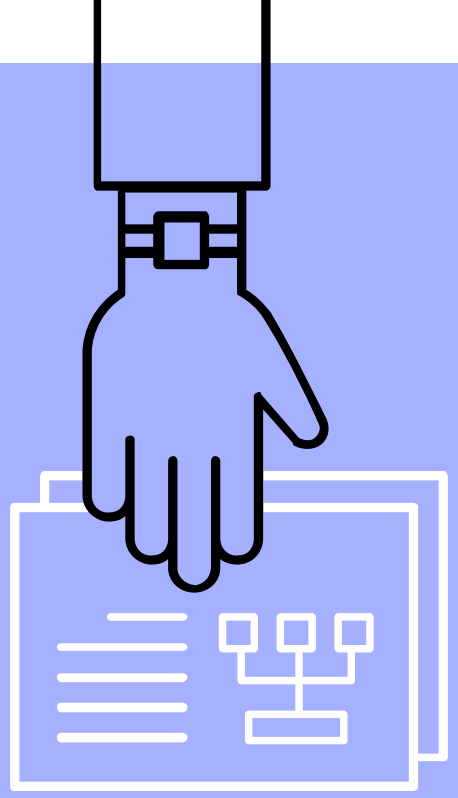
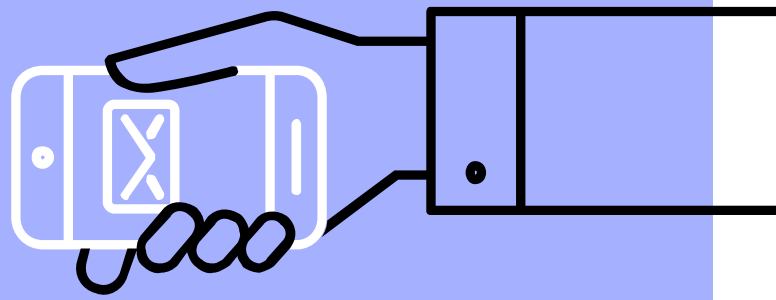
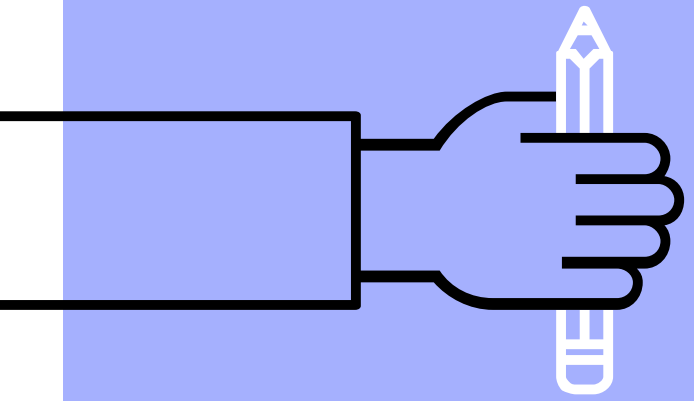
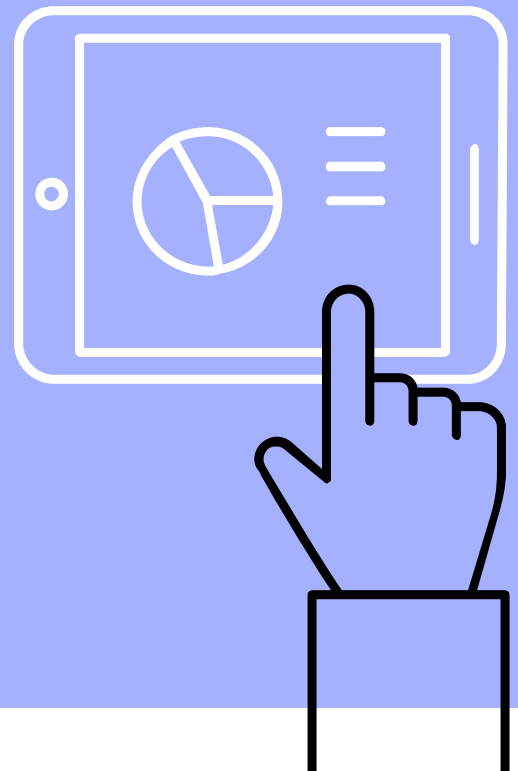




Webサイトセキュリティ
学習教材





＊＊＊注意事項＊＊＊

本日の授業の中では実際にWebサイトへの改ざんを行います。

※起こりうる可能性の高い問題を体験することを優先するため
　具体的な理論までは深入りしません。

悪用・誤って外部に送信した場合、以下の法律に抵触する可能性があります。

・不正アクセス行為の禁止等に関する法律
・電子計算機損壊等業務妨害罪
・偽計業務妨害罪、威力業務妨害罪
・器物破損罪

目次

- はじめに
- デベロッパーツールとは
- 実際にWebサイトの改ざんをしてみよう
- 演習問題
- 最後に

はじめにー　この授業の目的

- Webサイトに対する改ざんが如何にして行われているかを知り、対策の重要性を知る。

- 皆さんがセキュリティに興味を持ち、学習方法を考える一助に。

今日はWebサイトの改ざんの疑似体験をしてもらいます
（今回は私たちが攻撃者になります）

はじめに – 最近のWebサイトの攻撃動向

攻撃者の低年齢化

- 中高生がWebサイトへの攻撃、マルウェアの作成配布等によって検挙される事例が散見されるようになった。
- 攻撃手法が容易に学習できるようになったため悪用も容易になったと見られる

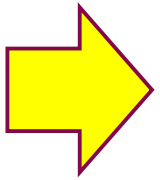
Webサイトを構成するソフトウェアに攻撃

- Webサイトを構築する際に使われるソフトウェアにセキュリティ上の欠陥（脆弱性）が発覚
  多くの組織・企業で使われているため被害が多発

はじめに –　一般的なWebサイトの構成

一般的なWebサイトは、役割ごとに別の拡張子に分けて作られています。

example.html・・・・（本文）
example.css・・・・　（レイアウト）
example.php・・・・（処理）



.XXX このようなドット（ . ）で仕切られた後ろの部分のことを拡張子といいます。

拡張子とは

コンピュータがファイルが何について書かれているか何が入っているかを
判断するためのもので代表的なものに.pngや.JPGなどの画像ファイル、 .mp3などの
音楽ファイルや.html　.css　.phpなどのWebサイトを構築するためのファイルがあります。

プログラミング言語の種類

HTML(Hyper Text Markup Languageハイパーテキスト・マークアップ・ランゲージ)

多くのWebサイトがこの言語で書かれていますタグといわれる<>で囲まれた文字で画像や字の大きさなどを決めています

例

<h1>xxxx</h1>・・・・・・・・・・・・・ 文字が大きく表示されます

<img src= 画像ファイルの名前>・・・・・指定された画像が表示されます

<body bgcolor="色"></body>・・・・・背景の色が指定した色になります

<!-- --!> ・・・・・・・・・・・・・・・・・プログラムの動きに関与しないコメントを入れることが出来ます。

プログラミング言語の種類

CSS(Cascading Style Sheetsカスケーディング・スタイル・シート)

HTMLと組み合わせて使用する言語です。HTMLで書いた文字の色を変えたり、見やすいようにリストを作ったりとWebページのデザインを作っています。

例
h1 {color:blue;}・・・・・・・・・・・・・・・・ h1の文字が青色で表示されます
h1 {background-image: url(“”);}・・・・・・ 指定された画像がh1の背景に表示されます
h1{background:blue;}・・・・・・・・・・・・h1の背景の色が青色になります

プログラミング言語の種類

PHP

HTMLと組み合わせて使用する言語です。主にサーバーといわれる外部の端末で
処理される動作を使うためのの言語であり通常であれば見ることはありません。

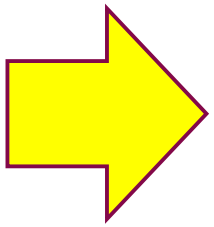
例

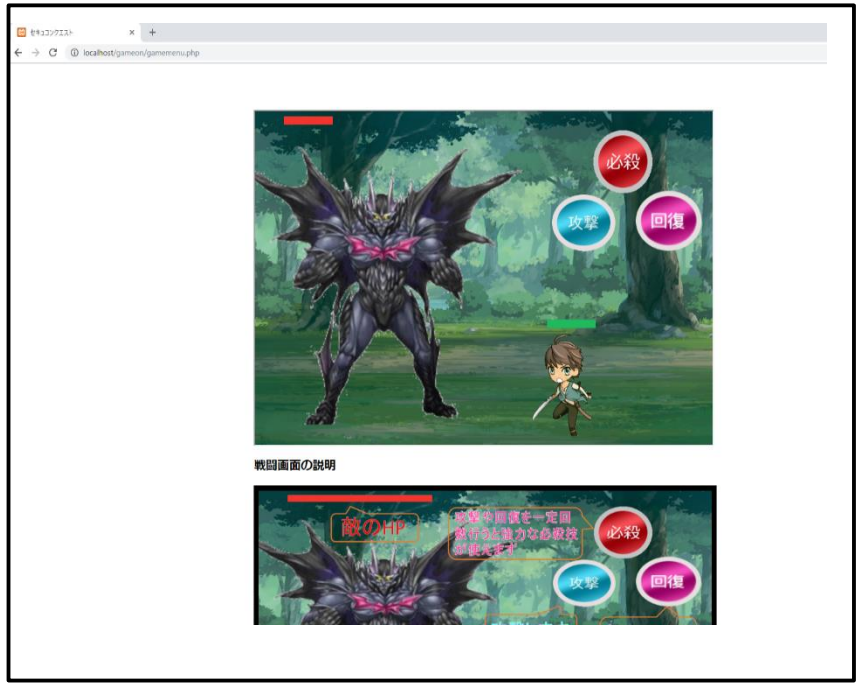
＜？php　echo “HELLO WORLD”;？＞・・・・・・ HELLO WORLDと表示されます
＜？php　if(条件){処理}　？＞・・・・・・・・・・・条件を満たしていれば処理をします。
＜？php for(条件){処理}　？＞・・・・・・・・・・・条件を満たすまで処理を繰り返します

Webサイト を構成する仕組み

Webサイトはもともとはプログラミング言語というコンピュータの言語で書かれています。
それを私たちが見やすい形に整えて出力されて いるのがいつも私たちが使っているWebサイトです。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
  "http://www.w3.org/TR/html4/loose.dtd">

<html>
<head>
<style type="text/css">
<!--
#center{
height:200px;
width:500px;
position:absolute;
top:50%;
left:50%;
margin-top:-450px;
margin-left:-550px;
border:solid 1px #666666;
}
.disabled {
  pointer-events: none;
}
-->
</style>

<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS">
<meta http-equiv="Content-Style-Type" content="text/css">

<title>セキュコンクエスト</title>
</head>
<body oncontextmenu='return false'>
<div id="center">
  <iframe src="game1.php" width="940" height="640" scrolling="no">
  </div>
  </iframe>
  <h2>戦闘画面の説明</h2>
  <img src="説明画面2.png"  alt="説明" width="930" height="530" border="10">

</body>


</html>
```



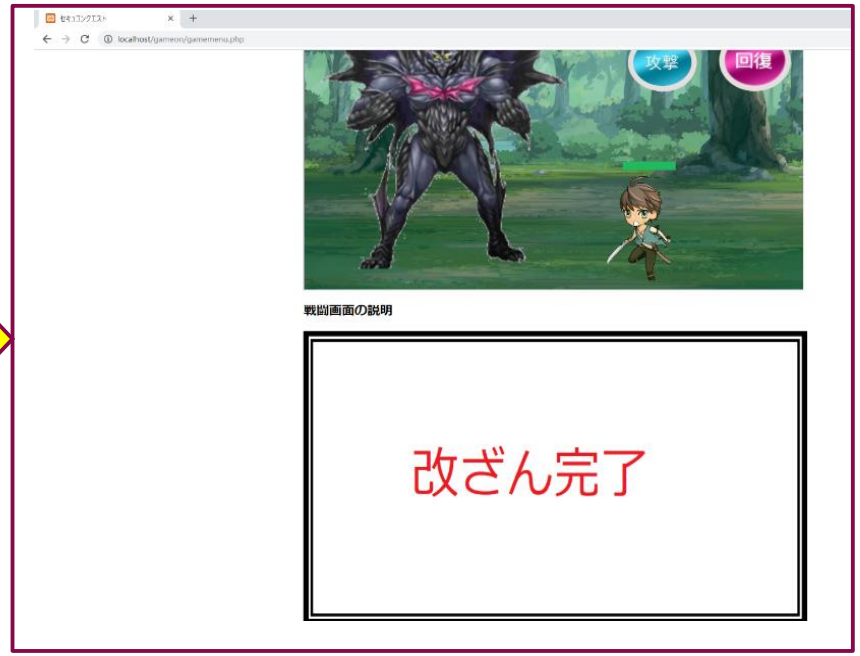


Webサイトを構成する仕組み

実は私たちが見ているWebサイトはこの中身を少し弄るだけで簡単に改ざんすることが出来ます。

```
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS">
<meta http-equiv="Content-Style-Type" content="text/css">

<title>セキュコンクエスト</title>
</head>
<body oncontextmenu='return false'>
<div id="center">
  <iframe src="game1.php" width="940" height="640" scrolling="no">
  </div>
  </iframe>
  <h2>説明画面の説明</h2>
  <img src="説明画面2.png" alt="説明" width="930" height="530" border="10">

</body>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS">
<meta http-equiv="Content-Style-Type" content="text/css">

<title>セキュコンクエスト</title>
</head>
<body oncontextmenu='return false'>
<div id="center">
  <iframe src="game1.php" width="940" height="640" scrolling="no">
  </div>
  </iframe>
  <h2>説明画面の説明</h2>
  <img src="改ざん.png" alt="説明" width="930" height="530" border="10">

</body>


</html>
```

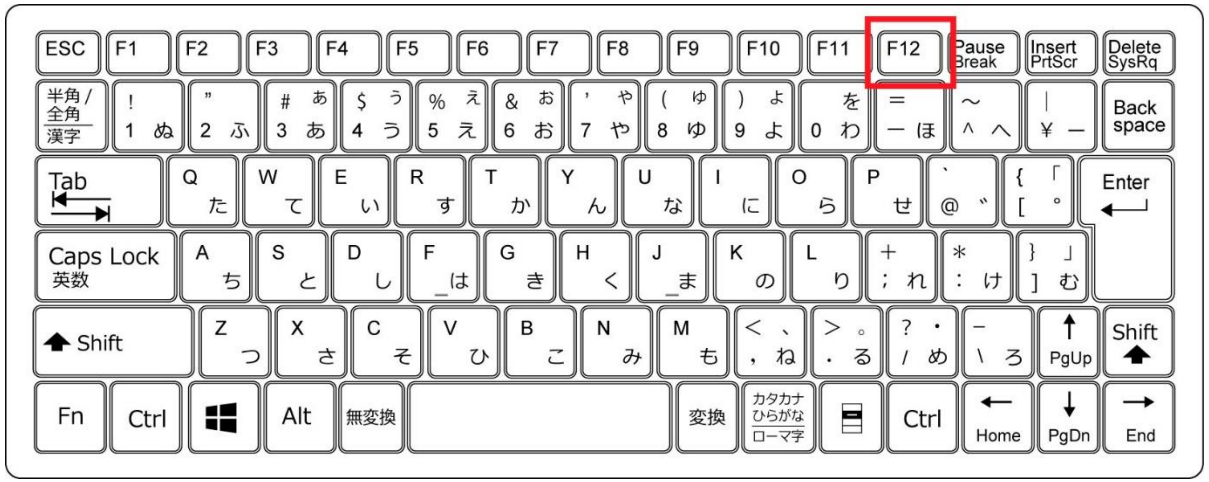


デベロッパーツールとは

デベロッパーツールとはGoogleが提供しているブラウザ、
Chromeに付属しているツールの一つでWebサイトの動作の確認や細やかな変更を
実際にプログラムを書き換えることなく確認することが出来ます。

デベロッパツールの起動

Chromeを起動しF１２キーを押すか起動したページで右クリックをして一番下の検証(I)をクリック



実際にWebサイトの改ざんをしてみよう

以下のURLを入力してください

http://xxx.xxx.xxx.xxx/sampleq/sample_slot.php

実際にWebサイトの改ざんをしてみよう

- サイトにアクセスしたらデベロッパツール（F12）を起動してください。

実際にWebサイトの改ざんをしてみよう

デベロッパツール右上の マークをクリックしたあとサイトの気になる部分をクリックするとその部分を構成するプログラムが表示されます。

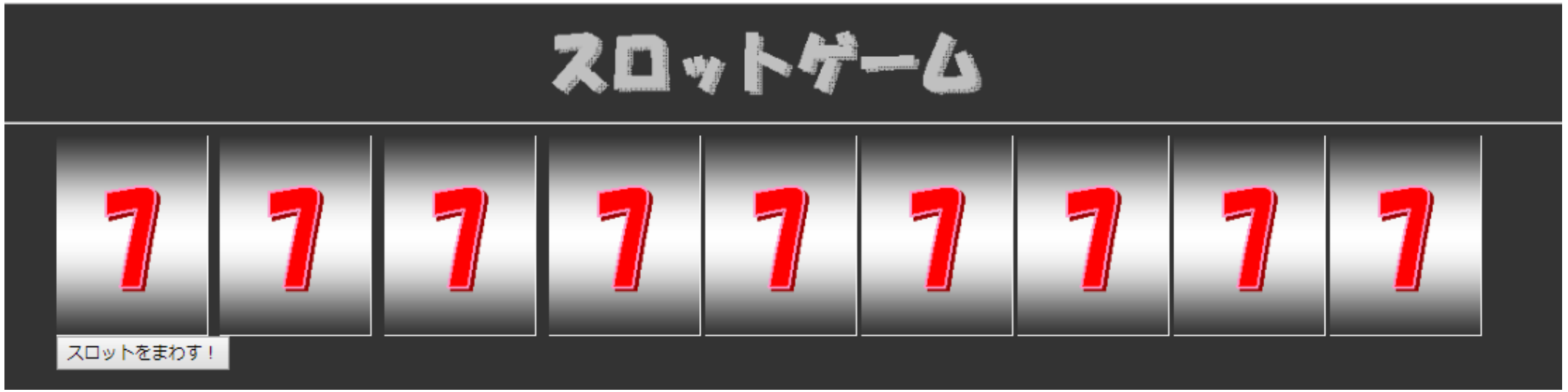
では、選択した<img src="./slot_images/X.png">のX部分を1～9の好きな数字に変えてみましょう。

プログラムの部分をダブルクリックすると編集できるようになります。

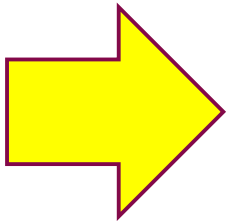
スロットの選択した部分が好きな数字に変わります。

実際にWebサイトの改ざんをしてみよう

- 次に下の図のようにすべての数字を同じにしてみよう

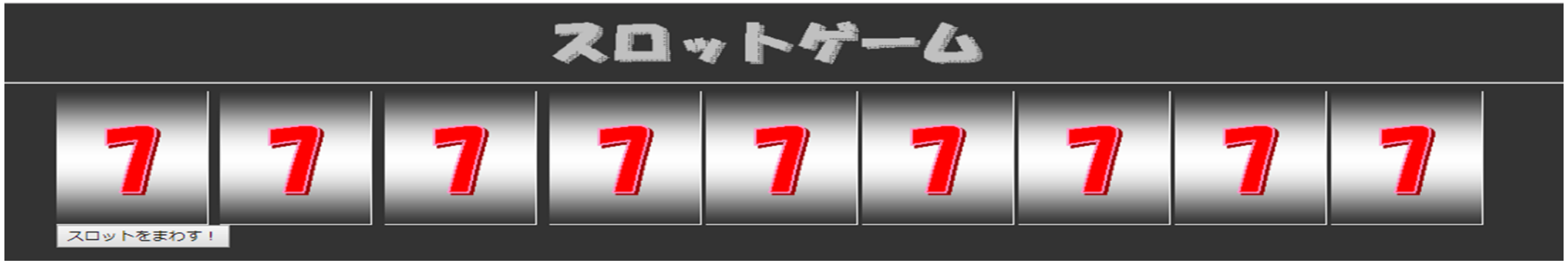


実際にWebサイトの改ざんをしてみよう



<img src="./slot_images/9.png">　　<img src="./slot_images/ 7 .png">

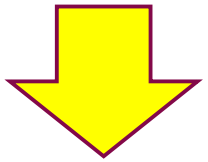
Webページの数字の部分を選択し好きな数字に書き換える
これを9回繰り返すと好きな数字でスロットを揃えることが出来る



実際にWebサイトの改ざんをしてみよう

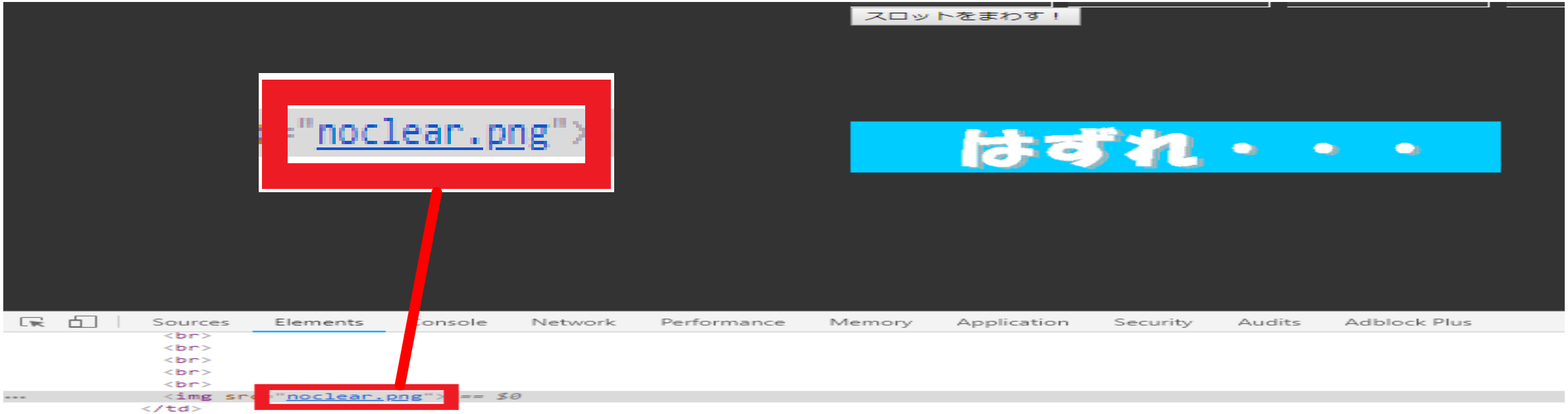
練習問題

通常だとどんなにスロットを回して
もはずれのままの画像を下のような
当たり画像に変えてみよう



実際にWebサイトの改ざんをしてみよう

はずれの画像を選択すると<img src="noclear.png">
と出てくる、noclear＝クリアしていないという画像が置かれている事が
わかる。では、noの部分を取ってclearという画像にしてみれば
違う画像が出てくるかもしれない。



実際にWebサイトの改ざんをしてみよう

実際に演習問題を解く前に・・・

次に出す問題は「CTF」という問題形式で

Capture The Flag（旗取りゲーム）

情報セキュリティ技術を競う競技・ゲームです。

隠された答え（FLAG）をセキュリティスキルを用いて探しだすゲームのようなものです。

FLAG を集めるとポイントが加算されていき最終的なポイントの総量で競い合います。

FLAG｛XXXXX｝のようにFLAGが表示されます。

演習問題

- ①ガチャを回してみよう（ガチャ結果の画面にFLAG）
- ②ガチャから排出されないNo.99のカードを出そう（No.99の画像にFLAG）

http://xxx.xxx.xxx.xxx/bbbb/Gacha.php （ガチャのページのURLは共通です）

- ③battle3に挑戦してみよう
  （battle3をデベロッパツールで見た時に中にある<head>部分にFLAG）
- ④battle3に勝利してみよう（メニュー画面のFLAG２に表示される）

http://xxx.xxx.xxx.xxx/gameon/gamemenu.php

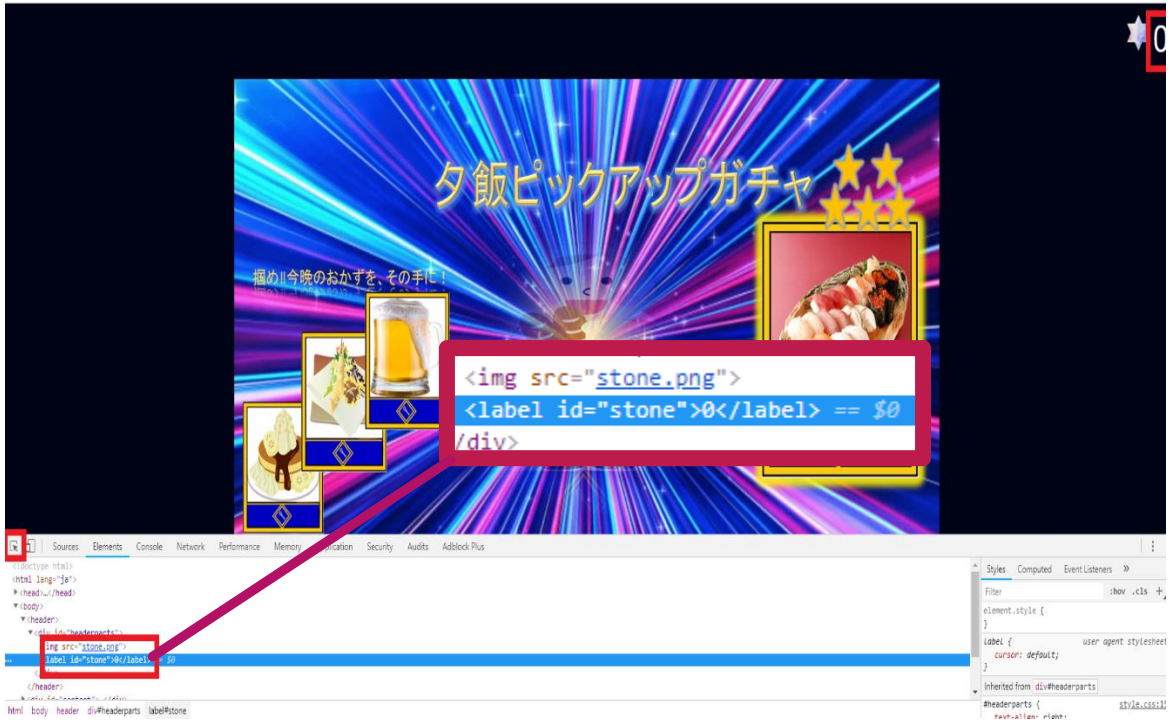
（battleのURLは共通です）

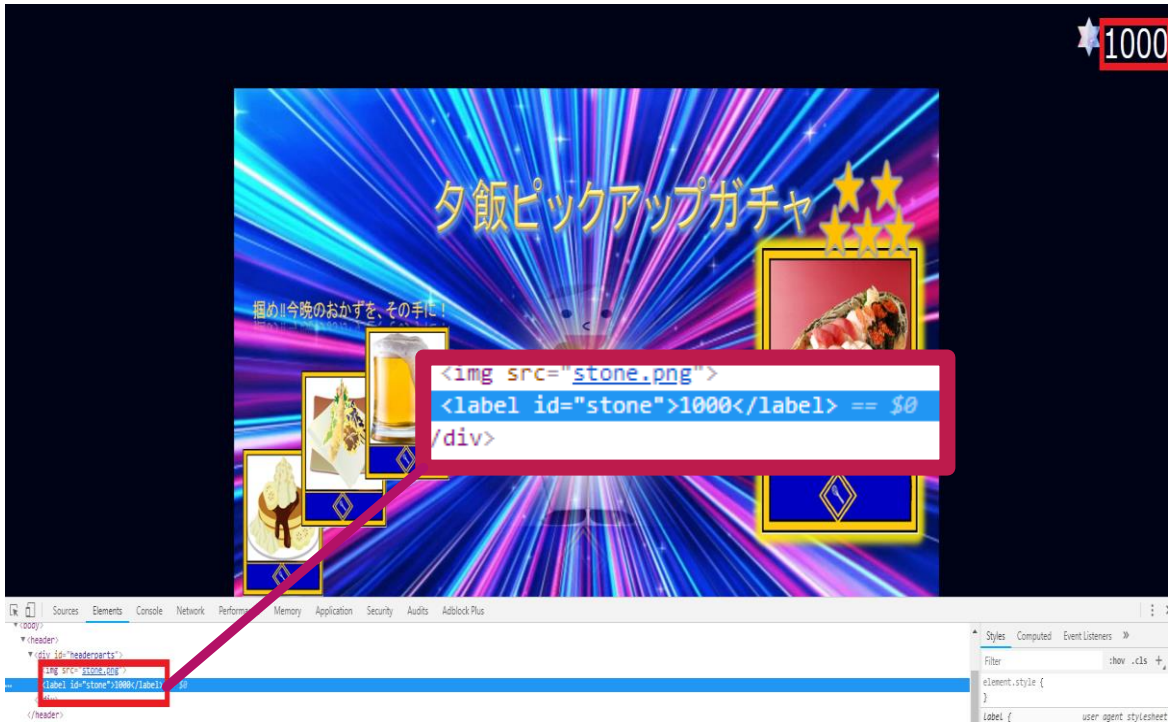
演習問題のヒント

① ガチャ石の部分をデベロッパツールで調べてみると
② カード画像を見てみると法則性が
③ チュートリアルとbattle1のページ名から考えてみると
④ 開発者がデバック用に作ったボタンがどこかに

演習問題解法①

- ページ上部の石の個数の部分を選択すると０から個数を増やすことが出来ます。





演習問題解法①-2

ガチャを回すとガチャ結果画面が表示されます。
ページの下のガチャを回すボタンの上にFLAGが表示されます。

演習問題解法②

ガチャ結果の画像を見てみると、一枚ごとに数字が割り振られていることがわかる。

cards/3.jpg

cards/31.jpg

cards/46.jpg

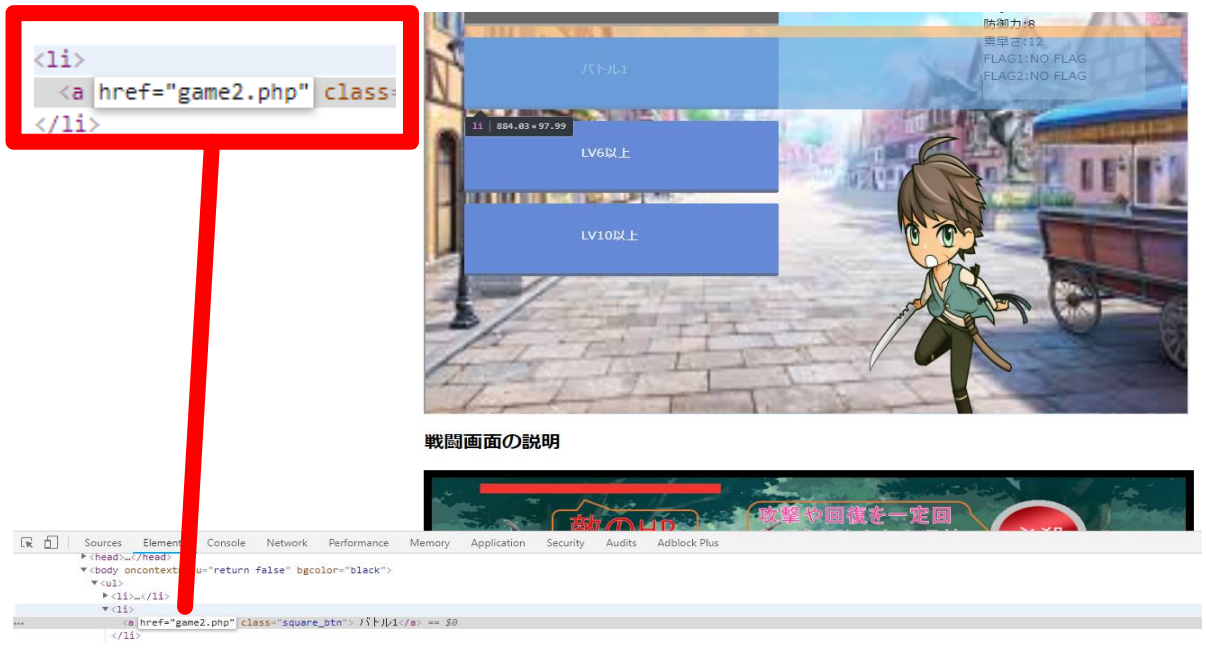
演習問題解法②-2

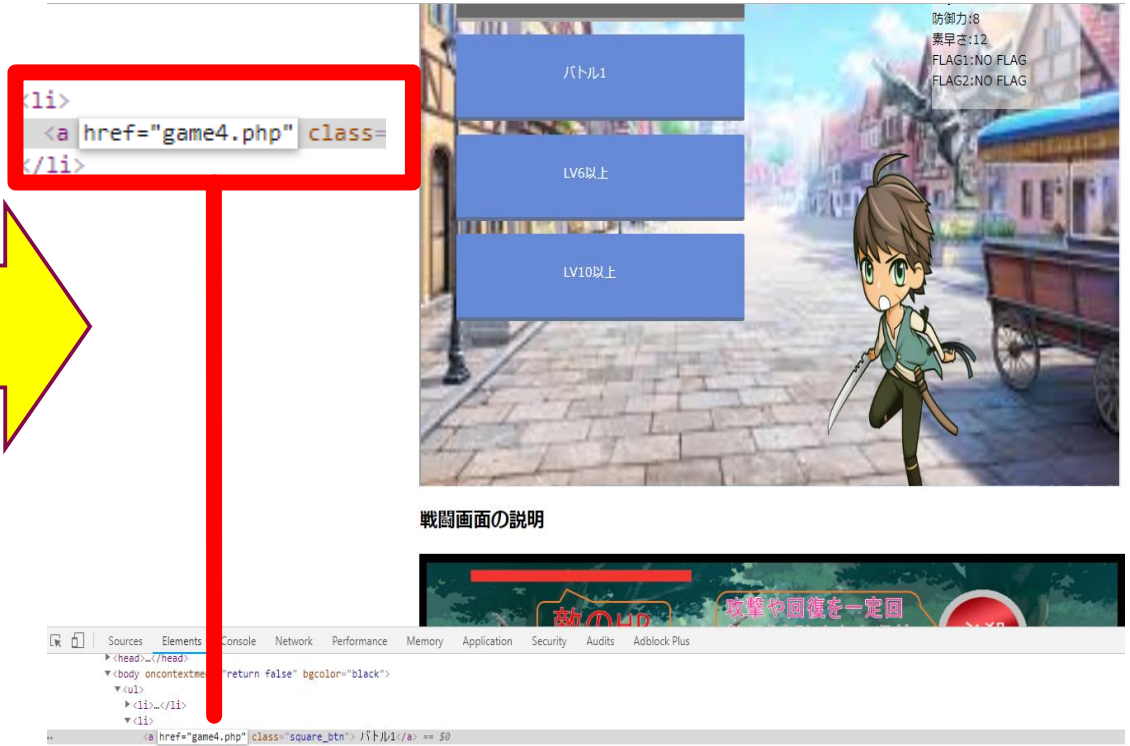
カードに割り振られた数字がカードのNo.になっていることが推測できる。

cards/X.jpgの部分のXを問題の９９に変えてみるとFLAGが出てくる。

演習問題解法③

チュートリアルとbattle1のページ名がgame1.phpとgame2.phpになっているためそれ以降のLV6,LV10もgame3.php、game4.phpになっていると考えることが出来る。その為、ボタンのURLを書き換えてgame4.phpにするとbattle3に入ることが出来る。battle3の<head>を確認するとFLAGが確認できる。





演習問題解法③- 2

```
</style>
<!-- FLAG{LV OVER10} -->
```

```
▼<html>
  ▼<head>
      <meta charset="UTF-8">
      <meta http-equiv="x-ua-compatible" content="IE=Edge">
      <meta name="viewport" content="width=device-width, user-scalable=no">
      <meta name="apple-mobile-web-app-capable" content="yes">
      <script type="text/javascript" src="jQuery.main.js"></script>
      <script type="text/javascript" src="enchant.js"></script>
      <script type="text/javascript" src="ui.enchant.js"></script>
      <script type="text/javascript" src="batorfl.js"></script>
      <style type="text/css">
              body {
                  margin: 0;
                  padding: 0;
              }
          </style>
      <!-- FLAG{LV OVER10} -->
    </head>
  ▶<body>…</body>
```

演習問題解法④

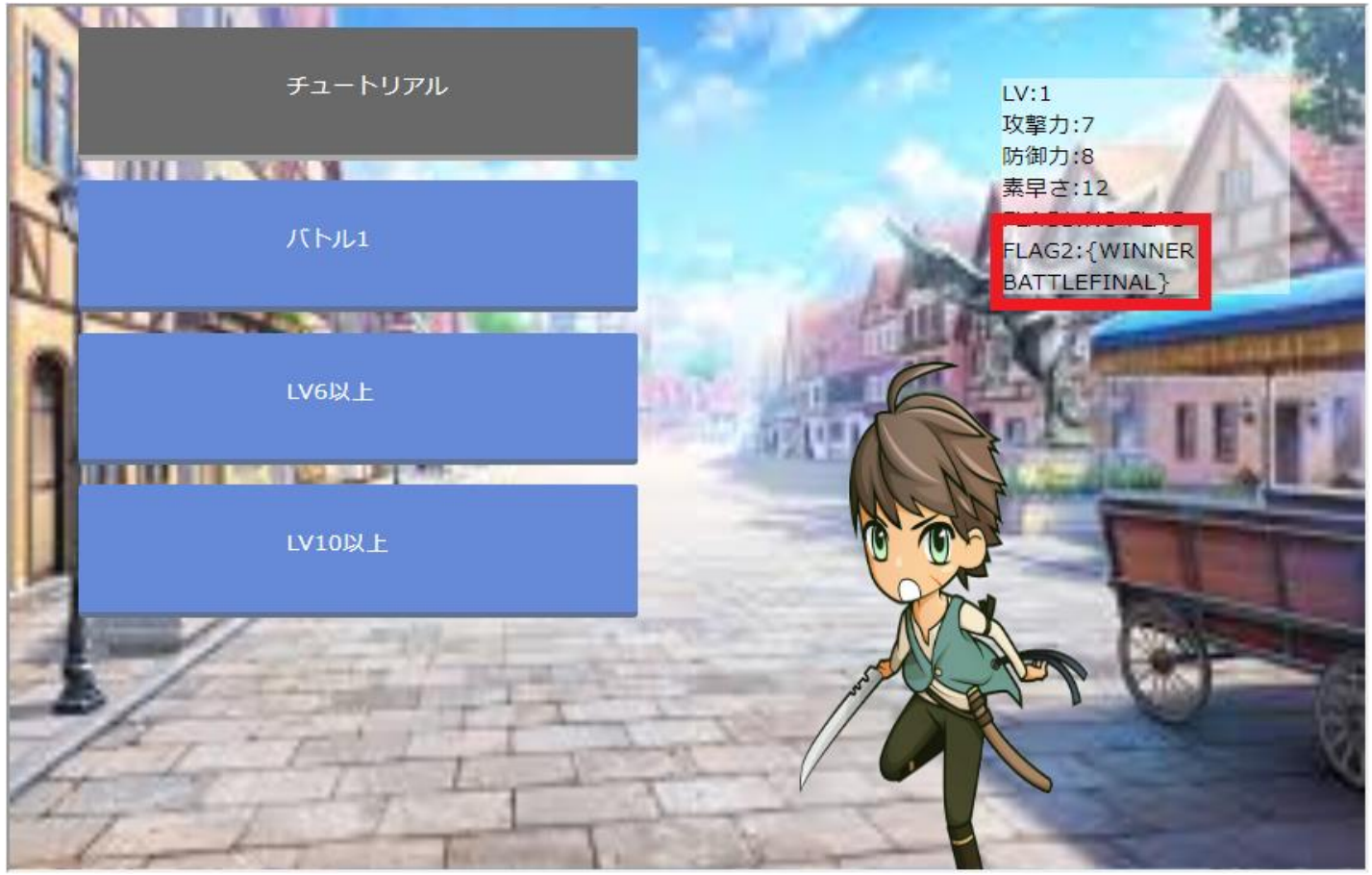
battle3のページ内の<body>の中に
開発者がデバック用に使っていた
隠しボタンがそのまま残っている。
そのボタンを使えるようにすれば
battle3を戦わずに勝つことが出来る。

演習問題解法④-2

ボタンがある部分を右クリックして
Edit as HTMLを選択すると
編集できるようになる。
その後コードの先端と末尾にある
<!-- --!>を消すと図のようなボタンが
出現する。

演習問題解法④-3

出現したボタンをクリックするとメニュー画面のFLAG２にFLAGが表示されます。



これらの攻撃を防ぐためには

- **プログラムの中身を見づらくする**
  プログラムを見られてもいいようにプログラムの中身を見づらくするとWebサイトの
  動きが予測しにくくなり攻撃箇所を見つけずらく出来ます。
- **プログラムファイルを簡単に予測できるものにしない。**
  プログラムファイルを簡単に予測できる名前にするとファイル名を推測され公開されていない
  情報を盗み見られることがあるためファイル名は予測しづらいものを付けましょう。
- **大事な処理をするプログラムは別の場所で管理する。**
  大事な処理は簡単に改ざんできるWebページに入れるのではなく別のプログラム
  で別の場所で管理するようにしましょう。

最後に

- 世の中には、多くの情報機器があり私たちはそれらに知らず知らずのうちに触れています。多くの情報機器は生活を豊かにしてくれます。しかし、それらの中に誰かが悪意を持って触れるだけで今回体験したような被害が出てしまいます。

- だからこそ、私たちが被害者にならないために**セキュリティ**を意識して触れていかなければいけません。