Webプログラミングとセキュリティ

ウェブティ株式会社　塚本　翔

今日の授業について

- そんなに難しいことはやりません。

  ただし、プレゼンのページ数は　　を超えています。

- 皆さんにWebについての興味をもって頂くための

  スタートアップになればなと思います。

- 興味が出た点があれば、

  おうちで勉強してみてください！（これ大事）

自己紹介

なまえ　：　塚本　翔（つかもと　しょう）

年齢　　：　22歳

学歴　　：　国立津山工業高等専門学校　情報工学科卒

会社　　：　ウェブティ株式会社

職種　　：　プログラマー（フロントエンド寄り）

やっている仕事　：　企業等のHP製作、PHPやPythonを用いたシステム作成、ハードウェア関連

企業名	ウェブティ株式会社
所在地	岡山市北区西古松
設立	2008年9月19日
代表取締役	中西　充

事業内容

Webサイト製作
Webシステムの構築
DTP（名刺・パンフレット・チラシなど）
広告代理業及び広告業
PC関連のOA機器の卸売販売
ネットワーク構築

Webty

10th Anniversary

ウェブ製作会社の１日

- 9:26　出社
- 9:30　始業
- 12:00　お昼休憩
- 13:00　休憩終了
- 18:30　業務終了
- 18:38　退社

・ ざっくりとした1日の流れです。

業務時間はひたすらプログラミングをしています。

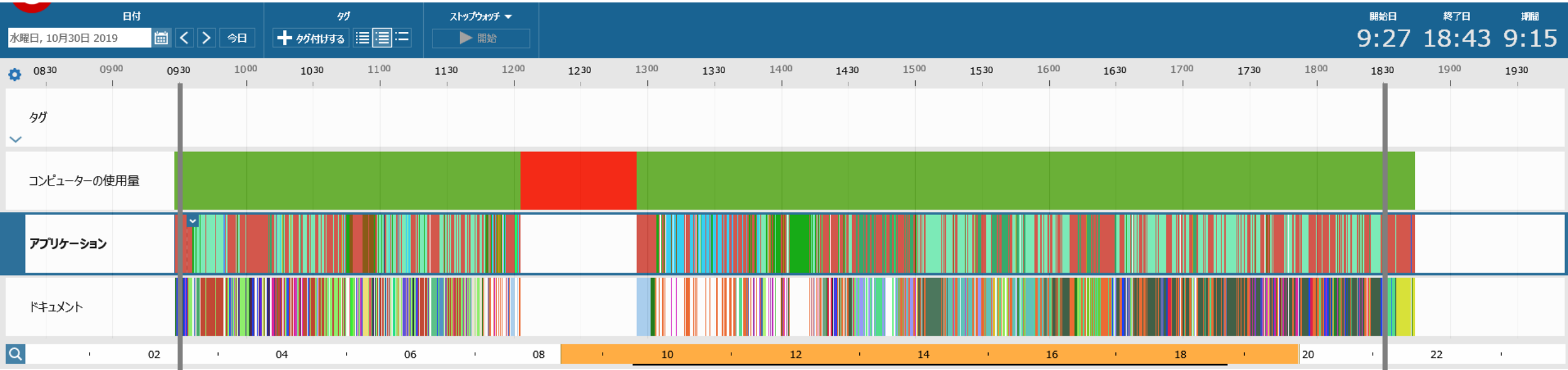
・ 午前は頭が働いていないことも多いので、

HTML/CSSなどのコーディング作業を多めに割り振っています。

・ ノッてきた午後はphpなどを使ったシステム部分等を

プログラミングしていくことが多いです。

業務を視覚的に捉える①

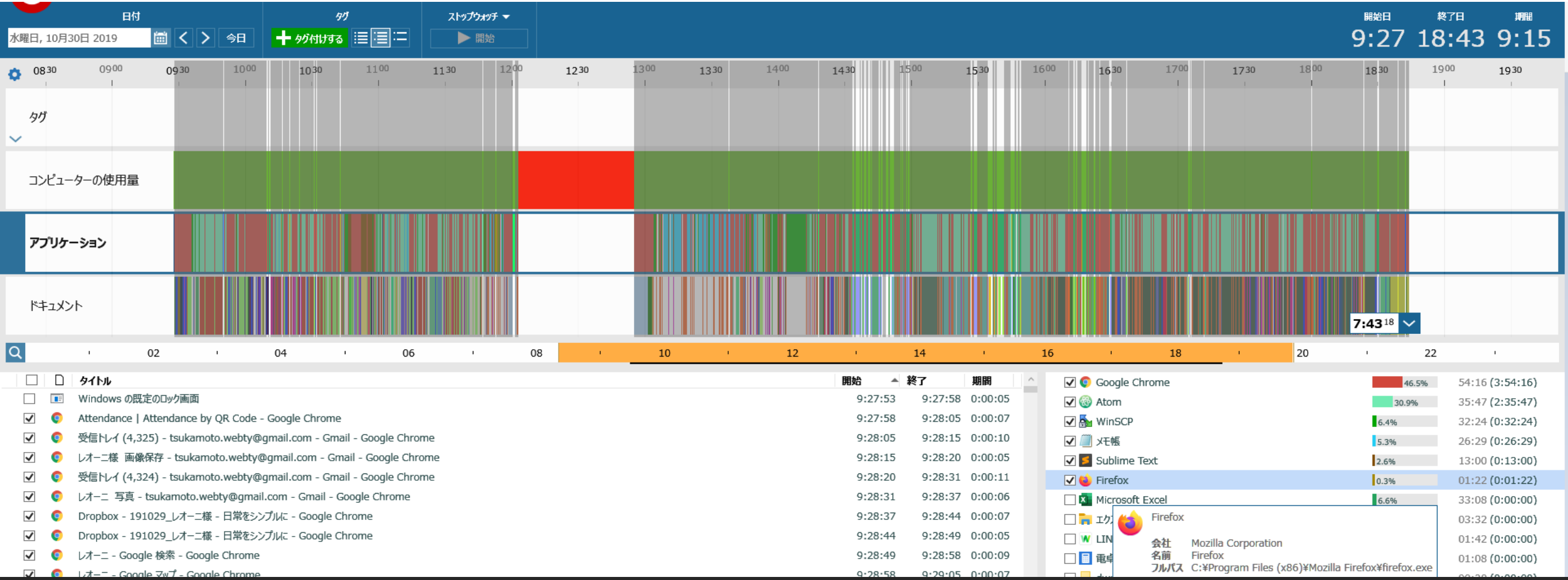


9:30

ManicTime ・・・ システムに常駐してPCの利用状況を
トラッキング・集計できるツール。

18:30

業務を視覚的に捉える②



Web製作について

テキストエディタの紹介（四天王）

Visual Studio Code

Atom

Sublime Text

メモ帳

- テキストエディタ　＝　Webプログラミングを語る上で切っては切り離せないモノ

  メインの仕事道具の一つ！！

テキストエディタの機能

```php
use glider\View\View;
use app\models\Item;

class ItemController extends AdminController
{
    protected $item;

    public function __construct()
    {
        parent::__construct();
        $this->item = new Item();
    }

    public function index(): string
    {

        $context = [
            'title'       => '商品管理',
            'items'       => $this->item->search([ 'delete_flg' => 0 ], [ 'update_at' => 'DESC'
            'update_time' => $this->item->getByLastUpdated(),
        ];

        return View::blade('item.index', $context);
```

- 関数やパラメータなどに色がつく
- コードの自動補完/自動整形がある
- ワードを一括置換できる
- リアルタイムでブラウザプレビューができる
- 

色が分かる

あなたはどっちが見やすい？

ItemController.php

```php
<?php

namespace admin\controllers;

use app\controllers\AdminController;
use glider\View\View;
use app\models\Item;

class ItemController extends AdminController
{
    protected $item;

    public function __construct()
    {
        parent::__construct();
        $this->item = new Item();
    }

    public function index(): string
    {

        $context = [
            'title'       => '商品管理',
            'items'       => $this->item->search([ 'delete_flg' => 0 ], [ 'update_at' => 'DESC'
            'update_time' => $this->item->getByLastUpdated(),
        ];

        return View::blade('item.index', $context);
    }

    public function new(): string
    {
        $context = [
```

untitled

```php
<?php
namespace admin\controllers;
use app\controllers\AdminController;
use glider\View\View;
use app\models\Item;

class ItemController extends AdminController
{protected $item;

public function __construct()
{parent::__construct();
$this->item = new Item();
}

public function index(): string
{$context = [
'title'=>'商品管理',
'items'=>$this->item->search(['delete_flg'=>0],['update_at'=>'DESC']),
'update_time'=>$this->item->getByLastUpdated(),
];
return View::blade('item.index', $context);
}

public function new(): string
{$context = [
'title'=> 'データの新規追加',
'item_names'=> $this->item->getByAllName(),
'item_counts'=> $this->item->getByCountName(),
'money_names'=> $this->item->getByAllMoney(),
'money_counts'      => $this->item->getByCountMoney(),
'categorys'=> config('admin.category'),
```

今日からテキストエディタマスター

- テキストエディタについて詳しくなかった方でも、今日の授業で

  テキストエディタ四天王を知ったので、テキストエディタマスターです。

- 明日から、良いプログラミングライフを歩んでください！

- それでは、次のページからは製作実績に移ります。

製作実績①

KeePerコーディング専門店
創car堂　様

https://socardo.com

【WordPress】

CAR SUPPORT LEAVE

車の事なら何でも"創car堂"にお任せください！

過去2015年よりキーパー選手権に出場しており、
2015年岡山県入賞、2016年岡山県優勝、
2017年岡山県準優勝、2018年岡山県準優勝の実績を持ったスタッフ達常駐。
丁寧にコーティング施工をさせていただきます。
認証整備工場併設なので整備から洗車、車検、車販売、板金塗装、
車の事なら何でもお任せください。代車無料、事前予約可。

製作実績②

ゴルフウェアショップ
MgM

https://mgm-netshop.com

【PHP】

MVC

不動産総合資金計画システム

LadyBug

キーワードを入力

ヘルプ　チャット　お問い合わせ

- 顧客管理
- 物件管理
- 資金計画
- ユーザー管理
- カレンダー
- TOPICS

TOPICS

2019.9.20	午前3時よりシステムメンテナンスにつき使用できません。
2019.9.19	新システムのモックを作成予定です。
2019.9.7	打ち合わせしましょう。
2019.9.3	画面設計してます。
2019.99.99	テキストテキストテキストテキストテキストテキストテキストテキストテキストテキスト

もっと見る ＞

todoリスト

- ☐ 打ち合わせしなきゃ！
- ☐ 打ち合わせしなきゃ！
- ☐ 打ち合わせしなきゃ！
- ☐ 打ち合わせしなきゃ！
- ☐ 打ち合わせしなきゃ！

＋追加する ＞　－削除する ＞

カレンダー

日	月	火	水	木	金	土
29	30	1	2 休み	3	4	5
6	7	8	9	10	11	12

製作実績③

不動産総合資金計画システム
LadyBug（フロントエンドのみ）

【Bootstrap　＋ PHP】

製作実績④

株式会社
クローバー不動産　様

https://clover-fudousan.jp

【WordPress】

ウェブティ株式会社

https://webty.jp

【Python】

MVC

Webプログラミング ①

使用言語について

- 弊社では圧倒的にphpです。次点でPythonになります。

- 昨今のWeb業界では、Ruby, php, Python等が筆頭にあげられます。

  もちろん、JavaやC#を使う会社もあるかもしれませんが…

phpとは？

- php = Hypertext Preprocessor を再帰的に略した名称

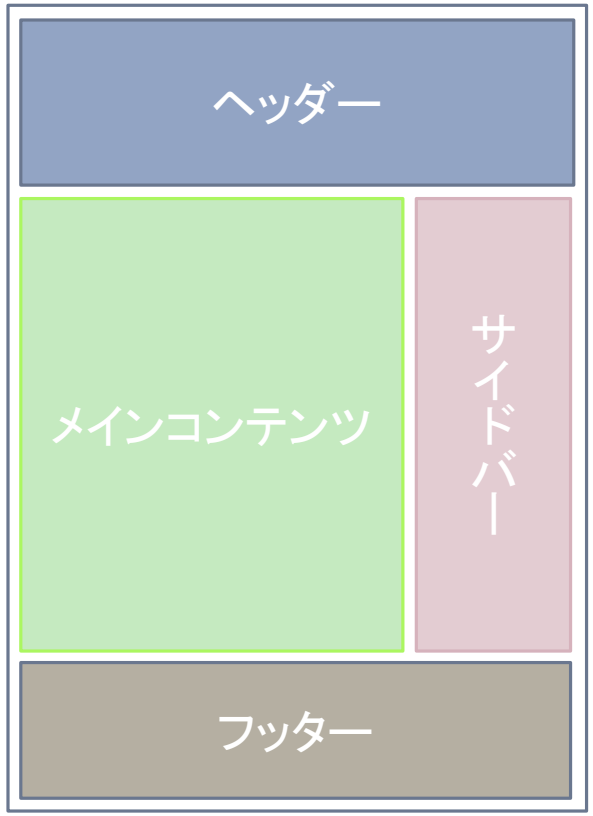
  HTML = 

- HTMLの中に埋め込んで使うことができ、動的なWebサイトを作ることが出来る。

  php で作られた代表的なサイト　=> **Facebook, Wikipedia ,Yahoo!** , CMS **: WordPress**

- phpはサーバーサイドの言語。DBとの連携も得意。

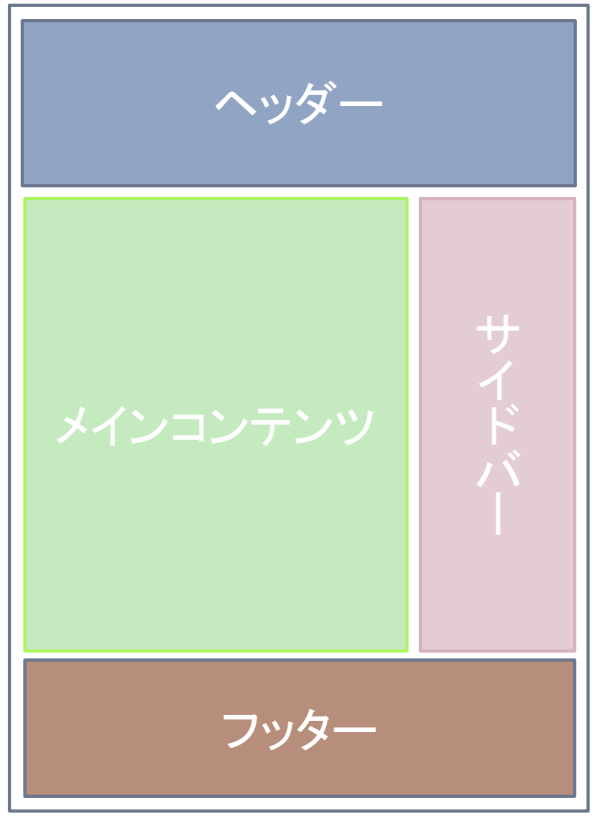
HTML/CSS での構築



index.html

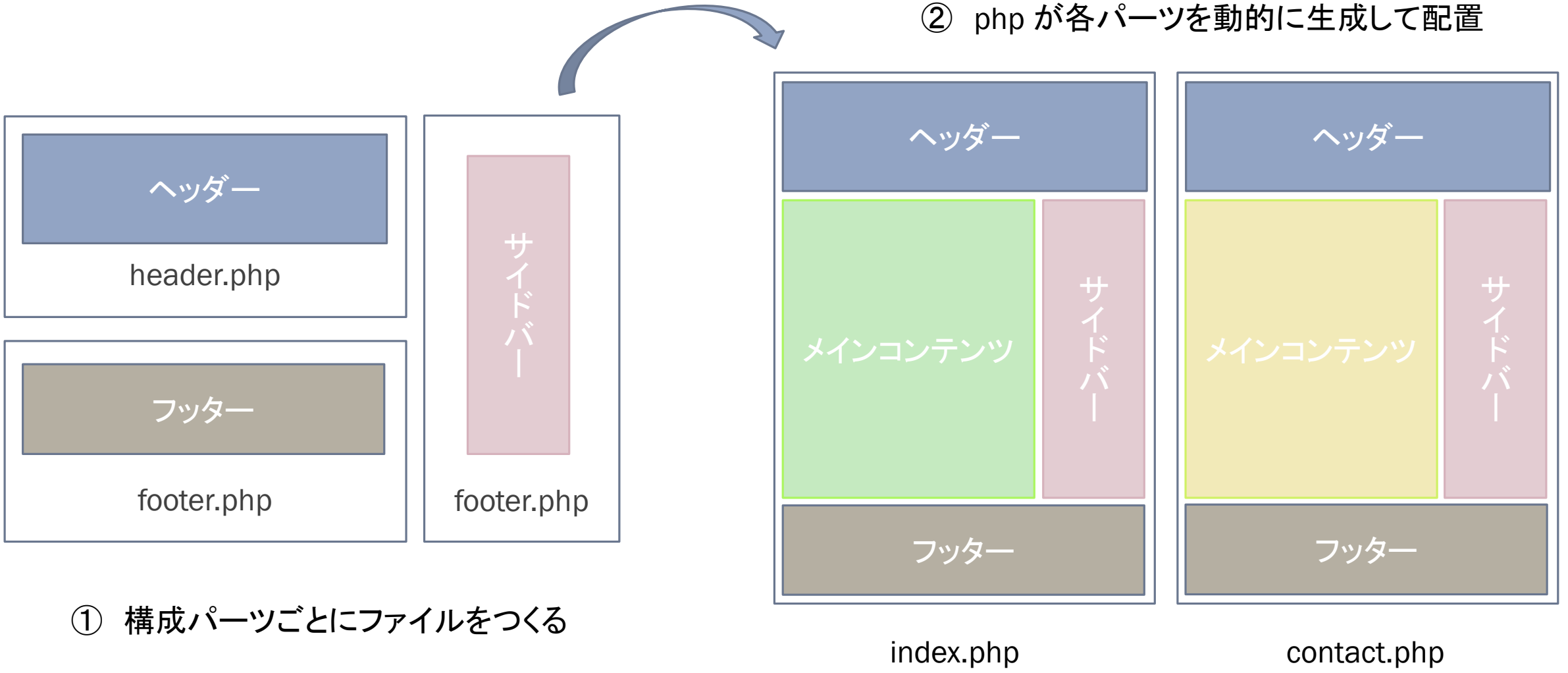
contact.html

topics.html



service.html

phpでの構築


ヘッダー
header.php
フッター
footer.php
サイドバー
footer.php
② php が各パーツを動的に生成して配置
ヘッダー
メインコンテンツ
サイドバー
フッター
index.php
ヘッダー
メインコンテンツ
サイドバー
フッター
contact.php
① 構成パーツごとにファイルをつくる

Component

- コンポーネントとは「**機能を持つ各パーツ（部品）の集合体**」のこと

  Web製作において、機能や振る舞いなどを明確に分離することが重要になってくる。

メリット

- 最初にコンポーネント(部品)を作っておけばあとはそれを組み合わせていけばページができる。
  一回、作ってしまえば他人とチームを組んでの開発でも分かりやすい。

- コンポーネントは汎用的であるので、角を丸くしたり色を変えたりと他サイトでも使い回しが容易。

- メンテナンスも簡単になる。

Webプログラミング ②

フレームワーク

- framework = 枠組み。

  よく使う機能等を予め用意して提供してくれるもの！例えるならカレーの市販固形ルー！

- Webフレームワークを使うことで、少ない記述でそれなりのものが作れる。

フレームワーク

【メリット】

- 既に必要な機能郡が準備されているので生産性が高い
- 工数、コストを減らすことができる（毎回、同じことばっかり書きたくないでしょ？）
- コードの書き方が統一される

【デメリット】

- 学習コスト　各フレームワーク特有の書き方を覚える必要がある
- コーディングが減る→仕組みを分かっていなくても作れてしまう→技術力の低下

Bootstrap

・ レスポンシブデザインに対応したフロントエンドのフレームワーク

フロントエンド＝HTML・CSS・JavaScript

・ https://getbootstrap.com/docs/4.3/components/alerts/

・ 部品の塊！HTMLからクラスを指定するだけで簡単にデザインが完了するスグレモノ

Ruby on Rails

“Convention over Configuration”

- Ruby　のためのフレームワーク，MVCに従う

  「設定より規約」、「同じことを繰り返さない」等の設計思想は

  他の言語やフレームワークにも影響を与える

- Webアプリケーションやシステム製作，スクレイピング等に強い

- Cookpad, Hulu, 食べログ, 価格.com, Github .....

django

“Batteries included”

- Pythonで作られているWebフレームワーク、MVCにゆるやかに従い
  開発者が “すぐに” やりたいことのほとんどを提供する

- 高品質なWebアプリケーションを簡単に少ないコードで作成できる
  「ユーザー認証」、「管理画面」、「RSSフィード」などがデフォルトで準備

- YouTube, Dropbox, Instagram, Spotify, NASA ....
  コメント機能、投稿機能、ログイン機能、シェア機能....

Laravel

“The PHP Framework for Web Artisans”

- ウェブ職人のためのphpフレームワーク

  php で 手軽に高機能なWebアプリやサイトを作れる

- ウェブティでは，LaravelとDjangoからインスパイアされた

  独自フレームワークでシステム等を作っています！

B

Block

E

Element

M

Modifier

BEMとは？

- Webサイトのコンポーネント化のためのフロントエンド設計方法(CSS)のひとつ

  Block – Element – Modifier　の頭文字をとってBEM

- BEMが目指す目標
  - 長期間メンテナンスできる設計で、ファーストバージョンの開発をすばやく
  - チームのスケーラビリティ
  - コードの再利用性

BEMのメリット・デメリット

【メリット】

- HTMLとCSSは、いつでもデザインの変化に対応できる
- 皆が同じ言語でやりとりできるので、コミュニケーションが取りやすくなる
- 見ただけでなんとなくサイトの見た目がわかる

【デメリット】

- 独特な記法のため、BEMを知らない人から見ると、違和感を持つ人もいる
- ElementやModifierの名前が冗長になりがち

BEMの書き方

.navbar

.navbar__list

.navbar__list--active

- BlockとElementは　___　でつなぐ　，　ElementとModifierは　ーー　でつなぐ！

Block__Element--Modifier

- 大きな要素のかたまりがBlock, その中身の部品がElement, 部品の中で見た目が違うのがM

Component

- コンポーネントとは「**機能を持つ各パーツ（部品）の集合体**」のこと

  Web製作において、機能や振る舞いなどを明確に分離することが重要になってくる。

BEM -> SaSS

Sass/SCSS

“Sass makes CSS fun again” な言語のことです

SCSS（Sassy CSS）と**Sass**（インデント構文）の2種類ある

できること

- ファイルをまとめること
- 変数の使用
- ネスト
- 継承


```scss
div {
    width: 100px;
}

div a {
    color: red;
}
```

```scss
div {
    width: 100px;

    a {
        color: red;
    }
}
```

SCSSの使用例

実際にWeb製作でどうSCSSを使っているかご紹介します
BEMとの相性が良すぎるのが特徴です。

```
.service__list--box {
    width: 100%;
    max-width: 1200px;
}
.service__list--box:first-child {
    border: 1px solid #008000;
}
.service__list--box--text {
    color: #333;
}
.service__list--box--text a {
    color: #fff;
}
```

```
.service {
    &__list {
        &--box {
            width: 100%;
            max-width: 1200px;

            &:first-child {
                border: 1px solid $green;
            }

            &--text {
                color: #333;

                a {
                    color: #fff;
                }
            }
        }
    }
}
```

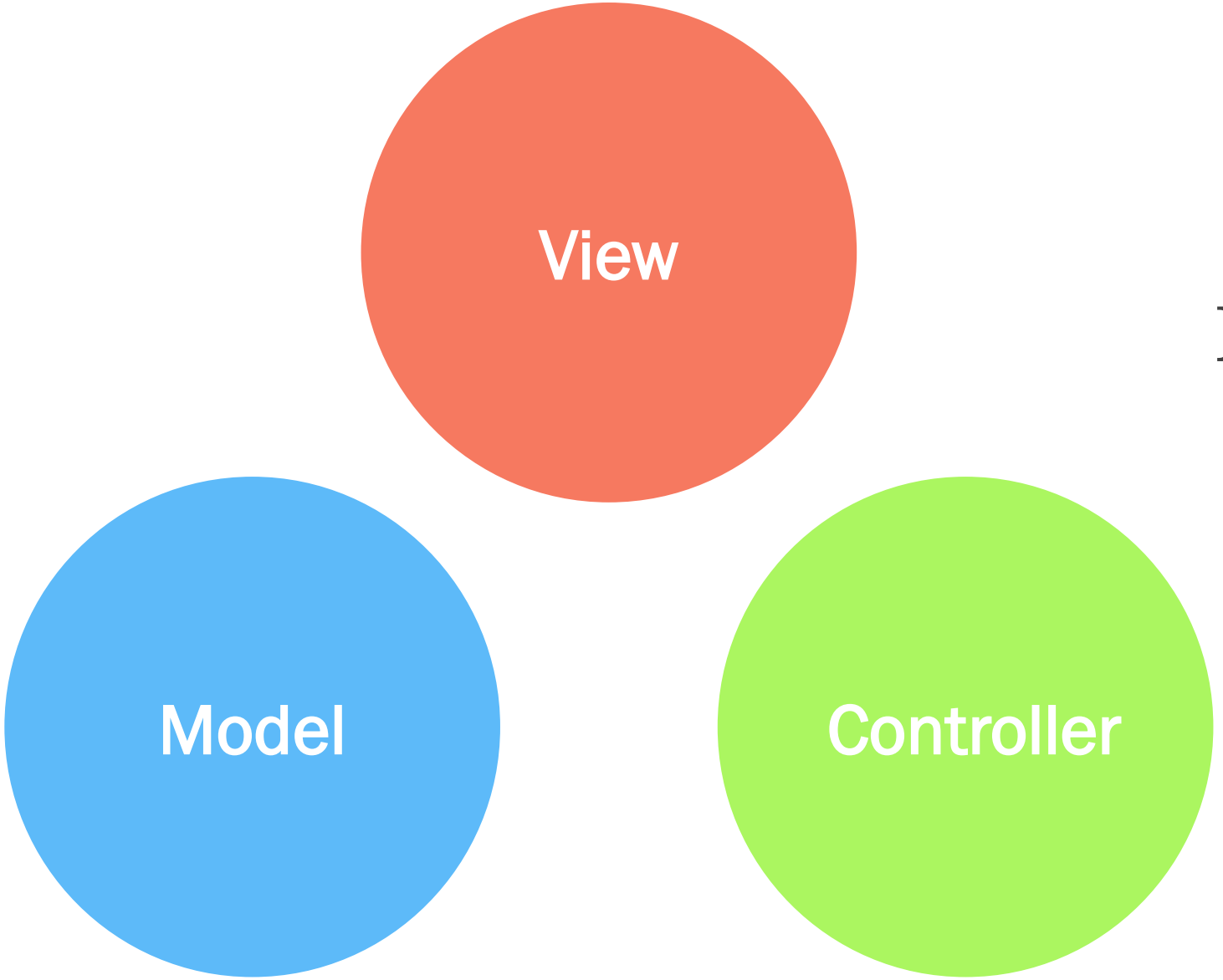
```scss
@charset "utf-8";

// config
@import "webty/variables";

// init
@import "vendor/normalize";
@import "webty/components/responsive";
@import "webty/components/reboot";

// components
@import "webty/components/btn";
@import "webty/components/font";
@import "webty/components/heading";
@import "webty/components/component";
@import "webty/components/page-nation";
@import "webty/components/spacing";
@import "webty/components/slick";

// parts
@import "webty/parts/header";
@import "webty/parts/footer";
@import "webty/parts/main-column";
@import "webty/parts/front_header";
@import "webty/parts/contact_part";
@import "webty/parts/breadcrumb";
@import "webty/parts/humburger";
@import "webty/parts/floating-btn";

// pages
@import "webty/pages/front";
@import "webty/pages/privacy";
@import "webty/pages/company";
@import "webty/pages/contact-form";
@import "webty/pages/service";
@import "webty/pages/single";
@import "webty/pages/topics";
```

- このように、部分ごとに分けたSCSSファイルをまとめることができる
- SCSSファイルを様々な要素に分けて作っておく

  → このページのCSSはどこのファイルの何行目…??? がなくなる
- ここでもコンポーネントの概念が登場している！
- SCSSの概要を知れたので、今日から君たちもSCSSマスターです。

  さっそく、使ってみましょう！

Webプログラミング ③



MVC

MVCとは

- Model – View – Controller の略称

  役割ごとにModel, View, Controllerに分割してコーディングを行うモデル

- それぞれの役割は,

  Model　　--> システムの中でビジネスロジックを担当する

  View　　--> 表示や入出力といった処理をする

  Controller --> ユーザーの入力に基づき，ModelとViewを制御する

- 簡単にいうと、プログラムの役割分担！

MVCのイメージ図

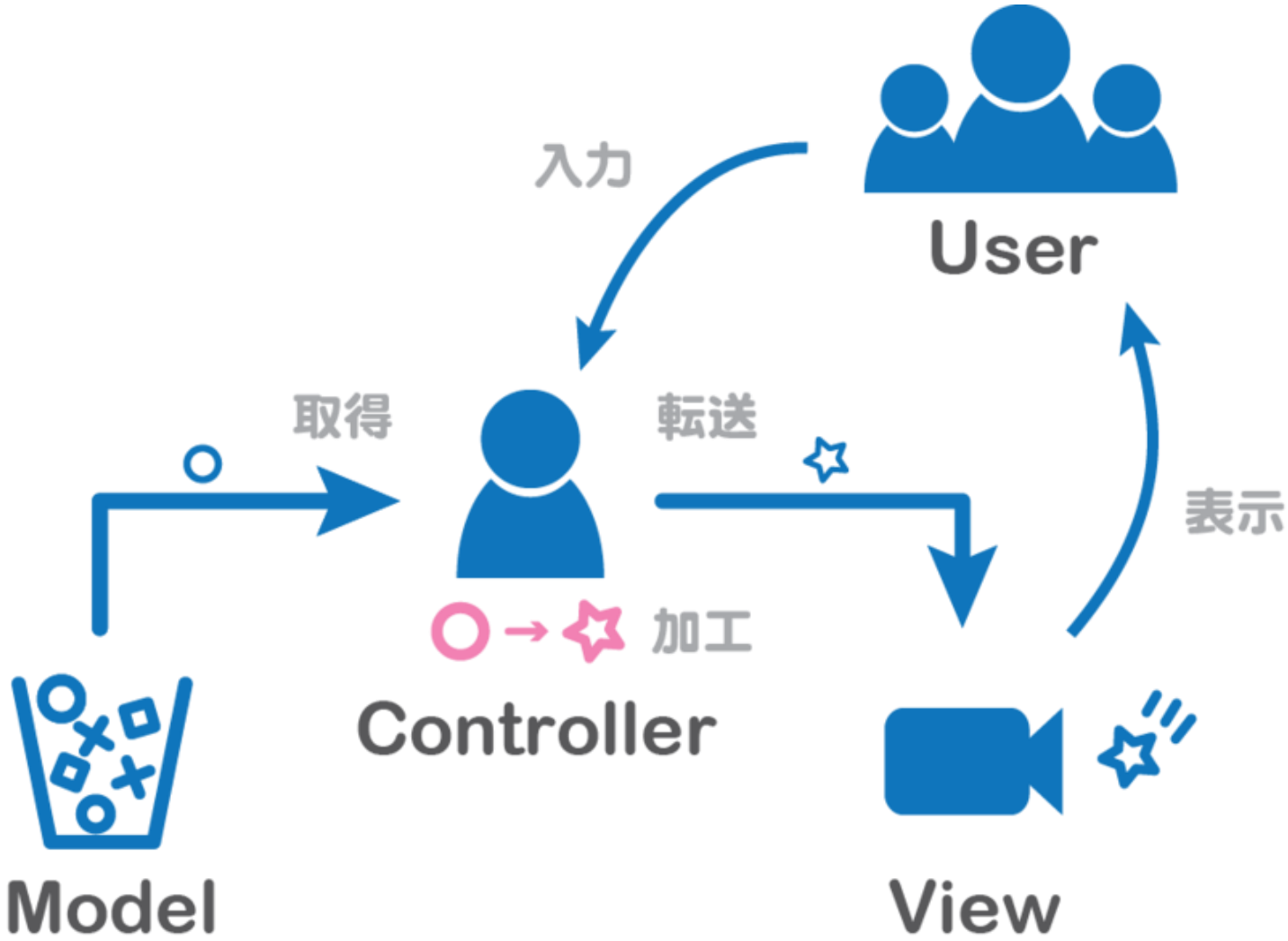
1. Userからの入力をControllerが受け取る

2. Controllerはデータ置き場であるModelからデータを取得する

3. 取得したデータをControllerが加工する

4. 加工したデータをViewに転送する

5. Viewは、受け取ったデータを視覚表現しディスプレイに表示する



なぜMVCができたか

- 最初はView, Model, Controllerもすべて1つのところで済まそうとしていた

- しかし、表示の見た目に関してはデザイナーが、
  データの処理の部分はエンジニアが担当した方がやりやすいのでViewとModelを切り離した

- Viewからの細かい指令により処理を分岐させるために、
  ViewとModelを繋ぐ橋渡し役としてControllerを切り離した

MVCを採用するメリット

- 機能毎に分割されているため，分業して作業を進めやすくなる(各人の得意な所に集中できる)

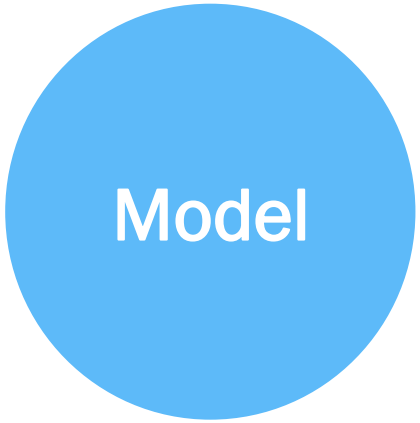
  → デザイナーの人とエンジニアの人がお互いに作業がしやすくなる

- それぞれが独立しているので変更・修正があった場合にその影響を受けにくい

- Modelにロジックを集中させることにより、コードの再利用がしやすくなる

Model

- 簡単にいうと，データベースからデータをとってくるところ ＆ それを加工するところ
- ショッピングサイトでの消費税計算や商品管理などをココで行う
- モデルにロジックを集めることで，ビューやコントローラーが変更になっても，
  ロジックは無駄にならず，他の部分に影響を与えづらい



View

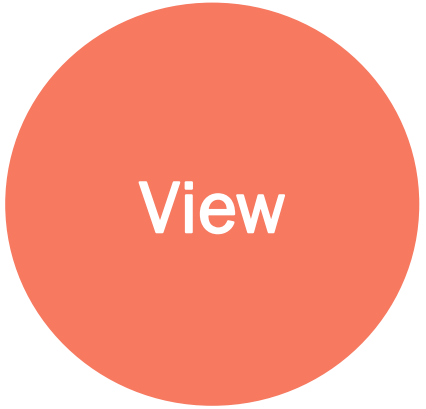
- 名前から想像できる通り，画面部分の担当

  HTMLやphpのテンプレートエンジンを使って，Controllerから渡されたデータを表示する

「カートに入れる」ボタン ← View

カートに商品が追加される ← Viewじゃない

決済 ← Viewじゃない



Controller

- Model や View を操作する指揮役

- Controller が Model にデータを渡したり，加工するやり方を教える

  → Model はデータを取ってくる ＆ 加工に専念できる

- 加工されたデータを View に受け渡す

なんとなくわかった？

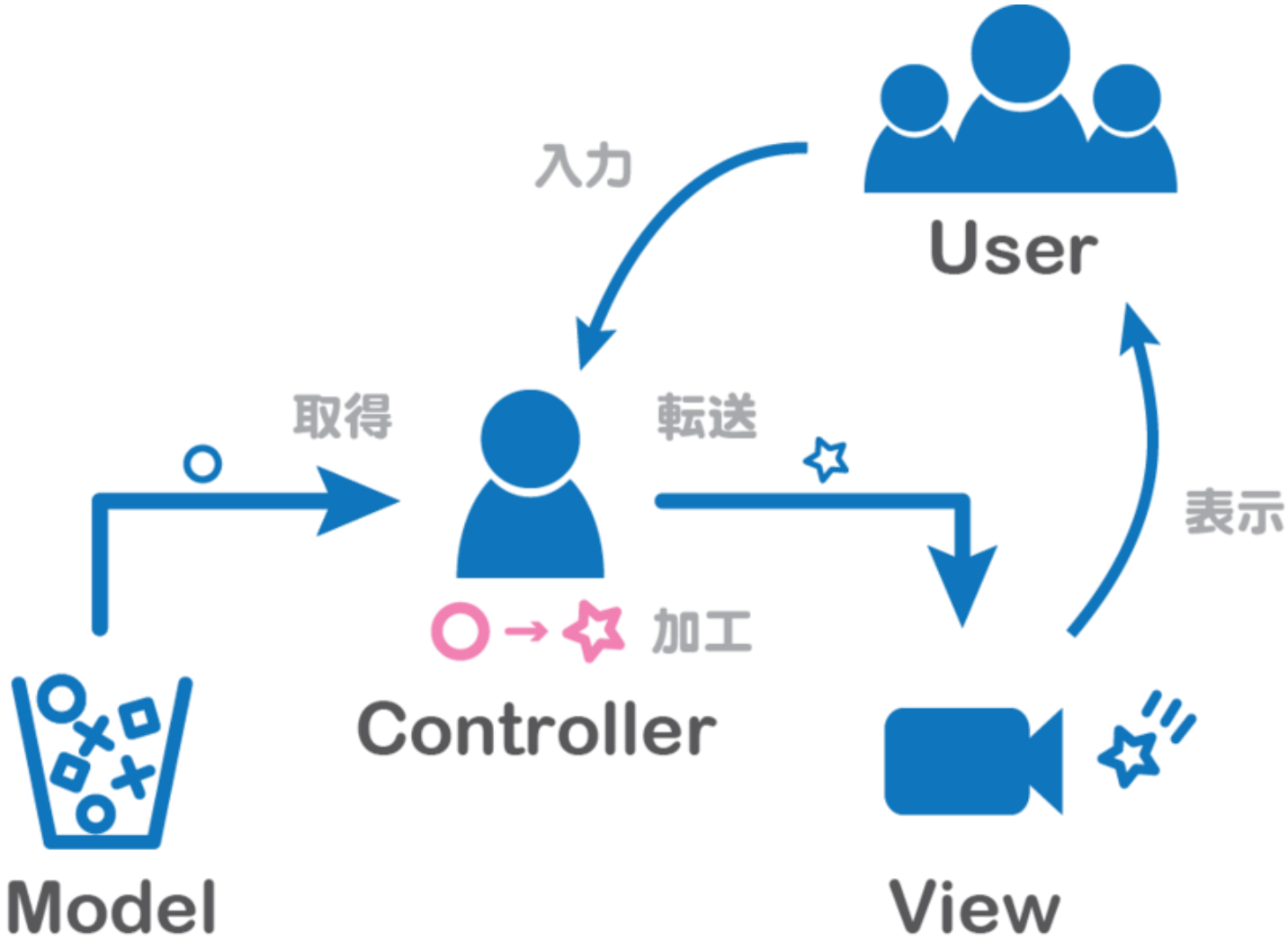
1. Userからの入力をControllerが受け取る

2. Controllerはデータ置き場であるModelから　　データを取得する

3. 取得したデータをControllerが加工する

4. 加工したデータをViewに転送する

5. Viewは、受け取ったデータを視覚表現しディスプレイに表示する



Webセキュリティ

守るべきもの

Webアプリケーションが守るべきセキュリティ

- 第三者への情報の流出を防ぐこと（機密性）
- 第三者による情報の改ざんを防ぐこと（完全性）
- 適切な権限を持った人間が適切な情報を利用できる事（可用性）

SSL

- TCP/IP上の通信を暗号化し、盗聴されても内容を分からなくするための技術
- HTTPによる通信をSSLで暗号化したものが「HTTP over SSL」 → https://~~~~~
- セキュリティの確保のためには、WebサイトのSSL化は必須！

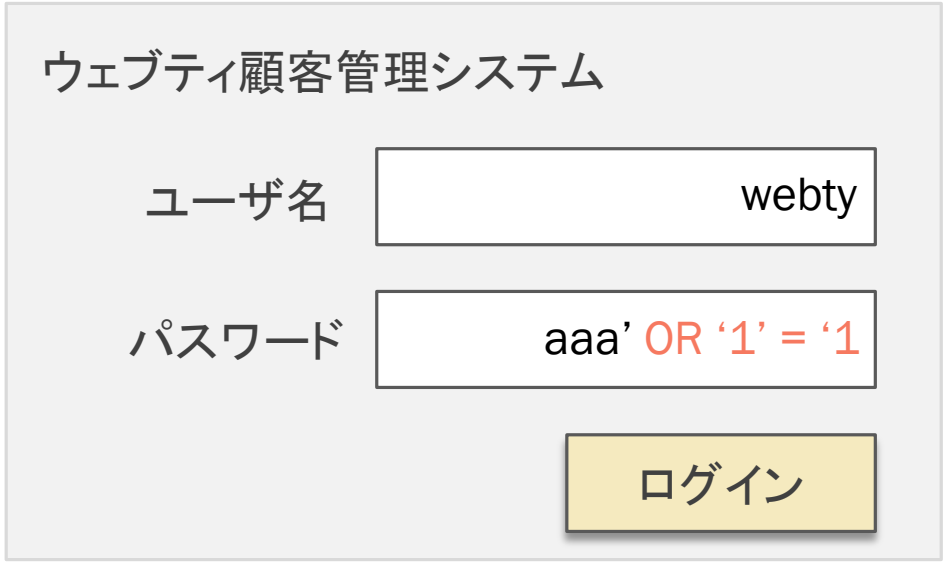
代表的な攻撃手法

以下のようなものが挙げられる

- SQLインジェクション
- XSS
- セッションハイジャック
- CSRF

SQLインジェクション

- データベースに発行されるSQLを攻撃者が書き換えて不正取得や改ざんを行う手法



“ SELECT * FROM USER WHERE USER_NAME = ‘ webty ’ AND PASSWORD = ‘ aaa ’ OR ‘1’ = ‘1’

XSS (クロスサイトスクリプティング)

「Webページにアクセスすることで不正なスクリプトが実行されてしまう脆弱性または攻撃手法」

- フォームに入力された文字列をそのまま出力するのは危険！

- 検索で「<script>alert(1);</script>」と検索するとどうなる？

  → XSS対策されていないサイトでやると，画面にアラートが出る

  これを利用して悪いことをしようというのがXSS攻撃

- https://webty.jp/staffblog/

XSSの危険性

- 悪意あるスクリプトを埋め込まれると、クッキーの盗難やページの改ざんなどができる

  → その結果、不正ログインや個人情報の流出につながる

このページは移動しました。
こちらのリンクをクリックしてください。

```
http://webty.jp/?user=<script>alert('document.cookie')</script>
```

XSS対策していないサイト

~~~.com からの通知

PHPSESSID = efaoietgiojgg

OK
~~~

対策

- htmlspecialchars関数やfilter_inputを用いて文字列をエスケープして無害なものにする

  また、HTML5ではinputにバリデーションがつけれる

- 特に素のphpで書くなら上記は必須です.

  フレームワークを使うと，独自関数でエスケープしてくれます

- https://webty.jp/staffblog/?s=XSS

除去フィルタ

- フォームからのデータをそのまま表示させる

```
$email = $_POST['email'];
echo $email;
```

- 除去フィルタを用いて、不要な文字を取り除く

```
$email = filter_input (INPUT_POST, 'email' , FILTER_SANITIZE_EMAIL);
echo $email;
```

英字、数字および
!#$%&'*+-=?^_`{|}~@.[] 以外の
すべての文字を取り除きます。

エスケープ

- 何もしない例

```
$data = ‘<script>alert(‘XSS’)</script>’;
echo $data;
```

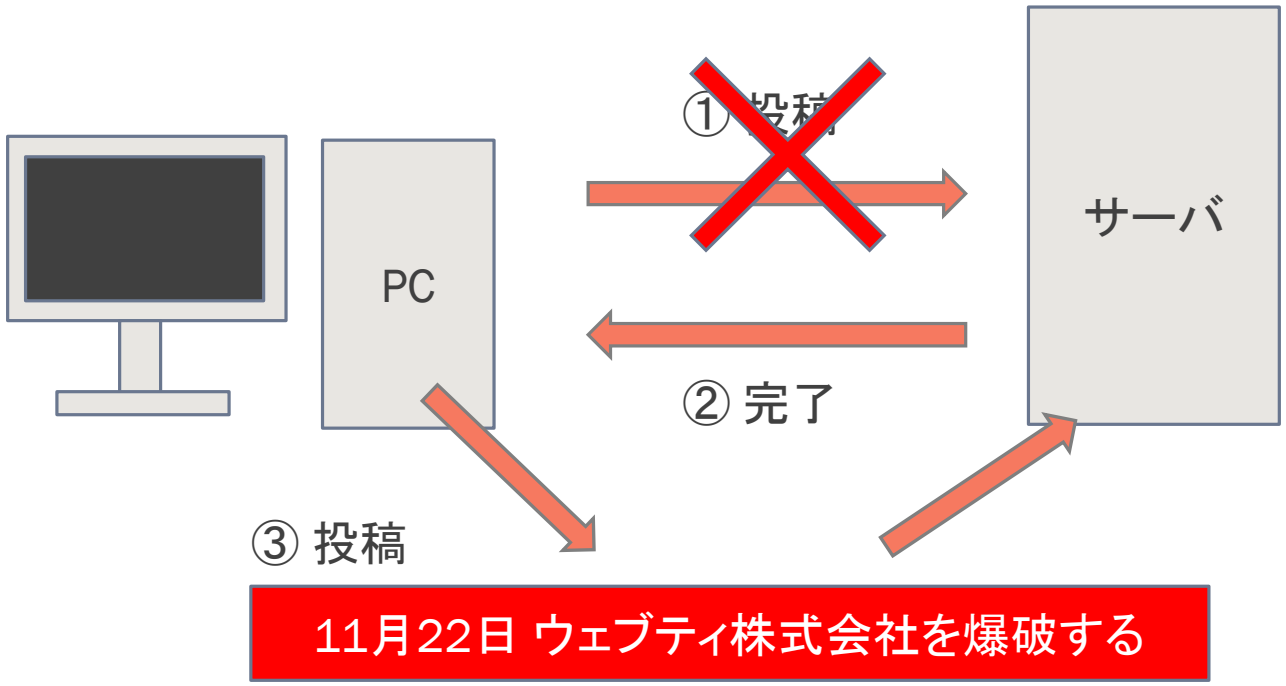
- htmlspecialchars関数を使う

```
$data = ‘<script>alert(‘XSS’)</script>’;
echo htmlspecialchars($data);
```

<script>alert(‘XSS’)</script>
と文字列が表示されるだけ

CSRF (クロスサイトリクエストフォージェリ)

「Webアプリケーション利用者自身が意図しない処理が実行されてしまう脆弱性または攻撃手法」



CSRF (クロスサイトリクエストフォージェリ)

このページは移動しました。
こちらのリンクをクリックしてください。

```
<form name=“attack” method=“POST” action=“~~~~.php”>
   <input type=“hidden” name=“title” value=“攻撃”>
   <input type=“hidden” name=“message” value=“Hacked”>
   <input type=“submit” value=“書き込み”>
</form>
```

投稿者：塚本翔 (2019-11-22 (金) 11:20:58)

こんにちは、はじめまして塚本です。
11月22日　ウェブティ株式会社を、
爆破しようと思います。

お昼頃に…

詳細記事をみてみよう

https://www.hypertextcandy.com/csrf-hands-on-tutorial

対策 (php)

- まず画面を読み込むときに特別なワンタイムトークンを発行する

  それをユーザーのセッションに入れて保管しておく

- 投稿する際にワンタイムトークンを同梱して送信する

  → サイト側は送られてきたトークンが正しいのかどうかを判定する

- 攻撃者はトークンを知らないのでこれで対策ができる

よく使うツール +

Markdown

- 文章を記述するためのマークアップ言語のひとつ

  → メールを書くような間隔で、テキストをHTML文書に変換できる！

【特徴】

- 簡単で覚えやすい記述
- 文章の構造を明示できる
- Markdownそのままでも理解できる
- 対応アプリを使うことでより快適に読み書きできる
- 拡張子は「.md」

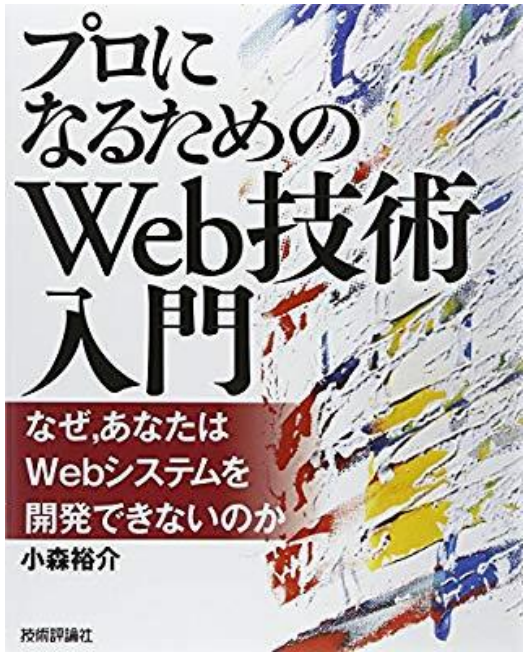
Hack MD

- Markdownで書いたドキュメントを複数人で編集でき、リアルタイムプレビューが可能なツール
- 適当に書いてもそれなりの見た目になる！
- 文法が分からなくても、入力補助やリアルタイムプレビューのおかげでわかりやすい！
- https://hackmd.io/@E3FSGXgNSOOEdV83P-euSg/HkOCRXgqr

Code Pen

- Web上で　HTML・CSS・JavaScript のコードをテストできるエディタ
- 開発中に各コンポーネントの動作をテストすることができる
- SCSSにも対応しているので、SCSSが使いたくなった方にもオススメ！
- https://codepen.io/

プレゼンの参考資料



- Quiitaの記事やGoogle先生
- 小森　裕介『**プロになるためのWeb技術入門**』 技術評論社, 2018年 (メイン)

ご清聴
ありがとうございました！

よかったらこのプレゼンを参考に
Webについて勉強してみてください。