# CORS 心得報告

看完這篇文章，讓我了解了什麼是 CORS，以及他的功能等等。我認為 CORS 是一個瀏覽器要做跨網域連線時，要遵守的規範。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。

CORS 是一種稱為跨來源資源共用（Cross-Origin Resource Sharing (CORS)）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）。因此，當我們在 JavaScript 中透過 fetch 或 XMLHttpRequest 存取資源時，需要遵守 CORS (Cross-Origin Resource Sharing，跨來源資源共用)。瀏覽器在發送請求之前會先發送 preflight request (預檢請求)，確認伺服器端設定正確的 Access-Control-Allow-Methods、Access-Control-Allow-Headers 及 Access-Control-Allow-Origin 等 header，才會實際發送請求。使用 cookie 的情況下還需額外設定 Access-Control-Allow-Credentials header。而且用 JavaScript 透過 fetch API 或 XMLHttpRequest 等方式發起 request，還必須遵守同源政策 (same-origin policy)。而什麼是同源政策呢?簡單地說，是用 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。因此，所謂的同源，必須滿足以下三個條件: 相同的通訊協定 (protocol)、相同的網域 (domain)、相同的通訊埠 (port)，不是同源的情況下，就會產生一個跨來源 http 請求（cross-origin http request），而這個時候就產生了一個跨來源請求。而跨來源請求必須遵守 CORS 的規範。當伺服器沒有正確設定時，請求就會因為違反 CORS 失敗，所以簡單地說，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。

舉個跨來源請求的例子：http://domain-a.com HTML 頁面裡面一個 <img> 標籤的 src 屬性 (en-US)載入自 http://domainb.com/image.jpg 的圖片。現今網路上許多頁面所載入的資源，如 CSS 樣式表、圖片影像、以及指令碼（script）都來自與所在位置分離的網域，如內容傳遞網路（content delivery networks, CDN）。基於安全性考量，程式碼所發出的跨來源 HTTP 請求會受到限制。例如，XMLHttpRequest 及 Fetch 都遵守同源政策（same-origin policy）。這代表網路應用程式所使用的 API 除非使用 CORS 標頭，否則只能請求與應用程式相同網域的 HTTP 資源。跨來源資源共用（Cross-

Origin Resource Sharing，簡稱 CORS）機制提供了網頁伺服器跨網域的存取控制，增加跨網域資料傳輸的安全性。現代瀏覽器支援在 API 容器（如 XMLHttpRequest 或 Fetch）中使用 CORS 以降低跨來源 HTTP 請求的風險。

而 CORS 的功能是可以讓跨來源資源共用標準的運作方式是藉由加入新的 HTTP 標頭讓伺服器能夠描述來源資訊以提供予瀏覽器讀取。另外，針對會造成副作用的 HTTP 請求方法（特別是 GET 以外的 HTTP 方法，或搭配某些 MIME types 的 POST 方法），規範要求瀏覽器必須要請求傳送「預檢（preflight）」請求，以 HTTP 的 OPTIONS (en-US) 方法之請求從伺服器取得其支援的方法。當伺服器許可後，再傳送 HTTP 請求方法送出實際的請求。伺服器也可以通知客戶端是否要連同安全性資料（包括 Cookies 和 HTTP 認證（Authentication）資料）一併隨請求送出。所以有了 CORS，讓我可以透過 HTTP header 的設定，可以規範瀏覽器在進行跨網域連線時可以存取的資料權限與範圍，包括哪些來源可以存取，讓瀏覽器和伺服器 知道他們必須互相溝通，進行資料交換。