ServiceWorkerは SameOriginを超えられるのか

結論

キャッシュには入れられる
キャッシュの内容には触れられない

ServiceWorkerではなくFetch APIの領域

Fetch API

- ServiceWorker内ではfetchやnew Requestを使用
- modeを指定する事で"same-origin", "no-cors" , "cors" を選べる
- "no-cors"を指定するとsame-originを無視してデータを取れる

```
fetch("http://example.com/", { mode: 'no-cors' });
// サーバ側でCORS未対応でもデータを取得出来る
// 返されるデータはopaque filtered responseとなる
```

'opaque' filtered response?

- same-originを無視して取得したデータをそのまま見れるのはまずい
- typeがopaqueとなり、statusが0、bodyがnullとフィルターされる
- エラーレスポンスと区別がつかないようなデータ
- キャッシュとしては使える(内部のみ)、APIとしては触れないデータ

結論

- SameOriginを無視して取得は出来る
  - 画像等のキャッシュのため
- それをユーザーレベルで扱う方法はない
  - セキュリティ的に色々壊れてしまうので
- ServiceWorker + XSS によって脅威が増えるかは課題