清流月刊中華民國九十七年十月號

世上沒有完美無瑕的網路防護措施， 因此關乎資訊安全之事必須未雨綢繆。

電腦駭客入侵網路相關模式之分析與防範(下)

◎ 顏榮昌

（接續上期）

九、社交工程攻擊

社交工程(Social Engineering)是一種攻擊行為，即攻擊者利用人際關係間的互動特性，所進行的攻擊法。社交工程攻擊是以影響力或說服力來欺騙他人，藉以獲得有利入侵的資訊，這是近來造成企業或個人極大威脅和損失的駭客攻擊手法。駭客利用社交工程假冒為同事、新進員工、廠商、客戶、政府單位等寄發E-mail，再將病毒與惡意程式隱藏在E-mail中，有系統地實施針對性精準攻擊。當受攻擊目標開啟駭客寄來之E-mail或點選E-mail中的超連結，就可能下載病毒或惡意程式；通常駭客利用電子郵件的社交工程攻擊成功率約80%。

十、擺渡攻擊(行動碟竊密)

目前政府機關防範駭客入侵的主要方法即是採用實體隔離，這種機制是將內部工作網與網際網路隔離，嚴防機密資料外洩；當內、外網電腦間有資料需交換時，再以行動碟(或拇指碟)為媒介傳遞資料。然而目前駭客已運用擺渡攻擊，破解實體隔離的防護機制。駭客擺渡攻擊的方法，是由連結網路的電腦將autorun.inf與ghost.pif(惡魔程式)等擺渡木馬程式植入行動碟中，待行動碟與內部工作網進行資料交換時，擺渡木馬程式立刻感染內網電腦，再將欲竊取的資料下載至行動碟中。完成上述擺渡程序後，只要使用者再將行動碟連接網際網路電腦，被竊取的資料就會自動傳送給駭客。

參、預防駭客入侵之資訊安全作為

雖然沒有一種方法可以保障電腦網路系統百毒不侵，但是遵守「多一分防備，少一分損失」的道理，一定可以使資訊系統多些安全保障。為了抵禦無所不在且技術高超的網路駭客，我們可藉由增加資訊系統入侵困難度的方法，減少系統被入侵的機會。針對預防駭客入侵之資訊安全作為，本文提供之建議如下：

一、重視防火牆(Firewall)、防毒、防駭系統之建置

防火牆是一種保護內部網路免於遭受外力威脅與破壞之裝置，它可以將內部網路隱形，避免未經授權的資料外流。通常防火牆分為硬體與軟體兩種，硬體防火牆強調的是較高的效能，針對作業系統作最佳的防護措施，同時使用防火牆廠商的作業系統，相較於常用的作業系統在安全上的漏洞會比較少。軟體防火牆則是提供較高的彈性與擴充性，通常可以將購買的軟體防火牆安裝在現有的閘道伺服器上，而不需要變更網路架構。另一方面，軟體防火牆也提供最佳的整合性，例如常與防火牆搭配的程式有內容過濾、加解密工具、防毒工具等。一套完整的防火牆至少需要有使用者認證、過濾封包、log分析工具、線上監控等相關功能；因而防火牆的建置是維護網站安全的基本要項之一。

二、加強資訊安全人員教育

由於網路駭客的教育水準及技術愈來愈專業，如果政府組織中負責網路安全的人員，未能持續進修與提升本身的專業素養，絕對難防駭客的入侵與荼毒。為了提升人員之資訊安全警覺，可配合行政院研考會已經擬定及實施的「資訊安全及電腦稽核種子人才訓練計畫」。這項計畫共有5個系列，針對各政府機關負責資訊業務處理的一般人員、政風人員、電腦稽核人員、資訊安全管理人員及網路安全管理人員，進行有計畫的培訓，以提升政府機關資訊安全管理的專業能力。

三、養成良好習慣，避免人為疏忽造成資訊安全漏洞

網路便利後已澈底改變人們郵件的使用方式，通常私人或公務郵件除非真有必要，否則很少使用書面郵件，多改用E-Mail進行溝通。鑒於E-Mail的使用頻繁，為了避免駭客利用E-Mail散布後門程式或電腦病毒，電腦使用者應養成不隨便執行或安裝來路不明之程式的習慣，甚至須強化防毒軟體的功能，使網路多一層防護，同時需要定期更新防毒軟體的病毒碼。

另外，儘量不要使用懶人或傻瓜密碼，例如用生日、身分證字號、電話號碼等容易讓有心人士猜到的文字或數字當密碼，以免個人系統遭到駭客入侵及破壞。再好的系統安全政策都難防人為的疏失，高明的駭客很可能會因為系統管理者一時的疏忽而入侵系統，任何使用者也可能只因未遵照資訊安全的規範，而成為駭客的跳板。所以疏失往往是駭客入侵成功的最大原因。

四、使用監控及掃描程式保護系統安全

負責資訊安全的資安人員必須經常監控資訊系統或網路流量是否有異常狀況，才能適時發現網路安全問題與解決問題。通常使用系統掃描程式或網路監聽程式，可以對網路中的封包進行攔截，並分析這些封包及流量對網路內主機是否有不正常的影響，然後做出適當的反應。因此使用監控及掃描程式是資訊安全負責人員必備的知識與技能。

五、實體隔離、多層次聯合防禦

貫徹執行「實體隔離」作為，重要資料庫或內部工作電腦不與網際網路連線，以降低被入侵破壞的機會。現階段許多政府機關均已採取實體隔離的措施，一般內部作業的電腦不能與網際網路連結，只連結內部網路(Intranet)；如需上網查詢資料或與外界通聯，則使用無任何機密資料的電腦上網。只要釐清資訊與機密的界線，便知此作為不是向駭客低頭，而是一項較消極卻有效的安全防護措施。此措施主要是將作業使用的網路區隔為：

(一)可對外連線的Internet(網際網路)

此網路系統僅供上網查詢資料、一般性資訊發布及非機密性資料的連結。如涉及機密性且必須與外界交換的資料，則應採取資料加密、身分鑑定、數位簽章與數位認證等機制，防止資料被竄改、刪除或破壞。

(二)僅供內部連線用的Intranet(內部網路)

政府機關中許多單位有關公務使用之辦公室自動化系統即屬此類型。此網路系統僅供企業或政府機關內部應用與服務的存取，也就是此系統只在組織內部作連結，無法與外部網路通聯，且擷取資訊限特定身分與存取地點，機密保護程度較佳。

(三)封閉性網路：

此系統為部分企業或政府機關間特定的通訊管道，必須透過「VPN」或專屬的網路才能進行資料交換；此類網路現有警政網路與國防部軍網等。

肆、結 論

隨著資訊科技的蓬勃發展，網路這項人類歷史上的新科技被應用的情形日漸普及，各種不同的應用及經濟活動正逐漸移轉至網路平台，依賴網路通訊的程度也日益加深，各機關、組織運用網際網路蒐集資料與便民服務的機會亦更形增加，甚至連軍隊的指揮管制、通訊情報系統都可能透過網路來連結，此舉勢必會產生越來越多的網路安全問題。據統計全球平均每20秒就發生一次網路入侵事件，有近80%的企業或機關至少每週在網路上要被大規模入侵一次，遑論如陸委會、國防部、國安局與總統府等重要的政府機關，被入侵次數更難數計。

雖然機關、組織或私人企業在推動資訊e化的過程中，為確保資訊品質及資料的完整與真實性，多少都已建置了相關之控管與防護措施。但世上沒有完美無瑕的網路防護措施，因此關乎資訊安全之事必須未雨綢繆，建立資訊安全的稽查與緊急處理機制，以發揮事前預防、偵測，事中監督及事後有效處理的功能。然資訊安全管理工作是否落實執行，必須建立獨立的網路資訊稽查機制，由客觀的資訊稽查人員，持續評估組織推動資訊安全的實施績效，以確保資訊安全管理機制之落實執行。

過去網路安全的概念往往是從上而下(從主機到個人電腦)，所以個人的網路安全防護反而是最脆弱；但當進入網際網路時代後，每個網路使用者都是網路上的一個節點(Node)，任一節點的破壞都可能造成整張資訊安全網的破損。從各種統計資料及實務經驗顯示，人為疏失、員工缺乏安全警覺，不了解網路安全問題的嚴重性，是網路安全出現嚴重缺口的重要原因之一。任何安全系統中最薄弱的一環通常是人，在各種資訊安全的防護策略中，投資報酬率最高的反制入侵對策，便是對組織員工進行警覺訓練與提高安全防護責任感。如所有人都對個人資訊安全抱持警戒態度，將有助於組織建立重視網路安全的組織文化，且其產生的正面效應將出人意表。

（作者是國立空中大學人文學系兼任講師）

▲Top

不重視資安防護問題， 會被敵人操弄於股掌之中。

資安防護是未來安全第一關鍵

◎ 王駿傑

日前美國《國防週刊》報導，美國北美防空司令部司令雷諾瓦特指出，美國下任總統可能面臨的新挑戰，其中之一是網際網路的安全威脅。另外，美軍聯參「資訊首席」的指管通資處長陸軍准將勞倫斯說：「美軍可在傳統戰場上輕鬆面對敵人，但是面對虛擬世界的敵人，則是一項嶄新的挑戰。」的確，在現實的社會，美軍擁有全世界最先進的科技與武器，可以在戰場上無懼敵人的威脅。但是，在網路的世界中，恐怖分子可自世界上任何地方、任何環境，並在十億分之一秒內及一天二十四小時的任何時段中發動攻擊，完全超脫了時間與空間、天時與人為的限制因素，而其策動的人力，可能僅僅只有一人，就能癱瘓某一國家的整個國防體系。所以，在如此打破比例原則的新世紀戰爭中，勞倫斯將軍也承認，如果不積極投注於資訊安全防護，就連美國恐也無法打贏全球的反恐戰爭。

美軍全球網路作戰聯合任務小組技術主任杭特上校也說：「美軍在全球資訊及網際網路方面的通信能力，基本上非常薄弱，甚至是不堪一擊。」從911事件中，恐怖分子運用網路探勘（Internet Mining），就能得到全美的飛機航線與時刻表；另從五角大廈每天有超過五百次以上的網路攻擊觀之，就可看出資訊攻擊是恐怖分子最有利的投資。而美國國防部在2005年向國會提出的中共軍力報告中也顯示，目前包含中共及北韓等二十多個國家，已經發展出專用的電腦攻擊程式。所以，美軍聯參指管通資系統次長施亞中將（Robert Shea）說道：「網路是美軍未來發展的重心，如不然，網路防禦能力將是強大美軍的致命弱點。」未來各國如不能重視資安防護問題，將無法在未來戰場上獲得主導權，並喪失戰略之有利態勢，最後恐會被敵人操弄於股掌之中。

資訊安全必定是未來戰爭勝負與國人安全的致勝關鍵。全體國人必須體認這種趨勢，隨時要求自己做到：

一、加強充實新知，提升資安防護概念：

據統計目前網路上已經超過一百萬個教導製造電腦病毒及訓練成為電腦駭客的網站。而有別於傳統武器的研發與製造，電腦病毒及攻擊程式不需要投入大量資金，也沒有政策限制，所以人人都能隨時隨地發動資安攻擊，而電腦病毒也已超過百萬種。如果不能時時更新資安防護措施，並認識新種的電腦病毒及駭客手法，便可能成為駭客下一個覬覦的對象。

二、培養保密習性，確遵資安政策指導：

資訊安全漏洞，有80%是來自於人為的破壞與疏忽，所以最有效的資安防護政策，還是要個人養成良好的保密習性、貫徹實體隔離政策、不將機密資訊儲存於電腦中、關閉不必要的分享設定、不下載來路不明的軟體，及使用加解密軟體，更重要的是，不要將機密資訊帶離作業區或公務家辦，才能將資安風險降至最低。例如，日前美軍退伍軍人事務部由於員工將不應持有的機敏資訊帶回家，使得美國大筆退伍軍人的個人資料外洩，讓美國數百萬的退伍軍人暴露於危險之中，成為美國史上最重大的資安漏洞，令人不得不深切檢討及採取更充分的資安防護措施。

三、貫徹資安查察，建立網路巡查機制：

警政署科技犯罪防制中心主任李相臣在近期的演講中表示：「企業網路定期實施網路巡邏、分析警示與異常網路流量，才能有效控管資料外洩及資訊攻擊的風險。」資訊安全是一項必須拋開空間思維的工作，因為內部人員不一定要在辦公室裡，才會對公司的資訊安全造成破壞，有可能是在家裡，也有可能在公車上或是世界的某個角落，而時間上更是不分晝夜。所以，培養資管人員、設立專職資安人力，是未來企業及犯罪防制的目標；政府各階層也應儘速成立專責的資訊部門，推廣資安教育，專司網路巡查及監控，才能確保資訊能量，適時防堵資訊攻擊。

孫子兵法指出：「兵貴勝，不貴久。」現代戰爭形態的重要特色就是講求時效，因此，不只一般企業，甚至國防事業對於資訊科技的需求都將日益增加。近年來「資訊安全」已是世界各國演習及全民保防教育的重點，各國對於軍人乃至國民的資安要求也往往立法規束，因為在未來戰場上，資訊攻擊除了會造成社會動亂之外，如果建置有C4ISR系統（即軍事指揮系統之統合，包括指揮、管制、通信、資訊、情報、監視及偵查），敵軍可以使用電磁脈衝武器，破壞對方整個作戰系統，另外也可以發動網路病毒癱瘓對方指揮與通訊系統，降低其聯合作戰的武力，阻礙其後勤支援體系，分化其國家與社會精神戰力的凝聚，最後入主對方之中央指揮體系，不費吹灰之力，解除其國防武力，瓦解其國家安全。

總而言之，再完善的資安規定，若國人不能建立資訊保密之安全共識，並提高保防警覺，縱使有再高階的防火牆、防毒軟體及複雜的鎖鑰，都抵不住人員的一個小失誤與蓄意洩漏。唯有大家依據國家資通機構的安全政策指導，安裝各項資安軟體與養成保密設定的習性，並嚴加保守個人的帳號與密碼，且不定時更新，才能由內而外地強化資訊安全的維護，鞏固國家整體安全。

▲Top

稽徵效能之提升，並非建立在稽徵機關強勢的公權力上， 而是建立在人民的信賴與信服。

淺論比例原則於稅務案件之適用

◎ 陳炎輝

壹、導論

我國憲法第19條規定：人民有依法律納稅之義務。司法院大法官對此稱為租稅法律主義，惟何謂租稅法律主義？大法官首先於釋字第217號解釋指出：係指人民僅依法律所定之納稅主體、稅目、稅率、納稅方法及納稅期間等項而負納稅之義務；至於課稅原因事實之有無及有關證據之證明力如何，乃屬事實認定問題，不屬於租稅法律主義之範圍。嗣後大法官並於釋字第415號解釋指明：係指稅捐主體、稅捐客體、稅基及稅率等稅捐構成要件，均應以法律明定之。綜上申言之，租稅法律主義之內涵包括：課稅要件法定原則、課稅要件明確原則、合法性原則、稅法不溯及既往等原則。

對於租稅法律主義，大法官於95年12月29日作成釋字第622號解釋再度闡明：係指國家課人民以繳納稅捐之義務或給予人民減免稅捐之優惠時，應就租稅主體、租稅客體、稅基、稅率、納稅方法及納稅期間等租稅構成要件，以法律明文規定。是應以法律明定之租稅構成要件，自不得以命令為不同規定，或逾越法律，增加法律所無之要件或限制，而課人民以法律所未規定之租稅義務，否則即有違租稅法律主義。綜合大法官解釋意旨，稽徵機關核課稅捐不得違反租稅法律主義，如有違背者，納稅人自可拒絕繳納。

稅捐核課具有強制性與無償性，憲法及租稅法規誡命人民負有繳稅之義務，等同強制剝奪人民財產權，已涉及憲法第15條人民財產權之保障。再者，納稅人如滯納稅捐，稽徵機關亦得依法予以限制出境，此更關聯憲法第10條人民居住及遷徙自由之保障。國家徵收稅捐乃係強制性公課，追求的是負擔之正義，而非交換之正義；對於脫法規避租稅、違法逃漏稅捐，破壞租稅正義及負擔公平之行為，自有加以處罰之必要。惟憲法第23條亦明定，國家欲拘束或限制人民之自由或權利，甚至加以處罰時，均須法有明文且必要者為限，除適用法律保留原則外，更有比例原則之適用。

貳、比例原則之理念內涵

我國憲法第23條明定：「以上各條列舉之自由權利，除為防止妨礙他人自由、避免緊急危難、維持社會秩序或增進公共利益所必要者外，不得以法律限制之。」學者認為本條所定之除外規定，乃係基於公益原則而設。又本條所用「不得以法律限制之」乙詞，學者認為此係法律保留原則之規範；而所謂法律保留原則，又稱為積極的依法行政原則，指行政機關若無法律之依據，便無從作成合法的行政行為。法律保留原則於稅務案件，即前述所稱之租稅法律主義，正如罪刑法定主義適用於刑事案件。至於本條所用「必要」乙語，學者認為此乃比例原則之淵源；在比例原則規範下，國家權力包括行政、立法及司法等之行使，均有比例原則之適用，要求國家之行政、立法及司法行為，其手段與所欲實現之目的間，須有合理之比例關係，現今更是防止國家權力濫用之「法治國家原則。」

比例原則源自於德國法制，其內涵在於嚴格禁止國家為達目的而不擇手段。比例原則乃是「目的與手段」間之衡量，在公法領域廣泛被研討運用，並經大法官承認具有憲法位階。是以納稅人如對核定稅捐之處分不服，認其所依據之租稅法規或解釋函令，有違反比例原則之疑慮時，得依法提起行政救濟（復查、訴願、行政訴訟），並於取得確定終局裁判後，依司法院大法官審理案件法第5條第1項第2款：「人民、法人或政黨於其憲法上所保障之權利，遭受不法侵害，經依法定程序提起訴訟，對於確定終局裁判所適用之法律或命令發生有牴觸憲法之疑義者。」之規定，檢具聲請書及關係文件，依同法第8條第1項規定，聲請大法官解釋。

比例原則本屬一般法律原則，在行政程序法實行前，我國法規原無明文之規定，惟最高行政法院83年度判字第2291號判決曾指出：行政機關對違反行政法規之行為，於行使裁量權決定應為何種程度之裁罰處分時，除應遵守一般法律原則（如誠信原則，平等原則、比例原則等是）外，應符合法規之目的，並不得逾越法定之裁量範圍，此為行政法理所當然。其中所稱之比例原則，係淵源於憲法上法治國家思想之一般法律原則之一種，具憲法層次之效力，故該原則拘束行政、立法及司法等行為。因而，行政機關於選擇達成行政目的之手段時，其所作成之行政處分必須符合比例原則，換言之，除該行政處分須最適合於行政目的之要求，並不得逾越必要之範圍外，尚須與欲達成之行政目的間保持一定之比例，始足當之。否則，即屬濫用權力之違法。

參、稅務案件發生之實例

納稅人違反稅法規定所受之處罰，有因逃漏稅捐所受之漏稅罰，例如所得稅法第110條規定：納稅義務人已依本法規定辦理結算申報，但對依本法規定應申報課稅之所得額有漏報或短報情事者，處以所漏稅額2倍以下之罰鍰（第1項）。納稅義務人未依本法規定自行辦理結算申報，而經稽徵機關調查，發現有依本法規定課稅之所得額者，除依法核定補徵應納稅額外，應照補徵稅額，處3倍以下之罰鍰（第2項）。由此可知，漏稅罰係就逃漏稅捐之金額，處以一定倍數之罰鍰，處罰金額並非無所限制。

納稅人違反稅法規定所受之處罰，尚有因違反稅法上之作為或不作為義務而受之行為罰，例如所得稅法第108條第1項原規定：納稅義務人違反第71條規定，未依限辦理結算申報，但已依第79條第1項規定補辦結算申報，經稽徵機關據以調查核定其所得額及應納稅額者，應按核定應納稅額另徵10%滯報金。滯報金之金額，不得少於1,500元。其中「加徵滯報金」係對納稅人違反作為義務所為之制裁，乃罰鍰之一種，具行為罰性質，其違規情節有區分輕重程度之可能與必要，自應根據違反義務本身情節之輕重程度為之。惟本項規定於納稅人已繳清稅款之情形下，行為罰仍依應納稅額固定之比例加徵滯報金，又無合理最高額之限制，已逾越處罰之必要程度，有違憲法第23條比例原則，並與憲法第15條保障人民財產權之意旨牴觸，大法官遂於95年9月15日作成釋字第616號解釋指出：應自本解釋公布之日起，至遲於屆滿一年時，失其效力。該法條遂於96年7月11日修正為滯報金最高不得超過3萬元，最低不得少於1,500元。

在我國尚未加入世界貿易組織（ＷＴＯ）前，前臺灣省公賣局產銷之米酒，在長期菸酒專賣、價格平穩之制度下，成為國人日常民生必需之消費

品，嗣後因菸酒專賣改制與加入世界貿易組織，廠商與民眾預期米酒價格將大幅上漲，又因國人料理習俗與飲食習慣，一時難以更易，故民間出現囤積爭購行為，造成市場混亂，消費者權益受損。為此91年1月1日施行之菸酒稅法第21條乃明定：「本法施行前專賣之米酒，應依原專賣價格出售。超過原專賣價格出售者，應處每瓶新臺幣2,000元之罰鍰。」

惟查本條之規定，純粹以單一標準來區分違規情節之輕重，並據以計算罰鍰金額；此種劃一之處罰方式，經大法官於97年4月18日作成釋字第641號解釋指出：於個案之處罰顯然過苛時，法律未設適當之調整機制，對人民受憲法第15條保障之財產權所為限制，顯不符妥當性而與憲法第23條之比例原則尚有未符，有關機關應儘速予以修正，並至遲於本解釋公布之日起屆滿一年時停止適用。

肆、結語

我國行政程序法業於90年1月1日施行，其中第7條規定：行政行為，應依下列原則為之：一、採取之方法應有助於目的之達成。二、有多種同樣能達成目的之方法時，應選擇對人民權益損害最少者。三、採取之方法所造成之損害不得與欲達成目的之利益顯失均衡。本條乃係比例原則之明文規範，屬於抽象之概念。學者認為在此概念下，尚涵蓋下列三項子原則，第一為適當性原則：指行政機關所採取者必須是有助於達成目的之措施，又稱合目的性原則；第二為必要性原則：指行政機關有多種措施均可達成目的時，應採取對人民侵害最小者為之，亦稱侵害最小原則；第三則為狹義比例原則：指行政機關所採取的行政措施，和欲達成的目的之間，應有相當之平衡，不能為達成很小之目的而使人民受很大損害，即手段和目的之間，其所存在之損害比例須相當。

稽徵機關肩負籌措國家財源任務，稅務人員莫不致力於提升專業素養與稽徵效能。惟稽徵效能之提升，並非建立在稽徵機關強勢的公權力之上，而是建立在人民的信賴與信服。蓋稅捐稽徵如未能獲得人民信任，極易招致納稅人無窮盡的抗爭及爭訟，如此勢必無法順利徵得稅款解繳國庫，更將產生許多無謂的行政訴訟案件，徒然耗費有限的行政及司法資源。是以稽徵機關核課稅捐，除應遵循依法行政原則外，基於比例原則，倘有多種同樣能達成稅收目的之方法時，更應選擇對人民權益損害最少的方案為之。

以海關緝私條例第36條規定：「私運貨物進口、出口或經營私運貨物者，處貨價1倍至3倍之罰鍰（第1項）。不知為私運貨物而有起卸、裝運、收受、貯藏、購買或代銷之行為，經海關查明屬實者，免罰（第4項）。」而言，對於私運行為係處以罰鍰及沒入私運貨物之處分，但對於不知私運貨物而購買之行為，因欠缺具備責任要件為論罰之依據，因此海關實務上，乃依第4項之規定而免予處罰。財政部基於比例原則，考量保障交易之安全，與保護善意之第三人；為兼顧交易安全之保障與行政目的之達成，乃於 89年10月18日 發布台財關第890062310號函示：「不知為私運車輛而購買並經交付取得所有權者，若該私運貨物非屬違禁品或管制物品，宜同時免除購買人之罰鍰及貨物沒入處分；反之，對於私運行為人部分，則在法定裁量權之範圍內加重處罰，以懲治其私運行為之惡性，亦能達到同樣之行政目的。」即為實證。

（作者是財政部臺灣省中區國稅局法務二科審核員）

▲Top

祇要竊嫌使用過被害人的手機，電信警察即可調閱雙向通聯記錄進行分析比對。

手機遭竊時如何尋回

◎ 許宏揚

壹、導論

在網路瀏覽知識網時，偶然看到網友回答「手機使用及遭竊時怎麼辦？如何尋回？」等相關問題，且非常熱心地提供手機遭竊時之尋回方法，大致上是可循其方法找回，但在細節須知、專業領域方面，則須再深入研究與了解，被害人才能有效維護自我權益。本人曾在電信警察隊服務，可將累積之經驗提供讀者分享與參考，一旦發生類似情形，能對被害人有所助益，並從容解決所面臨的窘境與困惑。

首先讀者應了解手機的身分證IMEI(位於手機盒子的側方，會有一組IMEI的數字，即通稱手機序號，俗稱手機的身分證），當手機在開機、使用的狀態下，按下「*#06#」時所浮現的15個阿拉伯數字，便是所謂手機的身分證IMEI，亦稱「序號」，例如：01234-56789-12345。何為IMEI碼？IMEI（International Mobile Equipment Identity）為TAC＋FAC＋SNR＋SP，是國際移動設備身分碼的縮寫，是由15位數字組成的「電子串號」，為國際移動裝備辨識碼；它與每支手機一一對應，而且該碼是全世界唯一的。每一支手機在組裝完成後都被賦予一組全球唯一的號碼，這組號碼從生產到交付使用，都將被製造生產的廠商所記錄。其組成為：前6位數（TAC）是「型號核准號碼」，一般代表機型；接著的2位數（FAC）是「最後裝配號」，一般代表產地；之後的6位數（SNR）是「串號」，一般代表生產順序號；最後1位數（SP）為檢驗碼。

臺北市警察局中山分局追查北臺灣某連續汽機車和民宅竊盜、搶奪案時，曾根據其中一名被害人遭竊的手機IMEI序號和一枚指紋而破案。然而，每支手機之型號、廠牌、顏色，皆有所不同，就如同汽車一般，辨識的特徵與方式迥異；目前所使用的雙頻手機，幾乎都是一機一卡，甚至一機雙卡（目前只支援2G SIM卡，不支援3G），有別於以往單頻內建無插卡手機，係透過雙證件所申請的SIM卡（SIM卡上有20位數碼，前面6位＜898600＞是中國的代號；第7位是業務接入號，在135、136、137、138、139中分別為5、6、7、8、9；第8位是SIM卡的功能位，一般為0，現在的預付費SIM卡為1；第9、10位是各省的編碼；第11、12位是年號；第13位是供應商代碼；第14～19位則是用戶識別碼；第20位是校驗位，故行動電話搭配植入SIM卡，始可撥打付費）。民眾在手機或SIM卡遭竊時，往往會擔心遭盜撥或盜（冒）用時，衍生複雜的刑事問題，及自我權益受損與連帶不必要的麻煩等等，困擾著當事人而舉足無措；然而，若接收不正確資訊而求助於人，反而愈幫愈忙，不可不審慎為之。以下幾點做法可供被害人確定手機遭竊或不慎遺失當時的前置作業參考：

1. 被害人若已確定手機遭竊或不慎遺失時，首先須向所申請通話的電信公司辦理停話，以免因手機遭盜撥或盜用而需支付龐大的話費（無法舉證時），這是最基本的觀念，亦是最重要的做法。

2. 其次是備妥個人身分證明文件及手機之序號、門號等等相關資料，加以整理、存檔，建立備忘錄，做好先前準備工作，俾於向警方備案及製作調查筆錄時，順利應答警方可能詢問之問題，藉以縮短所需時間與流程，亦可當作將來出庭作證時之有利佐證資料；另一方面則可作為保護自己、維護本身權益的法寶。茲將重點整理如下：
    a. 首先準備用戶本人或代理人年籍資料。
    b. 確認行動電話是否為本人名義申請及使用。
    c. 何時、何地、置於何處、如何發生、有無遭盜撥電話等問題，明確、清楚、詳實地提供警方作為辦案參考。
    d. 手機遭竊時有否含門號？有否植入SIM卡？手機遭竊時門號為何？有否遭人盜撥或盜用？
    e. 確認遭竊或遺失之手機是何種廠牌、型號、顏色、序號等資訊，必要時可上網下載相關圖檔或資訊備份，在備案時可提出案件發生經過之相關線索，以為警方偵辦時之佐證參考。
    f. 遭竊或遺失之手機現價大約多少錢？有無向電信公司辦理停話？

綜言之，無論一般（普通）或重大刑事案件，向當地、發生地或結果地之司法警察單位（警察局、分局或派出所）報案後，持報案三聯單正本（報案三聯單切勿丟失）至電信警察隊再次備案（流程大同小異）確認；經錄案、分案調查後，祇要竊嫌使用過被害人的手機，即可透過電信警察向國內電信公司調閱雙向通聯紀錄進行分析比對，或依據手機序號（IMEI）反求相關資料。若查有可疑人士（即嫌疑人）的發話地點及顯示之行動電話號碼，會進一步通知嫌疑人到案說明，並追查嫌疑人身分及盜用行動電話號碼情形，藉以釐清案情。經偵查詢問完畢，確認無訛後，會將所調閱之雙向通聯紀錄及贓證物（如被害人手機）、手機圖檔、盜撥或盜用所產生的話費明細表等明確事證，對竊嫌提出竊盜罪告訴，甚至通訊行業者若牽涉其中，必要時將一併提出收受贓物罪告訴。全案偵結完畢將相關事證移送地檢署偵辦，贓物（所找回的手機）入庫後，經地檢署起訴，法院判決確定後，自然會通知當事人，依程序前往法院領取所找回的手機。

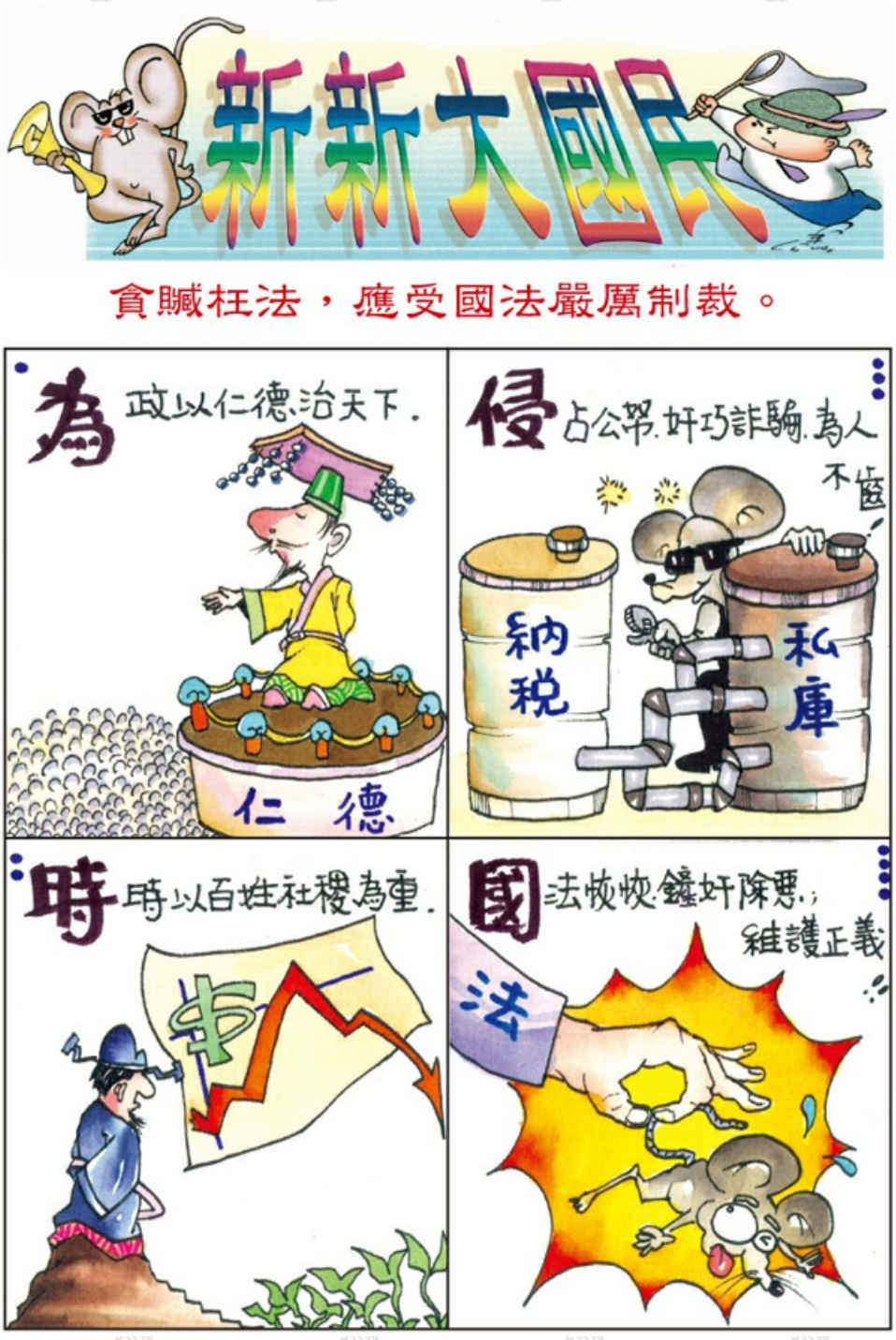
（作者為保五總隊分隊長）

▲Top

保防漫畫

◎本　社

貪贓枉法，應受國法嚴厲制裁



保防短語

專屬機密不能說，事涉安全不能寫，觸法犯規不能做

事屬機密不能說，事涉安全不能寫，觸法犯規不能做。

▲Top