

出席 2014 年國際密碼學與安全會議及參訪記要

A Summary of the Participation in the ICCS 2014 and Visit to the National Archives of Thailand and Bank of Thailand

尤暖霞 Yu, Nuan-Hsia

國家發展委員會檔案管理局文書檔案資訊組科長

Section Chief, Information Technology Division, National Archives Administration, National Development Council

魏寶菊 Wei, Bau-Chi

國家發展委員會檔案管理局文書檔案資訊組分析師

Analyst, Information Technology Division, National Archives Administration, National Development Council

壹、前言

西元（以下同）2014 年 7 月 18 日至 20 日為汲取各國資安防護新觀念與技術，筆者代表國家發展委員會檔案管理局（以下簡稱本局）前往泰國曼谷是隆假日酒店（Holiday Inn Silom, Bangkok, Kingdom of Thailand）參加國際密碼學與安全會議（International Conference on Cryptography and Security，簡稱 ICCS），該會議係由印度科學家開發人員和教職員專業協會主辦（Association of Scientists Developers and Faculties，簡稱 ASDF），探討密碼學及加解密技術之理論與實務，如存取控制（Access Control）、生物特徵安全和隱私權（Biometrics Security and Privacy）、關鍵基礎設施保護（Critical Infrastructure Protection）、資料完整性（Data Integrity）、資料保護（Data Protection）等。透過參與該會議瞭解各國如何應用加解密技術以強化資訊系統與網路安全，俾有效提升電子化作業系統或平台之隱密性、身分識別、資料完整性及不可否認性等。

本次行程除參與上開會議外，另安排參訪泰國國家檔案館（National Archives of Thailand）及泰國銀行（Bank of Thailand）博物館、圖書館與檔案館，以認識泰國各檔案館在檔案管理上之相關作法。

貳、國際密碼學與安全會議

2014 年國際密碼學與安全會議共計有 3 場專題演講及 11 篇論文發表，其主要內容涵蓋資料保護、雲端基礎服務、數位鑑識應用、密碼學、行動裝置管理及網路安全等，發表 11 篇論文名稱及摘要臚列如表 1：

表 1 2014 年國際密碼學與安全會議發表論文摘要表

項次	名稱	摘要
1	在新的雲端基礎下，利用確保隱私權的方法，檢測可疑的洗錢案件 Toward a New Cloud-Based Approach to preserve the Privacy for Detecting Suspicious Cases of Money Laundering	<p>洗錢手法變得越來越複雜，不僅對金融機構也給國家造成嚴重威脅。因此，打擊黑金及反恐融資是穩定國家財政和國際安全的關鍵指標。基於雲端運算平台具可擴展性、高性能、易用性及提高業務連續性與營運效率之特性，越來越多的金融機構選擇雲端運算作為 IT 平台和服務的解決方案。近期從客戶端、網路傳輸、企業端調查顯示，安全性仍是雲端運算最關鍵的問題。</p> <p>本研究為確保客戶資料具機密性、完整性、可用性、鑑別性與不可否認性，採取金鑰基礎建設（Public-Key Infrastructure，簡稱 PKI）以提供線上加解密及身分鑑別技術。</p>
2	影像區塊複製移動法的最新偽造偵測方法 State-of-The-Art in Block based Copy Move Forgery Detection	<p>隨著智慧型手機等行動裝置使用之普及，數位影像存取容易，影像處理軟體功能強大，數位影像後製更容易，致修改後的圖片常無法辨識其真偽。</p> <p>常見的圖片偽造方法為影像區塊複製—移動法。偽造時機是在原始影像檔複製和貼上時完成，並套用如濾波、縮放、旋轉、JPEG 壓縮及添加雜訊等效果，使其難以檢測此影像已經過偽造。本研究係探討如何加強數位影像之安全管理機制。</p>
3	衛生保健照護體系的安全主體概念 Conception of Ontology for Security in Health Care Systems	<p>網路技術日新月異，網際網路更是無遠弗屆。近年來，資安事件層出不窮，駭客手法持續演進與翻新，令人防不勝防。衛生保健照護體系內含敏感性個人資訊，為了杜絕駭客，首先要建置一個敏銳的安全防護系統。本研究係探討透過群組套用、網格技術或分佈式文檔系統等功能，將網路中大量且不同型式的儲存裝置，透過 XML 物件格式集合起來協同運作，共同對外提供由下而上的資料儲存和業務處理功能。</p> <p>經由內容授權系統、資料加密技術等機制，確保雲端儲存的資料，不會被未經授權的使用者存取；同時，透過各種資料備份和容災措施，確保雲端儲存資料已完整性與可用性，以提升雲端儲存之安全性與穩定性。</p>
4	使用者線上資訊安全實例：以南非為例 User Online Information Security Practices: The South African Context	<p>行動裝置的使用日趨廣泛，尤其在即時通訊、電子郵件、瀏覽網頁等部分，甚或有使用者習慣將手機與電腦連結使用。這種情形，輕者網頁遭到綁架，重者系統主機遭植入木馬或後門程式，造成機密資料或個人金融資料外洩。</p> <p>本研究係以南非為例，探討用戶上網習慣，以及是否具有資訊安全防護意識。本論文採定量調查方法，分析用戶的資料，提供使用者良好的使用規範與有效的管理措施。</p>
5	安全影像機制—多碼語義的視覺密碼協議 Multi-secret Semantic Visual Cryptographic Protocol for Securing Image Communications	<p>密碼學可安全地共享視覺秘密訊息。視覺密碼方案（Visual Cryptographic，簡稱 VCS）是一種加密方法，提供組合技術進行編碼加密。本研究提出了一種基於語義的視覺密碼協議（Multi-secret Semantic Visual Cryptographic Protocol，簡稱 MSVCP），為一種新的多碼加密法，可將兩個加密影像檔重構成一個安全的加密影像檔。其方法為先移除共享影像檔的干擾，再嵌入語義影像檔，最後重建加密影像檔。所提出的新機制稱為 MSVCP，可應用在灰階影像檔處理，實驗結果證明 MSVCP 的有效性和優點，以及保證重構的加密影像檔是兼具安全性與品質的。</p>

表 1 2014 年國際密碼學與安全會議發表論文摘要表 (續)

項次	名稱	摘要
6	使用細胞自動機技術保護影像資料之正確性 Securing Image Data's Using Cellular Automata Techniques	本研究將醫院資訊系統與數位影像系統整合，用於乳腺癌的早期檢測－乳房攝影。為確保影像資料之正確性，利用細胞自動機技術，透過 322 幅緻密的乳腺攝影圖像，去除雜訊、分割胸肌提取計算、檢測微鈣化等處理，最後將所採樣的特徵輸入到細胞自動機，分類成不同的規則，再用矩陣實驗室 (Matrix Laboratory，簡稱 MATLAB) 進行分析結果，以有效提升檢測之正確性。
7	有效改善目前手寫辨識系統和檢測的方法 Sanskrit Character Recognition with Improved feed forward BPNN and LSB Matching Patterns	本研究係探討梵文文檔辨識功能，囿於手寫梵文文檔中的樣式和輔音千變萬化，因此辨識手寫字符非常困難。本文論述了離線梵文手寫字符，提出了一個新的梵文文檔辨識系統，有效改善目前手寫辨識系統和檢測方法，並有較高的精確度。
8	利用二維影像波形和遺傳基因演算法，自動鑑別可疑器官區域 Identification of Suspicious Region in Secured Stegno-Mammograms with Two Dimensional Wavelets and Genetic Operators	本研究將醫療儀器導入電腦、通訊及多媒體技術，透過醫療數據、患者器官圖像及鑑別遺傳基因演算法、傳送信號與接收信號的差異，估測人體器官的狀態，定期自動檢查患者可疑器官區域，以便於遠距診斷、遠距監測、傳輸醫療數據和紀錄。
9	透過監測網路流量，檢測和分類網際網路上的異常行為，改善網際網路蠕蟲偵測 Internet Worm Detection based on Traffic Behavior Monitoring with Improved C4.5	蠕蟲每年造成世界各地網際網路數十億美元的損失。網際網路蠕蟲是一種自含程式，能將本身功能或程式碼的一部分，散播到其他電腦系統。這種病毒通常透過網路連線或電子郵件的附件加以散播，導致許多網路安全威脅，如：分布式拒絕服務攻擊、非法網路流量、散布垃圾郵件、竊取用戶個人資料等。本研究透過監測網路流量，檢測和分類網際網路上的異常行為，使用 C4.5 機器學習分類方法，歸納出決策樹。該方法有效減少大量的輸入處理時間，得到的實驗結果，確定本功能可檢測惡意流量的未知蠕蟲，具有較高的精確度。
10	基於混合人工免疫系統的技術，檢測副本節點的攻擊 Detection of Replica Node Attack Based on Hybrid Artificial Immune System Technique	以無線傳輸為基礎的無線感測器網路 (wireless sensor network，簡稱 WSN)，提供具有移動性、動態調整感測與通訊範圍、長傳輸延遲及低移動速率等特性，常應用於跟蹤和環境監測。鑑於感測器節點無人看管，較易遭到攻擊之弱點，本研究提出於靜態網路中使用證人發現策略與集中檢測方法，以檢測節點安全性，並結合入侵檢測的實際需求，提出整合人工免疫系統 (Immunoglobulin-based Artificial Immune System，簡稱 IAIS) 機制。此方法的優點包括：增加檢出率、降低錯誤率、有效性低消耗能量。
11	經由使用無基礎架構無線網路所提出來的繞徑演算法 (Ad Hoc On-Demand Distance，簡稱 AODV) 芒特可信節點的安全數據傳輸：SATEM Secure Data Transmission through Trusted Node in Mantas using AODV Routing Algorithm: SATEM	無線隨意網路 (Wireless ad hoc network，簡稱 WANET)，是一種分散式的無線網路系統。這種網路系統是臨時形成，由節點與節點間的動態連結串成一個網路。它不需要依賴既存的網路架構，如有線系統的路由器，或無線系統的基地台。 無線網路必須符合基本的安全需求，為確保公平、安全的移動，WANET 可針對不同使用者實施多種策略組合，對行動儲存裝置進行權限設定。但因缺乏基礎設施管理，執行移動自組網路之政策是相當具有挑戰性的。本研究係建立在可信任的平台上，執行監視器的強制策略，在此機制下，每個應用程序或協議都有一個相關的政策，故此方式可使節點形成信任的應用程序中心網路。

參、泰國國家檔案館（National Archives of Thailand）

會議結束後，順道參訪泰國國家檔案館，由 Ms. Korapin Taweta 及 Ms. Varanud Vinasandhi 兩位館方人員負責接待及導覽解說（如圖 1 至圖 3）。

一、泰國檔案館簡介

泰國國家檔案館最初在 1916 年係屬曼谷國家圖書館（the library for Bangkok）的一個部

門，直到 1952 年改隸泰國文化部（the Fine Arts Department Ministry of Culture）。泰國國家檔案館的職責為依法蒐集、保管和提供研究利用政府、國有企業和私立部門所產生的文件檔案，並提供管理檔案方法和建議。泰國國家檔案館下設有行政管理處、文件管理處、檔案服務處、當代歷史文件處、國家影片檔案館、10 個檔案館分館及泰皇的紀念檔案館。

依據泰國在 1983 年頒布的檔案法及 2005 年附加的檔案規範，各政府機關檔案保存超過



圖 1 作者（左 3、右 2）與泰國國家檔案館人員合影

資料來源：作者提供



圖 2 泰國國家檔案館外觀

資料來源：作者提供



圖 3 泰國國家檔案館閱覽中心

資料來源：作者提供

30 年，就必須要移轉給國家檔案館，並由檔案評鑑委員進行檔案評選，將具有歷史及保存價值的檔案轉為國家檔案進行永久保存。

二、泰國檔案館特色

該館主要蒐集的檔案媒體形式分為紙質及影音兩大類，其中影音類包含照片、底片、錄影帶、投影片、地圖集等。泰國係屬君主立憲國家，影音類資料絕大多數跟泰國皇室活動有關，因此泰國國家檔案館最大的特色是設有泰皇的紀念檔案館（The National Archives in Commemoration of H.M. the King's Golden Jubilee），主要展示泰國皇室所有的資料。目前泰國國家檔案館保存自國王拉瑪四世開始的檔案，計有 1,839,264 筆，及影音資料 1,352,070 筆。此外，泰國國家檔案館亦販賣可供收藏的皇室照片複本（如圖 4）。

三、檔案應用與服務

該館設有閱覽中心，供研究人員查閱公開檔案，泰國公民不需任何證明即可到館利用檔案，外國人則須事先填寫相關申請表格，經過泰國國家研究委員會的批准，才能查閱。為了

避免重要的國家檔案及經常使用的原件檔案毀損，該館使用微縮影片備份館藏檔案；微縮影片亦可提供民眾公開查閱及申請複製。

四、檔案保護

筆者在參觀檔案保護技術實驗室時，泰方陪同人員特別介紹由檔案館技術人員獨門研究配製的文件去酸溶液（如圖 5、圖 6）。工作人員將變黃發脆的歷史文件放入去酸溶液中浸泡一段時間後撈出，平放到隔板上待自然風乾後裱糊。據說，這種去酸技術的效果不錯，可減緩酸性紙張文件的老化過程，延長檔案的壽命。



圖 5 檔案館工作人員進行檔案的保護作業

資料來源：作者提供



圖 4 泰國國家檔案館販售泰皇相關照片複本

資料來源：作者提供



圖 6 檔案保護膠去酸溶劑

資料來源：作者提供

五、檔管人教育訓練及電子檔案管理

泰國國家檔案館每年均針對內部人員進行 3 天的教育訓練，藉以宣導檔案是國家重要的文化資產，可增進檔案管理效率及提升檔案管理人員專業技術能力。另，針對各政府機關和學校，該館每年亦針對各機關辦理 2 次研討會，教導如何依據檔案法規管理檔案。

而因應資訊科技的進步、電子化政府的形成，此次參訪也瞭解泰國對於電子檔案管理的相關作法。在泰國，所有政府機關的文件從產生、維護到銷毀，都依照 1983 年檔案法及 2005 年增訂的檔案程序指引來處理。然而這些法規對於電子檔案的規範僅大致說明電子檔案的輸入及輸出形式，並沒有規範電子文書及檔案的格式及欄位，例如：政府檔案和文獻的分類、文件索引、文件標題、文件編號等。每個政府機關各自使用獨立的電子文書製作及檔案管理系統，加上大部分的政府部門並未將其電子文件傳送給國家檔案館，故泰國在電子檔案的管理部分顯得較為薄弱，僅能說是檔案的電子紀錄，並沒有完整的、有規範的電子檔案管理生命週期及長期保存策略。

肆、泰國銀行博物館、圖書館及檔案館

參訪泰國國家檔案館同日下午，另前往泰國銀行圖書館、檔案館及博物館進行交流。（如圖 7）

一、泰國銀行博物館

泰國銀行（以下簡稱泰銀）是泰國的中央銀行，於 1942 年成立，掌管泰國貨幣政策、維持貨幣穩定、制定外匯政策及負責泰幣印

刷、發行、管理。泰銀在 1993 年成立博物館（如下頁圖 8），博物館內有 3 種常設展，分別為泰國歷代錢幣展（如下頁圖 9）、泰銀博物館的發展史展及泰銀的角色和職責展示。另外，該博物館也不定期安排各種不同的特別展，例如：黃金貨幣展、泰銀 60 週年展及泰皇生日慶等展覽。該博物館位於 1906 年建造完成之王子殿下的居所內，在 1988 至 1991 年時進行大整修，主要改善空調系統、光源照明和火災警報系統。2002 年至 2014 年間進行過數次裝潢，讓館內的展示品更生動、有趣地吸引參觀者。在金碧輝煌的巴洛克式古蹟建築裡，展示泰國貨幣的演變，相當特別。

二、泰國銀行檔案館

1969 年泰銀邀請國際專家參與「泰國銀行文書管理改造計畫」，當時專家們建議必須設置專門的檔案管理單位負責歸檔及保存一些值得永久保存的文書，以及管理銀行所有的文書調閱、參考及引用事宜。因此，泰銀在 1974 年成立檔案管理單位，將其隸屬於泰銀管理部秘書處、負責銀行內永久保存價值文書檔



圖 7 作者（左 2、左 3）與泰國銀行接待人員合影

資料來源：作者提供



圖 8 泰國銀行博物館外觀

資料來源：作者提供



圖 9 泰國歷代錢幣展示廳

資料來源：作者提供

案的人員，改隸為圖書館檔案和博物館處。檔案徵集、處理、運用及管理的主要遵循法規為泰銀內部檔案管理規則、泰國檔案法及泰國資訊法。

泰銀的檔案管理單位負責將銀行所有的文書紀錄、活動資料進行分析及評鑑，挑選出具有獨特性、證據價值及資訊價值等值得永久保

存之資料。檔案蒐集的主要來源為泰銀內部各局、處、室等單位，以及銀行員工個人捐贈與銀行有關的活動資料。泰銀檔管單位依檔案原始次序和出處進行分類和編目作業（archival cataloging），並由檔管人員進行檔案內容描述（包含實際位置、檔案、資料夾資訊、摘要和搜尋關鍵字等），俾使檔案查詢工具快速地查找檔案。由於泰銀所保存的檔案均屬重要且有價值的資料，其檔案管理單位也針對檔案庫房採行相關管理措施，包括適當的空調環境、溫溼度控制、光源監控等，以確保檔案受到良好的保護及保存。另外，泰國銀行的檔案館位於昭披耶河（Chao Phraya River）旁，在參訪過程中，泰銀特別說明他們在空間樓層的規劃設計，將欲銷毀的檔案放置於低樓層，若日後不幸遇到水災也毋需擔心，因為剛好符合用水銷



圖 10 檔案庫房

資料來源：作者提供



圖 11 檔案文卷依序編目，放入檔案盒

資料來源：作者提供



圖 12 照片及大圖檔案專門保存盒

資料來源：作者提供



毀的方式！

筆者也參觀泰銀的檔案庫房設施，瞭解其檔案保存實際作法（如圖 10 至圖 13）。泰銀檔案館目前保存的檔案約 100,000 筆，主要內容有泰銀從過去到現在主要業務和任務的發展歷史、相關董事會會議紀要、手稿文書、活頁資料、藍圖、圖表、影印資料、照片底片、投影膠片和數位紀錄等，目前由文件管理處（Records Management Team）負責管理。泰銀為保存這批珍貴檔案瑰寶，執行數位典藏計畫，轉換為數位檔案的型式以延續檔案的生命週期。



圖 13 待銷毀檔案儲存區

資料來源：作者提供

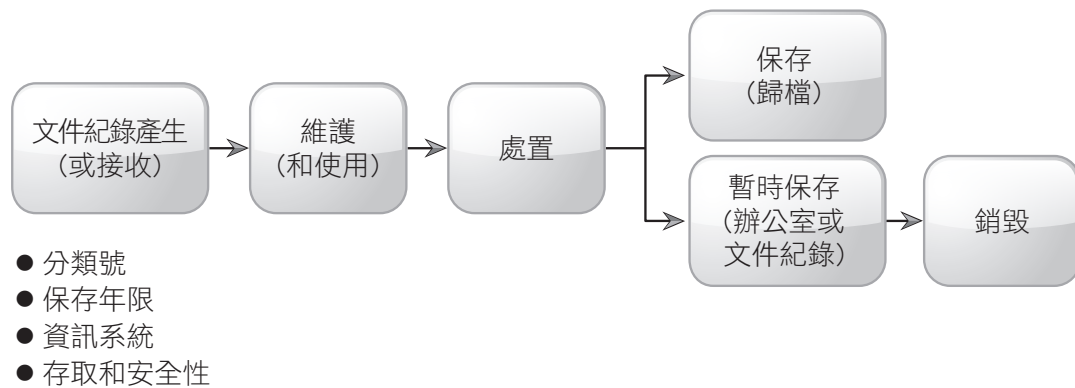


圖 14 泰國銀行的文件紀錄政策處理程序

資料來源：作者繪製

此外，泰銀於 2007 年制定內部文件紀錄管理政策，依照業務性質，訂定文件紀錄的分類及保存年限，規定所有泰銀的文件紀錄原則上都要公開，除非因特殊的豁免權限制或國家法規規定禁止公開。泰銀訂定此管理政策之目的，為提供泰銀內部產製文件紀錄的規範，以確保所有銀行的企業活動紀錄均有依照規定之程序製作、維護、存取和處置。文件記錄政策和處理程序如圖 14。泰銀和各國的金融業一樣，使用大量的資訊設備，電子化程度較泰國其他機關高出許多。雖然泰國國家檔案館並不像我國有制定文書及檔案管理電腦化作業規範，開發共通文編系統供各級機關使用，但泰銀在 2008 年也依據其內部文件紀錄管理政策，並遵循電子檔案的國際標準，開發企業用的文件紀錄管理資訊系統。此系統的主要功能有建立電子檔案、查詢及調閱檔案、管控存取權限及銷毀處置檔案。未來這套系統上線運作後，能降低泰銀同仁的紙張使用量，達到節能減紙之目的。

三、泰國銀行圖書館

泰銀的檔案館及圖書館屬同一個部門，因此，當日筆者也參觀了泰銀的圖書館總館。該圖書館主要提供有關經濟、金融、泰國銀行的相關資訊（含出版品）及世界各國中央銀行的資訊。目前共有 3 個分館，總館考量讀者需求的不同，規劃設計分為 2 區，1 區為交談討論區，為讓讀者可輕鬆閱讀交談，因此還有販賣書籍及咖啡（如圖 15）。另有專業閱覽區，提供電腦設備查詢書目資料及安靜舒適的閱覽空



圖 15 泰國銀行圖書館販售部

資料來源：作者提供

間（如圖 16、圖 17），並提供視聽專區，供讀者閱覽影音資料。雖然只是銀行所屬的圖書館，還貼心的建置自助還書系統，讓人覺得泰國銀行的圖書館規劃的非常專業。

伍、結語

透過此次參與國際性會議與國際資安界之交流機會，首次將我國電子檔案管理重要發展成果及實務經驗與各國專家學者交流分享，俾拓展未來合作發展與互訪之可行性，也藉此提升能見度。謹就此次與會及參訪所得，對於我國文書電子檔案管理工作發展建議如下：

一、持續發展電子檔案管理技術，成為創新領導者

本次研討會有多項議題探討電子檔案管理工作，包括應用雲端技術、金鑰基礎建設、無線傳輸、密碼學、資安防護、數位影像真偽辨識及電子檔案管理等，多數仍處於問題探討或實驗性質階段。自 2002 年檔案法施行以來，本局即積極推動各機關檔案管理資訊化作業，並成立電子檔案長期保存實驗室，對於原生性電子檔案之長期保存及媒體轉置等功能，投入研

發及導入工作。較之泰國，我國在電子檔案管理作業發展較具優勢，建議應持續發展電子檔案管理技術，並導入實務管理流程，藉由技術研發與實務運作之相輔相成，逐步朝雲端服務架構演化，並結合行動化、開放資料等趨勢，發展電子檔案創新管理的政策及規範，以協助我國推行電子檔案管理政策。

二、提升網路安全管理機制，強化資安防護能力

資訊安全與密碼學隨著網際網路、全球貿易及金融活動而日益緊密，結合行動裝置及社交工程的詐騙手法，易造成病毒感染、機密資料外洩、阻斷服務或駭客入侵等事件。本研討會有多篇論文介紹許多密碼學改良模型，透過演算法、漏洞攻擊、滲透測試等方法，加強原有模型之加解密功能，並提升原密碼模型演算效率。為了防範日新月異的資安事件，建議應建置一套敏銳的資安防護系統，如：網路防火牆、網路入侵防禦系統、一次性密碼（One Time Password，簡稱 OTP）身分驗證加密機制、電子郵件進階持續性滲透攻擊（Advanced Persistent Threat，簡稱 APT）防禦系統、側錄系



圖 16 泰國銀行圖書館電腦查詢及圖書區

資料來源：作者提供



圖 17 泰國銀行圖書館閱覽區

資料來源：作者提供

統及防毒軟體等設施，俾確保機關資訊系統的安全。

三、運用政府雲端基礎服務，共享電子文書檔案資訊

雲端運算使政府資訊進入共享時代，整合政府現有資訊服務資源及架構，可彈性擴充服務量能之政府雲端基礎服務，並提供資訊安全防護、運算資源等，以協助政府組織共享資訊資源，創造更多企業競爭優勢及降低行政成本。電子文書檔案之發展亦應朝此一方向推展，運用電子化政府雲端服務基礎建設，提供文書編輯製作與公文線上簽核、電子檔案封裝及瀏覽工具的軟體服務，並分散公文電子交換、檔案目錄彙送、備份處理作業，以提升跨平台、跨瀏覽器之服務效能。未來希藉由政府雲端基礎服務之發展，提供彈性靈活之電子文書檔案基礎架構，作為機關發展創新服務之基磐。

四、持續關注國外電子檔案開放與隱私保護議題

網路不僅帶動教育、醫療、商業交易型態的全球化，也進入開放資料（open data）

時代。近來各國興起「政府開放資料」的風潮，透過政府開放資料的措施，可統一各機關資料數位化格式、建立聯合目錄，並採取開放格式，以利電子檔案長期保存與使用。另一方面，實施政府開放資料之政策，不免涉及個人資料保護的問題。在推動政府開放資料時，因舊資料內含無法切割之機敏資料、個資資料、智慧財產，造成諸多檔案開放困難；故，政府開放資料時，宜請個人資料保護之專家，擔任開放資料政策執行的管理者，俾於各階段皆能針對隱私保護有周全的防護機制，有效進行政府開放資料。

五、強化合作關係，善用多方資源

為提升我國電子檔案長期保存規劃研究的質與量，以及協助機關解決電子檔案長期保存可能面臨的存取與應用問題，政府必須建立前瞻性與系統化的電子檔案長期保存架構，並多方汲取國外政府電子檔案管理新興技術與發展相關技術、法規與經驗，並透過國際經驗交流、互訪、研討及合作機會，協助我國電子檔案管理的規劃與落實，並提升電子檔案技術中心服務能量，以彰顯我國電子檔案管理技術，增加國際曝光機會。