機密維護常識彙編（102 年 12 月份）

＊ 從臺菲網路戰說起

說到先前最熱門的新聞莫過於菲律賓公務船槍擊我國籍漁船，並造成漁民死亡的事件。事件發生後不久，我政府部分官方網站陸續傳出無法正常開啟的狀況，經由反查發起攻擊的 IP 位置，發現原來是遭到來自菲律賓的 IP 對我政府官方網站所進行的阻斷式服務攻擊；而我國網友們也不甘示弱地紛紛向菲律賓政府網站發起攻擊，讓菲國許多網站飄揚著我國國旗，甚至使菲國總統府官方入口網站一度成了全球色情網站的分享載點。從這起事件我們清楚得知，網路攻擊無論是政府授意也好、個人自發作為也罷，已成為各國用來嚇阻、甚至攻擊敵方的手段之一。

基於民族意識的個別駭客，往往只針對流量的表層攻擊，多數不會真正危害系統。雖然這樣的行為已違反刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金」，但網路攻擊活動不易產生明顯的跡象，而且往往要在真正遭受實際損害時，才能從中找出責任歸屬，更何況這些攻擊經常來自境外，甚至是無法得知的地點，更遑論要將違法的駭客起訴。

不過更令人擔憂的是，可能有由政府支持的駭客組織，以竊取公務、國防及商業機密為目的；其主要手段包括社交工程攻擊、入侵電腦布建跳板等，以建立情蒐網絡，由於攻擊的對象往往是針對特定的目標，故使防護更加困難。根據聯合國統計，全世界四分之一的國家設有網路作戰部隊。而網路上的攻防戰，既看不到漫天烽火，也聽不見震天聲響，更不用說實際的人員傷亡，只要在電腦前輸入特定指令就可以癱瘓敵方網路，甚至奪得敵國基礎設施的運作控制權，造成該國的動盪。

今（102）年 3 月間，朝鮮半島劍拔弩張之際，南韓境內多家電視台以及相當多的金融機構，突然都因遭受不明網路攻擊，造成三萬多台電腦及伺服器全面癱瘓，南韓民眾甚至想在金融機構領點錢都無法辦到。以如此網路入侵的手法擾亂敵國的社會秩序，將造成該國內部的極大壓力；而受攻擊方甚至不知敵從何來？數量有多少？受到破壞的程度為何？剎那間一切彷彿陷入迷霧之中，不知何從反擊。

在《下一場世界戰爭》這本書中，著名軍事學家亞當斯就說過：「在未來的戰爭中，電腦本身就是一種武器，前線無所不在；奪取作戰空間控制權，不是砲彈或子彈，而是電腦網路系統中流動的位元組。」就以西班牙政府在 4 月間逮捕一名荷蘭籍的駭客來說，他在一輛自用的貨車內就發動足以影響荷蘭、瑞士、英國和美國網路伺服器的大規模分散式阻斷服務攻擊，其攻擊最大強度甚至高達每秒三千億位元。　　正因為網路攻擊的力量如此強大，故而美國特別將網路空間視為海、陸、空和太空以外的「第五戰場」，並加強國防部網路方面的開支，以攔截來自中共、伊朗、俄羅斯及其他國家逐日升高的網路威脅，並加強政府和民間電腦網路的防護措施。而我國國防部也將成立新的資電作戰部隊，藉由提高網路作戰投資，以強化「科技」與「速度」兩項攸關網路戰勝負的關鍵要素，並透過各項演練驗證相關資電作戰以及資訊防護成效；此外，更規劃在北、中、南、東建立地區資安防護管理中心，整合資安事件通報及應變機制，為的就是期望能夠掌握先機，應變制變。

正因資訊安全易攻難守，在不計其數的網路攻擊中，攻擊方只要成功一次，可能就足以致命；而在防禦方，不論就經費或是人員訓練上來講，所有相關作為都比攻擊方所付出的代價高出許多，就因如此，攻擊方在網路戰中可說是占有極大的優勢。此一威脅，無論政府公務部門還是民間企業，甚至是一般民眾，均不能掉以輕心。

隨著智慧型手機的普及，以往在電影上看到駭客使用攜帶型輕巧裝備，在短時間內癱瘓政府網站、竊取國家機密的場景，已悄然遊走在你我之間。而在看似便利的雲端架構下，資訊安全問題對國防、金融、基礎建設等方面可能造成的傷害，將比以往更大。所以每個人都應有「資訊安全，人人有責」的認識，建立「預防重於治療」的觀念，才能在享受資訊設備與網路服務所帶來便利之際，同時確保各項資訊的安全。

（本資料摘自於清流月刊/周晉平）

＊資訊安全應達成的目標

網際網路在 1990 年代以驚人的速度成長，從桌上型電腦、筆記型電腦，到現在的手機無線上網，都與網際網路連結在一起，使得病毒擴散與駭客攻擊更加頻繁。近年

來常見的木馬程式、間諜軟體、釣魚郵件及垃圾郵件等，不僅造成鉅大的損失，也難以單一技術防禦。

網路沒有絕對完美的防禦，因此資訊安全是一種相對「取捨」的作為，應在有限的條件下，將資源投資在最容易受到攻擊或是對單位傷害最大的安全弱點上。例如，一間 10 位員工的小企業，最該做的是為每台電腦安裝防毒軟體，而不是花大錢建構一個安全營運中心。

完整的資訊安全應同時建設 3 個 P 的防護，分別是「人員（people）」、「程序（process）」、「產品（product）」；可以用一句話來整合三者的關係：人員都遵守資訊安全程序，產品（資安工具）才能發揮功效。單位規定電腦要設定複雜度 8 碼以上的登入密碼，同時機敏資料必須要加密，這就是一種程序規範，單位必須依照資訊獎懲規定進行宣導及獎懲，使所有人員都能正確地執行這個程序，唯有如此，單位所購買的作業系統、防毒軟體及端點防護系統才能發揮保護資訊的功效。假使一個單位都照規定做了，但若有些人卻由於記不得經常更換的密碼，就寫在鍵盤或螢幕上，儘管有安全的產品和操作程序，然而缺乏資訊安全意識就會功虧一簣，可見 3 個 P 的防護缺一不可。

單位推動資訊安全所要達成的目標有三項：一、預防，事先預防比事後處理容易許多，防火牆的建立及 Nessus 等偵掃軟體的運用，均可預防電腦或漏洞被違規使用；二、偵測，除了人員的資訊安全警覺性外，入侵偵測系統（IDS）及防毒軟體（SEP）合成區域聯防（ZDBS），將可達到偵測之目的；三、反應，平時必須經常演練及資料備份，將有助於資訊安全事件發生後的反應與復原。

（本資料摘自於清流月刊/王志銘）

＊資訊系統密碼的管理

我國漁船廣大興 28 號遭菲律賓公務船掃射致一名船員被槍擊死亡事件，引發國人不滿情緒高漲，造成兩國關係緊張，意外地演出一場網路大戰。首先是匿名的菲國駭客對我國政府及民營企業發動網路攻擊，緊接著國內網友也在網路上發起反擊行動，

甚至直接拿下菲律賓的 DNS，同時也取得大量菲律賓網站的帳號、密碼，並在網路上公布。

這個新聞事件引起小潘的注意，心想：在高度資訊化的時代，我們每天都要接觸網路，而大多數具有權限管理功能的網站，在登入時均會要求使用者輸入帳號、密碼，以做為身分認證之用；如果這些網站的帳號、密碼這麼容易被取得，對使用者而言，豈不是危機四伏嗎？

在師生的下午茶約會中，小潘把握時間提出他的疑問：如果網站的帳號、密碼這麼容易被竊取，為了避免損失，我們是不是要在不同的網站使用不同的帳號、密碼？難道網站管理者不需要有什麼作為嗎？

司馬特老師喝口焦糖瑪琪朵後娓娓道來：網路安全不是只靠使用者或網路管理者單方面可以完成；除了防火牆、防毒軟體等設備外，管理上也是不可或缺的；在系統端的密碼管理，要從系統設計上去考量，存放使用者帳號、密碼的資料庫，如果只用明碼來儲存，就會產生這次菲律賓的案例，一旦遭到入侵，使用者的帳號、密碼就會全部被竊取。所以存放使用者帳號、密碼的資料庫，應該用加密的方式儲存資料。

司馬特老師看出小潘略顯疑惑，就提了一個問題：你郵局提款卡的密碼忘記了怎麼辦？小潘剛好前陣子發生過，於是很有經驗地回答：郵局會給一組新的密碼，讓您登入後再去改。司馬特老師接著問：郵局為什麼不能告訴你原來的密碼，而要另外給你一組新的？如果系統管理者能看到你的密碼，你會擔心什麼事？小潘直覺地回答：當然是擔心錢可能會被盜領，可是這跟給新密碼有什麼關係？

司馬特老師繼續說：郵局之所以給你新的密碼？就是因為連系統管理者也看不到使用者所設定的密碼；所以當使用者忘記密碼時，他只能給一組新的密碼，這樣做的好處除了可以防止系統的管理者監守自盜外，即使系統遭到入侵，也能確保使用者密碼的安全。

小潘又開始好奇了，接著問道：什麼是加密？要怎麼做？司馬特老師喝口咖啡後繼續說：加密就是透過一個演算法，把原來用明文顯示的資料，轉換成用亂碼顯示的密文。以郵局的密碼為例，當存戶在提款機上更改密碼時，所輸入的密碼資料是明文，

系統會以其內定的加密演算法，把存戶所輸入的密碼轉換成密文，再儲存於資料庫中；既然在資料庫中存的是密文，自然連資料庫管理員都無法看到，這就是為什麼存戶忘記密碼時，系統需產生一組新密碼的原因。透過這樣的機制，即使系統遭到駭客入侵，也可確保密碼的安全。

對於網站帳號、密碼的管理，除了系統端要有管理制度外，使用者對密碼的管理也要注意。國外 SplashData 網站每年都會公布最糟糕的密碼排名，根據該網站的調查，最近 3 年最糟糕密碼排名前 3 名是：password、123456、12345678，這也間接提高密碼被破解的可能性。

Intel 最近推出一個可以評估密碼強度的網頁，當使用者輸入任何字元，網頁便會計算以暴力破解密碼所需的時間。結果發現：由數字及字母組成 6 個字元的密碼，在 1.18 分鐘就被破解；如果密碼結合了數字與英文大小寫字母，則強度馬上暴增，需要很長的時間才能破解。

從這些容易被破解的密碼資訊可知，在使用者的密碼管理上，應該要避免使用順序或重複的字元、避免使用與登入名稱相同的密碼、避免使用任何語言字典中的單字作為密碼，才能提高密碼的安全性。

小潘在聽完司馬特老師的一番說明後，對於資訊系統的密碼管理，有了更深一層的了解。原來系統的安全，除了靠防火牆、防毒軟體的工具外，管理制度也是很重要的；由菲律賓網站被入侵造成的密碼外洩事件，正好可以檢視自己單位的資訊系統安全性，適時地修補漏洞，以防止危安事件的發生。

（作者為科技大學資訊管理系講師／魯明德）