用 JavaScript 透過 fetch API 或 XMLHttpRequest 等方式發起 request，必須遵守同源政策 (same-origin policy)。

簡單地說，用 JavaScript 存取資源時，如果是同源的情況下，存取不會受到限制，然而，在同源政策下，非同源的 request 則會因為安全性的考量受到限制。瀏覽器會強制你遵守 CORS (Cross-Origin Resource Sharing，跨域資源存取) 的規範，否則瀏覽器會讓 request 失敗。

什麼是同源?

1. 相同的通訊協定 (protocol)，即 http/https
2. 相同的網域 (domain)
3. 相同的通訊埠 (port)

舉例：下列何者與 https://example.com/a.html 為同源？

- https://example.com/b.html (○)
- http://example.com/c.html (✕，不同 protocol)
- https://subdomain.example.com/d.html (✕，不同 domain)
- https://example.com:8080/e.html (✕，不同 port)

CORS (Cross-Origin Resource Sharing) 是針對不同源的請求而定的規範，透過 JavaScript 存取非同源資源時，server 必須明確告知瀏覽器允許何種請求，只有 server 允許的請求能夠被瀏覽器實際發送，否則會失敗。

哪些請求會使用 CORS？

- 使用 XMLHttpRequest 或 Fetch API 進行跨站請求，如前所述。
- 網頁字體（跨網域 CSS 的 @font-face 的字體用途），所以伺服器可以佈署 TrueType 字體，並限制只讓信任的網站跨站載入。
- WebGL 紋理 (en-US)。
- 以 drawImage (en-US) 繪製到 Canvas 畫布上的圖形／影片之影格。
- CSS 樣式表（讓 CSSOM (en-US) 存取）。
- 指令碼（for unmuted exceptions）。

簡單請求

所謂的「簡單請求（simple requests）」——其滿足以下所有條件：

- 僅允許下列 HTTP 方法：
  - GET
  - HEAD (en-US)
  - POST
- 除了 user agent 自動設定的標頭（例如 Connection、User-Agent，或是任何請求規範〔Fetch spec〕中定義的「禁止使用的標頭名稱〔forbidden header name〕」中的標頭）之外，僅可手動設定這些於請求規格（Fetch spec）中定義為「CORS 安全列表請求標頭（CORS-safelisted request-header）」的標頭，它們為：
  - Accept
  - Accept-Language (en-US)
  - Content-Language (en-US)
  - Content-Type（但請注意下方的額外要求）
  - Last-Event-ID
  - DPR
  - Save-Data
  - Viewport-Width

        - Width
- 僅允許以下 Content-Type 標頭值：
        - application/x-www-form-urlencoded
        - multipart/form-data
        - text/plain
- 沒有事件監聽器被註冊到任何用來發出請求的 XMLHttpRequestUpload 物件（經由 XMLHttpRequest.upload (en-US) 屬性取得）上。
- 請求中沒有 ReadableStream (en-US) 物件被用於上傳。

預檢請求

滿足以下**任一項條件**時會發出預檢請求：

- **假如**請求方法為以下其中之一：
        - PUT (en-US)
        - DELETE (en-US)
        - CONNECT
        - OPTIONS (en-US)
        - TRACE (en-US)
        - PATCH (en-US)
- **或是假如**除了 user agent 自動設定的標頭（例如 Connection、User-Agent，或是任何請求規範〔Fetch spec〕中定義的「禁止使用的標頭名稱〔forbidden header name〕」中的標頭）之外，請求中包含了任何除了這些於請求規格（Fetch spec）中定義為「CORS 安全列表請求標頭（CORS-safelisted request-header）」以外的標頭，具體如下：
        - Accept
        - Accept-Language (en-US)
        - Content-Language (en-US)
        - Content-Type（但請注意下方的額外要求）
        - Last-Event-ID
        - DPR
        - Save-Data
        - Viewport-Width
        - Width
- **或是假如** Content-Type 標頭有除了下方所列出以外的值：
        - application/x-www-form-urlencoded
        - multipart/form-data
        - text/plain
- **或是假如**一或多個事件監聽器被註冊到一個用來發出請求的 XMLHttpRequestUpload 物件上。
- **或是假如**請求中有一個 ReadableStream (en-US) 物件被於上傳。

附帶身分驗證的請求

XMLHttpRequest 或 Fetch 在 CORS 中最有趣的功能為傳送基於 HTTP cookies 和 HTTP 認證（Authentication）資訊的「身分驗證（credentialed）」請求。預設情況下，在跨站 XMLHttpRequest 或 Fetch 呼叫時，瀏覽器**不會**送出身分驗證。必須要於 XMLHttpRequest 物件中或是在呼叫 Request (en-US) 建構式時設置一個特定的旗標。

身分驗證請求與萬用字元

在回應一個身分驗證請求時，伺服器**必須**於 Access-Control-Allow-Origin 標頭值中指定一個來源，而不是使用「*」萬用字元（wildcard）。