第二十五章

檔案資訊安全之探討

The Study of Archives Information Security

張文熙

Wen Hsi Chang

檔案管理局檔案資訊組 高級分析師

Senior Analyst , Archives Information Division,

National Archives Administration

壹、前言

由於政府機關所產出電子檔案數量與日劇增，因此相對地電子檔案管理之安全與稽核之重要性也越高。基於政府機關整體資訊安全，行政院業已建立「國家資通安全會報」，並成立「國家資通安全應變中心」，通令要求各級機關成立「資通安全小組」負責各機關之資訊及通訊的安全預防和危機處理，以健全資訊安全相關作業及通報管道。資訊安全所涉及範圍相當廣泛，從網路骨幹安全到一般性資訊安全預防均屬之，詳細內容及範圍於前述之「資通安全小組」職掌中均有規定，各單位均須據此建立「資訊安全計畫」來達成相關安全目標。檔案資訊安全除了一般性系統安全：如人員控管及系統權限等必須遵守外，特別著重電子檔案相關管理作業之安全，應是未來電子檔案發展的成敗關鍵，檔案資訊安全議題不外三大範圍：

一・機密性：使非合法授權者不得使用

二・鑑別性：可確定檔案來源的合法性

三・完整性：確保檔案是否遭受有意或無意地竄改

檔案資訊應用對象包含電子檔案本體及目錄(MetaData)二類，兩者資訊安全同等重要。現存檔案資訊應用以目錄相關活動爲主，包含檔案目錄資料線上及離線傳遞、產生、儲存、應用、線上付費等活動，其過程間可能存在之安全漏洞，均應採行相應之預防方案和緊急應變作業方式，以確保安全。我們把落實檔案管理認證（Authentication）、授權（ Authorization） 及稽核（Auditing）過程的安全，簡稱爲三 A 方案，以作爲檔案資訊安全發展之策略方向。

貳、檔案傳送安全

檔案資訊傳送的安全，建立於電子憑證。故機關間的電子檔案交換，應使用機關電子憑證。各機關上傳各類檔案資訊時，管理系統必須採取加密動作。以檔案管理局的全國檔案資訊系統爲例，使用 128bits SSL 來進行傳輸時加密作業。當相關檔案資訊送抵檔案管理局時，系統將自動建立操作該系統的人、事、時等記錄檔，再從各資料中取出檔案管理局的憑證，並加以檢驗此憑證的效期，若經檢驗結果憑證效期已過，或爲無效憑證則必須至政府憑證管理中心(GCA)重新取得憑證，並再次進行檢驗的動作；若仍未能通過檢驗，則須透過電話與政府憑證管理中心(GCA)進行處理。當檢驗通過後，則對檔案資訊目錄進行壓縮的動作，再加上數位簽章再上傳至檔案管理局。檔案管理局收到各機關上傳的檔案之後，會回覆訊息給各機關，並判斷訊息是否正確。若各機關未能收到訊息，則須打電話至檔案管理局確認原因，如所收回覆訊息不正確，則需進行重傳動作，但若重傳動作超過三次以上仍未能傳成功，爲作業安全的理由，應立刻停止再傳，待問題原因釐清後再行作業。

檔案資訊離線傳送時，媒體簽收過程及送交人員的管制是基本保護措施。不

同的貯存媒體，其保護措施應有所區別。如光碟片應注意包裝避免摔裂造成無法讀取；磁片或磁帶應注意防水防潮，避免運交過程中受到其他設備之干擾，造成磁性媒體損壞。大量的媒體運交時應於貯存媒體的外包裝加以註記，以便辨識。

參、人員安全

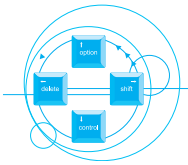
如果沒有嚴格的人員控管，不論資訊系統安全機制及加密技術如何複雜也徒具形式。絕大多數洩密事件不需要透過任何科技手段，如利誘或色誘關鍵人物，都可以不漏任何痕跡地取得資料。因此人員管制是整體資訊安全最基本環節。以檔案管理局爲例，使用者要使用個人電腦時必須透過 Windows 2000 進行網域登入，針對網域中使用者身份確認，落實權限控制。登入網域之帳號則包含單位別及職別，藉以清權責。如檔案資訊組單位代碼爲 250，故以 250 爲首碼的人員代碼，才可能給予管理者權限。特殊指定職位，才給予超級使用者，或者應用系統管理權限。以固定字頭區別系統人員身份，如果有意圖入侵系統的帳號不具備檔案資訊組單位代碼時，系統可以立刻排除。不過，這種編碼方式實務上不易做到，主要在單位內人員調動時，變更代碼對實際管理作業的困難度及複雜度大幅增加，故檔案管理局目前是以群組的方式來進行成員的歸併，依群組的屬性給予人員適當的權限。重點在於一定要選擇一個使用者身份確認機制，在管理上可以落實權限控制，才能維持基本的安全。

隨人員異動所帶來之權限及效期管理作業，爲帳號管理基本要務。單位內職位調動、離職、停職及退休等人員異動，宜採保留原職位號碼的方式。當人員跨越單位調職時，必須更換單位代碼，並停用舊代碼，以區分權責。新進人員禁止重覆使用前人使用過的代碼，如此可必免未來稽核作業混淆。任何人員接觸任何檔案資訊，進行各項相關作業時，首先要取得網域內電腦的使用權。以檔案管理局爲例，其是以 Wins 作爲區域網路分群的基礎，區隔伺服器、資料群組。同時，網域登錄密碼每六個月強制更換。使用者簽入網域成功後，才具備基本的網路電腦使用權，再依據不同應用系統區別使用權限。

人員代碼的付予方式和系統安全有直接關係。應用系統再如何設計嚴密安全，其實都抵擋不住人爲的洩密動作，人員往往是最大的安全缺口。有心取得電腦機密資料的人，與其投資千萬研究破解之道，恐怕遠不如直接買通具有接觸權限的人員來得有效。基本保護作法，如不輕易讓人猜到或看到使用中的密碼，離開電腦座位時，自動啓動螢幕保護程式的密碼等，都有相當嚇阻作用。指定空間作爲機密資料操作的唯一作業點，也是一可行的方式：在許多電影中可以看到類似這樣的情節，一個保有最高機密的電腦是放置在重重機關保護的密室中，接近密室必須經過層層的關卡，足以阻止大部分好奇的人接近，就實體安全保護的觀點確有相當功效，但是使用者確實掌握簽入代碼及密碼，不會輕易被別人誤用及盜用，才是檔案資訊安全首要步驟。

因此，藉由員工安全教育落實人員安全觀念是各級機關的必要手段。一般使用者之資訊安全教育，旨在宣導觀念及加強基本操作安全。包含個人電腦的防毒措施、資料備份等。如在個人電腦架設掃毒工具，並在郵件伺服器上架設 MailScan 之類的郵件掃毒軟體，避免由電子郵件挾帶病毒。宣導正確防毒的基本觀念，了解防毒軟體並非萬靈丹，但可減少中毒的機率。例如檔案管理局採用由伺服器自動更新病毒碼，但新生種類未能列入病毒碼者，仍有相當多入侵的機會，如網頁型病毒等，更是難以防堵。因此，養成資料備份的習慣，是避免遭到破壞後唯一補救的方式。

將資料存於伺服器中，由資訊人員定期對伺服器中之個人資料區域加以備份，並由使用者自行備份於光碟或磁片之中，減少還原失敗的可能。並於資訊安全計畫中明定相關訓練課程，施以適當稽核作業，使備份作業法制化，成爲使用者既定的習慣。進行必要的用人前審核，避免集中所有的系統權力在單一的人身上。此外，加強主管建立異地貯存的觀念之教育訓練，更有立竿見影之效。讓安全意外的通報程序成爲組織內成員的必要課程，讓資訊安全成爲習慣，應比任何形式的控制更有效。還要定期對所擬定的資訊安全相關條文定期進行調整及檢討，讓整體資訊安全計劃具可行性。



肆、設備及網路安全

以機房門禁系統管理維持設備實體安全，可直接提供檔案資訊安全之基礎。一般而言，不論磁碟陣列、磁片、光碟等電子貯存媒體大都置於電腦機房內。因此，機房必須有適當的門禁系統，以避免閒雜人等接近，採取磁卡鎖加上密碼鎖等方式爲主要的門禁管制方式。通常握有電腦機房卡片的只有首長及負責機房管理的業務負責人，其餘人等若有工作的實際需要必須經過核准，取得同意之後才得以進入。以人爲方式控制電子檔案貯存場所的接觸人數，當檔案資訊洩露時較易追查。

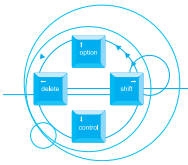
建立異地備援機制是爲確保設備持續運作及危機應變最佳的方式。其主要目的在當電子檔案貯存場所及貯存媒體，因爲外力被破壞，如天災、火災等，造成資料內容無法讀取或辨識時，可以從第二替代地點取得持續運作，恢復正常作業。如果系統運作是搭配大型 ISP 時，如政府服務網路，則可以中華電信機房作爲併行作業的中心，不僅對所貯存的各類電子檔案進行實質的異地備份，同時，可以進行立即的接續作業。至於相關伺服器的安全，只有負責實際操作之系統管理師具有進入伺服器主控台的權限。每一伺服器中的不同應用軟體系統的管理者權限，則是依業務職掌的需要付予，避免由相同的人握有所有檔案資源的權限，降低檔案遭到同一個人進行修改、變更或竊取的可能性。

網路安全在電子檔案開放對網路應用更顯重要。其帶來使用者的方便外，也帶來了安全的問題。由於電腦技術日新月異，破壞手法日日翻新，所以系統管理者也必須隨之引進新的安全技術才能抵擋。此外，研發及更新病毒偵測技術與清除方式，對各種現存攻擊手法進行統計分析，有助於規劃資訊安全政策，才得以建立更安全可靠的電子檔案作業之網路環境。並隨時注意政府服務網路的相關訊息，可以幫助我們節省許多時間，隨時接收 GSN-CERT 的網站(http://www.gsn-cert.nat.gov.tw)所提供之資訊安全相關資訊及相關報導，包含各類病蟲資料庫(Virus、Worm 及 Trojan Horse) 及木馬程式的介紹、弱點資料庫(Vulnerability)、及相關系統程式修補(Patch)等資料。並藉此交換資訊安全事故的處

理經驗、資訊安全教育訓練等相關訊息、其間所提供系統管理者相互間的諮詢資訊，對資訊安全事件實務處理技巧有很大的幫助。

網路應用時需要注意一些常用應用軟體使用問題：例如垃圾郵件的傳遞，郵件內容本身雖然無毒，卻因爲量過多而造成網路的壅塞；怪異封包造成電子檔案的傳送受到阻礙等均屬之。又如電子郵件中夾帶的文件炸彈或病毒，不一定會完全被防毒軟體所阻隔。另外，電腦假冒(Spoofing)及竊聽(Sniffing)行爲，都可能造成使用者權限資料截取，這類行爲就有賴於區域網路中架設監視系統來阻擋。如政府服務網路提供定期的骨幹設備安全漏洞的掃描，主動地定期偵測，例如有名的 Code Red 病蟲偵測就是一例。另外進行預約性偵測，針對指定的機關作全面性掃描。當發現網路異常時即會透過通報系統提出預約偵測。以檔案管理局爲例，是以 MRTG 軟體監控，定期針對局內網路的伺服器及重要設備進行流量監控，以便即早控制可能造成電子檔案的事件發生，或阻止事件的擴大及惡化。

現今網際網路是跨機關間檔案資訊作業傳遞作業核心，因此網際網路安全有舉足輕重的地位，其主要基礎網路安全架構包含公開金鑰基礎架構(Public Key Infrastructure, PKI)、虛擬私密網路(Virtual Private Network, VPN)、防火牆(Fire Wall)、網路設備存取控制(Access Control)以及入侵偵系統(Intrusion Deteciton System, IDS)的建立，等四大項目。我國政府服務網路骨幹設備在連外網路的閘口裝設了入侵偵測系統，使得任何外來的不當行爲，一旦經過閘口設備，立即會發生告警的訊息。同時，在政府服務網路上各項網路設備的相關設定資料，均定期備份，以確保萬一網路設備遭到破壞，或是設定值被更改，可以迅速的回復運作。其作業上會拒絕不合理的 IP 封包轉送，例如，10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 等來源的 IP 進行查核。政府服務網路定期分析系統紀錄(LOG)資料，如遇任何異常情況，隨即進行追查，定期針對各項可能的漏洞進行掃描測試，並隨進行相關的補強的安全措施。因此政府機關使用政府服務網路，除可解決網際網路骨幹安全事項，使業務機關負荷得以稍作疏緩，並切割出資訊安全事件責任。



伍、檔案產生過程的安全

系統無法控制資料輸入的人爲洩密問題，除此之外，輸入資料離線傳送，可能在郵寄或人爲運送中發生漏洞；而線上傳遞則與網路安全直接相關。傳遞安全分成兩大層面，一個是資料忠實到達適當系統進行適當的作業；另一個是確保資料進入後，不會造成同網內各系統作業的中止、破壞或其他資料的毀損。

影像掃描是回溯檔案電子化必要方式，其處理過程安全管理有其必要。影像掃描作業前必須對提取原卷的過程加以管束，掃描前與掃描後務必保持原件數量一致，並檢查原件並未遭受到破壞，此與系統無關，卻是整個製成電子影像的成功關鍵，避免影像遭到惡意刪改及盜用。文字形態電子檔案，則以電子簽章的方式解決，但是屬於影像文件的電子檔案，目前並沒有對浮水印(Watermarking)系統進行認證，對於回溯檔案不可避免以影像來進行建置，如果整電子簽章的體系中無法對影像檔有所規範，可以顯見其將成爲未來最大的安全漏洞。

檔案資料庫目錄及全文影像間的連結作業，也有發生安全事件的可能。由於開放檔案目錄應用查詢無法排除線上調閱，因此網路安全是應用必會面對的課題。由於無人可以對機密資料內容從網路洩露來負責，如此，機密資料的全文就不應透過網際網路服務。機密檔案不容許透過網路線上傳遞，所以只有在貯存作業及檢調過程的加解密動作，藉由電子簽章的控制來認定是否有相對應的處理權限來確保安全。

製成之電子檔案有儲存安全、電子簽章的數量及控管方式等問題。目前公文電子交換的過程中，僅能完成機關簽章，並且限於作業時間及檔案大小，會直接影響到傳輸速度，所以目前電子公文交換時，附件與本文並非同時作業。檔案管理局所製訂之「電子檔案管理作業要點」中規範檔管人員或承辦人員，均必須對公文產生的過程負責，對所經手的電子公文加註簽章。檔案管理局採行內政部所發行之自然人憑證，應是政府機關應用電子簽章作法的首選解決途徑，但是大多數人都沒有個人的憑證之外，而簽章的效期如何落實、實務上人員離職註銷、職務調動均有管理上的問題，有待克服。另外，對電子公文影像所加註的浮水印，

目前 GCA 並沒有提供認的服務，這使得電子檔案的應用在認證上必須選用第二種認證機制，增加使用者的麻煩，同樣也會有效期的問題存在，有待討論。

貯存文件及影像加密是爲了防止檔案被非法竊取，配合完善的存取控制，避免權限不足取得該資料的人員取得是項資料。由於儲存與加密都在同一端來進行，黃教授明祥認爲電子檔案管理系統的加密系統，應該選用對稱式的加解密系統(Triple DES)來進行。在系統安裝初期就產生加解密的金鑰，並由系統管理者選用一組 6-8 位的密碼對此金鑰再加密，來保護金鑰本身。所貯存之檔案不可再變動，因此儲存之前除作業者的簽章外，應加上機關數位簽章，用以維護資料的完整性，同時說明資料的屬性爲檔案管理局所有，未來才可藉以確認文件是否經過非法的修改。實務上，儲存加密技術再完善也無法避免系統人員的操作失誤，爲了避免操作上的人爲疏失，引起糾紛，在整套的電子檔案作業過程必須建立完整系統紀錄檔，以便日後追蹤及調查，包含操作系統的人、事、時、地、物。此外，還要參酌相關的法令，作爲責任歸屬的依據。同時，系統人員在下達重要的系統指令時也應加上其個人的數位簽章，以示負責，以明責任，如此有助於爭議事件發生時調處。

陸、應用安全

應用安全的範圍很廣，包含應用內容、應用程式及操作均屬之。資訊內容的安全分爲防毒軟體(Anti-Virus Software)、電子郵件的掃描軟體(E-mail Scanning)、內容的過濾系統(Content Filtering System)以及阻隔瀏覽網頁系統(URL Blocking System)。因爲檔案資訊在產生、傳遞及開放應用的過程中，極有可能使用電子郵件、檔案傳輸及網頁瀏覽等方式來進行，除了透過政府服務網路骨幹上提供的服務，包含配合用戶需求，進行過濾不友善的網路使用者 IP 位址，過濾出非屬政府服務網路使用者的 IP 封包，防止使用者攻擊他人，拒絕不合理或僞造來的 IP 封包轉送，以確保網內系統安全。

應用程式使用安全包含網頁存取控制(Web Access Control)、資料庫存取控制

(Database Access Control)、以及檔案系統存取控制(File System Access Control)。一般使用者以網頁作爲主要的呈現介面，對內則包含對資料庫管理系統的存取控制、作業系統內的檔案系統存取控制，搭配人員作業權限對網頁資料的存取及瀏覽，並對檔案內容加密處理才算完整。

至於操作安全則是對系統暨網路非法入侵偵測(Detection)、系統暨網路行爲的掃描(Scanning)以及系統暨網路行爲的監控(Monitoring)作業，屬於網路的操作性安全，其與政府服務網路連外部分相輔相成。以防火牆系統提供基本安全防護，劃分爲網外網路、網內網路以及非軍事區三大部分，分別對適當的應用伺服器加以界接。網內網路包含辦公室自動化作業，而提供民眾查詢的應用的檔案目錄伺服器則是在非軍事區中，然而經由伺服器所提出的查詢需求則透過防火牆轉入網內網路的資料庫管理系統。先使用弱點評估工具(Vunerability Assessment Tool)測量，確認一般性的操作性安全事件發生機率降到最低。離線應用的主要媒體爲磁片及光碟，可能發生以人工申請電子檔案應用之情事，當申請核准後將所需資料複製在光碟片上或碟片上，應對電子全文加入電子簽章，對於電子影像加入浮水印，才能攜出應用，此爲避免使用者再行複製作爲他用。

使用者付費是現代政府服務的趨勢，應考量選用之線上付費機制的安全。採用預付機制時要注意預付卡的帳號及密碼傳遞上的安全，如採 SSL 的安全協定來傳遞。一般預付機制係由管理單位製作預付卡，以相對金額來換取對價值的點數，只要在登入應用系統時，輸入所購得卡片上的帳號密碼，即可進入系統使用必須收費的功能。由於單純的預付機制，並沒有針對使用者的身份來區隔使用的權益範圍，所以僅適用沒有使用對象限制的功能上。信用卡、轉帳代繳及電子錢包是另一種線上付費應用方式。由於，涉及金融交易安全體系，使用者的信用卡或帳戶並非單作爲檔案相關功能的使用，當帳戶被盜用時會形成嚴重的問題。因此，除了帳戶資料傳輸的安全，必須加強使用者身份核對的功能。SET「電子交易安全」規格，是現今確保開放性網路(如 Internet)的標準方式，它提供了金融電子資料交換作業的完整性、鑑別性、存證與資料隱密性。

柒、結論

檔案資訊安全是電子化檔案開放應用基本條件。雖然檔案資訊安全，僅是整體資訊安全的一部分而已，但反言之，必須具備資訊安全環境，才可能提供檔案資訊作業安全。網際網路成爲檔案資訊應用的必要途徑，但其基本設計理念在於共享而非設防，因此外加的安全設計其實都和網際網路的原始構想相違。任何系統上網之後，門戶就有大開的可能，檔案資訊安全因對網際網路開放而洞開。所以機密檔案不直接上網以減少實質接觸的可能，是避免機密外洩的唯一途徑。我們堅信電子檔案安全應該人人有責，並非單依賴某些人或某一些產品可以確保檔案資訊安全，唯有多一分安全的規劃，才能多一層保障，並減少一分損害。