

http cookie

Cookie 是現在瀏覽網頁時非常常出現的東西。每次瀏覽網頁時都會有一個訊息跳出來「是否同意使用 **cookie**」。會有 **Cookie** 的出現是因為原本的 **http** 其實是無狀態的特性。**HTTP** 的無狀態特性會造成許多使用上的麻煩。像是每次登入需要重複輸入帳號密碼，瀏覽過任何東西後關掉再開啟就需要完全重新查詢沒有任何紀錄。因為這個無狀態的特性，造成使用者在使用網頁時需要做很多重複的事情。又或者是說假設在購買網站上會無法紀錄你之前選擇甚麼東西放入購物車中造成後續麻煩。因此才有了 **Cookie** 的發展。

Cookie 有幾個特性。第一、可以記錄使用者訊息。第二、儲存在客戶端。第三、連線時會自動帶上，但過多的 **cookie** 可能會浪費流量、或是帶上無用的 **cookie**。第四、大小限制 4kb 左右。第五、能夠設置過期的時間。第六、專屬於某個網域(路徑)，也就是不同的網域不能共用相同 **cookie** 內容。**Cookie** 主要用於三個目的。第一、**Session** 管理。這是讓伺服器可以記錄該記住的資訊。第二、個人化。紀錄使用者的設定、主題等等。第三、追蹤。紀錄並分析使用者行為。

Cookie 又分為第一方 **Cookie** 和第三方 **Cookie**。第一方 **Cookie** 是由使用者存取網站隸屬的網域所發行的 **Cookie**。第一方不可以跨網域使用，主要用在記錄限定於該存取網站之內的瀏覽紀錄等資訊、保持登入狀態等用途。因此如果不允許這類型的 **Cookie** 使用，可能會造成瀏覽網站時有些功能無法正常使用。第三方 **Cookie** 是由不屬於使用者存取網站隸屬的網域所發行的 **Cookie**。第三方 **Cookie** 會跨網域獲取使用者的瀏覽紀錄資訊，並用來發布使用者可能關注的廣告。

Cookie 是一種讓網路瀏覽更流暢方便的機制。使用 **Cookie** 能夠免去每次都要經常存取的會員網站輸入登入資訊的麻煩，也因為會有紀錄，更容易找到使用者想要搜尋的資訊。由此可以知道 **Cookie** 的存在可以造成使用者方便，但也會無意中透漏許多使用者的資訊，造成安全問題。**Cookie** 的安全問題也是大家需要關注的一個重點。

想要保護自己網路隱私可以選擇不使用 **cookie** 或是禁止使用第三方 **cookie**。直接選擇不使用 **cookie** 可能會造成上面有提到的瀏覽網頁時發生問題(些許網站功能會被限制)。第三方 **cookie** 是最大的隱私隱患。因為這些 **cookie** 並不來自於你正在訪問的網頁。因此可以從瀏覽器設定上去調整 **cookie** 使用設定，設定僅阻止第三方 **cookie**。這樣不但可以保持原本網頁的功能，還可以阻止將數據發送給第三方。