因應個資法之科技環境強化實務策略研討:以 A 銀行為例

曹竣傑* 張耀鴻**
*中國文化大學資訊管理學系碩士班 **中國文化大學資訊工程學系

摘要

隨著資訊科技之發展，個人資料之流通較以往普遍且迅速，加以在商業社會中，個人資訊具有行銷方面之商品價值，常成為交易標的之內容，因此，保護個人資訊隱私權已成為各國政府共同努力的目標之一。我國早在民國 84 年即已通過電腦處理個人資料保護法，對於個人資訊隱私權已提供全面性之保障，僅對於金融業或信用資訊機構部分，再補充為詳細的行政規定，即可減少金融業之個人資訊隱私權爭議。鑒於個資還是盜用頻繁，立法院於 2010 年完成新版個資法修訂，且於 2012 年 10 月實施。本研究蒐集個資法相關文獻及針對 ISO27001 控制項目加強分析，並以參與 A 銀行之策略實務擬定資訊安全暨個資保護管理建議之藍圖、個資保護對資訊科技環境風險分析建議之步驟、稽核軌跡與日誌管理建議程序及，達到因應個資法加強科技環境實務。

關鍵詞：個資法、資訊安全強化、ISO27001

1. 研究動機及目的

ISO27001 雖為目前國際上最廣泛採用之資訊安全制度標準規範，但是否在個人資料保護這一環節能夠做好完善的保護措施，有效能防止個人資料被竊取、竄改、毀損、滅失或洩露，企業需重新審視公司本身在「個人資料保護法」規範下所造成的影響。[2]由於新版個資法產生 資訊資產不再只有營運機密資料，個人資料亦被規範成為受保護的對象，因此企業必須對現有資訊安全架構做調整。本研究將以 A 銀行為例，達到以下研究目的：

(1) 探討 ISO 27001 與個人資料保護法有關聯之控制要項。
(2) 探討個案公司對於在個人資料保護實施後,管理面及法律面有何具體做法？
(3) 探討資保護管理藍圖及資訊科技環境風險分析步驟。

2. 文獻探討

2.1 資訊安全(information security，INFOSEC)之意涵：

資訊可透過網路來互通共享，部份資訊可公開，但部份資訊屬機密，不可公開且不可篡改，必須作保密的管制以防使用者有意或無意的讀取或更改，而有關資訊保護之研究的總合稱為資訊安全。[1]

在資訊安全中所討論的資訊，一般而言，指的是企業或組織在營運時所收集，產生，或運用的資料，它可以存在於任何形式，不論是有形或無形的，它可以是存在於電腦中的資料，列印或書寫在紙張上的資訊，甚至是存在於通訊中。

這些資訊對企業或組織而言都是有價的，對企業或組織的營運有相當的影響。因此，需要賦予適當的保護，降低其風險，避免遭受內在或外來的威脅。

2.2 資訊安全(information security，INFOSEC)之定義：

保護資訊之機密性、完整性與可用性；得增加諸如鑑別性、可歸責性、不可否認性與可靠性。

[17]

(1) 機密性 (Confidentiality)資料不得被未經授權之個人、實體或程序所取得或揭露的特性。

(2) 完整性(Integrity)對資產之精確與完整安全保證的特性。

i. 可歸責性 (Accountability)：確保實體之行為可唯一追溯到該實體的特性。

ii. 鑑別性 (Authenticity)：確保一主體或資源之識別就是其所聲明者的特性。鑑別性適用於如使用者、程序、系統與資訊等實體。

iii. 不可否認性 (Non-repudiation)：對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。

(3) 可用性(Availability)已授權實體在需要時可存取與使用之特性。

(4) 可靠性(Reliability)始終如一預期之行為與結果的特性。

2.3 個人資料保護法之意涵：

個人資料保護法，立法目的為規範個人資料之蒐集、處理及利用，個資法的核心是為了避免人格權受侵害，並促進個人資料合理利用。而所謂的個人資料，根據個資法第一章第二條第一項：「指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料」其中，個資法特別把醫療、基因、性生活、健康檢查、犯罪前科等資料歸納於特種資料範圍內，明令此類資料除非特殊情形，不得蒐集、處理或利用，如圖 1。[6]

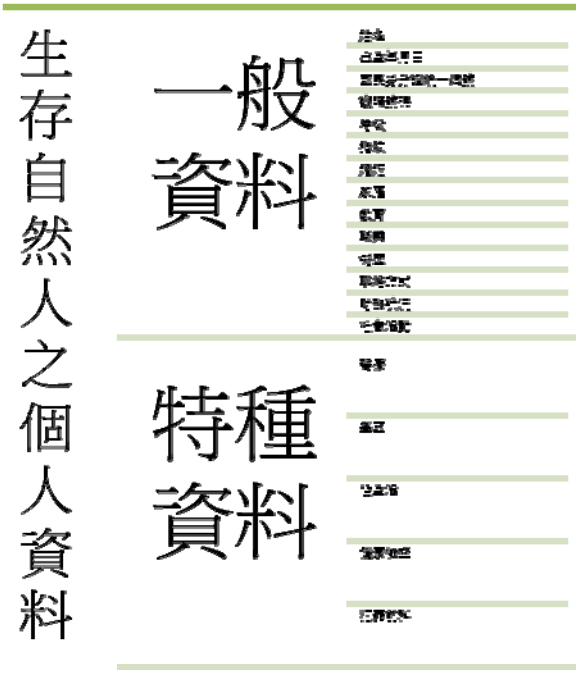

圖 1 何謂個人資料

個資法主要從蒐集、處理和利用等三個層面，來規範個人資料的合理利用，新個資法所保護的資料型態，也從原本的電腦處理之個人資料，延伸到無論是電腦處理的數位個人資料，或是紙本的個人資料，皆適用於直接或間接識別之個人資料中。[8]

根據個資法所明訂，蒐集、處理與利用之定義如表 1：

表 1 個資法所明訂蒐集、處理與利用之定義

蒐集	指以任何方式取得個人資料。
處理	指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
利用	指將蒐集之個人資料為處理以外之使用。

在蒐集個人資料時，個資法規定蒐集者應盡告知義務，除了部分特殊情形外，必須盡到告知當事人的義務，應明確告知當事人其公務機關或非公務機關名稱、蒐集目的、資料類別、資料使用期間、地區、對象及方式、當事人得行使之權利及方式、當事人選擇不提供個資時，對其權益之影響。[8]

處理與利用個資時，必須於個資法所明訂之特定目的之規定範疇內，並與原先蒐集目的有關聯，不得擅自挪用，並在特定目的消失或期限屆

滿時，主動或依當事人之要求，刪除、停止處理或利用該個人資料。

除了蒐集個資必須符合特定目的，蒐集者必須盡到告知義務外，個資當事人也有可行使之權利，包括了查詢、修改、補充個資，要求提供個資副本、要求停止蒐集、處理、利用個資，或者要求直接刪除個資，而且這些權利是不得被事先要求放棄或以合約限制的，如圖 2。[19]

圖 2 不得預先拋棄或以特約限制

2.4 ISO27001 之意涵：

國際標準組織（ISO）在 2005 年 10 月頒布了資訊安全管理系統（ISMS）的國際標準—ISO 27001:2005。ISO27001:2005 涵蓋所有和資訊交換相關的事項。制定 ISO27001 之目的在於防止企業資訊被濫用或竊取，如圖 3。[11]

因企業對資訊系統服務的仰賴日益加深，維持企業競爭力、財務健全、獲利率與企業形象的基本要件就是要，確保企業資訊的機密性（Confidentiality）、完整性（Integrity）、可用性（availability），確保企業的營運符合當地法律、合約規範等要求，改善公司治理，並對股東、客戶、消費者與供應商展示管理資訊安全風險的能力，透過適當的風險評估，確認對企業的威脅為何、並評估發生機率與潛在的影響，以完成企業合理的資訊安全設備投資計畫。[16]

圖 3 ISO27001 控制要項

2.5 個資法與 ISO 27001 之共通點：

個資法與 ISO 27001 標準有以下幾個共同之重點：[9]

(1) 資產（個資）盤點之實作：如何確認與盤點所有組織內之個人資料。
(2) 背景審查（篩選）之必要性：如何在資訊安全與個人資料保護兩者之間取得平衡。
(3) 儲存與備份管理：如何確保資料的生命周期已妥善定義與管理。
(4) 存取管理：資料之存取管理如何加強。
(5) 資訊安全事故管理：如何整合事故通報與處置程序。
(6) 遵循性：適法性之必要。

3. 研究方法：

本研究以某銀行導入 ISO27001 因應個資法強化科技環境策略為主題，對 A 銀行所實行強化資安策略加以分析，藉以瞭解銀行面對個資法資訊安全的管理現況，並透過國內文獻探討新版個資法之內涵，提出本研究的結論與相關研究建議。

3.1 個資法明定安全維護事項：

根據個資法明定安全維護事項，包括：[8]

(1) 配置管理之人員及相當資源
(2) 界定個人資料之範圍
(3) 個人資料之風險評估及管理機制
(4) 事故之預防、通報及應變機制
(5) 個人資料蒐集、處理及利用之內部管理程序
(6) 資料安全管理及人員管理
(7) 認知宣導及教育訓練
(8) 設備安全管理
(9) 資料安全稽核機制
(10) 使用紀錄、軌跡資料及證據保存
(11) 個人資料安全維護之整體持續改善

3.2 個資法明定細項重點方向：

從個資法明定細項重點方向，找出以下表 2 重點方向：[19]

表 2 個資法細項重點方向

依據個人資料保護法第27條	**依據個人資料保護法第29條**
「非公務機關保有個人資料檔案者，**應採行適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」	「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵 害當事人權利者，負損害賠償責任。**但能證明無故意或過失者**，不在此限」
符合法務部所提及之11項安全維護事項及以下配套措施 1) 建立或導入個人資料管理制度。 2) 輔導取得隱私權驗證標章。 3) 遵守中央目的事業主管機關發布之「個人資料檔案安全維護計畫及業務終止後個人資料處理方法之標準辦法」或其他指導原則。 4) **熟悉數位證據保存之鑑識程序與技術。**	企業須**留存有「證據能力」之紀錄**作為提供無故意與無過失重要證據，以提供企業個人資料保護的善良管理證據。
	企業除應留存完整之證據(紀錄)自保外，**採集證據的過程亦須符合蒐證程序。**
	數位證據的保存上更謹慎、攸關訴訟的勝敗。

3.3 企業面臨科技環境之挑戰：

因應個資法-企業面臨科技環境之挑戰分為以下幾點：[16]

(1) 善良管理的證據：面對資料外提供善良管理洩訴訟或爭議時，如何之證據？

(2) 難以瞭解證據留存現況：無法有效確認相關系統設備是否已留存足以識別鑑識對象之證據及紀錄 ？

(3) 個資外洩緊急應變計畫：於個資外洩事件發生時，尚無建置相關緊急應變計畫以供同仁依循。

(4) 數位證據鑑識標準程序：執行數位證據蒐證、保存及分析作業，內部尚無建置數位證據鑑識標準程序。

(5) 法令遵循：如「個人資料保護法」及「個人網銀業務服務定型化契約應記載及不得記載草案」之要求。

(6) 訟訴策略擬定：面對資料外洩訴訟或爭議時內部尚無針對不同情境擬定其訟訴策略。

(7) 數位鑑識分析環境建置：受限內部資源有限，尚無針對數位鑑識環境/工具進行建置及鑑識分析技術能力養成。

(8) 數位證據特性：數位證據本身特性所面臨之挑戰(易消滅、易竄改、不易取得的特性、製作人無法個體化)。

4.預期貢獻與成果：

面對個資法，最基本的是業者的態度，企業必須改變以往從自身立場去思考個資定位，轉而以個資當事人的角度出發，去思索倘若這些個資遺失會對個資當事人造成那些影響，產生何種侵害，而這些個資對企業而言是否為必要，進而將對個資的保護視為企業經營成本的一部分。

強化保護個人資料，是新版個資法與過去最大差異之一，在於要求個人資料蒐集、處理、及應用上的合理使用與規範，並彰顯證明已採取必要措施而「無故意或過失責任」，從 A 銀行的策略及文獻整理分析，整理出 ISO27001 跟個人資料保護法之間有相關聯之控制要項，規劃資訊安全暨個資保護管理建議藍圖，如圖 4。

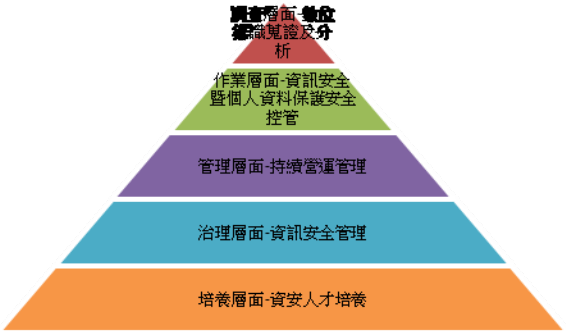

圖 4 資訊安全暨個資保護管理建議藍圖

資安最困難的是「取捨」，資訊安全、功能和效能三者，就像是三角形的三個頂點，越專注資安，就離另外兩者越遠，所以最困難的是安全與方便之間的取捨，以及成本與效能之間的取捨，針對「資訊安全暨個人資料保護安全控管」採取個資保護對資訊科技環境風險分析建議步驟如圖 5、表 3[16]及稽核軌跡與日誌管理建議程序如圖 6：

圖 5 個資保護對資訊科技環境風險分析建議步驟

表 3 個資保護對資訊科技環境風險分析建議表

個資生命週期	個資安全控管	防護方案	
資料蒐集(針對外部輸入)	應用系統安全防護	WAF(應用程式防火牆)、Code Review 機制、應用程式弱點掃描	稽核日誌管理分析
	入侵防護機制	入侵偵測防禦系統(IDS/IPS)、防火牆	
資料儲存(針對儲存標的保護)	資料庫保護	資料庫加密	
	備份媒體保護	磁帶加密控管	
	可攜式設備保護	硬碟加密、可攜式媒體控管及加密	
	共享主機/磁碟存取控管	儲存目錄加密、權限控管	
資料處理利用(針對人為操作)	資料存取權限控制	帳號存取權限控管、存取行為監控	
	資料庫活動監控	資料庫存取內容監控(DAM)	
	端點安全控管	防毒、儲存設備與周邊裝置管控 、DLP	
資料傳輸(針對傳輸行為)	資料傳輸保護	安全傳輸加密機制、DLP	
	電子郵件安全防護	郵件監控/加密/歸檔、郵件內容過濾識別、郵件附件加密	
	網路層保護	VPN、遠端存取控制	
資料銷毀	安全性銷毀	紙本及電磁記錄銷毀、硬碟抹除	

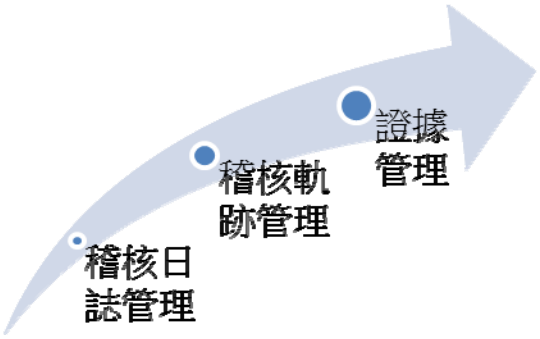

圖 6 稽核軌跡與日誌管理建議程序

數位鑑識之目的，透過蒐集、檢驗、分析、保存數位證據，透過專業的工具與技術採集有意義的證據資訊或從片斷資料描繪事件的大略情形以重建資料，使其獲得法庭接納，其常用工具之八大分類及分析工具如表 4：

表 4 數位鑑定八大分類及分析工具表

數位鑑識蒐證	磁碟處理與鏡像檔製作 壓縮與加解密工具 隱藏資料探勘 惡意程式碼鑑識 監看與檢視 資料搜尋 安全性工具 整合性工具
數位鑑識分析工具	Data Analysis and Visualization 工具 Data Mining 工具 (如 RapidMiner) Log 證據擷取工具 (如 Encase) Log 分析工具 (如 Highlighter、Log Parser)

參考文獻

[1] 林茹玉，「個資安全防護實作建議」，資訊安全通訊，17(3)，37-51，2011。
[2] 徐弘昌，「以ISO 27001為基礎評估電信業資訊安全管理－以第一類電信業者為例」，國立交通大學管理學院碩士在職專班管理科學組碩士論文，2009。
[3] 張碩毅、黃迺康、陳央庭、蘇仲杰，「企業個

人資料保護管理機制之建構與實證」，電腦稽核，25，91-113， 2012
[4]張慶勳，論文寫作軟實力－悠遊在研究寫作天地中。臺北市：五南圖書出版股份有限公司，2011。
[5]陳向明，社會科學質的研究。臺北市：五南圖書出版股份有限公司，2002。
[6]陳思穎，「個人資料保護法基本觀念介紹及因應規劃」，2010。
[7]陳盈成，「外商銀行業資訊安全管理之研究－以A銀行為例」，淡江大學資訊管理學系碩士在職專班碩士論文，2012。
[8]黃小玲，「個資法與國際隱私管理標準、規範之分析與應用」，資訊安全通訊，17(3)，22-36 ，2011。
[9]黃小玲，「個資法及ISO 27001相通性與操作概述」，行政院國家資通安全會報技術服務中心，2012。
[10] 黃廷弘，「ISMS 國際資安標準於電信業的應用」，ISMS國際資安標準之應用及資通安全威脅與管理研討會，2011。
[11] 經濟部標準檢驗局，「CNS 27001資訊技術－安全技術－資訊安全管理系統 －要求事項」，2006。
[12] 樊國楨、黃健誠、廖菊芳，「個人資料保護與資訊安全管理探微」，電腦稽核，23，1-15 ，2011。
[13] 穆震宇，「客戶資料外洩，新個資法2億伺候」，現代保險健康理財雜誌263期，2012。
[14] 林奇德，「以個案研究法探討企業因應個人資料保護法落實策略實務」，國立中央大學資訊管理學系在職專班，2013。
[15]余昌霖，「以ISO27001為基礎探討個資法對電信業者的影響-以F公司為例」，國立中央大學資訊管理學系在職專班，2013。
[16] 勤業眾信，「談後個資時代企業面臨的風險與因應之道」，2013.05.01
[17] William Stallings，「Network Security Essentials」，2009。
[18] 饒天，「因應新版個資法醫療資訊系統資料庫實測之研究」，2012,05
[19]個人資料保護法 http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021
[20] 鍾日迪，「金融資訊科技對銀行經營之影響-以世華銀行為例」，2001,07