電子檔案保存風險管理

課程大綱

壹、 電子檔案管理議題

貳、 電子簽章相關技術

參、 風險管理概論

肆、 電子檔案風險管理

伍、 長期保存策略

陸、 技術鑑定與保存工具

柒、 結語

前言

近年來，我國檔案資訊化作業積極發展，隨著電子化政府及節能減紙政策的推動，各機關原生性電子檔案(即線上簽核電子檔案等)與衍生性電子檔案(即掃描影像檔案等)數量激增，電子檔案管理與應用需求亦不斷提高，突顯電子檔案在未來檔案事業發展占了舉足輕重的地位。

檔案記錄政府施政作為，也保存了國家社會的共同記憶。然而，電子檔案的特性不同於傳統的紙本檔案，儲存電子檔案的載體及格式，受到資訊科技軟硬體快速蛻變的影響，使得閱讀這些檔案的軟硬體會遭遇過時或失效的問題，未來的電腦軟硬體，可能無法辨識閱讀過往保存的舊有電子檔案內容，電子檔案的長期保存與管理變成一件非常棘手又不得不正視的問題。

由於電子檔案存在著這許多不可確定的潛在風險，現今的檔案管理人員恐難再如往常地守著傳統的檔案庫房，運用資訊科技，瞭解與管理電子檔案，已成為檔案管理人員必備的技能。因此，各機關應持續有系統地透過風險辨識、風險評鑑、風險處理與監控回饋的循環過程，有效管控電子檔案的風險，以避免風險或降低風險發生的機率，使得機關管有之電子檔案得以永續保存。

壹、電子檔案管理議題

一、名詞定義

我國檔案法第二條第二款對於檔案的定義為「各機關依照管理程序，而歸檔管理之文字或非文字資料及其附件。」，檔案法施行細則第二條載明「檔案法第二條第二款所稱文字或非文字資料及其附件，指各機關處理公務或因公務而產生之各類紀錄資料及其附件，包括各機關所持有或保管之文書、圖片、紀錄、照片、錄影（音）、微縮片、電腦處理資料等，可供聽、讀、閱覽或藉助科技得以閱覽或理解之文書或物品」。

國際檔案理事會電子檔案委員會對電子檔案（Electronic Records）定義為「電子檔案是一種透過數位電腦進行操作、傳輸或處理的文件」，本局出版之檔案名詞彙編中對於電子檔案的定義為「電子檔案指由數值『0』與『1』組成之電子形式，且符合我國檔案法第二條第二款及檔案法施行細則

第二條所界定檔案之範圍，並為機器可讀式，適合電腦儲存、處理及傳輸之紀錄文件」，其範圍舉凡電子化的公文、電子郵件、資訊系統、資料庫、網站、影音數位化檔案等皆屬之。由於不同性質的電子檔案，其格式、內容、用途、結構及背景資訊差異極大，管理方式也多不相同，為因應各政府機關文件檔案實際運作狀況，行政院於 99 年 5 月 28 日函頒「文書及檔案管理電腦化作業規範」修正版，已調整電子檔案之定義為「指電腦可處理之文字與非文字資料，且符合檔案法及相關法令規定者」，已趨近國際上之電子檔案定義；另詮釋資料的定義為「指用以描述電子檔案有關資料背景、內容、關聯性及資料控制等相關資訊」，封裝檔的定義為「指將電子檔案與其詮釋資料及驗證檔案真實性、完整性之資訊，以包裹方式儲存之檔案」。

二、電子檔案管理架構

電子檔案管理架構區分為「制定計畫」、「電子檔案生命週期」、「檔案管理資訊系統」及「評估」4 大部分，如圖 1 所示。各階段主軸說明如下：

(一) 制定計畫：事前規劃是成功的關鍵，反映了各項資源之投入活動，亦代表機關對電子檔案管理的支持度，此階段為電子檔案生命週期階段的重要導引。機關制定各年度計畫時，均應考量前一年度之評估與考核結果，予以修正及改善，以獲得持續之進步。此階段應產出機關電子檔案管理策略、資訊架構、保存與銷毀計畫、人員配置表與訓練計畫。機關亦應依據電子檔案資訊架構，建置檔案管理資訊系統並規劃電子檔案長期保存策略。

(二) 電子檔案生命週期：此部分係電子檔案生命週期執行運作階段，包含蒐集與產生、保存與維護、應用、清理等階段。

1. 蒐集與確認階段：機關應規劃電子檔案蒐集範圍、方式與時機，並宜制定公文線上簽核推動範圍及限縮電子檔案格式，以達真實性、完整性與可及性之目標。此階段應考量「文書及檔案管理電腦化作業規範」、「機關檔案管理作業手冊」、機關電子檔案存取權限與管理需求及資訊安全政策等，以確立電子檔案所有權與管理權責，建立電子檔案資訊取得、保密、安全的政策與程序。同時，為利後續管理、檢索及應用，亦應依相關規定整理、分編。

2. 形成與保管階段：機關應依據相關法規、機關需求及檔案重要性，評估存取所需之電腦軟硬體，並進行適當之電腦軟硬體系統保存、電子檔案轉置與模擬等處置，定期進行電子檔案備份與災害復原演練，以確保機關所管有之電子檔案可存取應用，保全組織的記憶與重要知識資產。此階段之重點工作在於確保電子檔案之真實性、完整性與可及性。機關亦應定期辦理電子檔案清查作業，檢視並統計電子檔案數量、格式與版本等資訊。
3. 應用階段：機關考量機關內部與外在應用需求，應兼顧政府資訊公開政策與保護個人隱私之原則，於符合存取權限、保密與安全性政策與程序下，加強對民眾服務，有效地應用電子檔案，產出正確與可用之資訊，透過電子檔案應用及分享，讓機關具有特色之檔案得以呈現，以彰顯電子檔案之價值。
4. 清理階段：機關每年應定期辦理電子檔案清理作業，依檔案目錄逐案核對，將逾保存年限之定期保存檔案或已屆移轉年限之永久保存檔案，分別辦理銷毀或移轉，或為其他必要之處理。
   已屆保存年限之電子檔案，應依「機關檔案保存年限及銷毀辦法」相關規定製作檔案銷毀目錄，送會各相關業務單位同意及函送檔案中央主管機關審核後，才可以辦理銷毀作業。各機關永久保存之電子檔案則依「國家檔案移轉辦法」辦理檔案移轉作業。

(三) 檔案管理資訊系統：依據檔案法施行細則第二十五條規定：「各機關辦理檔案管理資訊化作業，應依檔案中央主管機關及相關主管機關之規定，使用檔案中央主管機關建置之全國檔案資訊系統或自行建置檔案管理系統」。因此，機關如規劃自行建置檔案管理資訊系統，其資訊系統應具備之功能需求請參見「文書及檔案管理電腦化作業規範」附錄 7 之檔案管理系統功能說明。

(四) 評估階段：機關規劃時應建立清楚之達成目標、績效衡量及衡量指標，以瞭解計畫實施績效。依據該績效成果，檢視機關資訊管理能力、定期稽核結果，以發現是否有特殊需求，並提出建議報告以供上級長官參考，並規劃下一年度重要工作及目標。

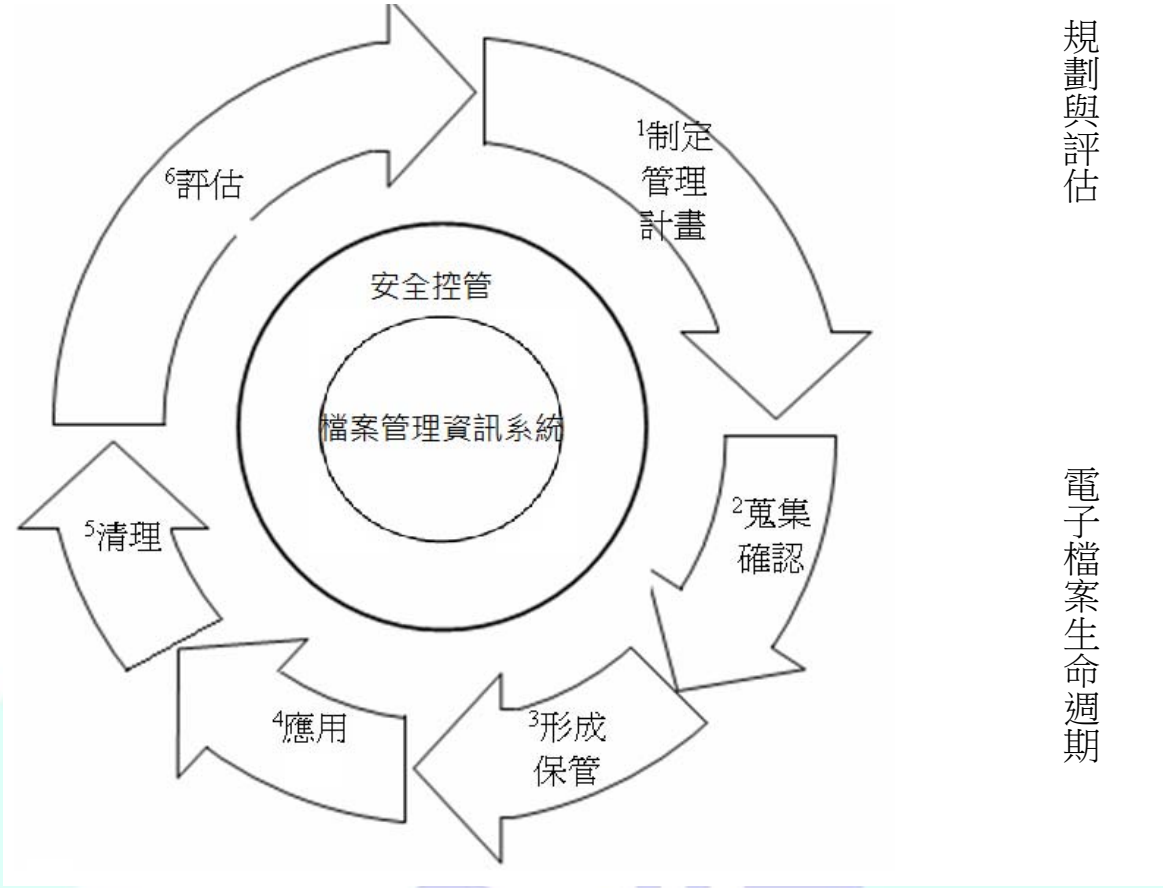


圖 1 電子檔案管理架構

三、電子檔案管理目標

開啟電子網路時代的源頭，可追溯至 1970 年，當時銀行間係運用既有的金融資訊網路進行電子資金轉換(Electronic Funds Transfer，EFT)。到了 1980 年，廣大的企業為因應即時傳遞商業資訊的需求，開始使用電子資料交換(Electronic Data Interchange，EDI)與電子郵件(Electronic Mail，e-mail)技術，透過約定的標準電子形式將文件內容傳遞出去，此舉大大提高業務效率，縮短資料文件交換的時間，更降低使用紙張的成本，當是節能減紙的先驅。到了 1990 年，全球資訊網的誕生，電子商務時代應運而起。基於網際網路的應用明顯地提升工作效率，行政院研究發展考核委員會開始推動 e 化政府，著眼於提升為民服務品質、紛紛要求各政府部門對民眾服務事項必須提供網路服務功能，因此網際網路在政府部門更是扮演不可或缺的角色，在商業環境中，企業主早已嗅到潛藏的無限商機，但是也驚覺電腦犯罪的溫床已在暗潮洶湧中獲得鼓動。美國政府體認到電子商務對全球未來商務活動的重要性，柯林頓總統於 1997 年 7 月

1 日發表「電子商務框架」(The Framework for Electronic Commerce)，提出建立全球電子商務環境之 9 大議題，如發展電子商務環境、研發資訊科技、拓展國際合作、保障消費者與企業權益等，均獲得全球熱烈的討論與回響。然而，就以電子公文交換為例，當公文經由網路傳遞交換，在傳遞過程如何確保不被竊取、不被竄改、不被偽造、不被非法存取，可以完整又正確地將電子公文傳送到收方的手中呢?因此，建立一個安全及可信賴的網路環境，才是成功的關鍵因素。在此，檔案管理人員對於完成公文線上簽核的電子檔案，或對於完成數位化後的電子影音檔案等，該如何管理呢?要管理這些電子檔案之前，不能不對電子檔案相關的專業知識略知一二。

首先，在「文書及檔案管理電腦化作業規範」第 11 點揭示著電子檔案管理應達成真實性(Authenticity)、完整性(Integrity)、可及性(Accessibility)等 3 項目標，在所謂的「安全及可信賴的網路環境」，主要是確保資訊在網路傳輸過程中，能夠鑑別（ Authenticate ）資料傳送(或商務交易)雙方的身分，防止事後否認其交易事實。 就資訊安全的觀點來看，電子檔案管理必須達成的目標臚列如下：

(一) 真實性(Authenticity)：或稱鑑別性，確保網路中個體(Entity)的身分確實如他所表明的，或由網路所接收的資料確實為該傳送者(Sender)傳送。亦即可鑑別及確保電子檔案產生、蒐集及修改過程的合法性。

(二) 完整性(Integrity)：確保網路中所傳輸之資訊與原來的資訊一致，不會遭到竄改或偽造。亦即在電子檔案管理流程中，確保儲存電子檔案的內容、詮釋資料及儲存結構之完整。

(三) 可及性(Accessibility)：指藉由電子檔案保存機制，配合法定保存年限，維持電子檔案及其管理系統的可用性。

要達成前述目標，其對應作為簡述如下表：

電子檔案管理目標對應作為一覽表

目標	對應作為
真實性	運用電子憑證加簽

完整性	運用雜湊函數計算雜湊值
可及性	制定一致性的線上簽核電子檔案格式
註：憑證金鑰做法，有對稱與不對稱處理方式	

上述對應做法，實須仰賴密碼技術(Cryptography Technology)中的加密技術(Encryption Technology)與數位簽章(Digital Signature)技術。本文後續將逐一簡介相關技術。

四、電子檔案管理要求

「文書及檔案管理電腦化作業規範」之電子檔案管理相關要求：

(一) 電子檔案點收作業

1. 線上簽核歸檔之公文點收確認，應加附機關憑證製成之電子簽章，並視需要附加檔案管理人員憑證。
2. 線上簽核歸檔之公文依簽核電子檔格式規定封裝處理，含括公文本文、來文、附件、各層級簽核者憑證公鑰、簽核意見、簽體及時間紀錄等。
3. 點收後之電子檔案，不得任意刪除或修改，且應依機關檔案分類系統將其歸入相關之案卷。
4. 應採案件及案卷分別著錄電子檔案之詮釋資料，其項目依附錄 2 之電子檔案詮釋資料格式規定辦理。

(二) 電子檔案儲存保管

1. 辦理電子檔案儲存時，應依附錄 8 電子檔案格式表及附錄 9 電子媒體規格表選擇適當者為之。
2. 各機關應配合電子檔案之保存年限，評估保存維護成本，依據附錄 9 之電子媒體規格表規定，適時辦理電子檔案之轉置、更新、模擬及封裝，並優先採取轉置之方式。進行前項作業時，應先製作 2 套以上備份，分置於不同地點保管。
3. 各機關保存電子檔案時，應進行電子媒體之檢測與維護，確保其安全；並應指派專人負責電子檔案軟硬體設施之維護、轉置、更新、模擬及封裝。

(三) 電子檔案清查作業

機關電子檔案清查作業項目如下：

1. 確認檔案數量，並檢視檔案版本及清查歷程紀錄。
2. 抽樣讀取檔案，檢視檔案保存狀況。
3. 採電子簽章者，抽驗其封裝檔之電子簽章、簽體及雜湊值等驗證資訊。

前項清查結果發現有毀損、遺失、竄改等異常情形或應移轉（交）、銷毀、轉置及更新作業等需求時，應採取必要之處置措施。

(四) 電子檔案移轉(交)作業

各機關辦理電子檔案移轉（交），應將詮釋資料併同封裝，驗證檔案之真實性、完整性及可及性，並依附錄 2 之移轉（交）電子媒體封裝檔格式規定附加機關憑證後，送交檔案管理局(接管機關)，其電子檔案命名原則應依附錄 10 之機關電子檔案統一命名原則規定辦理。

(五) 電子檔案稽核安全

1. 驗證檢查：各機關每年應辦理電子檔案稽核作業 1 次，應驗證電子檔案清查、鑑定、銷毀及移轉(交)作業之辦理情形，並將稽核結果作成紀錄。
2. 作業紀錄：記錄電子檔案異動事項，包括異動者、異動時間、異動內容及作業事項等。
3. 安全設定：具備憑證管理功能，公文檔案資料於網際網路傳輸時應加密處理，提供系統定期對時功能，提供應用檔案附加浮水印之防偽處理。
4. 各機關電子檔案之清查、技術鑑定、銷毀、移轉及稽核作業時，應由機關檔案管理人員會同相關資訊人員辦理。

貳、電子簽章相關技術

一、電子簽章法

在介紹密碼技術與數位簽章(Digital Signature)技術前，先來看電子簽章法第 2 條的用詞定義。

(一) 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。

(二) 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。

(三) 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。

(四) 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。

(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。

(七) 憑證實務作業基準：指由憑證機構對外公告，用以陳述憑證機構據以簽發憑證及處理其他認證業務之作業準則。

(八) 資訊系統：指產生、送出、收受、儲存或其他處理電子形式訊息資料之系統。

在日常生活中，人們通常會在文件上加蓋自己的印章或親筆簽名，用以證明這份文件的簽署人，並在法律上產生簽署效力，譬如政府機關在辦理採購標案，完成決標程序之後，甲、乙雙方會簽訂一個書面的契約文件，並且在文件上蓋上雙方代表人的印章或簽名，這樣才完成一個具有法律效力的商業交易，確定雙方的權利與義務。相同地，在網際網路電子商務的環境中，商業交易行為權利與義務的確定，就必須靠電子文件與數位簽章達成法律效力。就數位簽章、蓋印章、親筆簽名而言，三者功能相似，只是簽署的文件形式不同，數位簽章的對象是電子文件，而蓋印章、親筆簽名的對象是實體紙本文件。而電子簽章與數簽章又有何不同呢?電子簽章的方式如指紋、聲紋、瞳孔辨識等均屬之，而數位簽章也是電子簽章的方法之一。依電子簽章法第 10 條規定，應使用經主管機關核定的憑證機構所提供簽發的憑證，且憑證尚屬有效並未逾使用範圍，其所簽署的電子文件，才具法律效力。所以憑證機構必須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，送請主管機關審核，其憑證實務作

業基準變更時，亦同；而主管機關應公告經核定之憑證機構名單，目前電子簽章法的主管機關為經濟部。基此，各機關在推動線上簽核作業時，所使用的憑證，應使用經主管機關核定之憑證機構所簽發的憑證，目前使用最廣泛的憑證為內政部憑證管理中心所核發的自然人憑證。

二、密碼系統

在一個開放性網際網路的空間傳送資料，很容易被截取、竊聽、修改或偽造，為了保護資料傳遞的隱密性與完整性，同時要能辨識資料的來源，通常採用的方法，就是由送方運用密碼學技術，在傳送資料之前，先將資料加密處理。當收方收到資料後，再加以解密後取得原始資料內容。因此，在網路傳遞途中被竊聽或攔截時，竊聽者擷取的只是一堆無意義的亂碼，無法確知資料的真正意函。在密碼系統中有五個基本要素，分別是明文(Plaintext)、秘密金鑰(Secret Key) 、加密演算法(Encryption Algorithm)、密文(Ciphertext)、解密演算法(Decryption Algorithm)。

(一) 明文：是指加密前的原始資料。例如一組明文為「我是檔管人員」。

(二) 加秘密金鑰：秘密金鑰為一組電腦數字或文字。例如一組秘密金鑰為「lucky」。

(三) 加密演算法：是一個數學邏輯推演的運算式，通常是使用秘密金鑰對明文進行加密的編碼動作。

(四) 密文：加密之後的資料，如明文「我是檔管人員」，經由秘密金鑰「lucky」加密演算後，得到密文「dAeQc8Sw」。

(五) 解密演算法：是一個數學邏輯推演的運算式，通常是使用秘密金鑰對密文進行解密的解碼動作。

密碼學發展到現在，大概可分為對稱式金鑰（Symmetric Key）密碼系統、非對稱式金鑰（Asymmetric Key）密碼系統及信託式金鑰（Key Escrow）密碼系統等 3 類。本文僅針對對稱式與非對稱式二者略作介紹如後。

對稱式與非對稱式，其實它的概念很簡單，例如各位今天上班出門時，拿了一把鑰匙將大門鎖上，晚上回家時，拿出同一把鑰匙來開門，亦即鎖門、開門用的是同一把鑰匙，稱之為對稱式。相反地，非對稱式就是

指鎖門與開門是用不同的兩把鑰匙，第一把、第二把鑰匙的齒孔並不相同，但這兩把鑰匙又不是完全獨立毫不相關的鑰匙，可以用任一把鑰匙來鎖門，但開門時就必須用另外一把鑰匙(相關概念請參看圖 2、圖 3、圖 4)。

鎖門　開門

大門鑰匙

圖 2：對稱式概念

鎖門　開門

2 把配對鑰匙

圖 3:非對稱式概念

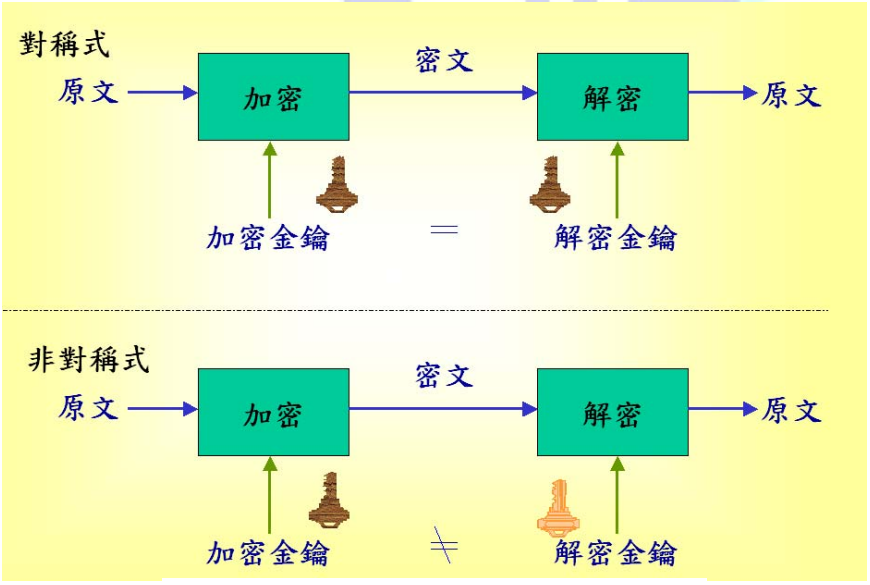


圖 4：對稱式與非對稱式加密概念

對稱式與非對稱式的觀念很簡單，但在系統實作時，技術就非常複雜，尤其是非對稱式金鑰密碼系統的建置與維護，都是相當耗費成本的一件事，圖 5 表達的就是對稱式與非對稱式加密處理的示意圖。

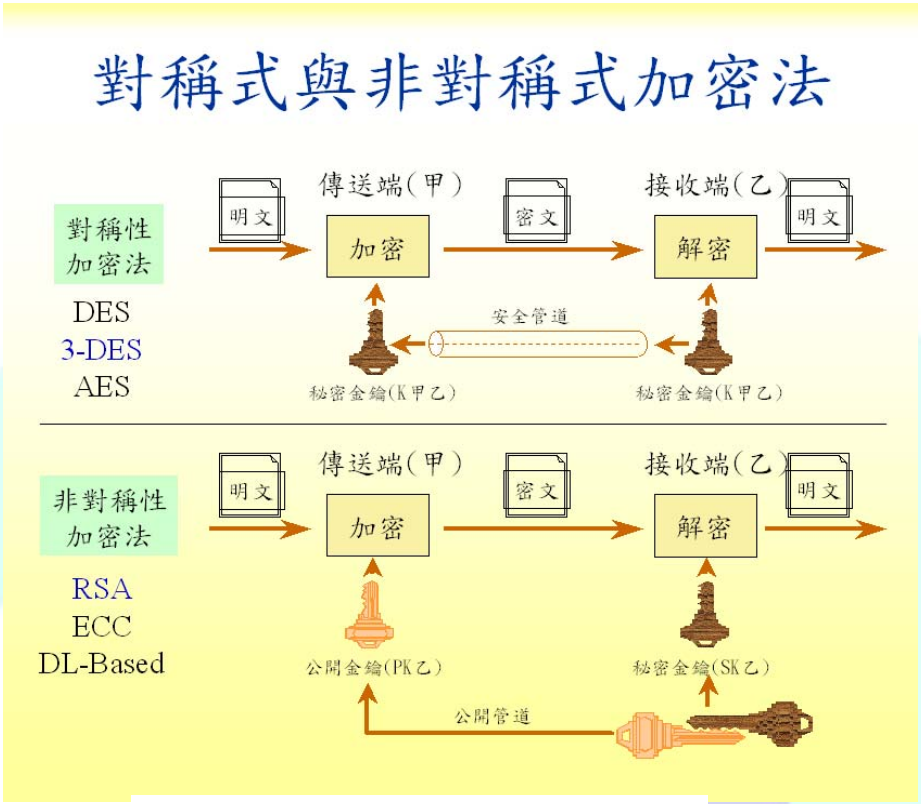


圖 5：對稱式與非對稱式加密法示意圖

對稱式金鑰密碼系統已經發展很長的一段歷史，加密及解密的速度優於非對稱式金鑰密碼系統，但是它最大的缺點是加密與解密是使用相同的一把鑰匙，很容易經由數學演算推估，讓陌生的收方獲得送方的鑰匙，較常見的對稱式金鑰密碼系統演算法有DES、3-DES、AES、IDEA、SAFER、FEAL、等。

非對稱式金鑰密碼系統，又稱為公開金鑰密碼系統，主要是針對對稱式金鑰密碼系統的缺點。非對稱式金鑰密碼系統之設計理念是產生一對 2 把相互對應的金鑰(*Key Pair*)，一把鑰匙公開於網路上，讓需要者可以自由取得，這把鑰匙稱為「公鑰(*Public Key*)」，另一把鑰匙是由持有者私密保存，稱之為「私鑰(*Private Key*)」，別人幾乎無法從公鑰推算出私鑰；看似完美的設計，實際上要達到精密的安全，相對地代價也很

昂貴，它最大的缺點就是運算速度較慢。較著名的非對稱式金鑰密碼系統演算法有 RSA、ECC、DL-Based、DSA、Diffie-Hellman、ElGamal、Knapsack、Rabin 等。

三、數位簽章

因為公開金鑰密碼系統的運算速度較慢，在實際運用時，會先對電子文件以雜湊函數(Hash Function)的演算法，計算出固定長度的雜湊值(Hash Values)，其概念如圖 6 雜湊值又稱為「訊息摘要」(*Message Digest*)，其次再就摘要訊息加以簽章，代替對整份文件的簽章。

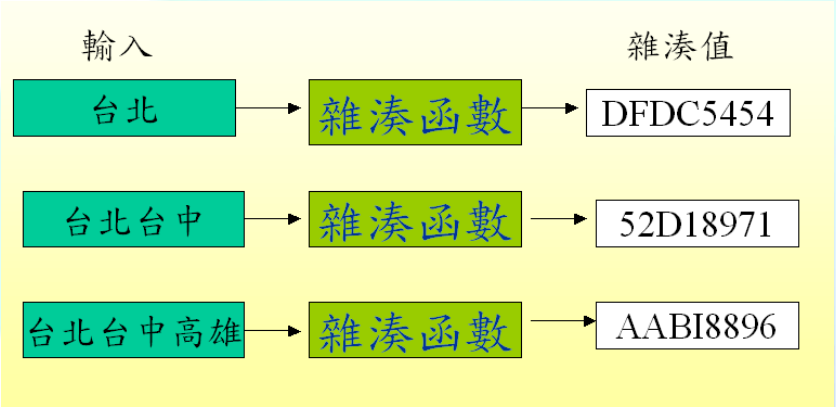


圖 6：雜湊值(Hash Values)概念

在簽章過程中所使用的雜湊函數是一種函數或演算法，它可以將任意長度的訊息原文，經過運算後加以濃縮轉換成為一固定長度的「訊息摘要」(如圖7)，較常見的產生訊息摘要的雜湊函數或演算法，有RSA公司MD家族的MD2、MD4、MD5、美國國家標準局(*National Institute of Standards and Technology*，*NIST*)制定的SHA、SHA-1，以及歐盟RIPE專案的RIPEMD、RIPEMD-128、RIPEMD-160等。

這種做法的特色是：

(一) 輸入任意大小的訊息，輸出固定大小的訊息摘要(Message Digest)。

(二) 單向(one-way)，無法從訊息摘要逆向推算取得訊息原文。

(三) 抗碰撞(collision resistance)，輸入不同的訊息原文，一定會輸出不同的訊息摘要。

(四) 計算速度快。

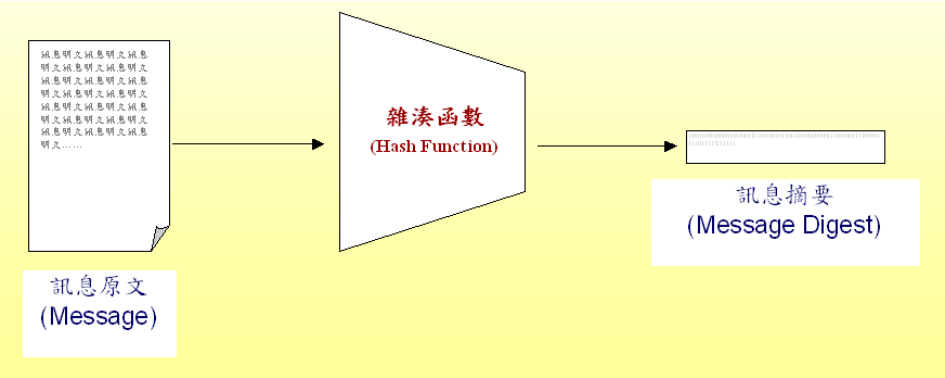


圖 7：訊息摘要示意圖

數位簽章是架構在公開金鑰密碼系統(Public Key Cryptosystem) 的基礎上，在這個系統中，每一位使用者都有自己所獨有的金鑰對(Key Pair)：一把私鑰(Private Key)和一把公鑰(Public Key)。私鑰由使用者自行私密保存，公鑰則公布在網路中。如圖 8 所示，張小姐要寫一封信給李先生，張小姐先用自己的憑證私鑰簽署信件內容，證明這封信是張小姐寫的，再拿李先生的公鑰加密，使這封信以密文方式透過網路寄送給李生生，因此，在傳送過程中，信件如果被截取，截取者沒有李先生的憑證私鑰，也無法開啟信件，或者開啟之後，也是一堆亂碼無法辨識信件內容。當李先生收到信件之後，必須用李先生的憑證私鑰解密與開啟信件，再拿張小姐的公鑰，確認信件確實是張小姐寄來的；經由前述複雜程序，對寄信的張小姐及收信的李先生而言，都產生了不可否認的作用，加密作法也強化了隱私機密性的功能，在張小姐簽署信件的同時再加上前述雜湊值的運算，更能確保信件內容的完整與真實。

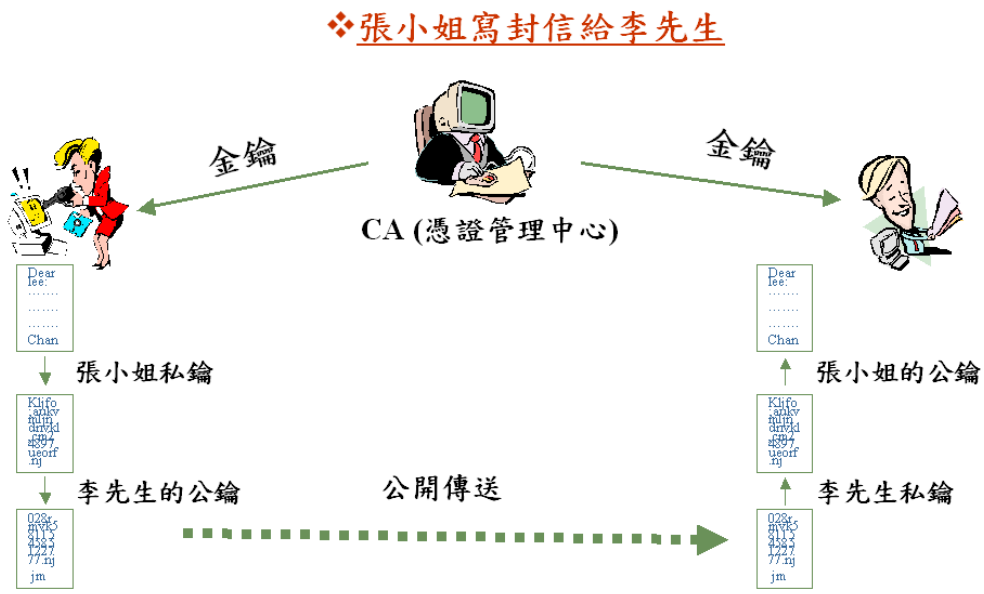


圖 8：私鑰/公鑰運用示意圖

由張小姐給李先生一封信的案例來看，數位簽章的設計就可以清楚得知寄信者，負責簽章證明自己是寄信的角色，而收信者則要驗證發信來源及信件內容是否被竄改或偽造。在數位簽章系統的設計，就是發送者要進行簽署時，他要將簽署的電子文件與個人的私鑰當作簽署演算法的輸入值，經由該演算法的計算後，便可取得電子文件的數位簽章。收信者收件後必須負起驗證者的角色，將收到的電子文件與數位簽章，以及簽署者的公鑰，加以演算驗證，這種用來驗證數位簽章有效性的方法或程序，就稱之為「簽章驗證機制」。藉由以上的機制達到完整性、真實性(鑑別性)、不可否認性等安全保護功能(如圖 9)。

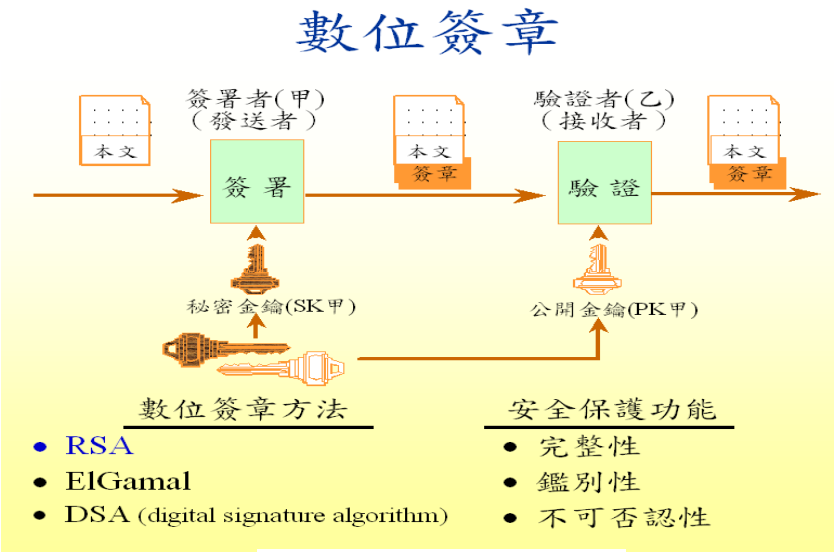


圖 9：數位簽章作法

當政府機關紛紛推動公文線上簽核之際，囿於線上簽核公文已無紙本文件可供日後稽核，尤其涉及法律層面時，更應小心謹慎，因此檔案管理局於 92 年著手設計電子公文檔案管理系統，為了確保簽核者的權利與義務，捨棄傳統帳號密碼的設計方式，以憑證加簽；惟考量電子文件的不可否認性、完整性、真實性及自建憑證機構，須耗費大筆建置成本及後續維護成本，乃採用內政部憑證管理中心簽發的自然人憑證，作為線上簽核加簽之憑證。基於效能考量，先將簽核文稿與附件，以「雜湊函數」計算出訊息摘要，再將此固定長度的訊息摘要，以簽核者私鑰加簽，產生數位簽章值，再將簽核文件併同數位簽章值，傳送給下一個簽核者。由於採用的雜湊函數係屬不可逆的單向函數，無法直接由簽章值推算訊息摘要值。系統在下一個簽核的收文開啟內容時，已在背後進行驗章處理，即電子文件先以相同的雜湊函數計算訊息摘要值，再以前一個簽核者的公鑰與接收到的數位簽章值，計算出訊息摘要值，如果前後二個訊息摘要值相同，就可確認電子文件未被竄改及簽章確為前一個簽核者身分無誤(如圖 10)。亦即數位簽章與電子文件息息相關，如果電子文件被非法變更，則數位簽章就無法通過驗證機制的驗證，也就可以證明簽署的文件被非法竄改。

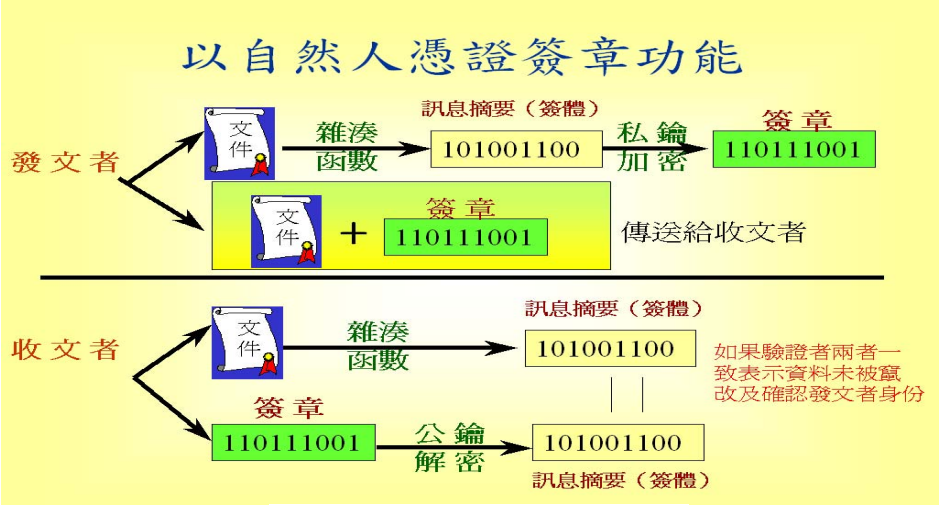


圖 10:自然人憑證簽章做法

檔案管理局規劃設計電子公文檔案管理系統時，結合訊息摘要、憑證加簽，逐層封裝處理模式，初步驗證已可將線上簽核電子公文檔案及其附件之數位內容檔案完整封裝，並透過電子簽章、雜湊值計算等技術，達到完整性、真實性規定。

參、風險管理概論

風險係指潛在影響組織目標之事件，及其發生之可能性與嚴重程度，而風險管理（Risk Management），又名危機管理，是一個管理過程，包括對風險的定義、測量、評估和發展因應風險的策略。風險管理的目的是將可以避免的風險、需花費的成本及可能造成的損失盡量最小化。因為組織的資源有限，理想的風險管理，應該依據風險的等級事先排定優先次序，可以優先處理引發最大損失及發生機率最高的事件，其次再處理風險相對較低的事件。

風險管理的步驟與過程常被視為一個持續改善的反覆過程或循環，以紐澳標準 AS/NZS 4360 風險管理架構為例(如圖)，步驟如下：

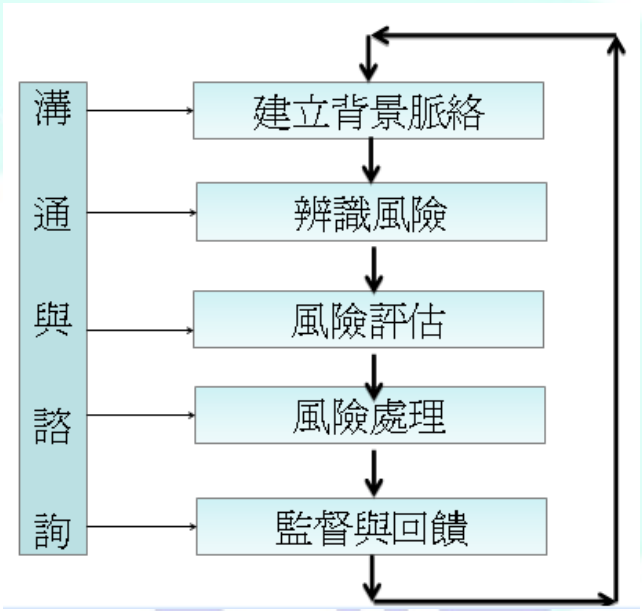


圖 11 風險管理管理架構

一、建立背景脈絡

風險管理架構須在外部環境要素與組織內部環境背景體系下執行，背景體系不但提供決策所需要的指導，也為了後續的步驟建立了框架。建立背景環境之細部工作為：

(一) 建立外部環境背景。

(二) 建立內部環境背景。

(三) 訂定風險管理步驟。

(四) 依組織目標和利害相關人期望，發展風險評量標準。

(五) 定義風險分析對象。

二、辨識風險

以有系統的方法，運用核對風險清單、SWOT 分析法、過去的經驗與紀錄、流程表、系統分析等工具或技術，找出所有可能影響風險分析對象的事件，並考慮這些事件可能發生的原因、時間、地點與順序。

三、風險分析

了解潛在的風險事件後，須利用定性、定量或綜合性方法，評估每一風險發生的機率及其可能造成的影響，將兩者結合成為風險等級。分析事件發生機率及其影響，並依照過去的紀錄、經驗、其他組織的應用經驗及專家意見等，以避免主觀偏見。

四、風險評估

此步驟與前述風險分析步驟合稱為風險評估。將風險分析結果與風險基準進行比較，排出優先順序，找出需要優先處理的風險。

五、風險處理

於風險評估結果中選出需優先處理之風險，根據風險屬性，訂出可行的風險對策，如規避、降低機率與轉移、分散、接受等方法。降低風險發生機率與影響的方法即為風險控管計畫，如新政策或程序改變、緊急應變及災後復原之規劃等，以降低潛在的損失。列出所有的風險對策後，須依各對策可降低風險的程度及其可創造的額外機會加以評估；執行成本也是評估因素之一，若資源有限，應排定執行優先順序，選擇合適對策，經準備後執行。

六、監督與回饋

此步驟貫穿整個風險管理架構，隨時了解內、外部環境的變化、事件機率和影響的變化，這些都可能影響風險處理之優先順序，執行風險控管計畫後，亦應監督執行成效、定期檢討，據以修正風險分析結果，訂出新的風險計畫。

七、溝通和協商

為了克服對風險認知不同所造成的執行障礙，溝通和協商提供風險利害關係人間的對話管道，確保雙方了解決策與行動的基礎。

管理循環的每個步驟皆互相影響，且為動態的過程，組織須隨時提高警覺，適時修正計畫，風險雖難以完全避免，但至少能儘量降低損失。

了解可能面對的風險後，如何降低風險發生的機率？若風險勢不可免，如何使損失降到最低？控制風險策略包括了下列方法：

一、 規避風險：可朝修改資訊作業方式或採用技術以避開風險，或經由政

策或標準，禁止從事高風險交易或活動。

二、轉移風險：將營運相關風險轉移給其他組織，例如：承保商、供應商。

三、接受風險：如該風險符合組織的政策與風險接受準則，並充分瞭解其影響程划度，則客觀地接受風險。

四、降低風險：可以參考標準選擇適當之控制措施，以降低風險。並可以藉由加強各項作業之內部控制，以降低風險發生之機會。

史丹佛大學 Rosenthal 等人於 2005 年根據美國國家研究諮詢會議對國家檔案與文件署所提的建議，提出數位典藏威脅模型，列出以下類型的潛在風險：

一、儲存載體失誤：儲存載體長期使用後損耗，引起無法回復的位元錯誤，或大量的資料流失。

二、硬體失誤：可復原的硬體失誤如短暫停電，不可逆的失誤如因電源供應器毀損。

三、軟體失誤：病毒即可能對資料造成風險。

四、傳輸錯誤：無法確知某特定時段所傳送或攝入系統的內容是否正確，或有無被更動。

五、網路服務失誤：外部網路，如網域名稱及 URL 可能會暫時或永久消失，無法提供服務。.

六、載體與硬體淘汰過時：因科技更新迅速，儲存載體與硬體很快就被新一代產品取代，舊產品雖仍可使用，但無法再與系統其他部分溝通。

七、軟體淘汰過時：當資料儲存格式有了新的標準，舊格式資料即使存在，亦難以再解讀取用。

八、人為操作失誤：人為的疏失，可能對電子檔案及其系統造成可復原或不可復原的傷害。

九、天然災害：水災、火災與地震都是可能的風險。

十、外部攻擊：與公共網路連結的系統可能遭駭客竊取、竄改資料或植入惡意程式。

電子檔案保存屬於數位典藏的一部分，美國 OCLC（Online Computer Library Center）提出名為「INFORM」的評估數位典藏風險的方法，將風險分為 6 大類，評估者可針對各類別下細分的風險項目評估機率及造成衝擊的程度，計算出風險係數，做為典藏行動的決策參考，其風險類型如下：

一、數位物件格式：規格本身，還有相關的壓縮演算法規格、專利或格式、

數位產權、加密、數位簽章等所引發的風險。

二、軟體：作業系統、應用軟體、轉置程式、壓縮演算法…等所有必需的軟體元件所引發的風險。

三、硬體：如儲存載體的形式、中央處理器、輸出入裝備與周邊設備等硬體元件所引發的風險。

四、相關組織：與上述 3 項風險有關的組織，如軟體開發者、廠商、數位內容擁有者等，也可能引發風險。

五、數位檔案館本身的風險，如系統架構、流程及機構組織因素。

六、格式轉置：除上述 5 類別風險外，轉置過程本身亦為風險來源。

電子檔案是組織的重要資產，它和其它重要的營運資產一樣具有價值，需要持續給予妥善保護。組織應以管理面、技術面與實體面規劃安全防護體系(如圖 12)，以保護電子檔案不受各種威脅，確保可以持續保存與應用，並將損失降到最低。

圖 12 安全防護體系

肆、電子檔案風險與管理

由於資訊科技進步得非常快，新的技術與設備不斷地推陳出新，使得電子檔案的格式、儲存媒體和使用方式都有相當大的改變。一般人最能感受的是個人電腦的演進，從 1946 年的 ENIAC、1964 年的 CDC 6600、1977 年的 Apple II(Z80)、286、386、486、到近期的 Pentium；作業系統則由 1969 年的 UNIX、1981 年的 DOS 到 Windows 3.0、Windows NT3.15、Windows NT、Windows 95、Windows 98 演進到近期的 Windows XP、Windows VISTA 及 Windows 7，1976 年發展的 vi 編輯器適用於 UNIX 作業系統；PE2（IBM Personal Editor II）為 1980 年 IBM 出產，於 PC-DOS 或 MS-DOS 電腦系統適用的個人文書編輯商業軟體，第一個 Windows 版本的 Word，到 WORD97、WORD98、WORD2000、WORD2003 及 WORD2010，在硬軟體演進的過程中，已有數不清的硬、軟體已過時失效。

隨著數位化資料的快速增加，高容量儲存媒體的需求也變得更加的迫切，新的技術與媒體也不斷問世，早期各機關使用的磁帶、軟碟片、光碟及硬碟等媒體，逐漸被新的儲存媒體所取代，而相關的電腦軟硬體也隨著淘汰換新，未來可能會找不到設備，可以讀取保存在磁帶、軟碟片上的電子檔案。因應不同的保存與應用的需求，產生各種動靜態的檔案格式，如文字檔有 xml、pdf、odf、txt、rtf、doc 及 ppt 等，圖片檔有 tiff、png、jpeg、wdl、pdf、iges、dxf、step、bmp 及 gif，聲音檔有 wav、mp3、midi、wma、ra，視訊檔有 mpeg-2、avi、mpeg-4、wmv、rm、mov，壓縮檔有 zip、7-zip、rar、tar 等。

為了確保電子檔案於法定保存年限仍可存取應用，機關應以國際或業界標準、穩定性、普及性等面向進行評估，並依「文書及檔案管理電腦化作業規範」附錄 8 電子檔案格式表(如表 1)，選擇適合保存的檔案格式，以避免未來維護之困難，並應定期檢視檔案格式及讀取軟體，評估是否有格式轉置需求。

電子檔案格式表係規定適合保存的格式，機關如果因為業務特性需求，採用非符合本表格式，應考量保存年限內電子檔案存取問題。如果採用符合本表之電子檔案格式，未來該格式過時或閱讀該格式之軟體已無廠商支援時，檔案管理局將會規劃開發轉置工具提供使用。。

表1 電子檔案格式表

類型	格式	說明
文字檔	XML	一、開放性標準。 二、電子公文傳遞交換格式。
	PDF	業界認定可攜性文件格式。
	ODF	一、國際標準（ISO/IEC26300:2006）。 二、XML 開放性架構，具可攜性文件格式。
圖片檔	JPEG	一、如檔案係以影像掃描製作，一律採全彩，壓縮品質為 75%以上，解析度 300 DPI 以上。 二、開放性標準。
	SVG	開放性標準。
聲音檔	MP3	開放性標準。
	WAV	開放性標準。
視訊檔	MPEG-2	開放性標準。
	AVI	專屬軟體。
	H.264	開放性標準。
工程圖檔	IGES	美國國家標準（ANSI Y14.26M）。
	DXF	開放性標準。
	STEP	國際標準（ISO/IEC10303）。
文字影像檔	JPEG	一、彩色影像：採全彩，壓縮品質為 75%以上，解析度 200 DPI 以上。 二、開放性標準。
	TIFF	灰階影像：採解析度 200 DPI 以上。
	TIFF	一、黑白影像：採 CCITT G4 標準，解析度 300 DPI 以上。 二、業界認定開放性標準。
	PDF	業界認定可攜性文件格式。
	WDL	國內開發之可攜性文件格式。
	PNG	一、索引色影像：採 256 色 ZIP 非破壞性壓縮，解析度 300DPI 以上。 二、線上簽核使用追蹤修訂功能時，採用本格式產生簽核頁面。
數位墨水	ISF	一、手寫簽核資料採用本格式以筆跡方式存檔。 二、筆跡檔案業界認定開放性標準。

許多人都以為檔案數位化之後，所有的管理工作都可以一勞永逸，然而因應長期保存與應用的需要，諸多問題正衝擊電子檔案的管理作業，究竟電子檔案存在著哪些問題呢?

(一) 資料與載體密不可分

資料必須依附在特定的媒體才能儲存，無法簡單地儲存記錄在紙本材

質。隨著數位化資料迅速增加，高儲存容量與高穩定性是選擇儲存媒體的重要因素，2003 年美國國家檔案及文件署修訂的 Code of Federal Regulation 建議機構以 DLT 磁帶及光學媒體，轉置須永久保存的電子紀錄。然而磁帶也有它的風險與威脅，相較於燒錄型光碟（如 CD-R、DVD-R、DVD+R 等）的使用壽命和資訊安全的顧慮，磁帶目前仍然是各機構所採用的主要儲存媒體，足見選擇儲存媒體也是一項慎重的事。為了長期保存檔案，媒體技術的快速發展，媒體格式與材質成分的多樣性，都造成磁性媒體選用的困擾。

(二) 易於修改與複製

電子檔案最大的方便就是可以很簡單、很方便地任意修改與複製，正因為它的方便性，也造成資料被任意複製而無法知悉，或被不當竄改而不易查覺，以致於危害電子檔案的公信力，也潛藏著資料遭竄改與洩露的危機。

(三) 軟硬體過時與淘汰

資訊科技軟硬體快速銳變，因應電子檔案格式、儲存媒體改變，程式與系統必須跟著變，硬體設施也隨著換新，曾經叱吒風雲的軟體、硬體，因新設施新程式的出現，不得不走入歷史，既存的電子檔案面臨著無軟硬體可讀取內容，隨著時間的過去，檔案格式時有變革，以致於降低電子化檔案的可讀性，迫使電子檔案持有者可能面臨有資料卻無法知悉的無奈。

(四) 儲存媒體劣化

各種儲存媒體都有化學性材質，這些材質的劣化都會導致資料的遺失，電子檔案的內容或與之相關紀錄也可能會遺失，以致於保存的電子檔案毫無價值可言。若以磁帶劣化的因素而言，包括：黏著劑劣化、磁粒不穩定、聚酯基底變形老化等，美國國家媒體實驗室進行媒體穩定性研究，期能有標準估測方法預測磁帶的壽命，對於習慣使用紙張及微縮的人而言，可能會對磁帶媒體的壽命感到苦惱，縱然光碟製造商聲稱其產品的壽命可達一百年，但是科技設備卻可能在十年內過時，因此縱使儲存媒體完好如初，卻仍須面臨無硬軟體閱讀的可能性。

(五) 檔案格式繁多

因應各種不同的使用目的，產生各種靜態、動態不同的檔案格式。又如大家耳熟能詳的電子郵件，也會因使用的郵件系統不同，而有 smtp、pop3、imap、http(s)、s/mime。實務觀之，許多的檔案格式，可能來不及被大眾使用，就已經被淘汰，為了長期保存，多如牛毛的檔案格式，只會增加各項維護成本的支出，因此對於必須長期保存的電子檔案，確實有必

要限縮格式的數量，甚至制訂公開、標準格式，如同美國麻州州政府力挺開放式標準文件(OpenDocument)，可視為確保電子檔案長期存取的重要措施。

因為電子檔案必須依附特定的儲存媒體，而媒體又必須透過電腦軟硬體才能讀取，因此在保存過程中，有任何一個環節出了問題，就會影響電子檔案的存取，因此必須透過各種保存技術與策略，逐一克服。

一、在過時軟硬體上執行

電子檔案軟硬體更迭周期縮短，平均電腦使用年限 4-5 年。過時設備及軟體往往讓使用者棄之如敝屣，不願意繼續使用，對新生代而言根本不會使用。當軟硬體、儲存媒體或格式過時失效時，要如何確保電子檔案仍可以讀取？

二、電子檔案保存的證據性不足

檔案文件的法律證據，係基於簽署及章戳的認定。然而，過去電子文件多數不具備電子簽章。現行電子檔案簽署以採行數位簽章方式為主流；惟數位簽章尚未全面施行於政府機關，即便採行數位簽章，仍有憑證效期管理、時戳統一性等實務問題必須克服。

三、線上簽核電子公文檔案與公文影像儲存的困難

無論採行封裝檔的電子公文檔案，與採行非封裝形式的電子影音檔貯存，都會面臨貯存媒體老化及劣化。以人工持續檢查貯存在媒體中大量電子檔案有實際的困難，然而當發現電子媒體已損壞時，一般檔案管理人員無法自行處理修復。

四、業務性電子資料保存困難

廣義的電子檔案包含因電子公文所產生之電子檔案，以及因公務所產生的各類電子文件及資料。例如專業性公務資料庫，一般檔案人員若不具相關專業能力，無法解讀，例如氣象數據等，加上資料庫無法單獨存在，必須配合應用軟體及系統才能查閱，大幅提高保存難度。

五、數位典藏存在風險，但缺乏管理機制

安全、有效的數位典藏(Digital Archives)是電子檔案管理的目的。電子公文檔案為目前數位典藏的重要部分。數位典藏面臨電腦軟硬體環境變化風險，包含數位物件內容格式、簽章方式、壓縮方法、加密演算法等變化，加上電子檔案管理組織成員異動，人為操作錯誤及不可抗力的資料外洩等，都是造成破壞數位典藏內容的風險，一般檔案人員卻無從防範。

以上有關電子檔案的問題並非單一存在，彼此間相互牽連，目前在國際間尚未找到快速、正確且一勞永逸的解決方式。電腦與傳播科技大師 Nicholas Negroponet 先生曾說：「從原子潮流演變到位元的潮流已是勢不可擋。」網路通訊的蓬勃發展與資訊科技的日新月異，使得網際網路(Internet)、全球資訊網(World Wide Web)、高速網路(Information Highway)、網際空間（ Cyberspace ）等前仆後繼，實體生活中所有文件資料、聲音、影像等資訊，皆可在彈指間分享給遠洋的親友，甚至分享給不知名的第三人。檔案管理人員要管理的電子檔案範疇究竟在哪裡？要如何因應電子檔案的諸多問題，是值得多方思索研究的課題。因此，檔案管理局在 96 年研提國家檔案數位服務計畫(97-100 年)，該計畫最重要的一環，就是為建構電子檔案長期保存機制而努力，100 年研提文書檔案資訊網路合一計畫(101-105 年)，賡續研發整合電子檔案長期保存相關技術與工具。

電子檔案的生命週期漫長，從蒐集與產生、保存與維護、應用、清理等階段，影響電子檔案保存與持續提供應用的變數甚多，從電腦軟硬體、檔案格式、儲存媒體、人為操作及天然災害等，這些不確定因素，都可能阻礙達成電子檔案保存與應用的目標。電子檔案面臨了各種不同的風險，組織應列出風險並評估威脅與衝擊，不斷持續地修正，以避免風險或降低風險發生的影響性，以下列出電子檔案風險控制：

一、技術過時風險控制

(一) 應配合電子檔案之保存年限，評估保存維護成本，選擇適當儲存媒體。

(二) 定期辦理電子媒體之更新或轉置作業。

(三) 定期檢討評估相關軟硬體設備之有效性。

(四) 評估國際或業界標準、穩定性、普及性等面向，選擇適合保存的檔案格式。

(五) 採用一致性的線上簽核電子檔案格式，並限縮附件檔格式。

(六) 定期檢視電子檔案格式及讀取軟體，確認其可及性。

(七) 保存閱讀電子檔案所需的軟硬體設備。

二、儲存媒體損毀風險控制

(一) 定期進行儲存媒體之檢測與維護，確保其安全。

(二) 異地備份儲存，並定期進行回復演練。

(三) 設立安全區域，建立門禁管制及環境控制設施。

三、電子檔案遭竄改、破壞(真實性與完整性)

(一) 採用電子簽章及雜湊值等機制。

(二) 定期採用工具檢測確認其完整性(技術鑑定工具)。

(三) 安全存取的應用系統、防火牆及入侵偵測，加強資訊安全，避免資料遭竄改或破壞。

(四) 採用唯讀型儲存媒體，避免資料遭不當竄改或刪除。

四、電腦病毒及惡意軟體的威脅

(一) 限制網路及可攜式媒體之使用。

(二) 建立備份政策

(三) 使用防毒軟體及防間諜軟體，並定期更新掃描軟體及病毒碼。

五、著作權保護風險控制

(一) 宣導著作權法。

(二) 法律約束。

(三) 於數位內容中加入浮水印，以保護數位內容之著作權。

(四) 採用數位版權管理(DRM)控管數位內容的的使用權。

六、隱私權保護風險控制

(一) 宣導個人資料保護法。

(二) 加強過濾詮釋資料/檔案目錄的內容。

(三) 安全存取的應用系統。

七、資料外洩，如間諜軟體(spyware)、駭客入侵、搜尋洩漏(search leakage)

(一) 建立資訊安全管理制度。

(二) 安全存取的應用系統。

(三) 防火牆及入侵偵測系統。

(四) 資料儲存加密及傳輸加密。

伍、長期保存策略

電子檔案長期保存是各國檔案主管機關共同面臨的挑戰，部分先進國家已於 8、9 年前即開始進行相關研究及實驗，惟迄今尚無確切有效的作法可供使用，一般較常被討論的電子檔案長期保存作法分述如後。

一、系統保存(system Preservation):將電腦軟硬體完整保留下來，類似建立電腦博物館。優點：可以完整呈現檔案原貌。缺點：過期軟、硬體無人能懂，系統異常無人能救，硬體故障無人能修，零件損壞沒有備料可供更換。

二、複製（Replication）:為降低軟硬體故障的風險，在一個或多個系統上重複製作一份或多份相同的資料，同時可辦理異地存放。優點：簡單方便。缺點：無法解決電子檔案格式與硬體過時的問題。

三、更新(Refreshing)：為防止儲存媒體過時或失效，將電子檔案內容從一儲存媒體複製至新的儲存媒體。優點：簡單方便。缺點：無法解決電子檔案格式過時的問題。

四、轉置(Migration)：電子檔案管理系統之軟硬體過時或失效，需進行軟硬體格式轉換，以便日後可讀取之作業程序。目前此作法是各界認為最常用且可行的方案；惟此作法會改變原始物件，使其適應新科技環境。轉置過程中可能會造成錯漏資料，需輔以人工檢核，惟大量檔案難以進行人工檢核作業。

五、標準化（Standardization）：將電子檔案格式朝向簡單化、開放式、標準化訂定，建立國際標準，提供大家共同依循使用。

六、封裝(Encapsulation)：將電子檔案及銓釋資料，以包裹方式儲存之。

七、模擬(Emulation)：於現有的技術環境下，將數位資料回復其原始作業環境，藉以呈現原有資料。

八、印成紙張或其他瀏覽媒體（Converting to Paper or Analog Media）。

陸、技術鑑定與保存工具

為了協助機關解決電子檔案長期保存與應用問題，檔案管理局自民國 97 年起執行「國家檔案數位服務計畫」，結合產官學界共同致力電子檔案生命週期管理制度、長期保存技術的研發工作，以解決國家及機關電子檔案移轉(交)及可能面臨的存取應用問題，並於 99 年 8 月 3 日正式啟用電子檔案長期保存實驗室。

為了擴大對機關服務範圍，以電子檔案長期保存實驗室的技術研發成果為基礎，於 100 年 4 月 29 日成立電子檔案技術服務中心，提供服務項目包括電子檔案格式轉置、媒體轉置、品質驗證、電子檔案修復、軟硬體設備系統保存、儲存媒體銷毀等技術服務與諮詢。目前已開發電子檔案技術鑑定工具、保存工具等，可免費提供機關下載使用，希望可以協助機關運用適合的工具，妥善保存管理電子檔案。

電子檔案內容易被竄改及偽造，而且電子簽章、加密及雜湊值等密碼學的運算，隨著電腦運算速度提升，被破解的機率與日俱增，因此，如何確保檔案的真實性及完整性，是檔案電子化後所必須面對課題。紙本檔案單靠肉眼即可看到檔案的內容，電子檔案則必須透過特殊的硬體設備及軟體才能讀取檔案的內容，因應資訊科技日新月異，當硬軟體更迭時，如何確保電子檔案內容仍可讀取，將是另一個必須面對的難題。

為了確保電子檔案在保存期間內仍具完整性、可及性及不可否認性，檔案保存價值鑑定規範規定了電子檔案技術鑑定辦理時機及原則，其中技術鑑定係分析電子檔案保存、移轉及應用過程中，所面臨軟硬體技術問題，就管理需求、技術變遷及法規面等因應策略，提出建議及報告。希望透過年度技術鑑定作業，定期檢視電子檔案，及早發現問題，避免因軟硬體過時、資訊系統異常、儲存媒體損毀、人員不當操作等因素，造成電子檔案缺漏或無法讀取等問題。

電子檔案技術鑑定的目的，是以技術方法確認保存電子檔案之真實性、完整性及媒體之有效性，在電子檔案法定保存期限內，可以有效的開啟及辨識內容技術方法，如載體是否有毀損等，提供電子檔案典藏的技術性統計資料，評估轉置必要性、規劃轉置方案及估算轉置成本之依據。

電子檔案技術鑑定評估指標可從下列各項工作著手：

一、電子檔案真實性及完整性

二、媒體之有效性。

三、電子媒體種類及數量。

四、電子檔案格式及數量。

五、憑證簽章之安全強度。

六、加密安全強度。

七、雜湊值安全強度。

電子檔案最大特點乃易於修改、複製、傳播，在高度便利特性下，檔案

的完整性(integrity) 、真實性（authenticity）、機密性(confidentiality)及不可否認性(non-repudiation)等成為維護管理電子檔案安全的重要指標，也是電子檔案後續再利用發展的關鍵因素。電子檔案之管理，涉及許多資訊科技，如何有效、正確管理電子檔案是檔案管理局目前最棘手的問題，為了建立一套完善的技術鑑定機制，檔案管理局率先進行電子檔案技術鑑定，藉由定期的檢視與確認，儘早發現電子檔案潛藏的問題，以協助機關更有效的管理電子檔案。

一、電子檔案技術鑑定工具

本工具可將符合「文書及檔案管理電腦化作業規範」附錄 2 之電子檔案封裝檔格式或機關自訂格式之封裝檔，以工具批次檢測封裝檔格式、外部檔案格式與雜湊值、憑證及簽章，並統計檔案格式及版本、憑證及簽章安全強度等，自動產出技術鑑定報告。

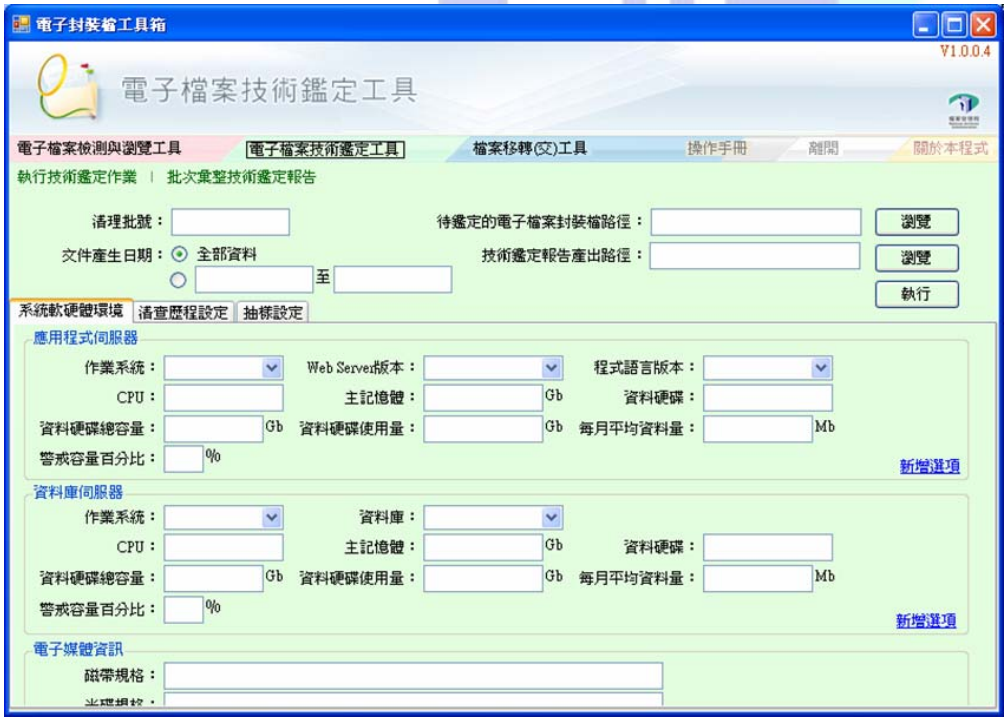
本工具目前整合於電子封裝檔工具箱(單機版)，安裝程式及操作手冊可提供機關下載使用(網址：http://erlp.archives.gov.tw)。本工具軟硬體需求如下：

(一) 作業系統：Windows XP 以上版本

(二) 處理器：1.5GHz 以上 處理器或同等級

(三) RAM：1GB 以上

(四) 安裝 Microsoft.NET Framework3.5 以上版本



二、電子檔案保存工具

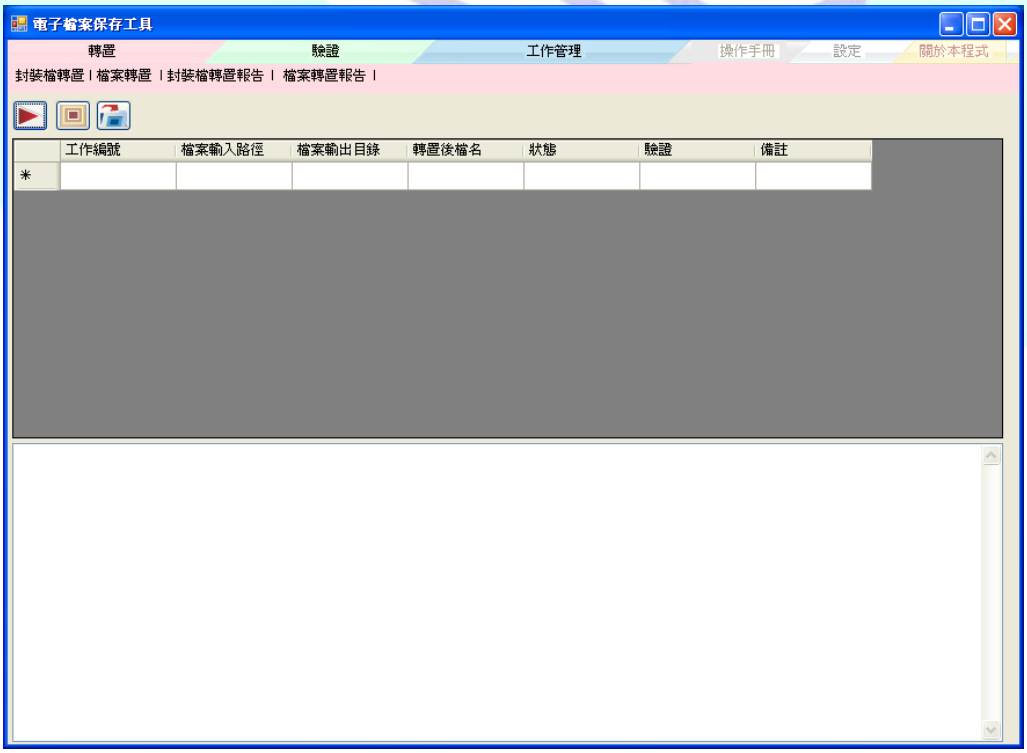
本工具目前區分完整版及簡易版(單機版)，提供電子檔案格式轉置、轉置品質驗證、影像檔及圖片檔修補(完整版)、OCR 辨識(完整版)及條碼辨識(完整版)功能。安裝程式及操作手冊可提供機關下載使用(網址：http://erlp.archives.gov.tw)。本工具之軟硬體需求如下：

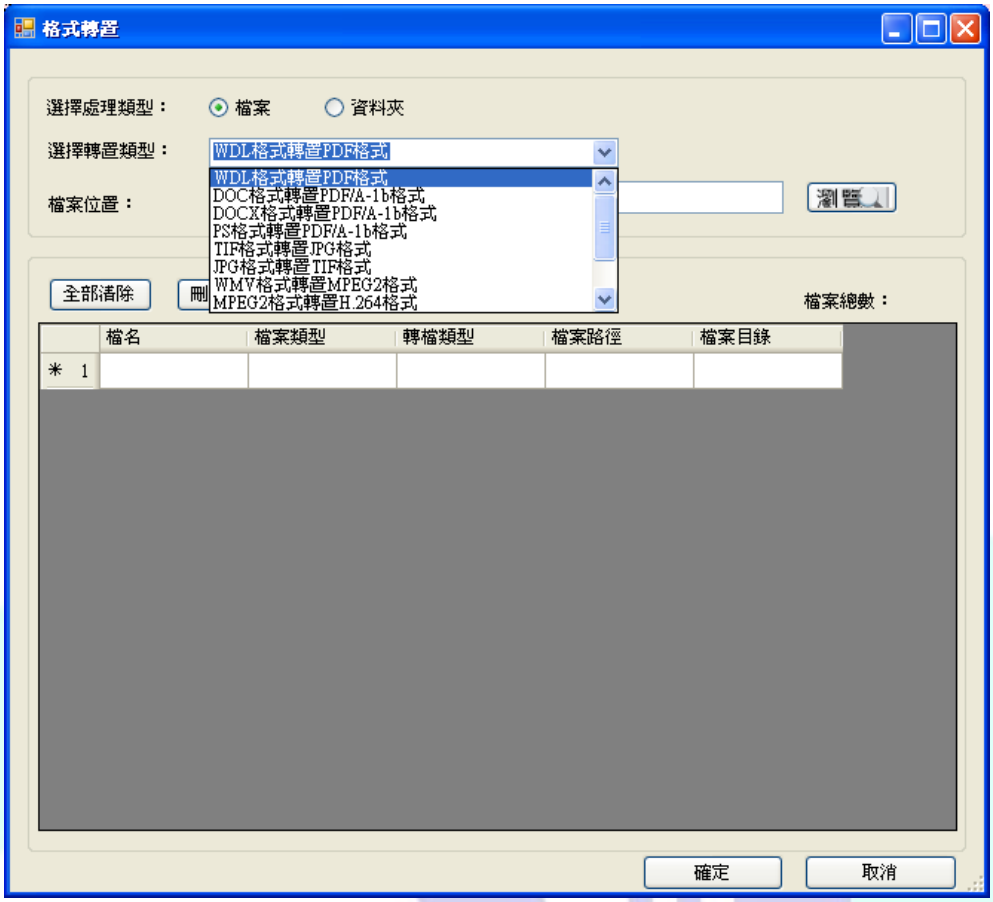
(一) 作業系統：Windows XP 以上版本

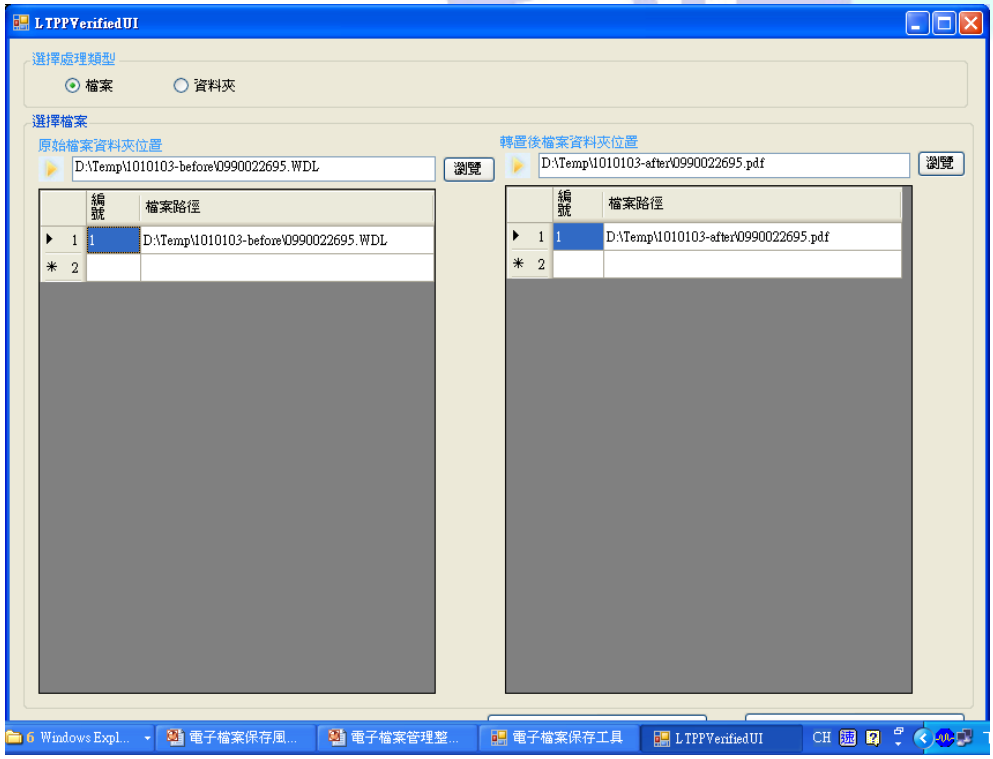
(二) 處理器：1.5GHz 以上 處理器或同等級

(三) RAM：1GB 以上

(四) 安裝 Microsoft.NET Framework3.5 以上版本




格式轉置
選擇處理類型：
檔案
資料夾
選擇轉置類型：
WDL格式轉置PDF格式
WDL格式轉置PDF格式
DOC格式轉置PDF/A-1b格式
DOCX格式轉置PDF/A-1b格式
PS格式轉置PDF/A-1b格式
TIF格式轉置JPG格式
JPG格式轉置TIF格式
WMV格式轉置MPEG2格式
MPEG2格式轉置H.264格式
檔案位置：
瀏覽
全部清除
檔案總數：
檔名
檔案類型
轉檔類型
檔案路徑
檔案目錄
確定
取消


LTPPVerifiedUI
選擇處理類型
檔案
資料夾
選擇檔案
原始檔案資料夾位置
D:\Temp\1010103-before\0990022695.WDL
瀏覽
轉置後檔案資料夾位置
D:\Temp\1010103-after\0990022695.pdf
瀏覽
編號
檔案路徑
1
D:\Temp\1010103-before\0990022695.WDL
D:\Temp\1010103-after\0990022695.pdf


參考影像
轉置影像
影像品質評估
差異圖
評估結果列表
過門檻值
未過門檻值
無法評估
轉置影像列表
D:/Temp/20120116_4/0991570120-P-00010.jpg
差異圖
選擇差異圖
評估分數
評估值
平均分數
MSE
PSNR
SSIM
90
0.997954
UQI
90
看差異圖
開始
下午 03:17

柒、結語

紙本檔案單靠肉眼就可看到檔案的內容，但是電子檔案必須依附在特定的媒體才能儲存，並透過特定的硬體設備與軟體才能讀取檔案的內容。面對電腦網路世界的瞬息萬變，儲存電子檔案的載體與格式受到資訊科技軟硬體快速蛻變的影響，使得閱讀這些檔案的軟硬體常會面臨過時或失效的問題。如果電腦不慎中毒或遭受破壞攻擊，甚至瞬間斷電等情形，都有可能造成電子檔案的損毀，由於電子檔案存在著許多不確定的潛在風險，因此，電子檔案的長期保存與管理變成一件非常棘手又不得不正視的問題。

電子檔案保存的目的就是為了便捷檔案檢調與應用，在數以萬計的電子檔案中，我們無法確知某件電子檔案何時會被調案，一旦有調案需求時，最重要的就是確保電子檔案的內容能夠開啟且正確完整的呈現，亦即如何確保電子檔案在法定保存年限內具真實性、完整性與可及性，是管理與保存電子檔案最重要的目標。在電子檔案「保存」的過程中，面對各種不同層次的風險。如何進行風險評估與管理，將風險概念融入電子檔案管理策略中，採取降低或避免風險衝擊之行動，才能確保國家社會的重要紀錄不至於流失。