108 年 3 月公務機密暨機關安全維護宣導電子報

--機關安全維護--

定期檢查滅火器 災時應變好幫手

鑑於 107 年 1 月 7 日晚間 7 時許，臺北市永吉路一間店面鐵捲門馬達起火，旁邊店面民眾，隨手拿起路旁滅火器滅火，因該滅火器為 69 年 12 月製造之加壓式乾粉滅火器、未定期檢查及底部嚴重鏽蝕(如圖 1)，肇致放射時滅火器底座爆裂，造成額頭及左胸受傷。

圖 1：滅火器底部嚴重鏽蝕

內政部消防署提醒您，滅火器為火災初期時常見的滅火設備之一，因其設計簡單可攜，一般人亦能使用來撲滅剛發生的小火，為確保滅火器為合格品及其功能隨時保持堪用，得就下列幾點簡單判定之，如有損壞或不堪用情形，應請滅火器廠商立即回收或更新，避免有無法使用或無法耐壓爆裂之情事：

一、滅火器本體是否貼有內政部委託之檢驗機構實施型式認可及個別認可合格之標示(如圖 2)。

二、滅火器是否每 3 年委請滅火器藥劑更換及充填廠商實施定期檢查，確認功能正常，並於本體上貼有標示(如圖 3，並請特別注意下次性能檢查日期未逾期)及瓶頸加裝檢修環(如圖 4，檢修環顏色為黃色及藍色交替更換)。

三、滅火器本體及裝置外觀上有無變形、腐蝕、損傷、老化及壓力應在綠色範圍(如圖 5)。

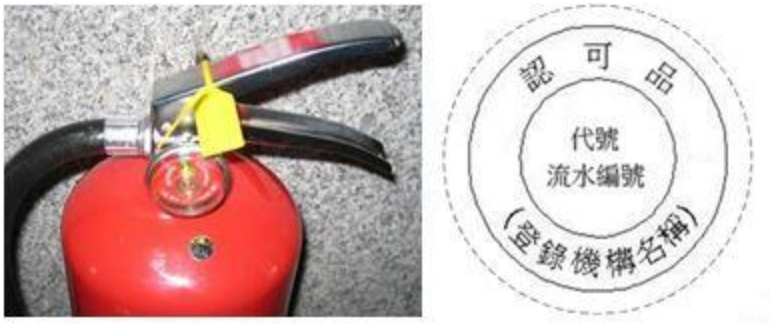

圖 2：合格標示

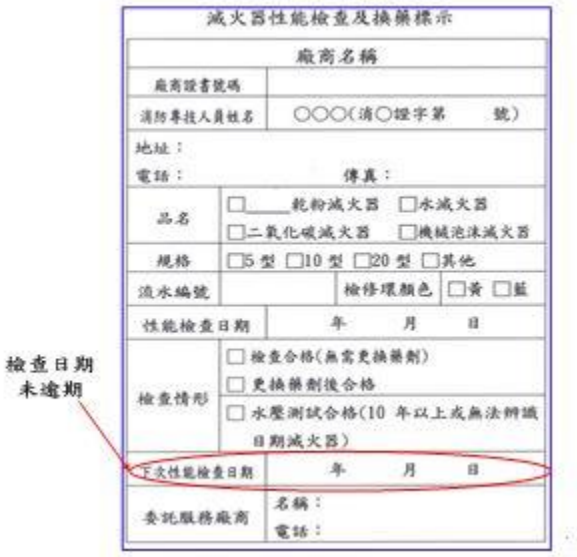

圖 3：注意滅火器性能檢查及換藥標示，檢查日期有無逾期

圖 4：滅火器加裝檢修環，兩色輪替提醒

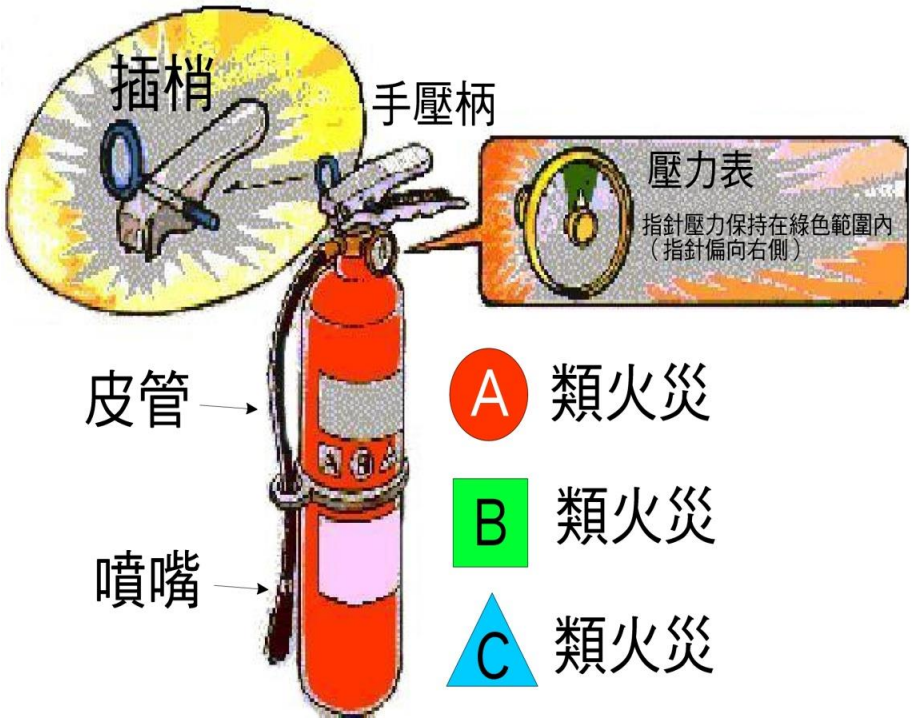

圖 5：滅火器壓力表應在綠色範圍

內政部消防署再次提醒您，使用滅火器時請熟記 4 字訣：「拉-拉插梢、瞄-瞄準火源底部、壓-壓握把、掃-向火源左右掃射」(如圖 6)。

圖 6：滅火器使用方法（圖片來源#新北市政府消防局

資料來源：內政部消防署

--公務機密維護宣導—

資訊安全的四項提「防」

隨著電腦應用的普及和網際網路的急遽發展，不僅改變了人類的生活模式，也帶來令人憂慮的資訊安全問題。因此，建立完善的資訊安全防護措施已是當務之急，唯有在安全無慮的前提下享用網路資訊帶來的便利，才是面對科技發展的正確態度。

資訊安全的種類可分為三個面向：

一、硬體的安全，包含對於硬體環境的掌握以及設備管理；

二、軟體的安全，包含資料軟體安全和通訊管道的安全性；

三、個資的安全，包含個人資料保密，隱私性等。

如何做到上述資訊安全的保護措施呢？首先我們要了解影響資訊安全的因素，包括：未經授權侵入使用者帳戶，進行竊取或是更動系統設定；資料在傳輸過程中被擷取，或被變更內容；透過感染電腦病毒與傳播惡意程式。諸如此類的資訊安全問題層出不窮，且手法日新月異，然而注意下面幾點防護措施，可在面對大部分的狀況時，具備基礎的防護手段。

一、防毒：當一隻病毒被製造出來之後，開始於電腦與網路設備中擴散，透過網絡無遠弗屆的傳遞，變成所有電腦使用者的夢魘，隨之而來的系統崩潰甚至硬體損壞，將損毀寶貴的資料。使用者防治的積極手段就是安裝來源合法的防毒軟體，並且定時更新病毒碼，以保持作業系統處於健全的防護程度。

二、防駭：隨著社群網絡和各式資訊系統的應用，駭客由開始時半開玩笑地更動系統設定，演變到後來的蓄意破壞、資

料竊取，也因此發展出了各式的系統安全通行證，包含使用者密碼、身分驗證、通訊鎖、晶片卡等設置，普遍使用於各層面。除了定期變更驗證方式以及使用多種防護作為外，也需隨時保持資安的警覺性。

三、防治天災：這是容易忽略的一個項目，電腦硬體從來就屬於耗損型的設備，隨著時間、溫度、濕度、跳電等，甚至震動都可能導致硬體的受損；因此使用者應該以嚴肅的態度準備更完整的防治計畫，例如定期更新易耗損的硬體設備，備份重要資料，以及安裝備用電源，預防斷電造成的資料損失等。

四、資料防竊：隨著智慧型手機的流行，現在低頭族已成為一種社會現象。而資訊的氾濫成為眾多使用者頭痛的問題，許多不同的應用程式都會記錄使用者的個人資訊，但設計這些應用程式的公司是否確實做好保護我們的個人資料？值得存疑！許多應用程式的分享與協同編輯功能權限設置不明，更是成為資料安全上的一大隱憂。因此，我們對於自身的資料處理應該抱著更謹慎的態度，切勿在網路上分享或是儲放機密資料。我們若能認真地思考資安問題，完善規劃這些資訊系統與網路設備，定期保養與維護個人資安，便可長保資料的可用性及可靠性了。

資料來源：法務部調查局