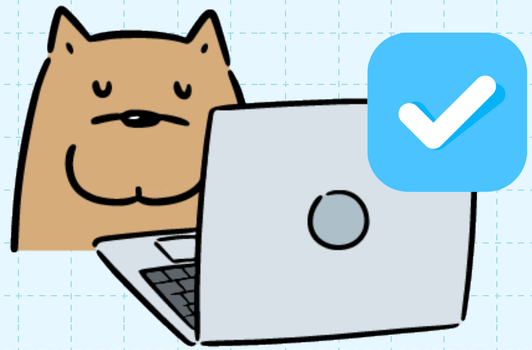
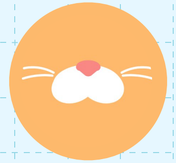
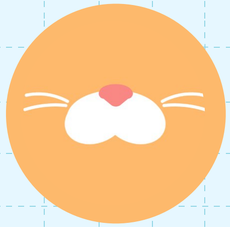


Webサービスを公開するときのチェックリスト



catnose



catnose

- デザインが好きなソフトウェア・エンジニア
- 個人でWebサービスとか作って「ワンチャン当たれば次も好きに作れる」方式で生きてる
- X は @catnose99
- いぬとねこ飼ってる

Webサービスを公開するときのチェックリスト

「同じミスは繰り返さないように…」

「明日は我が身…」

の精神で逐一メモってきたチェックリストの一部を公開します

偏りやヌケモレがいっぱいあります

あらかじめご了承ください

Webサービス公開前のチェックリスト

2024/07/04に公開 2024/07/05 5件

Web Tech

個人的に「Webサービスの公開前チェックリスト」を作っていたのですが、けっこう育ってきたので公開します。このリストは、過去に自分がミスしたときや、情報収集する中で「明日は我が身...」と思ったときなどに個人的にメモしてきたものをまとめた内容になります。

> ヌケモレや偏りがあることや、サービスの要件によって当てはまらない項目があることをあらかじめご了承ください。

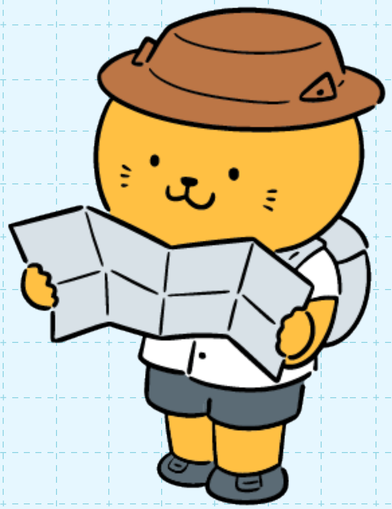
なお、この記事では各項目の解説はあまり入れていません。2024年7月10日のClassmethod Odysseyで少し詳しく話そうと思っているので、よかったら聞きにきてください。オンラインなので無料です。

catnose
フォロー
Zennを立ち上げた人

目次

その１

技術以前編



☑ サービス名が他言語でおかしな意味を持ってないこと

- 他言語圏の利用者がいる場合はとくに
- ChatGPTや wordsense.eu で調べとくと良い
- 例:「かっこいいサービスにしたい！
  よし、名前はKackerにしよう！」

Webサービスの名前を検討しています。「kacker」というサービス名は他の言語で口にしづらい意味を持ってないでしょうか？

1. **英語:**
   - 「kacker」は英語のスラングで「便秘している人」という意味に近いニュアンスがあります。このため、英語圏ではあまり好ましい印象を持たれない可能性があります。
2. **ドイツ語:**
   - ドイツ語では「kacken」という動詞が「排便する」という意味を持つため、非常に不快な印象を与える可能性があります。
3. **その他の言語:**
   - 他の多くの言語では特定の意味を持たない場合が多いですが、上記のように主要な言語でネガティブな意味を持つ場合は避ける方が無難です。

結論として、英語圏やドイツ語圏を含む国際市場での利用を考慮する場合、「kacker」という名前は避けた方が良いかもしれません。他の候補を検討することをお勧めします。

売上等の会計処理をどのようにするか
担当者と確認が取れているか

- どこが売上で何が経費になる？
  - 例えば返金が発生した場合はどう扱う？
- 経理担当者にお願いすることになるタスクは？
- 個人開発なら税理士と相談しとくと安心

後から「必要なデータが取れてない！」とならないように…

- たとえばStripeを使うならStripeに担当者を（必要最小限の）権限で招待し、会計に必要なデータが揃っているか確認しておく
- アプリケーション側で用意すべきデータがあればCSVエクスポート機能等をつけておく

☑ 法律上の懸念点がないか確認が取れているか

- 関連する法律に改正が入っていたりする
- とくに決済機能を持つ場合には要注意

  特定商取引法、インボイス制度、景品表示法、C2C決済なら資金決済法などなど…

- 個人開発でも弁護士と相談しとくと安心

クローズドチャット機能を提供する場合電気通信事業者の申請をしていること

- サービスに特定のユーザーだけが見れるチャット機能がある場合は要注意
- 参考:
  「個人開発でクローズドなチャットを作るので電気通信事業に届出」
  - https://zenn.dev/saikou_kunisaki/articles/3c39a2f83006d4

その２

セキュリティ編

認証に関わるCookieの属性 

- [x] `http-only`属性が`true`になっているか（XSS緩和策）
- [x] `same-site`属性は`Lax`か`Strict`か（CSRF対策等）

  Originヘッダの値を検証する対策等も合わせて検討したい

  参考: 令和時代の API 実装のベースプラクティスと CSRF 対策 | blog.jxck.io
- [x] `secure`属性が`true`になっているか（中間者攻撃対策）

  HTTPS通信でのみCookieが送られるようにする

認証に関わるCookieの属性 🍪

☑ domain属性が適切に設定されているか

- Cookieがサブドメインにも送られる設定の場合
  別サイトに脆弱性があるとインシデントに繋がるかも
- Set-CookieでDomain属性を空にするとそのドメイン
  にのみ送られるように
- Cookie名の接頭辞を__Host-とするとDomain属性が
  空になっていないCookieの指定を無視してくれる

ユーザーの入力値のバリデーション

- [x] バリデーションがクライアント側だけでなく
サーバー側でも行われているか
- [x] URLのバリデーションを忘れていないか
  プロトコル部分の検証を忘れがち。javascript:から始まる
  URLを許可してしまっていないか
- [x] SQLインジェクションが可能になっていないか

ユーザーの入力値のバリデーション

- [x] ユーザーの入力値をそのままHTMLとして表示していないか

  innerHtmlやdangerouslySetInnerHtml（React）により埋め込まれる文字列をユーザーが自由に指定できるようになっていないか

ユーザーの入力値のバリデーション

- [x] 正規表現のバリデーションがバイパスできるようになっていないか

  例: 文頭や末尾のチェック漏れなど

  参考: 正規表現でのURLのチェックとバイパス | mbsd.jp

ユーザーがURLに含まれるハンドルネーム等を指定できる場合そのバリデーションは十分か

https://x.com/username のような構造の場合は要注意

- 他ページのURLと被らないようになっているか

  例: /about や /admin など
  「reserved username」で検索すると良いかも

- フレームワークやホスティングサービスにより使われるURLもあるので注意…

  例: /404 や /_ah など

データの更新

- [x] 更新・削除を未認証もしくは権限を持たないユーザーができるようになっていないか

  改ざん可能なパラメータを信頼して本人確認をしてしまっていないか（例: userIdを他人の値に変えても更新できてしまう）

- [x] SQLのDELETEやUPDATE文でWHEREが適切に設定されているか

  例: とあるUserのPostsを一括更新するつもりがwhere句が適切に設定されておらず全Postsが更新されてしまう

その他セキュリティ系

- [x] 退会/メアド変更などの重要な操作は直前のログインを必須にしているか（XSS緩和策）
- [x] ユーザーにより内容が変わるレスポンスがCDN等にキャッシュされていないか
- [x] オブジェクトストレージのディレクトリページのが意図せず公開されていないか

参考: Cloud Storageでファイルは公開＆一覧ページは非公開にする - catnose

その他セキュリティ系

- [x] クライアントで指定されたURLにバリデーション無で
リダイレクトしていないか（オープンリダイレクト対策）

  例: https://example.com/login?redirect_to=https://evil.example
  のようにクエリ文字列で渡されたURLにそのまま遷移してしまう

- [x] ユーザーから渡された文字列をそのまま
レスポンスヘッダに含めてしまっていないか

  レスポンスヘッダが改ざんされてしまう可能性

その他セキュリティ系

- [x] ファイルアップロードのバリデーションは十分か
  画像の形式のバリデーションは行われているか

  例: 悪意のあるスクリプトを含むSVGをアップロードできてしまう等
  特にアップロードファイルのURLとアプリケーション本体のURL
  が同一ドメイン/サブドメインの場合は要注意

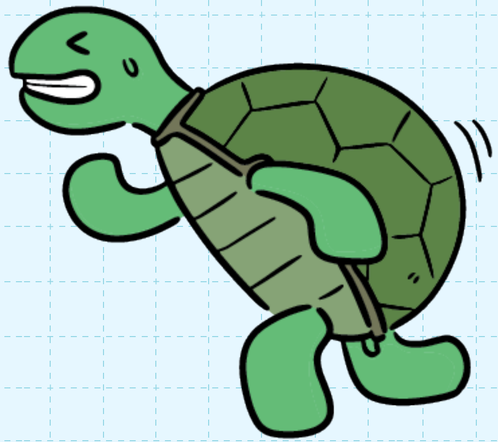
各種サービスの設定も確認しておきたい

- [x] DBの自動バックアップは有効になっているか
- [x] オブジェクトストレージもバックアップしているか
- [x] クラウドサービスには二要素認証を設定しているか
- [x] 余計な権限が付与されていないか

リリース後は使われてなさそうなIAMロールも消すのがこわい

その3

メール配信編



- [x] ユーザーの入力値がメールに含まれる仕様の場合その入力を悪用してスパムメールが送られないか

  例: ユーザー名やアイテムのタイトル等の文字列をうまく設定すれば宣伝やスパム的な内容のメールにできてしまう

- [x] 1ユーザーの操作によりに不特定多数に繰り返しメールが送られないか

  例: フォロー機能で1万人をフォローすると1万人に通知メールが送られてしまう

- [x] SPF / DKIM / DMARC 関連の設定ができているか
- [x] ログイン不要の購読解除リンクは設置されているか

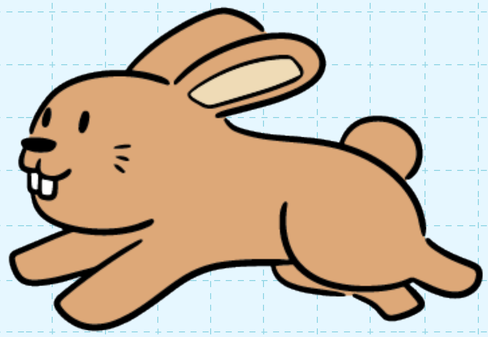
  大人数にメルマガを送るサービスの場合、 RFC8058に則った1クリック購読解除に対応しているか（Gmailの規制に関わる）

  参考: メール送信者のガイドライン
- [x] 連続でメール配信タスクが呼び出されたときに同一のメールが二度送信されてしまわないか
- [x] 退会したユーザーにメールが送られてしまわないか

休憩用スライド

その4

パフォーマンス編



- [x] パフォーマンスが重要なページで余計な
再レンダリングが発生していないか

  ※ Reactなどのフロントエンドフレームワークの話

- [x] 余計なパッケージがクライアントに配信される
JavaScriptにバンドルされてしまっていないか

  bundle analyzerなどを使ってチェックする

- [x] 巨大な画像がそのまま読み込まれていないか

  例: 幅400pxで埋め込まれている画像が実は1MBもあった

- [x] **静的ファイルがCDNにキャッシュされているか**

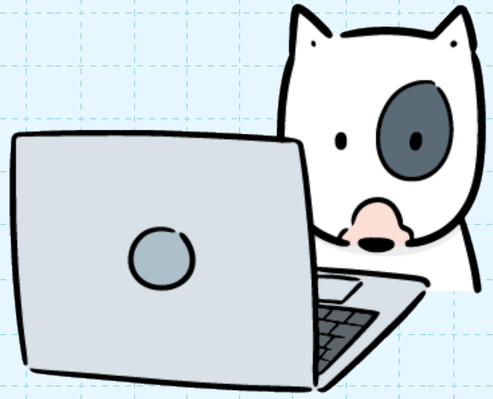
  Next.jsなどのフレームワークではJSやCSS等の大量の静的ファイルにリクエストが飛ぶ。これら全てがオリジンサーバーから返されないようにしておきたい

- [x] **画像によるレイアウトシフトが起きないか**

  widthとheightもしくはaspect-ratioを指定

その5

その他もろもろ編



SEO対策

- [x] 全ページでtitleタグが適切に指定されているか
- [x] エラー関連のページのステータスコードが40x もしくは50xになっているか

メンテナンス中に404になっていたらGoogleが
このページは削除されたのだと認識してしまう可能性
メンテナンス中は503を返すのが良い

SEO対策

- [x] 検索結果ページにnoindexもしくはcanonical URLが設定されていること

  検索キーワードがそのまま<title>に指定される仕様だと
  検索結果におかしなタイトルでインデックスされてしまうかも

- [x] 動的に検索結果にインデックスされて欲しいページが生成されるサービスの場合、XMLサイトマップを用意し、Search Consoleに登録していること

複数環境での動作確認

- [x] スマホで見たときにUIが崩れないか（ありがち）
- [x] ハンドルネームなどのユーザーの入力値が長いときに見た目が崩れないか（ありがち）
- [x] 主要ブラウザで動作確認したか
- [x] Cookieをオフにして動作確認したか

複数環境での動作確認

- [x] Macで開発しているなら「スクロールバーを常にON」にして表示をチェックしたか
- [x] 各OSで見たときにフォントがおかしくないか

その他

- [x] ローカルストレージやhttp-onlyでないCookie等が7日後に消えても問題ないか

  最近のiOS Safariでは、ブラウザ上のJavaScriptから保存されたCookieやローカルストレージの内容は7日以上ユーザーが触らないと削除されるって知ってました？

- [x] 3rd Party Cookieに依存した実装になっていないか

その他

- [x] robots.txtが配置されているか
  - クローラーへの指示等。記載することがなければなくてもいい
- [x] 日本語サイトの場合<html lang="ja">になっているか
  - 各フレームワーク、デフォルトで lang="en" がち
- [x] サーバーエラーが発生したときにエラーの内容が通知 or 検知できるようになっているか

その他

- [x] 実行されまくるとヤバい処理には
  レートリミットが設定されているか
  特にAI系のAPIを叩くサービスだと気を付けたい。
- [x] 404ページ/50xページは悪くない感じになっているか
  404の場合はトップページなどに戻る導線が表示されていると親切
- [x] Dependabotは有効になっているか/設定されているか

その他

- [x] ファビコンが設定されているか（意外と忘れがち）
- [x] apple-touch-icon は設置されているか
  iOS Safariがこのファイルを求めてめっちゃリクエストしてくる
- [x] OGPの設定はされているか
- [x] Google Analytics やCloudflare Web Analytics 等のアクセス解析ツールは導入したか（必要な場合に限る）

他にもいろいろあるけど
今日はここまで

ありがとうございました