惡意程式已和網路應用緊密結合，從攻擊面可嗅出駭客思維的轉變，包括鎖定特定目標輕易獲利、利用網路社群遂行社交工程較易得手及獲利等面向。

解析網路攻擊發展趨勢與防護之道

◎吳文進

一、前言

臺灣So-net網站近期遭駭客入侵，會員個人資料外洩，導致信用卡被盜刷約1,840張，國內幾乎所有發卡銀行都中獎。經警方調查，駭客可能來自中國大陸，係以俗稱「釣魚網站」的假網頁，藉由郵寄電子郵件、圖檔等方式夾帶木馬程式入侵，So-net員工甚至高層幹部都不知自己的電腦已中毒。無獨有偶地，日前有超過50家位於美國、歐洲及澳洲的銀行，也同樣遭駭客以網址嫁接（Pharming）的方式進行攻擊，駭客利用假造的銀行網站與pharming技術，讓使用者登入假網站，趁機竊取個人資訊，相關損失尚無法預估。駭客主要是利用微軟系統的漏洞，當使用者登入正確的網址時，會被導向事先假造的銀行網站，而未安裝修補程式的電腦，將會被載入主要木馬程式，以及來自俄羅斯網站的其他５個副檔，爾後若連上已被鎖定攻擊的網站時，就會被自動導向假網站，所鍵入的資料也都會被記錄，並送回位於俄羅斯的伺服器。

以上只是近年電腦網路犯罪的個案，就2006年而言，資安研究人員大多已觀察到並提出一種現象，那就是「目標式攻擊」（Targeted Attack）或「地區型攻擊」已逐漸成為主力，相較於以往如Code Red、Blaster、Sasser等病毒發作時期的無差別式蠕蟲攻擊行動，攻擊者已經鎖定特定目標族群或地區，攻擊的行動複雜但精準，並廣泛採用社交工程（Social Engineering）技術，其背後所牽引的動力，已不再是單純的駭客展現功力，而是以金錢獲利為主要的動機。

二、何謂「目標式攻擊」？

以往一支病毒程式攻擊所有電腦的「亂槍打鳥」模式已不復見，取而代之的是針對特定目標族群，成群結隊地入侵。這樣的狀況已不斷重複地上演，而各單位資安人員卻可能束手無策。依趨勢科技針對這類「目標式攻擊」所做的研究發現，目標攻擊通常區分3個步驟：首先由不法分子或犯罪組織針對特定對象發出網路釣魚郵件，邀請收件人前往瀏覽某個網站，而當收件人受誘騙進入該網站之後，其電腦便會被自動植入「下載器」（downloader），控制者便可在受害電腦上監聽傳輸資料，最後下載器除會向操控者報到之外，亦可自動連結到某些特定的網站，同時將所有的木馬工具包或更多的「下載器」運送到該電腦，使其能力不斷增強，而該受害電腦也可經由網路芳鄰的連結，伺機發動攻擊，使同一網段中的電腦無一倖免。目標式攻擊可怕的地方，在其成群結隊入侵的特性，以及不斷自動更新升級的手法，除可有效地避開防毒軟體的偵測之外，就算發現了，也可能因為複合式病毒或太多木馬，清不掉也清不乾淨。此外，因為每一台電腦的原始檔案都不一樣，感染途逕及處理方法也不盡相同，因此資訊部門人員無法以標準的作業程序，將解決方案快速部署至整個網路，而陷入左支右絀、疲於奔命的窘態。

目標式攻擊的另一個問題是中毒後的清除程序，由於清除工作不只是還原某一種惡意程式的某一種損害行為，因為一次攻擊所包含的惡意程式碼往往不只一種，而且攻擊的時程也可能持續一週甚或數月，檢測人員除須終止所有非正常的程序、刪除惡意程式所建立的檔案或修正登錄設定之外，還必須確認哪些資訊可能已遭受入侵、哪些惡意程式碼可能殘留、哪些系統是近期內的交互感染，有沒有新的病毒或木馬等，並應防止這些程式碼再度發動攻擊或進一步對系統造成損害等。

三、惡意程式也搞創新

以往的駭客以「零時差漏洞」（Zero Day Exploit）為標準配備，攻城掠地、搶奪地盤的入侵行動只為證明自己的功力，但隨著軟體及網路的複雜化，加上獲利的趨使，給予入侵者更強烈的動機，因此工具的發展不僅精緻化且模組化，可隨心所欲升級，而數個工具的組合可發起一次成功攻擊，但分開使用時沒人會發覺它們不軌的行徑。此外更令人憂心的是，安全防護是被動式的，本屈居劣勢，當攻擊的時間或地點分散，除加深資安或網管人員採樣解析的難度外，變種病毒不斷繁衍與自我更新，有愈來愈多的時候我們看到中毒時，防毒軟體卻默默無言，即使發現也大多無法清除或隔離，因此國外許多專家紛紛喊出「防毒軟體無用論」。

放眼今日，惡意程式已和網路應用緊密結合，從攻擊面可嗅出駭客思維的轉變，包括鎖定特定目標較易獲利、利用網路社群遂行社交工程較易得手及獲利等面向。另從實務上來看，木馬或間諜程式發威，不論銀行或公家機關無一倖免、網路釣魚技巧使詐騙行為隱匿於無形、專為行動裝置發展的惡意程式從概念驗證到威脅成真、病毒程式可讓主機報廢，以及商業軟體所提供的工具箱（Rootkit）淪為玩家作弊利器等案例，顯示惡意程式手法不僅日新又新，且創意十足。因為在這些攻擊者的眼中，當獲得的報酬愈來愈吸引人時，惟有持續研改攻擊的方式與技巧，整合駭客、間諜及惡意軟體，甚或發展成分工細密的組織，才能滿足發動攻擊的實需。而這些整合性的精準攻擊手法，在2007年及未來將持續為攻擊者所用，甚或不斷發揚與創新，網路世界將無法擺脫這些惡意攻擊者的糾纏。

四、資安廠商對網路攻擊之分析與預測

回顧2005年，網路攻擊主要來自即時通（IM）蠕蟲、木馬、病毒及混合式攻擊等威脅。以混合式攻擊的病毒來說，特洛依木馬程式的隱匿入侵、蠕蟲的迅速散播及間諜程式高超的偽裝技巧，三個惡意元件聯手出擊的「網路釣魚」，已使網路安全防線瀕臨崩潰。隨後，原專攻大型企業用戶網路的「勒索程式」，逐漸威脅家用電腦或小型企業用戶，因為網路勒索的歹徒不但覬覦企業大魚的豐厚回報，也狡詐地嗅出鎖定家庭用戶或小型企業可降低被捕的風險。而更甚者，利用僵屍網路（Bot Net），展開分散式服務阻斷攻擊，以驚人的流量癱瘓那些不願付款的網站。

到了2006年，這些模式除轉變得更精緻外，更有整合之勢。依資安公司Tipping Point近期公布2006年以20大網站為對象所遭受攻擊的分析報告指出，2006年由於網路詐騙而招致的損失，較2005年上升４至５倍。該公司並提出６大主要攻擊趨勢，這項公告將有助資安人員更有效率地調整組織的防

護機制，以對抗不斷出現的新漏洞，從而避免電腦遭非法操控及竊密，攻擊趨勢如次：

1. 零時差攻擊（Zero day attack）已不再只襲擊IE瀏覽器，更有蔓延至Microsoft其他應用軟體的趨勢。
2. 現存Microsoft Office產品如PowerPoint及Excel的漏洞，其攻擊有加遽之勢。
3. 針對性或目標性之攻擊持續上升。
4. 證據顯示較多針對軍方及政府機構外包合約商網站而發動的魚叉式網路釣魚攻擊（註１），已擴散至其他類型機構。
5. 網路語音（VoIP）攻擊已透過轉售通話謀利，並有可能加進錯誤引導訊息，屆時將影響傳統電話網路。
6. 網路應用軟體持續出現大量的漏洞。

此外，趨勢科技也發表2006年資安威脅分析與2007年的資安預測報告。其中2006年組織型犯罪仍以「身分竊取」、「商業間諜」及「商業勒索」為主，而殭屍網路已成為尋找攻擊目標的駭客們所普遍運用的工具。預判2007年網路攻擊事件將愈演愈烈，並以社交網站為主要的攻擊目標。究其原因，係多數國家頻寬已大幅提升，使得不管是影音檔案、新興的應用程式或其他資料類型檔案的下載運用，變得非常普遍。因此有愈來愈多的攻擊者入侵公開網站，將他們所撰寫的惡意軟體隱藏其中，讓毫無戒心的用戶在下載含有惡意軟體的檔案後，就會觸發多重的感染。此外，攻擊活動除具大規模外，還可迅速轉移，當混合式威脅變得愈來愈狡詐，將使威脅爆發的方式變得十分不同，而偵測、復原所投入的成本亦將倍增。

五、自我防護之道

網路有句名言：「網際網路的時代，有誰會知道坐在螢幕前的是一條狗或是病毒？」形容得十分貼切，因為吾人每日所瀏覽的網站、所收的e-mail到底是不是偽冒的，實難察知，因此，惟有建立資安憂患意識，隨時提高警覺，始能避免受駭。以下整理吾人上網時特應避免的行為，籲請網友注意：

1. 不隨意開啟不明來源之電子郵件。
2. 不隨意執行郵件內夾帶之檔案或連結。
3. 避免下載免費軟體或圖檔。
4. 不隨意點擊網頁內的連結網址。
5. 不隨意點擊彈出式廣告或不明內容視窗。
6. 避免使用點對點（P2P）軟體分享檔案
7. 不使用盜版軟體或破解程式。
8. 不使用網路駭客工具。
9. 避免點擊即時通或部落格內不明的網路連結。
10. 避免依安全警告訊息點擊或開啟視窗。

上列危險動作，僅提供網友自我檢查，惟當務之急，還是建議網友安裝一種以上的反間諜軟體，並定期掃描檢測，以確保安全；另以下幾項觀念，屬資安基本認知，亦應防範：

1. 沒有任何一種防毒軟體可以偵測所有的惡意程式，病毒檔案類型除傳統的.doc、.exe、.dll、.com、.sys外，.ppt、.xls.、.htm及.wmf等類型漏洞的利用則屬新興攻擊方式。
2. 駭客都是夜行性動物，根據各企業組織「資安監控中心」分析結果顯示「愈夜愈美麗」，因此隨手關機或中斷網路連線，環保又安全。
3. 所有p2p的服務除易招惹病毒或木馬外，等於在防火牆或防毒軟體開了一個門等著大家來光顧。
4. 所有的駭客手法中，以透過e-mail的釣魚手法最難防範，不管資安教育做得再落實，只要e-mail偽裝得夠好仍會淪陷（攻心）。
5. 如果你的防毒軟體在系統內重覆發現同一個病毒且清不掉，代表已知型的病毒夾藏未知病毒，複合病毒代表你的電腦具有高風險。
6. 所有的木馬都是用網路保密協定（SSL）加密與中繼站連結，因此網路型入侵偵測機制對木馬而言，形同虛設。
7. 所有的駭客工具通常夾帶有木馬程式（天下沒有白吃的餐）。
8. 軟體弱點仍以「緩衝區溢位攻擊（buffer overflow）」為榜首，因此安裝防火牆、防毒軟體及適時的漏洞修補是必要也是基本防護。

除了上述個人應注意的事項外，企業組織在架構對外的防禦機制之餘，應思考前端防禦除病毒防護、修正程式派送外，尚可強化各個終端抵抗深度攻擊的能力、加裝反間諜程式，並適當攔阻與管控威脅等，藉多重防護機制應可避免災損擴大。而在後端，則應強化內部存取控制、制訂身分識別機制，同時應定期對於內部網路流量、連線行為等實施追蹤與分析，如此將有助於即早預警及攔阻隱藏性的攻擊行為，並能防止內部人員的攻擊或竊取機密資訊。

六、結論

網際空間「所見不一定即所得」，這個道理每個人都應了解。當攻擊的目標從系統轉移到網路應用程式，再轉移至個人用戶時，表示「防毒以外的保護」才是防堵這些新型資安威脅的最佳對策。因為問題的根源不僅止於個人電腦，同時還涉及網路傳輸設備，除應廣擴網路安全防禦的縱深外，如何有效蒐證鑑識以訴諸法律行動，又屬另一個研究之範疇。當然，安全的解決方案與機制沒有所謂的照表操課保證成功的公式，網路社群也往往會鬆懈一般使用者的心防。一味地強調多重防護機制，可以有效防範來自外部的威脅，然而事情只做了一半；另一半，甚至是更大部份的威脅是來自內部人員，因此，惟有積極地縮小組織內部人員的資安貧富差距，使所有成員都是資安偵察員，才能化被動反應為主動防禦，才能在安全防禦與攻擊者這場無止盡的攻防競賽中超前。

註1：「魚叉式網路釣魚」（spear phishing）攻擊，是指駭客鎖定特定組織成員每天瀏覽固定網頁之習慣，在網頁或是受害系統中置入病毒自動下載器，並持續更新病毒變種到受害系統謂之。

▲Top

私宰斃死豬案件並非「天公巨案」但直接影響國民生計，所以獲得各級政府重視。

新木馬屠城記—智慧之戰又一章

◎田清濤

身為國家的調查員、民眾的調查員，我們深知民眾需要萬能的政府，因為只有萬能的政府，才能夠為國人提供一個安定無虞的生活環境和自由自在的生存空間，但是政府能否萬能，則必須身為國家機器一份子的每一位公僕，無私無我的奉獻，才能達成確保國民生計、增進民眾福祉的終極目標。因此，法務部調查局雲林縣調查站秉持各級長官的信念，將「民生案件」列為本站執行調查任務「重點中的重點工作」，務期擦亮調查局這塊招牌！

94 年年初，本站配合雲林地檢署並獲雲林縣警局之協助，一舉偵破雲林縣土庫鎮「王○○私宰斃死豬違法流用集團」，查扣斃死豬肉18 公噸，移送王某等犯嫌26 人，承辦檢察官以王某私宰斃死豬違法流用，具有「間接殺人」之故意為起訴法條之一，求刑18 年，併科新臺幣（下同）900 萬元罰金，經雲林地方法院一審判處有期徒刑8 年，案例經媒體報導震驚全臺；但私宰斃死豬違法流用集團並未因此而稍加收斂，故本站持續於95 年2 月間再度偵破雲林縣水林鄉「李○○私宰斃死豬違法流用集團」，查扣斃死豬肉20 公噸，移送李某等犯嫌18 人；並提供線索協助友軍單位破獲口湖鄉「陳○○私宰斃死豬違法流用集團」，查扣斃死豬肉6 公噸，移送陳某等犯嫌15 人。原本認為經過如此大力掃蕩之後，雲林縣境私宰業者應能體認政府取締不法之決心，從此洗心革面，真正做到「放下屠刀，立地成佛」的境界。孰料暴利之所在，仍有不法業者趨之若鶩，甚至變本加厲擴大私宰規模，本站為除惡務盡，又於95 年9月間偵破「陳○○私宰斃死豬違法流用集團」，查扣斃死豬肉20 公噸，移送陳某等犯嫌23 人，本案並首度查獲合法集運業者勾結私宰業者共犯牟利，亦係農委會推廣集運車強制裝設「GPS 衛星定位儀」稽查監控業者集運過程後，首度查獲集運業者涉案。

由於我們的努力，使國人對於所謂私宰斃死豬有了進一步的認識，但卻招致私宰業者的不滿與憤怒，理由簡單，因為私宰斃死豬可以賺取暴利，而本局的查緝動作就是斷了他們的財路，所以他們怨恨，更對外放話稱「若是調查員衝進來抓，就用豬刀插死他們！」。可是，身為國家的調查員，身為民眾的調查員，我們會畏懼嗎？我們能畏懼嗎？我們非但沒有停下查緝的腳步，反而邁開大步更加勇往直前。接連不斷的查緝動作，造成私宰業者慌了、亂了，因此他們風聲鶴唳、草木皆兵，派出「小蜜蜂」機車巡守隊四處梭巡監控進入村子的人車，不是為了協助維護治安，而是防堵查緝人員發現他們的惡行。

這樣的動作當然影響到本站的偵查作為，變裝、易容、使用私車等等偵查手段已經無法繼續沿用，所以「窮則變、變則通」，我們師法荷馬史詩敘述的希臘神話「特洛伊戰爭」中，希臘大軍盟主阿加曼儂王的謀臣綺色佳王奧德塞提出的「木馬屠城計畫」，設法商借一台冷凍車，在裡面藏置10名專案人員，直接衝向私宰業者屠宰分切斃死豬之現場，猶如特洛伊之戰中的木馬屠城。我們在96年2月1 日以「新木馬屠城記」—智慧之戰又一章的創意，順利偵破陳某等私宰斃死豬違法流用集團案，並連帶執行搜索13人18 處現場，傳喚27 人，逮捕1人，收押禁見9 人，直接查扣近29 公噸違法肉品，當然執法現場並非慘烈的爭戰場面，也沒有發生歹徒負隅頑抗的畫面，只是我們以歷史為借鏡，以冷凍車代替奧德塞的木馬，完成了上級交付的任務。

另外，值得一提的是，在96 年2月1日執行搜索並傳喚主嫌陳某時，陳嫌拒不到案，但卻於翌日即96年2月2日前往法院門前，意欲打探其餘到案人員是否遭到收押。適巧本站人員因主嫌未到案，前往法院申領拘票執行拘提，當調查員到達法院前，赫然發現疑係陳嫌平日駕駛之車輛停在法院前，乃在領取拘票並通知站部查詢車籍確定無誤後，由專案組人員趕至現場，在第一時間內出示拘票順利逮捕陳嫌歸案。過程雖然十分戲劇化，但也證明調查人員具備了敏銳的觀察力和靈活的機動性，當然，更確立了「百分之九十九的偵、百分之一的破」顛撲不破的偵查準則。

經查陳某等私宰斃死豬違法流用集團，自90年起就開始運作迄今，至我們查獲為止，5年多來他們銷售至全省各處的私宰斃死豬肉肉品數量，超過2,600公噸以上，以目前查獲94年9月1日至95年12月31日的運量統計即約500公噸，因此本案的偵破確實對「確保國民生計、增進民眾福祉」作了見證，亦相對提高國人對政府施政的信心與對本局的信賴，值得我們為自己喝采！其實，私宰斃死豬案件並非「天公巨案」，但因直接影響國民生計，所以獲得各級政府重視，在掌聲之後，我們已經悄悄展開其他新案件的偵查動作，我們不會也無法停下腳步，因為我們是國家的調查員，我們是民眾的調查員。

▲Top

如果收到行政執行處寄發的傳繳通知單，千萬不要置之不理。

出國玩卻在機場被擋下！

◎楊桂青

報載，日前有一位王先生向南區國稅局抗議，表示自己僅滯欠個人綜合所得稅40餘萬元，並未達到限制出境的標準，為何會遭限制出境？經過查證之後發現，南區國稅局並未對王先生作出限制出境的處分，而是因為他欠稅滯納期滿，國稅局將此案移送法務部各地區行政執行處後，遭行政執行處依行政執行法第17條規定而被限制出境。

您知道行政執行處是什麼機關嗎？您曾收過行政執行處寄發的傳繳通知書嗎？

行政執行處於90年1月1日成立，是專責處理關於公法上金錢給付義務之強制執行的機關。什麼是公法上的金錢給付義務？我們只要看一下目前全國13個行政執行處所受理的案件種類，就可以很清楚的了解。根據統計，截至95年9月底止，法務部行政執行署所屬各行政執行處共受理案件約2,935萬餘件，分為財稅案件、健保案件、罰鍰案件及費用案件等四大類。其中財稅案件包括欠繳所得稅、房屋稅、地價稅、營業稅、牌照稅、遺產稅等，約占27%，健保案件（即欠繳健保費），約占55%，罰鍰案件包括欠繳違反道路交通管理處罰條例、違反廢棄物清理法或違反各項法律之裁罰等，約占8%，費用案件包括欠繳勞工保險費、汽車燃料使用費、毒品防制戒治費等，約占10%。簡單的說，只要是積欠政府機關的稅、費，都可能被移送到法務部各行政執行處強制執行。

留意一下您的稅單繳納了嗎？健保費或勞保費繳了嗎？手邊有沒有交通罰單還沒繳？如果您還沒繳，請記得儘快繳納。如果您已經收到行政執行處寄發的傳繳通知單，千萬不要置之不理。如果您有疑問可以直接向各行政執行處詢問，否則不只您的銀行存款或薪水可能會被扣押，甚至您個人還有可能被限制出境！就像前面的王先生一樣，興沖沖的準備出國，卻在機場硬生生的被擋下！若您對於執行處傳繳的欠款目前繳納確有困難，也可以先到行政執行處和執行人員溝通，因為行政執行處在依法行政，維持社會公平正義之餘，仍會在不違背法令規範下，給予民眾適當的協助以解決欠款。

（作者任職法務部行政執行署屏東行政執行處）

▲Top

異常財產增加會被罰行政罰，如果調查貪污有據，將遭刑法追究。

期待陽光普照，弊絕風清

◎史　文

【前言】

公職人員財產申報法為我國制定的第一部陽光法案，雖然只是眾多陽光法案中的一環，然而它在當年的社會環境下，許多人對於公職人員財產申報法的施行寄予厚望，認為只要能順利推動，便足以遏止公職人員的貪污行為，使政商分離，達成政吏清廉的效果。然而，在歷經13 年的推動實施之後，我們發現公職人員財產申報法的施行，無法有效抑制各種層出不窮的弊端或貪瀆行為，顯然「陽光法案」的陽光，依舊無法普照全國公務機構的每個角落，陽光法案所希望達成清廉官吏、端正政風的立法目的，仍然有待加強與改進。

【修法內容摘要】

財產申報法修正案完成三讀，清廉政治更進一步經政府主管機關、學界及立法委員之共同努力，公職人員財產申報法修正草案，終於在96 年3 月5 日，經立法院第6 屆第5 會期院會完成三讀程序，樹立我國政府清廉執政之重大里程碑。公職人員財產申報法自民國82 年9月1 日施行迄今，歷經兩度小幅修正，然因社會對於公職人員的清廉有著更深的期待，且配合政府貫徹防貪、肅貪、反貪之決心，近年來行政院及法務部積極推動公職人員財產申報法之修法工作，此次修正主要內容如下：

1. **擴大申報義務人範圍：**將具有決策權、監督權之相關公職人員，如行政執行官、軍法官、政風及軍事監察主管人員、各級政府機關職務列簡任第10 職等以上之幕僚長及主管等，均納入申報義務人範疇。（第２條第１項）
2. **嚴密財產申報之時機及內容：**為落實財產申報之審核及了解申報人財產增減情形，增訂申報義務人卸（離）職者亦應申報；又一定財產之申報並應包括取得之時間、原因乃至價額。（第３條及第５條）
3. **由「財產信託及動態申報擇一辦理」之雙軌制，修改為「財產強制信託」之單軌制：**總統、副總統、五院院長、副院長、政務人員、公營事業總、分支機構之首長、副首長、直轄市長、縣（市）長其本人、配偶及未成年子女之不動產、國內上市、上櫃之股票及其他經核定之財產，均應辦理強制信託。（第７條第１項）
4. **增訂「財產變動申報」制度：**立法委員及直轄市議員其本人、配偶及未成年子女之不動產、國內上市、上櫃之股票及其他經核定之財產，應每年辦理變動申報。（第８條）
5. **強化申報資料之查核：**為利於受理申報機關（構）進行查核，以確保財產申報制度之落實，爰將查核之要件依實際需要酌予修正，並增訂監察院及法務部得透過電腦網路請求有關之機關（構）、團體或個人提供必要之資訊，受請求者有配合提供資訊之義務之規定，可節省公文往返時間及有關機關（構）回復查詢所必要之人力物力，且對可疑人員之財產進行監控，期能落實本法防杜貪瀆之功能。（第10 條）
6. **增訂意圖隱匿財產不實申報及財產異常增加違反真實說明義務之罰則規定：**有申報義務之人故意隱匿財產為不實之申報，或其前後年度申報之財產經比對後，增加總額逾其本人、配偶、未成年子女全年薪資所得總額一倍以上者，受理申報機關（構）應定1 個月以上期間通知有申報義務之人提出說明，無正當理由未為說明、無法提出合理說明或說明不實者，分別處予最高新台幣400 萬元或300 萬元之罰鍰。

【相關配套措施】

此次修法擴大應申報財產的公職人員範圍，爰此，本法之施行細則及相關配套措施之良窳，攸關本法執行成敗至鉅。據法務部政風司表示，現行應申報財產之公職人員人數約3 萬2 千人，修法後預估應申報人數將增加1 倍，約5 、6 萬人，法務部已成立專案小組，就修改施行細則、財產申報表格等作為進行籌備，迄今已召開２次會議，待總統公布施行後，將在6 個月內培育種子教官回其所屬機關進行教育宣導工作。

法務部另指出，因本次修法涉及監察院、行政院、考試院，法務部將通函各機關，並邀請監察院和考試院人員與會，就修改施行細則部分表達意見。

【反應與建議】

1. 部分人士批評甫修正通過之公職人員財產申報法，還是形同無牙老虎，一切除罪化，不必擔心坐牢，增加再多的罰款，對高官們還是不痛不癢，沒有震懾力讓大官們老老實實申報，這樣的陽光法案一點也看不到陽光。然而實際上，貪污行為另有貪污治罪條例加以規範及處罰，可以判刑並罰金1 億！因此，並不是貪污不用被查處，而是由不同的法律處罰，財產申報法本身是行政罰，與刑法的性質不同，換言之，異常財產增加會被罰行政罰，如果調查貪污有據，將遭刑法追究！
2. 監察院先前送出的公職人員財產申報法修正版本，增列申報者必需對不明的財產明顯異動，負舉證責任。此舉對防止公務員貪污必然甚具效果，朝野部門均應一鼓作氣，落實陽光法案的精神，賦予申報人對渠巨額財產來源不明罪的舉證責任，此係財產申報制度之重要核心價值，更是防止權力濫用和預防腐敗的重要措施。惟「巨額財產來源不明罪」舉證責任迄未明文規範。我國應儘快建立完善之財產申報制度，讓大眾對公職人員財產變化進行監督，方能有效落實陽光法案之精神。
3. 新法大幅擴大申報範圍及罰則，據監察院公職人員財產申報處表示，未來公職人員財產申報的人數將增加約1 倍，監察院現有員額、經費，將不足以應付大幅增加的財產申報業務，雖然立法院附帶決議中，請行政院協助增加監察院的人員和經費，但約聘人員畢竟是暫時的，治本之道還是得修正監察院組織法。監院組織法上次修正在1998 年，當時陽光法案僅有財產申報法，但之後陽光法案又陸續增加利益衝突迴避法、政治獻金法，未來可能還會有遊說法，監院組織法應該儘快修正，以因應時空變化之所需。

【結論】

所謂「太陽底下沒有新鮮事」、「陽光是最佳的防腐劑」，政治制度的透明化、公開化是政府清明的表徵，藉由立法將政府施政行為進一步的透明化、公開化，是防止公務人員貪污瀆職的最佳防腐劑。民國82 年9 月1 日施行之「公職人員財產申報法」是我國陽光法的起步，事實上，公職人員財產申報制度，僅是諸多陽光立法中的一小部分，陽光法案包括一系列的行政程序立法、資訊自由立法、機密檔案立法、政治捐獻立法、遊說行為立法等施政作為，才能真正將政府施政的過程及內容，公開在社會大眾面前共同檢視，才能達到端正政風的目的。

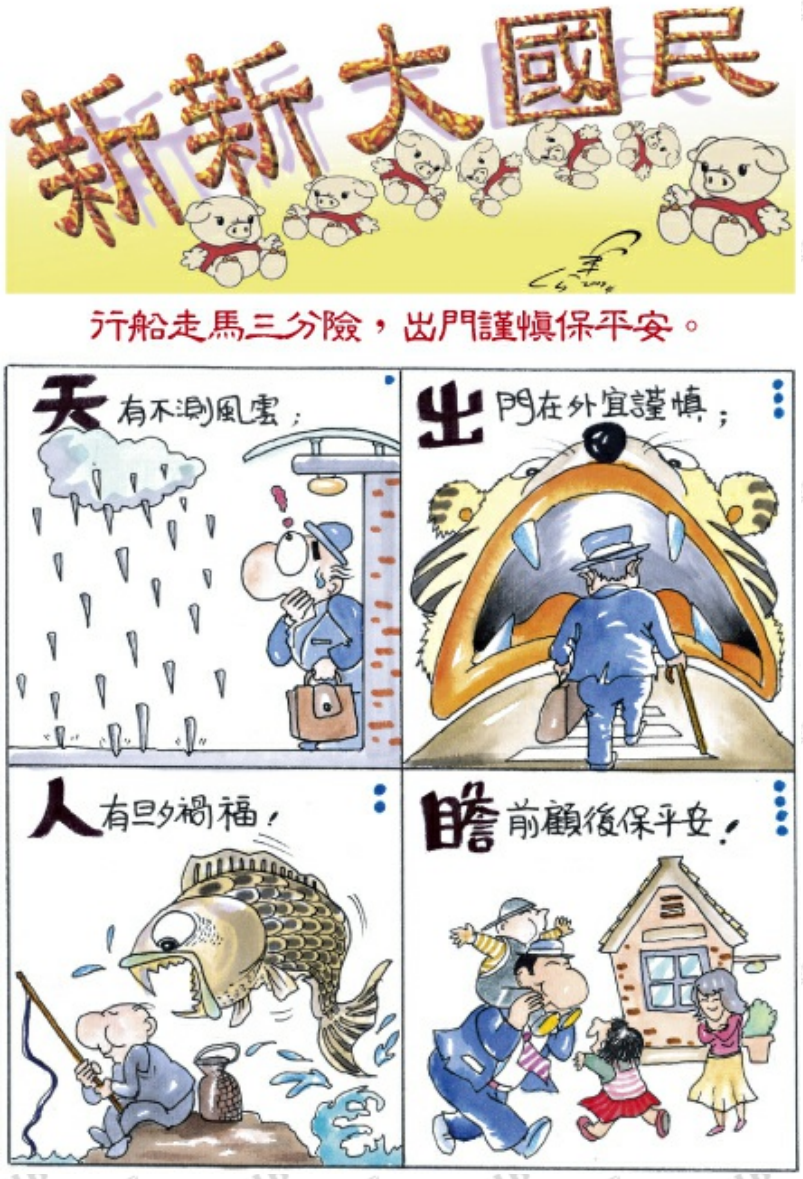
（作者任職監察院）

▲Top

保防漫畫

◎蘇　宏

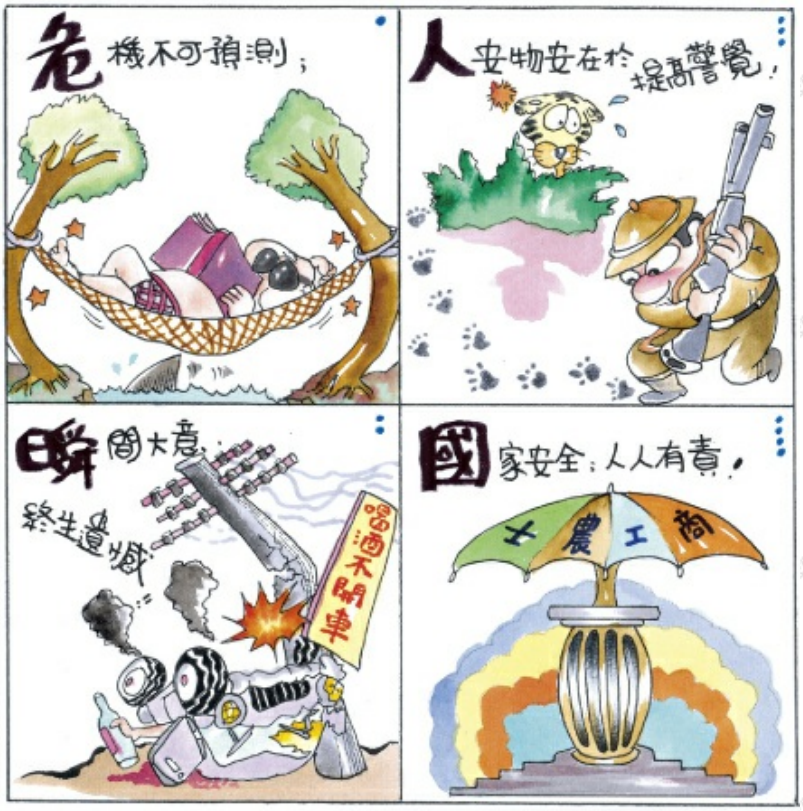
行船走馬三分險，出門謹慎保平安



保防短語

危機無預警，安全無假期

危機無預警，安全無假期 。



▲Top

清流月刊中華民國九十六年四月號

不可忽略網路便利性潛存的各種危險，一不小心就可能觸犯法律。

網路犯罪問題，你注意了嗎？

◎陳宏煇

近年來，網路早已成為你我生活中不可或缺的一項工具，而它的便利性，更被廣泛地運用在生活各方面，但原本只是單純被大家用來當做傳播資訊、溝通與聯絡的媒介，現在卻可能成為一項犯罪的工具。事實上，大部分的人都會認為網路犯罪問題不會牽扯到自己，因為只要對方或其他人看不到自己，在網路上要怎麼批評、侮辱或攻訐他人都沒有關係，也因此很多人往往就在沒有警覺的情形下，觸犯了法律而不自知。在此蒐羅常見網路犯罪實例，希望大家能夠正確看待如何使用網路，以避免誤觸法網。

一、故事內容

案例一：入侵他網竊資料，小心監牢待五年

國內某大學陳姓大三學生與洪姓高三學生共組駭客集團，以「ＸＳＳ（Cross Site Scripting）攻擊手法」入侵國內知名網站，不但竊取該網站的個人資料，甚至還提供檔案連結，讓網友可以自由下載他所竊取的用戶資料。

牽涉法律：刑法—妨害電腦使用罪

上述案例中，陳姓大學生與洪姓高中生二人，可能觸犯了：

1. 〈刑法〉第358 條「入侵他人電腦設備罪」：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。
2. 〈刑法〉第362 條「製作電腦程式妨害他人電腦使用罪」：製作專供犯妨害電腦使用罪章之罪之電腦程式，而供自己或他人犯妨害電腦使用罪章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

案例二：網拍健康食品，三年徒刑少不得

劉姓男子大學畢業後，因不習慣朝九晚五的生活，於是就在家中從事網拍工作，除了上網拍賣健康食品，自己還分裝成立網站銷售，短短的幾個月便賺了三十幾萬，但不久卻收到了衛生機關的舉發公文。

牽涉法律：健康食品管理法

劉姓男子可能觸犯：

〈健康食品管理法〉第21 條規定略以：未經核准擅自製造或輸入健康食品，或販賣、供應、運送、寄藏、牙保、轉讓、標示、廣告或意圖販賣而陳列者，處三年以下有期徒刑，得併科新臺幣一百萬元以下罰金。

案例三：網路抒發文字欲，五年苦牢不可少

國內中部某科技大學賴姓碩士生，一時興起在網路上聊天室打了「要員嗎？4 K可以嗎？」結果和對方相約見面時，卻遭警方逮捕。

牽涉法律：兒童及少年性交易防制條例

賴姓男子一時衝動，卻可能觸犯：

〈兒童及少年性交易防制條例〉第29 條規定：以廣告物、出版品、廣播、電視、電子訊號、電腦網路或其他媒體，散布、播送或刊登足以引誘、媒介、暗示或其他促使人為性交易之訊息者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。（註：釋字第６２３號解釋，認為本條規定對於行為人所傳佈之訊息如非以兒童及少年性交易或促使其為性交易為內容，且已採取必要之隔絕措施，使其訊息之接收人僅限於１８歲以上之人者，並不適用。）

案例四：網路貼文批明星，坐牢罰金樣樣來

日前偶像藝人許瑋倫因車禍不幸玉殞，結果一名薛姓女子在其個人部落格發表文章批評許瑋倫，並且以不堪入目的字眼辱罵她，因而招致其他網友的撻伐，除要求薛女道歉外，且公布她的工作地點、電話，並醜化她的網路照片，更有甚者還在網路上留言恐嚇她。

牽涉法律：刑法—誹謗死者、公然侮辱、恐嚇罪等

上述案例必須區分為二部分來處理，首先是薛女在自己的部落格上批評、誹謗許瑋倫，可能觸犯：

1. 〈刑法〉第312 條第1 項「公然侮辱死者罪」：對於已死之人公然侮辱者，處拘役或三百元以下罰金。
2. 〈刑法〉第312 條第2 項「誹謗死者罪」：對於已死之人犯誹謗罪者，處一年以下有期徒刑、拘役或一千元以下罰金。

另外，網友回應攻訐薛女，並公布她的工作地點、電話，則可能觸犯了：

1. 〈刑法〉第309條「公然侮辱罪」：公然侮辱人者，處拘役或三百元以下罰金。
2. 〈刑法〉第305條「恐嚇危害安全罪」：以加害生命、身體、自由、名譽、財產之事，恐嚇他人致生危害於安全者，處二年以下有期徒刑、拘役或三百元以下罰金。
3. 另網友涉嫌侵犯薛女個人隱私部分，薛女則可依〈民法〉求償。

二、經驗教訓

(一) 以上4個案例，讓我們了解「水能載舟，亦能覆舟」，網路的便利性讓許多人忽略了其中可能潛存的各種危險，我們可能在不經意的情況下，因為一小段文字或一張圖片而使自己身陷囹圄，須知網路上的犯罪問題形形色色，一不小心便可能觸犯法律。

(二) 其次，大家在倚賴網路的同時，更應該以正確的態度來看待網際網路可能衍生的許多犯罪問題，例如很多人都會將自己家中多餘的物品上網拍賣，但卻忽略了網路上有很多東西是禁止拍賣的，像菸、酒、醫療器材、情趣用品、統一發票等等，這些東西一旦在網路上拍賣，便可能觸犯「菸害防制法」、「菸酒管理法」等法規，因此大家悠遊在網路時，都應該提高警覺，以避免留下難以抹滅的污點。

(三) 最後，希望大家都能以上述的4個案例為借鏡，除了應知法，更應該守法，唯有大家小心翼翼，恪遵網路的禮儀與規範，才能在浩瀚的網路世界中遨遊。

（作者是淡江高中教官）

▲Top