序

網際網路為人類帶來美麗新世界的光明憧憬，但是伴隨而來的網路安全、網路犯罪、隱私保護及智財權保護等問題，已使網際網路逐漸成為影響國家安全、經濟穩定及社會安定的另一項隱憂。有鑑於此，我國政府特成立「行政院國家資通安全會報」，除協調各部會落實資通安全施政優先項目外，並以實際行動強化資安法治觀念，強化政府部門對資通安全重要性之意識及認知。

「行政院國家資通安全會報技術服務中心」（以下簡稱技服中心）自 91 年起已發行 5 冊「資通安全法律案例彙編」。此彙編透過對相關案例的分析與學習，幫助政府部門及社會大眾建立網路環境應有的法治概念及安全意識，並進而達成預防網路犯罪之目標。在「行政院國家資通安全會報」舉辦的各類資安宣導與推廣訓練活動中，此彙編之推廣發行普獲好評，政府機關 (構) 爭相索取運用，使「技服中心」深感持續推動此項工作之重要性。

此次 98 年編印之第六冊「資通安全法律案例彙編」，「技服中心」期待能有與以往不同的變化，故將內容概分為「資訊保護」、「資訊公開」、「資訊監察」及「資訊應用」等四個主軸鋪陳，並由「技服中心」委託「國巨律師事務所」蒐集近一年來發生之資安時事新聞與法院實際案例。內容除保持深入淺出的法律觀點與說明傳統外，更創新將內容與 CNS27001(資訊安全管理系統) 之概念相結合，相信此彙編必能成為政府機關及社會大眾學習資訊安全管理時最佳之參考教材之一。

行政院國家資通安全會報技術服務中心

劉培文主任　謹識

編者序

資訊安全議題在行政院研考會的推動下，在政府部門領域已經卓然有成。同時，為了推展與教育資訊安全意識，行政院國家資通安全會報技術服務中心（以下簡稱「技服中心」）歷年來共編輯了五冊的「資訊安全案例彙編」手冊以供社會各界參考，成效斐然。

此次第六冊「資訊安全案例彙編」委由「國巨律師事務所」負責編撰，內容概分為「資訊保護」、「資訊公開」、「資訊監察」與「資訊應用」等四個主軸，再以這四個主軸，將資訊安全相關法律予以分類，並蒐集近年來的時事新聞與法院實務個案，讓這些法律透過實際生活的報導與觀點差異，提供具有動態面的法律詮釋。

在版面的設計上，以「焦點話題」說明時事新聞、判決事實基礎或要旨。同時，摘錄出當篇「重點摘要」讓讀者迅速掌握閱讀重點，並配合法律分析內容，以「法律觀點」將相關法令與簡易法律分析意見讓讀者參考。值得一提的是，為了讓讀者熟悉個案事實，更精要點出資訊安全管理之控制措施，在每篇相關法律內容上參考 CNS27001（資訊安全管理系統）附錄 A 的管理要項，以「管理 Tips」方式呈現予讀者參考，而此部分特別情商資誠企業管理顧問股份有限公司蔡興樺協理協助提供資訊。

本次出版之第六冊「資通安全法律案例彙編」，藉由不同的呈現方式以及實務案例，希望達到協助政府推動資訊安全意識，並整合不同面向的法律，讓讀者從更多元的角度認識不同層面的資訊安全議題。

最後，以本彙編所建構的資訊安全法律架構，期待可以作為未來建立資訊安全法領域的檢證基礎，讓讀者以此基礎延伸學習興趣並認識整體資訊安全法律面貌。

國巨律師事務所

朱瑞陽律師　謹識

凡　例

壹、本案例彙編分為以下類別：

一、資訊保護（Security）

01 電腦處理個人資料保護法

02 國家機密保護法

03 營業祕密法

04 刑法

二、資訊公開（Disclosure）

01 政府資訊公開法

三、資訊監察（Monitors）

01 通訊保障及監察法

四、資訊應用（Application）

01 電子簽章法

貳、本案例編碼共 7 位數字：編碼方式以上述四大類別之英文字首為第一碼，再加上年份及上述各小類之編碼各兩碼，最後兩碼為該小類中之第幾篇案例。例如：S970101，即代表資訊保護類 97 年度之電腦處理個人資料保護法第一則案例。

資通安全法律案例宣導彙編

【目錄】

壹、資訊保護
（Security）

醫院可以將員工的健康檢查報告提供給雇主參考嗎？

【案號：S970101】
資料來源：法務部 96/01/05 法律決字第〇九五〇〇四六二二一號公告

焦點話題

常看到企業與醫院或診所合作提供員工健康檢查的福利。這個健康檢查的福利，除有法律規定[1]雇主應於就職或在職一定期間[2]提供健康檢查外，並要求該檢查報告要讓員工知悉，以讓員工知道自己的身體狀況。通常健康檢查報告都是由醫院直接通知，並且採取一定程度的保護措施以避免個人健康狀況遭外洩而影響個人隱私。

至於雇主如果想要知道員工的健康檢查狀況，是否必須要經過員工書面同意後，醫院才可以將檢查結果通知雇主？

重點摘要

1. 醫院是屬於「電腦處理個人資料保護法」（以下簡稱「個資法」）之適用行業，因此對於個人資料必須謹慎保護確認個人資料的安全。
2. 雇主所依法提供予員工的健康檢查福利，費用由雇主負擔，是否可以要求醫院將員工健康檢查狀況通知雇主是本案爭議的焦點。
3. 至於非雇主提供的健康檢查結果，原則上員工並沒有通知雇主的義務。

法律觀點

醫院是屬於「個資法」所規範適用的行業[3]。因此對於個人資

料檔案的電腦處理、蒐集或利用均必須符合「個資法」的要求。以本案為例，醫院是受雇主委託提供員工健康檢查，其因此而取得的個人資料檔案，除通知員工外，是否可以提供予雇主參考？在前述的勞工安全衛生法與勞工健康保護規則的相關規定，僅有提及雇主有義務付費提供員工此項健康檢查福利並且也要求雇主必須建立員工健康手冊，惟並未提及雇主是否可以要求醫院或員工提供該項健康檢查結果。以致當雇主要求醫院提供員工的健康檢查報告時，是否需要經過員工書面同意，就產生法律解釋與認定上疑義。

就這點，「個資法」的主管機關法務部認為，「個資法」第 23 條規定[4]，非公務機關對個人資料之利用，應於蒐集之「特定目的」必要範圍內為之。除有但書之情形外，不得為「特定目的」外之利用。因此，如醫院其所蒐集的個人資料是在「特定目的」範圍內利用，即屬適法。而所稱「特定目的」，法務部認為本案「體格檢查或健康檢查係法律強制規定雇主須為勞工辦理之項目，且雇主應負擔健康檢查費用，並須將檢查結果發給受檢勞工，則醫療機構將蒐集之受檢勞工個人資料提供雇主依法辦理相關事項，應屬『特定目的』內之利用而符合第 23 條本文規定」。換言之，醫院依據雇主委託辦理員工健康檢查是雇主基於法規上的義務。就該檢查報告提供予雇主參考是屬於該資料利用的「特定範圍」內。因此，醫院是不用經過員工書面同意即可將該健康檢查報告提供予雇主參考。如果個人資料的蒐集或利用，不是在「特定範圍」內，就必須在徵得當事人書面同意或有「個資法」第 23 條但書所規定的事由始得為之。

管理 Tips

1. 應依據法令、法規、契約及營運要求，保護重要紀錄，免於遺失、毀損或偽造（CNS 27001 附錄 A.15.1.3）。
2. 應如同相關法令、法規及若適用的契約條文所要求的，確保資料的保護與隱私（CNS 27001 附錄 A.15.1.4）。

資訊保護

一、電腦處理個人資料保護法

註釋：

[1] 勞工安全衛生法第 12 條規定：「雇主於僱用勞工時，應施行體格檢查；對在職勞工應施行定期健康檢查；對於從事特別危害健康之作業者，應定期施行特定項目之健康檢查；並建立健康檢查手冊，發給勞工。

前項檢查應由醫療機構或本事業單位設置之醫療衛生單位之醫師為之；檢查紀錄應予保存；健康檢查費用由雇主負擔。

前二項有關體格檢查、健康檢查之項目、期限、紀錄保存及健康檢查手冊與醫療機構條件等，由中央主管機關定之。

勞工對於第一項之檢查，有接受之義務。」

[2] 勞工健康保護規則第 11 條：「雇主對在職勞工，應就下列規定期限，定期實施一般健康檢查：

一、年滿六十五歲以上者，每年檢查一次。

二、年滿四十歲以上未滿六十五歲者，每三年檢查一次。

三、未滿四十歲者，每五年檢查一次。

前項一般健康檢查項目依前條規定辦理。

第一項健康檢查紀錄應參照格式三為之，並至少保存十年。

第一項之檢查期限，中央主管機關認有必要時，得調整之。」

[3] 電腦處理個人資料保護法第 3 條第一項第 7 款：「非公務機關：指前款以外之左列事業、團體或個人：

（一）徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。

（二）醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。

（三）其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。」

[4] 電腦處理個人資料保護法第 23 條：「非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之。

但有左列情形之一者，得為特定目的外之利用：

一、為增進公共利益者。

二、為免除當事人之生命、身體、自由或財產上之急迫危險者。

三、為防止他人權益之重大危害而有必要者。

四、當事人書面同意者。」

購物被詐騙，疑個資遭外洩

【案號：S970102】
資料來源：聯合晚報 97/09/22

焦點話題

65 歲的鄭姓單身老翁 3 個月前透過「某電視購物頻道」買了一台 46 吋的液晶電視，結果上個月底接到自稱是某購物客服人員電話，指稱他信用卡扣款有問題，歹徒甚至利用網路越洋電話竄改「來電顯示」，致被害人誤信是銀行人員來電，前前後後共匯款 11 次，歹徒還佯稱是警官登門詐騙。

單身且獨居的鄭姓老翁就這樣被詐騙集團耍得團團轉，卻苦無親友商量，當歹徒再來電要他交出 200 萬元，鄭姓老翁懷疑歹徒以手機搖控他的行動，於是把歹徒要求他將存款提交「監管帳戶」一事，寫在提款單上，偷偷地塞給銀行行員時，機靈的行員馬上要他把手機關掉，並告訴他：「你被騙了！」，鄭姓老翁才驚覺被騙上當。「165 反詐騙專線」指出，上周受理詐騙報案總數為 916 件，其中「購物個資外洩而遭詐騙」的案件即高達 625 件。

重點摘要

1. 電視購物頻道雖然目前尚不屬於「電腦處理個人資料保護法」（以下簡稱「個資法」）之適用行業，然而對個人資料仍必須謹慎保護，以確認個人資料的安全。
2. 若購物頻道未謹慎保管客戶之個人資料而外洩者，對於客戶因被詐騙而受損失，仍應負起法律責任。

法律觀點

「電視購物頻道」目前尚不屬於「個資法」所規範適用的行業[1]，亦即不屬所謂對個人資料之蒐集或電腦處理之非公務機關，因此其

對於個人資料檔案的電腦處理、蒐集或利用，尚不適用「個資法」之規範。然而電視購物頻道業者，擁有大量的會員資料，卻常常因為保管不慎或是內部人員的控管不當，而發生會員資料外洩的情形，導致讓詐騙集團利用會員與交易資料進行詐騙，受害者不計其數。

目前對於購物頻道業者之會員資料洩漏，僅能先以民法侵權行為規定[2]求償，但是受害人必須舉證購物頻道業者的過失還有受損害的金額，因此求償並不容易，所以在「個資法」修法前，「個資法」的主管機關法務部，正研議透過指定的方式，將購物頻道業者納入「個資法」規範的範圍內。

而若是購物頻道納入「個資法」的規範後，依「個資法」第 23 條本文前段規定，非公務機關對個人資料之利用，應於蒐集之「特定目的」必要範圍內為之，若購物頻道業者違反「個資法」規定，致他人權益受損害者，即應負損害賠償責任[3]。因此，對於購物頻道業者外洩客戶個人資料之情形，受害的當事人就可以依照「個資法」的規定，向購物頻道業者求償。

但是目前「個資法」規定之賠償範圍是有上限的，原則上以每人每一事件新臺幣 2 萬元以上至 10 萬元以下計算，而基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣 2,000 萬元為限[4]。因此對於有多數人受害時，賠償金額往往不足以補償受害者之損失，故而目前已經有修法的建議，要將每一事件的最高賠償總額提高為新台幣 5,000 萬元，如此將更能補償受害人的損失。

管理 Tips

1. 組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練（CNS 27001 附錄 A .8.2.2）。

2. 應依據法令、法規、契約及營運要求，保護重要紀錄，免於遺失、毀損或偽造（CNS 27001 附錄 A.15.1.3）。
3. 應如同相關法令、法規及若適用的契約條文所要求的，確保資料的保護與隱私（CNS 27001 附錄 A.15.1.4）。

註釋：

[1] 電腦處理個人資料保護法第 3 條第一項第 7 款：「非公務機關：指前款以外之左列事業、團體或個人：
（一）徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。
（二）醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。
（三）其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。」

[2] 民法第 184 條：「因故意或過失，不法侵害他人之權利者，負損害賠償責任。故意以背於善良風俗之方法，加損害於他人者亦同。
違反保護他人之法律，致生損害於他人者，負賠償責任。但能證明其行為無過失者，不在此限。」

[3] 電腦處理個人資料保護法第 28 條：「非公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。
但能證明其無故意或過失者，不在此限。
依前項規定請求賠償者，適用前條第二項至第五項之規定。」

[4] 電腦處理個人資料保護法第 27 條：「公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。
前二項損害賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。
基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣二千萬元為限。
第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。」

分享軟體出包？防外洩，警局要警刪除家中資料

【案號：S970103】
資料來源：自由時報 97/09/28

焦點話題

由於以往曾經傳出縣市警察局公文與筆錄等資料，因員警電腦內安裝了「P2P」[1]分享軟體導致外洩情事。警政署最近特別清查發現，網路上目前還是找得到包括調查筆錄在內的警察機關公文資料，經查其中北部某警局有 70 餘筆公文資料外洩到網路上。而經過分析，資料外洩除因感染電腦病毒或木馬程式以外，最可能的原因是員警將辦公室公文資料帶回家裡電腦作業，不慎經由家裡裝有 BT[2] 或 FOXY 等網路分享軟體的電腦外洩。

因此，該警局發出通告到轄下的各警分局與刑警大隊等各單位，要求所有員警將家中電腦內的公文資料全數刪除，如果因作業需要，務必將備份燒錄到光碟，不能把資料留存在電腦硬碟裡，以防止資料透過網路外洩。部分基層員警私下透露，因為業務公文量大，才會把公文資料帶回家處理，在家裡電腦上處理公文時，會把分享軟體關閉，作業中會隱去重要名稱與文號等資料，再燒錄成光碟後刪除，免去不必要的困擾。

重點摘要

1. 使用網路分享軟體須當心，避免個人資料外洩。
2. 對於公務機關造成個人資料外洩，民眾可以依照「電腦處理個人資料保護法」（以下簡稱「個資法」）之規定來求償。

法律觀點

P2P（Peer-To-Peer）分享軟體，是一種可以讓使用者直接連結到他人的電腦搜尋資料的軟體，目前在網際網路上相當廣泛地被使

用，常見被用來作為音樂與影片等檔案之分享。這種軟體安裝後，會先在電腦裡建立一個分享資料夾，放在分享資料夾的檔案，即開放讓安裝相同分享軟體的其他網路使用者，經由分享軟體的搜尋功能，而可以透過網際網路將裡面的檔案下載到自己的電腦。

由於 P2P 分享軟體的功能強大且使用方便，使用的人越來越多，因此造成的機密資料外洩情事，也屢見不鮮。如果電腦內有機密資料，為避免外洩造成困擾，最好的方式當然是不要安裝 P2P 分享軟體；而即使已經安裝，也要避免將機密資料儲存在分享資料夾，以免流出。

為規範電腦處理個人資料，以避免人格權受侵害，並促進個人資料之合理利用[3]，我國訂有「個資法」作為規範。以本案為例，警察機關屬於「個資法」所規範之公務機關[4]，而應依該法第二章「公務機關之資料處理」相關規定（第 7 條至第 17 條）辦理，其中「個資法」第 17 條[5]即有公務機關應妥善保管個人資料之規定。

因此以本案為例，如警察機關沒有妥善保管個人資料，而透過 P2P 分享軟體外洩者，即違反上開「個資法」第 17 條規定，應對於受損之民眾應賠償其損失[6]。

管理 Tips

1. 組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練（CNS 27001 附錄 A .8.2.2）。
2. 應依據法令、法規、契約及營運要求，保護重要紀錄，免於遺失、毀損或偽造（CNS 27001 附錄 A.15.1.3）。
3. 應如同相關法令、法規及若適用的契約條文所要求的，確保資料的保護與隱私（CNS 27001 附錄 A.15.1.4）。
4. 應定期查核資訊系統是否遵循安全實作標準（CNS 27001 附錄 A.15.2.2）。

資訊保護

一、電腦處理個人資料保護法

註釋：

[1]【名詞解釋】

所謂 P2P（Peer-To-Peer），係一種在兩台以上之電腦間，彼此直接分享對方電腦資源的網路傳輸型態，有別於傳統之網路使用者一定要連結上某網站的伺服器才可以下載取得檔案之主從式架構作業模式，亦即每一個網路使用者可以兼具使用者端與伺服器之特性，使用者間之地位係對等而非主從關係。

[2]【名詞解釋】

BT（Bittorrent）是一種 P2P 軟體，使用多點對多點的下載方式，BT 的優越性在於你下載別人檔案的同時，你同時也在上傳你已下載完成之部分檔案，所有當有越多人下載時，同時也有越多人上傳，因此下載速度越快。

[3] 電腦處理個人資料保護法第 1 條：「為規範電腦處理個人資料，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。」

[4] 電腦處理個人資料保護法第 3 條第 6 款：「本法用詞定義如左：六、公務機關：指依法行使公權力之中央或地方機關。」

[5] 電腦處理個人資料保護法第 17 條：「公務機關保有個人資料檔案者，應指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」

[6] 電腦處理個人資料保護法第 27 條第 1 項：「公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。」

私售考生個資，主嫌求刑十年

【案號：S970104】
資料來源：中時電子報 97/10/15

焦點話題

台中○○公司承攬民國 97 年國中基測試務涉嫌販售考生個資案，高雄地檢署偵結，將涉嫌販售考生個資給補教業與學校牟利的業者，依背信、詐欺、偽造文書及電腦處理個人資料保護法等罪嫌起訴，分別求處 10 年與 9 年的有期徒刑。

至於涉嫌向○○公司購買考生個資的北、中、南八名補教業者，因犯罪情節比較輕微，在檢方曉以大義下立下悔過書，同意各繳新台幣 120 萬元給國庫，並切結 240 小時的志工服務同意書，調派名師為少年監獄或低收入戶的學生輔導功課，但該「緩起訴」處分的條件仍需高等法院檢察署核定。

重點摘要

1. 販賣個人資料，應依「電腦處理個人資料保護法」（以下簡稱「個資法」）負擔刑事責任。
2. 檢察官求刑原則上並無拘束力，僅具有供法官參考之價值。
3. 檢察官為緩起訴處分時，可附加條件要求被告履行。

法律觀點

最近在社會上常聽見詐騙集團活躍犯案的消息，而詐騙集團犯案的手法雖然多樣化，但是目前最為人所知者，也就是先行取得被害人的個人資料，以取信被害人後，再要求被害人為轉帳或其他交付款項的動作。所以個人資料的外洩，助長詐騙集團的橫行，也因此對於個人資料之保護，不僅在於避免人格權受侵害，並促進個人

資料之合理利用[1]，更能使民眾免於受詐騙之傷害。

以本案為例，行為人販賣個人資料的行為，已構成「個資法」之違反，依法應負擔刑事責任[2]。且因其行為態樣另涉及「刑法」背信與詐欺及偽造文書罪之違反，故乃遭檢察官一併起訴，並具體求處重刑。然而檢察官的求刑，原則上並無拘束法官量刑效力[3]，法官之量刑，仍需依法為裁量[4]，故檢察官的求刑僅具參考價值。

另外，檢察官對於購買個人資料的業者，則係依「刑事訴訟法」之「緩起訴處分」之規定辦理。所謂緩起訴處分者，即「刑事訴訟法」第 253 條之 1 規定，允許由檢察官對於被告所犯為死刑、無期徒刑或最輕本刑 3 年以上有期徒刑以外之罪之案件，得參酌「刑法」第 57 條所列事項與公共利益之維護，認為適當者，予以緩起訴處分，期間為 1 年以上至 3 年以下，以觀察犯罪行為人有無施以「刑法」所定刑事處罰之必要，為一種介於起訴與微罪職權不起訴[5]間之緩衝制度設計。而為鼓勵被告自新與復歸社會之目的，「刑事訴訟法」更賦予檢察官於「緩起訴處分」時，得命被告遵守一定之條件或事項之權力[6]。

管理 Tips

1. 應依據法令、法規、契約及營運要求，保護重要紀錄，免於遺失、毀損或偽造（CNS 27001 附錄 A.15.1.3）。
2. 應如同相關法令、法規及若適用的契約條文所要求的，確保資料的保護與隱私（CNS 27001 附錄 A.15.1.4）。

註釋：

[1] 電腦處理個人資料保護法第 1 條：「為規範電腦處理個人資料，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。」

[2] 電腦處理個人資料保護法第 33 條：「意圖營利違反第七條、第八條、第十八條、第十九條第一項、第二項、第二十三條之規定或依第二十四條所發布之限制命令，致生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣四萬元以下罰金。」

[3] 例外者，如刑事訴訟法第 451 之 1 條第 1、3、4 項規定：「前條第一項之案件，被告於偵查中自白者，得向檢察官表示願受科刑之範圍或願意接受緩刑之宣告，檢察官同意者，應記明筆錄，並即以被告之表示為基礎，向法院求刑或為緩刑宣告之請求。」、「被告自白犯罪未為第一項之表示者，在審判中得向法院為之，檢察官亦得依被告之表示向法院求刑或請求為緩刑之宣告。」、「第一項及前項情形，法院應於檢察官求刑或緩刑宣告請求之範圍內為判決…。」

[4] 刑法第 57 條規定：「科刑時應以行為人之責任為基礎，並審酌一切情狀，尤應注意下列事項，為科刑輕重之標準：一、犯罪之動機、目的。二、犯罪時所受之刺激。三、犯罪之手段。四、犯罪行為人之生活狀況。五、犯罪行為人之品行。六、犯罪行為人之智識程度。七、犯罪行為人與被害人之關係。八、犯罪行為人違反義務之程度。九、犯罪所生之危險或損害。十、犯罪後之態度。」

[5] 刑事訴訟法第 253 條：「第三百七十六條所規定之案件，檢察官參酌刑法第五十七條所列事項，認為以不起訴為適當者，得為不起訴之處分。」

[6] 刑事訴訟法第 253 之 2 條第 1 項：「檢察官為緩起訴處分者，得命被告於一定期間內遵守或履行左列各款事項：一、向被害人道歉。二、立悔過書。三、向被害人支付相當數額之財產或非財產上之損害賠償。四、向公庫或指定之公益團體、地方自治團體支付一定之金額。五、向指定之公益團體、地方自治團體或社區提供四十小時以上二百四十小時以下之義務勞務。六、完成戒癮治療、精神治療、心理輔導或其他適當之處遇措施。七、保護被害人安全之必要命令。八、預防再犯所為之必要命令。」

某市政府網站擺烏龍，民眾個資外洩

【案號：S970105】
資料來源：華視 97/11/17

焦點話題

某市政府法規會，也就是主管消費者保護的機關網站，把民眾申請國賠的資料，全都開放提供檢索，不但個人身分資料全都查得到，就連就醫紀錄都被張貼在網站上。

當市民想申請國賠，而進入某市政府法規會網站時，在全文檢索中隨意輸入查詢字眼，就會出現一筆筆民眾的案例資料，不只是文字陳述，就連車禍照片與當事人的就醫紀錄，全都一覽無疑，還有民眾的身分證就這樣被顯示在網站上。某市市議員質疑，主管消費者保護的法規會，竟然成了洩漏個人資料的兇手。法規會則表示是外包資訊廠商，忘記把資料加密，才導致民眾的個資全都露，已經請廠商趕工補救。

重點摘要

1. 個人資料的保護還不夠落實，連政府機關也常發生洩漏民眾個人資料的情形。
2. 對於個人資料的保護，雖然有「電腦處理個人資料保護法」（以下簡稱「個資法」）作為規範，但是徒法不足以自行，仍然需要政府機關與企業及民眾等的支持。

法律觀點

最近常常發生個人資料外洩的新聞，除有購物頻道的消費者因業者外洩個人資料，而遭到詐騙集團鎖定行騙外，政府機關處理民眾的個人資料，也有疏忽的時候。除上面案例所提到的某市政府

法規會，發生外洩民眾申請國賠的資料外，同時間也發生某縣政府網站，外洩原住民學生個人資料的情形，顯見目前對於個人資料的保護還不夠落實，所以連政府機關也有發生洩漏民眾個人資料的情形。

目前我國對於個人資料的保護，是以「個資法」為規範。其中規範的對象即包括公務機關[1]。以本案而言，某市政府法規會即是受「個資法」規範之公務機關，而依「個資法」第 17 條規定[2]，應負有防止個人資料被竊取、竄改、毀損、滅失或洩漏之義務。由於某市政府法規會之管理不當而洩漏民眾個人資料者，應負起賠償民眾權益損失的責任，如果民眾名譽受損，依法[3]更可請求回復名譽的適當處分（例如登報道歉）。

「個資法」自民國 84 年公布施行以來，已經有十餘年，雖然對於個人資料的保護發生一定的功效。然而從這個案例看起來，公務機關對於民眾個人資料外洩的情形，特別是外包廠商的控管與責任分擔，都有強化的空間。所謂徒法不足以自行，對於個人資料的保護，仍然需要政府機關與企業及民眾等的支持。

另外，由於目前「個資法」適用的範圍僅及於以「電腦處理」[4]的個人資料；而規範對象之非公務機關部分亦有限制，並非所有涉及個人資料處理的企業都有適用，故其保護的範圍比較狹窄。目前修法的研議，已經針對這幾個方向為放寬的規劃，相信修法通過以後，對於個人資料的保護將更為周到。

管理 Tips

1. 管理階層應要求員工、承包者及第三方使用者，依照組織已制定的政策與程序施行安全事宜（CNS 27001 附錄 A.8.2.1）。
2. 組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練（CNS 27001 附錄 A .8.2.2）。

3. 應建立資訊的處置及儲存程序，以保護此資訊免於未經授權的揭露或誤用（CNS 27001 附錄 A.10.7.3）。
4. 應依據法令、法規、契約及營運要求，保護重要紀錄，免於遺失、毀損或偽造（CNS 27001 附錄 A.15.1.3）。
5. 應如同相關法令、法規及若適用的契約條文所要求的，確保資料的保護與隱私（CNS 27001 附錄 A.15.1.4）。

註釋：

[1] 電腦處理個人資料保護法第 3 條第 6 款：「本法用詞定義如左：
六、公務機關：指依法行使公權力之中央或地方機關。」

[2] 電腦處理個人資料保護法第 17 條：「公務機關保有個人資料檔案者，應指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」

[3] 電腦處理個人資料保護法第 27 條：「公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。
前二項損害賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。
基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣二千萬元為限。
第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。」

[4] 電腦處理個人資料保護法第 3 條第 3 款：「本法用詞定義如左：
三、電腦處理：指使用電腦或自動化機器為資料之輸入、儲存、編輯、更正、檢索、刪除、輸出、傳遞或其他處理。」

遏止垃圾郵件，擬修法求償

【案號：S970106】
資料來源：華視 97/11/25

焦點話題

全台每個月有上百億封垃圾郵件，每人平均一天 100 封，怎麼刪都刪不完。行政院國家通訊傳播委員會（NCC）日前通過垃圾郵件取締的管理辦法，只要立法院通過，未來濫發電子郵件者，每一封可以求償新台幣 500 元至 2, 000 元。

一打開電子郵件，相信很多民眾都很困擾，每天面對著上百封垃圾郵件，一封封地刪，即使刪到手軟，還是擋不了垃圾信件不斷湧入信箱。根據統計，全台灣平均每位民眾至少有 3 個電子信箱，初步估計至少每天就會收到 100 封垃圾郵件。

行政院國家通訊傳播委員會（NCC）討論通過「濫發商業電子郵件管理條例草案」，未來對濫發電子郵件者將開罰新台幣 500 元至 2,000 元，如果民眾收到 100 封垃圾郵件，以最低罰金 500 元計算，可向寄件者求償 5 萬元。目前台灣垃圾郵件至少有上百億封，以刪除一封信花 3 秒來計算，每年就浪費 30 小時在處理垃圾郵件。

重點摘要

1. 垃圾郵件內容以色情或暴力居多，對於電腦使用者已經造成困擾。
2. 外國已經有不少國家立有專法[1]，可對於發送垃圾郵件之業者求償，我國法律草案的提出，已追上先進國家的腳步。

法律觀點

網際網路的發達除帶來便利，也有一些後遺症。根據台灣網際

網路協會一項「垃圾郵件痛苦指數大調查」，結果發現台灣地區有 7 成 5 的垃圾郵件，與情色暴力相關，其次是網路購物的廣告郵件，但高達 7 成的受訪者，根本連看都不看就會刪除。更重要的是，有一些垃圾郵件夾帶著電腦病毒，電腦使用者一不小心，可能就會因此中毒，所以有網路業者指出，民眾應該將自己的電子信箱地址視為個人資料，不要隨便外洩，以免造成不必要的麻煩。

而日前行政院國家通訊傳播委員會（NCC）通過的「濫發商業電子郵件管理條例草案」，就是對於網路垃圾郵件取締的管理辦法，未來將報請行政院轉立法院，通過立法後，將可遏止日益嚴重的垃圾郵件問題。根據 NCC 通過的草案內容，分為 5 個部分，分別是電子郵件發送前階行為、合法發送要件、行為的法律效果選擇、業者的權利義務及相關的配套機制等。

其中，最主要的是除保留民事賠償的機制外，也特別明訂對於垃圾郵件的發送者與濫發人，受損害的民眾，對於每一封電子郵件，可以要求新台幣 500 元至 2,000 元之賠償[2]，並有團體訴訟之設計，以避免單一個人求償的困難[3]。而且為強化團體訴訟的效果，更明定負責團體訴訟的機構，可以分別向「服務提供者」、「廣告主」或「廣告代理商」要求提供濫發人之資料，以利民眾求償[4]。

雖然現在我國已經跟上先進國家的腳步，開始對垃圾郵件為管理與立法規範，然而實務上的困難是，垃圾郵件有 9 成 5 是自國外發送，來源不容易找到，而造成處罰與管理的困難，因此，電腦使用者還是應該當自強，做好個人資料的防護工作。

管理 Tips

1. 網路應適切地加以管理與控制，使其不受威脅，並且維護使用網路的系統與應用程式的安全，包括輸送中資訊（CNS 27001 附錄 A.10.6.1）。

2. 應識別所有網路服務的安全特徵、服務水準及管理要求，並應被納入網路服務協議中，不論是此等服務是由內部或委外所提供（CNS 27001 附錄 A.10.8.4）。

註釋：

[1] 根據「濫發商業電子郵件管理條例草案」之立法說明，目前已有美國、日本、澳洲、韓國、新加坡及中國大陸等國家訂定專法規範此類行為，歐洲則要求會員國必須於隱私與電子通訊之相關規定，納入商業電子郵件之規範，目前已有德國與法國及義大利等國透過相關法令管制。

[2] 濫發商業電子郵件管理條例草案第 7 條第 1 至 4 項：「發信人違反第四條或第五條規定，至收信人受有損害者，負損害賠償責任。
收信人雖非財產上之損害，亦得請求賠償相當之金額。
前二項損害賠償總額，以每人每封商業電子郵件新台幣五百元以上二千元以下計算。但能證明其所受損害高於該金額者，不在此限。
基於同一原因事實致多數收信人受有損害，其合計最高損害賠償總額以新台幣二千萬元為限。但因該原因事實所得利益逾新台幣二千萬元者，以該所得利益為限。」

[3] 濫發商業電子郵件管理條例草案第 9 條第 1 項前段：「公益社團法人或財團法人對於違反第四條或第五條規定造成損害之事件，得由二十人以上因同一原因事實受有損害之當事人授與其訴訟實施權後，以自己名義，提起損害賠償訴訟。」

[4] 濫發商業電子郵件管理條例草案第 9 條第 4 項本文、第 5 項：「公益社團法人或財團法人經受害當事人授與其訴訟實施權者，為確認被告身分，得向電子郵件服務提供者或網際網路接取服務提供者，請求提供發信人下列資料，被請求之服務提供者無正當理由不得拒絕。
前項規定於公益社團法人或財團法人向廣告主或廣告代理商請求提供發信人資料時，準用之。」

冒稱反詐專員，趁機套個資

【案號：S970107】
資料來源：聯合報 97/12/25

焦點話題

台東市有民眾接獲自稱刑事局「165 反詐騙專線」的宣導員，企圖誘騙民眾說出自己的個人資料，有人如實說出，有人懷疑求證，警方證實是詐騙新招，籲請民眾留意，以免受騙。

警方表示，台東市有一名黃姓民眾報案，指稱他接獲自稱刑事局警官「張志宏」的電話，佯稱要宣導新式詐騙手法。對方先向他宣導一些普遍的詐騙手法，然後開始套問他的個人資料，聲稱「我們需要有業務資料，證明我確實做過宣導」。黃姓民眾覺得很奇怪，「怎麼可能找得到我，卻不知道我的姓名電話？」，所以向警方報案，警方表示這是詐騙電話，籲請民眾勿上當。

重點摘要

1. 詐騙手段日新月異，警方宣導的「165 反詐騙專線」，反而成為歹徒的行騙藉口，因此民眾應該時時警覺，避免受騙。
2. 個人資料的保護，目前有「電腦處理個人資料保護法」（以下簡稱「個資法」）作為規範，而可以對非法蒐集個人資料者，為刑事之追訴與處罰。

法律觀點

目前社會上各種詐騙手段日新月異，以往常常可以見到，歹徒假冒法院人員或檢察官，以民眾帳戶涉及洗錢或詐欺等刑事案件為由，要求民眾提供帳戶密碼或甚至要求民眾轉帳至指定帳戶，而詐騙民眾金錢的案例。然而在警方大力宣導之下，這樣的詐騙手段漸

漸被民眾所知悉，因此受騙上當的人越來越少。但是，道高一尺，魔高一丈，歹徒的行騙手法也是日益翻新，本件案例歹徒甚至利用反詐騙專線的名義，來騙取民眾的個人資料，並進而利用個人資料，從事不法的勾當。

目前我國關於個人資料的保護，主要係規定在「個資法」。其中對於非公務機關[1]蒐集[2]個人資料者，設有專章（第三章）加以規範，並且對於違反者有民[3]、刑事責任[4]之規定。至於本案中之詐騙歹徒，其所為蒐集個人資料之行為，是否受「個資法」之規範，則需視其是否符合「個資法」第 3 條第 7 款第 1 目之「以蒐集或電腦處理個人資料為主要業務之團體或個人」。

以往一般實務係以行為主體的行業別為判斷基準，因此僅有特定的行業別才會被認為係以「蒐集或電腦處理個人資料為主要業務」，而限縮了「個資法」之適用範圍。但是有實務見解[5]基於「個資法」第 1 條明文揭櫫之「為避免人格權受侵害，並促進個人資料之合理利用」立法目的，而認為上開「主要業務」之判斷，應以蒐集與處理及利用個人資料之行為所造成之侵害程度，而非專以行為主體之行業別為斷，是除該法第 3 條第 7 款第 2 目之八大行業與同條款第 3 目之經指定之事業、團體或個人外，實際上大量蒐集或處理個人資料之團體或個人，亦應納入該法之規範範疇。因此對於定期不法蒐集與電腦處理個人資料計達 23 萬餘筆的該案被告，判處有期徒刑 4 個月。

則若依上述之法院判決意旨，因「個資法」第 19 條第 1 項規定[6]，未經登記並發給執照者，不得從事個人資料之蒐集，違反者有同法第 33 條 2 年以下有期徒刑、拘役或科或併科新臺幣 4 萬元以下罰金之刑責。故本案例中之歹徒是屬於實際上大量蒐集或處理個人資料之團體或個人，而有違反「個資法」第 33 條規定之虞。

資訊保護

一、電腦處理個人資料保護法

管理 Tips

1. 應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私（CNS 27001 附錄 A.15.1.4）。

註釋：

[1] 電腦處理個人資料保護法第 3 條第 7 款：「本法用詞定義如左：
七、非公務機關：指前款以外之左列事業、團體或個人：
（一）徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。
（二）醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。
（三）其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。」

[2] 電腦處理個人資料保護法第 3 條第 4 款：「本法用詞定義如左：
四、蒐集：指為建立個人資料檔案而取得個人資料。」

[3] 電腦處理個人資料保護法第 28 條第 1 項：「非公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但能證明其無故意或過失者，不在此限。」

[4] 電腦處理個人資料保護法第 33 條：「意圖營利違反第七條、第八條、第十八條、第十九條第一項、第二項、第二十三條之規定或依第二十四條所發布之限制命令，致生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣四萬元以下罰金。」

[5] 台北地方法院 95 年度簡字第 620 號判決參照。

[6] 電腦處理個人資料保護法第 19 條第 1 項：「非公務機關未經目的事業主管機關依本法登記並發給執照者，不得為個人資料之蒐集、電腦處理或國際傳遞及利用。」

媒體已經報導過的國家機密，還是國家機密嗎？

【案號：S970201】

資料來源：台灣高等法院 94 年訴字第 1 號，96 年 9 月 21 日宣判

焦點話題

乙○○於國家情報單位退役後，對於其在任職時所知悉的國家機密，例如總統緊急脫離動線，對總統陸空脫離的直昇機與裝甲運兵車待命位置、地點、脫離方式、路線及避難等處所，運用優勢兵力採取特攻、突（伏）擊等作為，分別於不同的時間點於接受平面或電子媒體訪問時，洩漏予媒體刊載或播出，而被高等法院檢察署檢察官提起公訴並經判決有罪處 2 年有期徒刑，緩刑 4 年。

重點摘要

1. 已經核定為「國家機密」，即必須依據保密等級維護「國家機密」。
2. 即使已經經過媒體報導的「國家機密」，在還沒完成解密條件時，還是機密，不可以主動洩漏。

法律觀點

政府資訊的公開，雖然對於民主政治之發展相當重要，但是某些應機密事項之維護對於國家安全亦有其必要性，因此資訊公開與機密保護兩者間必須取得平衡點。以「政府資訊公開法」第 18 條第 1 項第 1 款[1]規定來說，即將依法核定為「國家機密」者，排除於資訊公開之外。而所謂「國家機密」，其法制規範於我國即為「國家機密保護法」，對於「國家機密」之認定[2]與維護等均有所規定。

按政府機關持有或保有的資訊，是否屬於機密，其等級為何，

「國家機密保護法」訂有核定、變更、維護及解密規定，例如「國家機密保護法」第 7 條[3]、第 27 至 31 條[4]即明訂核定機密與解密的權責人員與程序。以本案而言，行為人於其職務上所知悉的「國家機密」，因涉及到國家安全或利益，而受「國家機密保護法」所建立的保護機制規範，行為人如果將該機密洩漏予報章媒體，即有相應的刑事責任，最重可以判處 7 年以下的刑責[5]。

而本案爭議中最值得討論的是，行為人主張其所洩漏之資料，早已見於報章雜誌等媒體，因此並非「國家機密」。但是法院卻認為「國家機密保護法訂有核定、變更、維護及解密規定，本件被告對外洩漏的本案案情，縱已經其他管道外漏、媒體披露，只要非經權責機關公開、證實或解密，前述各情的機密性質，並不因此受影響」，因此即使是媒體已經報導過的「國家機密」，在未依「國家機密」保護法解密程序規定為解密時，還是「國家機密」，如果對外洩漏的話，還是有處罰規定的適用。雖然本案例只是高等法院的見解，還沒有看到最高法院的意見，但是至少可以看出法院嚴守「國家機密保護法」規範的態度，因此本案例仍然具有相當的警示意義，也就是即使是媒體已經報導過的「國家機密」，還是「國家機密」。

管理 Tips

1. 宜識別與定期審查反映組織對資訊保護之需求的機密性及保密協議要求（CNS 27001 附錄 A.6.1.5）。
2. 資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類（CNS 27001 附錄 A.7.2.1）。

註釋：

[1] 政府資訊公開法第 18 條第 1 項第 1 款：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：一、經依法核定為國家機密或其他法律、法規命令規定應秘密事項或限制、禁止公開者。」

[2] 國家機密保護法第 2 條：「本法所稱國家機密，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者。」

[3] 國家機密保護法第 7 條：「國家機密之核定權責如下：

一、絕對機密由下列人員親自核定：

（一）總統、行政院院長或經其授權之部會級首長。

（二）戰時，編階中將以上各級部隊主官或主管及部長授權之相關人員。

二、極機密由下列人員親自核定：

（一）前款所列之人員或經其授權之主管人員。

（二）立法院、司法院、考試院及監察院院長。

（三）國家安全會議秘書長、國家安全局局長。

（四）國防部部長、外交部部長、行政院大陸委員會主任委員或經其授權之主管人員。

（五）戰時，編階少將以上各級部隊主官或主管及部長授權之相關人員。

三、機密由下列人員親自核定：

（一）前二款所列之人員或經其授權之主管人員。

（二）中央各院之部會及同等級之行、處、局、署等機關首長。

（三）駐外機關首長；無駐外機關首長者，經其上級機關授權之主管人員。

（四）戰時，編階中校以上各級部隊主官或主管及部長授權之相關人員。

前項人員因故不能執行職務時，由其職務代理人代行核定之。」

[4] 國家機密保護法第 27 條：「國家機密於核定之保密期限屆滿時，自動解除機密。

解除機密之條件逾保密期限未成就者，視為於期限屆滿時已成就，亦自動解除機密。」

國家機密保護法第 28 條：「國家機密核定之解除條件成就者，除前條第

二項規定外，由原核定機關或其上級機關有核定權責人員核定後解除機密。」

國家機密保護法第 29 條：「國家機密於保密期限屆滿前或解除機密之條件成就前，已無保密之必要者，原核定機關或其上級機關有核定權責人員應即為解除機密之核定。」

國家機密保護法第 30 條：「前二條情形，如國家機密事項涉及其他機關業務者，於解除機密之核定前，應會商該他機關。」

國家機密保護法第 31 條：「國家機密解除後，原核定機關應將解除之意旨公告，並應通知有關機關。

前項情形，原核定機關及有關機關應在國家機密之原件或複製物上為解除機密之標示或為必要之解密措施。」

[5] 國家機密保護法第 32 條第 1 項：「洩漏或交付經依本法核定之國家機密者，處一年以上七年以下有期徒刑。」

國防以外機密與國家機密之區別

【案號：S970202】

資料來源：桃園地方法院 95 年易字第 227 號判決，96 年 1 月 16 日宣判

焦點話題

被告甲○○原係海軍上校，任職行政院國防部某研究院，於民國 90 年 8 月間因屆最大年限以現役退伍，轉任該院文職科技聘僱人員，職司國防科技研發工作，為依法令服務於國家所屬機關而具有法定職務權限之公務員。[1]

甲○○明知其於 91 年間於公務上撰寫完成之「以國家安全戰略考量國家軍事戰略基礎國防科技產業化之經濟政策行動綱領」，內容有引用經權責單位核定為密等之國防以外應秘密之文書，或另有內容影印摘錄到某院及其人員於公務上應保守秘密之資訊，而均屬國防以外應秘密之文書。其竟先於 91 年 4 月初某日，在 A 立法委員辦公室內，交予 A 立法委員。其後，於同年 4 月底某日，將上開文章，與其於 89 年 9 月間撰寫完成，內有影印如上所示公務上應保守秘密文書之國防部「精實兵電飛彈武器系統壽期工程研發」備料更新促進現代化政策構想與研析及推動建議乙文，影印集結成一本後，於 91 年 6 月間某日，將上開國防科技產業化報告交予 A 立法委員。

嗣經桃園地方法院以被告甲○○連續犯公務員洩漏國防以外之秘密文書罪，處有期徒刑 6 月，如易科罰金，以銀元 300 元即新臺幣 900 元折算 1 日[2]，緩刑 2 年。

重點摘要

1. 以往法律上所稱機密大致可區分為「軍事機密」與「國防秘密」及「國防以外秘密」，而於「國家機密保護法」則明文規定「國家機密」之分類。

2. 因此對於不同等級的機密保護，規範也不同，機密等級越高者，洩漏之刑責隨之越重。

法律觀點

在「國家機密保護法」制定施行以前，以往法律上所稱機密大致有「軍事機密」與「國防秘密」及「國防以外秘密」之區分。而依 92 年 7 月 14 日修正前之「軍事機密與國防秘密種類範圍等級劃分準則」第 2 條規定：「本準則稱軍事機密，指與軍事作戰具直接關聯，為確保軍事安全或利益，而應保守之秘密，並經依法令核定機密等級之文書、圖畫、消息、電磁紀錄或物品。本準則稱國防秘密，指軍事機密以外，與國防整體安全或利益有關，而應保守之秘密，由國防部主管並經依法令核定機密等級之文書、圖畫、消息、電磁紀錄或物品」（現行條文移列為同準則第 3 條）。除上述「軍事機密」與「國防秘密」以外之應秘密之文書、圖畫、消息、電磁紀錄或物品，即屬「國防以外秘密」之範疇。至於「國家機密」之定義，依「國家機密保護法」第 2 條規定，則指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依「國家機密保護法」核定機密等級者。

由於對於不同等級的機密保護，規範也不同，洩漏之刑責自亦隨之不同。例如洩漏「軍事機密」者，規範在「陸海空軍刑法」第 20 條[3]；洩露「國防秘密」者有「刑法」第 109 及 110 條[4]規範；洩露「國防以外秘密」者有「刑法」第 132 條[5]規範，至於「國家機密」之洩漏則亦有「國家機密保護法」第 32 條規範[6]。

管理 Tips

1. 宜識別與定期審查反映組織對資訊保護之需求的機密性及保密協議要求（CNS 27001 附錄 A.6.1.5）。
2. 資訊應依其對組織的價值、法律要求、敏感性及重要性加以

分類（CNS 27001 附錄 A.7.2.1）。

註釋：

[1] 刑法第 10 條第 2 項：「稱公務員者，謂下列人員：
一、依法令服務於國家、地方自治團體所屬機關而具有法定職務權限，以及其他依法令從事於公共事務，而具有法定職務權限者。
二、受國家、地方自治團體所屬機關依法委託，從事與委託機關權限有關之公共事務者。」

[2] 此為刑法 95 年 7 月 1 日修正前之第 41 條規定，現行規定為：「犯最重本刑為五年以下有期徒刑以下之刑之罪，而受六個月以下有期徒刑或拘役之宣告者，得以新臺幣一千元、二千元或三千元折算一日，易科罰金。」

[3] 陸海空軍刑法第 20 條：「洩漏或交付關於中華民國軍事上應秘密之文書、圖畫、消息、電磁紀錄或物品者，處三年以上十年以下有期徒刑。戰時犯之者，處無期徒刑或七年以上有期徒刑。洩漏或交付前項之軍事機密於敵人者，處死刑或無期徒刑。前二項之未遂犯，罰之。因過失犯第一項前段之罪者，處三年以下有期徒刑、拘役或新臺幣三十萬元以下罰金。戰時犯之者，處一年以上七年以下有期徒刑。預備或陰謀犯第一項或第二項之罪者，處五年以下有期徒刑。」

[4] 刑法第 109 條：「洩漏或交付關於中華民國國防應秘密之文書、圖畫、消息或物品者，處一年以上七年以下有期徒刑。洩漏或交付前項之文書、圖畫、消息或物品於外國或其他派遣之人者，處三年以上十年以下有期徒刑。前二項之未遂犯罰之。預備或陰謀犯第一項或第二項之罪者，處二年以下有期徒刑。」

刑法第 110 條：「公務員對於職務上知悉或持有前條第一項之文書、圖畫、消息或物品，因過失而洩漏或交付者，處二年以下有期徒刑、拘役或一千元以下罰金。」

[5] 刑法第 132 條：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。因過失犯前項之罪者，處一年以下有期徒刑、拘役或三百元以下罰金。非公務員因職務或業務知悉或持有第一項之文書、圖畫、消息或物品，而洩漏或交付之

者，處一年以下有期徒刑、拘役或三百元以下罰金。」

[6] 國家機密保護法第 32 條：「洩漏或交付經依本法核定之國家機密者，處一年以上七年以下有期徒刑。因過失犯前項之罪者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。第一項之未遂犯罰之。」

臥底？某大房仲集團指控另一房仲集團老總弟弟涉嫌洩密

【案號：S970301】
資料來源：中廣新聞網 97/07/30

焦點話題

AA 房屋指控 BB 房屋總經理的弟弟○○○涉嫌竊取 AA 房屋公司內部的營業機密資料，AA 房屋法務表示，○○○明知公司人事規定，卻對有關家庭成員任職情況的詢問事項故意作不實填寫，多次資料校正也沒有如實說明，AA 房屋接獲檢舉，加上透過資訊部門調查，認為○○○涉及刑責，因此依法將他免職，並移送法辦。

至於究竟是什麼樣的資料被洩漏，AA 房屋則出示三份電子郵件影本，包括公司內部仲介買方經營作業標準書與仲介賣方經營作業標準書及一件房仲物件資料，認為這些都是被○○○以電子郵件轉寄出去的。

重點摘要

1. 商業競爭激烈，為了搶奪「營業秘密」或資訊，業者之間的諜戰與跟蹤及破壞等手段層出不窮。
2. 「營業秘密法」是為了維持產業倫理與競爭秩序，以保障合法業者。
3. 「營業秘密法」是屬於民事法規，對於竊取「營業秘密」的商業間諜，其刑事責任主要是由「刑法」背信罪或妨害工商秘密罪規範。

法律觀點

我國房屋仲介產業已經發展很多年，為了搶奪資訊，業者之間的諜戰與跟蹤及破壞等手段，在業界已經不是秘密，甚至在消費者與媒體間散播假消息等以打擊對手，也屢見不鮮。對於房屋仲介產業而言，房屋物件與委託者等資訊，就是其利基所在，因此對於營業上秘密的保護，更見其重要性。

依據我國「營業秘密法」規定[1]，其立法目的是為保障「營業秘密」，維護產業倫理與競爭秩序，調和社會公共利益。而所謂「營業秘密」[2]，必須不是一般業界之人所共知者與具有實際或潛在的經濟價值者，且已採取合理的保密措施的方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營的資訊。

而本件報導如果屬實，相關人等就涉及到侵害「營業秘密」[3]，依據「營業秘密法」的規定[4]，應對受損害的房仲業者為賠償，在侵害行為是基於故意的情況下，更可要求不超過損害額 3 倍的賠償。此外，除「營業秘密法」規範的民事賠償責任外，本案行為人的行為也有刑事責任的問題，例如可能涉及到包括「刑法」背信罪[5]與妨害工商秘密罪[6]。

雖然商業間諜可能有上開法律可以規範，然而利之所在，這樣的案子還是會層出不窮，因此最好的方式還是應該做好「營業秘密」的保護措施，才不會因疏忽導致重大的損失。

管理 Tips

1. 員工、承包者及第三方使用者的安全角色與責任，應依照組織的資訊安全政策加以界定與文件化（CNS 27001 附錄 A.8.1.1）。
2. 身為契約義務的一方，員工、承包者及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊

安全的責任（CNS 27001 附錄 A.8.1.3）。

2. 管理階層應要求員工、承包者及第三方使用者，依照組織已制定的政策與程序施行安全事宜（CNS 27001 附錄 A.8.2.1）。

4. 對於違反安全的員工，應有正式的懲處過程（CNS 27001 附錄 A.8.2.3）。

註釋：

[1] 營業秘密法第 1 條：「為保障營業秘密，維護產業倫理與競爭秩序，調和社會公共利益，特制定本法。本法未規定者，適用其他法律之規定。」

[2] 營業秘密法第 2 條：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：

一、非一般涉及該類資訊之人所知者。

二、因其秘密性而具有實際或潛在之經濟價值者。

三、所有人已採取合理之保密措施者。」

[3] 營業秘密法第 10 條：「有左列情形之一者，為侵害營業秘密：

一、以不正當方法取得營業秘密者。

二、知悉或因重大過失而不知其為前款之營業秘密，而取得、使用或洩漏者。

三、取得營業秘密後，知悉或因重大過失而不知其為第一款之營業秘密，而使用或洩漏者。

四、因法律行為取得營業秘密，而以不正當方法使用或洩漏者。

五、依法令有守營業秘密之義務，而使用或無故洩漏者。

前項所稱之不正當方法，係指竊盜、詐欺、脅迫、賄賂、擅自重製、違反保密義務、引誘他人違反其保密義務或其他類似方法。」

[4] 營業秘密法第 13 條：「依前條請求損害賠償時，被害人得依左列各款規定擇一請求：

一、依民法第二百十六條之規定請求。但被害人不能證明其損害時，得以其使用時依通常情形可得預期之利益，減除被侵害後使用同一營

業秘密所得利益之差額，為其所受損害。

二、請求侵害人因侵害行為所得之利益。但侵害人不能證明其成本或必要費用時，以其侵害行為所得之全部收入，為其所得利益。

依前項規定，侵害行為如屬故意，法院得因被害人之請求，依侵害情節，酌定損害額以上之賠償。但不得超過已證明損害額之三倍。」

[5] 刑法第 342 條：「為他人處理事務，意圖為自己或第三人不法之利益，或損害本人之利益，而為違背其任務之行為，致生損害於本人之財產或其他利益者，處五年以下有期徒刑、拘役或科或併科一千元以下罰金。前項之未遂犯罰之。」

[6] 刑法第 317 條：「依法令或契約有守因業務知悉或持有工商秘密之義務，而無故洩漏之者，處一年以下有期徒刑、拘役或一千元以下罰金。」

科技經理離職帶走資料因背信被起訴

【案號：S970302】

資料來源： Pchome 新聞 97/10/08

焦點話題

據載新竹科學園區某一家科技公司的研發經理，跳槽前將公司研發的商業秘密資料帶走，日前新竹地檢署依照刑法背信罪嫌將他起訴。檢方表示，該研發經理明知對公司負有保密責任，未經公司同意或授權不得複製應秘密之資料，若資料外洩而由同業取得，將可能對於公司造成嚴重損失。

任職於某一家科技公司研發部的研發經理，於 7 年前曾率領公司研發團隊負責設計核心商業機密業務，並研發出兩項高科技先進技術，對於公司之營業貢獻極大，光是民國 93 年的營業收入即高達了新台幣 13 億元。之後因為另一家半導體公司看準這項機密資料商機無限，重金挖角該經理，延攬擔任研發部副處長。該經理離職前則利用職務之便，將包括上述兩項電腦程式等 7 個檔案，複製在電腦磁片中存放，之後被原公司發現，而向地檢署提出告訴。

重點摘要

1. 受雇人於職務上研究或開發之「營業秘密」，原則上應歸雇用人所有，受雇人應負有保密義務。
2. 受雇人離職時，攜走屬於公司之「營業秘密」，已構成「營業秘密」之侵害，應依「營業秘密法」之規定，負損害賠償責任。

法律觀點

台灣有許多高科技產業，每年研發出不少專利與著作權等「智

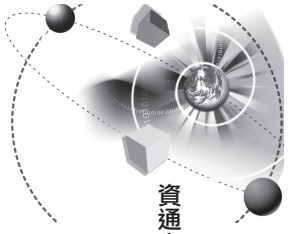
慧財產權」，或者方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊等「營業秘密」[1]。而無論係「智慧財產權」或是「營業秘密」，若是屬於受雇人於職務上研究或開發之產物，原則上即應歸雇用人之公司所有[2]，受雇人亦不得任意將其洩漏。

以本案為例，報導中行為人所洩漏者，既然屬於公司研發的商業資料，性質上應屬於公司的「營業秘密」。洩漏「營業秘密」者，即為典型侵害「營業秘密」行為[3]，依據「營業秘密法」之規定，應對受損害公司為賠償[4]，在侵害行為是基於故意的情況下，更可要求不超過損害額 3 倍的賠償。此外，除民事賠償責任外，本案行為人的行為也可能涉及到包括「刑法」背信罪[5]等刑事責任。

另由於「營業秘密」應秘密之特殊性，於法院訴訟審理上，亦必須顧及「營業秘密」的保護，而有特別規定。例如此類案件需由專業法庭審理、不公開審判、限制閱覽訴訟資料[6]，及由法院核發秘密保持命令[7]，並對違反法院秘密保持命令者，有刑事處罰之規定[8]，以保障「營業秘密」，維護產業倫理與競爭秩序。

管理 Tips

1. 員工、承包者及第三方使用者的安全角色與責任，應依照組織的資訊安全政策加以界定與文件化（CNS 27001 附錄 A.8.1.1）。
2. 身為契約義務的一方，員工、承包者及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任（CNS 27001 附錄 A.8.1.3）。
3. 管理階層應要求員工、承包者及第三方使用者，依照組織已制定的政策與程序施行安全事宜（CNS 27001 附錄 A.8.2.1）。



註釋：

[1] 營業秘密法第 2 條：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」

[2] 營業秘密法第 3 條第 1 項：「受雇人於職務上研究或開發之營業秘密，歸雇用人所有。但契約另有約定者，從其約定。」另外專利法第 7 條第 1 項、著作權法第 11 條第 2 項亦有相類規定。

[3] 營業秘密法第 10 條第 1 項：「有左列情形之一者，為侵害營業秘密：一、以不正當方法取得營業秘密者。二、知悉或因重大過失而不知其為前款之營業秘密，而取得、使用或洩漏者。三、取得營業秘密後，知悉或因重大過失而不知其為第一款之營業秘密，而使用或洩漏者。四、因法律行為取得營業秘密，而以不正當方法使用或洩漏者。五、依法令有守營業秘密之義務，而使用或無故洩漏者。」

[4] 營業秘密法第 13 條：「依前條請求損害賠償時，被害人得依左列各款規定擇一請求：

一、依民法第二百十六條之規定請求。但被害人不能證明其損害時，得以其使用時依通常情形可得預期之利益，減除被侵害後使用同一營業秘密所得利益之差額，為其所受損害。

二、請求侵害人因侵害行為所得之利益。但侵害人不能證明其成本或必要費用時，以其侵害行為所得之全部收入，為其所得利益。

依前項規定，侵害行為如屬故意，法院得因被害人之請求，依侵害情節，酌定損害額以上之賠償。但不得超過已證明損害額之三倍。」

[5] 刑法第 342 條：「為他人處理事務，意圖為自己或第三人不法之利益，或損害本人之利益，而為違背其任務之行為，致生損害於本人之財產或其他利益者，處五年以下有期徒刑、拘役或科或併科一千元以下罰金。前項之未遂犯罰之。」

[6] 營業秘密法第 14 條：「法院為審理營業秘密訴訟案件，得設立專業法庭或指定專人辦理。當事人提出之攻擊或防禦方法涉及營業秘密，經當事人聲請，法院認為適當者，得不公開審判或限制閱覽訴訟資料。」另外，智慧財產案件審理法第 9、24 及 34 條亦有相類規定。

[7] 智慧財產案件審理法第 11 條第 1 項本文：「當事人或第三人就其持有之營業秘密，經釋明符合下列情形者，法院得依該當事人或第三人之聲

請，對他造當事人、代理人、輔佐人或其他訴訟關係人發秘密保持命令。」

[8] 智慧財產案件審理法第 35 條第 1 項：「違反本法秘密保持命令者，處三年以下有期徒刑、拘役或科或併科新臺幣十萬元以下罰金。」

營業秘密保護—競業禁止與保密約款

【案號：S970303】
資料來源：自由時報 97/11/17

焦點話題

高等法院台南分院的合議庭法官指出，行政院勞委會頒佈有「簽訂競業禁止參考手冊」，對於雇主與勞工是否有簽訂競業禁止約定的必要，應審酌下列等因素：雇主的固有知識與營業秘密是否有保護必要、離職勞工的競業行為應有顯著背信或違反誠實信用原則的事實、雇主與勞方應本於契約自由與誠信原則為約定，及違約金應合理等。

法官特別說明，憲法固然保障人民的工作權，但工作權「並非不得限制的絕對權利」，最高法院著有的多件裁判要旨均指出，勞工對雇主有忠於職責的義務，所以雙方得約定競業禁止約款，亦即勞工離職後在特定期間內不得從事與雇主相同或類似的行業，以免產生不公平競爭，這與憲法工作權的保障，並不牴觸。

重點摘要

1. 對於雇主「營業秘密」的保護，常見以簽訂「競業禁止條款」或「保密契約」的方式為之，而此種約款涉及員工權益，應做合理的約定，方為適法。
2. 實務上對於「競業禁止條款」的內容，提出如上開所述的判斷標準，在擬定契約之際應注意是否符合，以避免遭法院認定該條款無效。

法律觀點

公司僱用員工為公司服勞務，因為工作關係，員工常常得以知

悉公司的「營業秘密」與「智慧財產權」內容。由於員工對於雇主有忠於職責的義務，為保護公司的「智慧財產權」與「營業秘密」，而有要求員工簽署「保密契約」之必要性。常見的是在勞動或僱傭契約裡做類似下列之約定，例如員工承諾在受僱於公司期間以及自公司離職後，均會將機密資訊嚴加保密，而不會使用該項機密資訊，或將之洩漏或以任何方式使第三人知悉。

另外，實務上也常見的是以離職後「競業禁止條款」方式，保護公司的「營業秘密」，也就是約定員工離職後在特定期間內不得從事與雇主相同或類似的行業。這樣的約定，因為涉及到對於員工「憲法」所保障的工作權[1]限制，所以須受法院的嚴格審視其合法性，也就是要符合下列標準：雇主的固有知識與營業秘密是否有保護必要、離職勞工的競業行為應有顯著背信或違反誠實信用原則的事實、雇主與勞工應本於契約自由與誠信原則為約定，及違約金應合理等。

而員工如果違反「保密契約」，可能涉及的法律責任，在刑事方面，可能構成的有「刑法」妨害工商秘密罪[2]或背信罪[3]；民事責任方面，亦有「營業秘密法」的賠償規定[4]。至於違反「競業禁止條款」者，由於通常「競業禁止條款」會有違約金的約定，因此公司得以約定條款所約定的違約金為請求，不過前面已經提到，違約金必須合理，否則其賠償的要求可能不會被法院採納。

管理 Tips

1. 身為契約義務的一方，員工、承包者及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任（CNS 27001 附錄 A.8.1.3）。
2. 管理階層應要求員工、承包者及第三方使用者，依照組織已制定的政策與程序施行安全事宜（CNS 27001 附錄 A.8.2.1）。

3. 所有員工、承包者及第三方使用者對資訊及資訊處理設施的存取權限，在其聘僱、合約或協議終止時，或因變更而調整時，均應予以移除（CNS 27001 附錄 A.8.3.3）。

註釋：

[1] 憲法第 15 條：「人民之生存權、工作權及財產權，應予保障。」

[2] 刑法第 317 條：「依法令或契約有守因業務知悉或持有工商秘密之義務，而無故洩漏之者，處一年以下有期徒刑、拘役或一千元以下罰金。」

[3] 刑法第 342 條：「為他人處理事務，意圖為自己或第三人不法之利益，或損害本人之利益，而為違背其任務之行為，致生損害於本人之財產或其他利益者，處五年以下有期徒刑、拘役或科或併科一千元以下罰金。前項之未遂犯罰之。」

[4] 營業秘密法第 13 條：「依前條請求損害賠償時，被害人得依左列各款規定擇一請求：

一、依民法第二百十六條之規定請求。但被害人不能證明其損害時，得以其使用時依通常情形可得預期之利益，減除被侵害後使用同一營業秘密所得利益之差額，為其所受損害。

二、請求侵害人因侵害行為所得之利益。但侵害人不能證明其成本或必要費用時，以其侵害行為所得之全部收入，為其所得利益。

依前項規定，侵害行為如屬故意，法院得因被害人之請求，依侵害情節，酌定損害額以上之賠償。但不得超過已證明損害額之三倍。」

十一名台鐵訂票系統駭客，檢方緩起訴

【案號：S970401】
資料來源：中央社 96/01/14

焦點話題

民國 94 年春節、中秋節間，台鐵訂票系統屢次遭到電腦駭客入侵，導致系統當機。調查局與警方當時一共查獲 11 名入侵系統的駭客，台北地檢署偵辦後，檢察官參酌這些駭客並無任何前科，且犯後深知悔意，全部給予緩起訴處分。

這 11 名駭客，還包括提供給網友付費下載自行設計撰寫的「火車票自動訂票系統」程式設計師。另有 7 名軍人是為了幫長官訂購火車票，而誤觸法網。

重點摘要

1. 這個案例是屬於以電腦程式「干擾」台鐵訂票電腦系統運作，進而認定構成犯罪行為之典型犯罪型態。
2. 將自己撰寫的程式放在網路上讓網友下載，從事犯罪行為，即使自己未參與該犯罪行為，也構成犯罪。
3. 檢察官給予緩起訴的內容，相當具有教育意義。

法律觀點

本案是因為這 11 名電腦駭客利用自行撰寫或網路下載的電腦程式，連結到台鐵訂票系統自動且連續訂票，造成台鐵訂票系統伺服器及主機代管的中華電信網路伺服器的損害。

這個案件，檢察官認定「駭客」所觸犯的罪是「刑法」第 360 條[1]的妨害電腦使用罪。原因是這些「駭客」因為私利，而使用電腦程式「干擾」台鐵的訂票系統運作以致當機，造成其他旅客無法

訂票與中華電信伺服器無法運作等損害。

同時，本案檢察官還有將自行撰寫軟體供網友付費下載的程式設計師一起究辦。雖然該程式設計師不見得有參與「干擾」台鐵訂票系統的運作，但是因為他讓網友下載「犯罪工具」，為預防此種幫助他人網路犯罪的擴散，「刑法」特別在第 362 條[2]規定此種犯罪型態。而且，本條規定的最重犯罪刑度為 5 年以下有期徒刑，還比前述妨害電腦使用罪的最重本刑 3 年以下有期徒刑還重，足見法律對於這兩種犯罪行為人的評價差異。

值得注意的是，對公務機關進行前述妨害電腦犯罪行為，另有加重其刑 1/2 的規定[3]，由於台鐵在屬性上是交通部隸屬的「公務機關」，檢察官是否有針對前述「駭客」認定加重其罪責，從該媒體報導中，還無法確知。

本案最後係由檢察官以緩起訴的方式進行裁處。所謂「緩起訴」可以理解為「暫時不起訴」。意思是說只要行為人符合一定條件，在緩起訴期間經過後，即視同「未起訴」，而不會有「前科」紀錄。

以本案來說，這些「駭客」因均無前科，且犯後深知悔意，惡行非重大，除有兩名「駭客」須支付 8 萬元與 3 萬元的緩起訴處分金外，其餘僅須於 1 年內在春節連續假日期間，分至各地台鐵車站協助疏導人潮「服完勞務」即可。此種「勞務」相當具有教育意義。

管理 Tips

1. 網路應適切地加以管理與控制，使其不受威脅，並且維護使用網路的系統與 應用程式的安全（CNS 27001 附錄 A.10.6.1）。
2. 對於對台鐵而言，亦需有下列適當管理之考量：
   A. 應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果（CNS 27001 附錄 A.10.10.2）。

B. 應使用適當的鑑別方法，以控制遠端使用者的存取（CNS 27001 附錄 A.11.4.2）。

3. 應識別所有網路服務的安全特徵、服務水準及管理要求，並應被納入網路服務協議中，不論是此等服務是由內部或委外所提供（CNS 27001 附錄 A.10.6.2）。
4. 應保護在公眾網路上傳輸而涉及電子商務的資訊，使其不受詐欺行為、契約爭議及未經授權的揭露與修改（CNS 27001 附錄 A.10.9.1）。
5. 應保護涉及線上交易的資訊，以防止不完整的傳輸、誤選路(mis-routing)、未經授權的訊息修改、未經授權的揭露、未經授權的訊息複製或重演（CNS 27001 附錄 A.10.9.2）。

註釋：

[1] 刑法第 360 條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，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：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，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。」

[3] 刑法第 361 條：「對於公務機關之電腦或其相關設備犯第三百五十八條至第三百六十條之罪者，加重其刑至二分之一。」

假 CNN 電子報，最新電腦病毒

【案號：S970402】
資料來源：蘋果日報 97/08/08

焦點話題

近來發現有電腦駭客以知名新聞頻道 CNN 電子報的方式，大量散布「十大新聞影片」（CNN.com Daily Top 10）的電子郵件，民眾若不警覺而點選其中網址下載後，就會讓電腦中了木馬病毒，不但個人資料可能被竊取，還會成為駭客攻擊的跳板。

防毒軟體業者表示，除熱門網站外，熱門事件也是駭客最愛，例如目前最熱的奧運話題也常被駭客所利用，而民眾則表示由於曾因電腦中毒造成極大的不便，現在都盡量不開不明電子郵件，以免中毒。

重點摘要

1. 新型態的電腦犯罪，我國「刑法」已經有所規範，木馬程式涉及入侵他人電腦、設備與取得他人資料及干擾系統運作的穩定性等犯罪行為，應受相關規定處罰。
2. 新型態的散佈病毒方式越來越難以防範，應該隨時有所警覺，不隨意開啟不明郵件或登入不明網站，以免遭電腦病毒入侵。
3. 定期更新作業系統與定期掃毒，及對重要的資料另做備份，這樣即使電腦中毒了，也可以事後亡羊補牢，以免造成更大的損害。

法律觀點

近年來由於網路溝通便利，許多軟體與程式透過網路快速交換

傳播，而電腦病毒往往夾帶其間，一旦瞬間爆發，會讓人措手不及，殺傷力驚人。而「電腦病毒」到底是什麼呢？「電腦病毒」是一種會不斷自我繁殖或複製的程式碼，通常它會寄存在可執行的檔案之中，或者是軟、硬碟的開機磁區啟動部分。

而「木馬程式」性質上屬於一種遠端管理程式，電腦若在無預警之情形下，遭植入安裝木馬程式，其後果為將藉由電腦對外連線傳遞電腦使用人不欲洩漏於外，或應隱藏與非以明碼方式呈現之資訊，例如連線密碼與信用卡號碼等，或將上揭應秘密之資訊集中，儲存在電腦硬碟特定資料夾中，再由植入者伺機至本機存取。它最常見的傳播技倆，就是透過電子郵件的附帶檔案傳遞。電腦中了木馬程式，不但個人資料被竊取，還會成為駭客攻擊的跳板，以隱藏駭客之身分與攻擊來源，避免被人追查。

因為個人電腦普及，使用者激增，特別是網際網路高度發展後，新型態的網路犯罪類型層出不窮，世界各先進國家如美國與歐盟等，均重新檢討或修訂電腦網路犯罪相關法規，我國「刑法」亦於民國 92 年間，增訂第 36 章之「妨害電腦使用罪章」，而分別就入侵電腦、破壞電磁紀錄、干擾電腦及製造電腦病毒等行為態樣，規定有刑罰之處罰，以維護電腦使用之安全。

就本案而言，木馬程式之運作上，可能涉及到入侵他人電腦、設備與植入遠端控制程式[1]及干擾系統運作的穩定性。因此寄發郵件散佈木馬程式者，即可能因此涉犯「刑法」第 358 條入侵電腦罪[2]與「刑法」第 359 條破壞電磁紀錄罪[3]及「刑法」第 360 條干擾電腦設備罪[4]，最重可處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。至於木馬程式的設計者提供自己或他人使用，同樣構成「刑法」第 362 條[5]之「製作專供犯罪電腦程式」罪，亦可處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。

管理 Tips

1. 組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練（CNS 27001 附錄 A .8.2.2）。
2. 應實做防範惡意碼的監測、預防及復原控制措施以及適切的使用者認知程序（CNS 27001 附錄 A.10.4.1）。
3. 網路應適切地加以管理與控制，使其不受威脅，並且維護使用網路的系統與 應用程式的安全，包括輸送中資訊（CNS 27001 附錄 A.10.6.1）。

註釋：

[1] 【名詞解釋】
遠端控制程式，即可藉由網路於遠端操控電腦之程式。

[2] 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。」

[3] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，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。」

[4] 刑法第 360 條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

[5] 刑法第 362 條：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，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。」

設計假網頁牟利，小駭客才十七歲

【案號：S970403】
資料來源：中國時報 97/08/20

焦點話題

就讀某高中的「小可」扮網路駭客，受人委託製作假網頁（即釣魚網站）程式牟利，刑事局偵九隊到住處查緝時，他稱不知道遭人利用。警方依妨害電腦罪將「小可」等人函辦。

17 歲的「小可」2 年多前迷上設計駭客程式，加上主修資訊，專研電腦程式設計，很快的就在駭客界小有名聲。今年 2 月間，因販售木馬程式與開設「網路徵信社」盜取他人帳號與密碼被判刑的嫌犯許○○，以 4,000 元的代價請「小可」幫忙設計「奇摩」與「無名小站」假網頁程式，讓「小可」成為警方查緝的目標。許○○利用該網站騙取 236 個帳號與密碼，已由奇摩通知被害人修改，減輕損害。

重點摘要

1. 小可設計駭客程式，製作假網頁牟利，已經觸犯「刑法」妨害電腦使用罪章的第 362 條製作犯罪電腦程式罪。
2. 未滿 18 歲之人刑事犯罪，應依「少年事件處理法」之規定辦理。
3. 使用電腦網路雖便利，但仍要提高警覺，以免被人竊取資料，造成嚴重損失。

法律觀點

台灣號稱科技之島，有著蓬勃的資訊產業與技術人才，由於電腦網路之使用便利，截至民國 97 年 1 月 31 日為止，台灣地區上網人口已突破 1,500 萬人，個人上網部分 (12 歲以上民眾) 上網率達

68.51％[1]。這樣的數據除肯定台灣網路發展成效與資訊操作能力的普遍提升外，更值得注意的是網路對日常生活的影響。因此，日後除重視更多元的網路應用軟體與創新服務內容發展外，還應該包括相關的網路規範與權利義務，避免網路便利帶來的副作用。

很多人由於從小接觸電腦，年紀很輕就擁有高超的電腦技術，可是由於心智還不成熟，或是過份沉溺於電腦網路世界，對於外界的事務，缺乏適當的認知，於是往往誤用技術，被人利用而不自知，成為網路犯罪集團的一份子或幫凶。

以這個案子的小可而言，年紀輕輕僅 17 歲，就有高超的電腦程式設計功力，卻被犯罪集團利用，為其設計假網頁（即釣魚網站）程式。小可的行為因為是設計供犯罪集團使用的程式，至少已經觸「刑法」妨害電腦使用罪章第 362 條製作犯罪電腦程式罪[2]，而如果小可知道他所設計的「奇摩」與「無名小站」假網頁程式，是為與犯罪集團一同竊取帳號與密碼，更有可能與犯罪集團構成「刑法」第 359 條破壞電磁紀錄罪[3]的共同正犯[4]。由於小可尚未滿 18 歲，還是少年[5]，因此他的犯罪行為會依照「少年事件處理法」的規定，由少年法院審理[6]。

電腦網路使用雖然便利，但是也潛藏著風險，為避免被人竊取帳號與密碼等資料，造成重大的損失，平常使用網路就應該提高警覺，不隨便下載不明程式，不上不熟悉的網站，才能安心享受電腦網路帶來的便利。

管理 Tips

1. 應實做防範惡意碼的監測、預防及復原控制措施以及適切的使用者認知程序（CNS 27001 附錄 A.10.4.1）。
2. 網路應適切地加以管理與控制，使其不受威脅，並且維護使用網路的系統與 應用程式的安全，包括輸送中資訊（CNS 27001 附錄 A.10.6.1）。

註釋：

[1] 台灣網路資訊中心民國 97 年 2 月 20 日公布之 97 年「台灣寬頻網路使用調查」報告。

[2] 刑法第 362 條：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，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。」

[3] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，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。」

[4] 【名詞解釋】
共同正犯，指二人以上共同實施犯罪，而應負相同的刑事責任。

[5] 少年事件處理法第 2 條：「本法稱少年者，謂十二歲以上十八歲未滿之人。」

[6] 少年事件處理法第 1 條之 1：「少年保護事件及少年刑事案件之處理，依本法之規定；本法未規定者，適用其他法律。」

駭客套密碼，裸照看光光

【案號：S970404】
資料來源：聯合報 97/09/20

焦點話題

台北縣民○○○與網友聊天，套出網友的生日或電話等資料後，逐一破解網友的相簿密碼，下載網友自拍私密照，還威脅須繼續放裸照，被板橋地院依妨害電腦使用等罪判刑，還得服 200 小時義務勞務。

判決書指出，○○○經常在家裡利用「即時通」軟體與網友聊天，與網友熟識後還會互留個人生日、電話或身分證字號等基本資料，作為聯繫用。○○○利用網友懶得設定特殊密碼的特性，開始以網友的生日等數字來猜測對方的即時通或無名小站相簿密碼，結果有八名網友的相簿密碼遭破解。○○○侵入相簿後，下載網友上傳到相簿的精彩私密照存入電腦觀賞，這些照片大多為裸露胸部或下體的自拍照片。

○○○食髓知味，還將網友的密碼變更，導致網友無法登入自己的相簿帳號，進一步威脅女網友繼續拍攝私密照後上傳，否則將公開已下載的裸照。法官認為○○○觸犯包括妨害電腦使用罪與強制罪，且嚴重危害他人生活安全判刑 2 年，但因○○○犯後態度良好，還主動寫悔過書道歉，法官因而予緩刑 5 年。

重點摘要

1. 網路使用雖然方便，但是安全性還是要注意，設定密碼時不要使用懶人密碼，否則很容易被人猜中，造成資料與隱私外洩的結果。
2. 除設定密碼時要多用心，避免被人猜中外，更重要的是不要

把重要的資料或個人隱私放在網路上，否則仍有外洩的疑慮。

法律觀點

網路部落格與相簿這幾年來，在網路上相當的風行，它之所以這麼受歡迎的原因，是因為提供網友們表現自己的管道。尤其是網路相簿，人人都愛看別人美美、有趣的相片，然後看到不錯的就一傳十，十傳百，百傳千，就這樣越來越多人瀏覽，也就更滿足網友愛現的心理。

雖然網路相簿上一些私密照片，會設有密碼以避免外流，然而除駭客入侵的風險外，事實上還有因為設定的是懶人密碼而造成外流之情形。也就是設定密碼時，因為偷懶而以個人生日、電話或身分證字號等基本資料當做密碼，這樣的密碼在有心人刻意的蒐集資料之下，很容易就被突破。以美國副總統候選人為例，也傳出遭網友以其個人公開之資料測試其信箱密碼，而成功侵入其信箱的新聞。

以本案為例，行為人就是利用網路聊天的機會，刻意套取網友的生日等資料，然後再利用網友設定懶人密碼的漏洞，不需要多高段的電腦技術，輕輕鬆鬆就能進入網友的網路相簿，然後更改密碼，取得權限。雖然這樣的行為，有「刑法」妨害電腦使用罪章可資規範，而應構成「刑法」第 358 條之入侵電腦或其相關設備罪[1]與「刑法」第 359 條之破壞電磁紀錄罪[2]，然而事後的追究責任，常常無法彌補已受的傷害。

所以設定密碼時要多用心，不要使用個人生日、電話或身分證字號等基本資料，以避免被人猜中以外，更重要的是不要把重要的資料或個人隱私放在網路上，否則仍有外洩的疑慮，多點事前的預防，就能保護自己的個人隱私不受侵害，何樂而不為？

管理 Tips

1. 組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練（CNS 27001 附錄 A .8.2.2）。
2. 網路應適切地加以管理與控制，使其不受威脅，並且維護使用網路的系統與 應用程式的安全，包括輸送中資訊（CNS 27001 附錄 A.10.6.1）。
3. 管理通行碼的系統應為互動式，並應確保通行碼嚴謹（CNS 27001 附錄 A .11.5.3）。
4. 應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私（CNS 27001 附錄 A.15.1.4）。

註釋：

[1] 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。」

[2] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，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。」

中華郵政：網路郵局個資未遭駭客入侵

【案號：S970405】
資料來源：中央社 97/08/27

焦點話題

對於媒體報導網路郵局疑遭駭客入侵案，中華郵政公司說明，由於郵局客戶資料都存放在後端大型主機，屬於嚴密封閉系統，沒有被破解導致資料洩漏的可能，目前研判網路郵局發生異常的交易可能是客戶端的電腦遭入侵，客戶個人資料外洩所造成。

中華郵政公司於民國 96 年 4 月 27 日處理網路電子商場交易帳務時，發現電子商務合作廠商〇〇〇公司的帳戶交易異常，經追查都是網路郵局交易，立即關閉網站，並向刑事警察局報案。中華郵政公司指出，由於被盜用的帳戶都是輸入帳號與密碼進入交易，在郵局來看都是循正常途徑登入，因此研判駭客是利用客戶端電腦軟體漏洞，從客戶端入侵，取得帳號與密碼。不過，因郵局無法舉證責任在客戶，因此這次駭客事件客戶損失的 100 多萬元仍由郵局負責賠償。

重點摘要

1. 目前電子商務[1]盛行，但是其中隱藏個人資料外洩的風險，可能是被駭客入侵電腦盜取資料，也可能是因為商家控管不當而外洩個人資料。
2. 為防範電腦駭客，最好經常更換網路交易密碼，一旦防毒軟體公司通知更新軟體時，應立即下載，以免電腦產生漏洞。
3. 至於個人資料部分，不要隨便提供給別人，多一份的小心，多一點的保障。

法律觀點

現今各國商業與消費透過電腦與網際網路，包含企業對企業（B2B）與企業對消費者（B2C）的貿易量與商機，這幾年來都是不斷的成長。透過電子商務，就算是偏遠地區的商家，都能以結合電腦與網際網路的方式，來對遠距的消費者銷售商品與提供服務。而由於電子商務講求速度、便捷而可以縮短時空的差距，並透過電腦與網際網路互相聯結，縮短交易時間與成本，而同時滿足廠商與消費者兩方的需要，所以在商業交易上，電子商務越來越風行。

然而電子商務的風行，也隱藏了個人資料外洩的風險，可能是被駭客入侵電腦盜取資料，也可能是因為商家控管不當而外洩個人資料。其中對於駭客入侵行為，我國「刑法」有妨害電腦使用罪章加以規範，對於無故侵入他人電腦[2]與取得他人電磁紀錄[3]干擾他人電腦使用的行為[4]，都有刑罰處罰的規定。而有關個人資料保護的部分，則有「電腦處理個人資料保護法」（以下簡稱「個資法」）的保障，對於適用「個資法」的行業[5]，未妥善保管其所擁有的個人資料，亦有刑事責任[6]與民事賠償責任[7]的規定。

然而再多的規範，仍然阻擋不了希圖僥倖，作奸犯科的人。因此，如何在法令的保障之外，也能夠做好保護自己的動作，就格外的重要。為防範電腦駭客，最好經常更換網路交易密碼，一旦防毒軟體公司通知更新軟體時，應立即下載，以免電腦產生漏洞。至於個人資料部分，需注意不要隨便提供，畢竟多一份的小心，就能多一點的保障。

管理 Tips

1. 網路應適切地加以管理與控制，使其不受威脅，並且維護使用網路的系統與 應用程式的安全，包括輸送中資訊（CNS 27001 附錄 A.10.6.1）。
2. 應保護在公眾網路上傳輸而涉及電子商務的資訊，使不受詐欺行為、契約爭議及未經授權的揭露與修改（CNS 27001 附錄 A.10.9.1）。

3. 應保護涉及線上交易的資訊，以防止不完整的傳輸、誤選路(mis-routing)、未經授權的訊息修改、未經授權的揭露、未經授權的訊息複製或重演（CNS 27001 附錄 A.10.9.2）。
4. 應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私（CNS 27001 附錄 A.15.1.4）。

註釋：

[1]【名詞解釋】
電子商務（EC，Electronic Commerce）是藉由電腦網路將購買與銷售、產品與服務等商業活動結合在一起，進而調整交易的基礎與型態。目前就交易的方式劃分，一般而言，有企業對企業的商務（B2B）與企業對消費者的商業（B2C）二種模式。

[2] 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。」

[3] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，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。」

[4] 刑法第 360 條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

[5] 我國較常見的電子商務，如電視購物、網路購物等，目前尚未經主管機關法務部公告為適用「個資法」的行業，惟個資法的修法方向，是將所有行業均納入，之後即可對於電子商務的商家有所規範。

[6] 電腦處理個人資料保護法第 34 條：「意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法輸出、干擾、變更、刪除或以其他非法方法妨害個人資料檔案之正確，致生損害於他人者，處三年以下有期徒刑、拘役或科新臺幣五萬元以下罰金。」

[7] 電腦處理個人資料保護法第 27 條第 1 項：「公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。」
電腦處理個人資料保護法第 28 條第 1 項：「非公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。」

彩虹橋程式，窺女子房內舉止

【案號：S970406】
資料來源：民視新聞網 97/12/02

焦點話題

許多人的電腦裝設有視訊裝置，不過現在要小心，因為有一種木馬程式「彩虹橋」，除可使電腦自動開機與恢復及傳輸，連同視訊功能也會啟動，屏東縣有一名陳姓女子的電腦，就是中了這個木馬程式，私生活全都被拍下。

陳姓女子的電腦被一名曾姓大學生侵入，利用木馬程式遠端操控，等於是複製陳姓女子的電腦，而且還盜用了陳姓女子的帳號與密碼，將錄下的畫面全 PO 在網路上，房間內的一舉一動全被拍下，當事人完全沒發現。

警方表示，網路世界四通八達，還是要提醒民眾，不要隨便下載來路不明的檔案。

重點摘要

1. 網路世界四通八達，但是也潛伏危機，需要做好資訊保護。
2. 不要隨便下載來路不明的檔案或登入不明網站，避免中了電腦病毒或是木馬程式。
3. 定期掃毒與更新防毒軟體，及對重要的資料另做備份，以避免電腦病毒造成的損害。

法律觀點

電腦與網路的使用帶來生活的便利，很多人不論食、衣、住、行、育、樂各方面都離不開電腦與網路。然而，電腦與網路發達也會帶來一些副作用，例如資訊的外洩等，也成為人類在享受科技進

步之外，不得不面對的問題。

現在翻開報章雜誌，常常可以看到一些電腦遭到入侵，而導致個人資料與私密照片等被人張貼在網路上，而造成當事人的困擾甚或是名譽損失。一般來說，這樣的例子，不外是因為中了電腦病毒（木馬程式）或是駭客入侵，而取得當事人電腦或網路相簿上的資料。因此，對於電腦與網路使用的安全維護，就成為避免發生上述事件的最好方式。例如，不要任意下載不明程式與不上不明網站，是避免電腦病毒或木馬程式入侵的不二法門，而定期掃毒與更新防毒軟體，及對重要的資料另做備份，則是可以避免電腦病毒造成的損害。

就本案例而言，該名大學生可能涉及的刑責，有因入侵他人電腦、設備與植入木馬程式，並干擾系統運作的穩定性，而因此涉犯「刑法」第 358 條入侵電腦罪[1]與「刑法」第 359 條破壞電磁紀錄罪[2]及「刑法」第 360 條干擾電腦設備罪[3]，最重可處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。

此外，他將錄下的影片未經他人同意張貼在網路上，也有「刑法」妨害秘密罪[4]的問題，尤其是錄下的影片涉及到身體隱私的部分，按其情形，也可能另有「刑法」散布猥褻物品罪[5]的問題，以上各罪最重也可以處到 3 年以下有期徒刑、拘役或 3 萬元以下罰金。

管理 Tips

1. 應實做防範惡意碼的監測、預防及復原控制措施以及適切的使用者認知程序（CNS 27001 附錄 A.10.4.1）。
2. 網路應適切地加以管理與控制，使其不受威脅，並且維護使用網路的系統與 應用程式的安全，包括輸送中資訊（CNS 27001 附錄 A.10.6.1）。
3. 應如同相關法令、法規及若適用的契約條文所要求的，確保

資料保護與隱私（CNS 27001 附錄 A.15.1.4）。

註釋：

[1] 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。」

[2] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，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。」

[3] 刑法第 360 條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

[4] 刑法第 315 之 1 條：「有下列行為之一者，處三年以下有期徒刑、拘役或三萬元以下罰金：

一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。

二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

[5] 刑法第 235 條第 1、2 項：「散布、播送或販賣猥褻之文字、圖畫、聲音、影像或其他物品，或公然陳列，或以他法供人觀覽、聽聞者，處二年以下有期徒刑、拘役或科或併科三萬元以下罰金。

意圖散布、播送、販賣而製造、持有前項文字、圖畫、聲音、影像及其附著物或其他物品者，亦同。」

金融網路詐騙多，關鍵字廣告也遭駭

【案號：S970407】
資料來源：卡優新聞網 97/12/02

焦點話題

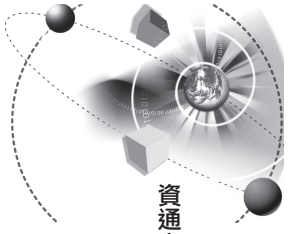
隨著網際網路蓬勃發展，越來越多的金融產品與服務，都可以透過網路銀行來完成，但以「網路釣魚」手法詐騙民眾個人資料的案例，卻也層出不窮。為使消費者在享受網路便利的同時，也能重視交易安全，金管會特別提供各式常見的「網路釣魚」手法，與使用網路銀行的安全小祕訣，希望藉此降低個人資料被盜用的風險，保障自我權益。

許多「網路釣魚」詐騙事件，常常會註冊與銀行相似度極高的網站名稱，只要民眾稍有不慎，就很有可能落入陷阱，而被盜取帳號與密碼等相關個人資料，進而造成財產上的損失。此外，近年來大行其道的網路「關鍵字廣告」，有些駭客會精心設計，當民眾在搜尋時不經意點選，同樣達到誘拐與上鉤的目的。

金管會表示，現在不論是筆記型電腦或無線上網，都已經十分普遍，但民眾最好還是不要在這樣的環境下，使用網路銀行服務，在安全性不足的情況下，很容易讓駭客有機可趁。同時使用網路銀行時，目光盡量不要離開電腦，完成操作後，也應該立即登出，只要接獲網路銀行交易結果通知，馬上就檢核資料是否正確，一經發覺或懷疑網路銀行帳戶與密碼未經授權而被他人使用，須儘速通知銀行。

重點摘要

1. 網路銀行交易便利，不用出門就能辦理金融交易，但是若不注意網路安全，反而會給自己帶來損失。
2. 層出不窮的駭客手段，令人防不勝防，所以要隨時提高警



覺，不認識的網頁與網址，不要隨便點選。

3. 由於無線上網安全性較低，公共電腦也可能暗藏木馬程式，所以應盡量避免使用無線上網或在網咖操作網路銀行。

法律觀點

根據交通部最近的調查統計，台灣的上網人數在民國 97 年已攀升至 1,550 萬人，平均每 1.5 人就有 1 人有上網經驗，這顯示我國網路市場已經成熟，也代表網路成為生活上重要的工具之一。然而網路詐騙事件頻傳，層出不窮的駭客手段，令人防不勝防。現在越來越常見的是一種「網路釣魚」詐騙事件，駭客常常會註冊與銀行相似度極高的網站名稱，而盜取不小心點入的使用者其帳號與密碼等相關個人資料。

金管會於日前為了提醒民眾注意網路銀行使用的安全性，特別提出了五大秘訣，分別是確認網路銀行網址、使用後立即登出、不使用生日與身分證字號等懶人密碼、不要在無線上網時使用網路銀行，及不要在網咖使用網路銀行。而目前流行的關鍵字搜尋也要特別留意，很多人利用關鍵字搜尋網址，但是搜尋到的卻是駭客為釣魚所設的假網址，只要一不小心登入，很可能就被盜走帳號與密碼等個人資料，然後因此造成財產損失。

雖然「刑法」有妨害電腦使用罪章來規範網路駭客等行為，例如「刑法」第 358 條入侵電腦罪[1]與「刑法」第 359 條破壞電磁紀錄罪[2]及「刑法」第 360 條干擾電腦設備罪[3]等，最重可以處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。然而，再多的規定都只是事後的亡羊補牢措施，隨時注意網路使用的安全，才是避免損失的不二法門。

管理 Tips

1. 網路應適切地加以管理與控制，使其不受威脅，並且維護使

用網路的系統與 應用程式的安全，包括輸送中資訊（CNS 27001 附錄 A.10.6.1）。

2. 應保護在公眾網路上傳輸而涉及電子商務的資訊，使不受詐欺行為、契約爭議及未經授權的揭露與修改（CNS 27001 附錄 A.10.9.1）。
3. 應保護涉及線上交易的資訊，以防止不完整的傳輸、誤選路(mis-routing)、未經授權的訊息修改、未經授權的揭露、未經授權的訊息複製或重演（CNS 27001 附錄 A.10.9.2）。
4. 應保護公眾可用系統上可取得資訊的完整性，以防止未經授權的修改（CNS 27001 附錄 A.10.9.3）。
5. 管理通行碼的系統應為互動式，並應確保通行碼嚴謹（CNS 27001 附錄 A .11.5.3）。

註釋：

[1] 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。」

[2] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，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。」

[3] 刑法第 360 條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

貳、資訊公開
（Disclosure）

國務機要費公開審理，旁聽可知機密

【案號：D970101】
資料來源：蘋果日報 97/08/07

焦點話題

總統府於民國 97 年 8 月 5 日宣布將註銷前總統任內核定五大項被列為「絕對機密」的物件與檔案。被註銷列為機密的物件與檔案，包括 90 至 94 年君悅飯店開出的發票明細表與 90 年 1 月 1 日至 95 年 6 月 30 日總統府支領國務機要費檢具的單據及領款人簽收的支出傳票影本等。總統府也已發函最高法院檢察署與台北地方法院，以利司法偵查。

不過，台北地方法院表示，既使這些卷證不屬於機密，依刑事訴訟法的相關規定，民眾還是可能無法看到這些卷證。惟亦有數名法官認為，全案將恢復公開審理，民眾有機會藉由旁聽得知曾被列為機密的文件內容。目前這些卷證資料是在法院的保管中，雖然已無國家機密保護法的適用，但是其公開仍將涉及到政府資訊公開法之相關規定。

重點摘要

1. 「絕對機密」核定與註銷的程序，「國家機密保護法」有詳盡的規定。
2. 註銷「絕對機密」後的文件，屬於自始不構成機密的性質，應屬於公開文書，而得由一般民眾依「政府資訊公開法」規定申請閱覽。
3. 法院保管的刑事卷證，原則上只有相關當事人（不包括被告）或律師可以申請閱覽。

法律觀點

按所謂「國家機密」，依「國家機密保護法」第 2 條規定，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者。而依同法第 4 條之規定，所謂的「絕對機密」，乃是洩露後足以使國家安全或利益遭受非常重大之損害的事項。

其次，「解密」、「降密」與「註銷機密」是兩種完全不同的概念，「解密」、「降密」的前提是，這些卷證原本確實屬機密，而為因應審判的需要，或是由於時間與情況的轉變，使得其機密的必要性降低或消除，才「降密」與「解密」，故若行政機關以「降密」、「解密」的方式處理這些卷證，是表示這些卷證的內容確實屬於機密只是機密性降低。至於「註銷機密」，則是表示這些卷證並沒有涉及「國家機密」。

再者，由於該卷證已經行政機關註銷「絕對機密」，即無「國家機密保護法」第 25 條法院與檢察機關受理之案件涉及「國家機密」時，其程序不公開之規定的適用[1]。另外，公開仍牽涉到政府資訊公開的問題。在該卷證原尚未註銷「絕對機密」之前，根據「政府資訊公開法」第 18 條的規定[2]，該內容是限制公開或不得公開的。不過，現在該卷證既然已經註銷「絕對機密」，依「政府資訊公開法」第 19 條[3]規定，政府即應受理民眾申請公開該卷證內容。然而，由於目前該卷證是由法院保管，並非一般民眾皆可閱卷[4]。故一般大眾要檢閱該卷證全部內容，還是有限制的。目前僅能透過旁聽訴訟的方式，窺見該卷證的部分內容。

管理 Tips

1. 宜識別與定期審查反映組織對資訊保護之需求的機密性或保密協議要求（CNS 27001 附錄 A.6.1.5）。

2. 資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類（CNS 27001 附錄 A.7.2.1）。
3. 應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序（CNS 27001 附錄 A.7.2.2）。

註釋：

[1] 國家機密保護法第 25 條第 1 項：「法院、檢察機關受理之案件涉及國家機密時，其程序不公開之。」

[2] 政府資訊公開法第 18 條第 1 項第 1 款：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：一、經依法核定為國家機密或其他法律、法規命令規定應秘密事項或限制、禁止公開者。」

[3] 政府資訊公開法第 19 條：「前條所定應限制公開或不予提供之政府資訊，因情事變更已無限制公開或拒絕提供之必要者，政府機關應受理申請提供。」

[4] 政府資訊公開法第 18 條第 1 項第 2 款：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：二、公開或提供有礙犯罪之偵查、追訴、執行或足以妨害刑事被告受公正之裁判或有危害他人生命、身體、自由、財產者。」

刑事訴訟法第 33 條：「辯護人於審判中得檢閱卷宗及證物並得抄錄或攝影。無辯護人之被告於審判中得預納費用請求付與卷內筆錄之影本…。」

會議記錄不公開，健保監理會：合於法令

【案號：D970102】
資料來源：中央通訊社 97/09/03

焦點話題

全民監督健保聯盟指衛生署全民健保監理委員會，未公開委員會議過程紀錄摘要，有違全民付託與政府資訊公開法。監理委員會今天表示，目前已依政府資訊公開法規定，上網公告監理委員會議案由與決議內容及出席人員名單，完全合乎法令規定。

監理委員會今天表示，有關委員會議紀錄摘要是否上網公開一事，歷經多次會議討論無法達成共識，在 8 月 29 日召開委員會議時，與會委員以不記名方式表決，決議維持現行公告項目。監理委員會指出，現行作法合於政府資訊公開法第 7 條第 3 項規定，並無不妥。

重點摘要

1. 「政府資訊公開法」有關政府資訊主動公開的主要規定在於第 7 條，規定應由政府主動公開之資訊內容。
2. 現行有關合議制機關之會議記錄，依法需主動公開者有審議案之案由、議程、決議內容及出席會議成員名單。

法律觀點

政府施政之公開與透明，乃國家邁向民主化與現代化的指標之一，為保障人民知的權利，本於「資訊共享」及「施政公開」之理念，我國乃於民國 94 年 12 月制定公佈「政府資訊公開法」，以便利人民公平利用政府依職權所作成或取得之資訊，除增進一般民眾對公共事務之瞭解與信賴及監督外，更能促進民主之參與[1]。

其中有關政府資訊公開之發動，分為「政府主動公開」及「應人民之申請提供」二種[2]，而與人民權益攸關之施政與措施及其他有關之政府資訊，更以主動公開為原則，並應適時為之[3]。有關政府資訊主動公開的主要規定是第 7 條，規定應由政府主動公開之資訊內容，其中第 1 項第 10 款[4]規定之「合議制機關之會議紀錄」，指由依法獨立行使職權之成員組成之決策性機關，其所審議議案之案由、議程、決議內容及出席會議成員名單[5]。

而其所稱「合議制機關」，指該機關決策階層由權限平等並依法獨立行使職權之成員組成者（如「行政院公平交易委員會」）。至於如「都市計畫委員會」等組織，其審議或討論之案件雖屬合議制，但屬機關內部為審議及研究都市計畫而設置之任務編組，因非為機關組織型態者，並不屬之[6]。

至於「衛生署全民健保監理委員會」，依其組織規程規定，屬於合議制之機關組織[7]，故屬於「政府資訊公開法」第 7 條第 1 項第 10 款所規範之範疇，應就其所審議議案之案由、議程、決議內容及出席會議成員名單，依法主動公開之。而其現行作法係將監理委員會議案由與決議內容及出席人員名單上網公告，雖然監理委員會宣稱其現行作法並不違法，然而全民監督健保聯盟對於監理委員會未公開委員會議過程紀錄摘要，擬透過訴願與行政訴訟等司法管道爭取應有之權利，既然相關爭議將進入司法程序，則監理委員會之現行作法是否違反「政府資訊公開法」之規定，即應待司法機關做最終判斷。

管理 Tips

1. 資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類（CNS 27001 附錄 A.7.2.1）。
2. 應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序（CNS 27001 附錄 A.7.2.2）。

註釋：

[1] 政府資訊公開法第 1 條：「為建立政府資訊公開制度，便利人民共享及公平利用政府資訊，保障人民知的權利，增進人民對公共事務之瞭解、信賴及監督，並促進民主參與，特制定本法。」

[2] 政府資訊公開法第 5 條：「政府資訊應依本法主動公開或應人民申請提供之。」

[3] 政府資訊公開法第 6 條：「與人民權益攸關之施政、措施及其他有關之政府資訊，更以主動公開為原則，並應適時為之。」

[4] 政府資訊公開法第 7 條第 1 項第 10 款：「下列政府資訊，除依第十八條規定限制公開或不予提供者外，應主動公開：十、合議制機關之會議紀錄。」

[5] 政府資訊公開法第 7 條第 3 項：「第一項第十款所稱合議制機關之會議紀錄，指由依法獨立行使職權之成員組成之決策性機關，其所審議議案之案由、議程、決議內容及出席會議成員名單。」

[6] 法務部民國 91 年 1 月 10 日法律字第 0090047712 號函。

[7] 全民健康保險監理委員會組織規程第 6 條：「本會設左列各組：一、業務監理組。二、財務監理組。」

全民健康保險監理委員會組織規程第 7 條：「本會置副主任委員、主任秘書、組長、專門委員、視察、專員、科員、助理員、辦事員、書記。」

全民健康保險監理委員會組織規程第 8 條：「本規程所列各職稱之官等及員額，另以編制表定之。

各職稱之職等，依職務列等表之規定。」

全民健康保險監理委員會組織規程第 10 條：「本會每月開會一次，必要時得舉行臨時會議，由主任委員召集，並為主席；主任委員未能出席時，得指定委員一人為主席。

本會開會須有二分之一以上委員出席，決議事項須經出席委員過半數同意行之。」

政府資訊主動公開與因具體個案申請閱覽之不同

【案號：D970103】

資料來源：台北高等行政法院 95 年訴字第 3986 號判決，96 年 5 月 29 日宣判

焦點話題

原告申請閱覽二份函文與相關資訊，目的在於了解被告機關作成將原告調職處分之依據，經被告認有保密之必要，不同意原告的請求。原告其後，向被告申請閱覽與複製上開二函文作成意思前，內部單位之擬稿與作業準備等資訊，又經被告以違反行政程序法第 46 條第 2 項第 1 款與政府資訊公開法第 18 條第 1 項第 3 款規定為由，拒絕所請。原告不服，提起訴願，亦遭決定駁回，遂提起行政訴訟。

法院審理後認為原告之請求不屬於「政府資訊公開法」第 6 條及第 7 條所訂應主動公開之資訊範圍；且原告因不服該調職處分，已提起行政訴訟，依法自應於該行政訴訟程序中，一併對於被告不同意其申請閱覽之處分聲明不服。這是因為行政機關應主動公開之資訊範圍，與具體事件中當事人向行政機關申請閱覽與複印有關卷宗資料者，兩者有所不同。

重點摘要

1. 「政府資訊公開法」有關政府資訊主動公開的主要規定在第 6 條與第 7 條，規定政府應主動公開之資訊內容。
2. 至於具體事件之當事人於行政程序或行政救濟中因主張或維護其法律上之利益，得向行政機關申請閱覽與複印有關卷宗資料者，則應適用「行政程序法」之規定。

法律觀點

基於民主憲政體制的運作之要求，希望可以讓民眾在享有充分

資訊的情況下，參與民主討論過程，世界各國均有類似政府資訊公開之法制。以我國而言，「政府資訊公開法」立法意旨即在於藉政府資訊之公開，便利一般民眾共享與公平利用政府資訊，保障人民知的權利，增進人民對公共事務之瞭解與信賴及監督，並促進民主參與[1]。

其中有關政府資訊公開之發動，分為「政府主動公開」及「應人民之申請提供」二種[2]，而與人民權益攸關之施政與措施及其他有關之政府資訊，更以主動公開為原則，並應適時為之[3]，而於「政府資訊公開法」第 7 條規定應由政府主動公開之資訊內容[4]。如人民依法申請提供遭拒絕者，自得採行對之提起訴願與行政訴訟等行政救濟手段。

惟行政法制內，有關政府資訊的獲得，除「政府資訊公開法」之規定外，尚有於具體行政程序或行政救濟中因主張或維護其法律上之利益，而向行政機關申請閱覽與複印有關卷宗資料者[5]。本案法院審理後認為，關於主動公開政府資訊之範圍與其方式，應以「政府資訊公開法」第 6 條與第 7 條規定者為限。其立法意旨在藉政府資訊之公開，便利一般民眾共享公平利用政府資訊，保障人民知的權利，增進人民對公共事務之瞭解與信賴及監督，並促進民主參與；是上開規定中行政機關應主動公開之資訊範圍，與具體事件之當事人或利害關係人於行政程序中因主張或維護其法律上之利益，所得向行政機關申請閱覽與複印有關卷宗資料者（「行政程序法」第 46 條規定參照），顯有不同。

管理 Tips

1. 資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類（CNS 27001 附錄 A.7.2.1）。
2. 應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序（CNS 27001 附錄 A.7.2.2）。

資訊公開
政府資訊公開法

註釋：

[1] 政府資訊公開法第 1 條：「為建立政府資訊公開制度，便利人民共享及公平利用政府資訊，保障人民知的權利，增進人民對公共事務之瞭解、信賴及監督，並促進民主參與，特制定本法。」

[2] 政府資訊公開法第 5 條：「政府資訊應依本法主動公開或應人民申請提供之。」

[3] 政府資訊公開法第 6 條：「與人民權益攸關之施政、措施及其他有關之政府資訊，更以主動公開為原則，並應適時為之。」

[4] 政府資訊公開法第 7 條第 1 項：「下列政府資訊，除依第十八條規定限制公開或不予提供者外，應主動公開：一、條約、對外關係文書、法律、緊急命令、中央法規標準法所定之命令、法規命令及地方自治法規。二、政府機關為協助下級機關或屬官統一解釋法令、認定事實、及行使裁量權，而訂頒之解釋性規定及裁量基準。三、政府機關之組織、職掌、地址、電話、傳真、網址及電子郵件信箱帳號。四、行政指導有關文書。五、施政計畫、業務統計及研究報告。六、預算及決算書。七、請願之處理結果及訴願之決定。八、書面之公共工程及採購契約。九、支付或接受之補助。十、合議制機關之會議紀錄。」

[5] 行政程序法第 46 條第 1 項：「當事人或利害關係人得向行政機關申請閱覽、抄寫、複印或攝影有關資料或卷宗。但以主張或維護其法律上利益有必要者為限。」

查看與影印考試答案卡，非屬政府資訊公開的範圍

【案號：D970104】

資料來源：台北高等行政法院 95 年訴字第 4311 號判決，96 年 9 月 13 日宣判

焦點話題

本案原告為某國民中學國三學生，參加國民中學學生基本學力測驗 (下稱國中基測)，因不服測驗成績之評定，向國中基測試務委員會的業務承辦學校申請複查國文與自然科目之分數，經複查結果無異動。原告仍不服，再以口頭申請閱覽其原始答案卡，仍經否准。原告猶未甘服，提起訴願，遭決定不受理後，遂向台北高等行政法院（以下簡稱「行政法院」）提起行政訴訟。

行政法院受理後認為，主管考試機關於適用職權範圍內，本於法律授權發布行政命命原非法所不許。本件原告雖指稱限制考生查看或影印答案卡應屬違法，惟本案被告否准原告閱覽原始答案卡，是否適法，應以原告申請時的法規有無賦予應考人此項請求權為準。

重點摘要

1. 有關考試成績評定，向來被認為司法審查應予尊重，除非有明顯的瑕疵，法院不得任意予以更動。
2. 對於考試事項的資訊公開，除「政府資訊公開法」有所限制外，其他相關法規也有規範，故具體而言，仍須視其他法規有無賦予應考人請求閱覽之權利。

法律觀點

我國重視考試制度，每年都有許多考試進行，像是各種國家考

試與升等升學考試等，而考試成績之評定向來是應考人最關心的部分。以現在的考試制度而言，雖然都有複查的制度設計，不過通常應考人更希望的是能夠重新為成績評定，這部分經過「司法院大法官會議釋字」第 319 號解釋[1]後，已確認考試成績的評定，除依形式觀察，即可發現該項成績有顯然錯誤外，不應循應考人的要求任意再行評閱，以維持考試的客觀與公平。

然而如果不是要求成績的重新評定，而是像本案要求查看與影印答案卡的情形，這就涉及政府資訊公開的問題。而就政府資訊公開，雖然有「政府資訊公開法」的規範[2]，但是其實已經有各種行政法規規定有關政府內部資訊的公開，例如本案原告主張的「行政程序法」第 46 條第 1 項[3]與本案涉及的「檔案法」[4]等規定，也都有申請政府資訊閱覽的相關規定。

於本案中，行政法院的立場是認為，原告申請查看與影印原始答案卡，是否適法，應以原告申請時的法規有無賦予應考人此項請求權為準，換言之，必須視上開政府資訊閱覽的相關規定有無賦予申請權而言。不過就考試資料的申請閱覽，其實在相關法規都有限制閱覽的規定，例如像「政府資訊公開法」第 18 條第 1 項第 5 款[5]規定與「行政程序法」第 3 條第 3 項第 8 款[6]規定及「檔案法」第 18 條第 4 款[7]規定等，所以就查閱考試的答案卡部分，即不屬於政府資訊應公開的範圍。

管理 Tips

1. 資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類（CNS 27001 附錄 A.7.2.1）。
2. 應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序（CNS 27001 附錄 A.7.2.2）。

註釋：

[1] 釋字第 319 號解釋文：「考試機關依法舉行之考試，其閱卷委員係於試卷彌封時評定成績，在彌封開拆後，除依形式觀察，即可發見該項成績有顯然錯誤者外，不應循應考人之要求任意再行評閱，以維持考試之客觀與公平。考試院於中華民國七十五年十一月十二日修正發布之『應考人申請複查考試成績處理辦法』，其第八條規定『申請複查考試成績，不得要求重新評閱、提供參考答案、閱覽或複印試卷。亦不得要求告知閱卷委員之姓名或其他有關資料』，係為貫徹首開意旨所必要，亦與典試法第二十三條關於『辦理考試人員應嚴守秘密』之規定相符，與憲法尚無牴觸。惟考試成績之複查，既為兼顧應考人之權益，有關複查事項仍宜以法律定之。」

[2] 政府資訊公開法第 2 條：「政府資訊之公開，依本法之規定。但其他法律另有規定者，依其規定。」

[3] 行政程序法第 46 條第 1 項：「當事人或利害關係人得向行政機關申請閱覽、抄寫、複印或攝影有關資料或卷宗。但以主張或維護其法律上利益有必要者為限。」

[4] 檔案法第 17 條：「申請閱覽、抄錄或複製檔案，應以書面敘明理由為之，各機關非有法律依據不得拒絕。」

[5] 政府資訊公開法第 18 條第 1 項第 5 款：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：五、有關專門知識、技能或資格所為之考試、檢定或鑑定等有關資料，其公開或提供將影響其公正效率之執行者。」

[6] 行政程序法第 3 條第 3 項第 8 款：「下列事項，不適用本法之程序規定：八、考試院有關考選命題及評分之行為。」

[7] 檔案法第 18 條第 4 款：「檔案有下列情形之一者，各機關得拒絕前條之申請：四、有關學識技能檢定及資格審查之資料者。」

參、資訊監察
（Monitors）

通訊保障及監察法，保障人民的秘密通訊自由

【案號：M970101】
資料來源：台中地方法院 96 年訴字第 3687 號判決，96 年 12 月 20 日宣判

焦點話題

甲○○與丙○○均為從事徵信業務者，為圖便利各項徵信調查業務需要，竟依距離之遠近與委託業務是否包括更換錄音帶等不同之工作內容訂價，以每件新臺幣 2,000 元至 1 萬元不等之費用，以按件計酬、月結收費之方式，連續委託他人著電信公司員工服帽，偽裝成該公司員工身分後，至所欲竊聽電話對象住所附近的電信公司電話電信箱，安裝竊聽錄音設備，違法進行竊聽。

其違法竊聽的方式是：先開啟被竊聽者住家附近的電信公司電話交接箱，且不破壞電信箱鎖頭與外觀設備，再找出被竊聽對象的電話線路，並以跳線方式，將電話線路跳線至電信箱外隱密位置，裝設竊聽錄音設備，藉此違法竊聽他人非公開談話內容，而侵害他人的通信秘密。

重點摘要

1. 「通訊保障及監察法」其立法目的在保障人民秘密自由，任何人違法監察他人之通訊，都將依該法第 24 條第 1 項[1] 違法監察他人通訊罪論處。
2. 「通訊保障及監察法」第 24 條關於違法監察他人通訊的處罰規定，係以行為人無合法權源而從事他人通訊之監察行為為處罰之對象，至於是否取得監聽資料並非犯罪構成要件。

法律觀點

由於通訊科技日漸發達，需要有完整的法制規劃，來保障「憲

法」第 12 條規定的秘密通訊自由；且若以通訊作為犯罪之工具，更將嚴重影響他人的權益。因此，為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序[2]，我國乃於民國 88 年間通過「通訊保障及監察法」，作為保障人民秘密自由的基礎規範。

既然「通訊保障及監察法」立法目的在保障人民的秘密自由，任何人違法監察他人通訊，都應該依該法第 24 條第 1 項違法監察他人通訊罪論處[3]。不過也有少數法院實務將之狹義解釋為「通訊保障及監察法」所使用之「通訊監察」或「監察」一詞，係指有關公務員所執行之通訊監察職務而言，與一般民眾竊聽或竊錄等妨害秘密行為毫不相涉。是「通訊保障及監察法」第 24 條第 2 項之處罰對象為直接執行或協助執行通訊監察之公務員或從業人員（例如擔任實施截收、監聽、開拆及檢查職務之警察或電信、郵政人員），同條第 1 項之處罰對象則為前開第 2 項直接執行通訊監察職務以外之公務員（例如故意下令實施違法通訊監察之法官、檢察官或其他有關公務機關人員）[4]。

再者，「通訊保障及監察法」第 24 條關於違法監察他人通訊之處罰規定，係以行為人無合法權源而從事他人通訊監察行為為處罰之對象，不以行為人因違法監察通訊而取得資料為必要，若行為人因此取得或知悉他人的秘密通訊內容，則另有違反「刑法」第 315 條之 1 之妨害秘密罪[5]與「電信法」第 56 條之 1 第 1 項之侵犯他人通信秘密罪[6、7]。

最後，「通訊保障及監察法」於 96 年 7 月份修法後，有一項重大的變革，就是將刑事監察之偵查中通訊監察書的發給權限，由原先檢察官發給的規定，修改為由法院發給[8]；並且條文明文規定違反法律規定進行監聽情節重大者，所取得之內容或所衍生的證據，於司法偵查、審判或其他程序中，均不得採為證據[9]。這樣的修法變革對於人民的秘密通訊自由保障更為周延。

資訊監察
通訊保障及監察法

管理 Tips

1. 應保護傳送資料或支援資訊服務之電源與電信佈纜，以防止竊聽或損害（CNS 27001 附錄 A.9.2.3）。
2. 電子傳訊涉及的資訊應適當地加以保護（CNS 27001 附錄 A.10.8.4）。
3. 應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果（CNS 27001 附錄 A.10.10.2）。

註釋：

[1] 通訊保障及監察法第 24 條：「違法監察他人通訊者，處五年以下有期徒刑。
執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處六月以上五年以下有期徒刑。
意圖營利而犯前二項之罪者，處一年以上七年以下有期徒刑。」

[2] 通訊保障及監察法第 1 條：「為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序，特制定本法。」

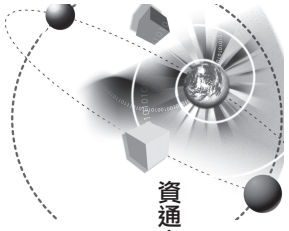
[3] 最高法院 94 年台上字第 5802 號判決參照。

[4] 高等法院花蓮分院 89 年上易字第 91 號判決參照。

[5] 刑法第 315 條之 1：「有下列行為之一者，處三年以下有期徒刑、拘役或三萬元以下罰金：
一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。
二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

[6] 電信法第 56 條之 1 第 1 項：「違反第六條第一項規定侵犯他人通信秘密者，處五年以下有期徒刑，得併科新台幣一百五十萬元以下罰金。」
電信法第 6 條第 1 項：「電信事業及專用電信處理之通信，他人不得盜接、盜錄或以其他非法之方法侵犯其秘密。」

[7] 基隆地方法院 93 年訴字第 473 號判決參照。



[8] 通訊保障及監察法第 5 條第 2 項：「前項通訊監察書，偵查中由檢察官依司法警察機關聲請或依職權以書面記載第十一條之事項，並敘明理由、檢附相關文件，聲請該管法院核發…。」

[9] 例如通訊保障及監察法第 5 條第 5 項「違反本條規定進行監聽行為情節重大者，所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據。」其他如同法第 6 條第 3 項、第 7 條第 4 項及第 31 條第 4 項亦有相同的規定。

MP3 密錄不能當證據！法官：因侵犯隱私

【案號：M970102】
資料來源：台中地方法院 97 年選訴字第 1 號判決，97 年 4 月 30 日宣判

焦點話題

本案檢察官起訴事實是以被告甲係參選民國 97 年第 7 屆立法委員選舉之候選人。因該次選舉尚有案外人乙表態參選，選情甚為緊繃，被告甲為求在該次選舉中能順利當選連任，竟以買票之方式爭取有選舉權人之支持。

而檢察官所憑以起訴之證據則有扣案 MP3 播放器與錄音拷貝光碟片及錄音譯文，扣案錄影拷貝光碟片與翻拍照片，及以上開錄音光碟與錄影光碟片所製作之同步影、音光碟片等。

其中扣案 MP3 播放器與錄音拷貝光碟片及錄音譯文，即證人 C 就被告甲到場後與證人 D 之對話內容部分所為之錄音。法院以該錄音純屬他人非公開之談話，而非證人 C 自己與他人之非公開談話，復因證人 C 錄音當時並未經談話人二人之同意，且證人 C 亦非基於舉發被告甲涉嫌賄選之犯行，而自行錄音搜證。故證人 C 所為上開錄音行為，顯非適法，足以侵害被告甲依憲法第 12 條所應受保障秘密通訊自由，而否定上開錄音之證據能力。

重點摘要

1. 「通訊保障及監察法」其立法目的在保障人民秘密通訊自由。監察他人之通訊，除非有法令之依據，否則都會構成違法，而有刑事責任。
2. 在判決中亦肯定如果是談話中或通訊之當事人一方，是可以進行錄音的。
3. 違法通訊監察而得到的證據，在刑事訴訟程序上有被法院認定為不具證據能力[1]之風險。

法律觀點

「通訊保障及監察法」立法目的在保障人民的秘密通訊自由[2]，所以監察他人之通訊，除非有法令之依據，否則都會構成違法，而有刑事責任[3]。除非依「通訊保障及監察法」第 29 條第 3 款規定，監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者，其所為之監察行為不罰。因此社會上常見以錄音之方式，錄下自己與他人的對話當成證據者，其合法性即是以「通訊保障及監察法」此條規定當成依據。

而此種錄音證據如果呈現在法庭上，能否作為證據，也就是是否具有證據能力？以本案而言，法院即認為私人監聽之行為，依「刑法」第 315 條之 1 及「通訊保障及監察法」第 29 條第 3 款規定「監察者為通訊之一方，而非出於不法目的者，不罰」之規範目的，通訊之一方私自錄音之取證行為，如非出於不法目的，即非「通訊保障及監察法」所規範之行為，其所取得之證據應有證據能力。

反之，如果不符合上開要件，因有侵害依「憲法」第 12 條所應受保障秘密通訊自由之虞。從而，若允許任何私人違法取得之證據，均得進入法院，作為認定他人犯罪與否之證據，將棄「憲法」所宣示應予保障之基本人權不顧，而使法院變相地默示允許或甚而鼓勵私人得以違法方式搜證，並使法院喪失原應有之公平與公正地位。換言之，基於法律體系的一致性，如果是違法通訊監察而得到的證據，在刑事訴訟程序上有被法院認定為不具證據能力之風險，這也更能凸顯保護私人的通訊不受侵害，而體現秘密通訊自由保障之重要性。

另外本案法院另認定，隨著科技之進步與犯罪查緝上之日益困難，一般人均得預見在各公開場所，均有政府相關單位所設立之攝影機，對該公開場所內之不特定人、物為常態性與概括性（非特定性）攝影存證。且一般人亦得預見在各營業場所或私人場所，常

有該營業場所或私人場所之所有人或使用人所設立之攝影機，對該營業場所或私人場所內之不特定人、物為常態性與概括性（非特定性）攝影存證，從而認為該等常態性與概括性（非特定性）攝影存證行為，與「憲法」第 12 條所保障之人民秘密通訊自由並無違背。惟此種見解是否會形成法院實務之一致見解，仍有待時間觀察。

管理 Tips

1. 電子傳訊涉及的資訊應適當地加以保護（CNS 27001 附錄 A.10.8.4）。
2. 應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果（CNS 27001 附錄 A.10.10.2）。

註釋：

[1]【名詞解釋】
證據能力：能作為證據使用的資格。

[2]通訊保障及監察法第 1 條：「為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序，特制定本法。」

[3]通訊保障及監察法第 24 條：「違法監察他人通訊者，處五年以下有期徒刑。
執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處六月以上五年以下有期徒刑。
意圖營利而犯前二項之罪者，處一年以上七年以下有期徒刑。」
刑法第 315 條之 1：「有下列行為之一者，處三年以下有期徒刑、拘役或三萬元以下罰金：
一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。
二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

調查局千萬採購監聽設備，立委擔憂台灣變警察國家

【案號：M970103】
資料來源：雅虎奇摩新聞 97/10/14

焦點話題

據載法務部調查局將耗資新台幣 6,000 萬元招標採購「行動偵蒐系統」，要求規格須具備「偵蒐範圍達 1 萬平方米以上」、「可讓歸向設備尋找到手機位置」、「系統置於車輛上，連接天線即可操作」及「每分鐘處理用戶數不得低於 300 個」，將來調查局依靠這項設備，不需要在私人住宅裝置其他器材，就能進行大量監聽。

立委召開記者會指出，依通訊保障及監察法的規定，監聽須經法院核發「通訊監察書」，調查局採購高規格的監聽設備，是遊走在法律邊緣，有侵犯人民隱私之嫌。依照此項監聽系統規格「偵蒐範圍達 1 萬平方米以上」，以後調查局只要在立法院旁停一輛偵蒐車，包括立法院院區與立委辦公大樓及監察院，都涵括在監聽範圍內，甚至連鄰近的喜來登飯店內消費的客人都難逃監聽。

另外有立委表示，依照通訊保障及監察法規定，監聽需要經過法官同意與核發「通訊監察書」才可以進行，如有緊急狀況，也要事後補申請；但調查局這項監聽設備卻可以同時監聽 300 人，難保不會對非核准監聽對象的隱私造成侵害，所以應該立即停止採購程序。調查局對立委質疑則回應表示，所有監聽案件都經過合法申請通訊監察書，目前沒有停止該項招標案的理由。

重點摘要

1. 依「通訊保障及監察法」規定，監聽發起需要經由法院核發「通訊監察書」。
2. 依「通訊保障及監察法」規定[1]，執行監聽機關不得於私人

住宅裝置竊聽器、錄影設備或其他監察器材。

3. 公務員若有不法監聽者，除其本身有刑事責任外，國家亦應對受害者負擔賠償責任。

法律觀點

「通訊保障及監察法」是為了保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序。因此，於確保國家安全與維護社會秩序之目的下，「通訊保障及監察法」雖然規定得以發動通訊監察之情況，然仍必須符合比例原則之要求，不得逾越所欲達成目的之必要限度，且應以侵害最少之適當方法為之[2]。另外，通訊監察之發起，依照「通訊保障及監察法」之規定，係必須經由權責機關聲請並以書面敘明理由與檢附相關文件，聲請該管法院核發「通訊監察書」，即使有急迫之情形，亦須於事後聲請該管法院補行同意[3]。

以本案而言，法務部調查局耗資 6,000 萬元招標採購「行動偵蒐系統」，要求規格須具備「偵蒐範圍達 1 萬平方米以上」、「可讓歸向設備尋找到手機位置」、「系統置於車輛上，連接天線即可操作」及「每分鐘處理用戶數不得低於 300 個」。此項監聽設備之採購，雖然可望大幅增進通訊監察之效果，然仍遭質疑會有違反「通訊保障及監察法」規定之虞，蓋「通訊保障及監察法」第 13 條第 1 項但書規定，執行監聽機關不得於私人住宅裝置竊聽器、錄影設備或其他監察器材，則若採購此項設備後，執行監聽機關只需將裝置上開系統之車輛停在私人住宅外，即可因其強大的偵蒐範圍而達成監聽之目的。

惟此項設備之採購是否影響通訊監察執行之合法性，仍應視其使用時，執行機關是否遵照「通訊保障及監察法」規定辦理，蓋科技設備應屬中性，重要的還是要視使用者如何使用。而公務機關若有違反「通訊保障及監察法」規定，違法監聽人民之通訊時，除其本身自應負相關刑事責任外[4]，國家亦應對人民之損害負起「國家

賠償」責任[5]，最高按其監察通訊日數，以每一受監察人每日新台幣 1,000 元以上至 5,000 元以下計算。但能證明其所受之損害額高於該金額者，不在此限[6]。

管理 Tips

應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果（CNS 27001 附錄 A.10.10.2）。

註釋：

[1] 通訊保障及監察法第 13 條第 1 項：「通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。」

[2] 通訊保障及監察法第 2 條：「通訊監察，除為確保國家安全、維持社會秩序所必要者外，不得為之。前項監察，不得逾越所欲達成目的之必要限度，且應以侵害最少之適當方法為之。」

[3] 通訊保障及監察法第 5 條第 2 項前段：「前項通訊監察書，偵查中由檢察官依司法警察機關聲請或依職權以書面記載第十一條之事項，並敘明理由、檢附相關文件，聲請該管法院核發。」另外同法第 6 條第 1 項後段、第 7 條第 2、3 項亦有相類規定。

[4] 通訊保障及監察法第 24 條：「違法監察他人通訊者，處五年以下有期徒刑。執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處六月以上五年以下有期徒刑。意圖營利而犯前二項之罪者，處一年以上七年以下有期徒刑。」

[5] 通訊保障及監察法第 22 條：「公務員或受委託行使公權力之人，執行職務時違反本法或其他法律之規定監察他人通訊或洩漏、提供、使用監察通訊所得之資料者，國家應負損害賠償責任。依前項規定請求國家賠償者，適用第十九條第二項、第三項及第二十條之規定。」

[6] 通訊保障及監察法第 21 條第 1 項：「前條之損害賠償總額，按其監察通訊日數，以每一受監察人每日新台幣一千元以上五千元以下計算。但能證明其所受之損害額高於該金額者，不在此限。」

竊聽外遇，仍有通訊保障及監察法之適用

【案號：M970104】

資料來源：最高法院 97 年台上字第 4546 號判決，97 年 9 月 18 日宣判

焦點話題

乙○○與甲○○為夫妻關係，乙○○因懷疑甲○○與他人有曖昧關係，故於民國 89 年 9 月間二人尚同住於台南市某住處時，乙○○為過濾甲○○的交往對象，無故在上開住處以錄音機竊錄甲○○所申請之的市內電話非公開談話的通話內容，因其後乙○○將上開竊錄所得的通話內容播放予甲○○與他人聽聞，甲○○始知悉上情，而提出告訴。後一審判決乙○○有罪後，復經高等法院台南分院駁回乙○○之上訴，並宣告緩刑 2 年。

乙○○向最高法院提起上訴，主張法律為保障「婚姻制度」，不僅於刑法規定通姦行為[1]的處罰，於民法親屬編亦設有「婚姻」專章，故夫妻間彼此具有「忠誠義務」與「貞操義務」[2]，配偶之一方應有權探知他方違反上述義務的情形。從而，為行使婚姻所保障配偶負有忠誠義務的權利，而監察他人電話通訊的內容，應不構成違法云云。惟其主張不為最高法院所採納，而駁回其上訴，全案確定。

最高法院認為配偶的一方如有外遇，對他方而言，自屬極難忍受之事，是有外遇的一方必極力隱藏，以避免他方知悉，此項隱密在道德上雖然可議，但「通訊保障及監察法」並未排除此種隱私權的保障。因此乙○○所為之竊錄行為，縱其目的係在探知配偶有無外遇或通姦的情形，與「無故」以錄音竊錄他人非公開談話的情形有別，而不構成刑法第 315 條之 1 之罪責[3]，惟仍有「通訊保障及監察法」第 24 條規定[4]適用。

重點摘要

1. 竊錄行為之目的如在於探知配偶有無外遇或通姦的情形，與「無故」以錄音竊錄他人非公開談話的情形有別。
2. 「通訊保障及監察法」並未排除外遇配偶通訊自由之保障，故即使是配偶的另一方亦不可任意侵害。

法律觀點

隨著社會環境不斷變遷，現代社會的離婚率越來越高，根據統計台灣是亞洲離婚率最高的國家。離婚的原因常見不外乎個性不合與經濟因素等，而因為配偶外遇的原因也有越來越多的趨勢。配偶外遇，對於另一方自然是很大的打擊，也因此常常有人為了抓姦，不惜花費重金，請徵信社調查，或是利用竊聽或竊錄的手段來探知，本件案例就是這樣的情況。

就竊錄他人的電話而言，較常涉犯的法條有「刑法」第 315 條之 1 的妨害秘密罪與「通訊保障及監察法」第 24 條的非法監聽罪等。其中，「刑法」第 315 條之 1 的要件裡，有所謂「無故」的要件，也就是沒有正當理由，而在本案中，最高法院認為竊錄行為之目的如在於探知配偶有無外遇或通姦的情形，並不是「無故」，所以不構成「刑法」第 315 條之 1 的妨害秘密罪。

可是最高法院還是認為「通訊保障及監察法」並未排除外遇之一方極力隱藏，以避免他方知悉，此種不道德隱密的保護。因此，除非為竊錄行為的配偶一方有「通訊保障及監察法」第 29 條規定[5]不罰之例外狀況，否則，仍然應該依「通訊保障及監察法」第 24 條規定處罰。

管理 Tips

1. 應建立資訊處理設施使用的監視程序，並定期審查監視活動

的結果（CNS 27001 附錄 A.10.10.2）。

註釋：

[1] 刑法第 239 條：「有配偶而與人通姦者，處一年以下有期徒刑。其相姦者亦同。」

[2] 民法第 1001 條：「夫妻互負同居之義務。但有不能同居之正當理由者，不在此限。」

民法第 1052 條第 1 項第 1、2 款：「夫妻之一方，有下列情形之一者，他方得向法院請求離婚：一、重婚。二、與配偶以外之人合意性交。」

[3] 刑法第 315 條之 1：「有下列行為之一者，處三年以下有期徒刑、拘役或三萬元以下罰金：

一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。

二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

[4] 通訊保障及監察法第 24 條：「違法監察他人通訊者，處五年以下有期徒刑。

執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處六月以上五年以下有期徒刑。

意圖營利而犯前二項之罪者，處一年以上七年以下有期徒刑。」

[5] 通訊保障及監察法第 29 條：「監察他人之通訊，而有下列情形之一者，不罰：

一、依法律規定而為者。

二、電信事業或郵政機關（構）人員基於提供公共電信或郵政服務之目的，而依有關法令執行者。

三、監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者。」

肆、資訊應用
（Application）

雅虎奇摩拍賣採用自然人憑證與動態密碼

【案號：A970101】
資料來源：ZDNet 97/07/15

焦點話題

為提升拍賣服務的帳號安全認證等級，雅虎奇摩宣佈採用自然人憑證與中華電信動態密碼鎖（OTP）[1]，將帳號登入認證由傳統的單因素[2]，提高為雙因素[3]認證。雅虎奇摩所推出「帳號安心鎖」新服務，是透過採用內政部自然人憑證的認證令牌的其中一種，在既有的帳號與密碼之外，再加上一道關卡，並藉此提高登入安全性。該服務將首先應用在拍賣，未來並將進一步推展到其他對身分認證較敏感的服務上，如電子郵件等。

重點摘要

1. 使用「自然人憑證」作為身分認證用途，其帳戶安全性大幅度提高。
2. 「自然人憑證」在法律定位上是與簽名或印章具有相同效力。
3. 登入帳號僅使用文字或符號的帳號（ID）與密碼（PASSWORD）其安全性是有疑慮的。

法律觀點

「自然人憑證」是由內政部簽發予個人使用的身分認證工具。在運作機制上，內政部是屬於「電子簽章法」第 2 條所稱的「憑證機構」，用以簽發確認簽署人身分資格的電子形式證明[4]，其依據「電子簽章法」第 11 條第 1 項的規定[5]，提供民眾簽發憑證服務。在屬性定位上，「自然人憑證」相當於戶政事務所核發的「印鑑證明書」，只是以往到戶政事務所去申請核發「印鑑證明」是帶自己

的印章去核對身分。現在因應網路應用需求，在「自然人憑證」IC卡中，除了有內政部簽發的「憑證」證明自然人身分外，也同時證明該IC卡中「私密金鑰」的使用人是該自然人。對應前述的「印鑑證明書」的概念，「自然人憑證I」C卡是內建「印鑑＝私密金鑰」與「印鑑證明書＝憑證」。

從這樣的屬性定位上理解，就可以知道自然人憑證在身分認證功能上所扮演的重要角色與其所具有的公信力。也因此，在「自然人憑證」以往應用領域上，均將其應用在身分認證敏感度高的應用，例如網路報稅與部分網路銀行的應用。

由此可知，在登入電腦系統或網路帳號時，如以單純的文字或符號作為登入帳號與密碼，透過駭客程式或釣魚網路即可輕易破解，其安全性確實是有疑慮。因此，不論在政府或企業，利用「自然人憑證」或其他安全認證機制，確保個人帳號使用安全，確實有其相當之必要性。

另一方面，由於「自然人憑證」在屬性定位上具有「簽名或印章」的法律效力，也因此，在勾稽網路身分與網路交易行為上，也具有比一般使用文字或符號的帳號與密碼機制更具有交易上的證明力。因此，使用「自然人憑證」可以確保身分認證的可信賴性，同時也可以強化網路交易的安全性。

管理 Tips

1. 應保護在公眾網路上傳輸而涉及電子商務的資訊，使不受詐欺行為、契約爭議及未經授權的揭露與修改（CNS 27001附錄A.10.9.1）。
2. 應保護涉及線上交易的資訊，以防止不完整的傳輸、誤選路(mis-routing)、未經授權的訊息修改、未經授權的揭露、未經授權的訊息複製或重演（CNS 27001附錄A.10.9.2）。
3. 應使用適當的鑑別方法，以控制遠端使用者的存取（CNS

27001 附錄 A.11.4.2）。

4. 應讓所有使用者應有僅限其個人使用的唯一識別符號（使用者 ID），並應選擇適切的鑑別技術，以證實使用者宣稱的身分（CNS 27001 附錄 A.11.5.2）。
5. 對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新（CNS 27001 附錄 A.15.1.1）。

註釋：

[1]【名詞解釋】
動態密碼鎖，全文為 One Time Password（OPT），簡單的說，就是每次都要輸入不同的密碼，而這個密碼是由系統指定的隨機密碼，藉此防止密碼被不當竊取。至於取得系統指定的隨機密碼方式，有需要另外搭配其他裝置或以其他媒介取得的方法。

[2]【名詞解釋】
單因素認證是指以使用者一般常用之登入密碼執行登入認證之機制。

[3]【名詞解釋】
雙因素認證（Two-factor authentication）**是指除使用者一般常用之登入**密碼外，再新增第二層認證機制，例如加入晶片卡，以執行第二道登入認證之機制。

[4]電子簽章法第 2 條第 1 項第 5 款與第 6 款：「五、憑證機構：指簽發憑證之機關、法人。六、憑證：指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。」

[5]電子簽章法第 11 條第 1 項：「憑證機構應製作憑證實務作業基準，載明憑證機構經營或提供認證服務之相關作業程序，送經主管機關核定後，並將其公布在憑證機構設立之公開網站供公眾查詢，始得對外提供簽發憑證服務。其憑證實務作業基準變更時，亦同。」

捷元積極轉型，網路交易破億元

【案號：A970102】
資料來源：工商時報 96/08/08

焦點話題

捷元自民國 94 年起積極與經濟部商業司共同合作推動運用工商憑證 PKI[1] 技術機制，進行安全網路下單系統開發。短短 2 年內超過半數經銷商申請 PKI 工商憑證，在捷元 B2B（企業對企業）經銷商專區上進行交易。第二季 B2B 經銷商專區每日流量最高達 15,000 人次以上，B2B 網路下單訂單占捷元每日訂單總數 4 成以上，7 月份網路下單金額更已超過 1 億元，占整體營收近 2 成。

捷元積極轉型的成效顯現，未來將持續以網路機制支援實體作業，可減少接單作業人力成本，並減少人力運用於產品與通路的開發，服務更多的經銷商與供應商，大幅提升公司整體競爭力。

重點摘要

1.「工商憑證」是企業在網路上的「大小章」。
2. 應用數位簽章機制讓電子文件有「推定為真正」的證據力。

法律觀點

透過網際網路建構 B2B 電子商務交易平台，已經不是什麼新鮮事。但是使用經濟部工商憑證管理中心簽發的「工商憑證」在 B2B 電子商務交易平台（以下簡稱「交易平台」）則是還在起步與發展中的應用。

以企業觀點來看「工商憑證」，它是企業在網路上的「大小章」或「印鑑章」。為什麼會具有這樣的重要性，是因為「工商憑證」係由經濟部依據企業申請經比對公司資料正確後，始發予企業使用

的網路印鑑。經濟部提供「工商憑證」的目的是為建構電子化政府應用所需的身分認證機制。

至於為什麼要使用「工商憑證」在電子商務的交易平台上？除有公信力的身分認證機制考量外，也有使電子文件[2]具有法律上證據力的優勢。有關電子文件的證據力，其主要依據是「民事訴訟法」第 358 條[3]規定私文書[4]如經本人或其代理人簽名或蓋章者，推定為真正。也因此，使用「工商憑證」的數位簽章[5]機制簽署網路交易所需的電子文件，在證據力上的效力也可以取得「推定該私文書為真正」的法律效力，藉此保障網路交易的安全，也取得舉證責任的優勢地位。

因此，不論是電子化政府的應用或電子商務交易，應用政府或民間的數位簽章與憑證機制在交易系統中，應是有效確保交易安全的重要機制。

管理 Tips

1. 應保護在公眾網路上傳輸而涉及電子商務的資訊，使不受詐欺行為、契約爭議及未經授權的揭露與修改（CNS 27001 附錄 A.10.9.1）。
2. 應保護涉及線上交易的資訊，以防止不完整的傳輸、誤選路 (mis-routing)、未經授權的訊息修改、未經授權的揭露、未經授權的訊息複製或重演（CNS 27001 附錄 A.10.9.2）。
3. 應讓所有使用者應有僅限其個人使用的唯一識別符號（使用者 ID），並應選擇適切的鑑別技術，以證實使用者宣稱的身分（CNS 27001 附錄 A.11.5.2）。
4. 對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新（CNS 27001 附錄 A.15.1.1）。

註釋：

[1]【名詞解釋】

PKI：全文為 Public Key Infrastructure 即公開金鑰基礎建設。其所指為使用公開金鑰與私密金鑰的數位簽章機制，該機制在電子簽章法的要求是要由合法的憑證機構簽發憑證始具有電子簽章法第 9 條的法律效力。

[2] 電子簽章法第 2 條第 1 項第 1 款：「電子文件：指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。」

[3] 民事訴訟法第 358 條第一項：「私文書經本人或其代理人簽名、蓋章或按指印或有法院或公證人之認證者，推定為真正。」

[4]【名詞解釋】

私文書，是指由私人所製作的文書，主要是有別於公文書即公務員職務上製作的文書而作的法律上區分。像是一般企業或個人間的交易文件都是屬於私文書的範圍。

[5] 電子簽章法第 2 條第 1 項第 3 款：「數位簽章：指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。」

政府電子發票整合平台上線

【案號：A970103】
資料來源：ZDNet 96/02/26

焦點話題

財政部建構之電子發票整合服務平台已正式上線啟用，期能普及電子交易之應用。

政府大力推動電子發票平台，被認為是推廣公鑰基礎建設（PKI, Public Key Infrastructure ）的一環。由於電子發票系統須仰賴 PKI 進行認證，推動電子發票之餘，也有助於推廣企業採用 PKI，並為未來更多電子交易應用鋪路。

所謂電子發票，是以網際網路或其他方式開立、傳輸或接收之統一發票，為財政部自民國 89 年起試行的計劃，並於 94 年起陸續由業者開發自用或銷售給其他企業採用，例如○公司自行開發之電子發票系統，即提供關係企業與供應商使用。與早前計劃不同的是，此次財政部推出之電子發票整合服務平台，是首個由政府推動與公開招標設置的免費電子發票平台，企業不需另外向電子發票系統供應商購買，可直接向政府申請使用。

相較於傳統之手開式或電子計算機發票，電子發票具有節省人工處理成本、減少實體發票儲存成本、省去郵寄成本及縮短買賣方交易週期等好處。

電子發票整合平台雖然提供了 B2B（企業對企業）與 B2C（企業對消費者）兩種服務，但初步僅針對 B2B 部分推廣，且不限產業。

欲申請使用 B2B 電子發票功能之企業必須未欠繳營業稅與營利事業所得稅等稅款或罰鍰，且擁有經濟部核發之 PKI 工商憑證 IC 卡，即可至電子發票入口網站線上申請，通過後便可免費使用電子發票平台來開立、傳輸、交換及儲存電子發票。

重點摘要

1. 電子發票具有節省人工處理成本、減少實體發票儲存成本、省去郵寄成本及縮短買賣方交易週期等好處。
2. 電子發票使用「PKI 工商憑證機制」，可以確保電子發票上所記載內容與發票人資格的真正與適法。
3. 電子發票是電子文件[1]，在符合一定條件下可以取代依法令必須使用、提出正本或保存書面文件的場合。

法律觀點

統一發票是營業稅的繳納憑證。大部分 B2C（企業對消費者）的統一發票還是以紙本為主，目前還不能交付電子文件格式的統一發票，其中原因之一是對於消費者來說，電子發票在兌獎與索取方式上還沒有完全克服。

然而在 B2B（企業對企業）的交易環境需求，統一發票是進銷項的憑證之一。因此，在文書作業上，只要能證明發票人資格與交易內容，就能以電子文件方式呈現與傳輸。惟因電子文件本身如未以加密[2]方式處理，該文件即易遭竄改，也無法證明該文件真正。因此，於電子文件上簽署電子簽章[3]後，即可辨認簽署人身分與資格及電子文件內容真偽。其中，對於使用公開金鑰基礎建設（PKI, Public Key Infrastructure ）的簽章技術以「數位簽章」[4]名之。

基此，為讓 B2B 交易雙方得以取得電子文件格式的營業稅憑證，且得以電子方式傳輸與驗證，對於電子發票之使用，即由財政部制定相關作業規範以使電子發票符合「電子簽章法」的要求。

其中，「電子簽章法」對於依法令規定應以書面為之者[5]與依法令規定應提出文書正本或原本[6]及文書依法令應以書面保存者[7]，均要求「其內容可完整呈現，並可於日後取出供查驗者」，其所指即為電子文件加簽電子簽章或數位簽章，即得依法取代文書或書面正

本等。所以，在電子發票系統運作上，必須使用數位簽章即經濟部「工商憑證」，其目的即在於此。

管理 Tips

1. 應保護在公眾網路上傳輸而涉及電子商務的資訊，使不受詐欺行為、契約爭議及未經授權的揭露與修改（CNS 27001 附錄 A.10.9.1）。
2. 應保護涉及線上交易的資訊，以防止不完整的傳輸、誤選路(mis-routing)、未經授權的訊息修改、未經授權的揭露、未經授權的訊息複製或重演（CNS 27001 附錄 A.10.9.2）。
3. 應讓所有使用者應有僅限其個人使用的唯一識別符號（使用者 ID），並應選擇適切的鑑別技術，以證實使用者宣稱的身分（CNS 27001 附錄 A.11.5.2）。
4. 使用密碼控制措施以保護資訊的政策應加以發展與實作（CNS 27001 附錄 A.12.3.1）。
5. 應備妥適當的金鑰管理，以及支援組織使用密碼技術（CNS 27001 附錄 A.12.3.2）。
6. 對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新（CNS 27001 附錄 A.15.1.1）。

註釋：

[1] 電子簽章法第 2 條第 1 款：「電子文件：指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。」

[2] 電子簽章法第 2 條第 4 款：「加密：指利用數學演算法或其他方法，將電子文件以亂碼方式處理。」

[3] 電子簽章法第 2 條第 2 款：「電子簽章：指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。」

[4] 電子簽章法第 2 條第 3 款：「數位簽章：指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。」

[5] 電子簽章法第 4 條：「經相對人同意者，得以電子文件為表示方法。

依法令規定應以書面為之者，如其內容可完整呈現，並可於日後取出供查驗者，經相對人同意，得以電子文件為之。

前二項規定得依法令或行政機關之公告，排除其適用或就其應用技術與程序另為規定。但就應用技術與程序所為之規定，應公平、合理，並不得為無正當理由之差別待遇。」

[6] 電子簽章法第 5 條：「依法令規定應提出文書原本或正本者，如文書係以電子文件形式作成，其內容可完整呈現，並可於日後取出供查驗者，得以電子文件為之。但應核對筆跡、印跡或其他為辨識文書真偽之必要或法令另有規定者，不在此限。

前項所稱內容可完整呈現，不含以電子方式發送、收受、儲存及顯示作業附加之資料訊息。」

[7] 電子簽章法第 6 條：「文書依法令之規定應以書面保存者，如其內容可完整呈現，並可於日後取出供查驗者，得以電子文件為之。

前項電子文件以其發文地、收文地、日期與驗證、鑑別電子文件內容真偽之資料訊息，得併同其主要內容保存者為限。

第一項規定得依法令或行政機關之公告，排除其適用或就其應用技術與程序另為規定。但就應用技術與程序所為之規定，應公平、合理，並不得為無正當理由之差別待遇。」

附錄

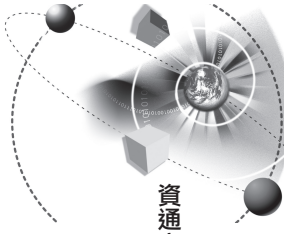
CNS 27001 附錄 A

附錄
CNS 27001 附錄 A

CNS 27001 **附錄** A.6 **資訊安全的組織**	
A.6.1	**內部組織** **目標：於組織內管理資訊安全。**
A.6.1.5	宜識別與定期審查反映組織對資訊保護之需求的機密性及保密協議要求。

CNS 27001 **附錄** A.7 **資訊管理**	
A.7.2	**資訊分類** **目標：確保資訊受到適切等級的保護。**
A.7.2.1	資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類。
A.7.2.2	應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序。

CNS 27001 **附錄** A.8 **人力資源安全**	
A.8.1	**聘僱之前** **目標：確保員工、承包者及第三方使用者了解其責任，並勝任其所被認定的角色，以降低竊盜、詐欺或設施誤用的風險。**
A.8.1.1	員工、承包者及第三方使用者的安全角色與責任，應依照組織的資訊安全政策加以界定與文件化。
A.8.1.3	身為契約義務的一方，員工、承包者及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任。
A.8.2	**聘僱期間** **目標：確保所有員工、承包者及第三方使用者認知資訊安全的威脅與關切事項、其基本責任與強制責任，並有能力在日常工作中支持組織安全政策與降低人為錯誤的風險。**
A.8.2.1	管理階層應要求員工、承包者及第三方使用者，依照組織已制定的政策與程序施行安全事宜。
A.8.2.2	組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。
A.8.2.3	對於違反安全的員工，應有正式的懲處過程。
A.8.3	**聘僱的終止或變更** **目標：確保員工、承包者及第三方使用者以有條理的方式脫離組織或變更聘僱。**
A.8.3.3	所有員工、承包者及第三方使用者對資訊及資訊處理設施的存取權限，在其聘僱、合約或協議終止時，或因變更而調整時，均應予以移除。



CNS 27001 **附錄** A.9 **實體與環境安全**	
A.9.2	**設備安全** **目標：防止資產的遺失、損害、竊盜或破解，並防止組織活動的中斷。**
A.9.2.3	應保護傳送資料或支援資訊服務之電源與電信佈纜，以防止竊聽或損害。

CNS 27001 **附錄** A.10 **通訊與作業管理**	
A.10.4	**防範惡意碼與行動碼** **目標：保護軟體與資訊的完整性。**
A.10.4.1	應實做防範惡意碼的監測、預防及復原控制措施以及適切的使用者認知程序。
A.10.6	**網路安全管理** **目標：確保對網路內資訊與支援性基礎建設的保護。**
A.10.6.1	網路應適切地加以管理與控制，使其不受威脅，並且維護使用網路的系統與應用程式的安全，包括輸送中資訊。
A.10.6.2	應識別所有網路服務的安全特徵、服務水準及管理要求，並應被納入網路服務協議中，不論是此等服務是由內部或委外所提供。
A.10.7	**媒體的處置** **目標：防止資產被未經授權的揭露、修改、移除或破壞，以及營運活動的中斷。**
A.10.7.3	應建立資訊的處置及儲存程序，以保護此資訊免於未經授權的揭露或誤用。
A.10.8	**資訊交換** **目標：維護組織內及與任何外部個體所交換資訊與軟體的安全。**
A.10.8.4	電子傳訊涉及的資訊應適當地加以保護。
A.10.9	**電子商務服務** **目標：確保電子商務服務的安全性及其安全的使用。**
A.10.9.1	應保護在公眾網路上傳輸而涉及電子商務的資訊，使不受詐欺行為、契約爭議及未經授權的揭露與修改。
A.10.9.2	應保護涉及線上交易的資訊，以防止不完整的傳輸、誤選路 (mis-routing)、未經授權的訊息修改、未經授權的揭露、未經授權的訊息複製或重演。
A.10.9.3	應保護公眾可用系統上可取得資訊的完整性，以防止未經授權的修改。
A.10.10	**監視** **目標：偵測未經授權的資訊處理活動。**
A.10.10.2	應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果。

CNS 27001 **附錄** A.11 **存取控制**	
A.11.4	**網路存取控制** **目標：防止網路服務遭未經授權的存取。**
A.11.4.2	應使用適當的鑑別方法，以控制遠端使用者的存取。
A.11.5	**作業系統存取控制** **目標：防止作業系統遭未經授權的存取。**
A.11.5.2	應讓所有使用者應有僅限其個人使用的唯一識別符號（使用者 ID），並應選擇適切的鑑別技術，以證實使用者宣稱的身分。
A.11.5.3	管理通行碼的系統應為互動式，並應確保通行碼嚴謹。

CNS 27001 **附錄** A.12 **資訊系統獲取、開發及維護**	
A.12.3	**密碼控制措施** **目標：藉由密碼方式以保護資訊的機密性、鑑別性或完整性。**
A.12.3.1	使用密碼控制措施以保護資訊的政策應加以發展與實作。
A.12.3.2	應備妥適當的金鑰管理，以支援組織使用密碼技術。

CNS 27001 **附錄** A.15 **遵循性**	
A.15.1	**遵循適法性要求** **目標：避免違反任何法律、法令、法規或契約義務，以及任何安全要求。**
A.15.1.1	對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。
A.15.1.3	應依據法令、法規、契約及營運要求，保護重要紀錄，免於遺失、毀損或偽造。
A.15.1.4	應如同相關法令、法規及若適用的契約條文所要求的，確保資料的保護與隱私。
A.15.2	**安全政策與標準的遵循性以及技術遵循性** **目標：確保系統遵循組織的安全政策與標準。**
A.15.2.2	應定期查核資訊系統是否遵循安全實作標準。