

PHPセッション入門

Introduction to **PHP Session**



2017-12-01 ピクシブ社内勉強会

！ お前誰よ

- うさみけんた、@tadsan、Zonu.EXE
- Emacs PHP Modeメンテナ
- 省略



注意

この発表は新規のWebサイト
Webアプリケーションフレーム
ワークに依存しないPHP開
発を推奨する目的ではない

※今回ログイン
の話はしません

セツシヨシ

とは何か

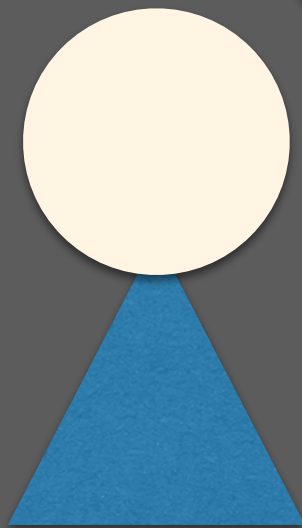
この用語(セッション)
が意味するところは
いろいろあるけど

ここではWebで、
ユーザーと継続的に
通信する機構

繼續的？

はじめて訪問したとき

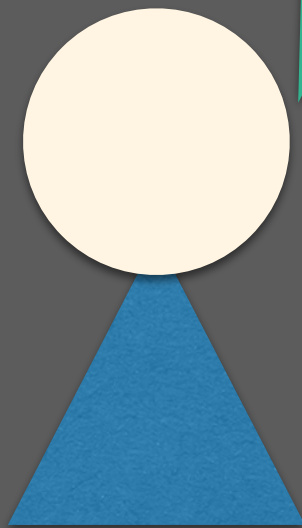
こんにちは
「ゲスト」さん！
あなたは誰ですか？



Webサイト

ここに名前をいれてね

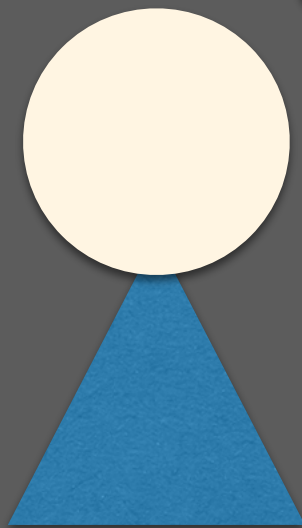
私は「tadsan」だよ



Webサイト

次に訪問したとき

こんにちは
「tadsan」さん！
また来ましたね！



Webサイト

Webブラウザでセッションを
実現するには、一般的には
Cookie(クッキー)が利用される

あとで話すよ

注意

セッションの実装は
Webサイトのプライバシー
ポリシーと密接に関連する

pixivのプライバシーポリシー

11 クッキーの使用等について

当社は、ユーザーが当社サービスを利用したりページを閲覧した際に、ユーザーのクッキー情報やユーザーが閲覧した広告・ページ、ユーザーの利用環境などの情報をユーザーのブラウザから自動的に取得し、当社のサーバーに記録いたします。この情報は個人を特定する目的はなく、サービス向上や広告配信の最適化を目的として利用されます。

TIPS

Cookieを使ったセッション
を利用するときはプライバ
シーポリシーを明記しよう

PHPで
セッション

超かんたん

| name.php

```
<?php
```

```
session_start();
```

```
// これで別ページでも session_start() すれば
```

```
// $_SESSION['name'] として参照できるようになる
```

```
$_SESSION['name'] = '太郎';
```

```
header('Location: /betsu.php');
```

| betsu.php

```
<?php session_start() ?>
```

```
<p>
```

```
こんにちは<?= htmlspecialchars($_SESSION['name']) ?>さん
```

```
</p>
```

TIPS

PHPのフレームワークはセッション機構が
いい感じに統合されてることがある。
ただし、マイクロフレームワークではオ
ミットされてることが多くPHPデフォ
ルトのセッションを気にする必要がある。

TIPS

`session_start()`および後述するセッション設定は個別のページで呼ぶのではなく、共通初期化スクリプトに記述すること

まあとりあえず
session_start()で
簡単にできる

ね、 かんたん
でしょ？

完

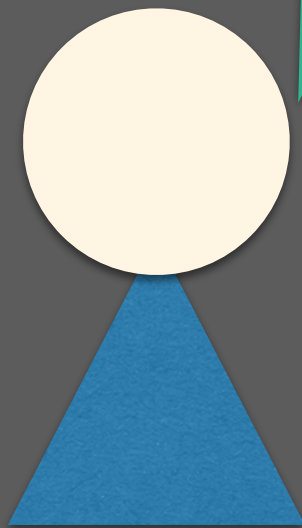


だと思っただか

どうして
セッションは
動くのか

よし、Webサイトを見よう

GET /index HTTP/1.1
Host: example.com



Webサイト

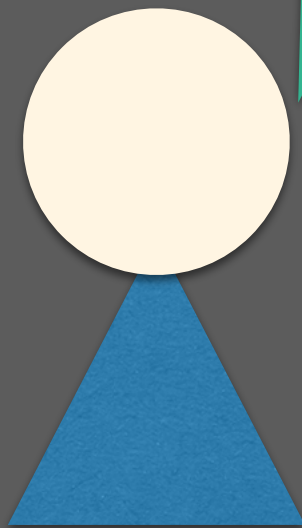
はじめて訪問したとき

GET /index.html
Host: example.com

こいつはCookie持っていないな…
ちっ、新参か。

セッションIDを発行するか

「こんにちはゲストさん」



Webサイト

はじめて訪問したとき

200 OK

Set-Cookie:

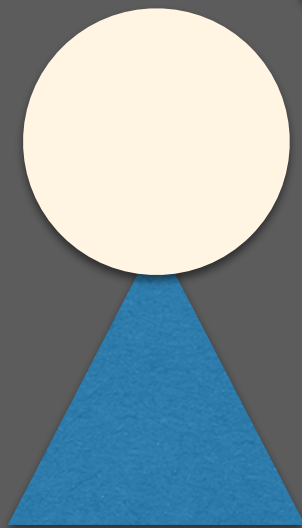
PHPSESSID=xxxxxx;expires=...

<!DOCTYPE html><html>...

っていないな...
か。

発行するか

ストさん」

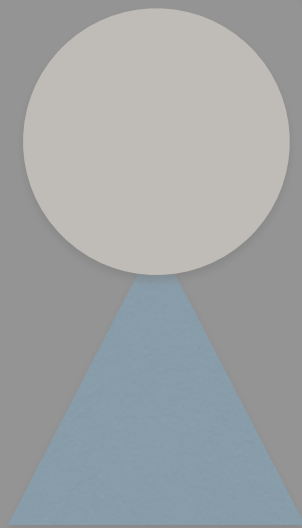


Webサイト

はじめて訪問したとき

200 OK
Set-Cookie:
PHPSESSID=x...
<!DOCTYPE html><html>...

Set-Cookie!



Webサイト

RFC 6265
HTTP State
Management Mechanism

HTTP上でWebサイトと
UA(ブラウザ)が状態を
共有するためのしくみ

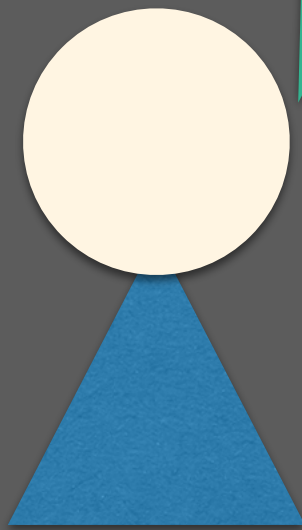
状态？

話は長くなる

Cookieに対応したユーザーエージェント(Webブラウザ)がSet-Cookieを受け取ると、次からそのサイトにリクエストするときにCookieヘッダを付加する

次回に訪問するとき

```
GET /index HTTP/1.1  
Host: example.com  
Cookie:  
PHPSESSID=xxxxxx
```

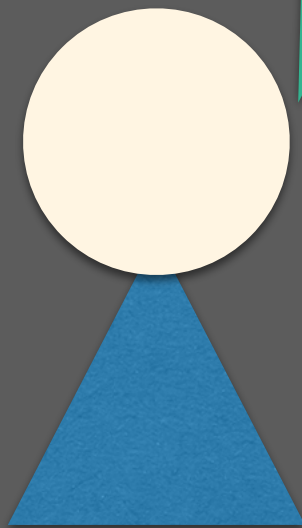


Webサイト

次回に訪問するとき

GET /index.html
Host: example.com
Cookie:
PHPSESSID=xxxxx

おっこいつは前も来たxxxxだな
「こんちわー またきたね」



Webサイト

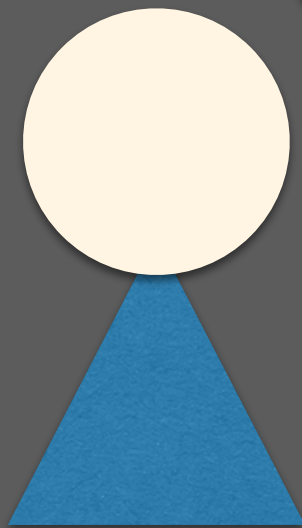
次回に訪問するとき

200 OK

<!DOCTYPE html><html>...

来たxxxxだな

たきたね」



Webサイト

どうして
セッションは
動くのか

Q. どうしてセッションは特に設定しなくても動くのはなぜ？

A.PHPはきみのことを
ファイルに保存して

覚えてるからだよ

ファイルっすか



ファイルです



`session_save_path()`
保存するディレクトリ
を設定できる

session_save_path

(PHP 4, PHP 5, PHP 7)

session_save_path — 現在のセッションデータ保存パスを取得または設定する

説明

```
string session_save_path ( [ string $path ] )
```

session_save_path() は、現在のセッションデータ保存パスを返します。

パラメータ

path

セッションデータのパス。これを指定すると、データを保存するパスが変更されます。ただしそのためには [session_start\(\)](#) がコールされる前に **session_save_path()** がコールされている必要があります。

注意:

いくつかのオペレーションシステムでは、多くの小さなファイルを効率的に処理するファイルシステム上にパスを指定することが望ましいです。例えば、Linux では ext2fs よりも reiserfs の方が性能面でより優れています。

<http://php.net/manual/ja/function.session-save-path.php>



Q. ファイルの
問題点とは何か？



A. サーバーまたいで
セッションを
共有できない！



Q.具体的に
何が起こる？

A.サーバーを増やして
分散させた瞬間に、セッ
ションが消えたりする

$/ (\wedge o \wedge) \backslash$

実用PHP セッション

本題はここから

SessionHandlerInterface

クラス概要

```
SessionHandlerInterface {  
  
    /* メソッド */  
    abstract public bool close ( void )  
    abstract public bool destroy ( string $session_id )  
    abstract public bool gc ( int $maxlifetime )  
    abstract public bool open ( string $save_path , string $session_name )  
    abstract public string read ( string $session_id )  
    abstract public bool write ( string $session_id , string $session_data )  
}
```

<http://php.net/manual/ja/class.sessionhandlerinterface.php>

これを実装して

| MySessHandler.php

```
<?php
```

```
class MySessHandler implements SessionHandlerInterface  
{  
    // 実装…  
}
```

| bootstrap.php

```
<?php
```

```
$handler = new MySessHandler();  
session_set_save_handler($handler, true);  
  
session_start();
```

登録できる

実装って何を
すればいいの？

Redis/Memcached/
SQLなどに保存する

極端な話、 データベ
ースじゃなくてもいい

例)Cookie

(セキュリティの面で
面倒なのでおすすすめはしない)

設定

デフォルト設定 の問題

デフォルトでは、Cookie
にSecure,httpOnly属性
がついてない

現代においては
ありえない

session_set_cookie_params

(PHP 4, PHP 5, PHP 7)

session_set_cookie_params — セッションクッキーパラメータを設定する

説明

```
void session_set_cookie_params ( int $lifetime [, string $path [, string $domain [, bool $secure = false [, bool $httponly = false ]]] ] )
```

ファイル `php.ini` で定義されたクッキーパラメータを設定します。この関数の効果が持続するのは、スクリプトの実行が終了するまでです。したがって、リクエスト毎や [session_start\(\)](#) がコールされる前に **session_set_cookie_params()** をコールする必要があります。

この関数は、PHP の ini 設定の値を実行時に上書きします。値の取得には [ini_get\(\)](#) が使えます。

<http://php.net/manual/ja/function.session-set-cookie-params.php>

絶対設定しよう

PHPSESSIDださい

| bootstrap.php

```
<?php
```

```
session_name('hoge_session_id');
```

```
$handler = new MySessHandler();
```

```
session_set_save_handler($handler, true);
```

```
session_start();
```

php.ini
VS
PHP関数

セッション系の設定
設定ファイル(*.ini)と
PHP両方で設定できる

環境によってphp.iniは手を入れにくいので、実行時にPHPスクリプトで設定関数を呼ぶようにする方がおすすめ

関数で書いてやれば
(同じコードである限り)
事故が起きにくい

今回しなかつ
た話

ログインの 実装方法

ログイン処理を実装するため
にはセキュリティ的に考慮す
べき事柄がいろいろあるよ

この発表の
反響があつたら
続きを書くよ！