CORS 心得

因為安全性的考量，瀏覽器預設都會限制網頁做跨網域的連線。但如果要提供資料存取的服務給其它人使用，就必須要開放對應的 API 給其它人連線。而 CORS 就是一個瀏覽器做跨網域連線的時要遵守的規範。

CORS(跨來源資源共用（Cross-Origin Resource Sharing）) 是一種使用額外 HTTP 標頭令目前瀏覽網站的使用者代理 (en-US)取得存取其他來源（網域）伺服器特定資源權限的機制。當使用者代理請求一個不是目前文件來源，例如來自於不同網域（domain）、通訊協定（protocol）或通訊埠（port）的資源時，會建立一個跨來源 HTTP 請求（cross-origin HTTP request）。假如用 JavaScript 透過 fetch API 或 XMLHttpRequest 等方式發起 request，必須遵守同源政策，而非同源的 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。其中要符合同源的條件為:

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)

在 CORS 的規範裡面，跨來源請求有分兩種：「簡單」的請求和非「簡單」的請求。

一、簡單請求，必須符合下面兩個條件：

1. 只能是 HTTP GET, POST or HEAD 方法
2. 自訂的 request header 只能是 Accept、Accept-Language、Content-Language 或 Content-Type。

其中瀏覽器發送跨來源請求時，會帶一個 Origin header，表示這個請求的來源。Origin 包含通訊協定、網域和通訊埠三個部分。當 server 端收到這個跨來源請求時，它可以依據「請求的來源」，亦即 Origin 的值，決定是否要允許這個跨來源請求。如果 server 允許這個跨來源請求，它可以「授權」給這個來源的 JavaScript 存取這個資源。

二、非簡單的跨來源請求，例如：HTTP PUT/DELETE 方法，或是 Content-Type: application/json 等，瀏覽器在發送請求之前會先發送一個 「preflight request（預檢請求）」，其作用在於先問伺服器：你是否允許這樣的請求？真的允許的話，我才會把請求完整地送過去。

預檢請求(preflight request) 是一個 http OPTIONS 方法，會帶有兩個 request header：Access-Control-Request-Method 和 Access-Control-Request-Headers。

所以這個 CORS 的規範就有點像我們日常生活中的智慧財產權。網站就好比我們的作品，而 CORS 的規範就像我們去跟原作者申請這個財產的動作。只是一個是隨便盜用的話有可能會觸及法律，另一個則是網路中的規範，沒照

CORS 規範的動作去存取資料的話頂多無法讀取使用他人網站的資源。
參考資料: https://developer.mozilla.org/zh-TW/docs/Web/HTTP/CORS
https://shubo.io/what-is-cors/