出席 2015 年國際資訊安全與加密技術研討會暨參訪紀要

A Summary of the Participation in the 2015 International Conference on Information Security and Cryptology and Onsite Visit

邱菊梅 Chiu, Chu-Mei
國家發展委員會檔案管理局文書檔案資訊組組長
Director, Information Technology Division, National Archives Administration, National Development Council

徐綉茹 Hsu, Hsiu-Ju
國家發展委員會檔案管理局文書檔案資訊組分析師
System Analyst, Information Technology Division, National Archives Administration, National Development Council

壹、前言

2015 年國際資訊安全與加密技術研討會議（ International Conference on Information Security and Cryptology，簡稱 ICISC）於西元（以下同）2015 年 5 月 28 日、29 日舉行，由 World Academy of Science Engineering and Technology（簡稱 WASET）主辦，會議地點安排於日本成田機場附近之東武飯店。議程公布於該研討會官網（https://www.waset.org/conference/2015/05/tokyo/ICISC），該研討會旨在匯集資訊安全和密碼學等相關學術領域的研究成果，提供跨學科論壇，進行意見交流及經驗分享，與會者包括研究人員、從業人員以及教育工作者，討論課題包括最新創新技術、趨勢、關注議題、面臨的實際挑戰，以及資訊安全與密碼學領域解決方案等。

基於我國電子化政府推動成果，使得各機關、學校、公司行號、組織團體，莫不依賴公文電子交換系統進行公文書傳遞交換，以加速交換時效並提升行政效率，該系統業經行政院於 2014 年列為國家關鍵基礎設施資訊系統之一。由於資訊科技發展迅速，駭客攻擊行為變本加厲，處於敵暗我明之際，除了加強防禦措施，更應參與國際相關事務，以瞭解相關領域之研究發展，汲取經驗與知識，以提升本局整體資訊安全的防護能量。

此次國家發展委員會檔案管理局（以下簡稱本局）指派筆者參與 ICISC 研討會議，瞭解最新的資訊安全技術、應用以及發展方向，除藉以來強化改善資訊系統及網路安全，希能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，並能有助於擴展本局同仁的國際視野，俾應用於資訊安全業務。另藉本次研討會之便，特別安排於研討會前一天，前往日本國立公文書館參訪。距離上一次本局派員前往參訪已逾 10 年，藉由本次的訪視瞭解該館近年來的發展及運作現況。

貳、ICISC 研討會重點

本次研討會的主題，依據主辦單位 WASET 官網公布資訊，包含存取控制與稽核（Access Control & Audit）、生物識別技術（Biometrics）、雲端計算安全（Cloud Computing Security）、密碼分析（Cryptanalysis）、數位取證（Digital Forensics）、分散式系統安全（Distributed Systems Security）、電子商務（Electronic Commerce）、同態加密（Homomorphic Encryption）、個人身分為基礎的密碼系統（ID-based Cryptography）、入侵偵測和預防（Intrusion Detection and Prevention）、行動安全（Mobile Security）、公開金鑰加密系統（Public Key Cryptography）、安全管理（Security Management）、旁路攻擊和防禦（Side Channel Attacks and Countermeasures）、社會網絡安全（Social Network Security）、身分驗證和授權（Authentication and Authorization）、資料區段加密法和資料流加密法（Block and Stream Ciphers）、版權保護（Copyright Protection）、加密協議（Cryptographic Protocol）、數位簽章（Digital Signature）、有效建置（Efficient Imple-mentation）、雜湊函數（Hash Function）、身分管理（Identity Management）、資訊隱藏（Infor-mation Hiding）、金鑰管理（Key Management）、隱私強化（Privacy Enhancement）、多方計算安全（Secure Multiparty Computation）、安全政策（Security Policy）、智慧型設施安全（Smart Device Security）及軟體安全（Software Security）等。

赴研討會現場方得知本研討會實為跨多個學術領域的研討會，其涵蓋層面極為廣泛，並不侷限於資訊安全及密碼學領域，尚涵括教育發展、物理力學、公共衛生、健康照護、地理地質、天災地震海嘯、組織領導與角色、任務績效、組織管理、文化資產、政經旅遊、金融危機、證券交易及電子商務等包羅萬象的議題，計有 354 篇的學術論文發表，其中 1 篇為專題演講，253 篇口頭發表，100 篇海報發表；2 天的會議，每天都分別於 3 個會場同時進行（議程如下頁表 1）；另，可能礙於場地之限，大會將海報發表調整為 5 分鐘的口頭發表，因此，許多的海報發表者皆缺席。而現場並無論文以海報形式發表，會場實際發表篇數共計 175 篇（部分作者發表 2 篇論文）。根據大會的簽到紀錄，本次研討會參與者共計有 173 人次（相關照片如下下頁圖 1 至圖 4）。

茲將本次研討會與資訊系統、資訊安全、密碼學等相關論文之概要說明如下：

一、以雲端為基礎的企業資源規劃系統效能分析研究（A Performance Analysis Study for Cloud Based ERP Systems）

製造業與服務機構都需使用企業資源規劃（Enterprise Resource Planning，簡稱 ERP）系統整合許多業務功能，如：從採購到倉儲、生產計畫到成本計算等。使用資訊整合的 ERP 系統有助於公司瞭解其獲利能力、生產力及效率方面的顯著優勢。邇來資通訊科技最顯著的變化之一算是雲端運算，所謂雲端運算意識著更大的儲存區域、更能節省成本且更快地資料傳輸速率。此外，透過各種效能標準以檢驗分析雲端環境 ERP 系統效能，比較傳統與雲端 ERP 系統之間差異，可以發現許多新的商業模式、新的研究領域以及實務上可行的解決方案，未來仍可持續探討 ERP 系統的

表 1　研討會議程表

廳別	A 廳	B 廳	C 廳
日期	2015 年 5 月 28 日		
第 1 節時間	8:00-10:20	8:00-10:00	8:00-10:15
主持人	Isaac Gbadura Adanlawo, Asiha Muhammad Gadanya	Tung Liang Liao, Mei-Chu Ke, Chiung-Yao Huang	Sunantha Teyarachakul, Alan Lin
論文篇數	17	11	10
第 2 節時間	10:35-13:30	10:15-13:30	10:30-13:30
主持人	Md Kamal Uddin, Ni Yang	Zaimal Abu Zarim, A.K.M. Ahasanul Haque	Md Mizanur Rahman, Rong Liu
論文篇數	17	16	17
日期	2015 年 5 月 29 日		
第 1 節時間	8:00-10:30	8:00-10:30	8:00-10:00
主持人	Chien Chon Chen, Yi-Feng Lin	Gu Pang, Tai Mei Kin	Chun-Chuan Yang, Vadim Vagin
論文篇數	14	12	10
第 2 節時間	10:45-13:30	10:45-13:30	10:15-13:30
主持人	Ruichong Zhang, Ashok Tejankar	Celia Barreto Carvalho, Sung-Chun Tsai	Ahmad Termini, Mohd Md Noorani
論文篇數	13	19	19

資料來源：作者整理

改造工程。

二、以蟻群優化演算法建構評估軟體（Software Assessment Using Ant Colony Optimization Algorithm）

近年來，隨著軟體產業機構蓬勃發展，軟體之品質優劣亦成為產業界的重要課題。因為，許多的機構都無法保證其產品的品質，徒增使用者許多的不確定性。確保品質做法之一，就是進行軟體驗證，意即品質的量測必須於軟體完成製作發版前進行驗證。透過軟體模型與產品驗證的品質保證策略，以解決軟體評估的問題，理想模式就是要改善緊湊度與模型的模糊規則，經由蟻群優化演算法（Ant Colony Optimization，簡稱 ACO）[註 1] 之使用，可以試圖從傳統單一規則的詮釋，找到良好的組合規則。以案例研究測試，結果顯示該模型在真實環境之可行性與實用性。

三、用以發掘 IPv6 芳鄰設備之輕量加密定址模式（Lightweight Cryptographically Generated Address for IPv6 Neighbor Discovery）

受限於第 4 版網際網路協議（Internet Protocol version 4，簡稱 IPv4）的功能，有必要開發下一代的網際網路協議（Internet Protocol next generation，簡稱 IPng）以面對新的挑戰。IPng 亦稱之為第 6 版網際網路協議（IPv6），係應用發掘芳鄰協議（Neighbor Discovery Protocol，簡稱 NDP）執行地址自動配置、發掘路由器（Router Discovery，簡稱 RD）與發掘芳鄰（Neighbor

圖 1　研討會會議資料

資料來源：作者提供

圖 2　研討會場外長廊及廳別指示標幟

資料來源：作者提供

圖 3　研討會議中

資料來源：作者提供

圖 4　Keynote speech

資料來源：作者提供

Discovery，簡稱 ND）。此外，NDP 也扮演重定向服務的角色，以檢測重複的地址，並檢測無法完成的服務。儘管假設 NDP 存在聯繫信任的節點，但有些關鍵的攻擊可能會影響協議。因此，網際網路工程團隊（Internet Engineering Task Force，簡稱 IETF）建議確認可靠的發掘芳鄰協議（Secure Neighbor Discovery Protocol，簡稱 SEND）以解決 NDP 的安全問題。SEND 主要用於驗證地址的權利、惡意反應的抑制技術及最終路由器的認證程序。有關這些任務的常態運作，SEND 採用了加密定址（Cryptographically Generated Address，簡稱 CGA）、RSA 簽章與時間戳記（Timestamp）等選項，惟 CGA 最大的缺點就是可能會產生額外的高成本。

四、應用協同式日誌基礎即時偵測應用層阻斷服務攻擊之入侵偵測系統（Real Time Detection of Application Layer DDoS Attack Using Log Based Collaborative Intrusion Detection System）

近年來，網路與重要基礎設施的攻擊暴行不斷地上演且持續進行中。由於易於以低價獲取大量的殭屍網路電腦，加上

和普遍缺乏防禦作為，致使分散式拒絕服務（Distributed Denial of Service，簡稱DDoS）是最普遍且最容易的攻擊行為。應用層DDoS攻擊為DDoS的攻擊模式之一，其攻擊目標為網站伺器（Web Server）、應用系統伺服器（Application Server）或資料庫伺服器（Database Server），這類型攻擊更具複雜和挑戰性。在面對複雜、多面且同步的攻擊，安全系統的慣用技術漸漸缺乏有效性。為了克服這些議題，提出了協同入侵偵測系統（Collaborative Intrusion Detection System，簡稱CIDS），當單一設備不足以偵測本身的惡意威脅時，就需多重網路設備共享有價值的資訊，以辨識外來的攻擊行為，因此，CIDS有助於分析來自不同來源的蒐集資訊，並採取應有的決定。這種新穎的攻擊偵測技術有助於偵測關鍵基礎設施的可用性，並提出解決方案，應可於事件發生初期讓相關團隊可偵測到DDoS攻擊，並對攻擊採取反應對策，以確保服務的正常運行而不受影響。實驗評估顯示，該協同偵測方法比以前的單兵作戰方法更為有效率。

五、混合雲機密資源的新安全措施（New Security Approach of Confidential Resources in Hybrid Clouds）

目前企業變得愈來愈需要雲端環境，這種新技術提供了在任何地方、任何時間都可存取資料的機會，為資源優化與安全存取，給予儲存在平台中的資料更具安全性，有些企業不信任雲端服務供應商（Cloud Providers），據其觀點，認為雲端服務供應商可以存取並修改其機密資料，如：銀行帳戶。雲端服務供應商也意識到了這些狀況，因此採用加密方法確保資料的機密性，用以加強供應商的服務品質及提高客戶的信任。

六、網路實體系統的防偽挑戰（Challenges in Anti-Counterfeiting of Cyber-Physical Systems）

本文分析在網路實體系統（Cyber Physical Systems，簡稱CPS）的保護，CPS是一種結合電腦運算、感測器和趨動器裝置的整合控制系統，其主要特徵意味著網際網路系統元件（components），可以適應使用者與其環境的需要。CPS具備了保護對抗反偽冒、技術訣竅損失及操作等全新、特定的需求，因為盜版攻擊更加多樣化，系統保護的要求就更高了，例如：首先，必須先辨識越來越多的介面或穿越網際網路的能力，下一步則是要符合應有的保護措施。本文對介於選擇措施瞭解與最初結果呈現之間，都已獲得有效性的比較。

七、網路恐怖主義對國家安全潛在威脅之理論框架（The Potential Threat of Cyberterrorism to the National Security: Theoretical Framework）

電腦與網路革命可能出現革命性的恐怖主義，同樣地也帶來了生活上的各項改變。於現代化的科技時代，每個國家都面臨著一系列新的安全挑戰，因為許多國家和潛在對手都有能力與潛力，發動網路攻擊。有些正在部署監視、蒐集、分析技術資訊，以及繪製對手的網路、節點及基礎設施，而這些都可能運用在未來的攻擊衝突之中。為了瞭解網路恐怖威脅，透過定量研究（調查）結果驗證理論框架的有效性。此理論框架有助於深入瞭解新的數

位恐怖威脅手法；對於關鍵基礎設施的管理者及技術人員而言，可能是一份實用指引，藉以瞭解並評估所面臨的威脅，甚至可能成為建立國家策略的基礎，以因應日漸盛行的網路恐怖主義。本研究方法是先進行資料清理、可靠性分析、探索性因素分析（Exploratory Factor Analysis，簡稱 EFA）及驗證性因素分析（Confirmatory Factor Analysis，簡稱 CFA），再以結構方程模式（Structural Equation Modelling，簡稱 SEM）檢驗理論模型，並評估該模型與所蒐集資料集之間的整體適配度。

八、電子護照身分驗證協議的 BAN 邏輯驗證（BAN Logic Proof of E-passport Authentication Protocol E-Passport）

電子護照是一個相對較新的電子文件，它保持了護照功能，並提供更好的安全性，所運用的新技術，如：生物識別與射頻識別（Radio Frequency Identification，簡稱 RFID）。國際民用航空組織（The International Civil Aviation Organization，簡稱 ICAO）與歐洲聯盟定義的機制及協議，以提供安全，惟其解決方案仍存有許多威脅。在本文中，提出一個新的機制，以強化電子護照的安全性及認證過程，該新協議是以橢圓曲線、身分加密及實體之間秘密共享為基礎。在驗證方面的貢獻就是以 BAN 邏輯（BAN-Logic）驗證持有電子護照者與服務提供者在通訊過程中，達成鑑別效果及所建立交談金鑰（session key）的正確性，以提供一個更安全的資料儲存與認證機制。

九、物聯網虛擬平台事件資訊系統設計（Design of Incident Information System in IoT Virtualization Platform）

以事件資訊系統為基礎而提出的物聯網（Internet of Things，簡稱 IoT）虛擬化平台（Virtualization Platform），是為了蒐集 IoT 資訊環境的各式資料而開發的平台，優點是在管理區域易於散佈 IoT 設備，便於分析從各地收集而得的資料；此外，也提供感測資料的事件資訊，並提供相同的輸入 / 輸出介面，如：UNIX 和 Linux 搭配於 IoT 設備的檔案系統目錄。因此，不僅可以應用在事件資訊，也可應用於不同的平台。本文提出的事件資訊系統，就是要即時識別緊急事項及提供各種可視覺化的資料。

十、公共網站利用數位資料作為可鑑別的資訊隱藏新方法（A New Authenticable Steganographic Method via the Use of Numeric Data on Public Websites ）

經由公共網站數位資料之使用，提出一個具有自我鑑別能力的全新的資訊隱藏（Steganographic）方法[註 2]，此項技術是根據 Shamir 提出的秘密分享系統（Secret Sharing Scheme），將秘密訊息轉換成部分分享（Partial Shares），目的在於兼顧安全性及方便性。秘密分享系統的基本概念是將一個主金鑰 K 拆成 N 份子金鑰（K,N），本文即基於前述原理，將 Shamir（K,N）概念衍生運用於確保網站數位資料的安全性。

十一、發展支援物流安全之智慧型多重追蹤引擎系統（Development of Intelligent Smart Multi Tracking Agent System to Support of Logistics Safety）

邇來，使用 GPS 與無線通信技術以確定貨物位置訊息，愈來愈普及且方便。IoT 技術與追蹤系統的發展，在所有的行業與

社會環境中，使我們能夠確認現場狀況，也使我們能夠運用資訊技術（Information Technologies，簡稱 IT）於物流追蹤管理。惟礙於及時位置資訊的辨識難度及系統追蹤功能較簡單，致使該系統之使用仍有諸多限制。全球化的相關物流追蹤系統仍有待進一步的研究，以解決前述問題。另一方面，本文提出設計開發以 IoT 與即時定位系統（Real Time Location Systems， 簡稱 RTLS）為基礎的智慧型多重追蹤引擎系統，使得相關的物流運輸更為安全、精確及可靠。

十二、採用瀑布模型開發具有成本效益方法的中型企業軟體（A Cost Effective Approach to Develop Mid-Size Enterprise Software Adopted the Waterfall Model）

中小企業講究有限經費與工作時程，都是軟體工程師設計和開發資訊資源管理軟體的挑戰。因此，本文特就瀑布模型（Waterfall Model）加以介紹，該模型為軟體發展生命週期（Software Development Life Cycles，簡稱 SDLC）的一環，就是以成本效益方法來設計中型企業軟體。為了實現研究目標，作者們開發了一個名為「BSK管理系統」的軟體，以幫助企業軟體客戶的資訊資源管理，並執行複雜的組織任務。應用瀑布模型的各階段，可確保所有的功能符合使用者需求、策略目標及達成目標。又導入豐富的畫面、結構化英語和資料字典，並以工程方式進行適度的調查。該系統的功能界面簡單、易於操作與維護、處理快速及交易具可靠性與準確性。

參、日本國立公文書館參訪紀要

得本次研討會之便，特別安排於研討會前一天，前往日本國立公文書館參訪。該館係日本總理府附屬機關，於 2001 年改制為獨立行政法人。該館位於東京都千代區北之丸公園 3-2（該館網址 http://www.archives.go.jp），源起於 1971 年 7 月 1 日合併內閣文庫，設立國立公文書館為總理府附屬機關，1998年設置筑波分館，2001 年 4 月 1 日改制行政法人化（隸屬內閣府管轄）。2001 年 11 月 30 日設置亞洲歷史資料中心，將國立公文書館、外交省外交史料館及防衛省防衛研究所戰史研究中心收藏之近代、現代日本和亞洲各國等關係之原始資料（檔案）進行數位化，並將資料庫（http://www.jacar.go.jp/）以網際網路方式公開給國內、外使用者。

本次參訪行程，首先拜會國立公文書館次長佐佐木奈佳先生，並贈送本局電子檔案服務中心紀念品；接著進行座談會，委請臺北駐日本經濟文化代表處政務組徐副組長鼎昌擔任翻譯工作；實地導覽由岡本詩子小姐帶領及解說，徐副組長鼎昌亦全程陪同翻譯。由於時間有限，且該館可提供參訪或拍照的區域不多，僅實地參觀 2 樓閱覽室及 1 樓展覽空間，其他空間如編目作業區、檔案修復室、典藏庫房及數位化作業環境均未提供參觀。展覽區設於 1 樓，面積不大，目測約為本局 1 樓展覽廳的三分之一，以回字型設計展覽空間，展覽設施極樸實，僅見將文書影印複製品以櫥窗及裱掛方式展出，未見任何電腦型式的線上主題展或其他形式的輔助展具。1 樓展區可攝影但禁用閃光燈。其鎮館之寶為大日本帝國憲法及二次世界大戰終戰後 70 年之終戰詔書特別展（參訪相關照片如下頁圖 5 至圖 8）。

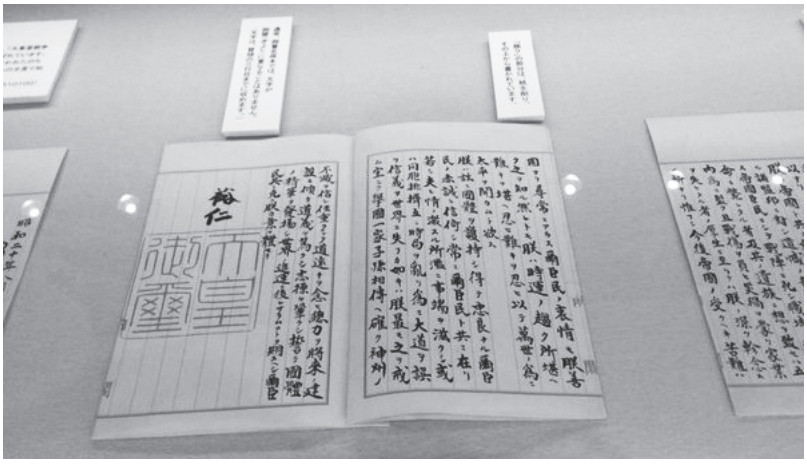

圖 5　日本國立公文書館展件 (終戰的詔書)

資料來源：作者提供

圖 6　日本國立公文書館外觀

資料來源：日本國立公文書館網站

圖 7　作者（左 2、左 3）與國立公文書館參與人員合影

資料來源：作者提供

圖 8　閱覽室

資料來源：作者提供

肆、心得分享及建議

繼 2014 年在泰國舉辦之密碼學與安全國際年會，今（2015）年在日本的年會，為本局持續 2 年派員參加之國際年會，與前屆同仁參與研討會經驗相較，今年所探討資訊安全、密碼學相關之雲端運算安全、行動裝置管理、數位鑑識應用、網路安全及電子檔案管理等相關議題，相對少了一些。本次研討會並非專屬資訊安全與密碼學之單一性質研討會，而是綜合各領域研究成果的發表會，其議題範疇甚為廣泛，前述研討會重點已說明，不再贅述。此外，經由本次參加研討會發現，部分國家的研究議題，多著墨於中國大陸，如「中國遊客在曼谷的旅遊購物行為」、「文化距離的影響和對外國直接投資選擇的制度：以土耳其和中國為證據」。而在日本參訪與研討會期間，無論於電車、街道商店或研討會場飯店，處處可見許多簡體字，較之筆者 10 年前日本行，非日語行不通的景象，顯有極大差異，足見中國大陸之崛起，身處臺灣之中華民國，絕不能輕忽。謹以本次參訪日本國立公文書館及參與國際研討會經驗，提出相關心得與建議。

一、應持續參與相關國際會議

隨著資訊科技不斷躍進，資訊人員應學習的領域與知識日增，所謂不進則退，因此必須經常接觸相關的研究發展，藉由參與國際研討會，堪稱與國際接軌、吸取新知與技術的絕佳管道。在本次研討會發現，其實國內學術研究機構也有很多的研究，值得我們進一步瞭解，並可探討學術與政府部門是否有合作機會。縱使本次國際研討會所發表之論文，與原定密碼學相關議題之論文篇數較少，惟藉由其他主題論文之參與，還是有預期之外的收穫。過往本局亦主辦多次電子檔案管理相關議題之研討會，在整體經費有限情況下，本局也可考量邀請國內外學術機構或實務機關之專家學者，召開小型研討會，讓參與者得以充分討論、暢所表達觀點與論述，無需每次都以廣邀機關派員方式辦理，不僅可大幅縮減經費支出，又能獲得較具體的研討成果，或許對於非本國的出席者（觀眾），可考量採適度的收費機制。

二、參訪國外機關仍屬必要

雖然本次參訪日本國立公文書館未能進入該館典藏庫房或看到核心作業區域，惟從其展廳及閱覽室樸實無華、整齊清潔的佈置，略可窺見該機構（目前為法人化機構）之嚴謹。所到之處、所見之人均為輕聲細語。經由本次的拜訪，結識該館亞洲歷史資料中心資料情報專門官松尾弘子小姐及研究員大野太幹先生，2 位隨即利用參加本（2015）年 6 月 22 日至 24 日中央研究院舉辦之研討會的機會，於 6 月 25 日下午到本局參訪（如下頁圖 9 至 12）及經驗分享。或許未來有機會，雙方可建立長期合作機會，諸如輪流舉辦研討會、互派人員交流訪問實習等。

三、擴展及建立友好合作夥伴關係

本局配合行政院組織改造政策，組織職掌增列行政院與所屬各機關公文時效管制之規劃及推動、文書與檔案管理資訊系統之規劃及協調推動，原檔案資訊組更名為文書檔案資訊組，是以自 2012 年起開始承接公文電子交換系統、文書編輯製作、基層公文管理系統等及研

圖 9　由本局張副局長（右）代表致贈文宣品

資料來源：作者提供

圖 10　由本局張副局長（中立者）主持座談會

資料來源：作者提供

圖 11　松尾弘子小姐（右）及大野太幹先生（左）於本局檔案瑰寶區留影

資料來源：本局企劃組提供

圖 12　松尾弘子小姐（中）及大野太幹先生（右 2）與本局同仁於展覽廳合影

資料來源：本局企劃組提供

提節能減紙續階方案，並持續辦理各項推動作業，諸如電子會議、公文線上簽核、跨機關陳核會稿及行動簽核等業務；該等文件檔案之編輯製作、傳遞轉送、儲存管理，均與資訊系統之處理及資訊安全有密切關係。藉由參與國際研討會之機，可以廣泛接觸其他國家之相關學者專家，擴展國際人脈。此外，藉由參訪國外機關，相互交流，進而選定目標，強化接觸，期有機會締結姐妹關係，建立長期友好合作夥伴，彼此分享電子檔案保存管理技術之研發成果，互謀利基。

註　釋

註 1：蟻群優化演算法是 1992 年由 Marco Dorigo 提出，意指模仿螞蟻覓食行為的演算法。螞蟻覓食時，會沿途分泌留下特殊的賀爾蒙，以告訴其他螞蟻循著該路徑前往搬運食物。也有螞蟻會另闢新路，而找到更簡潔的路線。然該賀爾蒙會隨時間的經過而蒸發，為免路徑中斷，其他螞蟻循該路徑回巢時，會繼續分泌賀爾蒙補強之。因此，該賀爾蒙成為良好的食物指標，讓螞蟻齊心協力搬回食物。螞蟻演算法就是把好的組合規則比擬成螞蟻覓食的路徑，並不斷地局部調整組合規則，使之達到最佳組合規則。

註 2：Steganographic 是由 steganos 和 graphein 兩個希臘字根組合而成，steganos 字義為遮蔽、隱藏（covered），graphein 則是 to write 兩個字合併，意指隱藏所寫的字。而密碼學之 Cryptography 亦由 Crypto 和 graphy 二個希臘字組成。Crypto 的希臘字義是 secret 。因此，Steganography 的意義近似於 Cryptography 。Cryptography 是隱藏訊息（message）的意義（meaning），使他人看不懂涵意；而 Steganography 則是隱藏訊息本身的存在性（existence），讓人完全不知有訊息的存在。