

電子檔案保存風險與管理措施

檔案管理局

課程目標

- 協助學員了解電子檔案與風險管理的基本觀念，進而學習電子檔案保存風險及其控制方法，以因應電子檔案管理技能需要。

大綱

- 認識電子檔案
- 風險管理概論
- 電子檔案風險
- 電子檔案風險控制方法
- 結語

認識電子檔案

檔案的定義

- ◆ 檔案法：指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：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。

檔案的分類

◆ 依檔案管有機關：

■ 機關檔案

■ 國家檔案

◆ 依保存期限：

■ 定期檔案

■ 永久保存檔案

◆ 依檔案使用頻率：

■ 現行檔案

■ 半現行檔案

■ 非現行檔案

◆ 檔案媒體類型：

■ 紙質類

■ 攝影類

■ 錄影(音)帶類

■ 電子媒體類(電子檔案)

電子檔案相關名詞定義

◆ 文書及檔案管理電腦化作業規範：

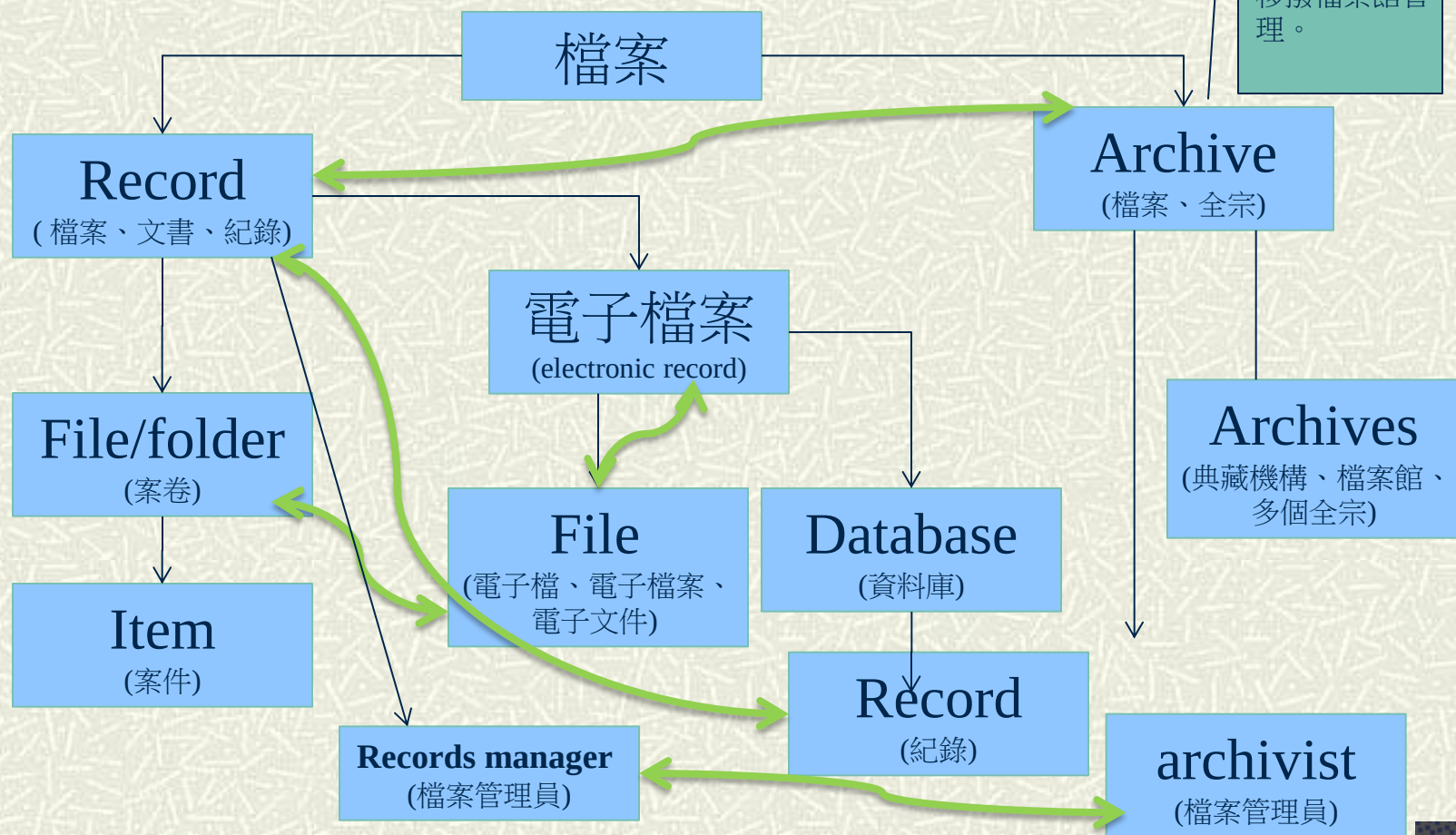
- 電子檔案：指電腦可處理之文字或非文字資料，且符合檔案法及相關法令規定等。
- 詮釋資料 (metadata)：指用以描述電子檔案有關資料背景、內容、關聯性及資料控制等相關資訊。
- 封裝檔：指將電子檔案與其詮釋資料及驗證檔案真實性、完整性之資訊，以包裹方式儲存之檔案。

電子檔案定義參考資料

機構/國家	說明
國際檔案理事會 電子檔案委員會	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。
美國聯邦檔案法	可記錄於任何電腦、電腦可讀取，且符合檔案定義的數字、圖檔與文字。
英國國家檔案局	電子化形成、收藏或傳輸的紀錄，不包含實體部分。
澳洲國家檔案局	由電子設備產生或維護的文件。
日本公共檔案法	由電腦上的軟體(如WORD)編輯而成的資料檔。
中國大陸電子公文歸檔管理暫行辦法	電子公文：各地區、各部門通過由國務院辦公廳統一配置的電子公文傳輸系統處理後形成的具有規範格式的公文的電子數據。

一個檔案名詞，各自表述

指具有永久保存價值的非現行檔案，通常移撥檔案館管理。

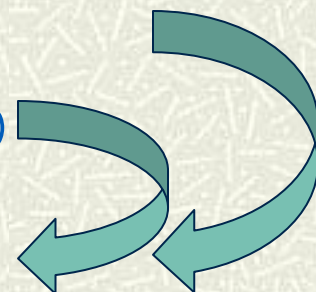


電子檔案管理目標

- ◆ 真實性（authenticity）：指可鑑別與確保電子檔案產生、蒐集及修改過程之合法性。
- ◆ 完整性（integrity）：指電子檔案管理過程，應確保儲存電子檔案內容、詮釋資料及儲存結構之完整。
- ◆ 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可供使用。

電子檔案相關法規

- ◆ 檔案電子儲存管理實施辦法
- ◆ 機關電子檔案管理作業要點(99年6月停止適用)
- ◆ 機關檔案管理資訊化作業要點(99年6月停止適用)
- ◆ 文書及檔案管理電腦化作業規範(99年12月修訂)
- ◆ 電子簽章法
- ◆ 行政院及所屬各機關公務人員電子識別證管理作業要點



電子檔案的分類

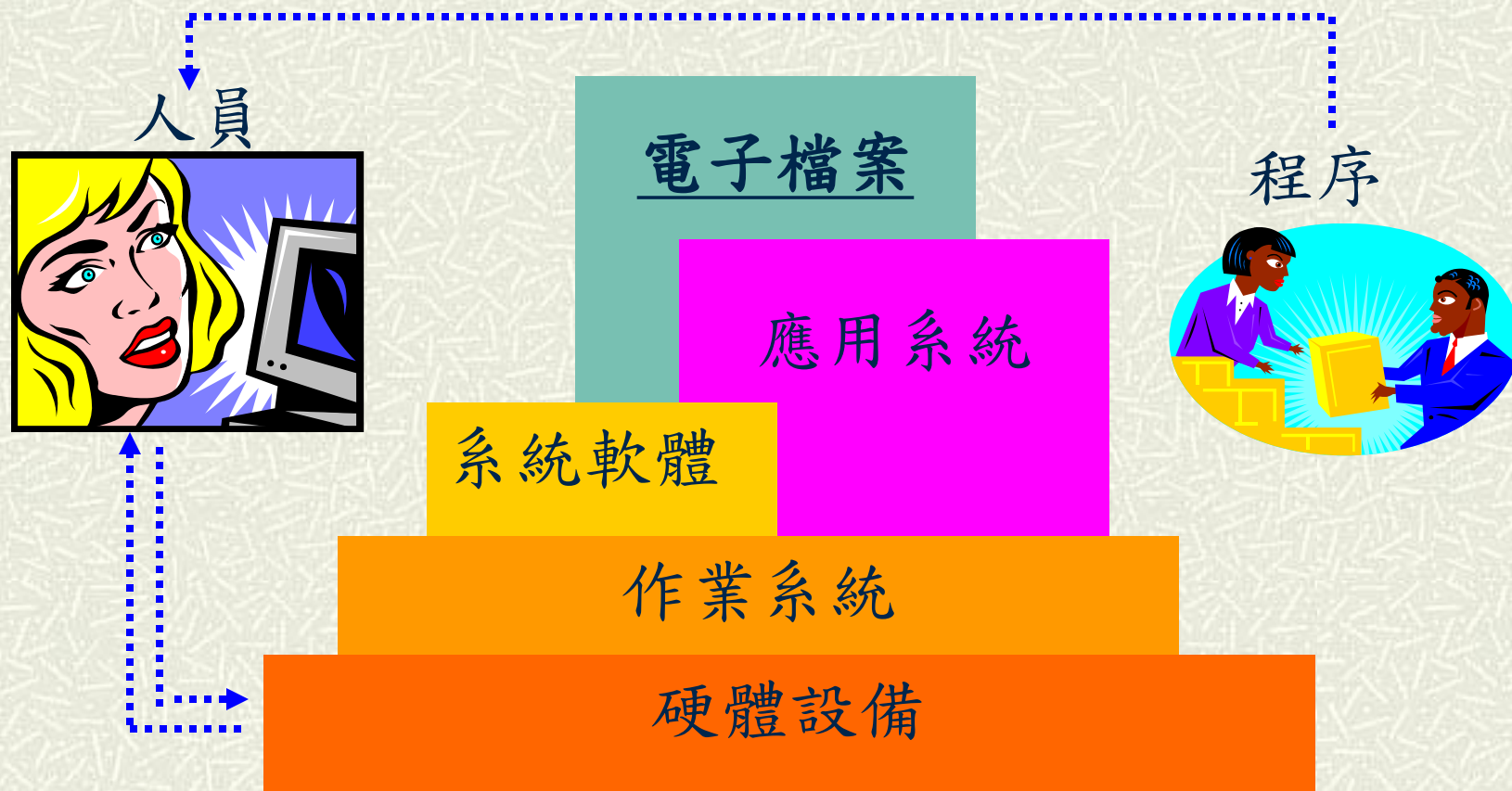
◆ 依格式：

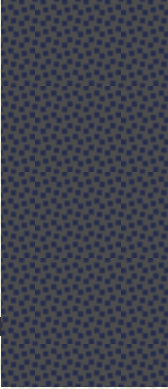
- 文字檔
- 圖形(片)檔
- 圖型檔
- 聲音檔
- 視訊檔
- 超文本(Hyper text)
- 混合型
- 雲端運算的檔案=雲深不知處(型)?

◆ 依媒體材質：

- 磁性媒體(如磁碟片)
- 光學性媒體(如DVD-ROM)
- 磁光性媒體(如MO)
- 積體電路(如 SD CARD)

電子檔案系統模型





風險管理概論

風險的意義

◆ 風險：

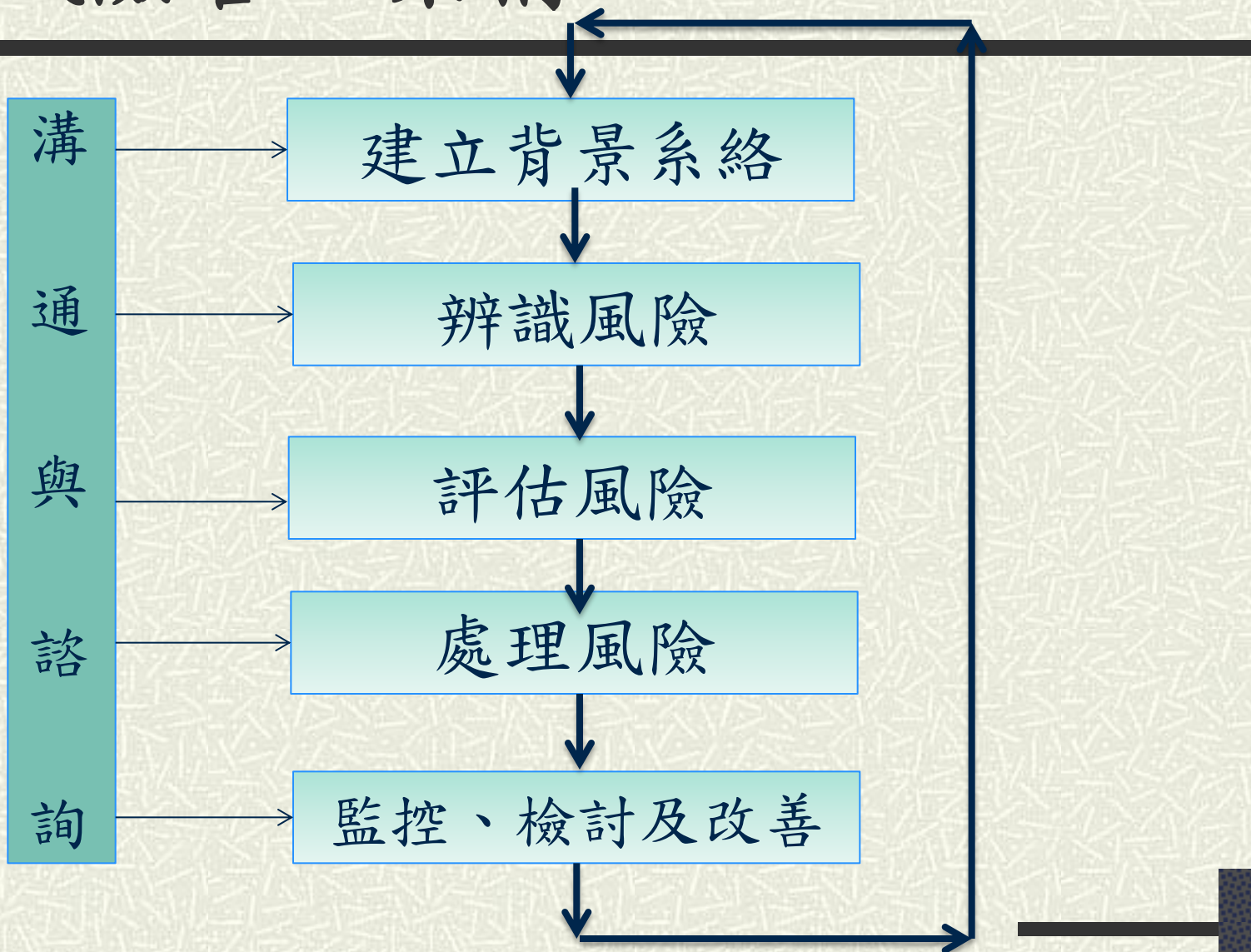
- 風險(risk)風險是指在某一特定環境下，在某一特定時間段內，某種損失發生的可能性。風險是由風險因素、風險事故和風險損失等要素組成。
- 風險的損害發生與否，損害的程度取決於人類主觀認識和客觀存在之間的差異性。

◆ 分為情況只會惡化的純粹風險和情況可好可壞的投機風險。

風險管理的意義

- ◆ 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。
- ◆ 目的是將可避免的風險、成本及損失極小化。
- ◆ 理想的風險管理，事先已排定優先次序，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。

風險管理架構



控制風險策略說明

◆ 規避風險

- 修改資訊作業方式或採用技術以避開風險。
- 經由政策或標準以禁止從事高風險交易或活動。

◆ 轉移風險

- 轉移相關之營運風險至他者，例如：承保商、供應商。

◆ 接受風險

- 符合組織的政策與風險接受準則，則知悉且客觀地接受風險。

◆ 降低風險

- 參考標準選擇適當之控制措施以降低風險。
- 藉由加強各項作業之內控以降低風險發生之機會。

資訊安全防護體系



電子檔案風險

電子檔案癥結問題

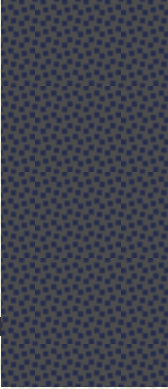
- ◆ 機讀性(Machine readable)：
 - 唯有靠機器，才可閱讀電子檔案；不同的軟硬體設備或設定，可能有不同呈現結果。(可及性)
- ◆ 電子檔案原件與複製品難以區別，檔案可在不同載體不同媒體儲存。(真實性)
- ◆ 電子檔案易於新增、修改及刪除。(完整性和真實性)
- ◆ 電腦病毒及惡意軟體的威脅。(可及性)

電子檔案癥結問題(續1)

- 著作權保護。
- 隱私權保護。
- 資料外洩，如間諜軟體(spyware)、駭客入侵、搜尋洩漏(search leakage)。(機密性)
- 業務委外。

電子檔案癥結問題(續2)

- 電子檔案長期保存及應用。(可及性)
 - 檔案格式及資料庫綱要。
 - 硬體設備
 - 系統軟體及應用系統
 - 人員(操作及維護)
 - 程序書(如操作手冊)
 - 雲端運算的衝擊？



電子檔案風險控制

機讀性風險控制

◆ 管理面：

- 培養專業(教育訓練)
- 建立職務代理制度
- 建立文件管理制度
- 建立設備維護體制

機讀性風險控制(續1)

◆技術面：

- 評估國際或業界標準、壓縮處理、操作難易、普遍性等面向，選擇合適的檔案格式。(標準化)
- 考量材質、容量、保存期限、存取方式、效率等因素，選擇合適的儲存媒體。(標準化)
- 採購合適的硬體設備及軟體。(標準化)
- 安全存取控制：製作及傳遞、點收歸檔、申請調閱、銷毀、移轉及移交。

機讀性風險控制(續2)

◆實體面：

- 設立安全區域，建立門禁管制及環境控制設施。
- 保存閱讀電子檔案所需的軟硬體設備。

原件與複製品區分風險控制

◆ 管理面：

■ 由機關確認：

- 依檔案法第9條第2項規定，經檔案管有機關確認者，視同原檔案，或複製品推定為真。

◆ 技術面：

- 區分正版與副版，兩版檔案格式或解析度不同。
- 加浮水印(water mark)。

原件與複製品區分風險控制(續)

- 記錄雜湊值。
- 以電子簽章加簽。

■ 實體面：

- 檔案原件實體隔離保存(封存)。

浮水印概念

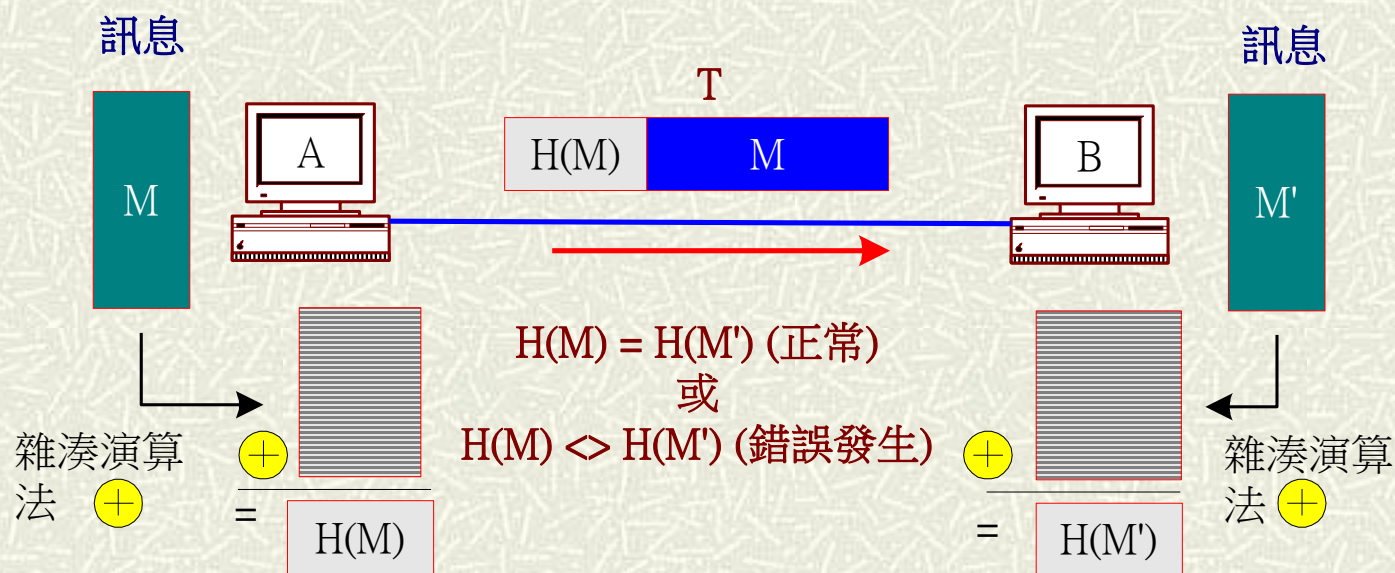
- ◆ 一種保護數位媒體著作權的機制。
- ◆ 透過將可鑑定版權的標記（密碼、文字或Logo）隱藏至被保護的資料中，使數位資料被下載使用時，仍保有這些標記。將來若發生版權爭議，誰能夠自影像中取出有效標記，誰就是合法擁有者。
- ◆ 浮水印依人類肉眼是否能夠識別，分為顯性浮水印(visible watermark)與隱性浮水印兩類(invisible watermark)

雜湊函數概念

- ◆ 雜湊值((Hash Value) $h = H(M)$
M：明文訊息 H：雜湊函數
- ◆ 對任意長度的訊息輸入(M)，產生固定長度的雜湊值輸出。
- ◆ 任何M，都有H(M)，並可經由硬體或軟體來實現。
- ◆ 『單向雜湊』(One-way Hash)之特性。
- ◆ 對於訊息 M_1 ，在計算上是無法找出另一個訊息 $M_2 \neq M_1$ ，使得 $H(M_1) = H(M_2)$ ，即抗碰撞(collision resistance)

雜湊函數概念(續)

- ◆ 若 $H(M_1) = H(M_2)$ ，則 $M_1 = M_2$ ，若 $H(M_1) \neq H(M_2)$ ，則 $M_1 \neq M_2$ 。
- ◆ 計算速度快



易於新增、修改及刪除的風險控制

◆ 管理面：

- 建立備份政策

◆ 技術面：

- 安全存取的應用系統
- 唯讀型儲存媒體
- 防火牆及入侵偵測

◆ 實體面：

- 實體隔離

電腦病毒及惡意軟體風險控制

◆ 管理面：

- 限制網路及可攜式媒體之使用。
- 建立備份政策

◆ 技術面：

- 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。
- 資料加密。

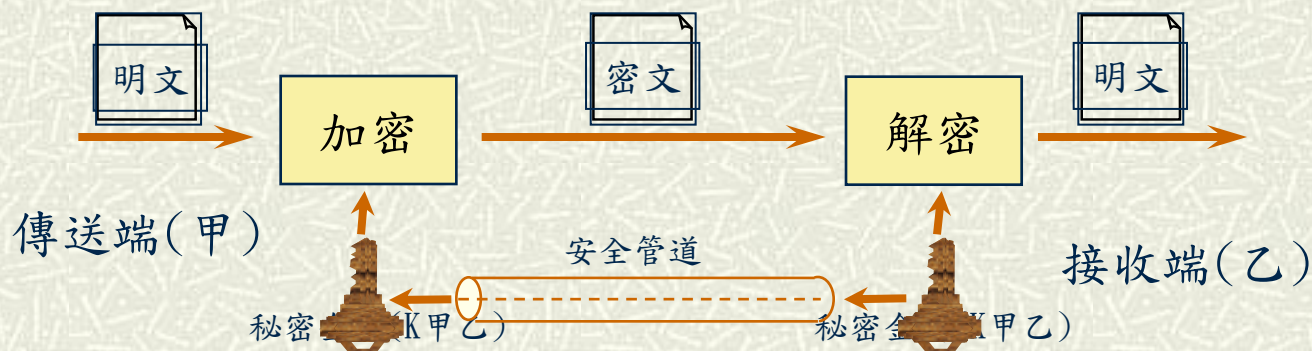
◆ 實體面：

- 實體隔離。

加密概念

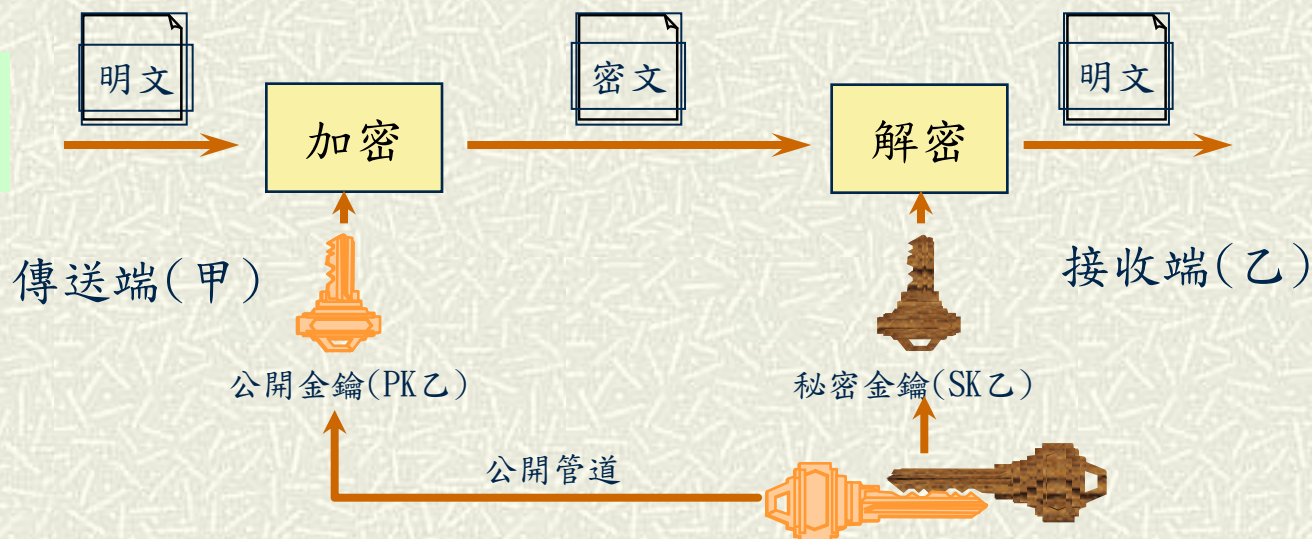
對稱性
加密法

DES
3-DES
AES



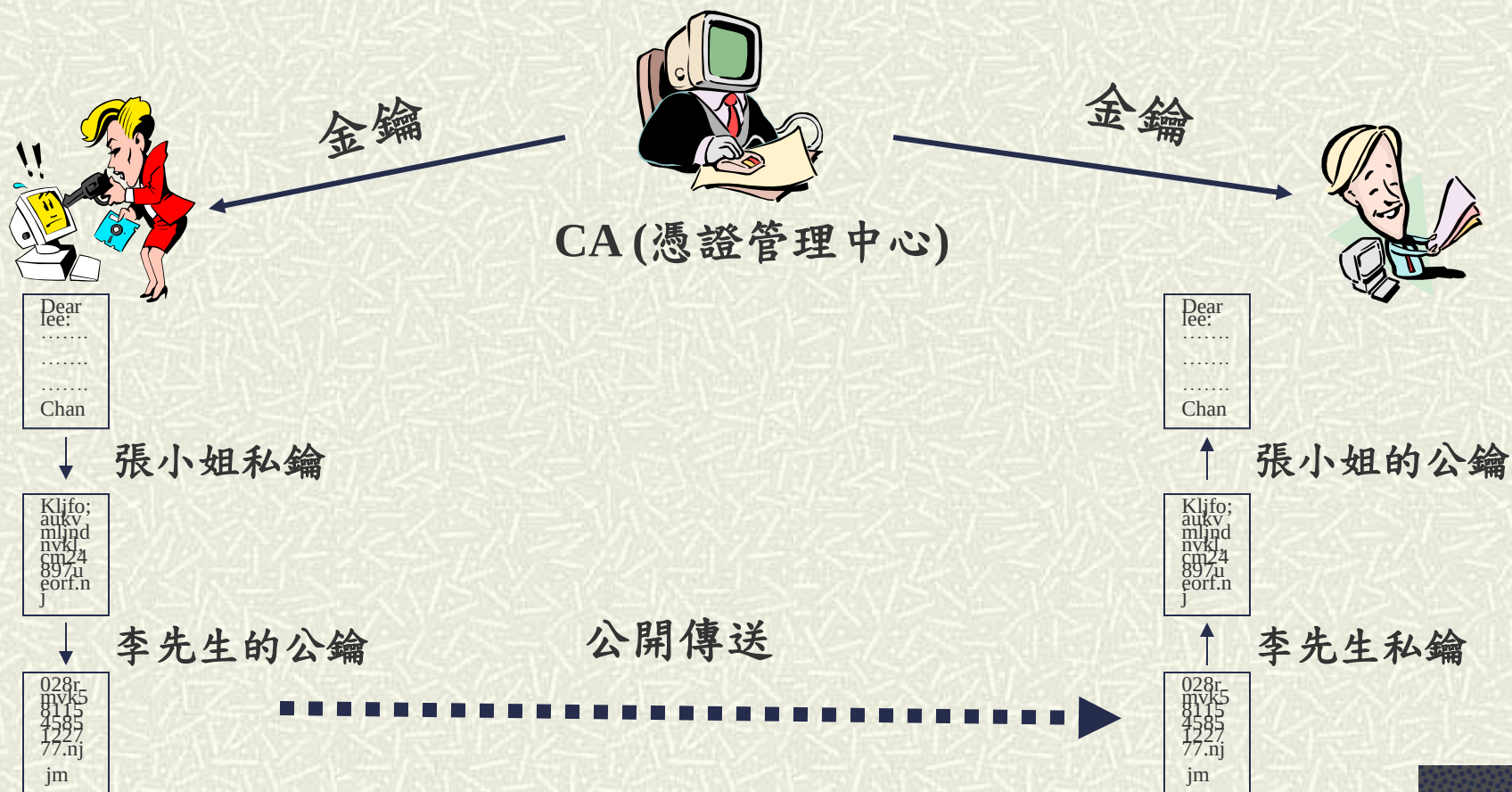
非對稱性
加密法

RSA
ECC
DL-Based



非對稱式密碼系統應用範例

❖ 張小姐寫封信給李先生



著作權保護風險控制

◆ 管理面：

- 宣導著作權法
- 法律約束

◆ 技術面：

- 加浮水印
- 電子簽章
- 數位資源管理(DRM)

◆ 實體面：

- ?

電子簽章概念

◆ 電子簽章法：

- 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。
- 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。
- 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。（為電子簽章型式之一）
- 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。
- 憑證機構：指簽發憑證之機關、法人。
- 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。（相當於身分證 + 私章，機關憑證相當於關防）

電子簽章概念(續1)

- 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。(6條1項)
- 以數位簽章簽署電子文件者，應符合下列各款規定，始生前條第一項之效力：(10條)
 - 一、使用經第十一條核定或第十五條許可之憑證機構依法簽發之憑證。
 - 二、憑證尚屬有效並未逾使用範圍。

◆ 自然人憑證：

- 內政部憑證管理中心所簽發的憑證。
- 申辦資格：只要年滿18歲(含)以上，設籍於本國之國民(即為自然人)，且未受監護宣告者。

電子簽章概念(續2)

◆ 行政院及所屬各機關公務人員電子識別證管理作業要點

- 電子識別證指依電子簽章法、公文程式條例及檔案法等法令規定，以符合政府資訊及通信安全（以下簡稱資通安全）管理法令及相關規範，且具有網路身分識別及電子簽章功能，得供公務人員製作、簽署電子文件、電子檔案或其他資通安全管理之用，而存放於安全載具之憑證。（第3點）
- 各機關應自行選用下列經濟部核定之憑證機構依法簽發之憑證，據以製作電子識別證：（第5點）
 - （一）內政部核發供自然人使用之自然人憑證。
 - （二）各機關自建之憑證機構簽發之憑證。
 - （三）前二款以外憑證機構簽發之憑證。

資料外洩風險管理

◆ 管理面：

- 建立資訊安全管理制度

◆ 技術面：

- 安全存取的應用系統
- 防火牆及入侵偵測
- 資料儲存加密及傳輸加密

◆ 實體面：

- 實體隔離

隱私權保護風險控制

◆ 管理面：

- 宣導個人資料保護法
- 加強過濾詮釋資料/檔案目錄的內容

◆ 技術面：

- 安全存取的應用系統

◆ 實體面：

- ？

長期保存及應用風險控制

◆ 管理面：

- 標準化

◆ 技術面：

- 技術鑑定
- 轉置(migration)
- 轉製(conversion)

◆ 實體面：

- 系統保存

技術鑑定概念

- ◆ 技術鑑定，指分析電子檔案保存、移轉及應用過程中，所面臨軟硬體技術問題，就管理需求及技術變遷等因應策略提出建議。（檔案保存價值鑑定規範第18點第2項）
- ◆ 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。
- ◆ 各機關辦理電子檔案之清查、技術鑑定、銷毀、移轉(交)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。

技術鑑定評估指標

- 電子檔案真實性及完整性
- 媒體之有效性
- 電子媒體種類及數量
- 電子檔案格式及數量
- 憑證簽章之安全強度
- 加密安全強度
- 雜湊值安全強度

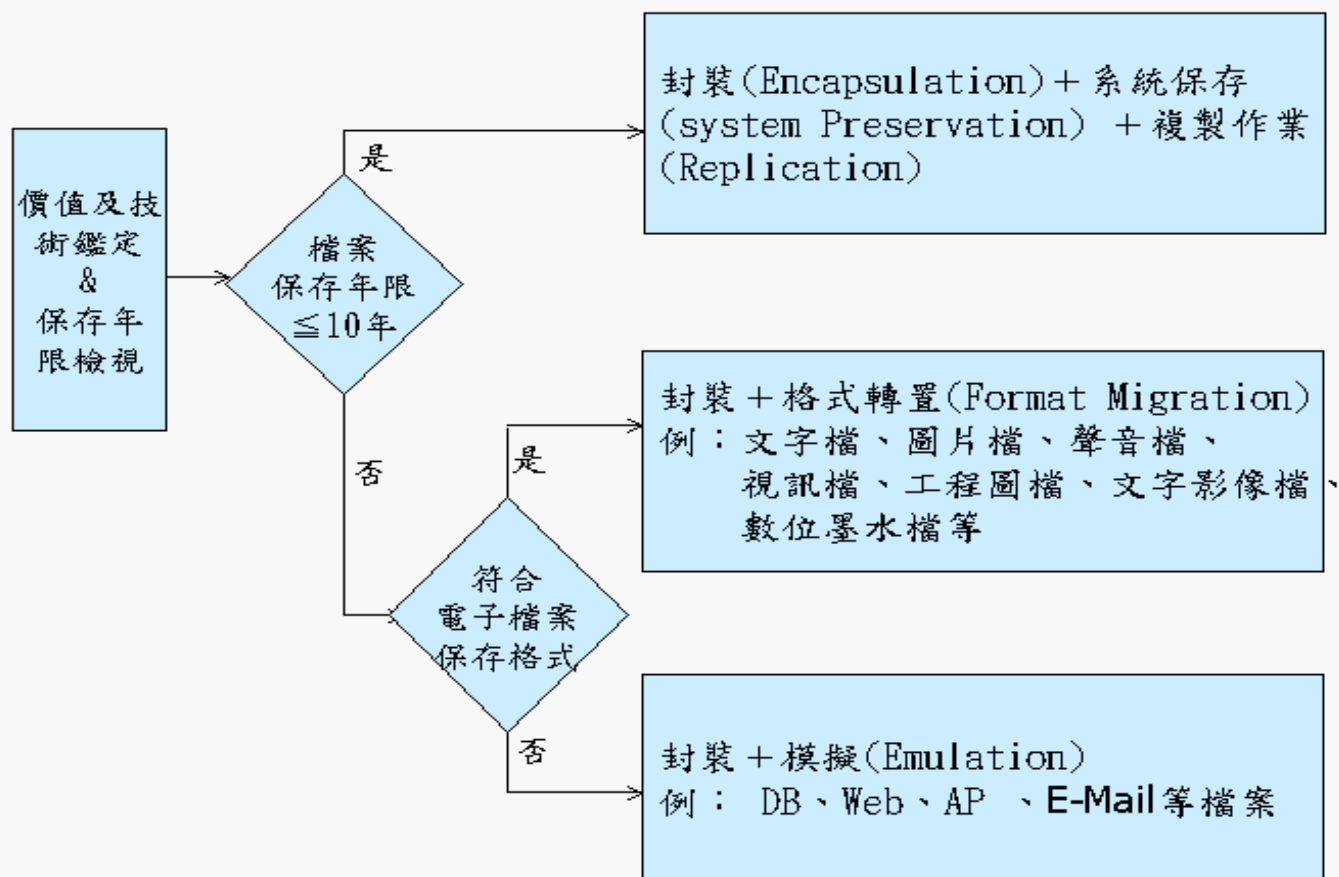
常見長期保存方法

- ◆標準化：將電子檔案格式朝向簡單化、開放式、標準化。
- ◆系統保存：將電腦軟硬體完整保留下來，類似建立電腦博物館。
- ◆複製：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。
- ◆更新：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相同儲存媒體。

常見長期保存方法(續)

- ◆ 轉置：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。
 - ▣ 公認最可行作法，惟會改變原始物件，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。
- ◆ 封裝：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。
- ◆ 模擬：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。
- ◆ 轉製：印成紙張或微縮等類比媒體。

電子檔案長期保存架構



難解的保存風險

◆ 雲端運算

- 資料無特定的儲存媒體
- 應用軟體太過複雜
- 看不見的廠商

◆ 業務委外

- 來來去去的廠商。
- 知識、經驗和機密隨廠商和其員工異動而流失/擴散。
- 無人事權，難以約束廠商員工。

微縮的優勢與劣勢

◆ 優勢

- 有足夠能力擷取紙質檔案內容。
- 已有完善的國際標準，確認使用指南及儲存環境。
- 在正確儲存與使用情況下，長期保存安全無慮。
- 可以重製、儲存、複製與分享。

◆ 劣勢

- 無彩色微縮片的國際標準。
- 類比式媒體，品質易隨著複製次數而流失。
- 不易整併至電腦系統，故功能性受限制難以強化。
- 應用不易普及。

數位化的優勢與劣勢

◆ 優勢

- 資料類型涵蓋範圍較廣，包含聲音、動畫等。
- 原版與複製品之間，無品質流失之慮。
- 確定使用標準與儲存環境相同狀況下，原版與複製品應無安全顧慮。
- 易於整併至電腦系統作業，可強化功能如檢索、縮放、列印、分析、統計。
- 利於應用，提供途徑多樣性。

◆ 劣勢

- 檔案易遭竄改而未被及時察覺。
- 使用標準與儲存環境的安全仍待努力與發展。
- 面臨長期保存議題。

未來展望

- ◆ 使電子檔案保存結果如同傳統文件般可長可久，須結合電子檔案生成之技術、生命週期與環境特性。
- ◆ 因應機關檔管人員眾多、人員替換頻繁及資訊專業認知稍嫌不足狀況下，適當的資訊科技教育平台、多元的專業技術學習機會，以及完整的電子檔案教育訓練環境。
- ◆ 暢通的國際交流管道，透過國際經驗交流及合作機會，可截長補短，減少系統開發及制度設計之摸索時間，降低失敗風險。

謝謝聆聽，敬請指教

電子檔案技術服務中心

電話：(02)2775-1580

傳真：(02)2775-1507

電子信箱：lab@archives.gov.tw