脆弱性体験学習ツール

AppGoat

カスタマイズマニュアル

2016 年 7 月

改定履歴

更新日	更新内容
2016 年 7 月 29 日	第 1 版 発行

内容

1. はじめに

1.1. 本マニュアルについて

本マニュアルは管理者向けに、「脆弱性体験学習ツール AppGoat」（以降、実習ツール）の画面に表示されている文言をカスタマイズ（修正）する方法を説明したものです。

1.2. カスタマイズ可能な項目

実習ツールのカスタマイズ可能な項目は以下になります。

表 1 実習ツールで可能なカスタマイズ項目と本マニュアルでの記載箇所

カスタマイズ項目	本マニュアルでの記載箇所
画像の変更・追加	2 シナリオフォルダ構成 6.1 画像の変更（追加）
シナリオの削除	2 シナリオフォルダ構成
テーマタイトルの変更	2 シナリオフォルダ構成 3.1 テーマタイトル
ステージタイトルの変更	2 シナリオフォルダ構成 3.2 ステージタイトル
コンテンツ文章の変更	2 シナリオフォルダ構成 3.3 コンテンツ文章の記述箇所 3.4 コンテンツ文章の編集ルール 6.3 説明用コンテンツの記載内容修正（学習環境に合わせたファイルパスの追記）

カスタマイズ項目	本マニュアルでの記載箇所
ヒントの追加・削除・変更	2 シナリオフォルダ構成 4 ヒント編集手順 6.2 ヒントの追加
称号名の設定	2 シナリオフォルダ構成 5.1 称号名の設定

図 1 カスタマイズ項目とリンク（タイトル・画像編）

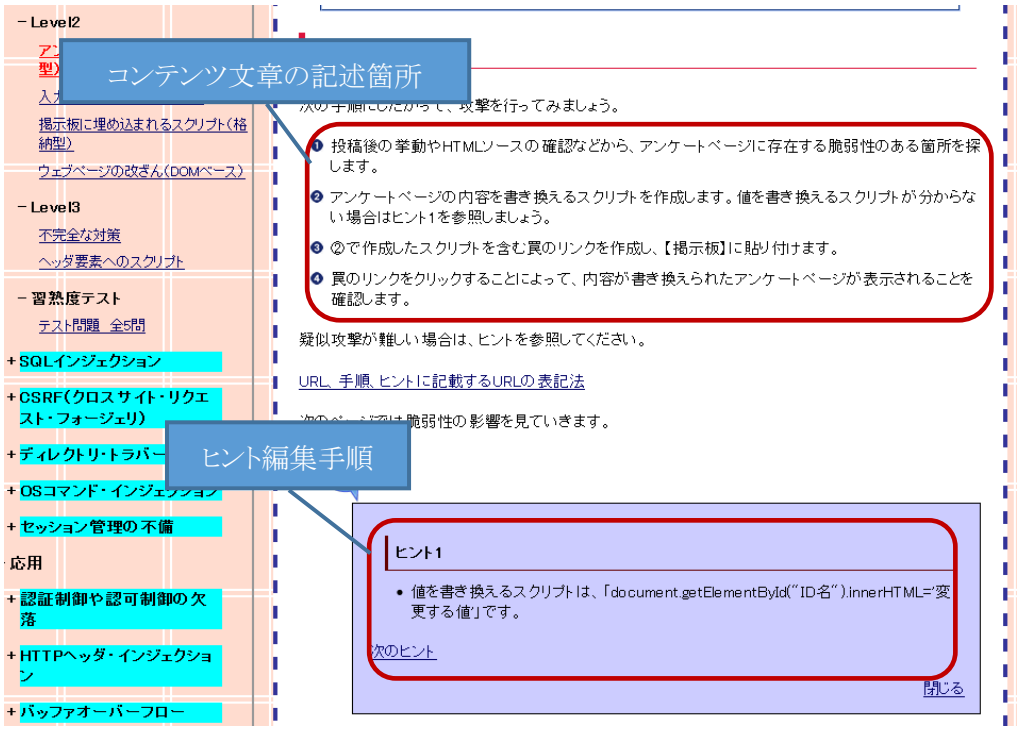

図 2 カスタマイズ項目とリンク（コンテンツ文章偏）

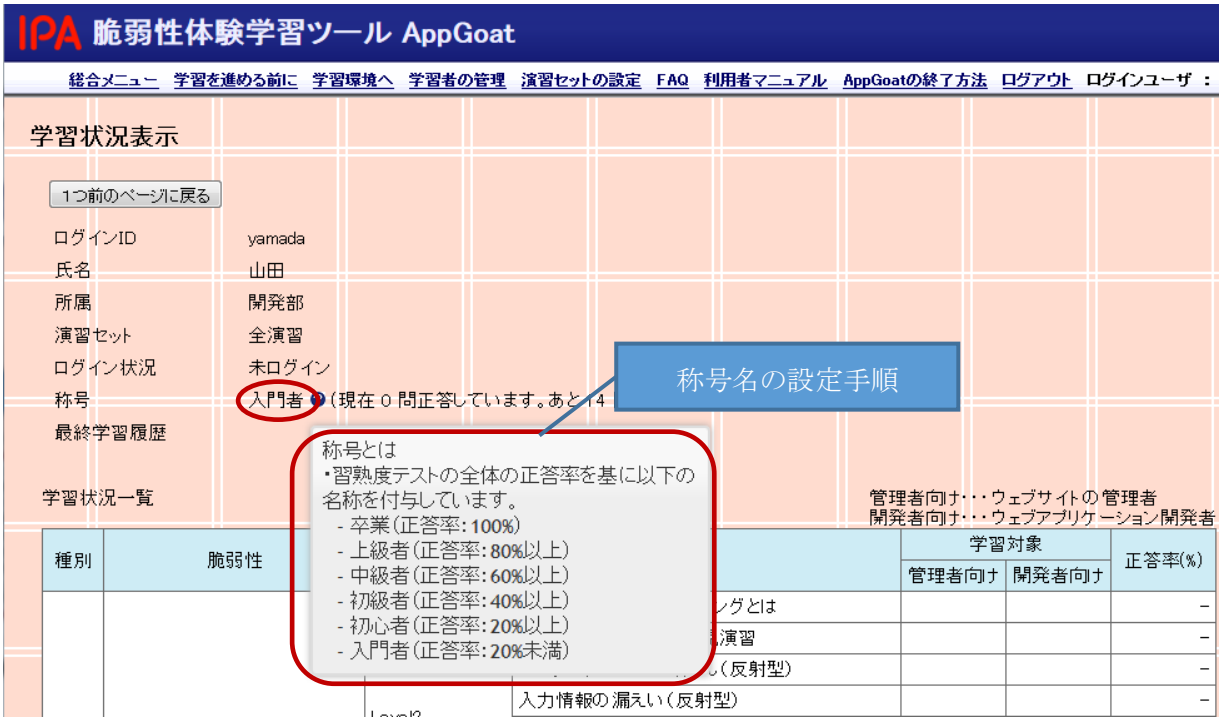

図 3 カスタマイズ項目とリンク（称号偏）

1.3. カスタマイズ上の注意

コンテンツ内では HTML の文法や AppGoat 上で作成されたクラスが多用されています。**表 1** に含まれないカスタマイズなど、修正内容によっては画面レイアウトが崩れる、演習が動かなくなる、想定外の脆弱性が生まれる、といったことが懸念されます。これらは全て修正者の自己責任で行ってください。

カスタマイズ項目の中にはアカウント作成時にのみ反映されるものが存在します。その場合、学習者のフォルダに直接反映や、アカウントの作り直しが必要になります。コンテンツのカスタマイズはアカウントの作成前に行うことを推奨します。

1.4. 用語

表 2 用語一覧

用語	意味
シナリオ	実習ツールの学習単位。複数のステージで構成される。
シナリオ番号	種別、カテゴリ、レベル、演習によって各シナリオに割り振った番号。
シナリオ ID	各シナリオに割り振った識別子（ID）。Scenario + シナリオ番号の形式で記述され、フォルダ名や呼び出し時に用いる。
テーマ	シナリオに任意の名前をつけたもの。
ステージ	テーマを分割したもの。複数のページで構成される。
ページ	テーマを構成する最小単位。
コンテンツ	ページ内に表示する文章や画像。
ヒント	演習問題において、学習者を解答に導く文言。表示非表示の切り替えが可能。
言語ファイル	実習ツールのコンテンツ（文字列）を各言語で書いたファイル。これを複数作成することで多言語化を行う。

2. シナリオフォルダ構成

ここでは、シナリオの編集や削除手順について説明します。

シナリオフォルダは「AppGoat01¥IPATool¥Scenarios¥Web」および「AppGoat01¥IPATool¥Users¥アカウント名¥Web」に格納されている、1つ1つのシナリオのファイルを格納しているフォルダで、それぞれ図 4 のような構成になっています。
「AppGoat01¥IPATool¥Scenarios¥Web」のシナリオフォルダは学習者アカウントを作成するときに「AppGoat01¥IPATool¥Users¥アカウント名¥Web」にコピーするため、全体に影響するものとなります。「AppGoat01¥IPATool¥Users¥アカウント名¥Web」のシナリオフォルダはログイン時に参照するフォルダでその学習者に影響するものとなります。

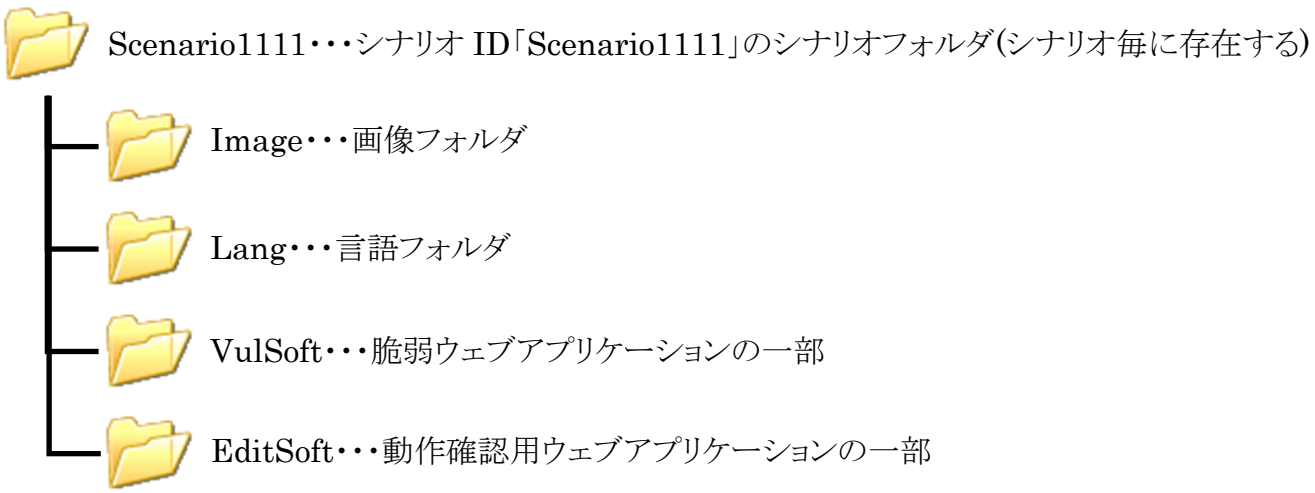

図 4 シナリオフォルダ構成

このうち、シナリオの編集をする場合は主に、言語フォルダにある言語ファイル(ja.txt)を編集します。画像を変更したい場合には画像フォルダのファイルを変更します。

シナリオの削除を行う場合には、対象のシナリオフォルダを削除します。削除したフォルダの中身は復元できませんので、削除する場合にはバックアップを取るようにしてください。削除したシナリオをもとに戻すには、元のシナリオフォルダと同じ名前で、削除したフォルダをもとに戻します。

3. シナリオ編集手順

ここでは、シナリオのコンテンツ文章（文言）の編集方法について説明します。コンテンツ文章は全て言語フォルダ内の言語ファイルに保存されています。言語ファイルは JSON という形式を使用しているため、記述の仕方を誤ると、テーマのコンテンツが表示されなくなってしまうことに注意が必要です。編集内容は変更後に作成したアカウントに反映が行われます。変更前から存在するアカウントへ反映するには、学習管理画面で対象アカウントへの「学習状況の全初期化」の実行が必要です。詳細は「6.2 ヒントの追加」の手順⑤をご覧ください。

※特定の文字の前の¥について

「”」~「”」を編集するため、「”」が文字なのか、終わりを表すのか区別するために文字の場合には「”」の前に¥の文字を記載する必要があります。このように、特定の文字の前には¥の文字の記載が必要です。

3.1. テーマタイトル

テーマタイトルは図 5 の赤い丸で囲んだ部分に相当します。

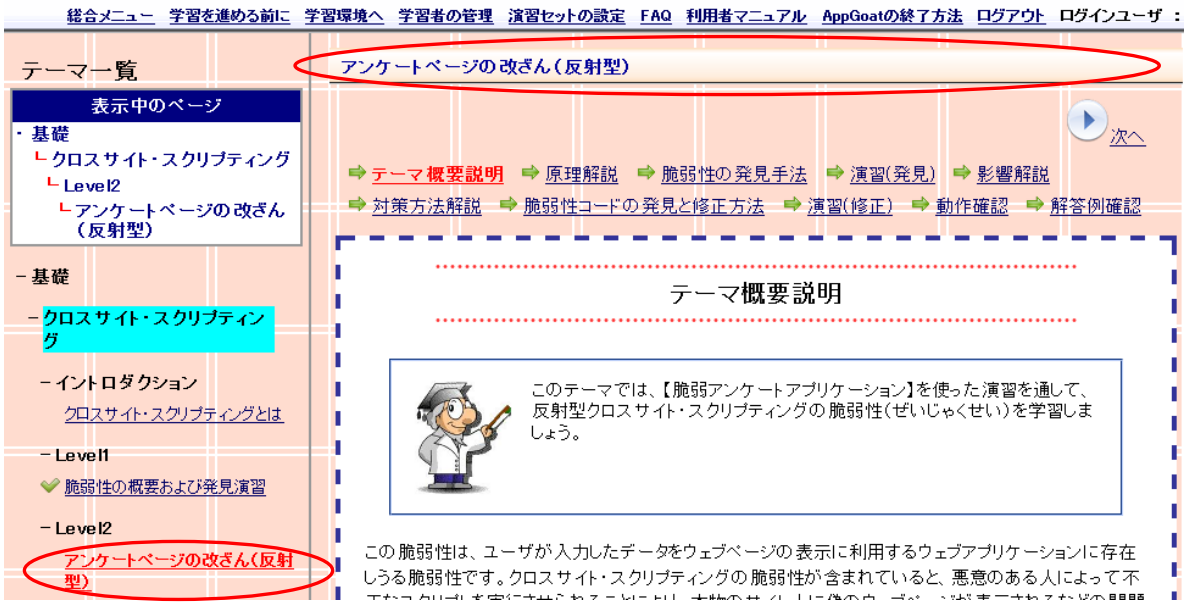

図 5 テーマタイトルの位置

テーマタイトルを変更したい場合は、シナリオ言語ファイルの「scenario_title」を編集します。

```
{
  "scenario_title" : "アンケートページの改ざん（反射型）",
...
}
```

図 6 テーマタイトル

3.2. ステージタイトル

ステージタイトルは図 7 の赤い丸で囲んだ部分に相当します。

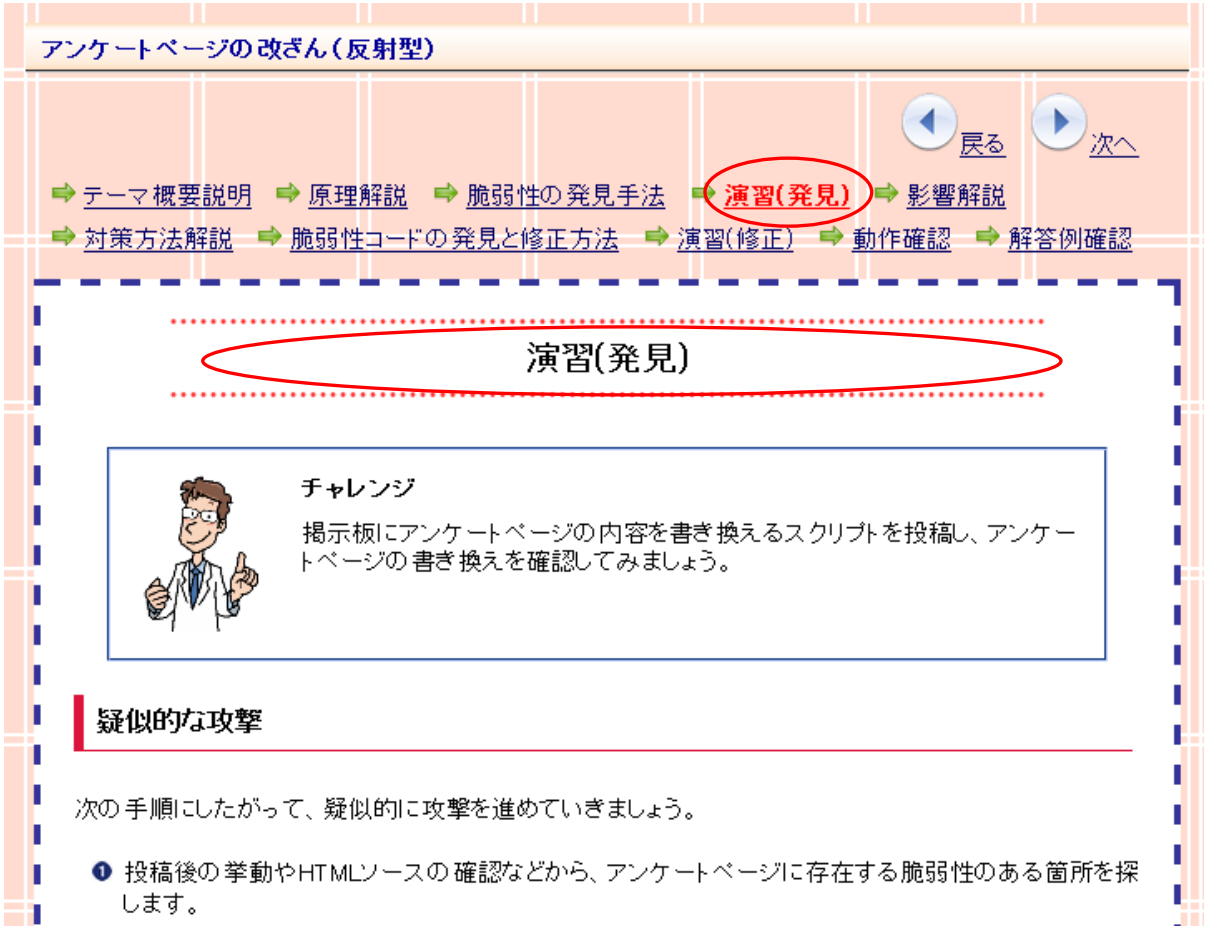

図 7 ステージタイトルの位置

ステージタイトルを変更したい場合は、シナリオ言語ファイルの「stage_title」を編集します。

```
…
  "stage4" : {
    "stage_title" : "演習(発見)",
…
```

図 8 ステージタイトルの例

3.3. コンテンツ文章の記述箇所

テーマは１つ以上のステージ(stage1～stage[n])で構成され、ステージは１つ以上のページ(page1～page[n]) で構成されています。HTML コンテンツは、ページ単位に用意され、HTML コンテンツを編集する場合は、ページの「contents」という項目を編集します。

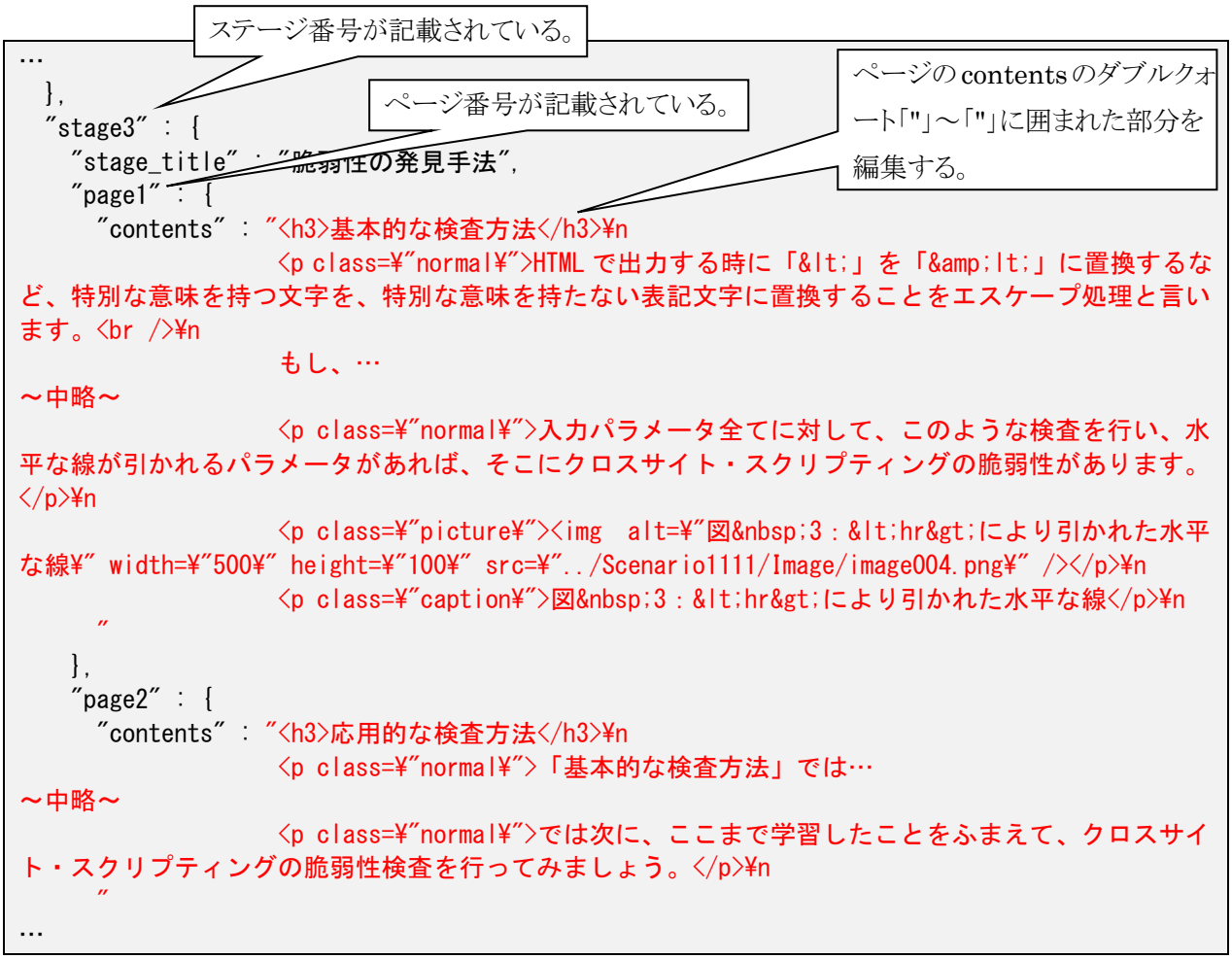

図 9 HTML コンテンツの記述箇所

3.4. コンテンツ文章の編集ルール

コンテンツ文章の編集にはいくつかのルールがあります。以下に示す記述ルールにしたがい編集します。

表 3 コンテンツ文章編集ルール一覧

分類	言語ファイルの 修正箇所	目的	記載コード
改行	<code>~</code>外	HTML ソース	¥n
	<code>~</code>外	HTML コンテンツ	
	<code>~</code>内	HTML ソース HTML コンテンツ	¥n
ダブルクォート	<code>~</code>外	HTML ソース	¥"
	<code>~</code>外	HTML コンテンツ	"
	<code>~</code>内	HTML ソース HTML コンテンツ	¥" または "
シングルクォート	<code>~</code>外	HTML ソース	'
	<code>~</code>外	HTML コンテンツ	'
	<code>~</code>内	HTML コンテンツ	' または '
円マーク	<code>~</code>外 <code>~</code>内	HTML コンテンツ	¥¥
「<」および「>」	<code>~</code>外 <code>~</code>内	HTML ソース	< および >
	<code>~</code>外 <code>~</code>内	HTML コンテンツ	< および >

改行

JSON 形式データでは改行は特に意識しませんが、HTML ソース上で改行を表すために、明示的に「¥n」を用います。文章が長くなったときは改行を行い、ブラウザからソースを表示した際の可読性を向上させましょう。HTML コンテンツとして改行を行うには<code>～</code>外は明示的に「
」を用います。<code>～</code>内では明示的に「¥n」を用います。また、言語ファイルの ～ 内の文章は、次の ～ 内の文章との間に行間が入る設定にしています。

```
      "contents" : "<h3>基本的な検査方法</h3>¥n

                   <p class=¥"normal¥">HTML で出力する時に「&lt;」を「&amp;lt;」に置換するなど、特別な意味を持つ文字を、ブラウザで特別な意味を持たない表記文字に置換することをエスケープ処理と言います。<br />¥n

                   もし、受け取った入力データを、エスケープ処理を行わずに画面に出力している箇所があれば、クロスサイト・スクリプティングの脆弱性になります。</p>
                   <p class=¥"normal¥">検査方法の一例を以下に示します。</p>¥n
...
}
```

1 行で改行される。

この場合、言語ファイルの見た目上は複数行でも、HTML ソースとして出力されると 1 行として扱われ、ここで改行される。

図 10 改行の例

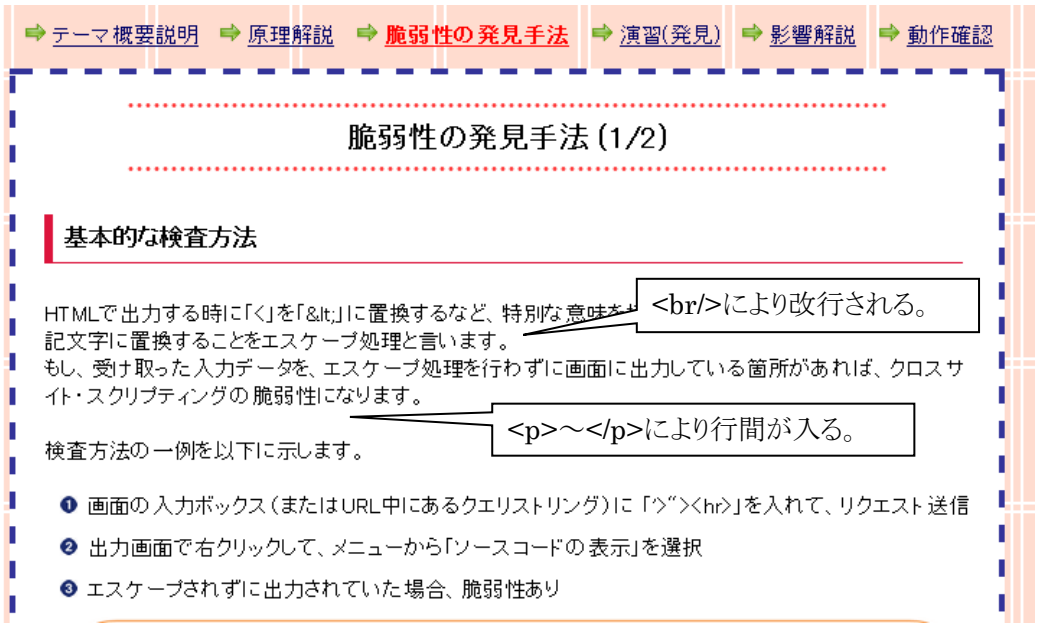

図 11 改行の例

ダブルクォート

ダブルクォートはJSON形式の引用符を表すため、ダブルクォートの前に¥の文字を記載します。ただし、HTMLコンテンツとしてダブルクォートを表示する場合はHTML特殊文字「"」を使用します。また、ソースコードを表す<code>～</code>内にダブルクォートを使用する場合にもダブルクォートの前に¥の文字を記載するか、HTML特殊文字「"」を使用します。

```
…
                    <p class=¥"normal¥">外部に出力している箇所において入力パラメータを受け取
った後、出力文字列にエスケープ処理をせず                    箇所があれば、クロスサイト・スクリプティ
ングの脆弱性になります。<br />¥n
                    PHPでは外部
$_GET[&quot;name&quot;]などが使
いない箇所                    ことを確認しましょう。</p>¥n
…
```

タグの属性に使用するダブルクォートは、ダブルクォートの前に¥の文字を記載する。

HTMLコンテンツとして表示する場合は「"」を使用する。

図 12 ダブルクォートの例1

```
…
        <pre><code>¥n
public function login()¥n
…
$stmt = $db->prepare(¥"SELECT * FROM user WHERE id = ? AND password = ?¥");
…
</code></pre>¥n
…
```

ソースコード中でダブルクォートを表す場合は「¥"」か「"」のどちらでもよい。

図 13 ダブルクォートの例2

シングルクォート

シングルクォートはJSON形式の引用符ではないため、シングルクォートの前に¥の文字の記載は必要ありませんが、HTML コンテンツとして表示する場合には「'」を使用します。ただしソースコードを表す<code>～</code>内にはそのまま「'」を使用することもできます。

```
…
            <p>たとえば、&amp;lt;script&amp;gt;alert(&amp;#39;Hello&amp;#39;);&amp;lt;/script&amp;gt;という文字列を出
力する場合には、エスケープ処理を施して
&amp;amp;lt;script&amp;amp;gt;alert(&amp;amp;#39;Hel                                    す。</p>
…
```

HTMLコンテンツとして表示する場合は「'」を使用する。

図 14 シングルクォートの例1

```
…
<pre><code>¥n
public function proc_send()¥n
…
if(!preg_match('/¥¥n|¥¥r/ ',  $param[self::FROM])){¥n
…
</code></pre>¥n
…
```

ソースコードの箇所(<code>～</code>内)には「'」を使用してもよい。

図 15 シングルクォートの例 2

また、タグの属性値の引用符としてシングルクォートは使用せず、ダブルクォートを使用してください。

間違った例：　

正しい例：　

円マーク

円（¥）マークを表示するには、円マークの前に¥の文字の記載が必要なため、円マーク 1 つを表すのに「¥¥」とします。ソースコード中の円マークも同じです。ただし、Faq の HTML ファイルはフレームワークで処理されないためそのまま「¥」を用います。

```
…
                    <ol>¥n
                      <li class=¥"order1¥">商品管理ページの変更後ファイル名入力欄に、以下のフ
ァイル名を入力してみましょう。<br>「exampe.txt &amp; dir /b c:¥¥」</li>¥n
                     </ol>¥n
…
```

円マークの前に¥の文字を記載して「¥¥」にする。

図 16 円マークの例1

```
…
<pre><code>¥n
public function proc_send()¥n
…
if(!preg_match('/¥¥n|¥¥r/ ', $param[self::FROM])){¥n
…
</code></pre>¥n
…
```

ソースコードで「¥n」を文字として表す場合、「¥¥n」にする

図 17 円マークの例 2

「<」および「>」

半角記号「<」と「>」は HTML におけるタグ文字にあたるため、そのまま記述すると、デザインが崩れることがあります。「<」と「>」はそれぞれ『<』と『>』にします。これは<code>～</code>内のソースコードの部分でも同じです。

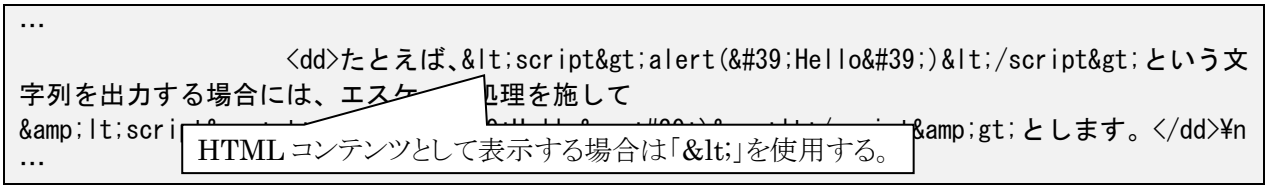

図 18「<」および「>」の例

4. ヒント編集手順

ここでは、演習のヒント文章（文言）の編集方法について説明します。ヒント文章は全て言語フォルダ内の言語ファイルに保存されています。言語ファイルは JSON という形式を使用しているため、記述の仕方を誤ると、テーマのコンテンツが表示されなくなってしまうことに注意が必要です。

4.1. ヒントボタン

ヒントボタンは図 19 の赤い丸で囲んだ部分に相当します。

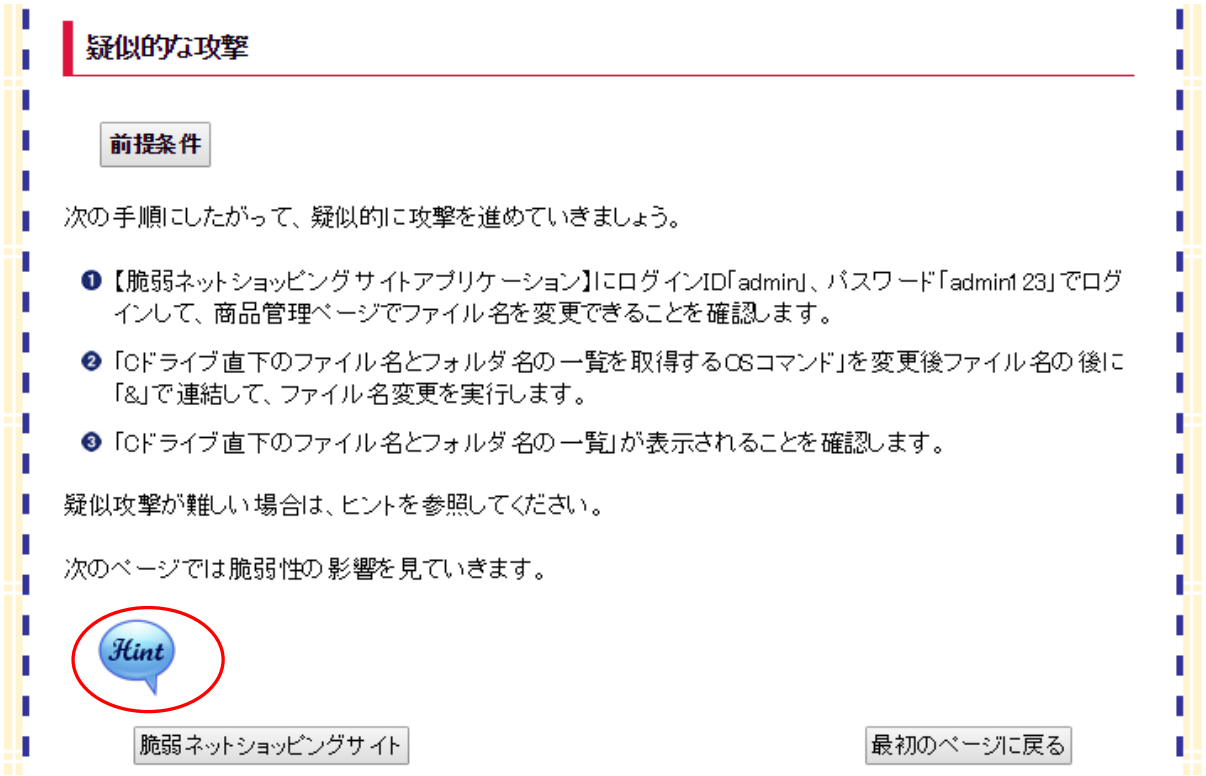

図 19 ヒントボタンの位置

4.2. ヒント内容

ヒント内容は図 20 の赤い丸で囲んだ部分に相当します。

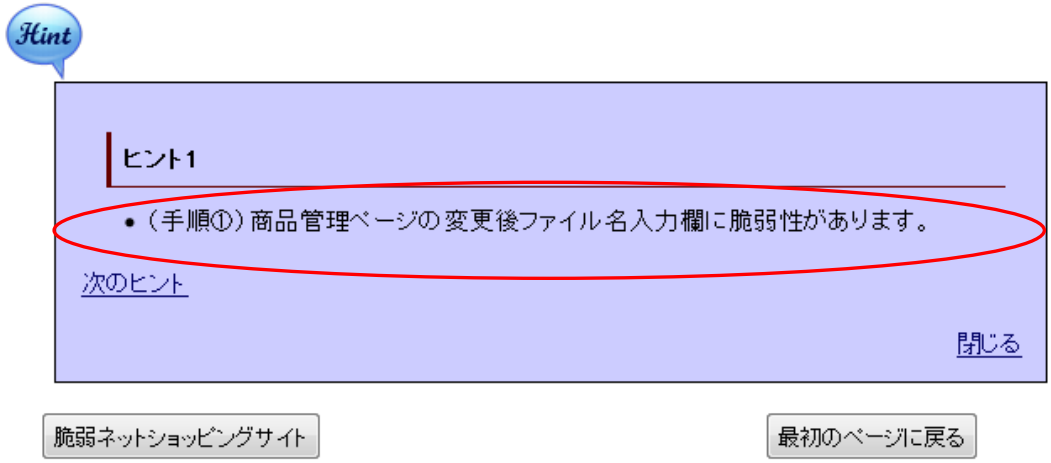

図 20 ヒント内容の位置

ヒント内容を変更したい場合は、シナリオ言語ファイルの「hint[n]」を編集します。

```
…
      "contents" : "…",
      "hint1" : "<ul><li>（手順①）商品管理ページの変更後ファイル名入力欄に脆弱性があります。
</li></ul>",
      …
…
```

図 21 ヒント内容

4.3. ヒント内容の記述箇所

ヒントはステージ内でコンテンツと演習アプリケーションの間に位置します。ヒントは 1 つ以上のヒント項目（hint1～hint[n]）で構成されています。ヒントは演習単位に用意され、ヒントを編集する場合は、ページの「hint[n]」という項目を編集します。ヒント項目は必要に応じて、増やしたり減らしたりできます。

```
…
      "contents" : "…",
      "hint1" : "<ul><li>（手順①）商品管理ページの変更後ファイル名入力欄に脆弱性があります。</li></ul>",
      "hint2" : "<ul><li>（手順②）「C ドライブ直下のファイル名とフォルダ名の一覧を取得する OS コマンド」は「dir /b c:&yen;」です。</li></ul>",
      "vulsoft1" : {
        "title" : "脆弱ネットショッピングサイト",
        "src" : "VulSoft/netshopping.php"
      }
```

図 22 ヒント内容の記述箇所

4.4. ヒント文章の編集ルール

ヒント文章の編集にはいくつかのルールがあります。以下に示す記述ルールに従い編集します。

表 4 ヒント文章の編集ルール

分類	目的	記載コード
ダブルクォート	HTML ソース	¥"
	HTML コンテンツ	&quot;
シングルクォート	HTML コンテンツ	&#39;
円マーク	HTML コンテンツ	&#92;

ダブルクォート

ヒント内容中にダブルクォートをコードとして表示する場合は HTML 特殊文字「"」を使用します。

```
…
      "hint1" : "<ul><li>（手順①）アンケートページの名前欄に脆弱性があります。</li>
                  <li>（手順②）document.getElementById(&quot;account&quot;).innerHTML の
値を書き換えると、アンケートページの内容を書き換えることができます。</li></ul>",
…
```

コードとして表示する場合は「"」を使用する。

図 23 ダブルクォートの例

シングルクォート

ヒント内容中にシングルクォートをコードとして表示する場合は「'」を使用します。

```
…
      "hint3" : "<ul><li>（手順③）次の URL を【掲示板】に投稿してみましょう。「http://ホスト
/Web/Scenario1121/VulSoft/enquete.php?page=2&amp;sex=0&amp;old=1&amp;company=&amp;xss=1&amp;
trouble=1&amp;
      content=&name=&lt; script&gt;
document.getElementById(&quot;account&quot;).innerHTML =
&#39;&lt;font color=&quot;blue&quot; size=&quot;3&quot;&gt;もれなく一万円をプレゼ
ントいたします。名前、住所、口座番号を入力してください。&lt;/font&gt;&#39;;&lt;/script&gt;」
</li></ul>",
…
```

「'」を使用する。

図 24 シングルクォートの例

円マーク

円（¥）マークを表示するには、「\」を使用します。コード中の円マークも同じです。

```
…
      "hint3" : "<ul><li>（手順②）次のように変更後ファイル名を入力してみましょう。<br />
「exampe.txt &amp; dir /b c:&#92;」</li></ul>",
…
```

「\」を使用する。

図 25 円マークの例

5. 称号名の設定手順

ここでは習熟度テストで得られる称号名の設定の変更を説明します。称号名は全て言語フォルダ内の言語ファイルに保存されています。言語ファイルは JSON という形式を使用しているため、記述の仕方を誤ると、テーマのコンテンツが表示されなくなってしまうことに注意が必要です。

5.1. 称号名の設定

称号は図 26 の赤い丸で囲んだ部分に相当します。称号の説明が記載されているツールチップが存在し、それは図 26 の噴出し部分に相当します。また、学習の進め方にも図 27 のように称号の説明が記載されています。

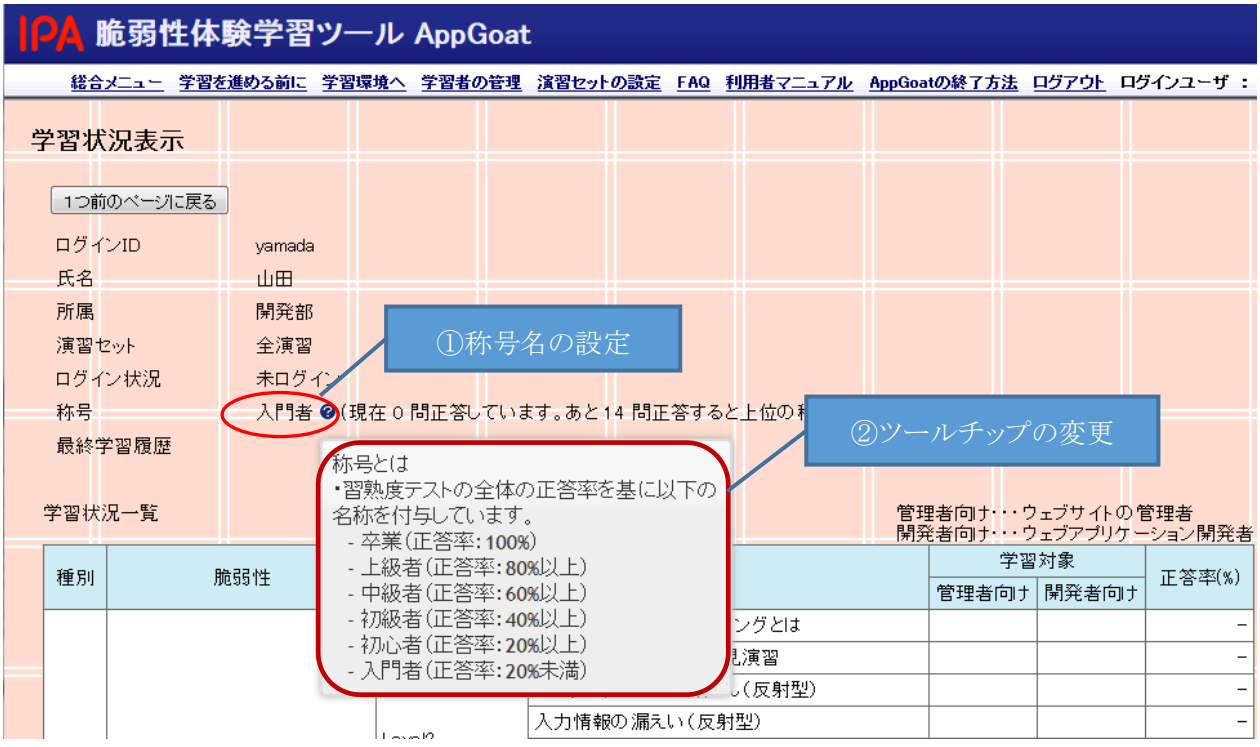

図 26　称号名の修正箇所とリンク

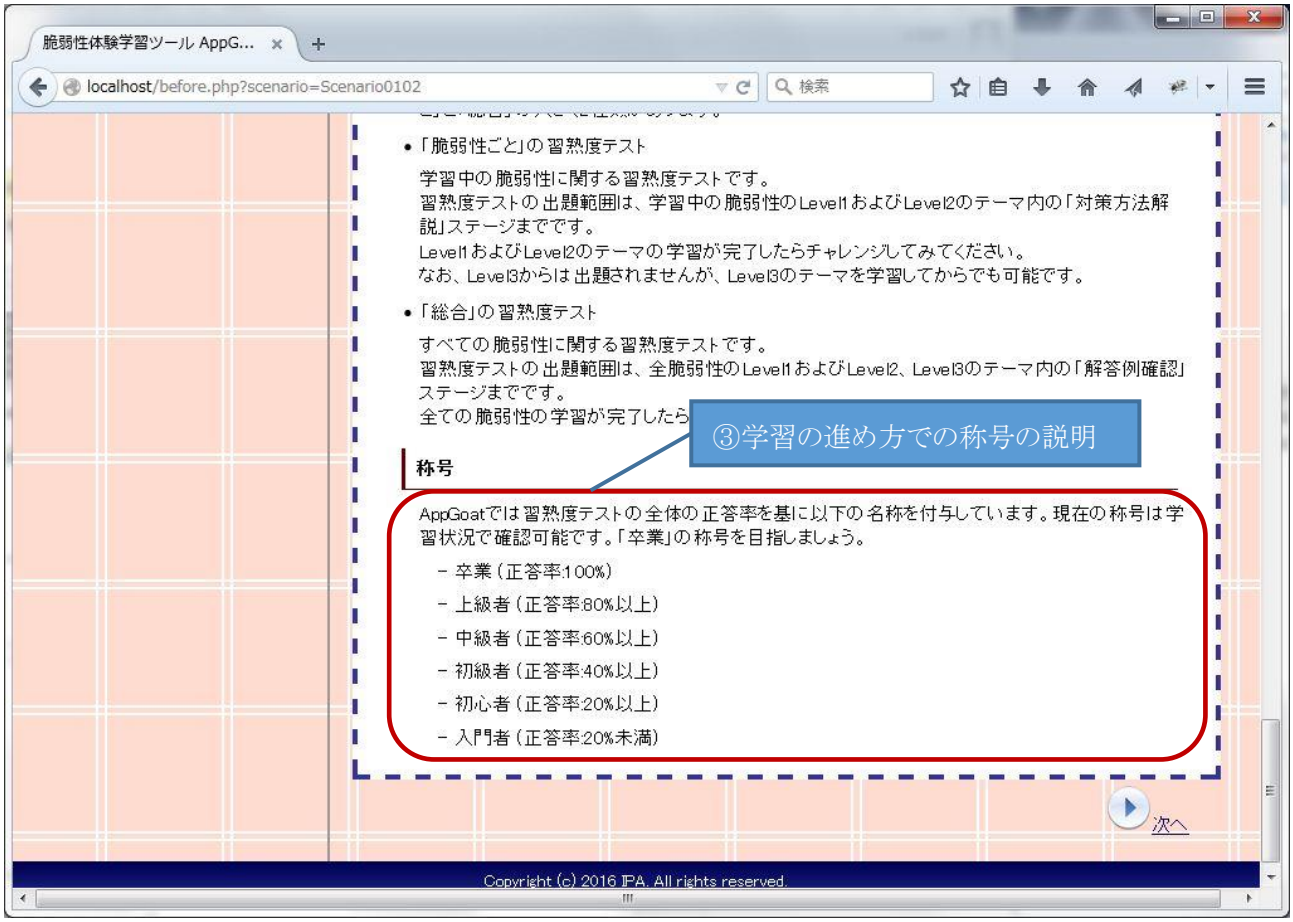

図 27 学習の進め方での称号の説明とリンク

図 26 や図 27 のようにデフォルトで称号名が設定されています。称号名を変更したい場合は、

① 称号名の設定

② ツールチップの記載

③ 学習の進め方での称号の説明

以上の 3 箇所を変更する必要があります。また、①、③の反映は一括処理の「学習状況の全初期化」では行えません。変更後に作成する学習者アカウントには自動で反映されますが、変更前から存在するアカウントに対しては、一度削除してアカウントを作成しなおすか、「IPATool¥Users¥アカウント名¥Web」のフォルダに対して同様の処理を行う必要があります。

5.1.1. ①称号名の設定

称号名の設定は「IPATool¥Scenarios¥Web¥Lang」の ja.txt ファイルに記載されています。称号名を変更したい場合は、「rank」を編集します。

```
    },
    "rank" : {
      "RANK1" : "卒業",
      "RANK2" : "上級者",
      "RANK3" : "中級者",
      "RANK4" : "初級者",
      "RANK5" : "初心者",
      "RANK6" : "入門者"
    }
  }
```

図 28 称号の設定

5.1.2. ②ツールチップの変更

ツールチップの内容は「IPATool¥Framework¥Lang」の ja.txt ファイルに記載されています。称号名を変更した場合は、学習者が混乱しないように「tooltip_rank_note」を編集します。

```
{
    …
    "label_progress" : "最終学習履歴",
    "label_no_progress_quiz" : "未実施",
    "tooltip_rank_note" : "称号とは<BR>・習熟度テストの全体の正答率を基に以下の名称を付与しています。<BR>　- 卒業（正答率 : 100%）<BR>　- 上級者（正答率 : 80%以上）<BR>　- 中級者（正答率 : 60%上）<BR>　- 初級者（正答率 : 40%以上）<BR>　- 初心者（正答率 : 20%以上）<BR>　- 入門者（正答率 : 20%未満）",
    "title_show_practice_set_menu" : "演習セット管理",
    …
}
```

図 29 ツールチップ

5.1.3. ③学習の進め方での称号の説明

学習の進め方の内容は「IPATool¥Scenarios¥Web¥Scenario0102¥Lang」の ja.txt ファイルに記載されています。称号名を変更した場合は、学習者が混乱しないように内容を変更します。

```
        </ul>
          <dt>称号</dt>¥n
           <dd>AppGoat では習熟度テストの全体の正答率を基に以下の名称を付与しています。
現在の称号は学習状況で確認可能です。「卒業」の称号を目指しましょう。</dd>¥n
           <dd>&amp;nbsp;&amp;nbsp;&amp;nbsp;-&amp;nbsp;卒業（正答率:100%)</dd>
           <dd>&amp;nbsp;&amp;nbsp;&amp;nbsp;-&amp;nbsp;上級者（正答率:80%以上)</dd>
           <dd>&amp;nbsp;&amp;nbsp;&amp;nbsp;-&amp;nbsp;中級者（正答率:60%以上)</dd>
           <dd>&amp;nbsp;&amp;nbsp;&amp;nbsp;-&amp;nbsp;初級者（正答率:40%以上)</dd>
           <dd>&amp;nbsp;&amp;nbsp;&amp;nbsp;-&amp;nbsp;初心者（正答率:20%以上)</dd>
           <dd>&amp;nbsp;&amp;nbsp;&amp;nbsp;-&amp;nbsp;入門者（正答率:20%未満)</dd>
      </dl>¥n
      "
    }
 },
"stage2" : {
```

図 30 学習の進め方での称号の説明

6. カスタマイズ実施例

ここでは、利用が多そうなカスタマイズをピックアップして修正方法例を紹介します。

6.1. 画像の変更(追加)

ここでは画像を変更・追加する手順を説明します。

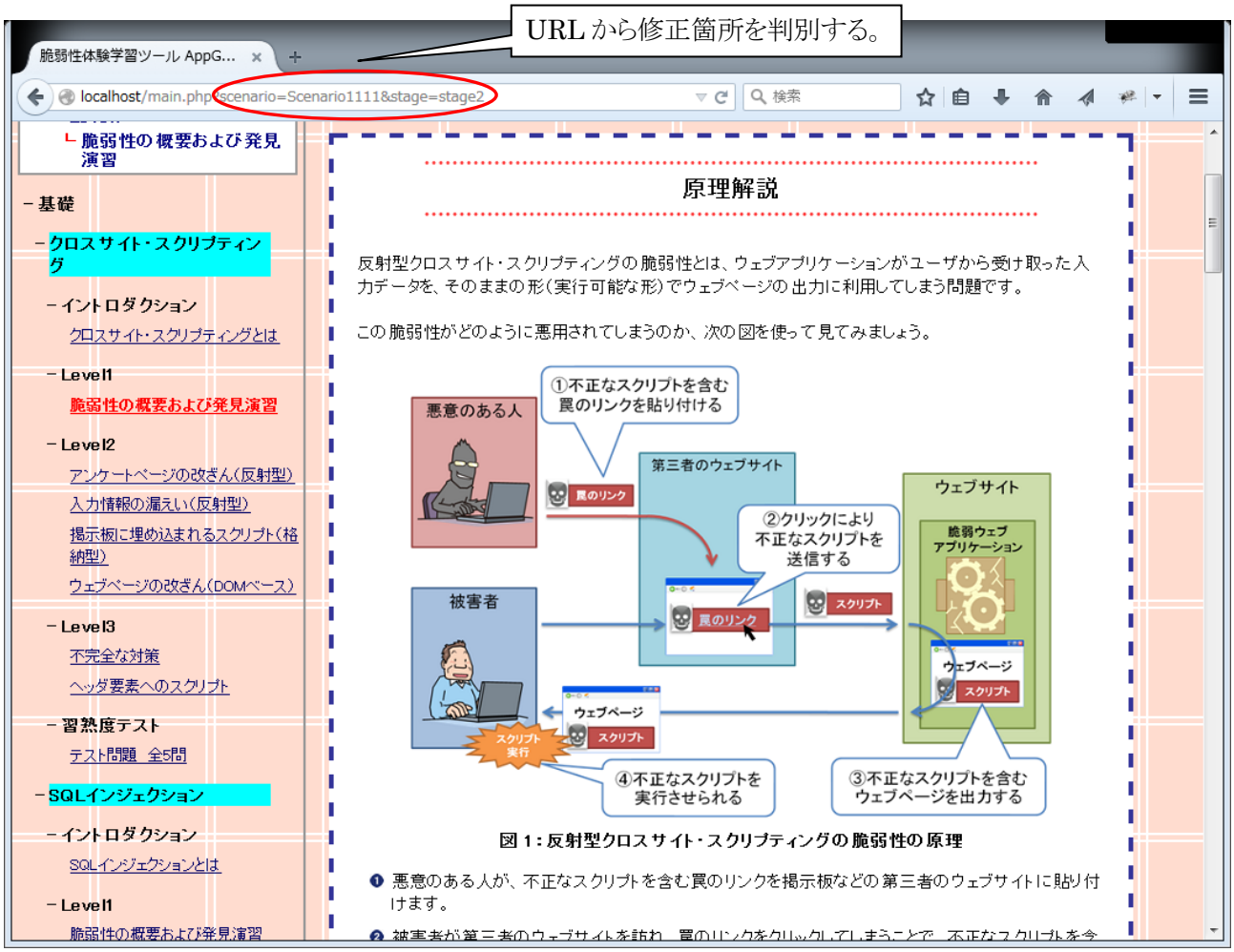

図 31　カスタマイズ対象の画面

概要　シナリオ ID「Scenario1111」の原理解説の画像を変更（追加）する

手順

① 修正するシナリオの画像フォルダを開く

URL に着目すると、「scenario=Scenario1111」となっています。対象となるシナリオフォルダは「IPATool¥Scenarios¥Web¥Scenario1111」となります。画像フォルダである Image フォルダを開きます。

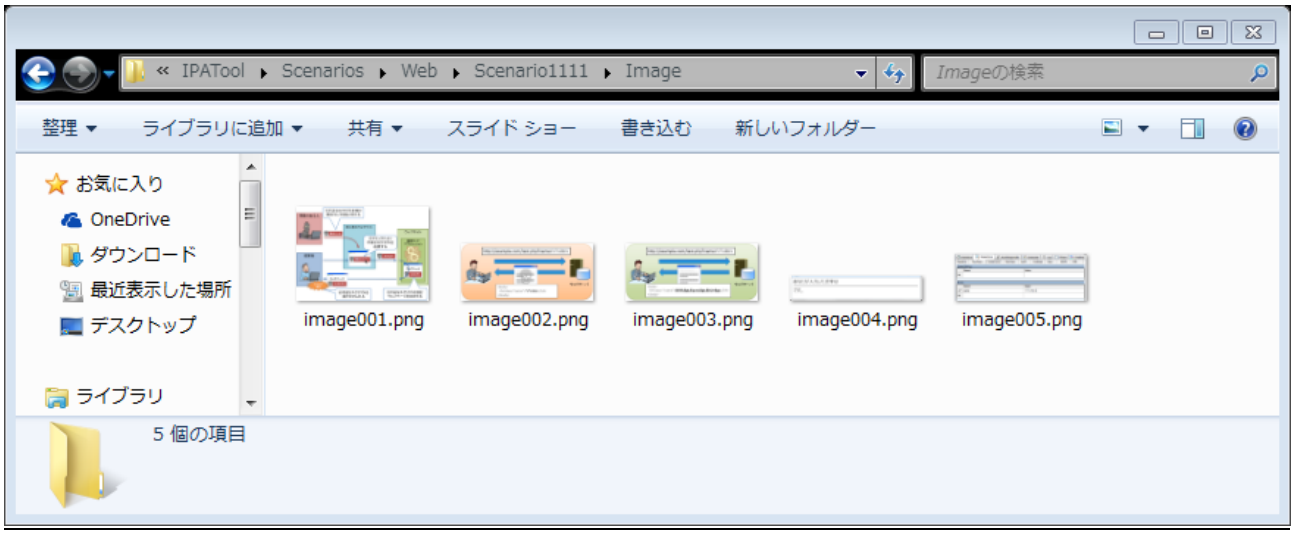

図 32　変更前の画像フォルダ

② 画像ファイルを変更する（画像変更の場合）

変更する画像を変更したい画像に置き換えます。手順⑥に移ります。

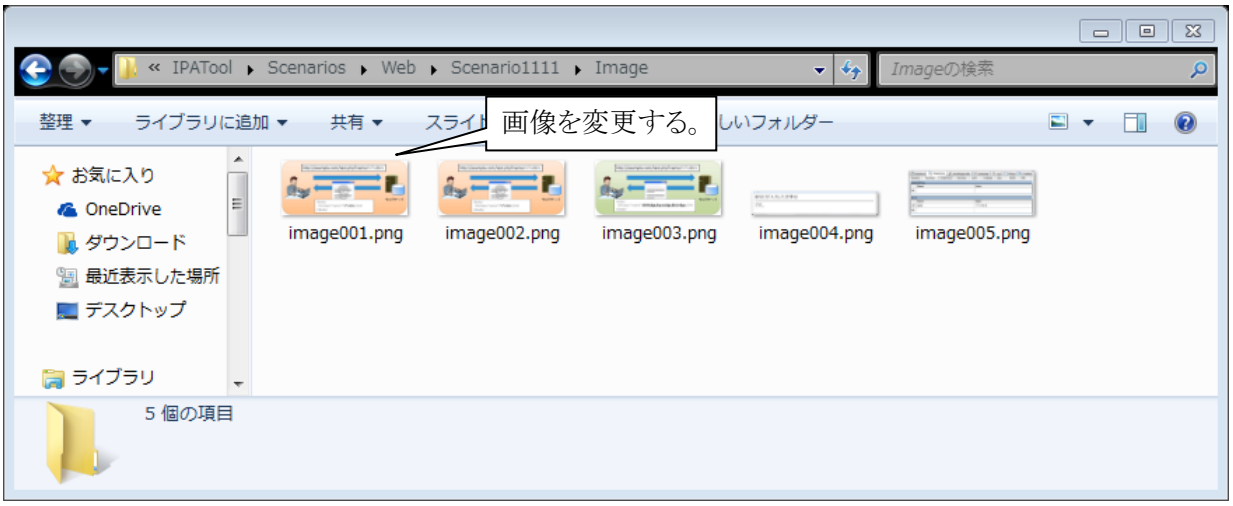

図 33　画像変更後の画像フォルダ

③ 画像を追加する（画像追加の場合）

画像フォルダに追加したい画像を追加します。

図 34　画像追加後の画像フォルダ

④ 言語ファイルを開く（画像追加の場合）

文章（画像）は言語ファイルで記述されているので、シナリオフォルダ配下の Lang フォルダの ja.txt を開きます。

⑤ 言語ファイルに画像の表示を記載する（画像追加の場合）

URL に着目すると「stage=stage2」となっているので stage2 を確認します。変更前の記述は**図 35** のようになっており、画像の表示には赤枠部分を用いています。画像を追加したい場所にこの赤枠部分をコピーします。その後、この場合パスの「image001.png」部分を追加した画像ファイル名に置き換えます。また、width、height の値で横と縦のサイズの調整、図タイトルの変更を行います。

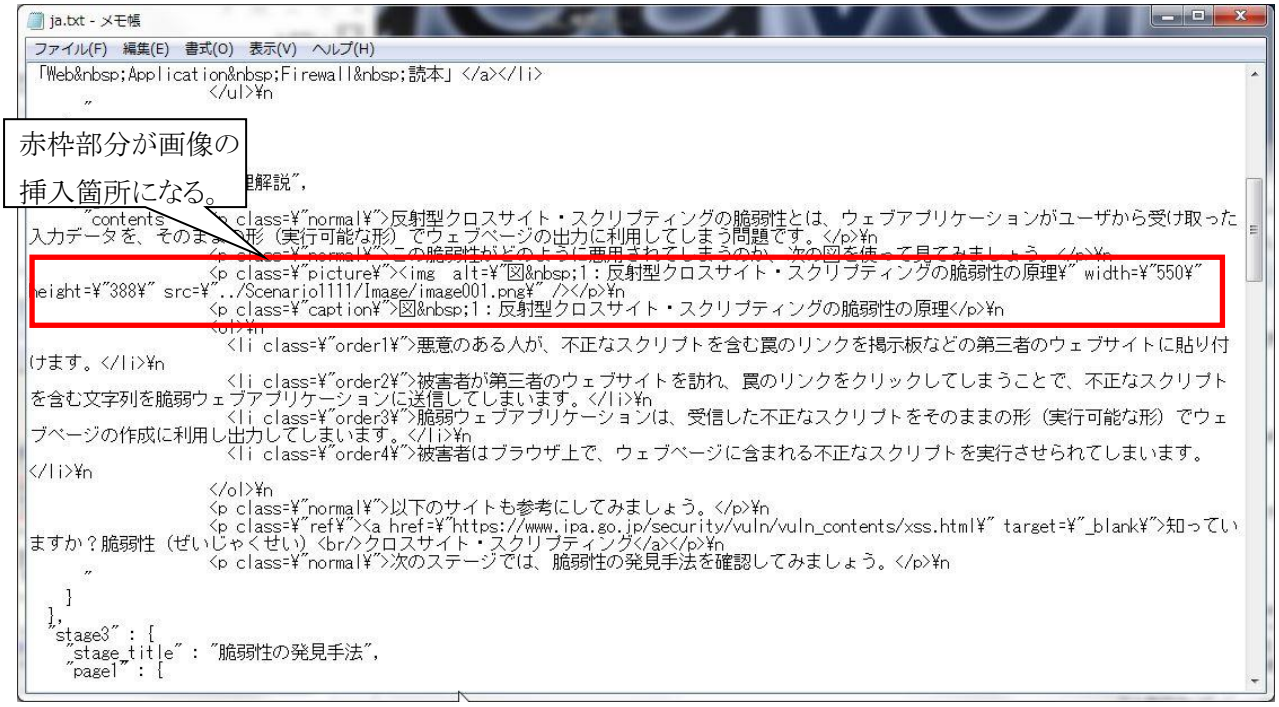

図 35　変更前の記述

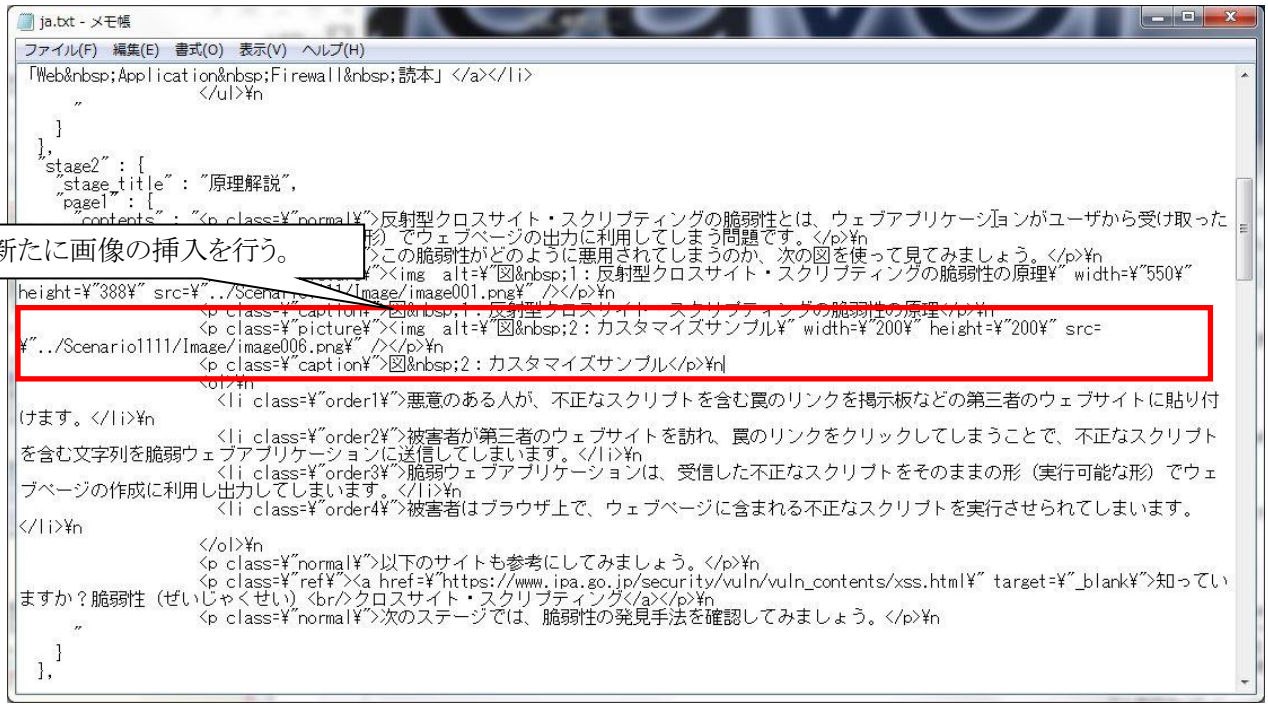

図 36　変更後の記述

⑥ 各アカウントへの反映

画像ファイルの反映は一括処理の「学習状況の全初期化」では行えません。画像の変更（追

加）後に作成する学習者アカウントには自動で反映されますが、変更前から存在するアカウントに対しては、一度削除してアカウントを作成しなおすか、「IPATool¥Users¥アカウント名¥Web」のシナリオフォルダに対して②～⑥の処理を行う必要があります。

カスタマイズ結果

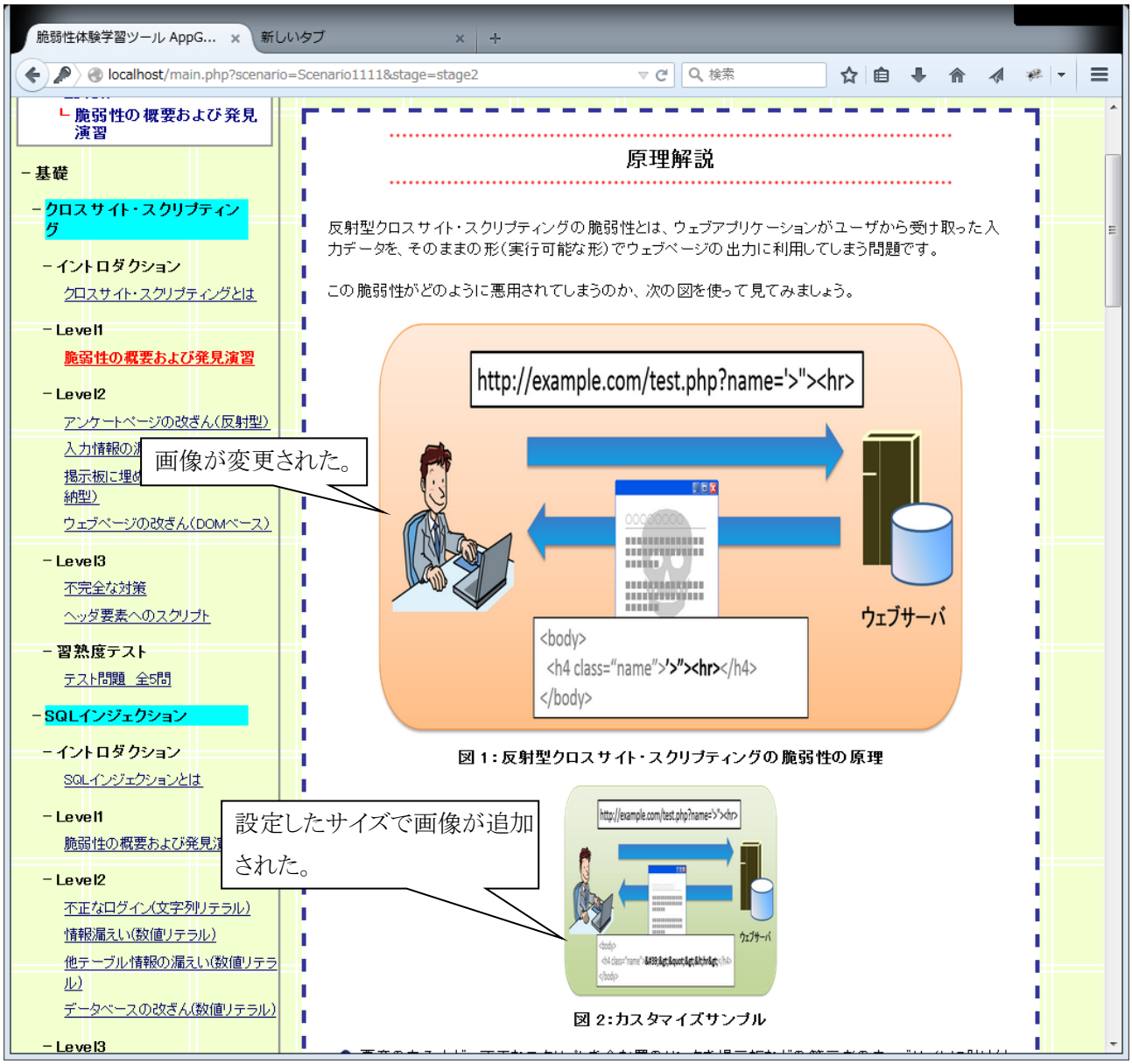

図 37　カスタマイズ後の画面

6.2. ヒントの追加

ここでは、ヒントの追加およびコンテンツ文章の変更を学習者全体に反映する手順を説明します。

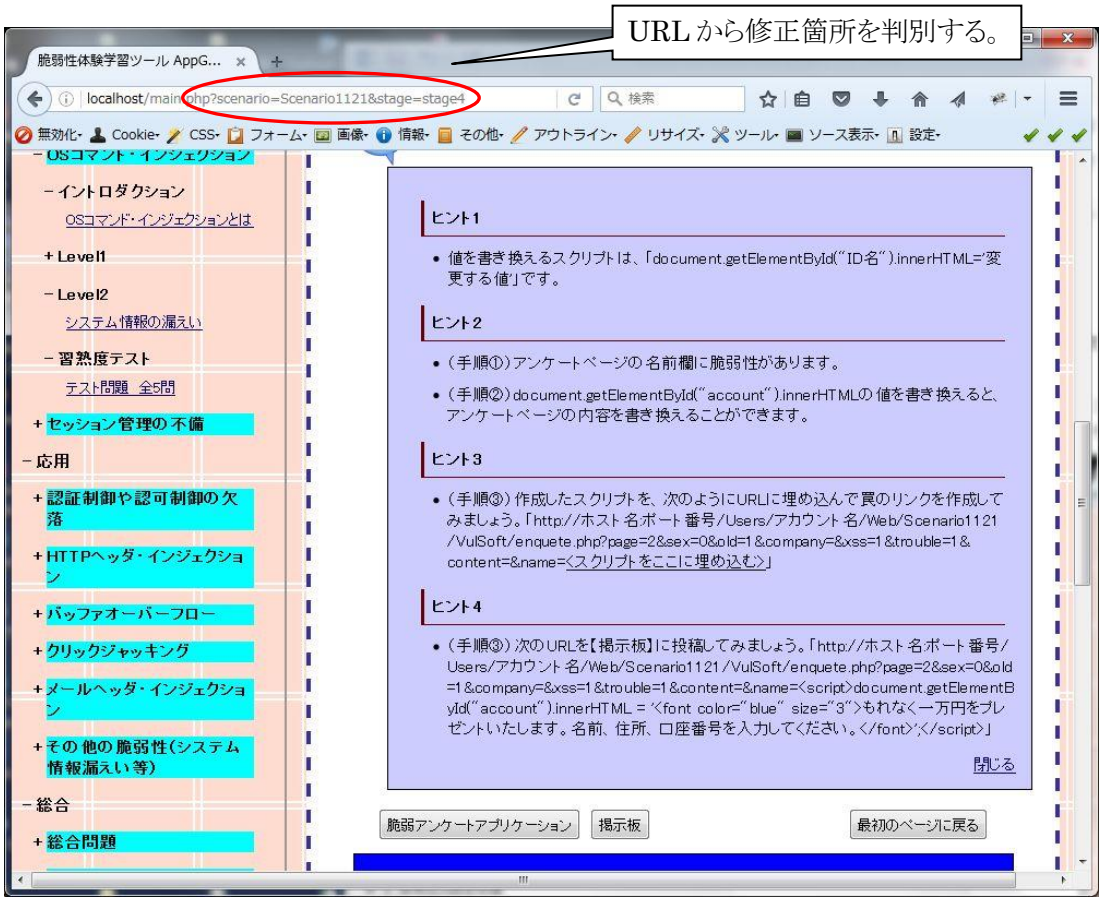

図 38　カスタマイズ対象の画面

概要　シナリオ ID「Scenario1121」のヒント 2 を 2 つにわけ、ヒントを 5 段階にする

手順

① 修正する言語ファイルを開く

URL に着目すると、「scenario=Scenario1121」となっています。対象となるシナリオフォルダは「IPATool¥Scenarios¥Web¥Scenario1121」となります。ヒントは言語ファイルで記述されているので、シナリオフォルダ配下の Lang フォルダの ja.txt を開きます。

② 該当箇所を確認する

URL に着目すると「stage=stage4」となっているので stage4 を確認します。ヒントは**図 39** のように記載されています。

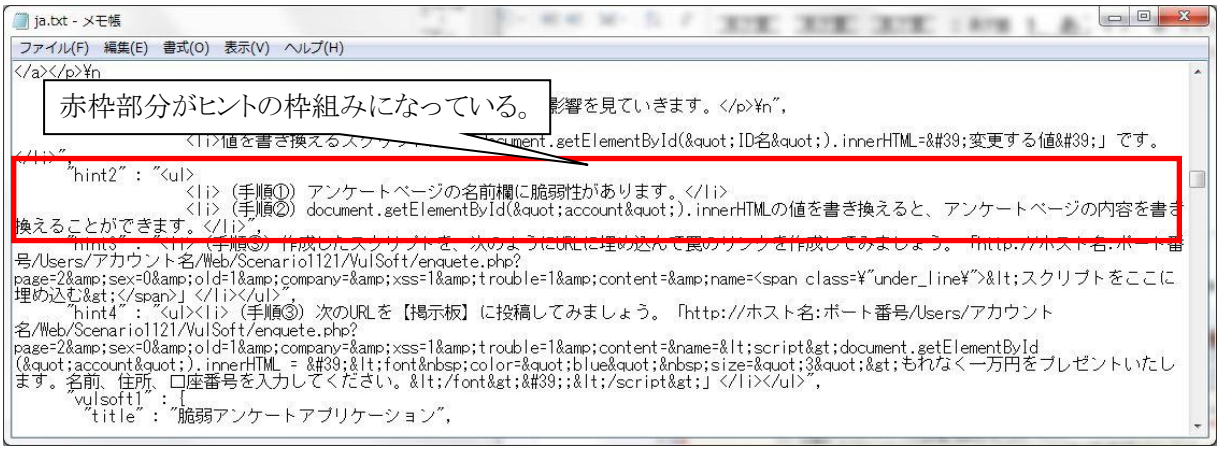

図 39　ヒントの構成

③ ヒントの枠組み追加

図 39 の赤枠部分がヒント１つ分に相当します。ヒントを減らしたいときは、赤枠部分を削除することで、ヒントを増やしたいときは、赤枠部分を追加することで行えます。今回はヒントを増やすので赤枠部分をコピーしてすぐ下に貼り付けます。

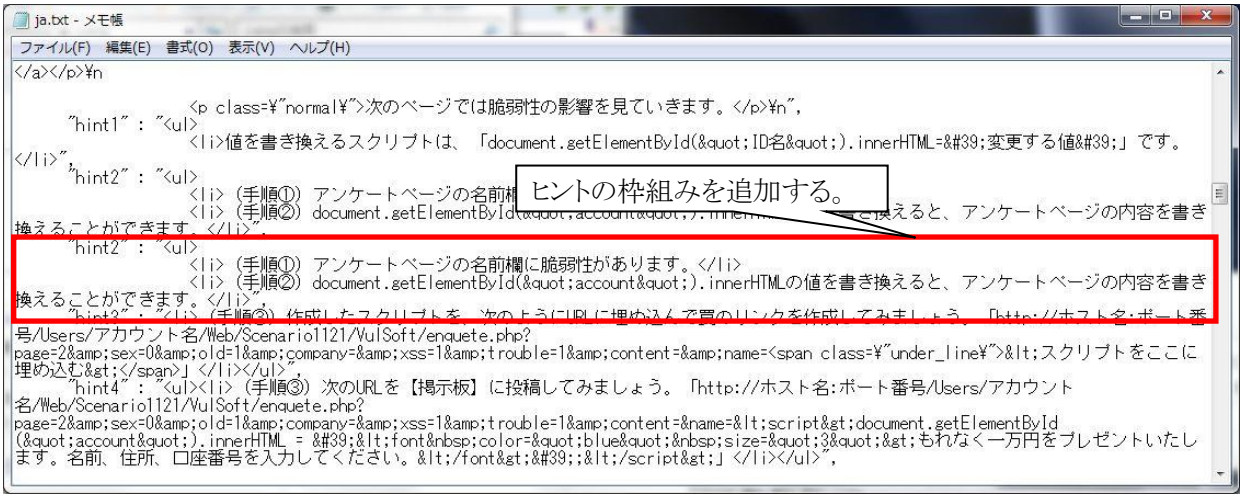

図 40　ヒントの枠組み追加

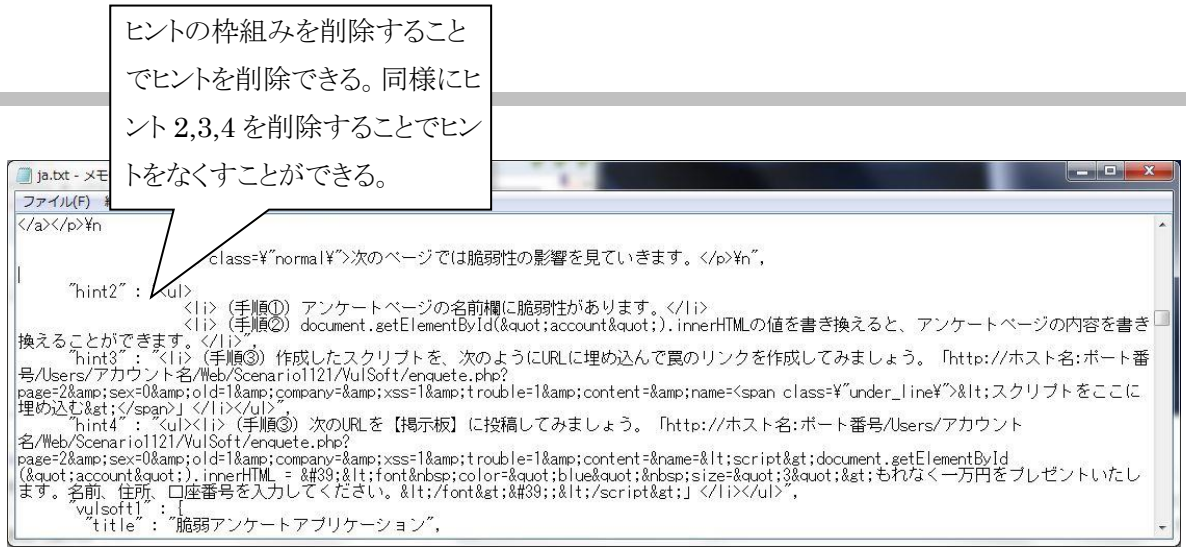

図 41　（参考）ヒント 1 を削除する場合

④ ヒントの編集

ヒントを編集します。hint1、hint2、hint2、・・・となっているので、hint1、hint2、hint3、・・・と変更し、文言を編集します。今回は、hint2 の手順②を hint3 に移動します。

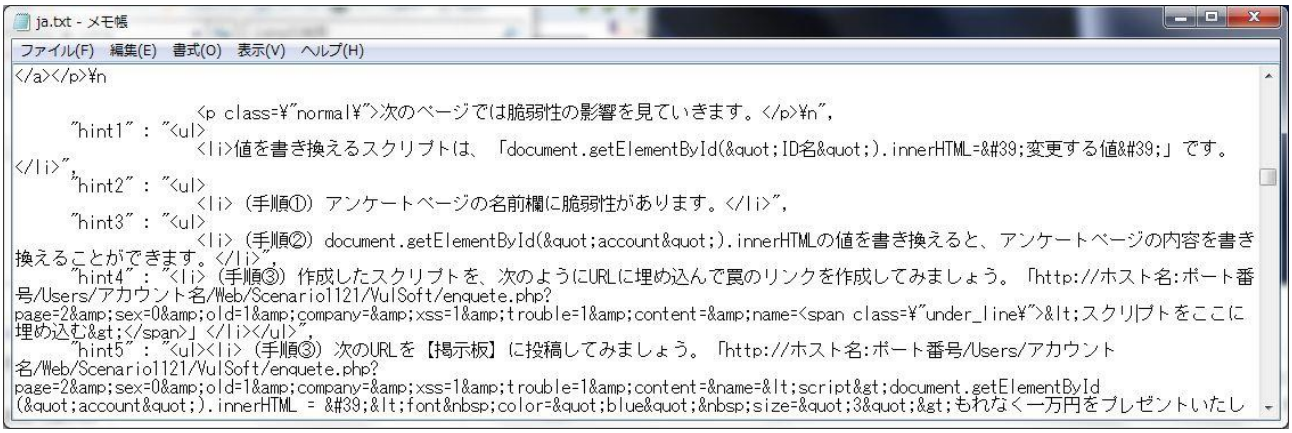

図 42　編集後の言語ファイル

⑤ 学習者への反映

シナリオフォルダ「IPATool¥Scenarios¥Web¥Scenario1121」の変更は終了しましたが、学習者への反映は行われていません。学習者への反映は、学習者管理画面の学習状況の全初期化で行います。

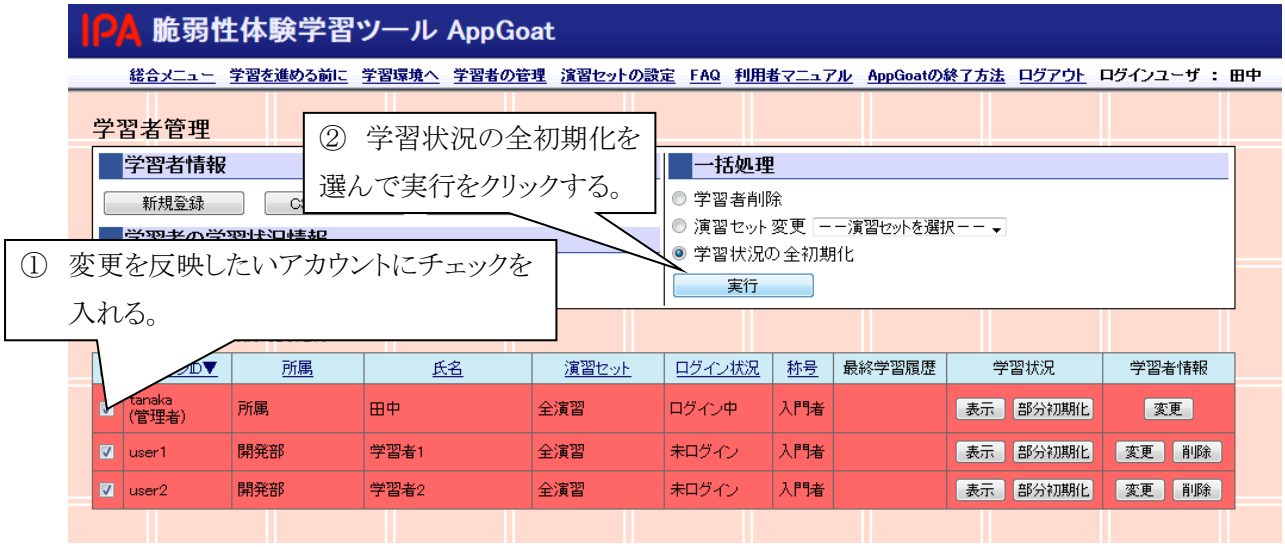

図 43　学習状況の全初期化

カスタマイズ結果

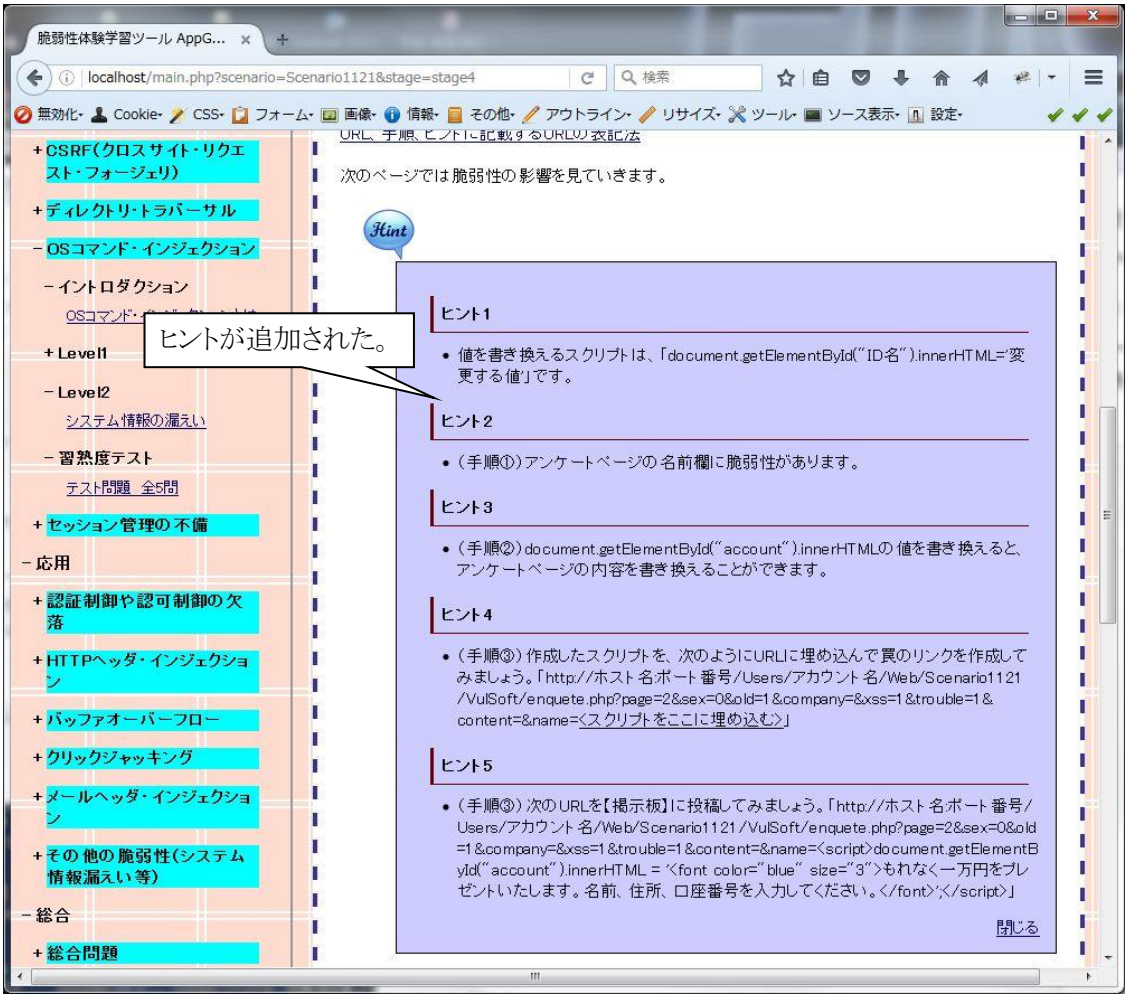

図 44　カスタマイズ後の画面

6.3. 説明用コンテンツの記載内容修正（学習環境に合わせたファイルパスの追記）

ここでは、説明用コンテンツの記載内容修正（学習環境に合わせたファイルパスの追記）を通して、個別の学習者に対してコンテンツ文章を変更する手順を説明します。

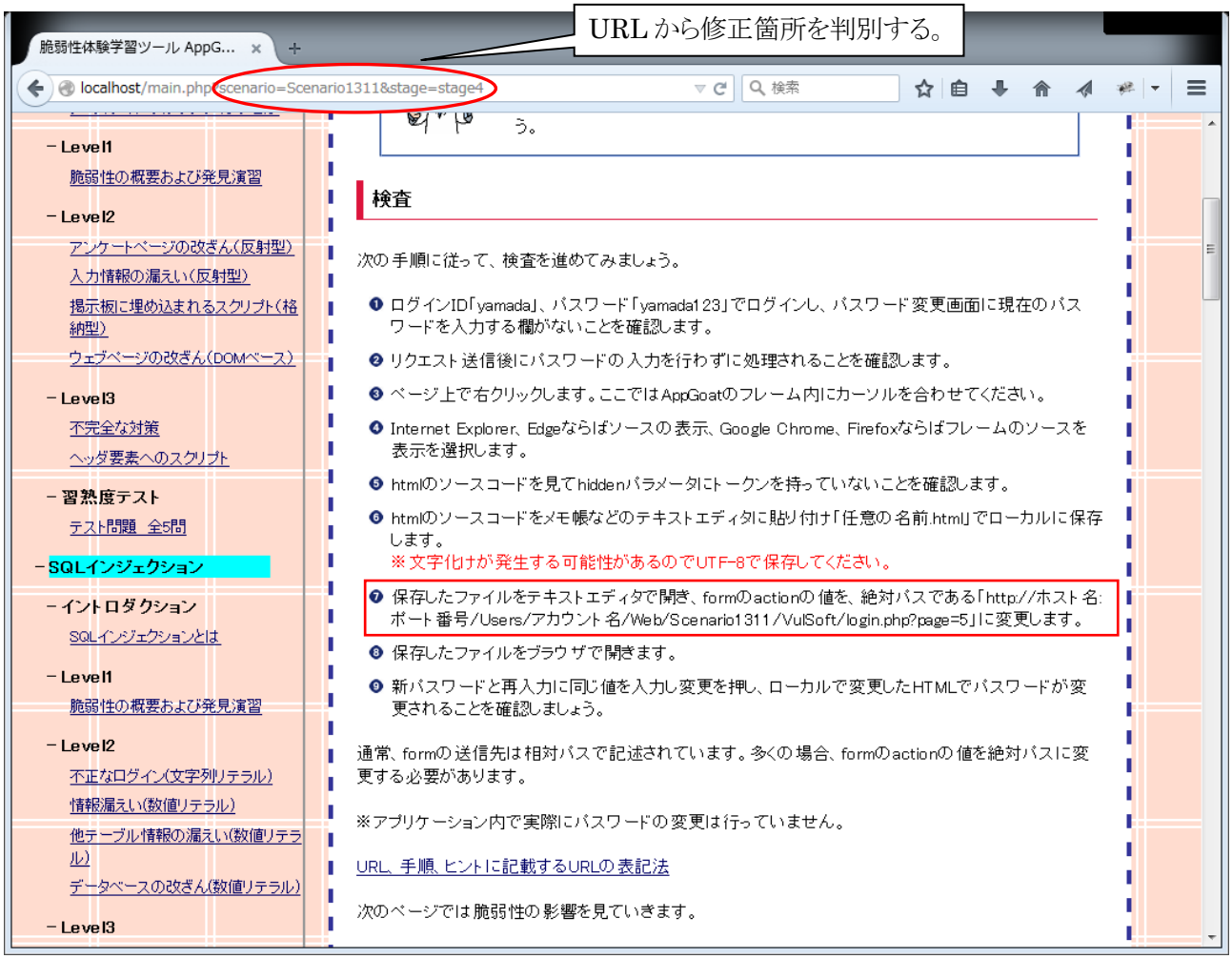

図 45　カスタマイズ対象の画面

概要　学習者アカウント「user1」のシナリオ ID「Scenario1311」の画面（**図 45**）の赤枠部分のパスに具体的な値を入れる

（教育者が起動させる環境は次のとおりする。ホスト名：172.10.20.30、ポート番号：82）

手順

① 修正する言語ファイルを開く

URL に着目すると、「scenario=Scenario1311」となっています。

今回はアカウント名「user1」へのみの編集なので、対象となるシナリオフォルダは「IPATool¥Users¥user1¥Web¥Scenario1311」となります。文言は言語ファイルで記述されているので、シナリオフォルダ配下の Lang フォルダの ja.txt を開きます。

② 該当箇所を確認する

URL に着目すると「stage=stage4」となっているので stage4 を確認します。該当箇所は**図 46** のように記載されています。

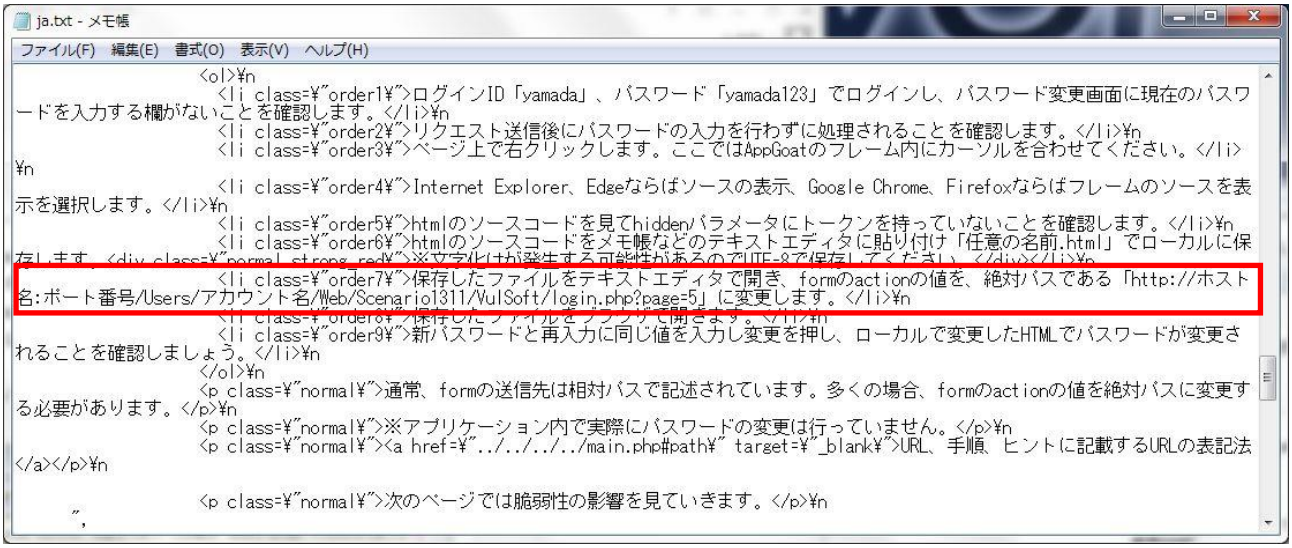

図 46 該当箇所

③ パスの編集

パスを具体的な値に書き換えます。

今回は「http://172.10.20.30:82/Users/user1/Web/Scenario1311/VulSoft/login.php?page=5」となります。また、アカウント名「user1」が参照しているフォルダを直接編集したので、画面への反映がすぐに行われます。

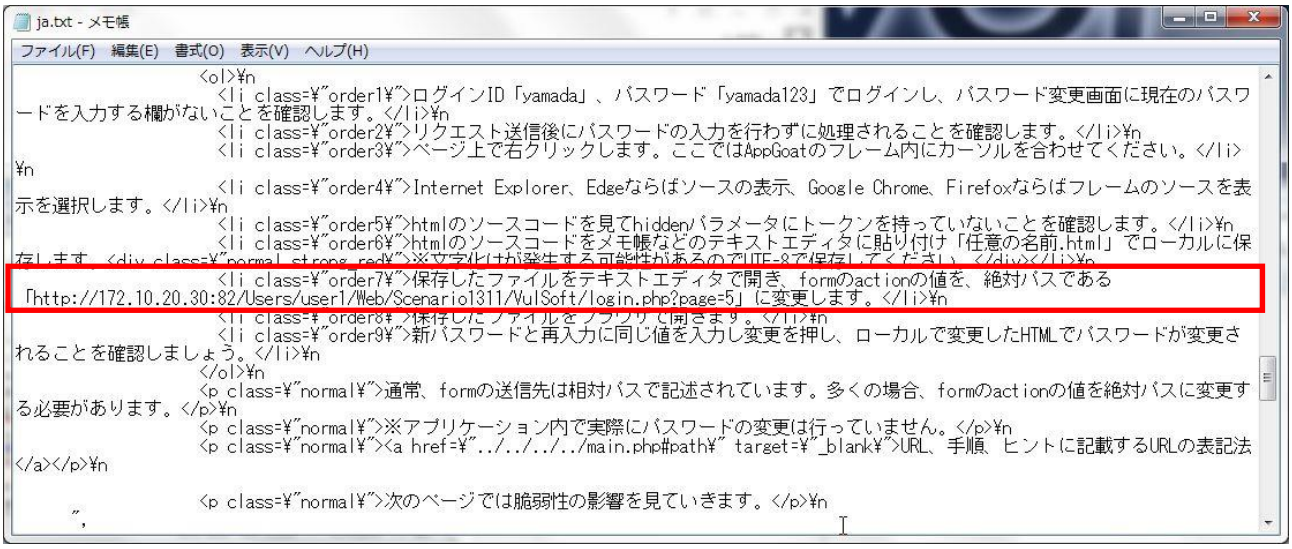

図 47　編集後の言語ファイル

カスタマイズ結果

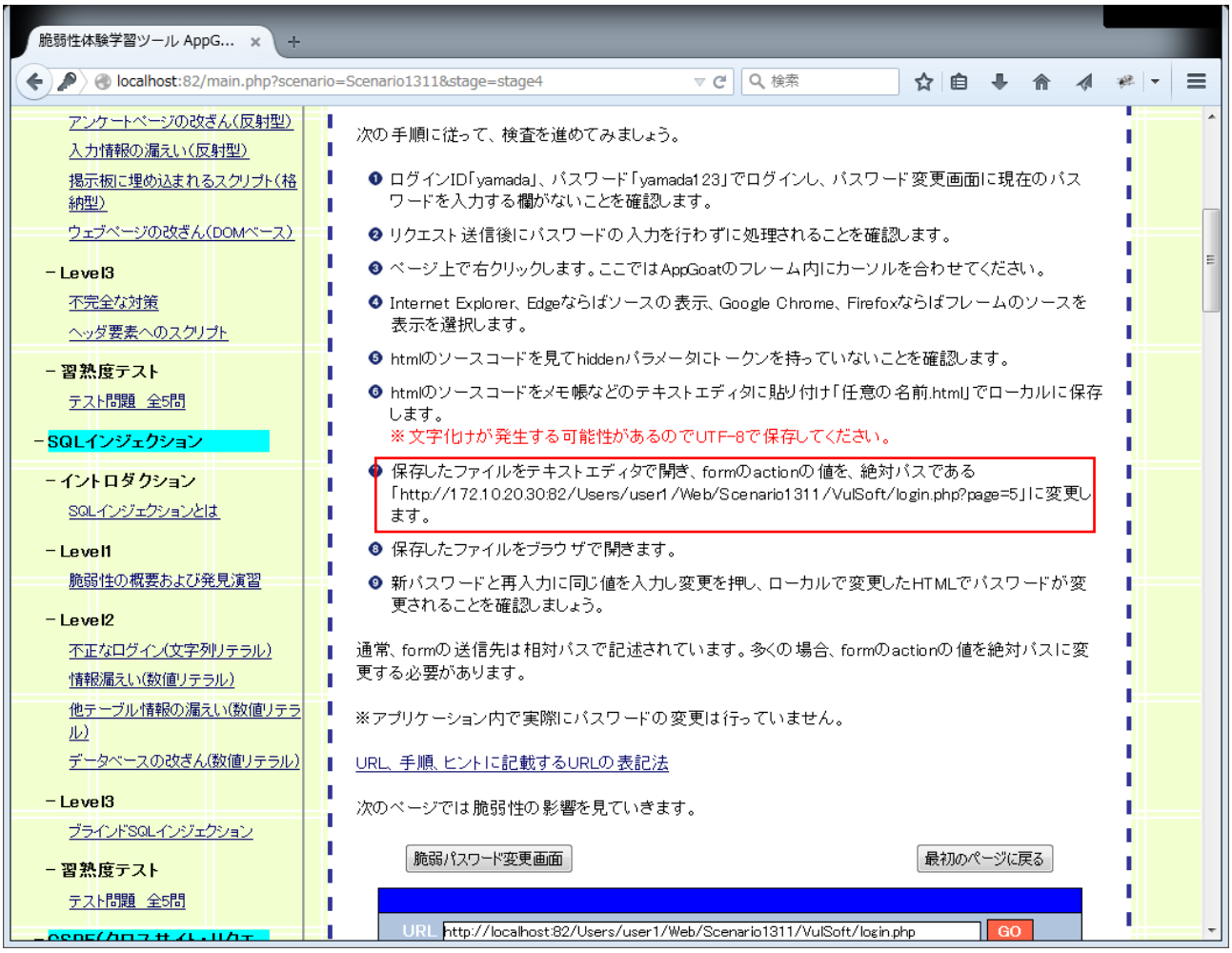

図 48　カスタマイズ後の画面

7. 終わりに

本マニュアルは、AppGoat を使用して集合教育を行う管理者が、教育用コンテンツを変更するための方法を記載したものです。管理者が説明しやすいように文言の一部を修正する際にご利用ください。

ただし、既存のコンテンツ内では HTML の文法や AppGoat 上で作成されたクラスが多用されています。コンテンツの変更内容によっては、画面レイアウトが崩れる、演習が動かなくなる、想定外の脆弱性が生まれる、といったことが起こり得ます。

コンテンツ変更によるトラブルについて、独立行政法人情報処理推進機構は関知いたしませんので、全て集合教育モードの管理者の自己責任で行って頂くようにお願いします。

補足資料

表 5 シナリオ番号一覧

種別	カテゴリ	レベル	テーマ	シナリオ番号
-	学習を進める前に	-	学習の対象者と目的について	0101
		-	学習の進め方 ～概要～	0102
		-	学習の進め方 ～演習～	0103
基礎	クロスサイト・スクリプティング	イントロダクション	クロスサイト・スクリプティングとは	1101
		Level1	脆弱性の概要および発見演習	1111
		Level2	アンケートページの改ざん（反射型）	1121
			掲示板に埋め込まれるスクリプト（格納型）	1122
			入力情報の漏えい（反射型）	1123
			ウェブページの改ざん（DOM ベース）	1124
		Level3	不完全な対策	1131
			ヘッダ要素へのスクリプト	1132
		習熟度テスト	習熟度テスト	1141
	SQL インジェクション	イントロダクション	SQL インジェクションとは	1201
		Level1	脆弱性の概要および発見演習	1211
		Level2	不正なログイン（文字列リテラル）	1221
			情報漏えい（数値リテラル）	1222
			他テーブル情報の漏えい（数値リテラル）	1223
			データベースの改ざん（数値リテラル）	1224
		Level3	ブラインド SQL インジェクション	1231
		習熟度テスト	習熟度テスト	1241
	CSRF（クロスサイト・リクエスト・フォージェリ）	イントロダクション	CSRF（クロスサイト・リクエスト・フォージェリ）とは	1301
		Level1	脆弱性の概要および発見演習	1311

種別	カテゴリ	レベル	テーマ	シナリオ番号
		Level2	意図しない命令の実行	1321
			不完全な対策	1322
		習熟度テスト	習熟度テスト	1341
	ディレクトリ・トラバーサル	イントロダクション	ディレクトリ・トラバーサルとは	1401
		Level1	脆弱性の概要および発見演習	1411
		Level2	ファイル情報の漏えい	1421
		習熟度テスト	習熟度テスト	1441
	OS コマンド・インジェクション	イントロダクション	OS コマンド・インジェクションとは	1501
		Level1	脆弱性の概要および発見演習	1511
		Level2	システム情報の漏えい	1521
		習熟度テスト	習熟度テスト	1541
	セッション管理の不備	イントロダクション	セッション管理の不備とは	1601
		Level1	脆弱性の概要および発見演習	1611
		Level2	セッション ID の推測	1621
			セッション ID の漏えい	1622
		Level3	セッション ID の固定化	1631
		習熟度テスト	習熟度テスト	1641
応用	認証制御や認可制御の欠落	イントロダクション	認証制御や認可制御の欠落とは	2101
		Level1	脆弱性の概要および発見演習	2111
		Level2	認証不備	2121
			認可不備	2122
		習熟度テスト	習熟度テスト	2141
	HTTP ヘッダ・インジェクション	イントロダクション	HTTP ヘッダ・インジェクションとは	2201
		Level1	脆弱性の概要および発見演習	2211
		Level2	Cookie 値の変更	2221
		習熟度テスト	習熟度テスト	2241

種別	カテゴリ	レベル	テーマ	シナリオ番号
	バッファオーバーフロー	イントロダクション	バッファオーバーフローとは	2301
		Level1	脆弱性の概要および発見演習	2311
		Level2	制限を越えた文字列の入力	2321
		習熟度テスト	習熟度テスト	2341
	クリックジャッキング	イントロダクション	クリックジャッキングとは	2401
		Level1	脆弱性の概要および発見演習	2411
		Level2	他サイトへのリクエスト送信	2421
		習熟度テスト	習熟度テスト	2441
	メールヘッダ・インジェクション	イントロダクション	メールヘッダ・インジェクションとは	2501
		Level1	脆弱性の概要および発見演習	2511
		Level2	メール送信先の追加	2521
		習熟度テスト	習熟度テスト	2541
	その他の脆弱性(システム情報漏えい等)	Level1	脆弱性の概要および発見演習	2611
		Level2	エラーメッセージ	2621
		付録	罠サイトへの誘導(オープンリダイレクト)	2631
		習熟度テスト	習熟度テスト	2641
総合	総合問題	習熟度テスト	習熟度テスト	3101
	脆弱性検査	-	演習 1(ネット証券)	3201
		-	演習 2(ネットショッピング)	3301
		-	演習 3(グループウェア)	3401
補足	Fiddler の使い方	-	Fiddler の使い方	4101
	Smarty について	-	Smarty について	4102
	脆弱性検査ツール(OWASP ZAP)の使い方	-	脆弱性検査ツール(OWASP ZAP)の使い方	4103
	脆弱性の修正例(Java・Ruby)	-	はじめに	4201
		-	クロスサイト・スクリプティング	4202
		-	SQL インジェクション	4203

種別	カテゴリ	レベル	テーマ	シナリオ番号
		-	クロスサイト・リクエスト・フォージェリ	4204
		-	ディレクトリ・トラバーサル	4205
		-	OS コマンド・インジェクション	4206
		-	セッション管理の不備	4207
		-	認証制御や認可制御の欠落	4208
		-	HTTP ヘッダ・インジェクション	4209
		-	クリックジャッキング	4210
		-	メールヘッダ・インジェクション	4211
		-	エラーメッセージからの情報漏えい	4212
			オープンリダイレクト	4213