**１．同一オリジンポリシーとは**

**（１）定義**

同一オリジンポリシーとは、Webブラウザが異なるオリジン（Origin）間でのアクセスを制限する仕組みです。

これは 「ブラウザ側で強制されるセキュリティモデル」 の一つで、悪意あるサイトが別サイトの機密情報を盗むことを防ぐ目的で導入されました。

**２．オリジン（Origin）の構成要素**

オリジンは以下の３要素で決まります。

|  |  |
| --- | --- |
| **要素** | **例** |
| スキーム（protocol） | http / https / file |
| ホスト名（host） | [www.example.com](https://www.example.com) |
| ポート番号（port） | 80, 443, 8080など |

**同一オリジンの条件：**

* スキーム・ホスト名・ポート番号の全てが一致すること

**例：**

https://example.com:443 と https://example.com は同一オリジン（省略時のポートはデフォルト443） https://example.com と http://example.com は異なるオリジン（スキームが違う）

**３．同一オリジンポリシーの対象範囲**

SOPはすべてのブラウザリソースに一律適用されるわけではありません。リソース種類ごとに制限内容が異なります。

**（１）JavaScriptによるDOMアクセス**

制限が最も厳しい分野です。 異なるオリジンの iframe 内のDOMには直接アクセスできません。

**例：**

example.com 上のページが、evil.com の iframe 内テキストを .contentWindow.document で読む → 禁止

**（２）Cookie・LocalStorage・IndexedDB**

同一オリジンでのみ共有可能です。 例外的にサブドメイン間共有は Domain 属性設定で可能です（例：sessionidをexample.com全体で共有）。

**（３）XMLHttpRequest / fetch（AJAX通信）**

デフォルトでは同一オリジンのみ通信可能です。 異なるオリジンと通信する場合はCORS設定が必要です。

**（４）画像・スクリプト・CSSの読み込み**

読み込み自体は異なるオリジンから可能です（CDN利用など）。 ただし、JavaScriptでピクセルデータを取得（Canvas API）する場合はクロスオリジン制約があります。

**４．例外と緩和策**

同一オリジンポリシーは厳格ですが、Webの利便性のために例外・緩和策が存在します。

|  |  |
| --- | --- |
| **緩和策** | **目的・特徴** |
| CORS（Cross-Origin Resource Sharing） | サーバーが Access-Control-Allow-Origin ヘッダで許可するオリジンを明示 |
| postMessage API | 異なるオリジン間で安全にメッセージをやり取り（iframe間通信） |
| JSONP（古い） | <script> タグでスクリプトとして取得し、コールバック関数でデータ受け取り |
| サーバーサイドプロキシ | 同一オリジン内サーバーが外部リソースを取得して返却 |

**５．同一オリジンポリシーが必要な理由**

もし同一オリジンポリシーが無ければ、以下のような攻撃が可能になります。

* **CSRF（クロスサイトリクエストフォージェリ）強化版**：悪意あるサイトから利用者がログイン中の別サイトへ勝手にデータ送信
* **機密情報の窃取**：他オリジンのDOMから直接ユーザー情報やトークンを読み取る
* **セッションハイジャック**：Cookieを盗み取り別人になりすます

**６．用語の由来**

**Origin**：英語で「起源・発端」。Webでは「通信の出発点＝スキーム＋ホスト＋ポート」を意味します。 **Same-Origin Policy**：直訳すると「同一の起源ポリシー」。

要するに「同じ出発点からのリソースは自由にやりとりしてよいが、違う出発点とは制限する」というルールです。

**７．関連技術との位置付け**

Webブラウザのセキュリティモデル

├─ 同一オリジンポリシー（SOP）

│ ├─ DOMアクセス制限

│ ├─ Cookie/Storage制限

│ ├─ AJAX通信制限

│ └─ Canvas画像データ制限

├─ CORS（SOPの例外許可）

├─ サンドボックス（iframeの隔離）

└─ コンテンツセキュリティポリシー（CSP）

はい、承知いたしました。ご提示いただいた優れた枠組みはそのままに、各項目の解説を、ウェブ開発初心者の方でもイメージしやすいように、比喩や具体例を交えて加筆・修正します。

---