

跨源資源共享（**Cs-Origin Resource Sharing CORS**）是一種使用額外的 **HTTP** 頭令當前瀏覽網站的用戶代理（**en-US**）標明訪問其他（網域）服務器資源權限的機制當一個用戶不是當前文件來源（例如來自於（域名）、跨不同時網端口（跨端口協議）請求）的來源——例如建立一個來源（域名）或通訊的 **HTTP**（跨端口）的資源請求）。

舉個跨來源的例子：<http://domain-a.com>HTML 頁面裡面有一個<img>請求標籤的 **src** 屬性（**en-US**）來自 <http://domain-b.com/image.jpg> 的圖片。當前網路頁面所加載的資源，如 **CSS** 樣式表、圖片圖片、以及指令碼（**script**）都來自與所在位置分開的網域，如內容傳遞網路（**content delivery networks**，**CDN**）。

基於代表性安全考量，程序所發出的跨源 **HTTP** 碼請求會受到限制。例如，**XMLHttpRequest** 及 **Fetch** 都遵循這同源政策（同源策略）。網路應用程序所使用的 **API** 使用 **CORS** 標頭，否則請求與應用程序相同的網域只是 **HTTP** 資源。

跨源資源共享（**Cross-Origin Resource Sharing**，簡稱 **CORS**）機制提供了網頁服務器跨網域的訪問控制，增加了跨網路數據傳輸的安全性。現代瀏覽器在 **API** 容器（如 **XMLHttpRequest** 或支持 **Fetch**）中使用 **CORS** 以降低跨源 **HTTP** 請求的風險。

來源資源使用標準的准許方式是通過新增的 **HTTP** 標頭讓服務器以提供能力瀏覽器來訪問的 **GET**。或用於某些 **MI** 類型的 **POST** 方法），規範要求瀏覽器必須請求“預檢”（**preflight**）請求，以之 **HTTP** 的 **OPTIONS (en-US)**方法從服務器獲得其支持的方法。當設備許可後，再發送 **HTTP** 請求方法送出具體的請求。服務器也可以通知客戶端是否需要安全性資料（包括 **Cookies** 和 **HTTP** 認證（**Authentication**））一併隨送出。

們將在此展示內容中，提供不同來源的說明，用於使用不同的資源進行選擇。所有的翻譯都 **XMLHttpRequest** 支持 **XMLHttpRequest** 的瀏覽器可以讓任何跨站請求。

本節的 **JavaScript** 程序（以及處理跨站請求的服務器端設備運行實體）可以在 <http://arunranga.com/examples/access-control/>查看，並可以運行在跨站 **XMLHttpRequest** 請求的瀏覽器上。

對於服務器端的跨資源共享討論（參考包含 **PHP** 範例）可服務器端訪問控制。

其他送出“簡單請求”的例子，“預置請求”的例子，“預置請求”請求請求會發送到另一個網域，確認實際（實際）請求是否可以安全發出，以跨站請求可能會攜帶用戶資料，所以要先進行預檢請求。

準確地說，如果滿足以下任一條件時會發出預檢請求：

某些請求方法為以下其中之一：

**PUT**（英文）

刪除 (en-US)

**CONNECT**

選項（英文）

**TRACE**（英文）

補丁（英文）

某些除了用戶代理自動設置的標頭（例如 **Connection**、**User-Agent** 或任何請求規範[獲取規範]中定義的“禁止使用的標頭名稱[禁止標頭名稱]”中的標頭）之外，包含了這些除了在任何請求規格（**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**

接受語言 (en-US)

內容語言（en-US）

**Content-Type**（但請注意下面的額外要求）

**Last-Event-ID**

**DPR**

**Save-Data**

**Viewport-Width**

**Width**

**Content-Type** 市場上的一些標有除名以外的其他頭值：

**application/x-www-form-urlencoded**

**multipart/form-data**

**text/plain**

某個或多個事件監聽器被註冊到一個發出請求的 **XMLHttpRequestUpload** 物件上。

某某請求有一個 **ReadableStream (en-US)**物件被上傳。