Cookie 是一種保存狀態的機制，也是我們開發 Web 應用程式經常要面對的事，關於 HTTP 本身無狀態（Stateless）的特性，要在網路上識別瀏覽者的身份，必須透過一些機制來保存狀態，此時就會用到 Cookie。

Cookie 的運作是 Server 端回應給 Browser 一個或多個 "Set-Cookie" HTTP Header，然後 Client 端（Browser）接收到 Set-Cookie 指令時，會將 Cookie 的名稱與值儲存在 Browser 的 Cookie 存放區，並記錄該 Cookie 隸屬的網域、網址路徑、過期時間、是否為安全連線。當 Browser 再次發出 HTTP Request 指令到 Server 時，就會比對目前在 Browser 內的 Cookie 存放區有沒有「該網域」、「該目錄」、「過期時間尚未過期」且「是否為安全連線」的 Cookie，如果有的話就會包含在 HTTP Request 指令的 "Cookie" Header 中。

假設 Browser 在取得一張網頁時如果裡面包含 20 張圖、3 個 CSS、2 個 JavaScript 檔的話，同樣一份 Cookie 就會送出 25 次到 Server 端，如果你 Cookie 的大小有 4K 的話，光是看一張網頁你可能就要從你的電腦發送出 100KB 的頻寬，且可能只有一張網頁用的到這個 Cookie 而已。 所以使用 Cookie 並非「多多益善」，而是要「小心使用」，否則光是 Cookie 就會讓你的網頁顯示的時間變慢。

由於 Cookie 是儲存在 Client 端，所以一些比較機密的資料不建議存放在 Cookie 中，例如有套軟體 IECookiesView 就可以輕易的將一台電腦中的所有 Cookie 取出，如果你的 Cookie 中有帳號、密碼、身份證字號等資料，那就真的全都露出來了，如果真的要放也要加密過後再放比較安全。

通常 Cookie 有兩種類型 Persistent Cookie 與 Session Cookie，Persistent Cookie 這種類型的 Cookie 可以設定存在 Browser 一段時間（明確指定 Cookie 的 Expires 時間），如果你設定的時間夠長（例如：一天），即便 Browser 全部關閉或重開機後再開啟也還會存在。而 Session Cookie 這種類型的 Cookie 是當不特別指定 Expires（過期時間）時，該 Cookie 只會存在目前這個 Browser 的續存期間(Session)，只要 Browser 全部關閉後 Cookie 會自動被清除。

大部分的 User Agent（瀏覽器）都有定義 Cookie 的最低儲存量，但是每一個 Browser 在實做的時候還是有其限制，大多 Browser 都僅實做最低的儲存量，因為使用過多的 Cookie 會消耗頻寬，反而沒有效率，在 RFC 上面的定義是至少可以儲存 300 個 Cookies、每個 Cookie 所儲存的值至少可以儲存 4096 位元組(4KB)及每個網域(domain name)至少可以儲存 20 個 Cookies。當你設定 Cookie 的大小超出限制，瀏覽器就會丟棄整個 Cookie，而不是將你設定的值取

可以儲存的部分。