作業報導

●數位證據保全標準作業程序及第一線人員使用工具之簡介

法務部資訊處共用系統科設計師 吳典松

壹、 前言

日新月異的資通訊技術正逐漸改變現代人的生活方式，當我們享受於科技所帶來便利與助益之時，伴隨而來的資訊安全威脅與電腦犯罪現象卻也日趨嚴重，例如電腦病毒、駭客入侵、網路攻擊或竊取機密等事件更是層出不窮，要如何有效應對並打擊這些事件已成為各國政府關注的焦點。惟當相關事件發生時，第一線人員往往僅關切控制事件影響範圍與消弭事件所造成之風險，卻忽略了保存數位證據的重要性。有鑑於此，政府近年來為因應個資法施行後，各項潛在訴訟需要及雲端服務潮流所帶來之數位爭訟事件，正發展數位鑑識技術與產業扶植計畫，並推動證據保全機制與規範，以強化國家資通訊安全能力。

行政院於102年12月25日函頒「行政院於國家資通訊安全發展方案（102年至105年）」，在該方案附錄2：「行動方案執行要點與績效指標說明」之行動方案3.3.1「完善數位證據保全及相關標準作業程序」中明確指定法務部於103年制定數位證據保全標準作業程序規範。其執行要點略以：1.訂定符合證據能力的數位證據保全標準作業程序。2.推動所屬各機關依標準作業程序進行數位證據保全。據此，法務部於103年著手訂定「政府機關(構)資安事件數位證據保全標準作業程序」草案，於103年12月函報行政院，並依行政院資通安全辦公室於104年5月6日召開之研商會議中相關機關所提意見進行修正，俟再報院審核後函頒施行。

為使第一線人員能透過適當工具程式，收集保存相關數位證據紀錄，法務部於103年度辦理數位鑑識作業環境建置暨教育訓練委外案，開發第一線人員數位證據保全自動化蒐集工具，以期資安事件發生時，本部所屬機關第一線人員能透過工具蒐集現場數位證據紀錄，確保數位證據的證據能力，俾利後續數位鑑識分析作業能順利進行。另為提高現有行政資訊系統共用程度，法務部於行政院主計總處所推行資訊資源整合共用系統中，研提「數位證據保全自動化蒐集工具」推動計畫，期能將第一線人員數位證據保全自動化蒐證能量推展至其他相關政府部會機關，並透過人員訓練機制，以確保相關政府部會機關能有效進行此作業。

貳、 數位證據保全標準作業程序簡介

當機關發生資安事件之際，須於第一時間進行數位證據保全的工作，以有效蒐集相關證據資料供後續鑑識分析之用，並應同時保有證據能力與公信力。法務部資訊處爰委由具有數位鑑識實務經驗之業者協助，參考相關數位鑑識國際標準（ISO/IEC27037），研擬「政府機關(構)資安事件數位證據保全標準作業程序」草案，

該程序經邀集相關機關(單位)研商修正意見，並由資訊處多次審視及實作檢驗。訂定本作業程序之目的，在於使行政機關於資安事件調查時，能有效保全及使用數位證據，俾執行人員於執行數位證據識別、蒐集、擷取、封緘及運送作業時有所依循(圖1)，相關作業程序概述如下：

一、 數位證據識別

記錄人員應維護現場完整，避免改變數位證據原始狀態，判斷與案情相關之數位證物，視現場狀況以錄影、拍照或其他方式記錄現場。

二、 電腦設備或儲存媒體蒐集

系統於可關機情況下，應封緘完整電腦設備及儲存媒體，若為無法中斷服務之伺服主機系統等，應在上級機關或鑑識單位的監督下，進行嚴謹的資料轉錄，並將其數位證據蒐集結果填寫於「數位證據蒐集工作表(電腦設備)」或「數位證據蒐集工作表(儲存媒體)」。

三、 揮發性與邏輯性資料擷取

數位證據保全人員應考量事件類型及現場狀況後，擷取揮發性資料(如記憶體中的資料)及系統邏輯性資料(如作業系統資訊、網路狀態及執行程序資訊等)。擷取資料完畢後，應產生相對應之雜湊運算值及擷取資訊記錄之報表，經執行人員與事件發生單位主管簽名。

四、 數位證據封緘

應確實清點數位證據，每一項數位證據應分別填寫一張「證據監管鏈表」，並固定至對應之證據收集容器或公文袋上。數位證據於封緘前應妥善包裝並考量其保護措施，以避免靜電或運送過程中發生碰撞與震動等。數位證據攜出機關前應填列「證據取得清單」並交由在場相關人員確認及簽章。

五、 數位證據運送

證據運送過程中應符合證據監管鏈要求，無被篡改等不當行為發生之可能性，並於每一交接過程中其交接流程應記錄明確，交付人員與接收人員應填寫「證據監管鏈表」，詳載交件人、收件人、日期時間及目的等資訊，以示負責。

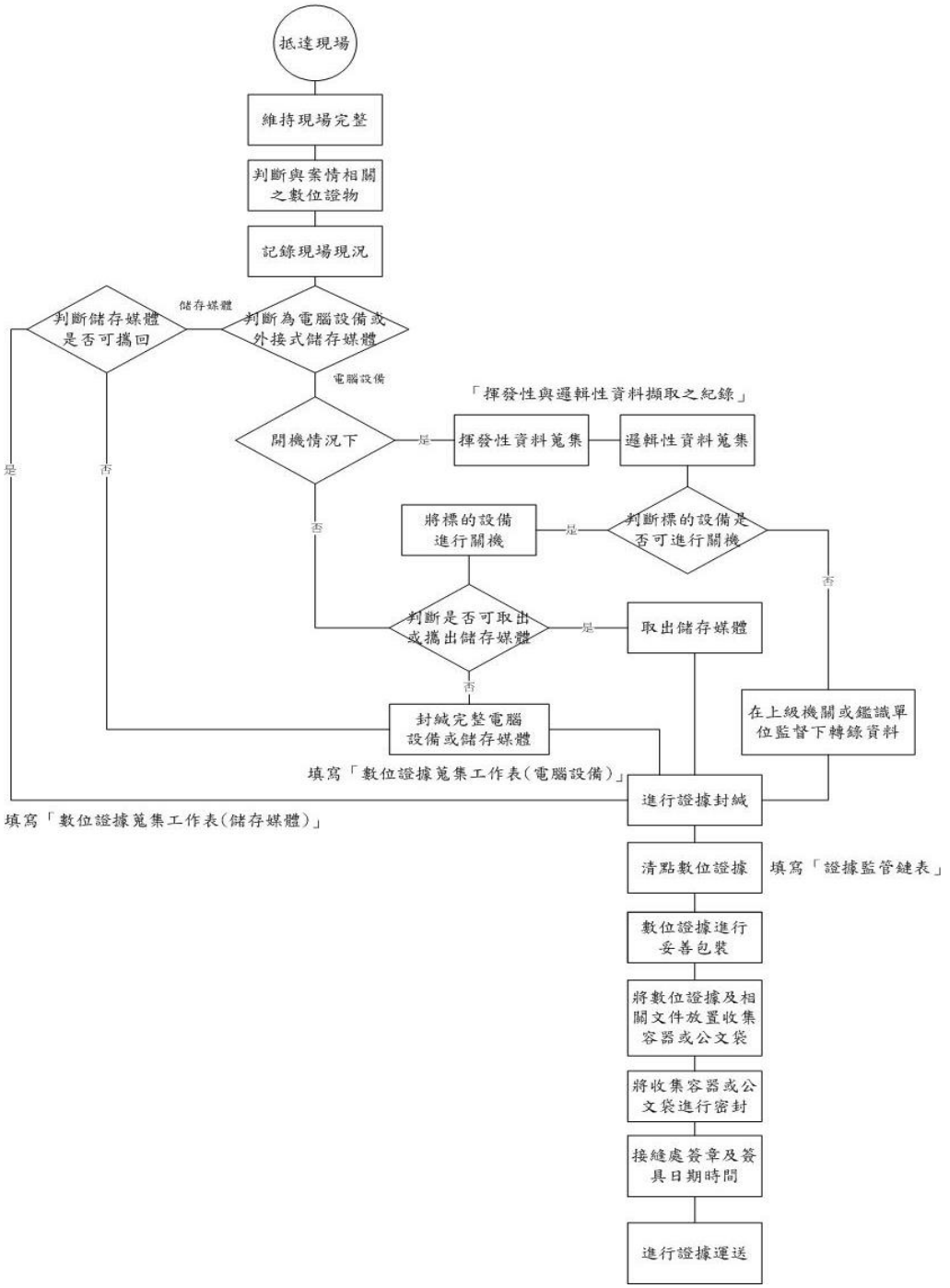

圖1　數位證據保全作業流程圖

參、 第一線人員使用工具簡介

當遭遇到資安事件或個資侵害事件時，為使第一線人員能透過適當工具程式，擷取保存相關之數位證據紀錄，法務部爰於103年辦理開發「第一線人員資安事件反應自動化輔助工具」，其目的在於簡化擷取、蒐集、封存及運送程序，降低第一線人員操作難度，進而保護其證據能力。本工具包含七大功能模組(表1)，適用於目標主機為開機運作中狀態，且該主機可使用USB之情形下。數位證據紀錄匯出至工具載體時，可自動產生對應之雜湊值(MD5 Hash)，便於驗證檔案之正確性及供後續鑑識分析使用。

表1　七大功能模組說明

模組	功能
1. 系統日誌篩選及匯出模組	將系統日誌自動匯出至檔案，並可篩選特定事件屬性，呈現於報告中。
2. 作業系統資訊匯出模組	自動蒐集所有系統相關訊息，如作業系統版本、帳號列表、系統時間等。
3. 作業系統註冊碼匯出模組	將目標主機所有系統註冊碼匯出，供往後鑑識分析比對使用。
4. 網路狀態資訊匯出模組	記錄現場網路相關狀態，包括使用中網路埠、路由表、ARP 表等。
5. 執行中程序匯出模組	將目標主機正在運行中之執行程序列表匯出，供往後鑑識分析比對使用。
6. 記憶體資料匯出模組	將記憶體內容存為映像檔。
7. 報表產出模組	以報表方式呈現上述各項蒐集作業結果。

在蒐證步驟上，蒐證人員首先須輸入案件基本資訊，接著在功能選擇清單勾選要執行的功能項目，隨後呈現蒐證進度畫面與蒐證結果報表(圖2)。利用工具執行數位證據蒐集作業後，會將所蒐集之檔案存於以模組命名之資料夾中，並計算個別檔案之雜湊值。隨後將個別模組之資料夾分別製作不可變更之數位證據映像檔，並於報告中呈現各模組證據映像檔之雜湊值。第一線人員列印執行結果摘要時，須將工具自標的主機拔除後於另一台主機上列印該報表，以避免影響標的主機狀態(圖3)。

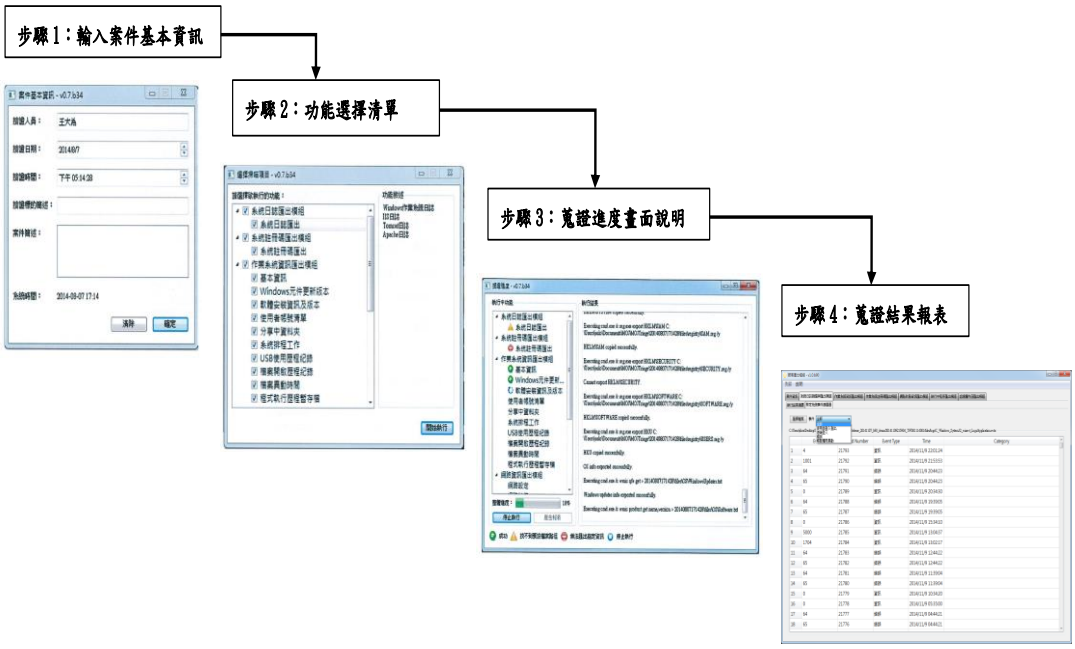

圖2　自動化輔助工具蒐證步驟

圖3　操作流程示意圖

肆、 未來展望

有鑑於資安事件的發生，小則影響機關正常運作，大則甚至威脅國家安全。因此，法務部依循行政院所指示，於103年完成「政府機關(構)資安事件數位證據保全標準作業程序」草案，後續將依各相關機關所提意見修正，報請行政院核定後供各機關依循。法務部預定於104年將已開發完成之「第一線人員資安事件反應自動化輔助工具」派發該部所屬機關，先由該部及所屬機關依數位證據保全標準作業程序草案和所派發之第一線人員工具試辦，並規劃擴充自動化輔助工具之功能，將工具所蒐集之數位證據進行初步分析，俾瞭解資安事件發生之初步原因及嚴重程度，以作為後續處理之參據。後續也將依循行政院主計總處推動「資訊資源整合共用系統」之理念及期程，推動各政府機關試辦及推廣作業，使各政府機關使用一致性的工具與完善的數位證據保全標準作業程序，俾對後續資安事件調查工作有所助益，以強化國家資通安全能力。