機密維護常識彙編（96 年 12 月份）

＊漫談現代生活應具備的保密觀念

前言

身處在這個資訊交遊快速的 e 時代裡，現代人均普遍地利用各類事務機器及通信、資訊設備，俾得以快速地連絡及處理各類業務，然在此同時，您是否已確實做好相關保密措施，來確保機密資料不外洩呢？在此特彙集個人實際工作經驗及相關報載資料供各界先進鑒參，期能凝聚維護幾密認知，俾在安定安全的環境下，共創事業高峰。

使用電話應注意保密事項

一、談論機密前，務先確認對方身分，竊密者可能會以虛構職銜或關係來套問機密事，在應答前務必先行確認來話者身分，否則一旦造成洩密，將後悔莫及;預防方法為，請對方留下連絡電話等資料作查證，並建議在話機明顯處黏貼警語標籤，提醒同仁注意防範。

二、如須保密個人使用電話號碼，建議將一般電話及行動電話設定為「發話號碼不顯示」，否則在受話方「來電顯示器」螢幕中，私人電話號碼將被一覽無遺。

三、使用具有「自動重複撥號（auto redial）」功能之話機，撥叫隨身碼、信用式電話或做其他有輸入密碼之線上轉帳或交易時，應注意清除紀錄，俾免遭人試撥盜打（用）。

四、以個人行動電話發送簡訊、E-mail，受訊（信）方將會顯示你私人行動電話號碼，無法隱秘身分。

五、個人行動電話語音信箱及電話答錄機密碼，應妥慎保管，以免遭人竊聽。

六、常檢視住宅大樓電信配線箱,查看有無遭人掛線竊聽或盜撥電話。

文書作業應注意保密事項

一、重要應秘密事項，應儘量避免書寫於便條紙或桌曆上，此舉極易因疏忽未收妥而遭窺視或翻閱，造成洩密。

二、具機密性之廢棄文稿應隨手以碎紙機銷毀，並將碎屑扯裂，以避免遭蒐集做重整復原;或改以焚燬處理;如因量多不便銷燬，可以整批運往紙廠當場請其溶燬，安全可靠又可秤重計價;切勿逕交清潔工清運，以免機密資料外流。

三、傳真機密文件前，應先連絡好收件人等候於傳真機旁，以避免遭他人截走;傳送前務先確認傳送號碼無誤，以避免誤傳洩密;傳送完成前不可離開，係為避免遭他人取走而洩密。

四、具機密性之廢棄文稿應隨手銷毀，避免做為資源再利用用紙;影印重要文件如遇夾紙應即取出，印壞部分亦須帶走，以免被有心人取走做不當利用。

資訊作業應注意保密事項

一、個人電腦做單機作業或辦公室 OA 網路連線，務必設定密碼保護，並定期變更密碼;螢幕保護裝置應設定密碼保護，以防範須央離座道人窺探畫面內容。

二、透過公司內部網路做檔案資源分一口子時，應安慎審核資訊內容是否涉及公務機密或公司營業秘密，能否給其他單位使用，並應加設密碼管制;如園內容係屬機密，必須依權限高低只提供給特定人員使用及能追蹤登入、使用紀錄要求時，建議改建置網站做控管。

三、各種經常使用密碼，例如 E-mail 帳號、網頁設計密碼等，切勿將之另紙書寫並黏貼於電腦上：更應避免利用各種作業系統(如

Windows)內建「自動記憶密碼」, 否則即喪失密碼保護之功能。

四、在無法確定網站的保密安全機制下，勿任意上網登錄個人重要應秘密資料，以免資料遭截取被移作其他用途;據報載國內某家網路銀行曾遭人拷貝該行網站網頁, 進而誘騙該行客戶輸入身分證字號、密碼等資料，進行轉帳盜取款項。

日常生活應注意保密事項

一、陌生人以問卷調查、寄資料等藉詞，電話詢問相關資料時，應特別留意並查證對方身份，勿輕易告知。

二、個人擬廢棄信件、單據、資料等件，勿以垃圾處理，以免外流。

三、每日應檢視信箱，重要信函如信用卡帳單、電話、網路連線費用帳單應隨時收取，以免被有心人截獲做其他運用。

四、據報載曾有詐騙集團假冒銀行人員套問金融卡帳號、密碼或信用卡卡號等資料，應提高警覺注意預防。

五、對外公開的資料，如個人名片、停車留言板等登錄資料，不宜太過詳細，以免洩漏個人資料。

結論

多一分保密警覺，少一分洩密風險。建立起每個人重視維護機密的認知，處處謹慎小心，可以幫助你經常處於一個安全叉安定的環境中，有助於防杜危害、犯罪、破壞等事件發生之機會;在事業上於公得以知法守法，確保公務機密安全，不因疏忽洩密損及公眾利益又遭處罰;於私得以保護好公司商業機密、營業秘密，厚植企業競爭實力，開創個人事業;更會因為您這種重規機密的認知，影響到您的家人、杜會及全民，進而促使社會更加安定，國家更為安全。

＊淺談密碼保護技術的現在與未來

◎ 吳文進

一、前言

當前電腦與網路犯罪率逐漸攀升，一方面是電腦網路的普及率提高，另一方面則是自動化攻擊工具取得容易，致入侵的技術門檻降低。在 FBI 最近的調查研究顯示， 85%的企業組織在過去一年中曾發生入侵事件，而以財損狀況來比較，近年因資安事件損失金額相較於 2000 年增加了 42%，因此如何採取適當的防衛措施以降低資訊資產損失的風險為當前重要的課題。然而值得注意的是，目前常見的入侵模式，大部分都是利用規避密碼保護的方式來取得存取權限。因此，基本的密碼保護技術已不足以防衛企業組織的機敏資產，故需發展更高階的密碼防護技術。本文將由密碼技術本身的問題談起，並簡介身分鑑別的方法，及由其概念衍生的雙因素認證技術，最後則說明未來密碼技術發展的走向。

二、「密碼」技術所面臨的挑戰

密碼技術是最傳統的認證方法，從電腦開機密碼到登入系統或電子郵件等隨處可見，但單純的帳號及密碼，不像我們所想像的那麼可靠，整個密碼的觀念是基於一種矛盾的修飾法。它的構想是利用一串好記的隨機字元，但容易記憶也代表易遭破解，複雜密碼則因不利記憶而可能抄錄於筆記本或置於便條紙、行事曆等易取得之處，更甚者，一只密碼遊走天下而成為駭客們的最愛，只要設計一些可資吸引目標群眾如下載軟體、影片等網站，不需付費只要求以帳號及密碼註冊，然後就可坐收一堆可用的資料，其間所隱藏的危機使用者不可不察。數十年來，密碼一直是資訊安全防護的基礎，然而密碼難用且變得難以管理，使用者必須記住的大小寫字母和數字，當持用的密碼組

數過多時，如何記憶及避免重覆都是個難題，因此企業組織必須訂出一套可行的密碼政策，但遺憾的是每一種作業系統和應用程式密碼使用的方式各不相同，欲以同一方法來管理，在實務上管理不易。尤其目前網路應用程式劇增，使用者需求五花八門，多元的組合加劇問題的複雜度。為解決這個問題，各種對策應運而生，於是便有所謂「單一簽入」（single sign-on）、密碼同步化等技術。

然各項研究雖專注於密碼工程，但常忽略身分認證和授權的問題。例如運用同一密碼來存取多重資源之整合身分的概念，但實務上存取這些應用程式所需的權限等級不一，因此認證服務須與授權服務充分整合才能提供足夠的安全。而身分管理則是由多種功能組合而成，目的在管理包括識別符號和密碼在內的身分，必須依使用者資料提供、工作流程及稽核等項目，訂定各項優先順序，這些顯示出密碼的發展已有長足的進步，與當年只被顧客、服務檯和管理員視為惱人麻煩的情況，不可同日而語。但相關的研究團體指出，多數密碼保護機制都是將認證的部分單獨抽離後，置入各種應用程式當中，並結合目錄服務或網路單一簽入的產品來提供基本的防護功能。然而，軟體不能解決多數企業所面臨密碼的問題，因為密碼政策屬安全政策的一部分，係因應特定商業需求而設，並視所存取資料的價值而定。許多企業花費大錢去發展複雜的政策和規則，只為限制存取其實不太需特別保護的資源，而部分企業則是花費太少資源，欲以同一套政策來保護企業內重要的資產，過與不及如何平衡都是難題。

回顧 2004 年 11 月，微軟在哥本哈根召開「資訊科技論壇」，比爾．蓋茲預測依賴密碼保護資訊系統的時代即將結束，人們將利用其他的身分驗證技術如生物辨識且加以取代。生物辨識是指識別人類臉形、指紋或視網膜等特徵的技術，在高科技領域，已獲認同並逐漸

風行。多年來，微軟一直忙著修補視窗系統的安全漏洞，而密碼不安全的話題又引爆另一安全議題，因為當密碼由「安全措施」變成「安全風險」時，我們不得不尋求較佳的解決方案來確保資安防護需求，因此許多企業利用集控式伺服器對網路用戶進行身分驗證，這些身分管理系統簡化了網路管理，但這也表示所有有價資料通通放在同一地方（如資料庫），僅以一個密碼來保護確顯不足。根據估計，釣魚騙術（phishing）造成美國消費者每年的損失在 1.5 至 5 億美元之間；另調查亦顯示有 80%的家用電腦感染間諜軟體。這更突顯密碼保護的另一問題：即使是最好的密碼也會被盜取。密碼的數位竊賊與合法的系統用戶根本上是沒有什麼區別的。安全專家就此提出利用二道以上的關卡來提高系統安全防衛強度的解決方案，也就是所謂的「雙因素認證」，這種方案結合了用戶自行保管的安全裝置與一組個人辨識密碼（PIN），可以遏止對系統的非授權存取，軍事及重要政府部門均普遍使用這種安全方案，但造價昂貴，必須從確保機密性的安全防衛角度來審視，否則將不符成本效益。

雖然密碼有其缺點，但仍是目前唯一實質的身分驗證標準，因為不論是利用指紋或虹膜的生物識別法或智慧卡，在沒有官方採用的身分驗證標準前，密碼仍無法被取代。因為一個單一、可攜帶、容易遺失的卡片，本身就不是很好的答案，密碼或通關密語在使用上雖然較不便，但卻易於攜帶且安全，若輔以驗證流程管控及政策，只要有適當的訓練，遺失或外洩可能性均可降低。

三、身分鑑別的方法

資訊系統如何防止非法盜用以提高安全性，第一個直接而重要的方法就是系統使用者之識別與鑑別，系統必須考慮誰被允許簽入(login)及如何判定使用者是合法的，這兩個問題就是在資訊安全管理

系統架構之技術控制所談的識別(Identification)與鑑別(Authentication)的問題，識別是你告訴系統你是誰的方法，而鑑別則是你對系統證明確如所宣稱的你之方法，在多使用者系統中，你必須表明自已的身分，而系統必須鑑別你身分正確後才允許你使用。一般而言有以下三種方式來證明你自已，而我們可以採用其一或數個混合使用：

(1)基於所知(Something You Know)：

基於所知最典型的方式是使用通行碼(password)，而挑戰--回應(Challenge-Response)的方式則藉一連串的問題與回答，使攻擊者必須猜中或掌握比通行碼更多的資訊才能破解。

(2)基於所有(Something You Have)：

基於所有就是使用鑰匙(Keys)、標籤(Badges)或智慧卡(Smart Cards)等你所擁有的東西來解開你的終端機或帳號。此方法的理論在於這些鑰匙或實體的擁有者才能使用，但相對的這些鑰匙也可能遺失、被偷或別人借用而遭複製。

(3)基於所具特徵(Something You Are)：

基於所具特徵是根據生物或行為上的特徵，諸如指紋、掌紋、聲紋、筆跡、敲鍵特徵及靜脈紋路等，皆可以用來作為識別及鑑別的工具。

前述三種身分鑑別的方法，單獨使用都可能產生問題，如「基於所有」的物品可能被盜走；「基於所知」的內容可以被猜中、分享或忘記；而「基於所具特徵」的代價昂貴且擁有者本身易受攻擊，但如依安全需求混合搭配，則能增加攻擊的難度，因此兩種以上要素結合起來充作身分認證的方法就是所謂的「雙因素認證」，也是多層防衛的運用。

四、雙因素認證的原理

雙因素認證用戶需雙重認證，因此可降低電子商務的兩大風險：外部非法侵入者之身分欺詐與內部人員的身分竊用。雙因素認證的解決方案，是採用經過授權的使用者都可被分配到一個獨有的、經註冊的、以時間運算法則為基礎所產生僅可使用一次的認證權杖（token），token 每 60 秒會產生一次不同的權杖碼，認證伺服器則用這個獨一無二、且無法猜中的動態密碼來實施身分識別。透過雙因素認證伺服器，使用者認證可以存取內部網路的、遠端撥接或連結虛擬私有網（VPN）。

當使用者試圖存取一個受保護的系統時，一個特別的網路代理程式（Agent）便取代基本的密碼機制，開始執行雙因素身分伺服器的認證機制。在認證過程中，使用者被要求輸入使用者名稱及替代密碼，此替代密碼即為由其所持有的權杖裝置所顯示的權杖碼，加上一個識別碼（PIN）。Agent 混和了使用者輸入的資訊以及只有此受保護的裝置所知道的資料，然後使用 SHA-1 或專利的雜湊演算法則，將使用者的識別及權杖碼透過加密封包傳送雙因素認證伺服器，當伺服器接收到認證需求後即搜尋其使用者資料庫，並以識別碼及權杖碼進行比對以確認身分，若兩者的組合證實是有效與合法的，則使用者的存取即被允許。

權杖有許多不同的型式，如硬體、軟體及智慧卡等。最常見的硬體權杖是鑰匙環，其內建有晶片，可顯示最多 8 位數字碼，並可與鑰匙串在一起。此鑰匙環會先設定成唯一的 64 位元的初始值，每分鐘內建晶片會執行雜湊演算，並將初始值及目前時間以亂數組合以產生隨機亂數。除了鑰匙環的型式外，其他的權杖種類還包括信用卡大

小的權杖卡或是智慧卡，甚至可與門禁卡、車輛防盜系統等結合，有效支援日常安全需求。

五、結論

使用密碼的時代雖看似過時，然實際上融入新的方法理論與技術，使其防護效力得以延續，當前資產保護的主流仍以使用者授權為概念，有效的存取控制是保護企業資訊、系統及資源的重要方法之一，因此當企業組織投資高效率的認證解決方案來保護重要資訊資產時，應從保護標的與成本效益來考量，以建構合理可行的方案。而相關的密碼工程研究，是否應以資訊科技是否仍為企業的競爭優勢所引發的討論，研思密碼安全產業的明天在哪裡？如果資訊科技已轉變成單純的企業基礎技術，則發展更安全、更便宜的認證機制，將是創造資安領域的「藍海策略」。（本資料摘自於清流月刊）

＊辦理採購作業應有的保密

自政府採購法實施以來，有關政府機關的營繕、購置定製財務、勞務等採購案件，常見百家競爭的局面，也因此各家廠商無不期望能有相關管道，可以獲得一些在招標作業過程中，規範應受保密的資訊以增加自己的籌碼或得標之成功率，即便是限制性招標，雖僅有一家廠商參加，但就廠商的立場而言，相信一樣是冀望能多掌握開標的有關資訊。

根據政府採購法第三十四條已明文針對採購作業之規範要點:

第一款:機關辦理採購，其招標文件於公告前應予保密。但須公開說明或藉以公開徵求廠商提供參考資料者，不在此限。

第二款:機關辦理招標，不得於開標前洩漏底價，領標、投標廠商之名稱與家教及其他足以造成限制競爭或不公平競爭之相關資料。

第三款:底價於開標後至決標前，仍應保密，決標後除有特殊情形外，應予公開。

第四款:機關對於廠商投標文件，除供公務上使用或法令另有規定外，應保守祕密。

另外，依據採購評選委員會組織準則第六條第一款亦指出；本委員會委員名單，於開始評選前應予保密。

綜合政府採購相關法令要點觀之，公務人員對各項採購案件尤應謹慎小心，嚴守作業流程應保密作為，否則非但導致招標紛爭不斷，相關業管人員恐亦難逃刑事或行政懲處之責任。

＊如何做好分類保密、資料清繳與清理？

所謂「保密」便是「保守秘密、保護機密」，所謂保密，當然是指與公務應密 秘資料，因為機密洩漏，小則害己、大則亡國，因此，我門必須注意，不管任何事，不問是公或私，都不應該隨意洩漏，在業務上不應讓別人知悉的，都應 該保守機密。

保密的基本方法有限制、禁止、防護、銷燬等，在執行上或許會增加少許的不 便，但卻是保障單位及確保工作成效的不二法門，在分 類保密資料清理上有以下規定：

1. 絕對機密、極機密件：

   保管人員應會同政風人員監辦，用燒燬、浸蝕、打碎或製成紙漿等方法，予以銷燬。凡屬此等文件之來文單位、字號、奉准銷燬之日期、地點、保 管人及監燬人之級職姓名，均應做成紀錄備查。

2. 機密、密件：

   由保管人員會同政風人員監視下銷燬，並做成紀錄備查。

3. 如大量之分類保密資料，不能由保管人親自銷燬時，可由主官指定專人或數人執行，若 係數人，必須指定其中一人為其領隊，另再派政風人員全程監燬；原保管人應取得並妥慎保管銷燬紀錄，以利爾後查考。
4. 對於作廢文件之清理，包括製作分類保密資料所使用之草稿、複寫紙、底片 等材料，除非有規定不須銷燬，否則一律銷燬。製作「絕對機密」、「極機密」 件之作廢文件，承辦人隨時予以銷燬，至於「機密」、「密」件之作廢文件，如無立即銷燬之必要時，可將其裝入非法定人員不能取出之容器，於下班前予以集中銷燬。印刷分類保密資料之製版，應於印刷完成後立即拆燬。保密工作是具有約束性、強制性，其中任何一項規定，都關係國家的生存，故我們不論何時何地都要特別謹慎小心，發現有洩密情事，應據實迅速報告主官或反映有關機關，千萬不可漠不關心。

＊洩密與圖利

一、案例事實：

范○標自就任湖×鄉長後，即指派吳○政擔任建設課課長，二人與范○標之親信范○金，共同基於對湖○○公所經辦工程索取回扣之概括犯意聯絡，明知「湖○○公所營繕工程及購置定製變賣財物內部審核程序」規定，一百五十萬元以下，二十萬元以上之營繕工程，係以公開比價或簽報首長核定通知三家以上殷實廠商於廠商所在地郵寄投遞並公開比價，受通知之廠商只能領取一張空白標單進行投標，而范○標為鄉長，對於該工程之發包為其監督之事務，而吳○政為承辦人，對於主管之事務，明知工程底價應依法

保守秘密，卻違背職務將鄉長范○標告知所核定之工程底價，於八十六年六月十日上午，洩漏消息予該等包商，由該等包商取得每一項工程三張空白標單後，經由其他二家陪標廠商之同意填寫後，以通信投標方式完成投標形式，違背上述公開比價及不得洩漏底價之職務規定。承辦人吳○政並於比價日向上開不合規定得標之羅○洲、羅○河、羅○鈿再次期約收取工程款二成回扣，其中羅○洲乃以范○金於八十六年五月十三日預借之一百五十萬元抵扣，並以此方式，將范○標、吳○政違背職務行為之賄賂交付予范○金。范○標、范○金及吳○政所為，觸犯貪污治罪條例第四條第一項第三款經辦公用工程收取回扣罪及刑法第一百三十二條第一項洩漏國防以外應秘密之消息罪。

二、案情研析：

范○標、范○金及吳○政所為所犯經辦公用工程收取回扣罪，係同條例第四條第一項第五款對於違背職務之行為收受賄賂罪之特別規定，依特別法優於普通法之法條競合原則，僅論以經辦公用工程收取回扣罪；而就經辦公用工程收取回扣及洩密行為，有犯意連絡與行為分擔，范○金雖非從事公務之人員，但與依據法令從事公務之人員范○標、吳○政共同犯罪，依同條例第三條及刑法第三十一條第一項規定，仍應論以共同正犯；范○標、范○金及吳○政共同內定廠商、洩漏底價使廠商得標之圖利行為，復就相同之圖利行為收取回扣，圖利行為應為收取回扣行為所吸收，不另論罪。再被告共同向羅○洲、羅○河及羅○鈿同時期約並分別收取回扣，乃至分別洩漏國防以外應秘密之底價消息，係利用同一次發包工程之機會，所侵害者為國家公務執行之公正，被侵害之法益仍屬一個，祇成立單純一罪；又被告犯上開經辦公用工程收取

回扣罪及洩漏國防以外應秘密之消息罪，有方法結果之牽連關係，應從一重之前罪處斷。

三、結論：

保密是用以防制非法定人員獲得或知悉我機密文書資料，所採取的預防措施，其目的在維護國家機密，以增進國家的安全與利益，俾有利政令之推行。本案是藉洩密以獲取不法利益，涉及違背職務收賄、利用職權圖利他人等瀆職行為，適用「貪污治罪條例」從重論處，可為殷鑑。故每一個公務人員應嚴密保守而不得洩漏或交付之責任與義務，須以臨深履淵之心情，時時防範之嚴謹作風，始保無洩密之虞。否則，即使過失，亦要受到法律之制裁，切莫掉以輕心。