Cookie 通常存於瀏覽器中，並隨著請求被放在 Cookie HTTP 標頭內，傳給同個伺服器，讓瀏覽更順暢的關鍵，因為 HTTP 協定是狀態的，需藉由 cookie 記錄使用者在瀏覽器上的一些行為，當使用者再次造訪相同網站時，伺服器會傳送給使用者的瀏覽器一個小片段資料，方便使用者回到上次瀏覽的狀態，像是在網路購物上，記錄使用者的購物車資訊，以及自動登入功能、個人化設定、記錄分析使用者行為等，都是 cookie 的實際應用。

Cookie 專屬於某網域，可以紀錄使用者訊息，大小限制 4kb 左右並儲存在客戶端，連線時會自動帶上，能夠設置過期時間，但過多的 cookie 可能會浪費流量。因為 cookie 是儲存於用戶端，所以需要搭配使用 session，來驗證身分。

收到一個 HTTP 請求時，伺服器可以傳送一個 Set-Cookie 的標頭和回應。Cookie 設定：*Set-Cookie: <cookie-name>=<cookie-value>*，告訴客戶端要儲存一個 cookie ，現在隨著每個請求，瀏覽器會使用 Cookie 標頭將所有先前儲存的 cookies 傳給伺服器。如果沒有設定一個特定日期(Expires)為 session cookie，當客戶端關閉時即被刪除，因為它並沒有註明日期(Expires)或可維持的最大時間(Max-Age)。但網頁瀏覽器可以使用 session restoring，讓 session cookies 永久保存。常駐 cookies 不會在客戶關閉後到期，而是在一個特定的日期 (Expires) 或一個標明的時間長度 (Max-Age)，當到期日被設定後，時間與日期即為相對於用戶端設定 cookie 的時間，而非伺服器。

JavaScript 可以用 document.cookie 來查看、設置、刪除 cookie，cookie 是 key=value 的形式，想要設置 cookie 就用 document.cookie = “user-name=;expires=;path=;” 的形式，去設定使用者、日期及路徑。此外，還可以設置 Secure cookie，只有在以加密的請求透過 HTTPS 協議時，傳送給伺服器。為了避免跨站腳本攻擊，Cookie 中的 HttpOnly 屬性，能藉由防止透過 JavaScript 取得 cookie 內容。

Cookie 依據網域的所有權分為一方（First-party）Cookie 以及第三方（Third-party）Cookie 兩種。第一方 Cookie 是由使用者瀏覽的網站所建立，也就是網址列中所顯示的網站，不可以跨網域使用，主要用於記錄使用者的資訊及登錄狀況等，讓瀏覽體驗更方便。通常會在剛進入網站時詢問是否同意使用 Cookie，若不同意可能會讓網站無法正常運作。第三方 Cookie 則是在造訪的網站上來自其他網站的廣告，是由其他網站建立，提供能跨網域存取的暫存資料。因此對於使用者來說，接受第一方 Cookie，授權給信任網站，不僅能提升瀏覽體驗，而第三方 Cookie 則會比較難掌握來源網站的安全性。

參考資料：https://developer.mozilla.org/zh-TW/docs/Web/HTTP/Cookies
https://ithelp.ithome.com.tw/articles/10203123
https://blog.trendmicro.com.tw/?p=63387