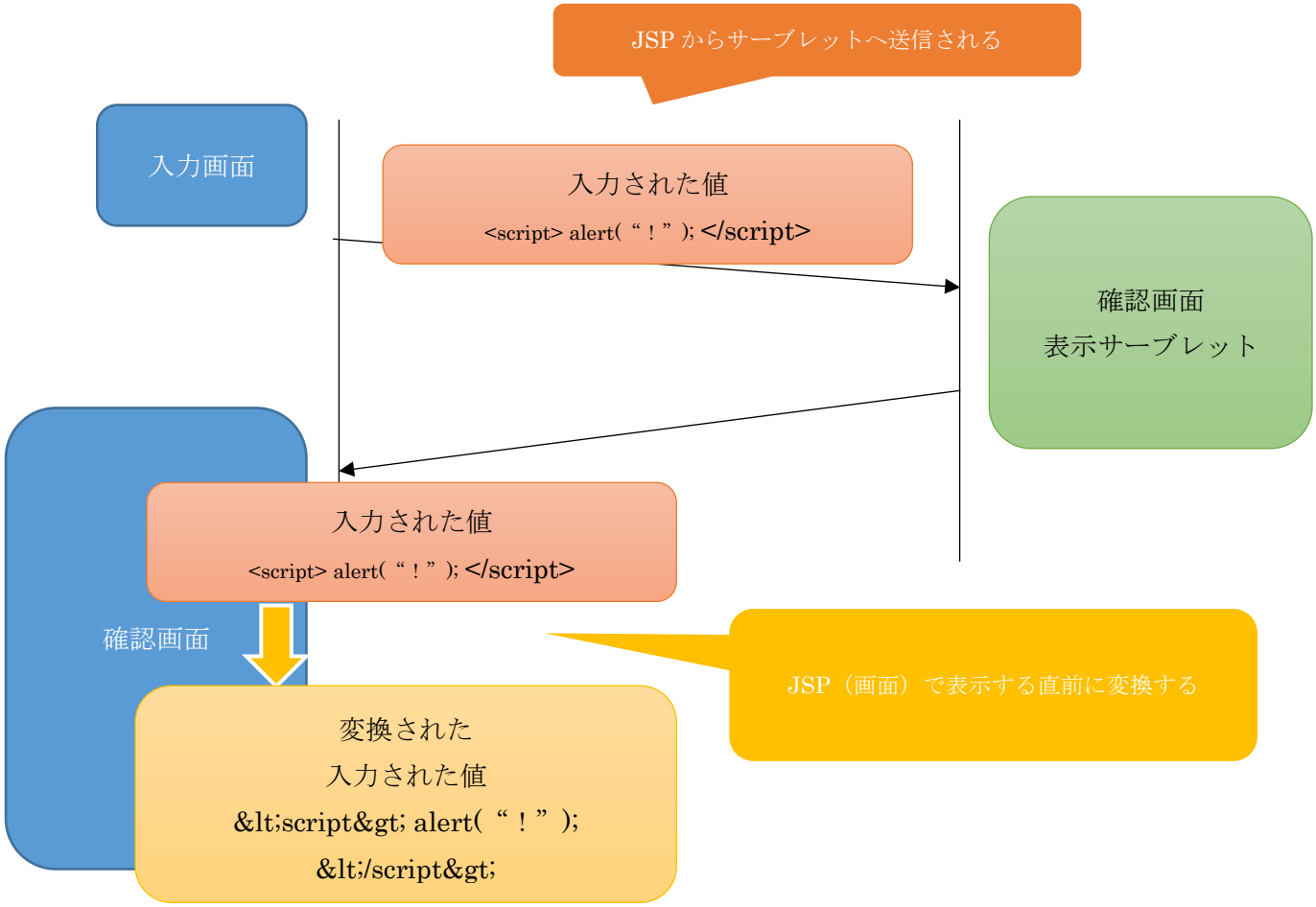
これを防ぐには、入力エリアに入力されたタグ（< , >）などを無効化する必要があります。
無効化するには、＜や＞などを「特殊文字」に置き換え、タグを表す＜や＞では無いようにすれば OK です。

特殊文字の一覧は以下の通りです。

<	<
>	>
&	&
″	"
’	'
空白文字	
文字	特殊文字

例えば、先ほどの例でテキストボックスに
　<script> alert(“！”); </script>
と入力されましたが、以下のように<と>を特殊文字に置き換えることで無効化できます
　<script> alert(“！”); </script>

この変換を入力値がサーブレットに送られてきて、サーブレットでは行わず
次の画面に表示するときに行えば OK です。



つまり、以下のようなサイニタイジング用のクラスを作って、表示直前で呼び出し入力値を変換してあげれば OK です。

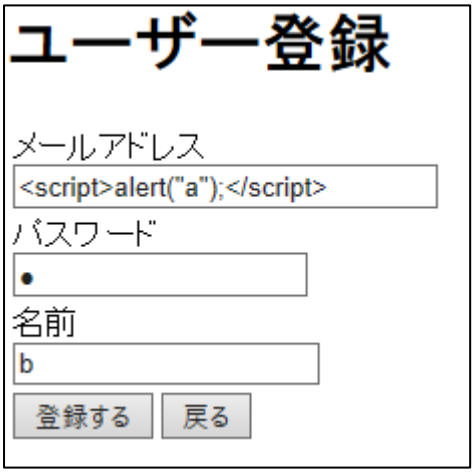
```
public class HtmlUtil {

    /**
     * 改行を＜BR＞に変換する
     * @param text
     * @return
     */
    public static String nl2be(String text){

        if( text == null ){
            return "";
        }

        text = text.replaceAll("&", "&amp;");
        text = text.replaceAll("<", "&lt;");
        text = text.replaceAll(">", "&gt;");
        text = text.replaceAll("¥"", "&quot;");
        text = text.replaceAll("¥n", "<BR>");
        text = text.replaceAll("¥r¥n", "<BR>");
        text = text.replaceAll("¥t", "    ");
        text = text.replaceAll(" ", " ");
        text = text.replaceAll("  ", " ");

        return text;
    }
}
```

サニタイジングのクラス↑

JSP にて表示直前で↓のようにして呼び出す

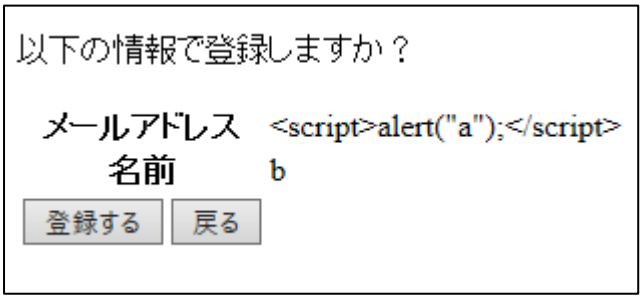
```
<table class="table table-bordered">
  <thead>
    <tr class="info">
      <th>
      問題
      <% if( taskdto.isRequiredFlg() ){ %>
        (必須)
      <% }else{ %>
        (任意)
      <% } %>
      :難易度 <%= Difficalty.search(taskdto.getDifficalty()).getMsg() %>
      </th>
    </tr>
  </thead>
  <tbody>
    <tr>
      <td><%=HtmlUtil.nl2be( taskdto.getQuestion() )%></td>
    </tr>
  </tbody>
</table>
```

このような処理を施すことで、このように表示されます。



このような入力をしても・・・・

↓



このようにタグが表示される。

↑の画面のソースを見てみると・・・

```
<form action="insertuser" method="POST">
<table>
        <tr>
                <th>メールアドレス</th>
                <td>&lt;script&gt;alert(&quot;a&quot;);&lt;/script&gt;</td>
        </tr>
        <tr>
                <th>名前</th>
                <td>b</td>
        </tr>
        <tr>
```