安全維護常識彙編（96 年 4 月份）

❋從危機管理談保防工作

一、前言

動員戡亂時期結束後，兩岸在經貿、文化或是學術交流皆蓬勃發展，敵我意識也日益淡薄，然而在風平浪靜的表象下，兩岸真是一點危機也沒有嗎？這其實是國人感受不到「立即而明顯的危機」所致。孟子云「生於憂患、死於安樂」，隨著知識之提昇與傳播科技之日新月異，人民獲得國家安全資訊機率大增，當我們失去應有的警覺心時，一旦危機降臨，難保「特洛伊木馬屠城」悲劇不會重演，與其在發生重大危安事件時，再來採取「亡羊補牢」措施，甚或懊惱追悔，不如在事件伊始，以「防微杜漸」的心態加以面對，畢竟事後的檢討、究責都已經於事無補。因此，先知先制的預防工作乃是保防工作的重點。

當今國內政治生態丕變，兩岸在加入 WTO 國際組織後交往越來越密切，國家安全工作也必然面臨新的挑戰與衝擊。不確定的年代中，任何事都有可能發生，因此當危機來臨時，危機的預防、危機的處理及危機的事後檢討及改進皆與保防工作息息相關，本文將藉由「危機管理」來探討保防工作的核心價值。

二、危機及保防的意義

危機一詞在字典上詮釋為「轉機與惡化的分水嶺」，亦即當面臨世局及社會的動盪，處變及應變能力將是成功與失敗的關鍵點。危機管理是一種針對危機情境所做的管理措施及因應策略。共可分為三個階段：危機預防、危機處理、復原。危機預防就是預測危機的發展，以期及早消滅於無形之中，分析可能導致危機的各

種情況，將發現之潛藏危機，立即加以化解處理或嚴加防範，進而研擬各種應變計畫，以備不時之需。

保防一詞在字典上詮釋為「保守秘密，防範間諜」。其內涵就在於確保國家安全，預防犯罪。保防對國家而言，就是一種自衛能力，有了充分的自衛能力，就不怕外來各項衝擊與挑戰。保防落實在工作上，範圍則包括「機密保護」、「防制滲透」、「安全防護」、「保防教育」等四大工作主軸。

三、從危機管理看保防工作

危機管理大致分成危機預防、危機處理、復原等三個階段，恰好與保防工作不謀而合。掌握機先預警，爭取最先黃金五分鐘，貫徹任務全程，堅持最後五分鐘。

保防工作就是國家安全的重要防線，因此我們該如何加強呢？在機密保護方面，近來兩岸交流頻繁，國內各類科技研發單位與大陸科技單位互相參訪、座談演講，因而導致國內科技產業機密外洩及安全維護的問題受到重視，而在危機預防觀念中，當我們發現危機之所在，就要盡力去防杜，除了加強公務人員及專業情治人員養成保密的基本素養外，對廣大的民眾亦應加強宣導，讓全民一心，方可確保國家安全與利益。

在防制滲透方面，兩岸頻繁的交流讓我們漸漸失去戒心，藉由通婚、學術交流、經濟交流等名義，敵人隨時有可能潛伏在你我身邊，預防之計就是培養高度的警覺心，注意是否有任何違反常理的作為，明辨敵我，這才是身為現代公民應具備之素養。

在安全防護方面，美國九一一事件震撼了全球，更讓我們深刻了解到舉凡各項重要設施、人員、物資、器材都應該受到嚴密的保

護，因為一旦遭受損害，將對我方產生重大不利之影響。而安全防護工作，著重於防患未然及應變措施，不僅事先加強計畫檢查，產生危安預警機制，更要擬定應變措施，做到有備無患。

至於保防教育，更是危機預防的的第一線防衛，由於日益頻繁的交流讓人民漸漸失去「保密防諜」的警覺性，甚至開始質疑保防工作是否有存在的必要性，此乃對保防工作抱持錯誤的認知，認為保防工作僅是少數保防工作人員的工作，目的在於思想控制、找人麻煩、打小報告，因而對保防工作產生排斥的偏差觀念。

事實上，保防工作乃是國家安全防護網中重要的一環，也是世界各國為維護其國家安全必有之作為。此外，不僅國家重視保防工作，許多私人企業為維護企業安全、防止商業間諜滲透、竊取商業機密，亦多設有安全部門，所職掌的業務又何嘗不是「保防」呢？由此可見，保防工作無論對國家或是私人企業的整體安全皆有其存在之必要性。因而政府應宣導保防的觀念於無形之中，除了導正錯誤觀念外，更讓廣大的民眾了解保防的真諦，讓保防深植於人心，建立全面性的安全網，如此國家必將富強康盛而安全無虞。

四、結論

「歷史的教訓就是永遠不知記取歷史的教訓」，這句話在在告誡我們健忘可能帶來的災禍，綜觀兩岸現況及島內情勢，表面上似乎相安無事，事實上，中共謀我之心卻未曾稍歇，不論是軍事恫嚇、外交打壓，亦或是滲透統戰、分化離間等各種手段，均無所不用其極。因此，我們除要具有敵諜無所不在的憂患意識，更要

有充分的警覺性，如此方能讓敵諜「進不來、藏不住、動不了、逃不掉」，這就是全民保防的真諦。

此外，在國會監督、媒體關注及網路資訊無國界之下，沒有一項公務運作能永保秘密，面對透明化、公開化，仍要兼顧安全工作力求萬全之任務需求，保防工作更需要所有國民深刻體認、共同參與，進而提昇使命感，我們須知國家安全與百姓福祉息息相關，保防工作除了靠專業情治單位戮力以赴之外，全民積極參與深刻體認才是面對兩岸特殊情勢應有之作為。當全民的危機處理觀念能與保防工作融合為一，保防工作危安預警功能也就能充分發揮，國家安全自可確保。（本文摘自於月刊月刊作者/陳瑩璇）

❊婦女人身安全工作艱難—婦團期待支持力量

日前「捷運雙狼」等性侵案件發生後，婦女人身安全的議題再度受到重視；現代婦女基金會表示，隨著嫌犯被捕後，話題告一段落，相關議題很可能再度邊緣化，然而，致力婦女安全工作相當艱辛、漫長，希望社會大眾以行動或捐款來支持她們的努力。

現代婦女基金會表示，這些經披露的案件只是冰山一角，根據基金會的統計資料顯示，去年度通報的性侵害案件高達六千多件，但沒有出面通報的黑數可能有七到十倍之多；也就是可能有六萬多件性侵害案發生，其中卻只有三千多件報案、一千六百件被起訴，最後只有六百多件的性侵害加害人入監服刑。

現代婦女基金會指出，被害人創傷的巨大，鮮少被媒體及社會大眾關注，在二十年來服務的經驗中，許多被害人要花十年以上的歲月才能稍稍平復。

基金會舉例，有的被害人自此不敢顯露女性特質，怕再招致其他的傷害；有的被害人長期昏睡，逃避令她恐懼的世界；有的被害人出現暴飲暴食的行為，呈現自我放棄的態度等。

基金會表示，長期陪伴性侵害被害者度過復原歷程、致力相關法案制度建立等，對於婦女人身安全議題的關注，並不會隨著重大案件落幕就不再重視。期望在有限的資源下，能有社會大眾的支持，每一筆小額捐款，都是婦女人身安全工作的一大支柱！

（2007.03.21/中央社/晚報）

❊高樓建築物火災之特性

近年來由於建築技術提昇，建築物為增加空間的利用性，紛紛不斷向上發展，各大都市如雨後春筍般，陸續出現一棟棟高樓，甚至超高樓建築物。然而隨著建築物高度的不斷升高，火災發生時，建築物外部消防搶救的能力，也隨之降低，雖然依建築技術規則設計施工編，第 12 章第 227 條規定：高層建築物，係指高度在 50 公尺或樓層高度在十五層以上之建築物。但是現今消防隊之雲梯車僅可達九樓，若利用水柱灌射，僅可再向上射二層樓高，因此消防隊對高層建築物之外部滅火能力僅能達十一層樓。

因此高度在十二樓以上之高樓建築物，其發生火災時，要撲滅火災，唯有靠其內部之消防設備，如自動灑水、水霧設備、室內消防栓及連結送水管等滅火設備之運作；另外人們逃生的方式，唯有依靠最原始的步行方式逃生，因為依現行消防法令，建築物高度在十一層以上是不強制要求設置避難器具的，因為高度過高，就算設置恐怕也無人敢使用。

有鑑於目前高樓建築物之火災有日益增加的趨勢，在此特別向大家介紹高樓建築物之火災特性，期使大家對高樓建築物之火災有更深一層之了解：

一、濃煙密佈：高樓建築物屬鋼構、水泥結構，牢固且屬不燃材料，由於結構不會燃燒，內部易燃材料因外部初期進入之空氣不足，通常形成不完全燃燒，而產生大量濃煙，由於煙有向上竄升之特性，經由各種開口部、通道、樓梯及管路向上層漫延，再加上高樓建築物常有之煙囪效應，使得整棟高樓建築物在極短時間內迅速佈滿了濃煙，造成了視線之阻礙與搶救之困難。

二、內部高溫：由於高樓建築物大多屬密閉式建築，內部因燃燒所產生的高溫，無法藉由空氣之對流傳遞至建築物外部，導致內部熱量蓄積，形成內部高溫、灼熱，此種現象不但使受困者造成灼傷，亦使建築物外部救援人員不易靠近，但是此時如有玻璃破裂或門窗突被開啟，都將因為帶入大量空氣而瞬間產生猛烈之火勢。

三、延燒迅速：由於火燄燃燒之特性是垂直向上延伸之速度遠大於向平面擴張的速度，因此高樓建築物向上聳立，正符合火燄向上延燒的特性，另外由於高樓建築物內垂直管道與上下樓梯通道亦形成火勢延燒的孔道，更形成所謂的煙囪效應（StackEffect），也就是由於內部與外部溫差過大，導致內部熱空氣迅速向上竄升，外部之冷空氣則迅速進入補其空位，形同煙囪一般的效應。這種現象在樓層越高時，其牽引力量越大，越易顯見。

四、逃生不易：高樓建築物由於高度過高，腹地較大，通路轉折變化，人們在火災發生時，通常較平日為緊張、慌恐，再加上內部漆黑、濃煙嗆鼻，都增加了逃生之困難性。

五、搶救困難：由於目前消防隊之雲梯車高度僅能到達九層樓高度，水注灌救恐無法達到預期之效果，即使雲梯車高度可達，然因風力、荷重及噴水反作用力之關係，均對雲梯車本身產生相對的風險性。

綜觀上述所言，高樓建築物火災發生時，無論逃生或救災之危險，尤勝於一般建築物所發生之火災，因此為避免高樓建築物火災的發生，就必須先由認識高樓建築物之火災特性做起，藉由對高樓建築物火災的認識，共同做好防火管理之準備，平日加強各項消防設備之維護，及避難逃生之訓練，如此才能消弭火災的發生，確保大眾的生命財產安全。

（作者為國家專技高考「消防設備師」）

※漫談網路駭客

壹、前言

國內網際網路與電子商務蓬勃發展，網路遭駭客入侵的案例層出不窮，連政府單位網站都曾遭駭客入侵，凸顯網路安全防護的重要性。為防範網路駭客入侵，維護國家安全，防護政府資訊作業，保障民眾權益，政府已經從技術工程、執行管理及教育訓練等層面，推動多項資訊安全措施，同時資訊工業策進會亦成立「網路安全防護服務組」，協助政府及企業面對日益複雜的網路安全防護需求，提供各項諮詢服務，並協調各相關資訊業者通力合作，以解決網路安全問題。

駭客入侵政府機關網站，揭開了兩岸電腦戰的序幕。根據美國最新統計資料，在所有的電腦犯罪當中，屬於企業或機構內部人員

不當存取或惡意竊取、破壞的比例甚高。在網路風行全球的今日，網路安全管理是當今網路世代最迫切要正視的問題，你還能忽略網路安全管理的重要性嗎？什麼是「駭客」？它在網路上進行那些顛覆破壞？我們該如何防護？本文將針對這個問題，做深入淺出的說明。

貳、網路安全問題

連上網際網路代表的是更多的方便，還是更大的災難？世界上每天有人因為受到網路駭客的攻擊而傷腦筋。不管是政府機關、公司行號或是個人，在上網之前必須先要有心理準備，如果你平時並不在意網路安全的問題，這將使意圖不明的侵入有機可乘，你有可能因此受到傷害，輕者可能是資料的遺失或是當機，嚴重的會導致財產與名譽的損害。

網路的危機主要來自「網路駭客」的侵害和「電腦病毒」的傳播。網路駭客在網路上口耳相傳，逐漸蔓延開來，再加上傳播媒體的推波助瀾，甚至讓人常將它與間諜戰或陰謀論聯想在一起。它是網路主要危機的來源之一，因為它會進而竊取或破壞你的資料，甚至假借你的名義去做壞事。而網路的另外一個危機是來自電腦病毒，有些人會藉由四通八達的網路到處傳播病毒，造成某種程度上的傷害。

參、網路安全的漏洞

網路上導致受害的主因有軟體本身設計上的缺失，以及使用者忽略本身資料的保密性。想要連上網路，就必須要使用各式各樣的軟體，而這些軟體本身設計時，有時因為考慮不夠周全（畢竟程

式太龐雜了），於是當使用者利用這些程式連上網路時，就有可能受到有心人士的攻擊。

大多數的瀏覽器程式都曾經有報告指出，會有安全性的臭蟲（Bug，指的是程式的缺失）存在，所以使用者必須小心才能躲過駭客的攻擊。

另一個原因就是密碼被竊取或破解，這樣的缺失佔網路安全失誤的半數以上。還有線上購物如果沒有注意安全，自己或網路商店不小心將信用卡卡號外漏，也會造成財產的損失。網站本身也存在了很多的臭蟲，所以在網際網路的世界裡其實並不是完美的淨土。

肆、安全缺失造成的損害

一、對個人的損害

上網可能導致的損害，基本上就是電腦當機，再不然就是一些個人的資料被竊取。最近網路上一個比較嚴重的問題，就是瀏覽器所附的電子郵件程式有漏洞，許多有心人只要寄出一些特定格式的檔案，就可以把使用者的硬碟格式化（即將原本電腦內的所有資料全部刪除掉！），這樣的後果，可能是你在上網時所始料未及的吧。

這樣的損害還尚屬輕微，如果你在網站上登錄資料或是買東西，而這個網站並沒有做好安全把關的工作，使你和你的信用卡資料外流，再被有心人士利用，如：盜刷信用卡，或是在網路上做壞事、發黑函，將對你的金錢與名譽造成莫大的傷害。

上網時對於商務及本身資料上的應用，安全性的問題尤其不能忽略！一般而言，若企業或機構經常忽略對一般的電子郵件及內部

人員的管制，可能會導致資料被竊取，甚至遭到商業間諜長期入侵而不自覺。

二、對企業體的損害

通常政府機關或是私人企業會以專線的方式連接到網際網路上，也因此網路處於二十四小時連線的狀態，很多網路駭客藉此便可查詢你的主機，進而進行潛伏。有時他們會利用電腦主機裡所執行程式的安全性漏洞，慢慢竊取重要資料；有時他們會很有耐心的分析企業或機構在網路上所流通的資料，進而找出它們的帳號與密碼，最後再以這個帳號的名義進入主機，竊取或破壞資料。對企業而言，最大的損害就是商業機密的損失、客戶資料的外流、帳目資料遭破壞等種種的危害。在國外，許多推銷網路安全產品的業務員會帶一、兩個駭客到你的機關去，示範它們如何在一、兩個鐘頭內竊取並且破壞你的資料，然後老闆就會滿頭大汗地買下產品，因為網路的漏洞真的太多了，讓人很難去防堵。

伍、什麼是網路駭客？

駭客造成了網路族不少的恐慌，到底他們是怎麼樣的人呢？「駭客」這個名詞的來源，其實是由英文「Hacker」音譯而來，在早期的網路拓荒時代就已在電腦玩家間流傳開來，意思原來指的是「電腦很強的人」，就像美國西部牛仔一樣，到處行俠仗義。但是電腦很強的人，心地未必善良，所以又有了另外一個名詞「Cracker」，表示有犯罪記錄或是行為的電腦高手。但是後來大家卻都混淆了這兩個字的含意，再加上中文在翻譯時，也乾脆把「Hacker」翻成有點邪惡形象的「駭客」，於是大家將錯就錯，將凡是在網路上利用技術危害他人的人，統稱為「駭客」了。

其實駭客們基本上並沒有什麼心理上的問題，他們常常是為了一點點的成就感，不眠不休地破解一些原版軟體。駭客的行為大多出於好玩，因為他們發現了一些電腦安全上的漏洞，再加上想對自己技術的挑戰心理下，難免產生壞念頭。現在的傳播媒體，把他們塑造成是一群在社會邊緣，高智商但心理不平衡的傢伙，賦予他們自閉、偏執狂之類的奇怪形象。其實駭客早在人類開始應用電腦系統來處理生活相關事物即已存在，那時的駭客只是一個寧靜社區的入侵者，猶如一群展示個人膽量與另類文化的機車嬉皮族，它們有自己的國度與道義，對電腦系統並不具致命的殺傷力。然而，隨著電腦與網路系統所處理的資料越來越敏感（例如國防機密），或越具價值（例如商情資料），人性的價值觀越來越沈淪之際，現今的電腦駭客已儼然成為一群難以捕捉與防範的高科技電腦犯罪者，1990 年代的網路大盜凱文．米特尼克就是典型的代表人物。

總之，在現實世界裡，駭客和你我一樣，也是安分守己的一分子；只是在網路的虛擬世界裡，他們比你我更具有足夠的破壞力。

陸、駭客在網路上進行的破壞

駭客的犯罪手法不一：有些駭客會去蒐集每個人的人事資料，然後賣給徵信公司或獵人頭公司；有些則會利用網路散布自己寫的病毒，或是不停地對一些特定的對象進行攻擊，例如有些離職員工會在公司的程式中，放入「邏輯炸彈」（意思就是說會在某些特定的狀況下，讓程式發生問題）；而許多的商業間諜與軍事的情報販子則會透過網路，取得一些你所無法想像的資料呢！駭客在網路上進行的顛覆與破壞，大致有以下四項：

一、散發黑函

在臺灣，大多數的駭客都喜歡利用別人的名義去做壞事，之前有人利用臺北醫學院的電腦，發送電子郵件給美國白宮，說要暗殺總統之類的話，然後再逃之夭夭，等到大家發現時，已經為時已晚，造成國際形象不小的傷害。

二、盜用信用卡

在網路上買東西時，對方通常會要求你輸入信用卡的卡號，有時因為程式的漏洞，你的卡號被駭客得知了，就會造成破財的悲劇。目前一般網路購物所使用的安全認證的位元數不足，一般來說，一個有心的駭客只要使用一台 Pentium 的電腦，不眠不休地計算，九個月之內就可破解，順利竊取你的資料。雖然在網路上購物或交友十分便利，但也要注意對自我安全的維護，千萬不要輕易外流自己的資料（尤其是金融資料）唷！由於目前信用卡的消費行為很普遍，交易時也力求便捷，被盜刷的情形真是抓不勝抓， 所以在網路上買東西時，一定要要求對方再以電話通知或是認證，雖然有些麻煩，但是如果你有一天發現自己的信用卡被刷了好幾十萬時，你一定會後悔自己當初為什麼沒有做好這些小動作。

三、販賣個人資料

在美國，有徵信社請駭客專門從政府機關或是一般的民間醫療系統裡，取得個人的人事資料，藉以調查客戶委託的案件中的人士背景；有時也會請駭客長期監看特定對象的電子郵件與個人的信用交易；而很多被監看或資料被竊取的人，往往都是渾然不知的。一般的玩家，也可利用駭客寫出來的程式進行破壞，這些程

式操作簡單，但是功能卻很強大，可以讓一個平凡的使用者突然間變成極大破壞性的駭客。最簡單的例子，我們可以輕易地下載電子郵件蒐集程式，到處蒐集別人的電子郵件，然後廣發廣告等電子信件來賺錢。

電子郵件信箱、信用卡帳號、甚至一個人的身家背景都可以利用四通八達的網路查到。你可以試試看連線到各個搜索引擎（比如 GAIS 引擎），然後輸入自己的名字，就可以看到一大堆有關於自己的資料。而事實上，很多玩家也都藉蒐集或竊取別人的資料賺了一筆為數不小的錢呢！

四、竊取機密

科技越是先進的國家，依賴網路的程度則是越高，對於防禦駭客入侵的能力也相對越低，因為網路實在是太龐大了，到處都有可能出現致命的漏洞。在國外，駭客喜歡對國際型的大企業下手，取得一些機密或是重要資料。有趣的是，由於智慧型犯罪電影的盛行，美國國防部變成了全世界駭客喜歡去練習猜密碼的地方，據報一年內都有上千次的入侵，而其中竟然只有不到百分之十的入侵會被偵測出來，這真是一個可怕的隱憂。其他像是微軟（Microsoft）、雅虎（Yahoo）等大型的商業網站，也正不斷地面臨著駭客的攻擊。

現在的駭客已經不需要很高超的技巧，在網站上便可抓取許多程式，以破解各種密碼或仿造信用卡號碼，探測要攻擊的主機上有那些漏洞可以鑽，過濾網路上的資料，看看那些是密碼，那些是人事資料等等。告訴你一個可怕的事實，即使你沒有上過網路，但是你的資料也有可能因為戶政機關的資料被竊取而散布出去。

柒、駭客的行為犯法嗎？

很明顯地，駭客的行為確實觸犯法律，因為網路的主機屬於私有財產，是不容許他人不經同意而任意取用的。而我們常言的「網路入侵」，就是指非法進入他人主機，甚至是利用他人的名義，散發不良的消息或是破壞別人的網路，這種情形就更嚴重了！對於這樣的行為，可是要負法律責任的，有可能要償付罰鍰及賠償他人名譽及公務上的損失，並且要負刑事責任。

至於毀掉或修改他人公司資料的這種犯罪，就等於是跑到人家家裡去砸壞東西，一定是會吃上官司的，而且這種影響他人公務上的犯罪行為，其賠償金額通常都是很龐大的，往往在百萬元之譜。

駭客的犯罪行為雖是舉證歷歷，但是有辦法抓到嗎？答案是可以的，因為每一個人在上網時都會有一個專屬的 IP，同時主機也會把所有上網人的記錄，都寫在裡面，所以如果順利的話，其實不難抓到這個人。用數據機連上網就可以躲掉嗎？別天真了！因為 ISP 也會有記錄，否則他怎麼跟你算錢呢？

所以警告許多對駭客躍躍欲試的人，千萬別因為想向自我「潛能」挑戰，而聰明反被聰明誤，其實你上網的一舉一動，都會在不知不覺中被記錄下來，國內已有數起破獲駭客的記錄，要順利破獲駭客，除了需要網路上的各單位通力合作外，其實每一位網路管理人員的安全概念也是很重要的，只要經由耐心的分析主機上的記錄檔，每個駭客的影蹤都將無所遁形的。

捌、自保從密碼開始

在這裡把網路世界說得這麼恐怖，無非是希望你在進入網路世界時，能時時提高警覺。其中最基本也是一定要做的，就是把你的

密碼設定好，一個好的密碼必須含有英文大小寫和阿拉伯數字的混合，最少不得低於六個字，而八個字算是基本的要求，就像「XevOr6yn」。這樣的密碼，你可以自己編，也可以到網路上抓程式來編，如此駭客就比較難查到你的密碼。因為大多數的網友都喜歡使用容易記的字（例如名字或是出生年月日等），來當成密碼，因此駭客可以依此建立一本「字典」，再運用工具程式不停地把字典裡的字拿出來測試，如果你用「cat」之類的密碼，大概不到一分鐘就可以被破解了。

所以一旦成為網路族，真的要千萬小心，因為現在沒有出問題並不代表以後沒問題。駭客通常都很有耐心，而且他有可能利用你的帳號，偷看你的個人資料或信件，也可能更進一步的造成更大的傷害！當然像是「XevOr6yn」這種密碼的確比較難記，但是千萬別因為一時偷懶，而造成日後更大的損害。

玖、減少安全性漏洞的防火牆

我們可以運用「防火牆」（FireWall）的軟體，來保護你的網路，但是保護的程度，就要看企業內部的員工配合的程度而定了。比如我們架設了防火牆，但是有些有權限操作防火牆軟體的員工，使用自己的密碼時不夠小心（譬如：最常見的”1234”），那麼便會很容易地被駭客猜中。

防火牆的種類也很多，必須請網路管理人員仔細評估，否則可能在買了之後，發現不符合效用。防火牆運作的原理，就是在公司的電腦與網際網路之間隔一道防線，凡是通過防線的資料都需要仔細盤查，才能通過。因為有了防線的守護，在防線外的人，便無法得知防線內的情形（也就是無法利用網路工具得知），以達

到真正保護的目的。防火牆基本上有兩種，一種是完全隔絕式，另一種是過濾式。前者適合流通量較小的情形，一旦資料流通量很大時，則必須使用過濾式。這兩種互有優劣，但是基本上完全隔絕式的安全性比較高。

然而防火牆並不等於駭客剋星，從學理上來看，防火牆只是系統進出口的一項控管措施，就像是大樓的門戶管理員，並不是該大樓唯一的安全所繫。門戶管理員的職能素質與認真態度不盡相同，影響住戶安全甚鉅，我們不可能因為有了門戶管理員，便將貴重的物品明目張膽地任意放置在明顯的地方，而高枕無憂。正確且確實地使用防火牆，才能真正發揮它的防護效果。

拾、結語

最後以一個網路上流傳已久的故事，來為本文做一個結語：一位公司的網路管理人員向老闆提出要設置防火牆的申請，老闆面有難色，因為他覺得電腦室空間已經很小了，那裡還能再砌一面牆，同時電腦室有隔間的必要嗎？但他不愧是一位好的老闆，從善如流，相信專業人士的建議，馬上批准這項申請。等廠商將報價單送來時，老闆看到上面物品的名稱竟然是「看門狗」（一種防火牆廠牌的名稱），他恍然大悟，原來他們在電腦室隔間是要養狗啊！

希望這篇短文能讓你在網路安全以及電腦駭客的了解上，有所幫助。

安全保防宣導圖片

本資料摘自於清流月刊