

オンラインによる教育現場 で活かせる実践的 情報セキュリティ実習

講師自己紹介

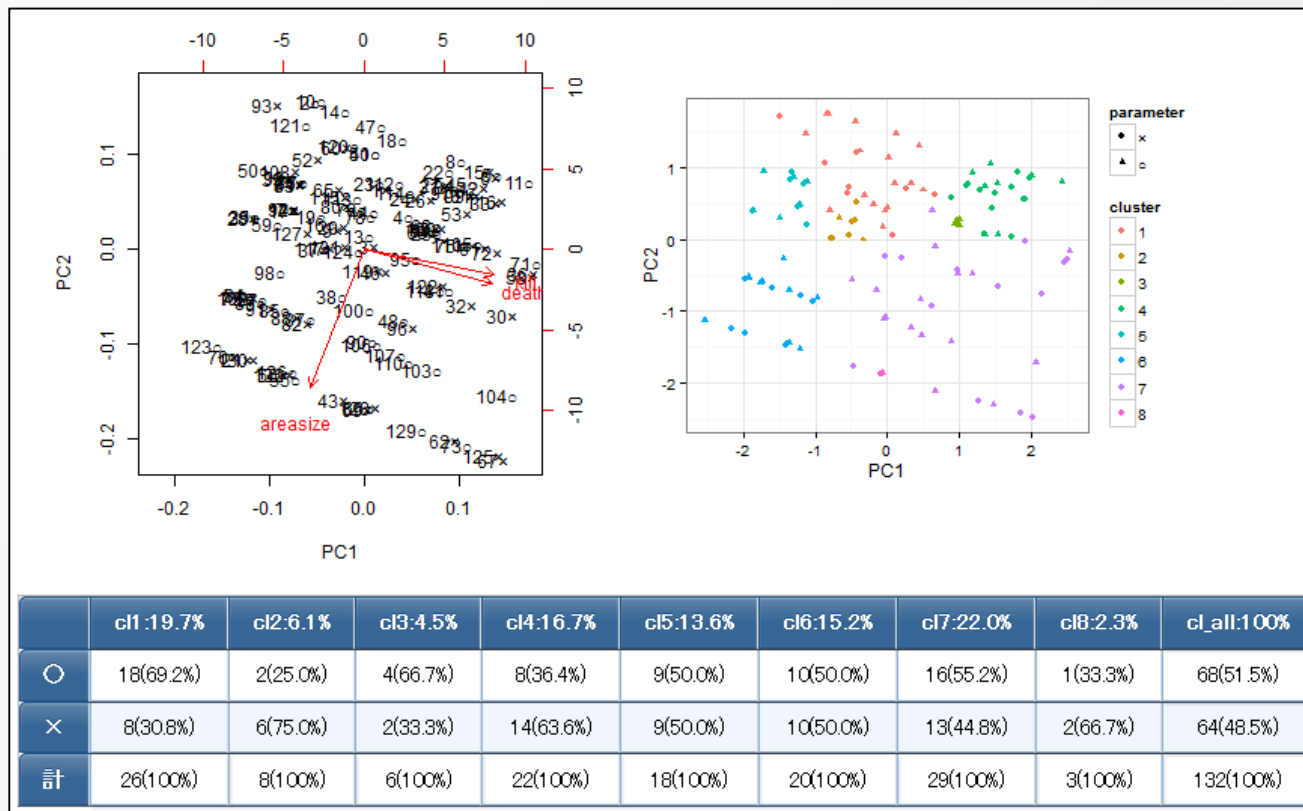
滋野 謙太郎 (しげのけんたろう)



- 理学部情報学科の大学を卒業後、SE(システムエンジニア)として13年間、システム開発を主とした多種のIT系業務に携わる
- SE時代後半はセキュリティに関わる仕事に携わる
 - マルウェア識別情報分析・システム脆弱性診断等
- 2017年9月から、情報科学専門学校で教員としてセキュリティ分野を主に教え、現在に至る

講師自己紹介

- SE時代はデータ分析も手掛けてました



勝敗分析もできる、ITならね

講師自己紹介

- 燻製とかも最近始めました



割と手軽にできるので、興味ある人はぜひ！

実習する前に

本日学ぶ内容を

絶対に悪用しないでください



- 実際のホームページにも行うことができる実践的な内容をお伝えします。
- 相手の許可なく脆弱性診断を行うことは**犯罪**となります。
(今回のページは勉強用のページなのでOK)

今回の講義内容

- Webページの仕組み
- URL欄からの送信内容改ざん
- デベロッパーツールを使った改ざん
- 総合演習



Webページの仕組み



普段よく見るWebページの例

- メモ帳アプリで作るメモよりも豪華な表現ができますよね



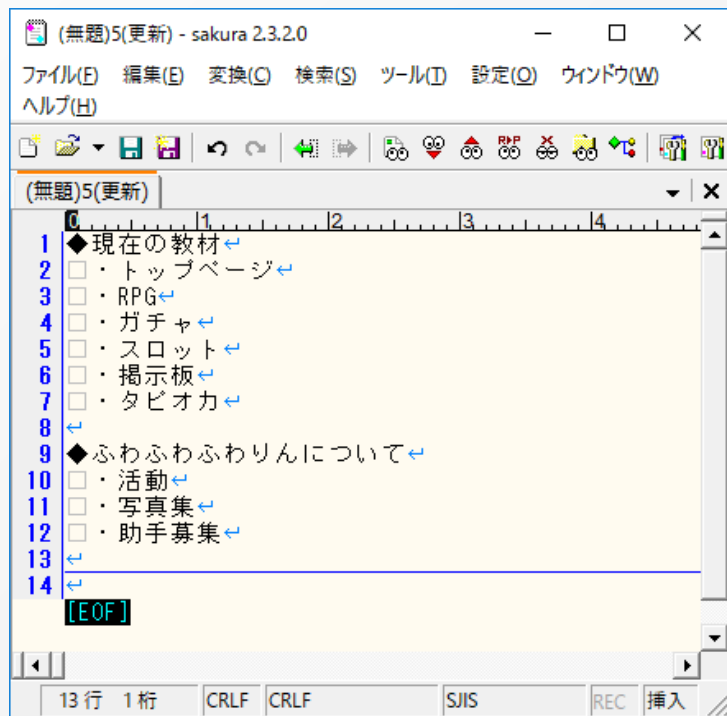
どうして？



形式の違い

- WebページはHTMLという形式で記載をしている為です！

普通のテキスト



HTML形式

```
    <th>ふわふわふわりんについて</th>
  </tr>
</thead>
<tbody>
  <tr>
    <td><li><a href="index.html">活動</a></li></td>
  </tr>
  <tr>
    <td><li><a href="picture.html">写真集</a></li></td>
  </tr>
  <tr>
    <td><li><a href="index.html">助手募集</a></li></td>
  </tr>
</tbody>
</table>
</div>
<div class="col-lg-10 order-lg-2">
  <div class="title">
    <h1>あのアイドルが！！</h1>
  </div>
  
</div>
```

HTMLのメリット

- タグと呼ばれる形式(<>で囲った部分)で要素を記載する事で、リンクや画像等、そのまま文字を表示するだけでは表現できないものを表現することができます

```
    <th>ふわふわふわりんについて</th>
  </tr>
</thead>
<tbody>
  <tr>
    <td><li><a href="index.html">活動</a></li></td>
  </tr>
  <tr>
    <td><li><a href="picture.html">写真集</a></li></td>
  </tr>
  <tr>
    <td><li><a href="index.html">助手募集</a></li></td>
  </tr>
</tbody>
</table>
</div>
<div class="col-lg-10 order-lg-2">
  <div class="title">
    <h1>あのアイドルが！！</h1>
  </div>
  
```

リンク

画像

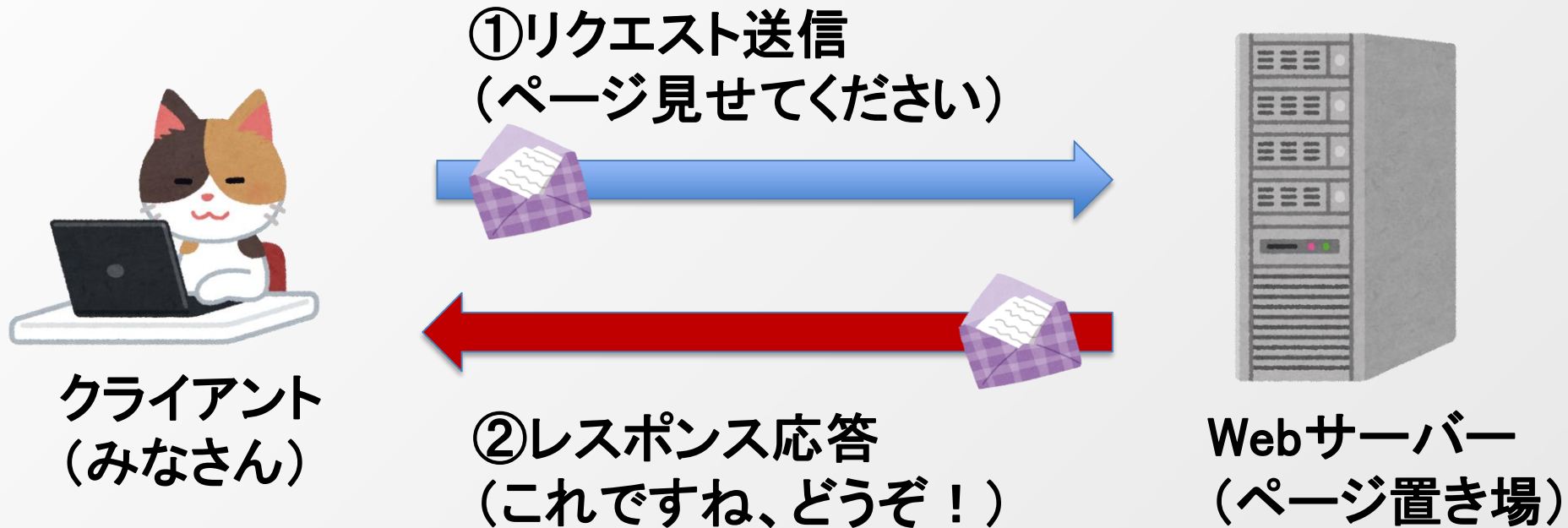
形式によって記載する内容の違い

- 通常のテキスト
 - 残しておきたい情報だけメモとして残す
- HTML
 - Webページの構成を含めた、ブラウザで表示するための設計図としての情報も含めて記載する

設計図となるHTMLを受け取ったブラウザが
皆さんのパソコンでイイ感じに表示を
してくれる仕組みになっています

Webページ参照の流れ

情報を取得する為のやりとり



リクエスト

実際に送っているリクエストの内容

メソッド

リクエストの対象

HTTPのバージョン

POST /cgi-bin/badstore.cgi?action=logi HTTP/1.1

Host: 127.0.0.1:8528

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: ja,en-US;q=0.7,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: http://127.0.0.1:8528/cgi-bin/badstore.cgi?action=loginregister

Content-Type: application/x-www-form-urlencoded

Content-Length: 45

Connection: close

Upgrade-Insecure-Requests: 1

画面での入力内容

email=test%40test.com&passwd=test&Login=Login

リクエスト行

ヘッダー

空白行

ボディ

レスポンス

HTTPのバージョン

ステータスコード

HTTP/1.1 200 OK

Content-Type: text/html

Server: Apache/1.3.20 Sun Cobalt (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b

PHP/4.0.6 mod_auth_pam_external/0.1 FrontPage/4.0.4.3 mod_perl/1.25

ETag: CPE1704TKS

Cache-Control: no-cache

Pragma: no-cache

Set-Cookie:

SSOid=dGVzdEB0ZXN0LmNvbTowOThmNmJjZDQ2MjFkMzczY2FkZTRlOD

MyNjI3YjRmNjp0ZXN0OjU=; Path=/

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">

<head>

ステータス行

ヘッダー

空白行

ボディ

画面に表示される
html

今回の講義内容



- Webページの仕組み
- URL欄からの送信内容改ざん
- デベロッパーツールを使った改ざん
- 総合演習

URL欄からの送信内容 改ざん



URLとは

- URLとは、Webサーバー（ページ置き場）の住所です！



クライアント
(みなさん)



住所：
<http://www.google.co.jp/>



Webサーバー
(ページ置き場)

インターネット広すぎるけど
住所を頼りにすれば
場所分かるよね

URLの例

- 例えば、Googleで「yabai」という単語で検索すると、以下の様なURLを元に検索結果を出してくれます



URL書き方

- これをもう少し詳しく分解すると、こんな意味を持っています
(実際に検索すると、もう少し末尾に色々ついてきます)

プロトコル

Webサーバの名前

http://www.google.com/

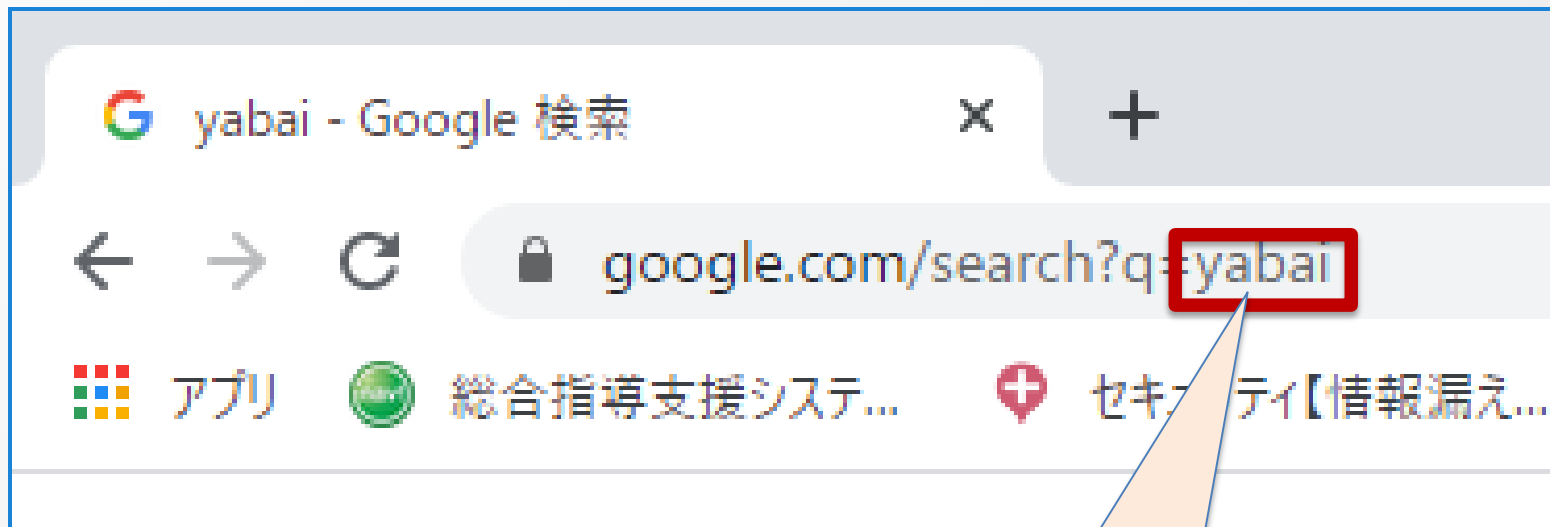
search?q=yabai

サーバの中の場所

ページを見る時に
伝えたい内容

URL変えるとどう動くのか

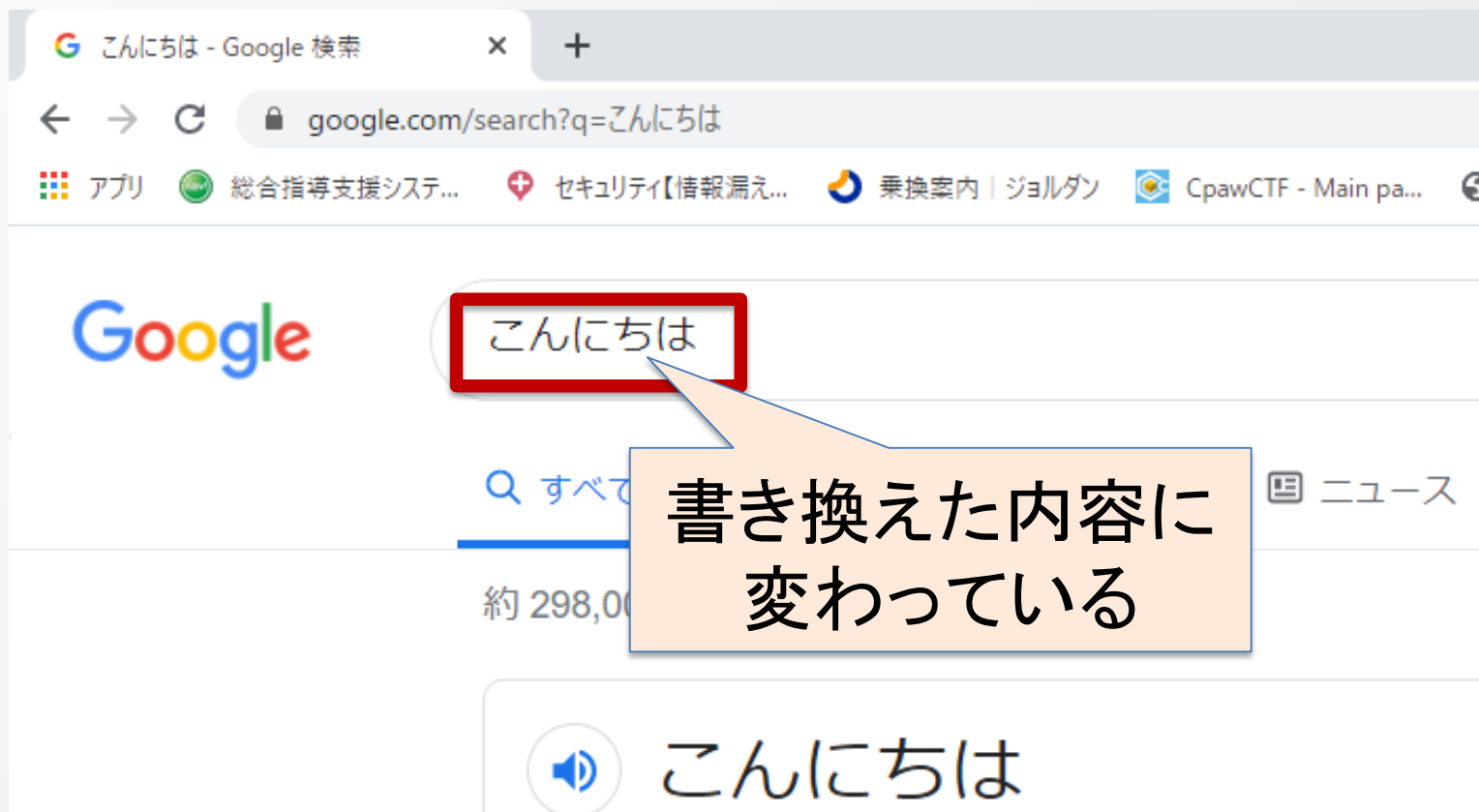
- 先ほどの検索結果の「yabai」という単語を別の単語（例えば「こんにちは」等）に書き換えて開いてみましょう



書き換える

書き換え後の動作

- 検索欄を使うことなく、書き換えた単語での検索結果を得る事ができます



これができると何がまずいのか

- 送る前に入力された内容をチェックする様なページがあったとする
- 書き換えられた内容を勝手に送られることはシステムを作った人は想定していな
い(場合が多い)



これができると何がまずいのか

- つまり、システムを作った人が許可して
いない動作ができてしまう
 - 例えば、想定していないページが表示
させられてしまったり
 - インターネットバンキングの振込機能
でマイナスの値を振り込めてしまう



実際に送信内容の改ざんを試みよう

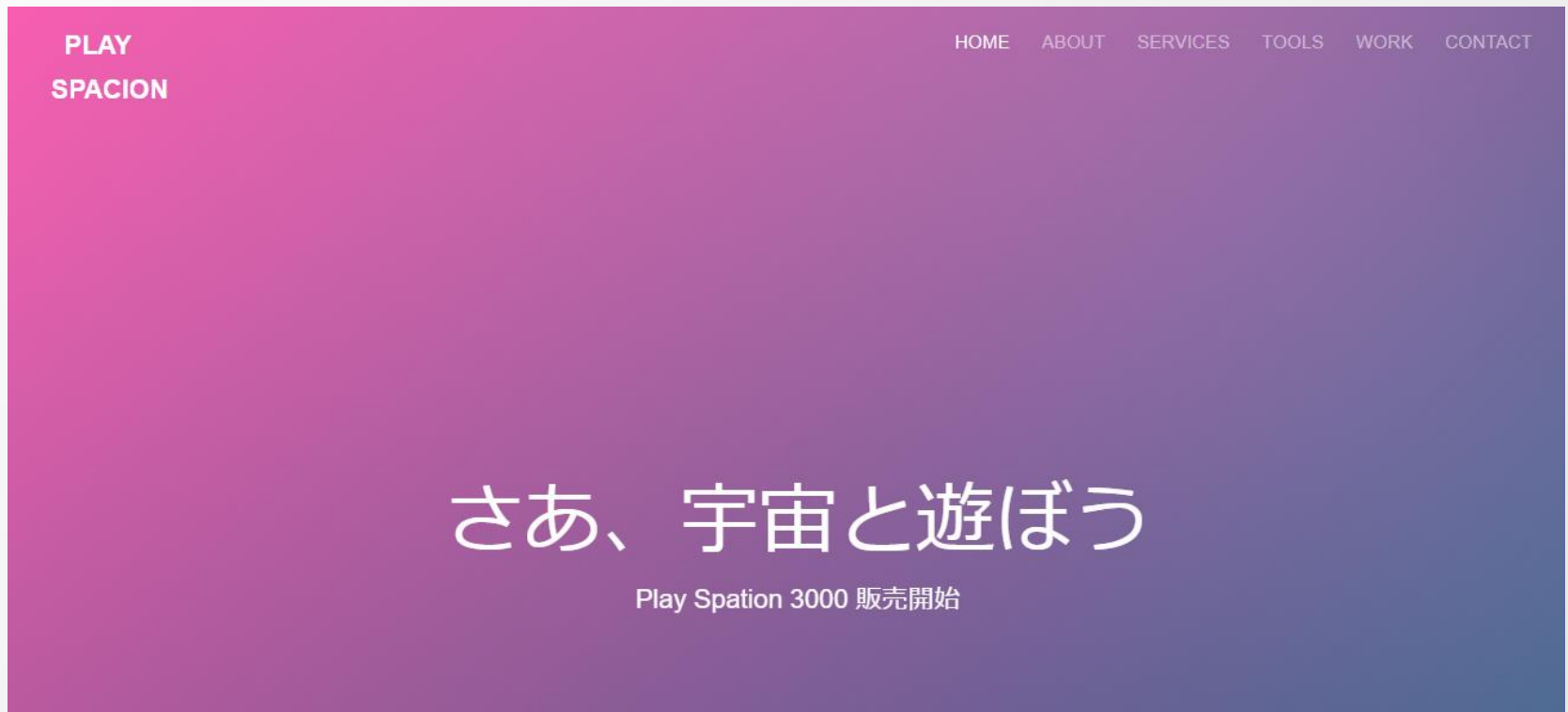
以下のURLを入力して移動してください

<http://learn.secret.jp/ps>



実際に送信内容の改ざんを試みよう

架空のゲーム機「プレイスペーション3000」の購入画面が表示されます



実際に送信内容の改ざんを試みよう

画面を下にスクロールして、「購入する」ボタンを押して1台購入してください



さあ、宇宙と遊ぼう

Play Spation 3000 販売開始

購入情報入力

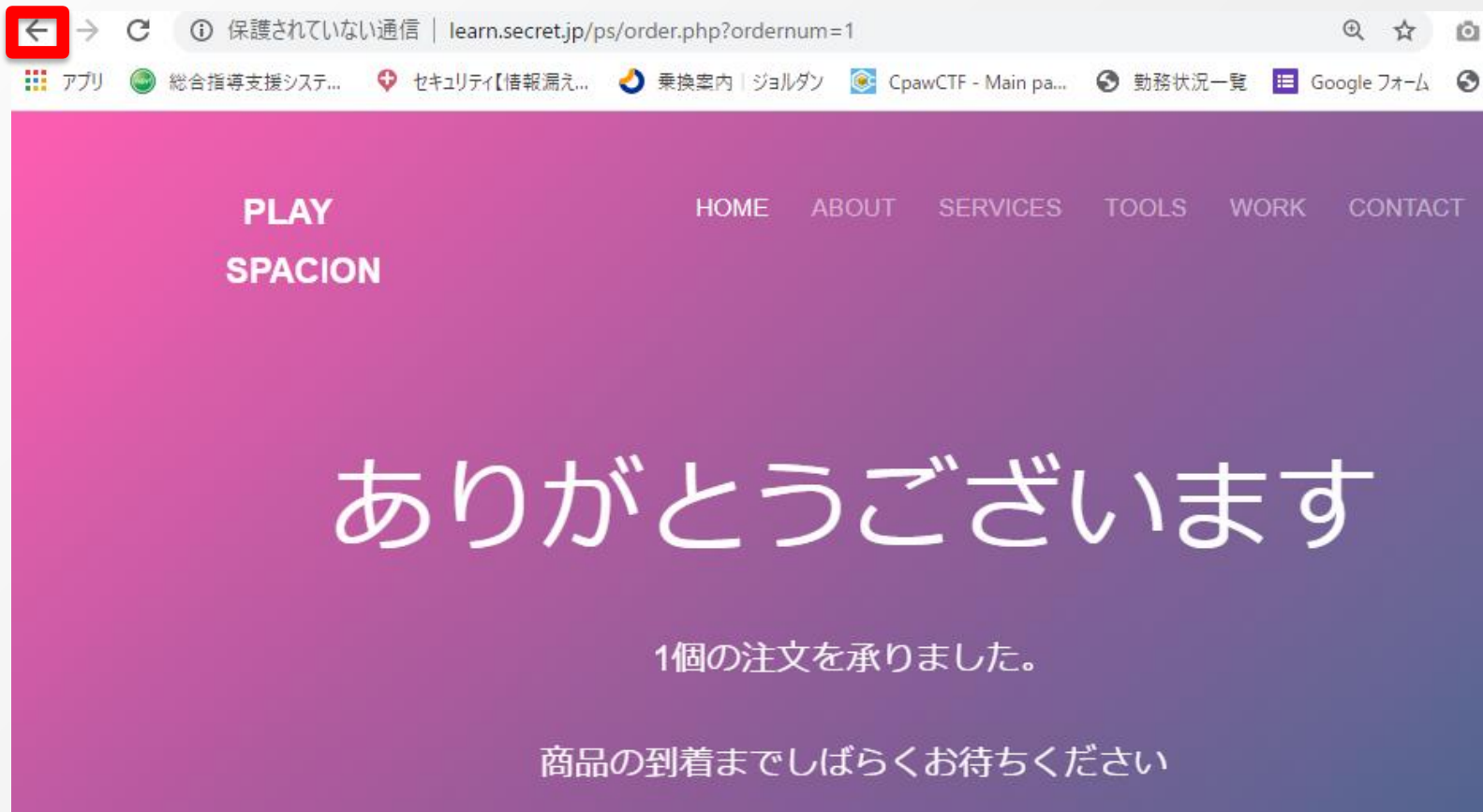
購入個数を入力してください(お一人様2台まで)

1台 ▼

購入する

実際に送信内容の改ざんを試みよう

成功すると、以下の様な画面が表示されます。ブラウザの戻るボタンで一つ前の画面に戻ってください

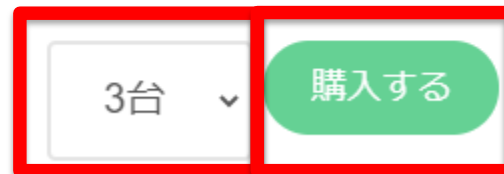


実際に送信内容の改ざんを試みよう

画面を下にスクロールして、購入個数を3台にしてから「購入する」ボタンを押してください

購入情報入力

購入個数を入力してください(お一人様2台まで)



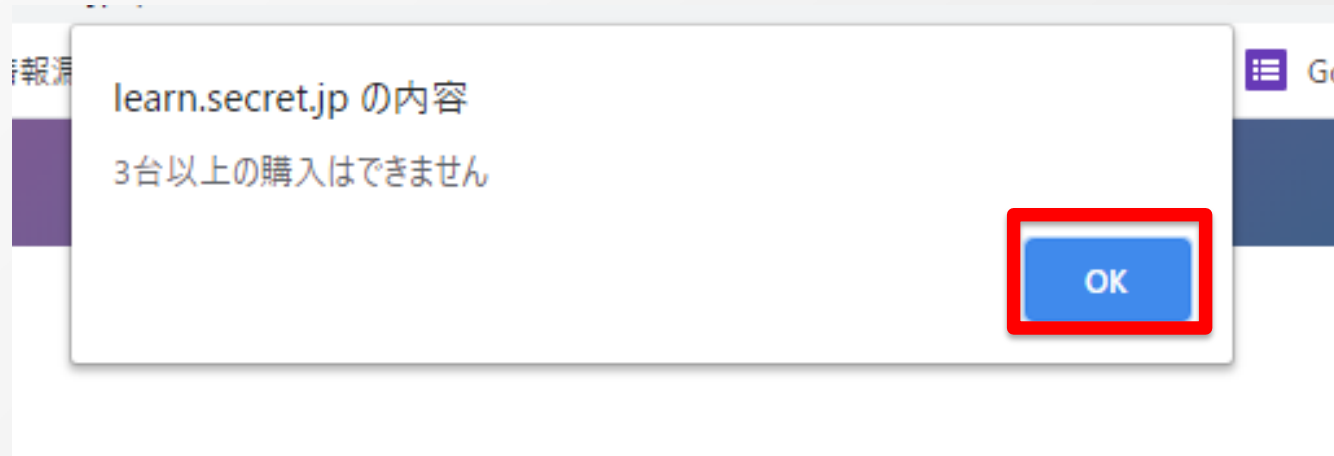
The image shows a purchase information input form. It consists of a dropdown menu on the left and a green button on the right. The dropdown menu is currently set to '3台' (3 units) and has a small downward arrow next to it. The green button is labeled '購入する' (Purchase). Both the dropdown menu and the button are highlighted with a red rectangular border.

3台 ▼	購入する
------	------

実際に送信内容の改ざんをしてみよう

購入台数チェックによって、3台以上の購入ができない旨が表示され、購入に失敗してしまいます。

OKボタンを押してエラー表示を閉じましょう



実際に送信内容の改ざんをしてみよう

【練習問題】

送信内容を書き換えることによって
プレイステーション3000を10000台
購入してみましょう。

ありがとうございます

10000個の注文を承りました。

商品の到着までしばらくお待ちください

ヒント！

- ・購入するボタンを押すと購入台数がチェックされてしまいます。
どのように購入個数を送信すればチェックされずに
購入処理をさせる事ができるのでしょうか。
- ・そもそも選択ボックスに10000台購入する選択肢がない中
どうやれば購入個数10000台を送信する事ができるのでしょうか。

実際に送信内容の改ざんをしてみよう

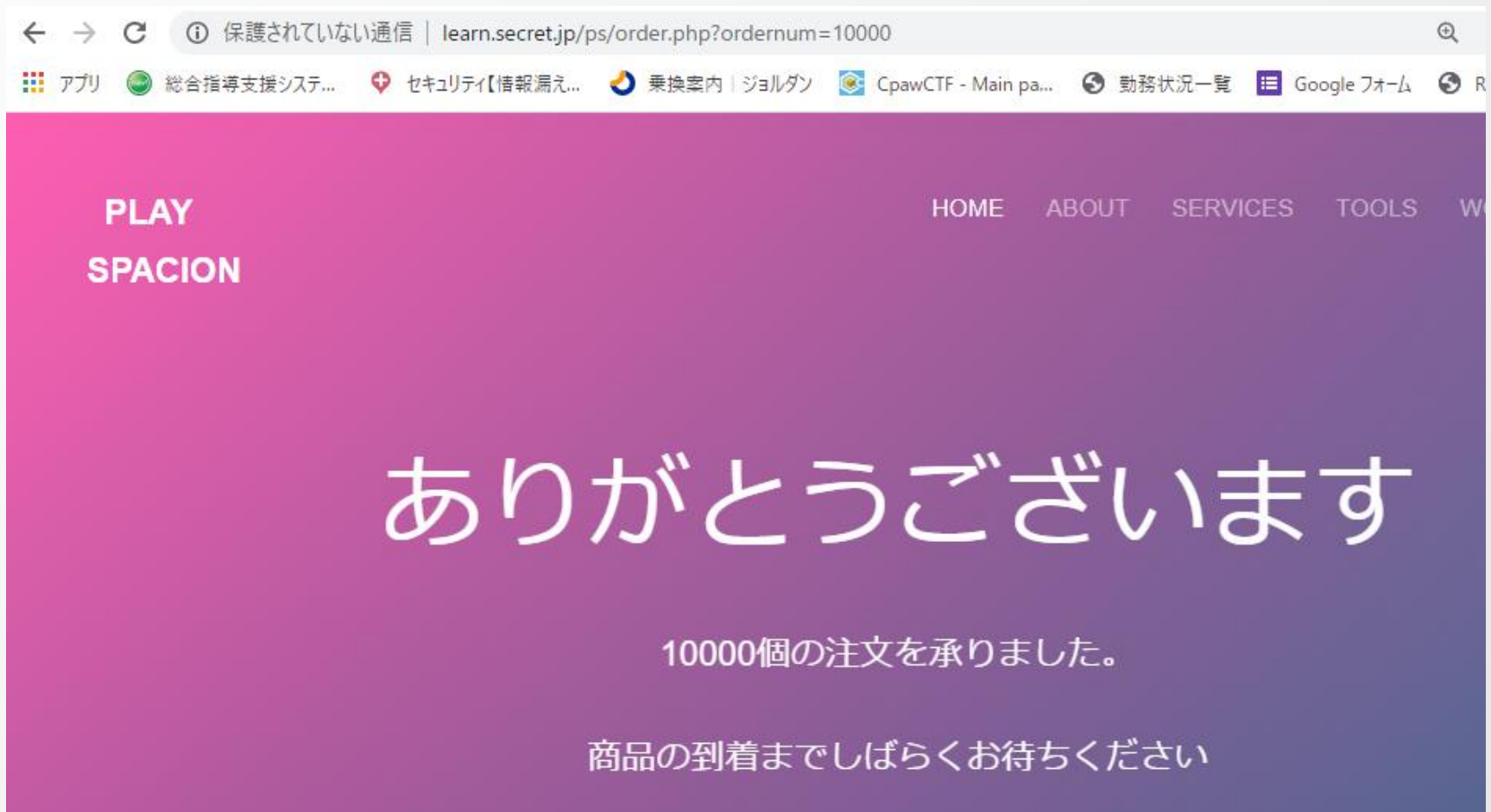
【練習問題 解答例】

1台購入した際のURLの中の、ordernum(注文数)の値を10000に書き換えて送信してみましょう



実際に送信内容の改ざんを試みよう

10000台の購入処理が実施された旨が表示されます



実際に送信内容の改ざんをしてみよう

【ポイント！】

今回の送信内容チェックは、「購入するボタンを押した時」に動作するものでした。

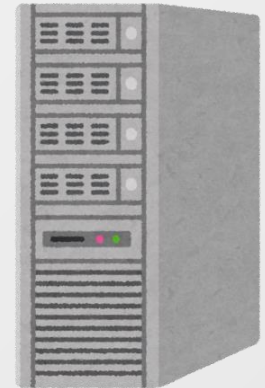
そのため、そもそも「購入するボタンを押さない」ことで、チェックそのものを行わせないことが可能となってしまいます。

【通常の流れ】



購入ボタン
押す

台数チェック
する



【送信内容を改ざんした場合】



自分で送る内容を用意する

Webサーバー
(ページ置き場)

今回の講義内容



- Webページの仕組み



- URL欄からの送信内容改ざん

- デベロッパーツールを使った改ざん

- 総合演習

デベロッパーツールを 使った改ざん



脆弱性を見つけてみよう

攻撃者の立場を知るために、どのように脆弱性を見つけるのか、体験してみましよう！

Webサイトを構成する仕組み

我々が普段見ているWebサイトは、中身を少し書き換えるだけで簡単に改ざんすることが出来てしまいます。

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

<title>セキュリティリスト</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>

</body>
```

画像ファイルの名前を
書き換える



表示される画像も書き換わる

改ざん完了

デベロッパーツールとは

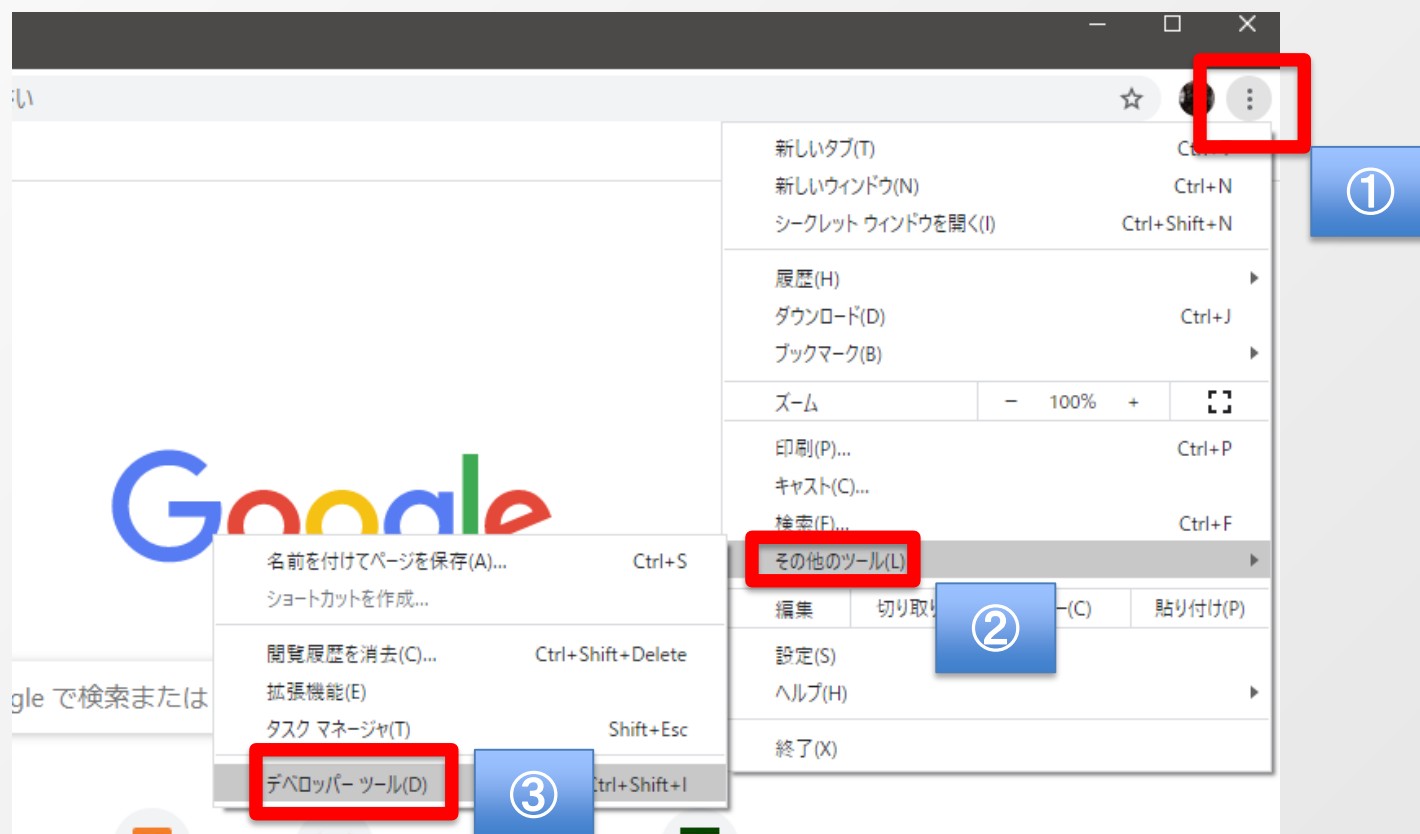
多くのブラウザに付属しているツールです。
Webサイトの動作の確認や細やかな変更を実際にプログラムを書き換えることなく確認することが出来ます。



本来はシステムを作る人
(デベロッパー)用のツールです

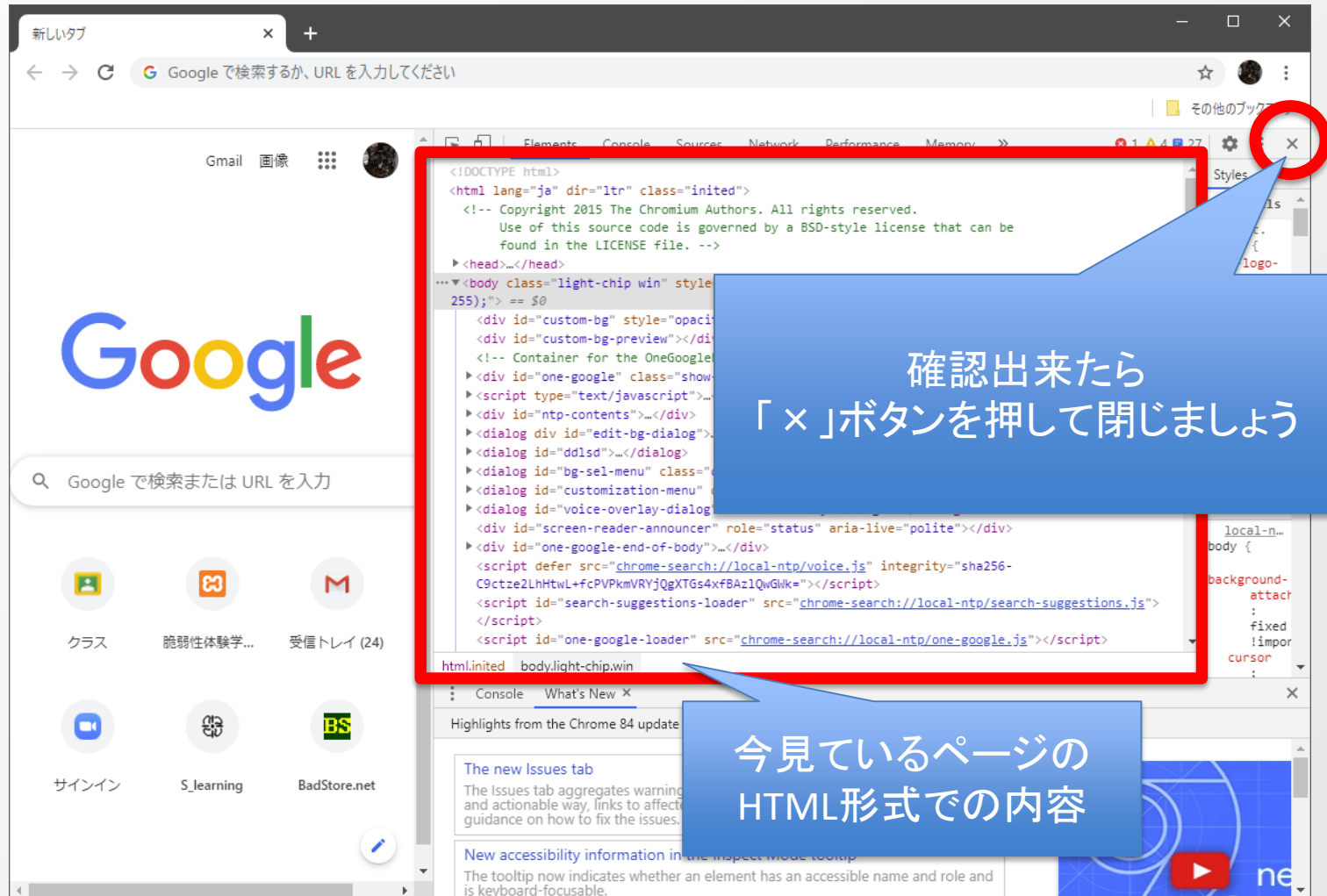
デベロッパツールの起動

Chromeを起動して、以下画像の順にクリックしましょう



実際にWebサイトの改ざんをしてみよう

画面右側に以下の様な画面が表示されればOKです



実際にWebサイトの改ざんを試してみよう

以下のURLを入力して移動してください

<http://learn.secret.jp/>



実際にWebサイトの改ざんを試みよう

画面左の「スロット」のリンクをクリックしてください



実際にWebサイトの改ざんを試してみよう

- ・デベロッパツールを起動してください。

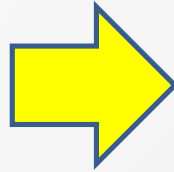


実際にWebサイトの改ざんを試してみよう



実際にWebサイトの改ざんを試してみよう

数字を変える



``

``

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できる

スロットゲーム



スロットをまわす!

実際にWebサイトの改ざんを試してみよう

【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です。
下のような当たり画像に変えてみましょう！

はずれ・・・



当 た り

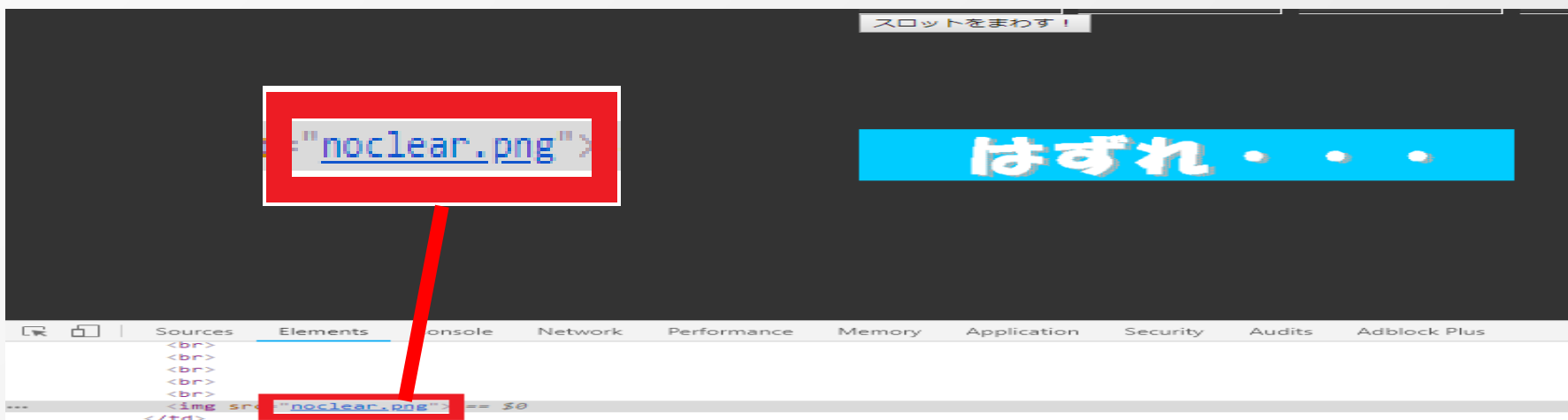
ヒント！

数字を全て同じにしても、外れのままです。
スロットの画像を変えたように、はずれをあたりにすると...？

実際にWebサイトの改ざんを試してみよう

はずれの画像を選択するとと出てくる、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サイトの改ざんを試してみよう



今回の講義内容



- Webページの仕組み



- URL欄からの送信内容改ざん



- デベロッパーツールを使った改ざん

- 総合演習

総合演習



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。



実際に演習問題を解く前に・・・

各問題へは、以下のサイトのメニューから移動することができます

<http://learn.secret.jp/>



演習問題その1

ソーシャルゲームで不正ができてしまわないか調査しよう

演習問題 その1

- ・ 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)

ヒント！

- ▷ ① ガチャ石の部分をデベロッパツールで調べてると？
- ▷ ② カード画像を見てみると法則性が見えませんか？

演習問題その2

勝手に管理者になりすまされてしまわないか調査しよう

演習問題 その2

このサイトは、ユーザー登録されたユーザーのみがログインできる投稿サイトです

- ・ ユーザ「admin」(管理者)としてログインしてみましょう
(adminユーザとしてログインする事でFlagが表示されます)

皆さんが使用可能なユーザID、パスワードは以下です

ユーザID: fuwa3

パスワード: masimasi1029

ヒント！

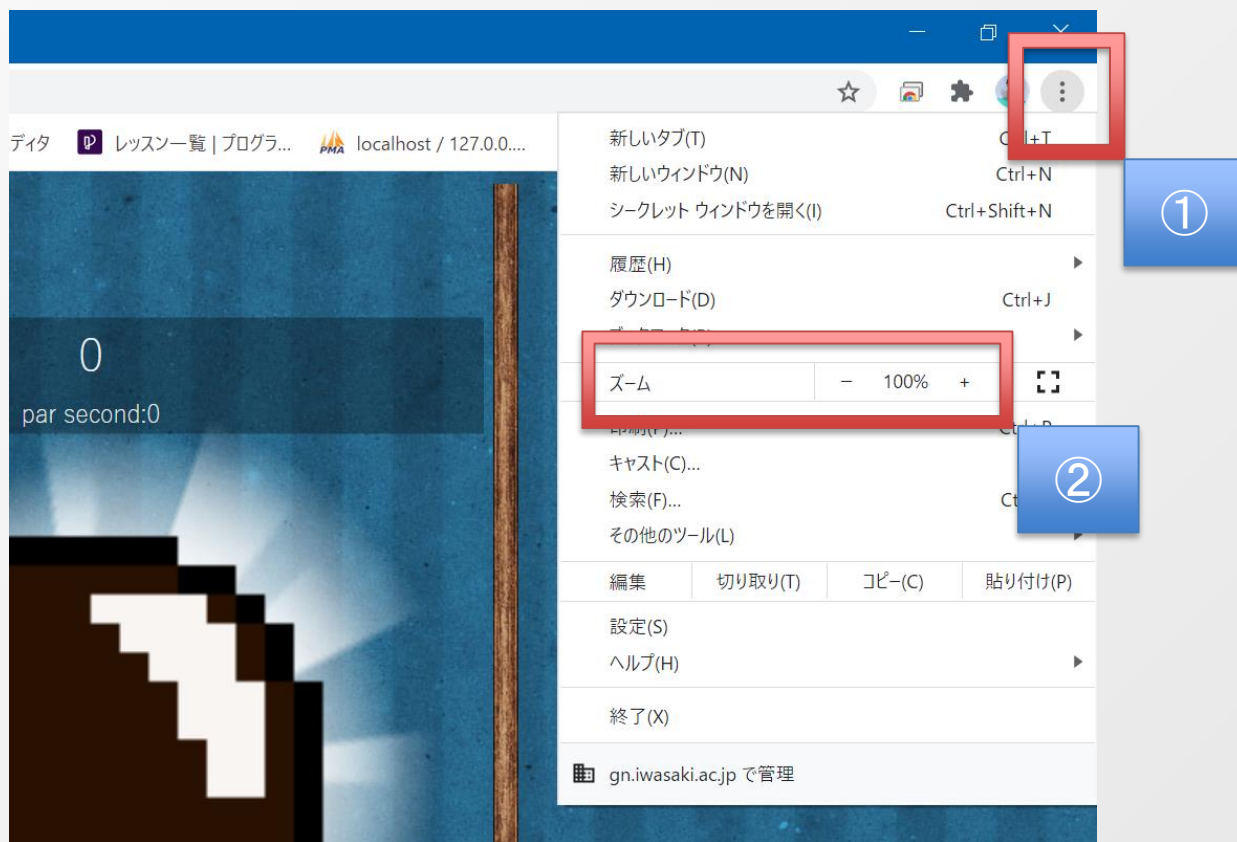
- ▷ マイページで登録された個人情報を見る事ができます
- ▷ パスワードは個人情報に関係した値に設定されることが一般的に多いです
- ▷ Adminユーザのマイページはどうすれば見れるのでしょうか？

演習問題その3

ゲームに脆弱性がないか調査してみよう

演習問題に入る前に ①

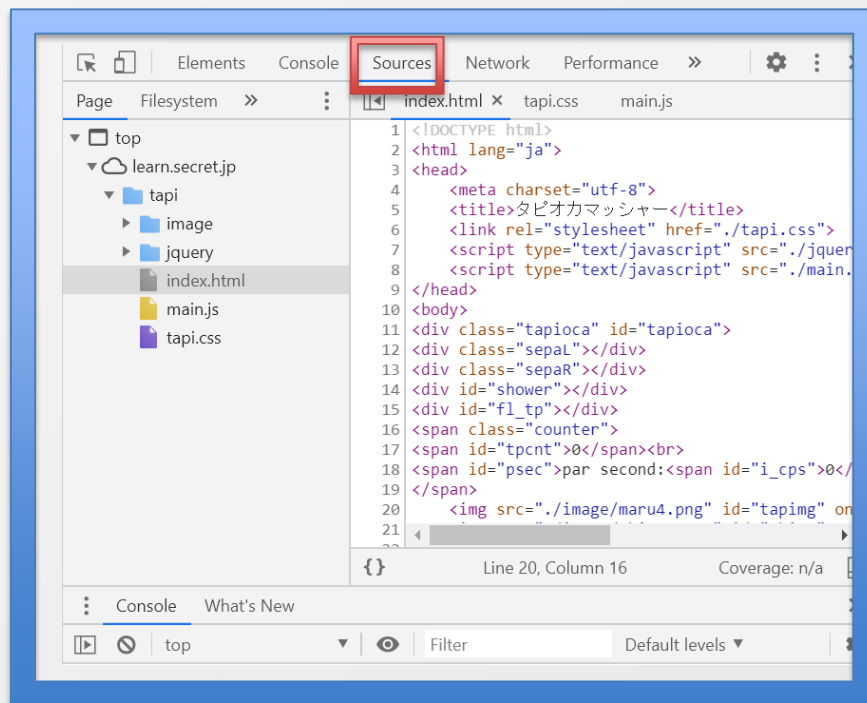
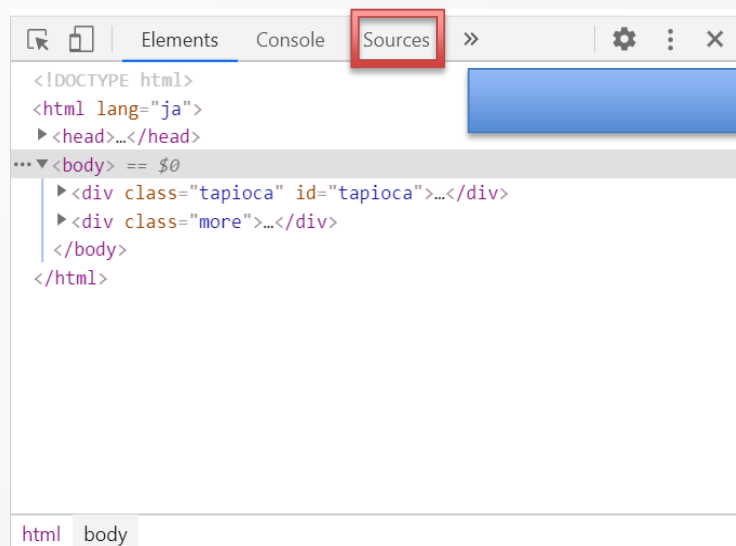
画像の順にクリックしズームが100%になっていることを確認してください



演習問題に入る前に ②

この問題ではデベロッパーツールの[Sources]を使用します。
[Sources]はデベロッパーツールを起動後、**赤枠**をクリック

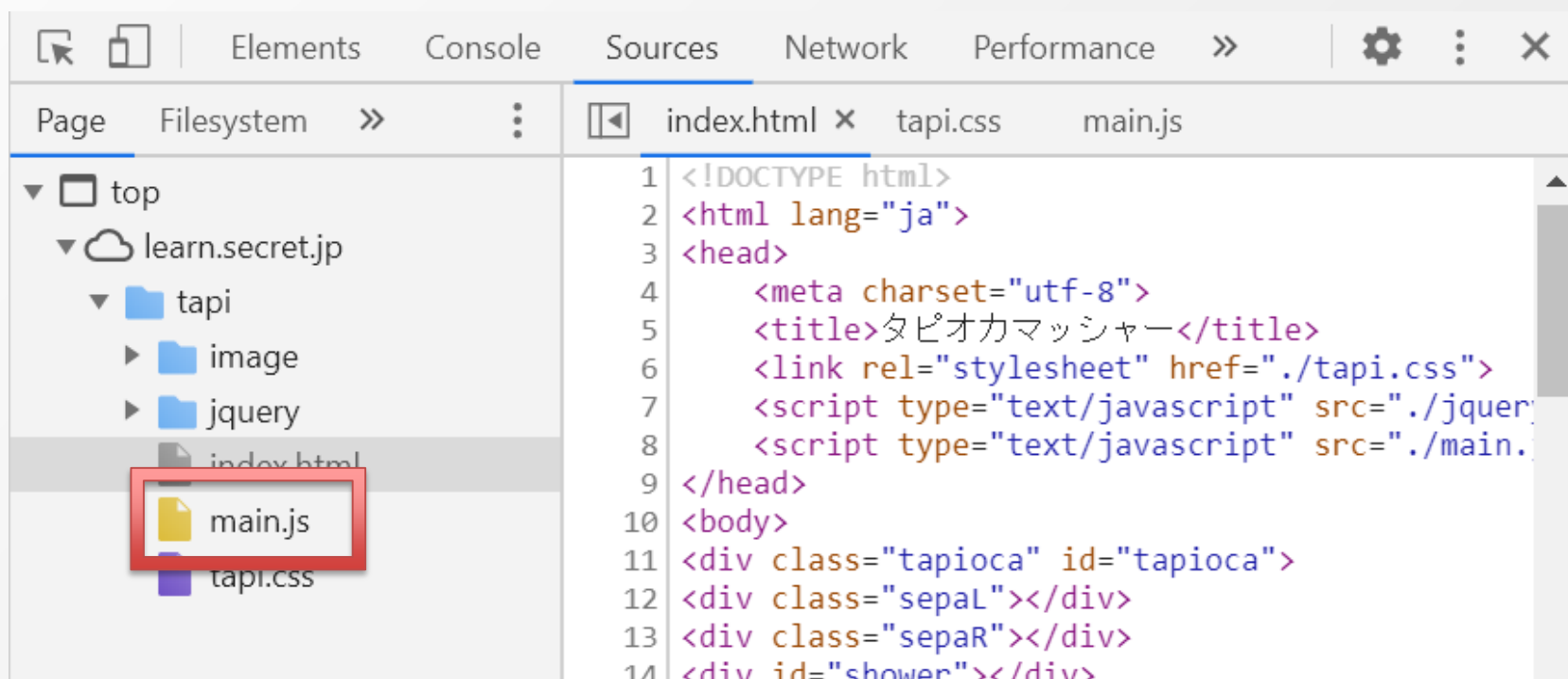
この画面になればOK！



演習問題に入る前に ③

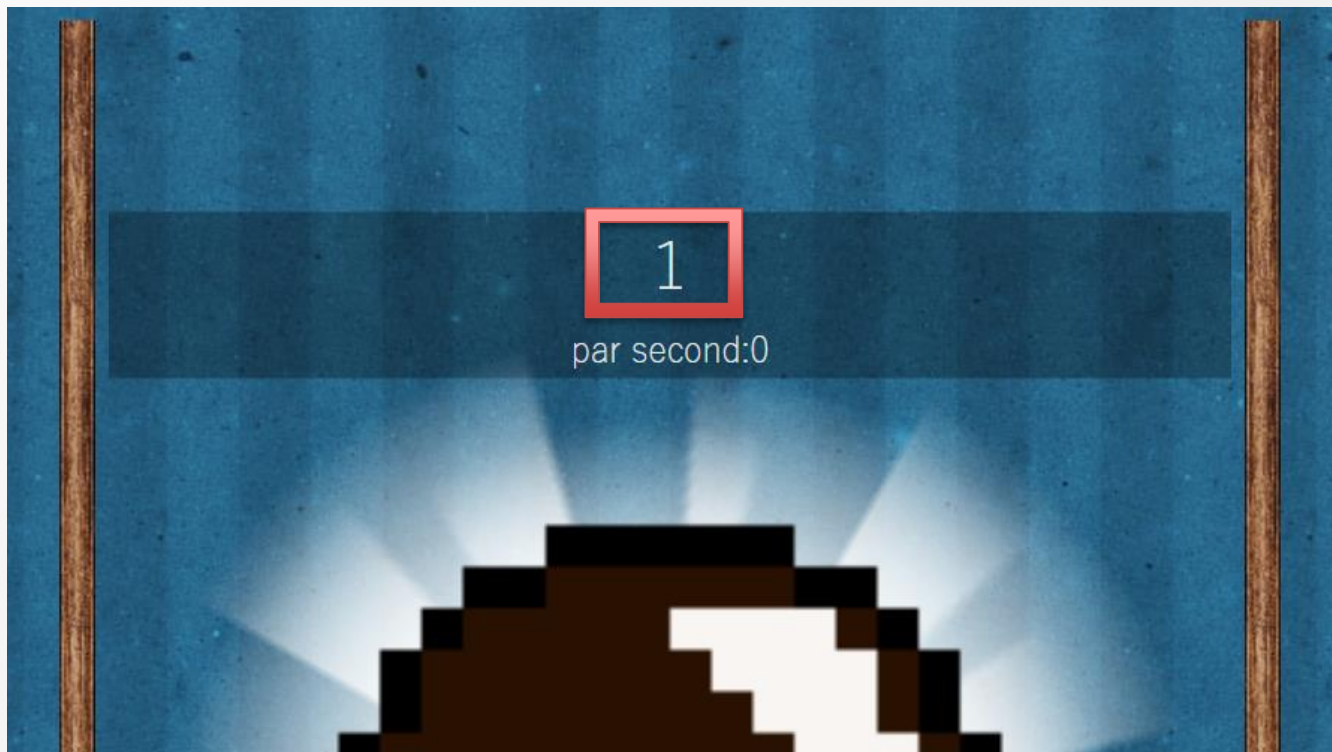
この問題では**赤枠**main.jsを使用します。

また、[Sources]からプログラムの変更を行う場合、変更後、保存
(Ctrlキーを押しながらSキーを押下)をしないと反映されません！



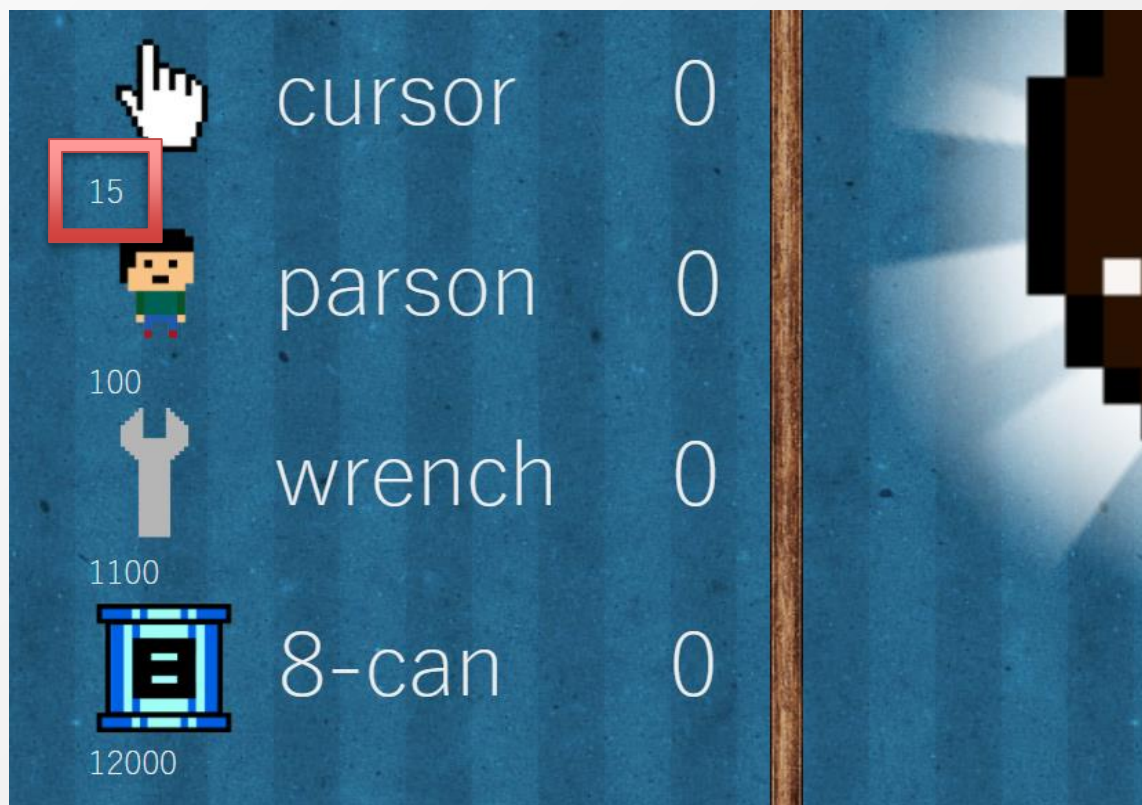
演習問題 その3 ゲーム説明

画面中央のタピオカをクリックすると**赤枠**の数字が増えます。
この数字は現在所有しているタピオカの数を表しています。



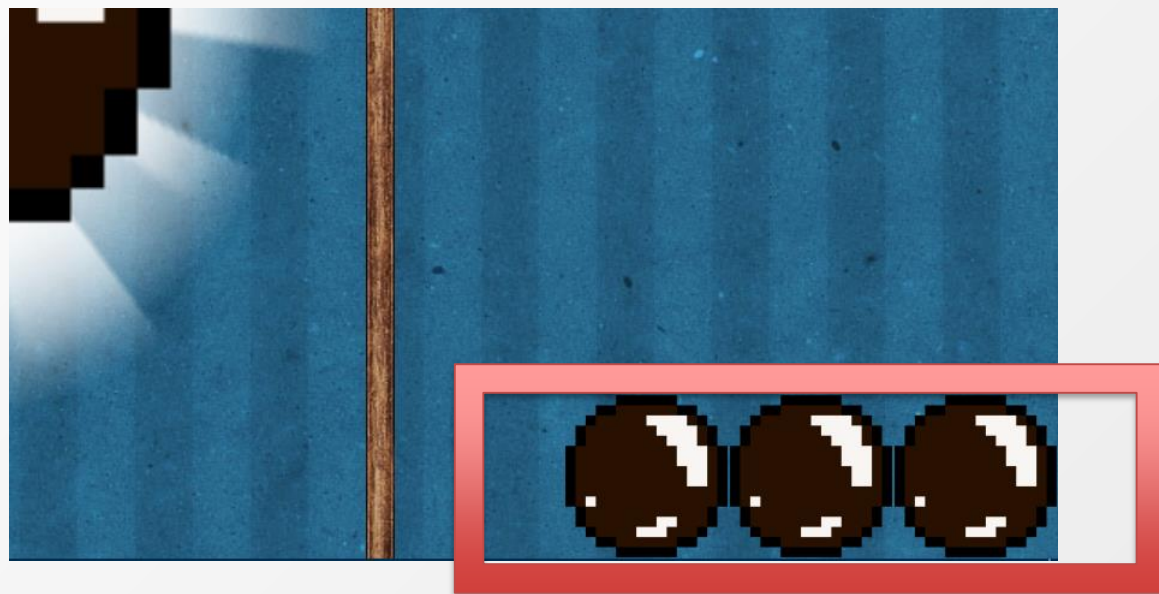
演習問題 その3 ゲーム説明

画面左下は、お助けアイテム！
タピオカを**赤枠**分消費して購入すると、
1秒ごとにタピオカを増やしてくれます！



演習問題 その3 補足

タピオカを貯め続けると右下に小さなタピオカが出現します
このタピオカを画面いっぱいまで積み上げ、あふれさせると
FLAGを入手できます。



演習問題 その3

タピオカを増やして、画面からあふれさせよう！

（画面右に表示されるタピオカが上限を超えるとフラグが表示されます）

ヒント！

- ▷ ① Sourcesからmain.jsを調べてみると？
- ▷ ② main.jsの中にタピオカを増やしている部分が...？

今回の講義内容

完了

- Webページの仕組み

完了

完了

完了

- 総合演習

おつかれさまでした！

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。

最後に

ご清聴ありがとうございました！

