整合資訊安全管理系統與個人資料保護數位證據鑑識流程之初探

林宜隆教授
元培科技大學資訊管理學系
cyberpaul747@mail.ypu.edu.tw

伍台國教授
國防大學管理學院資訊管理系
w13464@yahoo.com.tw

張文耀
國防大學管理學院資訊管理系
yao.chang2010@gmail.com

鄭香貝
國防大學管理學院資訊管理系
cc665603@gmail.com

摘要

我國公布新版修訂個人資料保護法是最近政府、企業組織與資訊界熱衷討論的議題，企業組織實施的資訊安全管理系統（ISMS），能否導入法規遵循（Compliance），支撐控制項目的運用，以達到個人資料保護法所規範要求，是本研究希望藉由 ISMS ISO27001 管理要項，配合國內學者林宜隆教授提出 PLSE Model 及個人資料保護 IPO Model 理論，結合數位鑑識流程進行研究對應，進一步提出個人資料保護數位證據鑑識標準作業流程（DEFSOP for PIPM），建構雛型架構，以提供專職鑑識人員數位鑑識工作流程之參考或可供後續研究學者實作參考。

關鍵詞：資訊安全管理系統、個人資料保護法、數位證據鑑識標準作業程序。

壹、前言

我國於2010年修訂個人資料保護法（簡稱新版個資法），顛覆過去電腦處理個人資料保護法（簡稱舊版個資法）的相關管理架構與舉證方式，新法的施行細則草案於2011年10月27日已公告，行政院宣布具爭議性的部分內容尚待修正後施行，新版個資法將會於2012年底前全面上路。新版個資法的施行上路，衝擊企業組織面臨重新檢視稽核內部及導入個資保護相關措施及資訊安全管理系統的方法，如何能尋求一項更好或是具說服力的制度、系統或架構，以提供日後法院舉證善盡保護的比例原則，將是值得關注與投資的方向。本研究希望透過國內林宜隆教授提出PLSE Model、IPO Model for Personal Data Protection（簡稱個資保護IPO Model）理論、數位證據鑑識標準作業程序（DEFSOP）整合資訊安全管理系統的初步探討，建構個人資料保護數位證據鑑識標準作業流程及雛型架構，可達到強化個人資料保護的目的，並為企業投資資訊安全管理系統之立基點，提升數位證據保全及善盡保護之責。

貳、個人資料保護與 ISMS 相關文獻探討

本文首先探討資訊安全管理系統（ISMS）、PLSE Model、個人資料保護IPO Model理論及個人隱私保護等相關文獻。

一、資訊安全管理系統

“現在企業與組織最普遍使用及能取得驗證的ISO27001資訊安全管理系統”（楊期荔、林宜隆；2011），資訊安全管理系統為國際規範具有認證代表性，而ISO27001前身為國際資訊安全管理規範BS7799-2，是由BSI（British Standard Institution）於1995年2月提出，1995年5月修訂為國際公認的安全準則（BSI官方網站）。資訊安全廣泛涵蓋應遵守的事項，於2005年被國際標準組織ISO所認可，命名為ISO27001（BSI官方網站）。其主要目的即資訊安全運用PDCA的要求應於組織確實施行，這對組織導入與建立一個ISMS的過程，分為規劃（Plan）執行（Do）檢查（Check）行動（Act）等四個作業程序。ISO27001提供組織在資訊安全管理系統的建立實作、運作、審查、監視、維持及改進之標準化作業程序（葉家銘、林宜隆，2009），其價值性除了進行評鑑資訊風險性的資產外，核心價值為防堵不當的資訊於組織外部與內部的行為規範，用於建立預防環境制度。

ISMS具有系統化與文件化的管理程序系統（林宜隆，2009），主軸概念以預防控制為主軸，基於系統、整體面、科學化的安全評估風險，作為組織在導入建置與稽核所遵循資訊管理系統（ISMS）之方法論，其控制要項內容分為11大項管理領域，39項執行目標、133項的內容實作指引方式（林東清，2005；葉家銘、林宜隆，2009；周瑞國、林宜隆，2011）。使資訊面臨環境風險的發生機率及風險事件降低至可接受收水準的結果，組織保持業務持續性的運作，確保資訊的保密性、完整性和可用性（謝昆霖、呂易

儒，2006；林宜隆，2009）。

二、個人資料保護 IPO Model 理論與 PLSE Model

對於近期將施行的新版個資保護法，國內學者林宜隆教授提出參考維基百科中IPO Model，將其IPO模型整合新版個人資料保護的觀點進一步解釋為IPO Model for Personal Data Protection理論，其原理說明如下：

（一）輸入蒐集面（Input）：透過外部環境反饋到內部系統組織，所以在一個組織內部系統中，由輸入觀點將組織進行預防和防護措施，可避免將具有風險的因素預先進行門檻篩選過濾。例如，以個人資料保護法中，在蒐集個資預先設定那些因避免蒐集機敏性的個人資料，在事前整合必須經由個人資料的當事人同意時，對於組織進行資訊蒐集的活動必須符合法規限制。

（二）處理階段面（Process）：透過組織內部的硬軟體設施完成資訊處理機制，在此階段重點為保全的措施，任何處理過程皆需脈絡可循，這是組織需舉證之關鍵所在，保全操作措施過程必須有效的控管資料確保在處理分析階段確保資料完整性。

（三）輸出利用面（Output）：後續輸出利用面相關個人資料在處理傳輸並且將最後反饋於輸入蒐集面後續修正，達到善盡保護及呈現的良善循環。

IPO Model與提出PLSE Model（藍添興、林宜隆，2004）模型的四個面向（政策面Policy、法律面Law、技術面Security、教育面Education）與數位鑑識計算科學(Forensic Computing）數位鑑識專家（Jill Slay and I-Long Lin, 2008）中，提出4P's模型，分別是以傳統資通安全相關的預防（Prevention）、防護（Protection）和對於數位鑑識有絕對關聯的保全（Preservation）、呈現（Presentation）等四個資通安全的構面，進而與ISO/IEC27001對應說明（如表2-1、圖2-1所示），由此可知IPO Model、PLSE Model與4P's Model可套用於ISO/IEC27001以及其對應關係。

<個人資料保護IPO Model>

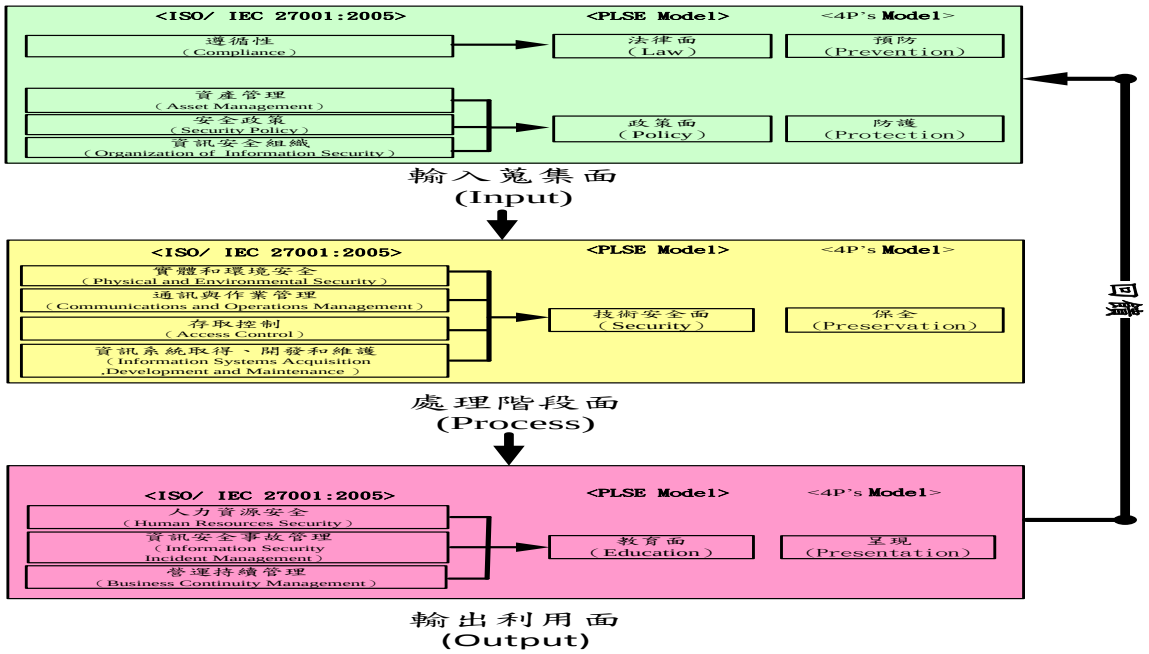

圖2-1 IPO Model、4P's Model、PLSE Model可套用於ISO/IEC27001對應圖

（資料來源：本研究整理）

表2-1 IPO Model、4P's Model、PLSE Model可套用於ISO/IEC27001表列對應說明

個資保護 IPO 模型	4P's 模型	PLSE 模型	ISO/IEC27001	說明
輸入蒐集面 （Input）	預防 （Prevention ）	法律面 （Law）	遵循性 （Compliance）	符合組織遵循資訊安全政策規定或法令。
	防護 （Protection）	政策面 （Policy）	資訊安全組織 （Organization of Information Security）	建立管理組織內部與外部團體的架構，用於資訊安全的管制及執行資訊安全的規則。
			資產管理 （Asset Management）	達成對於組織的各項有形或無形資產資訊安全進行分類確保有效保護的責任。
			安全政策 （Security Policy）	營運依據相關法規與法律制定要求，提供管理階層表達對於資訊安全管理的支持與指示。
處理階段面 （Process）	保全 （Preservatio n）	技術安全面 （Security）	實體和環境安全 （Physical and Environmental Security）	對於組織營運實體場所與資訊環境，對於安全事項簡單明確提出規範要求。
			通訊與作業管理 （Communications and Operations Management）	規範作業程序，盡可能完善防範對於組織內外部的溝通聯繫，監視未經授權的資訊活動，以利對於資訊安全管

				理運行順利的責任。
			存取控制（Access Control）	規範資訊的存取權限的控制。
			資訊系統取得、開發和維護（Information Systems Acquisition ,Development and Maintenance）	確保組織 IT 資訊系統專案或相關專案支援活動已施行安全控制，必要時管制施行加密和資料管制。
輸出利用面（Output）	呈現（Presentation）	教育面（Education）	人力資源安全（Human Resources Security）	規範組織人員明訂對於安全方面的職位與各項責任。
			資訊安全事故管理（Information Security Incident Management）	要求確保在傳達與資訊系統有關的資訊安全事故與弱點，應即時採取對於安全事故改進矯正與即時通報，對於全事故管理，確保施行管理資訊安全事故的方法有效與一致性。
			營運持續管理（Business Continuity Management）	規範發展保護遭遇重大事件組織能維持營運計畫，確保關鍵業務營運避免受到重大災害或中斷影響。

（資料來源：林東清，2005；林宜隆，2009；周瑞國、林宜隆，2011；本研究整理）

三、個人隱私保護原則

“新版個人資料保護法有導入國際間普遍性的隱私權保護原則”（楊期荔、林宜隆，2011），國際上亞太經濟合作組織（APEC）參考經濟合作暨發展組織（OECD）的隱私保護8個使用個資應用基本原則及個人資料國際傳輸指導方針，2004年於APEC制訂出隱私保護綱領（APEC Privacy Framework），做為提升各國隱私保護之重要推動方針，

並確保亞太地區各會員國間資訊自由流動，各會員國規範國內推行制定需符合隱私保護綱領之規範原則。APEC提出的九大隱私權保護原則（劉佐國、2005；林宜隆，2009；楊期荔、2011），APEC提出的九大隱私權保護原則，以加強隱私權的保障。茲將內容摘要敘述如下：

（一）　避免損害原則（Preventing Harm）：有關蒐集、處理與利用於個人資料，應避免損害當事人權益。

（二）　告知原則（Notice）：需蒐集當事人個人資料時，對當事人應告知蒐集資料的目的、原因與用途等。

（三）　限制蒐集原則（Collection limitation）：個人資料蒐集應符合蒐集必要之範圍，逾越目的範圍資料，不得隨意蒐集機敏資料。

（四）　利用個人資料原則（Uses of Personal Information）：個人資料之利用，符合當初告知時蒐集目的範圍內，未經當事人同意不得將該蒐集資料做其他利用處理。

（五）　當事人選擇原則（Choice）：依當事人作自主決定有關個人資料的蒐集或利用，可自由選擇參與或退出的機制，對於資料蒐集利用者應遵守當事人的選擇意願。

（六）　個人資料完整原則（Integrity of Personal Information）：持有個人資料管理者應確保蒐集資料完整正確，避免當事人因不正確資料，使其權益受到侵害。

（七）　安全維護原則（Security Safeguards）：個人資料管理者應採取必要的安全措施用於保護，避免持有的個人資料遭受侵害。

（八）　查詢及更正原則（Access and Correction）：當事人對其自我資料有擁有隨時查詢閱覽、補充更正的權力。

（九）　責任原則（Accountability）：針對違法無故蒐集或利用個人資料，使個人遭受不法使用，應追溯並課相關法律責任，以保障當事人應有的權益。

目前我國為加強隱私權的保障，表2-2為APEC、OECD、IPO Model與新版個人資料法保護條文對應表，透過IPO Model對應表可APEC九大原則與OECD8個使用個資應用基本原則，更容易了解新版個資法。

表2-2 APEC、OECD、IPO Model與新版個人資料法保護條文對應表

APEC九大原則	OECD8個使用個資應用基本原則	個資保護 IPO Model	新版個人資料保護法條文
預防損害原則	限制使用原則	輸入蒐集面（Input）	§12,§18,§27~§40
告知原則	公開原則	輸入蒐集面（Input）	§7,§8,§9
蒐集限制原則	限制蒐集原則	輸入蒐集面（Input）	§6,§15,§19,§53
責任原則	責任義務原則	處理階段面	§21

安全維護原則	安全保護原則	（Process 處理階段面 （Process ）：	§9,§27
個人資料之利用原則	目的明確化原則	輸出利用面 （Output）	§5,§16,§20
查閱和更正原則	個人參與原則	輸出利用面 （Output）	§3,§10,§11,§13,§17
當事人自主原則	個人參與原則	輸出利用面 （Output）	§3,§10,§11,§13
個人資料之完整性原則	資料內容原則	輸出利用面 （Output）	§11

（資料來源：（1）楊期荔、林宜隆；（2）本研究整理）

參、個人資料保護數位證據鑑識標準作業程序

本研究在探討國內外文獻整理分析與歸納，以及參考國內學者林宜隆教授所提出數位證據鑑識標準作業程序（DEFSOP），認為建構個人資料保護之數位證據鑑識標準作業流程雛型架構，主要可分為四大階段，例如原理概念階段、準備階段、操作階段及報告階段。鑑識標準流程四大階段其中以操作階段最為關鍵，操作階段又分為蒐集、分析、鑑識，另在數位鑑識計算科學（Forensic Computing）數位鑑識專家（Jill Slay and I-Long Lin, 2008）中，提出4P's模型，分別是以傳統資通安全相關的預防（Prevention）、防護 （Protection）和對於數位鑑識有絕對關聯的保全 （Preservation）、呈現（Presentation）等四個資通安全的構面；並將其應用在國內學者（林宜隆，2007；顏雲生， 林宜隆，2011；楊期荔、林宜隆，2011 ）提出的數位證據鑑識標準作業程序（Digital Evidence Forensics Standard Operation Procedure, DEFSOP）的模型中，進行修正並於後續本章節將個人資料保護數位證據鑑識標準作業程序（DEFSOP for PIPM）雛型架構四個階段分別介紹。

一、建構個人資料保護數位證據鑑識標準作業程序雛型架構-原理概念階段

建構個人資料保護數位證據鑑識標準作業程序雛型架構-原理階段是將數位鑑識專家（Jill Slay and I-Long Lin，2008），提出4P's模型預防（Prevention），對應國內林宜隆教授數位鑑識原理階段如圖3-1，圖3-2所示。

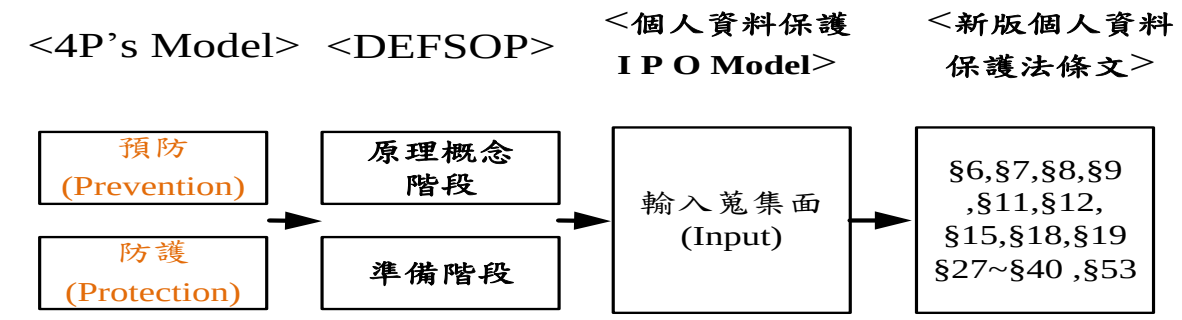

圖3-1 個人資料保護數位證據鑑識標準作業程序雛型架構-原理概念階段對應個人資料輸入蒐集面相關條文

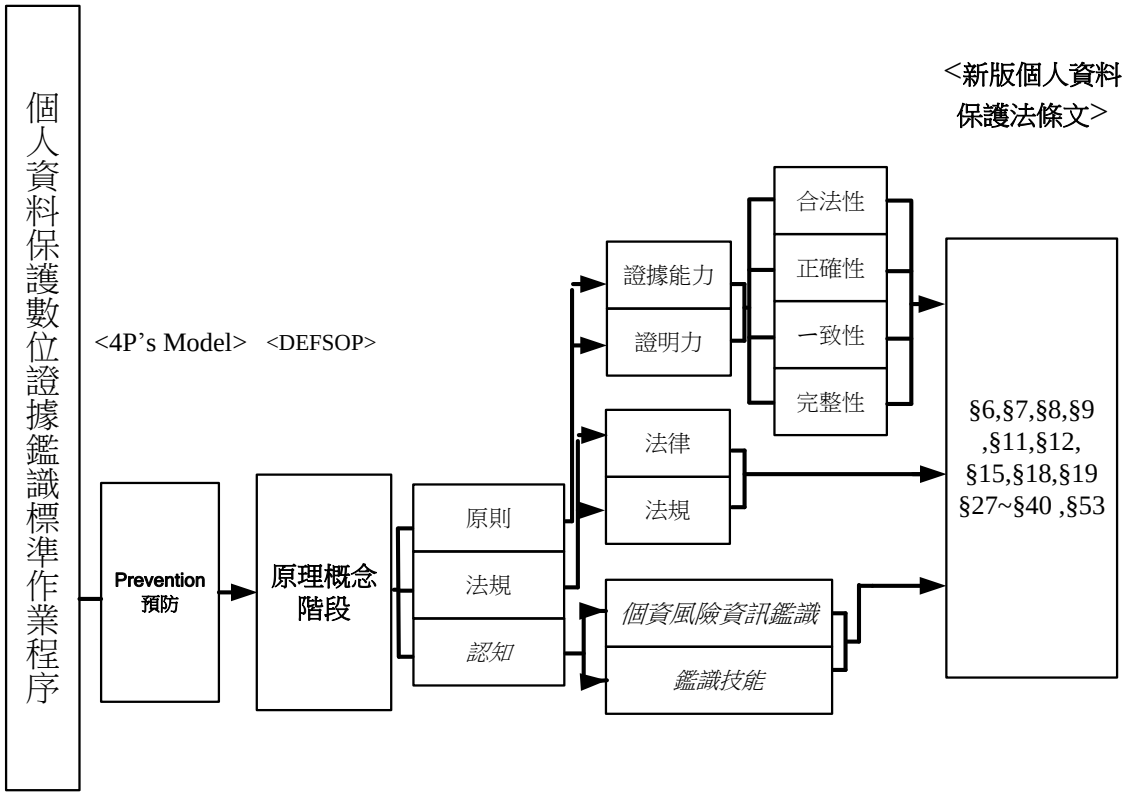

圖 3-2 個人資料保護數位證據鑑識標準作業程序雛型架構-原理階段

在資訊安全管理機制整合個人資料保護鑑識準備階段為組織單位未遭受破壞時，必須透過此原理階段進行相關預防的必要安全防護措施與規範，預防發生資訊安全管控重點流程，以下為個人資料保護鑑識標準流程-原理階段項目說明。

（一）法規：係指個人資料保護法、民法、刑法等法定之犯罪事項為限。

（二）原則：任何數位證據取得需遵循合法、自願、真實的重點原則，不得以未經授權同意非法侵入他人電腦資訊系統的方法獲取證據；在蒐集時都應當有相關第三公正方的證人於現場，特別是其記載該資料的電腦的操作人或資產管理者在現場。

（三）認知：從事鑑識專業人員應保有相關職業道德、具備個人資料保護相關法規與法學基礎知識、強化專業鑑識本職技能與數位證據鑑識流程。

二、建構個人資料保護數位證據鑑識標準作業程序雛型架構-準備階段

建構個人資料保護數位證據鑑識標準作業程序雛型架構-準備階段是將數位鑑識專家（Jill Slay and I-Long Lin，2008），提出4P's模型防護 （Protection），對應國內林宜隆教授數位鑑識原理階段如圖3-3，圖3-4所示。

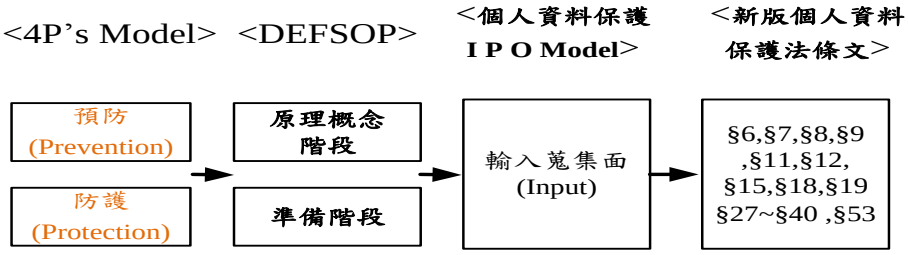

圖3-3個人資料保護數位證據鑑識標準作業程序雛型架構
-準備階段對應個人資料法條文

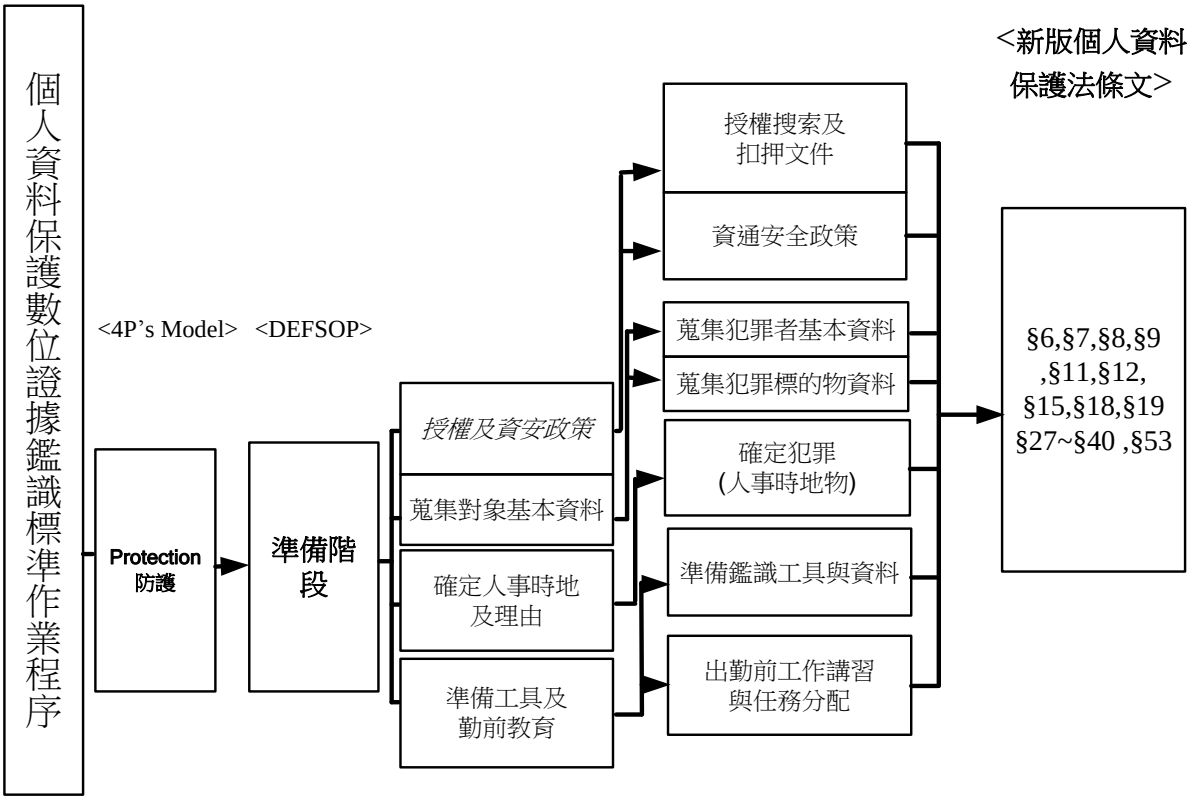

圖3-4 個人資料保護數位證據鑑識標準作業程序雛型架構-準備階段

在資安管理機制整合個人資料保護鑑識準備階段為為組織單位未遭受破壞時，必須透過此準備階段進行相關防護的必要安全防護措施，避免及預防資安發生重點管控流程，以下為個人資料保護鑑識標準流程-準備階段項目說明。

（一）授權：申請搜索票及扣押證物證明合法同意蒐證相關文件。對於一些鑑識工具的使用，鑑識人員必須具備專業性的知識與技術，另鑑識從業人員應該考取相關職能鑑識證照或教育訓練認可。

（二）蒐集犯罪：根據犯罪的類型，並利用已掌握的情況分析可能作案嫌疑的人員，若有案情需要也可訪談相關人員，並規劃鑑識執行的策略方針。

（三）確定人事時地物：根據並利用已掌握的情況進行分析，決定搜索地點、特定對象與時間，依據所蒐集嫌疑人資料後，決定搜索地點和時間。

（四）準備工具資料及勤教：鑑識相關工具資訊需準備電腦軟硬體規格的參考手冊、犯罪工具程式的參考手冊、破解電腦及智慧型手機裝置。在每次出任務前，必須針對鑑識人員與委任專職之個人資料保護專業人員進行進一步的說明，說明搜索任務、項目，並檢查軟硬體及工具是否準備齊全，以避免一些意外狀況發生。

三、建構個人資料保護數位證據鑑識標準作業程序雛型架構-操作階段

建構個人資料保護數位證據鑑識標準作業程序雛型架構-準備階段是將數位鑑識專家（Jill Slay and I-Long Lin，2008），提出4P's模型保全（Preservation），對應國內林宜隆教授數位鑑識操作階段如圖3-5, 圖3-6所示。

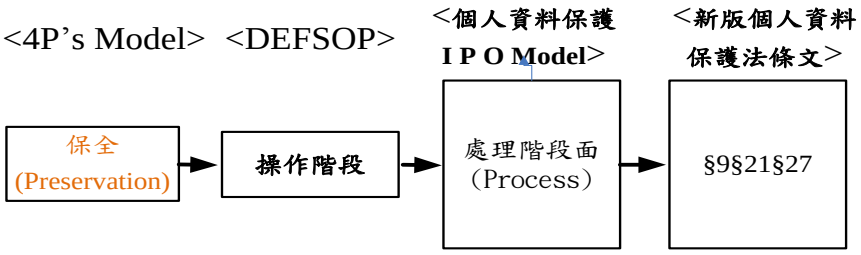

圖3-5個人資料保護數位證據鑑識標準作業程序雛型架構
-操作階段對應個人資料法條文

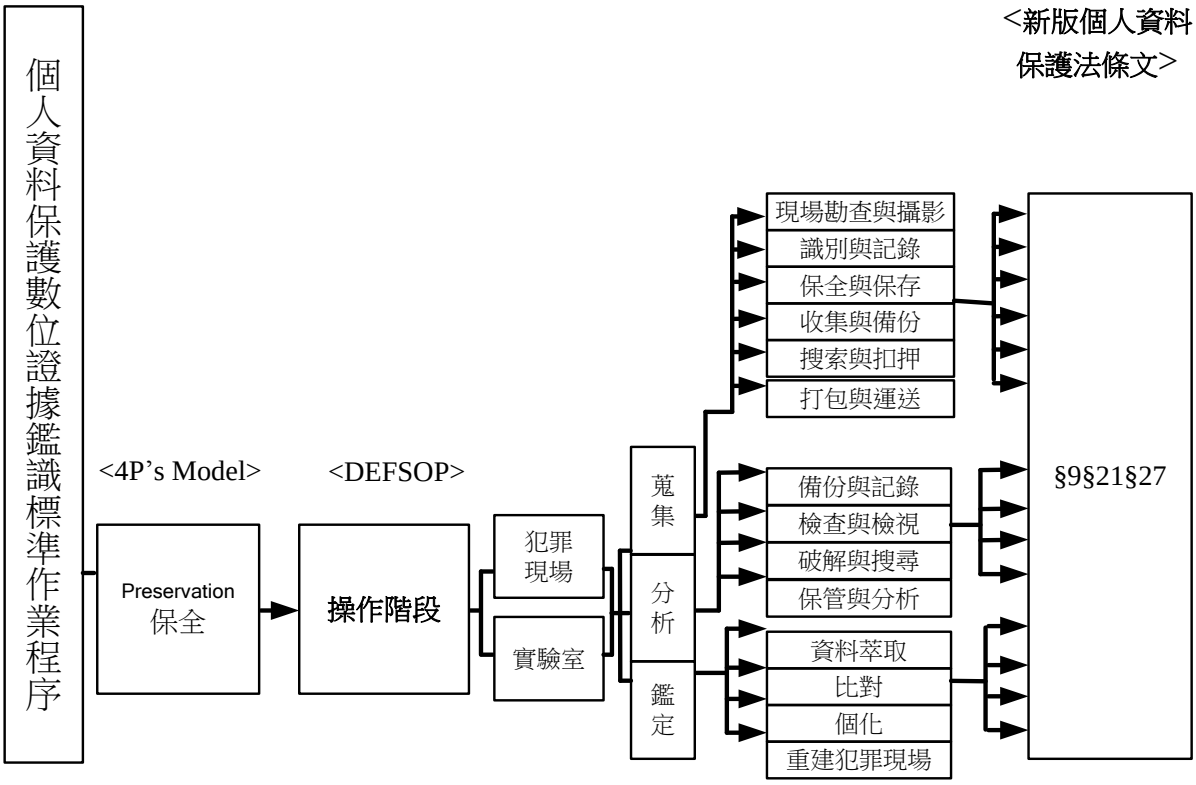

圖3-6 個人資料保護數位證據鑑識標準作業程序雛型架構-操作階段

在資安管理機制整合個人資料保護鑑識操作階段為為組織單位已遭受破壞時，必須透過此操作階段進行相關的將發生時的事證進行保全重點流程，以下個人資料保護鑑識標準流程-操作階段項目說明。

（一）蒐集程序：程序大致分為現場勘查與攝影、辨別與紀錄、保全與保存、蒐集與備份、搜索與扣押、打包與運送等操作程序部分，在各個執行操作程序部分，對何種數位資料該用何種工具整理出來用於順利進行蒐集處理方案。

（二）分析程序： 程序大致分為備份與紀錄、檢查與搜索、分析與保管，在各某些部分整理對應出何種數位資料該用何種工具來順利進行分析。

（三）鑑定程序： 程序大致分為五個流程部分，分別為資料萃取、比對及個化、重建犯罪現場，在比對及個化整理對應出數位資料該用何種工具來進行鑑識。

四、建構個人資料保護數位證據鑑識標準作業程序雛型架構-報告階段

建構個人資料保護數位證據鑑識標準作業程序雛型架構-準備階段是將數位鑑識專家（Jill Slay and I-Long Lin，2008），提出4P's模型呈現（Presentation），對應國內林宜隆教授數位鑑識報告階段如圖3-7、圖3-8所示。

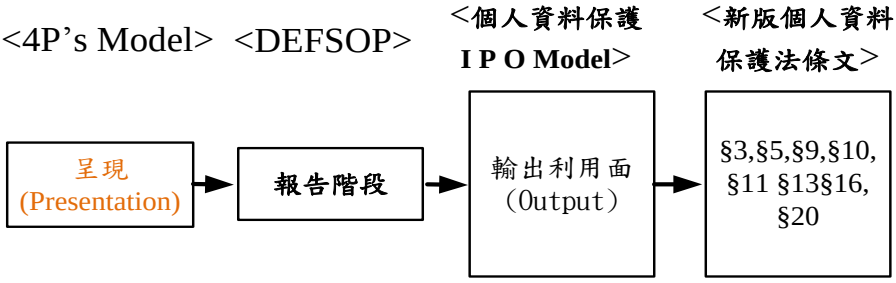

圖3-7 個人資料保護數位證據鑑識標準作業程序雛型架構
-報告階段對應個人資料法條文

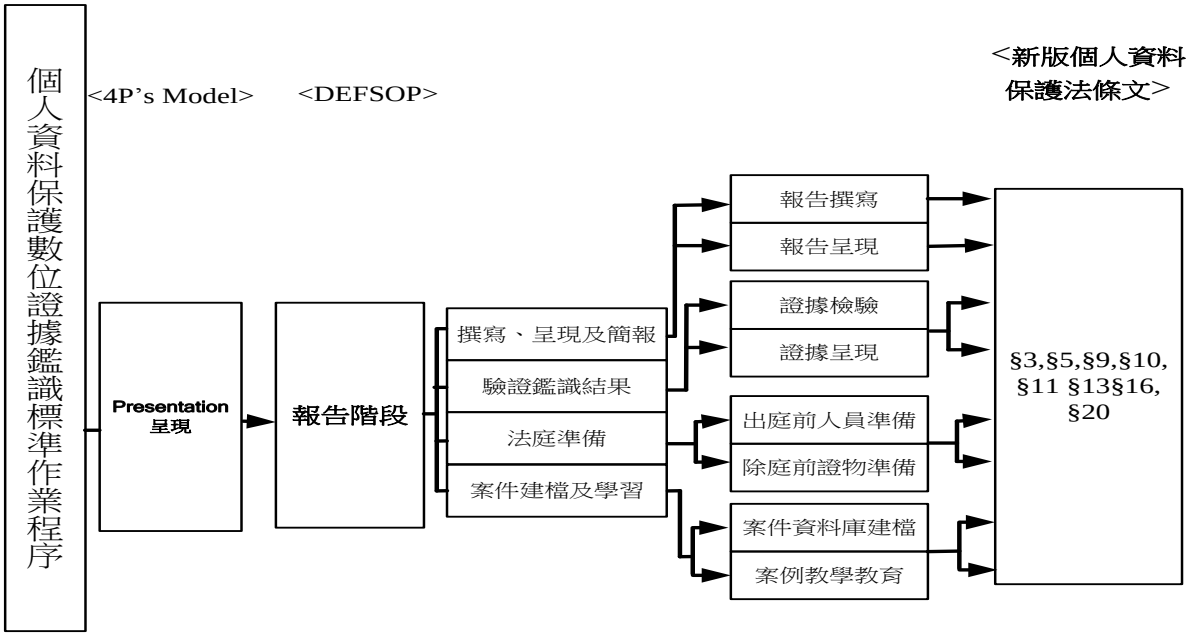

圖3-8 個人資料保護數位證據鑑識標準作業程序雛型架構-報告階段

在資訊安全管理機制整合個人資料保護鑑識操作階段為為組織單位已遭受破壞後，接續操作階段報告鑑識將發生時的事證進行保全與證據檢驗與證據呈現的重點流程項目，需指派相關法務結合資訊背景的專業人員進行後續訴訟舉證的責任，與反饋於鑑識標準流程準備階段以避免後續資安外洩事件再度發生。以下為個人資料保護鑑識標準流程-報告階段項目說明。

（一）撰寫呈現及簡報：大致分兩個部分，分為報告撰寫與報告呈現，其內容重點必須視證據之內容與使用者之目的，依照所鑑識得到的證據針對其客觀平衡及完整正確的以查核之結果事實提出方案報告。

（二）驗證鑑識結果：大致分為兩個部分，分為證據檢驗與證據呈現，對於證據之鑑識結果如果尚需進行相關驗證程序，無論是紙本書證或是數位化的證據，都需要進行驗證程序，為了確保所得到的證據之有效性、一致性與完整性。

（三）法庭準備：大致分兩個部分，分為出庭前人員準備與出庭後證物準備，對於個資鑑識專職從業人員對在法庭係以專家證人之身份或是檢調團隊之一員身份出庭

作證，在證詞與地位上應有不同之認知，但都必須以專業人員的自我要求進行準備，對於鑑識報告上所提及之證據，應妥為保管，以利法庭之判案。

（四）案件建檔及學習：為了相關稽核人員或組織人員教育訓練日後的查調便利性，鑑識完畢後之鑑識相關報告與證據，應採用合理的方案建立保存之方法與設置閱覽相關人員的權限規範，不論是書面或電子檔案，應有備份方案機制存在，最好設立保存地點於不同位置。對於案例教育則屬於組織內部知識管理與傳承經驗範圍的分享，雖然已非專職鑑識工作的主要部份，但是對於從事專職從業人員鑑識技巧與效率的發展重要性，卻也是十分重要的。

肆、結論

未來在新版個人資料保護法正式施行後，對於業務需求而擁有大量個人資料的公務與非公務機關的組織而言，最重要的轉變是要接受任何有關於個人資料的保護都要有嚴謹的機制管控，已不再是舊版個資法所規範僅僅交由「ICT資訊部門單位」即可負擔全部的資料控管責任，若僅限於ICT資訊部門資訊室的機房實體防護、主機與應用系統、系統資料庫定期弱點掃瞄與滲透測試偵測弱點就能確保個人資料的安全性，對資訊安全控管有其存在之必要性，唯ICT資訊單位外的每個環節、每位因業務所持有、操作、傳遞、儲存與銷毀（如蒐集、處理、利用等IPO Model ）的承辦人員，都必須確依規定辦理，因為稍有不慎，資料內涵的機敏個人資料就會外流至惡意或無惡意的組織或個人，造成無法挽回的態勢。對照新版個資法所述之罰鍰與處分，以及連帶可預期公務與非公務機關的組織形象的損失，更加考驗組織面對此風險管理議題所需強化投入的精神與資源，面臨個人資料保護之要求，已是各個組織無可迴避的任務與使命。

參考文獻

1.莊裕澤、葉逢明、鄭南昌、徐國安，（2003），資訊安全管理認證制度-BS7799。.

2.林宜隆、葉家銘，（2009），『論述ISMS資訊安全管理系統發展網路犯罪預防策略的新方法』，TANET 2008臺灣網際網路研討會，義守大學主辦。

3.林宜隆，（2009），網路犯罪理論與實務台北：中央警察大學出版社。

4.林東清，（2005），資訊管理：e化企業的核心競爭能力，台北：智勝文化。

5.陳彥駿、林宜隆、伍台國，（2010），植基於資安治理建構數位證據鑑識機制之研究-以數位證據蒐證系統為例，國立國防大學管理學院資訊管理研究所碩士論文。

6.周瑞國、林宜隆、伍台國，（2011），植基於雲端安全之數位證據鑑識標準作業程序之研究，國立國防大學管理學院資訊管理研究所碩士論文。

7.劉佐國、2005，我國個人資料隱私權益之保護-論「電腦處理個人資料保護法」之立法與修法過程，律師雜誌（307期），臺北律師公會。

8.楊期荔、林宜隆、李建裕、張志欉、戴崇賢，（2011），『資訊安全管理系統結合情境犯罪預防理論保護個資之策略初探-德爾菲法的應用』，TANet2011臺灣網際網路研討會，國立宜蘭大學主辦。

9.謝昆霖、呂易儒，（2006）『非營利單位資訊備援機制建置之研究』，南華大學資訊管理研究期刊，第6期，81~100頁。
10.維基百科IPO Model http：//en.wikipedia.org/wiki/IPO_Model。
11.BSI台灣官方網站 http：//www.bsigroup.tw/zh-tw/。
12.Yun-Sheng Yen , I-Long Lin , Bo-Lin Wu ,"A study on the forensic mechanisms of VoIP attacks： Analysis and digital evidence", *the Journal of Digital Investigation*, July 2011,Vol. 8 , pp. 56-67。
13.I-Long Lin and Yun-Sheng Yen, "VoIP Digital Evidence Forensics Standard Operating Procedure," *International Journal of Research and Reviews in Computer Science（IJRRCS）*,Vol. 2, No 1, March, 2011,pp.173- 179 。

To Investigate of Information Security Management System Integrate Personal Information Protection Digital Evidence Forensics Standard Operating Procedure

I-Lung Lin
Department of Information Management, Yuanpei University
cyberpaul747@mail.ypu.edu.tw

Tai-Kuo Wu
Department of Information Management, Management College of National Defense University
w13464@yahoo.com.tw

Wen-Yao Chang
Department of Information Management, Management College of National Defense University
yao.chang2010@gmail.com

Hsiang-Pei Cheng
Department of Information Management, Management College of National Defense University
cc665603@gmail.com

Abstract

Our government released the new version of amendments to the Personal Data Protection Act is a recent government, business organizations and IT industry are keen to discuss issues. Corporate organization and implementation of information security management system （ISMS）, can import compliance, support the use of control project, specifications in order to achieve the Personal Data Protection Act. This study is to hope to be managed by the ISMS ISO 27001, with domestic scholars, Professor I-Lung Lin the Model theory of the PLSE model and personal data protection IPO, combination of digital forensic process to study corresponding, further proposed the protection of personal data to digital forensic evidence standard operating procedures （DEFSOP for PIPM）, construction of the prototype structure, as a reference implementation to provide full-time forensic personnel digital forensics workflow reference or for follow-up studies scholars.

Keywords： Information Security Management System, the Personal Information Protection Act, DEFSOP