因應個資法實施後應有之作業程序建議

陳受湛[1] 鄭健行[2] 吳佳翰[3] 宋子莉[4]
法務部調查局資通安全處 勤業眾信聯合會計師事務所
[1]dan-chen@seed.net.tw [2]safenet@mjib.gov.tw [3]chiahwu@deloitte.com.tw
[4]lsung@deloitte.com.tw

摘要

本研究係針對組織為因應法規要求之紀錄軌跡、證據保存、舉證責任與查明義務，所應有之作業程序進行研究。除瞭解我國相關現行法規所要求內容與歸納組織所面臨之困境，並探討國際間公信組織的數位鑑識作業程序做法。綜理各國觀點與考量民間組織能力，進而建議出事前之數位資料留存、事發之數位證據保全、事後之數位證據分析與呈現，此三種情境適用之作業程序。

關鍵詞：稽核軌跡資料留存、證據保全、證據分析與呈現

壹、前言

我國近幾年各種組織單位發生之個人資料侵害事件時有所聞，動輒影響無辜民眾之個人隱私備受侵擾，更甚者則造成重大金錢損失。當個人資料侵害事件發生後，組織是否已做好足夠之應變措施準備，才能保護民眾之個人資料安全，以免組織與社會日後付出更大的成本代價。

我國個人資料保護法於 2010 公布後，開始納入個人資料侵害事件的查明義務及個資持有者的舉證責任要求**錯誤! 找不到參照來源。**，方使各界關注起數位鑑識技術在民事案件可協助保全數位證據與後續分析調查之運用。然而除了事後的追查專業技術，目前普遍民間單位組織情況為並無證據體質良好之資訊環境，且常見情形為並未事前保留足夠與有效稽核資料，因此縱使有專業技術人員之進駐調查，亦有無從著手追查之遺憾。

本研究報告即希望透過結合國內外相關經驗之分析，研擬具體可提供組織單位因應個資法需求之作業程序，針對事件發生前之數位證據留存、事件發生時之數位證據保全及事件發生後之數位證據分析的議題，探討適用於政府機關及民間企業之數位鑑識標準作業程序，最後提出具體做法及建議，希冀其研究結果得以協助政府機關與民間企業面對個人資料外洩事件時，能確保所留存之數位證據可具備證據能力並提升其證明力，以降低訴訟風險並符合證據管理之需求。

本研究報告在研究架構、研究方法上，力求專業與完整，在資料蒐集上力求充分詳實，但有其限制與範圍：於事前留存方面，因欲達成完整之證據留存效果，必須考量各組織之環境規模與資源設備現況，並非能以單一任務作業即可完成，故本研究僅於資料留存

作業程序之整體設計上，提出較為大方向之觀點與說明。另針對事後證據分析方面，因現行作業系統平台種類眾多無法一一列舉，本研究僅針對最常用之 Windows 與 Linux 作業系統平台兩類進行探討說明。

貳、 文獻探討

一、作業程序

美國 FEMA 組織對於作業程序之定義[2]為：一份完整的參照性文件，為執行一項功能或一些相依性功能而詳細描述其步驟。制定作業程序之目的為，讓組織從事某項任務時能夠有所明確依循，以減少人員執行時因知識不足所造成錯誤產生，並能提高人員執行效率。

為達成對組織有明確效益，作業程序一般係基於下述功能與特性而設計，如提供細節、指定應達成的分派工作、將一般人員需要瞭解的資訊載明、闡述人員如何執行的指導內容，藉以明確規範達成任務的各個步驟。

二、相關法規

於個人資料保護法施行後，擁有龐大電子資料的企業對於數位鑑識之意識也逐漸覺醒，綜觀近幾年相關法規的修法趨勢，於法條內容方面亦逐步帶入了鑑識調查觀點，分別說明於下：

（一）個人資料保護法及施行細則

行政院於民國 101 年 10 月 1 日實行個人資料保護法，其主要與個人資料事件應變相關之要求條文有三：

1. 個人資料保護法第 12 條

「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」此條表示若個人資料侵害事件發生，組織有責任義務進行查明與通知。因此，數位鑑識調查與分析對於組織有其必要性，無論是採用內部具備或與外部合作，才能在事件發生時立即啟動，掌握調查之黃金時間，對於組織查明真相才會有最大效益。

2. 個人資料保護法第 27 條及施行細則第 12 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。」第二十七條所定義之所謂安全維護措施，其定義於施行細則第 12 條進行補充說明。其中第二項所述「前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：」，並具體闡明於第四款：「事故之預防、通報及應變機制」、第九款「資料安全稽核機制」與第十款「使用紀錄、軌跡資料及證據保存。」第 12 條所定義組織應執行事項中，除了要求組織對於個人資料侵害事件需做好應變準備外，另包含對於個人資料的安全稽核、使用紀錄、軌跡資料及證據保存，組織都應有相對應的準備措施。

3. 個人資料保護法第 29 條

「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。但能證明其無故意或過失者，不在此限。」第 29 條所透露之法規精神即為「舉證責任倒置」，其用意為將證明故意或過失的責任移轉至持有個人資料之組織中。倘若組織未曾留存系統日誌或稽核軌跡，則無法提供具有舉證價值之相關證據，亦不能證明組織具備合法資料存取與適當保護之行為。

（二）個人網路銀行業務服務定型化契約範本

行政院金融監督管理委員會於民國 101 年 10 月 8 日所公告，針對銀行與網路銀行客戶間之協議進行規範，其中對於個人資料保護與調查責任也有明確要求。

1.契約範本第 15 條（電子文件之合法授權與責任）

「銀行接受前項通知前，對第三人使用該服務已發生之效力，由銀行負責。但有下列任一情形者，不在此限：一、銀行能證明客戶有故意或過失。」「針對第二項冒用、盜用事實調查所生之鑑識費用由銀行負擔」由此條文可看出，無論是查明事件真相或釐清責任藉以保護自我，組織皆需負起發動調查之義務。

2.契約範本第 16 條（資訊系統安全）

「銀行及客戶應各自確保所使用資訊系統之安全，防止非法入侵、取得、竄改、毀損業務紀錄或客戶個人資料」「第三人破解銀行資訊系統之保護措施或利用資訊系統之漏洞爭議，由銀行就該事實不存在負舉證責任。」在範本第 16 條之要求，與個人資料保護法相似精神為對於資訊系統安全有必要之保護要求，且就侵害事件發生時，需負起自我舉證之責，以證明組織確實做到良善管理。

三、個資法施行後組織面臨數位鑑識現況問題

無論是基於何種法律要求稽核軌跡之留存，都說明企業於科技環境中使用之稽核日誌（Audit Log）在調查中扮演了非常重要的角色。以往組織可能因為效能（Performance）或成本（Cost）的考量，一般都將記錄稽核日誌的功能關閉，當組織為因應個資法欲開啟稽核日誌功能時，通常面臨到不少問題，如稽核日誌應該保留多久、所開啟稽核日誌是否足夠因應個資法要求...等，更需針對組織現況而進行更深入探討。

組織擔負起舉證責任義務在近年修訂之法律中時有所見，似乎成為對於組織社會責任要求之一環。一般民眾身為客戶或消費者的相對弱勢，在事件發生時，法律期待組織身為資源豐厚的一方，應負起主動舉證的責任；而面對訴訟爭議時，組織是否做好舉證環境準備、是否能有效確認相關系統設備、是否已留存足以識別需查明對象之證據及紀錄、組織如何能提供善良管理之證據，皆值得作為組織投入資源的考量要點。

組織面對法律規範之查明要求，於個人資料侵害事件發生時，組織要如何進行應變，另外假若內部並無籌備數位鑑識能量，也無相關資源/環境/工具/能力/標準程序，又如何把握第一時間儘速查明事件發生之原因。

本研究基於組織因應個資法而普遍面臨之挑戰，針對數位鑑識作業程序進行探討，以期對於「事前留存」、「事發保全」與「事後分析與呈現」三方面提出建議。

參、國際間數位鑑識作業程序探討

一、事前留存相關作業程序探討

在事件發生之前，組織應如何確認稽核軌跡留存之足夠與有效，在美國國家標準研究院所公布之 NIST SP800-92 電腦安全日誌管理指引[3]中，其主要探討組織在規劃自身稽核日誌管理時，應有哪些做法，並考量哪些要點，以確保稽核軌跡對於組織能發揮最大的效益。該指引探討了稽核軌跡管理的相關議題，其中與事前留存作業最相關者，分別為日誌的產生/儲存與日誌的安全防護。

在組織審視稽核軌跡在資訊環境狀態時，通常會遇到的困境為日誌的巨量性與多樣性。隨著組織的成長，各種層面平台的軟硬體設備、應用系統等每日都可能產生大量稽核日誌而需要巨量儲存空間，而各家廠商的呈現內容不一、產出格式不一，都可能造成管理與檢視的複雜性與負擔。

因此在對應此項議題，組織在設計稽核軌跡留存環境時，就必須先依序釐清組織現行資訊環境下，確實需要利用稽核軌跡紀錄監控的標的為何？如何在組織資源與最佳監控間取得平衡？並加以檢視稽核軌跡內容可記錄的事件及所呈現的資訊是否足夠？且格式是否能轉換一致？才能確保稽核軌跡在組織環境下的充分性。

而在日誌活動的生命週期中，日誌的產生、傳輸、儲存與歸檔等動作，所面對的議題則為機密性、完整性與可用性的可能損害，是否可能蓄意修改或刪除，是否因容量滿載而自動覆蓋或停止記錄，是否因未導入集中管理設施而於系統損毀時有日誌資料丟失。

組織資源充分的理想狀態下，現行的自動化工具可能提供上述在機密性、完整性與可用性三方面的保護，因現行組織的資料量龐大，單憑人工手動解讀對於通常身兼稽核日誌分析工作的網路/系統/資安人員而言，確實為執行上的重擔且有獨立性遭質疑的風險。

針對以上兩項議題，NIST 指引所提出的稽核軌跡留存方式為以下程序：

1.認稽核日誌管理範圍：要求先行瞭解資訊環境，明確釐清組織監控與記錄的需求範圍。
2.制定稽核日誌管理方式：定義組織的稽核日誌管理政策，確認稽核日誌管理遵法現況，並對現況加以審查。
3.建置稽核日誌管理設施：評估實際環境需求資源，導入足夠軟硬體設施。
4.專責人員設置：專責人員之培訓與技術能力強化，及日誌管理工具操作培訓。

二、事發保全相關作業程序探討

在事件發生時，組織關注之焦點將轉降如何保存證據，才能確保其證據能力在法庭上可接受，期間有關之任務內容包含出勤前之準備，與封存、運送證據等部分，本研究探討了國際間較為公信組織所發佈之證據保全相關作業程序，包含 ISO/IEC、英國警察協會、與美國國家司法研究院等組織各自發佈與證據保全相關之作業程序，分別歸納出共通性原則與個別特色要點：

（一）共同基本原則

1.確保數位證據未受外力影響：由於數位證據擁有易遭改變、毀損、破壞與易被時間影響[4]之特性，故在處理上亦必要格外地強調數位證據之完整性，以保全其證據能力。
2.執行人員須有專業能力：由於數位證據之蒐集、分析過程皆有可能導致原始資料之改變(如 1.所述之特性)，故當須存取原始資料時，應確保人員之能力足以實作且可以說明即將進行之行為與證據之關聯性為何[5]。
3.證據鏈之紀錄完備：如 1.所述之特性，數位證據之處理過程中之每一道程序皆應被完整記錄下來(即證據監管鏈[4])。以備第三方得以依據留存之紀錄重現程序並得到相同的結果[5]。如此以驗證數位證據之正確。

（二）ISO/IEC 27037：2012

ISO 27037 主要以鑑識九大原則為主軸：證據鏈監管原則、現場處理注意事項、角色與職責、人員能力建議、謹慎處理原則、文件化要求、勤前會議簡述、證據蒐集及擷取優先序、數位證據保存。除前述與共同基本原則章節內容一致者外，將其標準之特點分述於下：

1. 現場處理注意事項：為保持現場之完整，該規範要求應設置現場管制負責人以確保管制現場進出與證據之存取，除隔離嫌疑人員與現場的接觸外，並應記錄現場環境與設備狀態，並管制設備現況與相關資訊等。
2. 角色與職責：ISO/IEC 27037 該標準規範將涉及數位鑑識證據保全作業程序之人員分為兩種角色，其一是數位證據一線應變人員，主要職責為數位證據辨識、蒐集、擷取與保存，包含數位證據蒐集及擷取報告內容編列、數位證據保存及處理；其二是數位證據鑑識專家，具備專業鑑識職能，主要在一線人員面臨無法處理情形時，提供技術性協助，例如複雜之伺服器架構或磁碟陣列儲存裝置等。
3. 文件化要求：要求詳細記錄操作動作與所存取之資料名稱、螢幕顯示畫面、目標設備之廠牌、型號、規格等資訊，並建議可用攝影方式記錄。
4. 勤前會議簡述：由於進行證據保全時，現場環境情況可能無法預料，因此必須先透過勤前會議討論案情方向、處理證據類型、人員職責分工、異常狀況處理對策等。
5. 證據蒐集及擷取優先序：若電腦主機是開機狀態，則非必要時不要關閉電腦主機。揮發性資料，如 RAM、Cache RAM、Register、主機正在執行中的程序、網路連線與應用程式開啟通訊埠等，可能因關閉主機而資料就此消逝無法回復。
6. 證據封存、運送及儲存：在證據取得完畢後，在證據封存時應有明確標示記錄與阻隔防護性包裝；在證據運送過程中應處於受到監管與保護之環境；最終於證據儲存地點，應確保實體與防護之安全性。

（三）數位證據良好實務指引

主要重要分為四大部分：數位證據處理原則、犯罪現場注意事項、網路鑑識與揮發性資料、向內部調查人員進行簡述。除與共同基本原則一致之處外，其餘重點分述如下：

1. 現場處理注意事項：在現場處理時，該規範所關注的是電腦關機與開機狀態下的不同處置，以及運送時的狀態保護與儲存時的防護環境狀態。
2. 網路鑑識與揮發性資料：於某些情況下，目標主機仍在運作狀態時，須對設備擷取相關揮發性數位證據，如存在於記憶體內資料，此時須謹慎處理以避免對證據造成不必要之變動。

（四）NIJ 電子犯罪現場調查

一線應變人員指引[4]，所闡述之作業要點與前述文獻要點相似，惟在證據擷取部分有細部說明為其特色，簡述如下：

1. 應確保檢查人員的鑑識用儲存裝置是事先鑑識性抹除過。
2. 當對證據資料存取時，皆應使用具防寫功能之方法存取。
3. 應取得調查儲存媒體的實體大小與邏輯大小以確定所有配置空間，包含主機保護資料區域，或是否有刪除分割、硬碟序號等資訊。
4. 應使用適當鑑識專用軟硬體擷取目標證據至檢查人員的儲存裝置。
5. 比較原始與複本的 Hash 驗證值以確認是否成功擷取。

三、事後分析與呈現相關作業程序探討

本研究綜理數位國外學者所發表之證據分析相關作業程序，以及知名組織提供之分析結果呈現指引，以下討論將分為證據分析與證據呈現兩部分進行說明。

（一）數位證據分析

證據保全之後，立即會遭遇到的問題即是如何處理儲存媒介上之檔案，如：已刪除之檔案、資料夾中之檔案、檔案中之檔案或在其他容器。而儲存媒體分析的目標就是：識別(Identification)、取出(Extraction)、分析(Analysis)在儲存媒體上之檔案。

於個人資料侵害之情境下，只要經過電腦與網路之使用即可在電腦之作業系統與網路行為之稽核軌跡上找到與事件相關之稽證。故以下就作業系統(Windows、UNIX/Linux)分析與網路行為分析分別討論：

1. Windows 作業系統主要奠基於 2 種檔案系統之上——FAT 與 NTFS。此二種檔案系統所留存之資訊不盡相同，但可比較如下：
2.

3. 表 1 Windows 檔案系統提供資訊

檔案系統	**FAT**	**NTFS**
提供資訊	➢ 檔案變更、存取、建立時間 ➢ 已刪除或未刪除	➢ 檔案變更、存取、建立時間 ➢ 已刪除或未刪除 ➢ 檔案或資料夾 ➢ 檔名變更、存取、建立時間 ➢ MFT 對應欄位最後變更時間

於檔案系統之上，Windows 作業系統仍保有許多可供鑑識人員取得案件資訊之紀錄，如：登錄檔(Registry)、Prefetch Files、捷徑、事件日誌(Event Log)、Hibernation Files、排程工作(Scheduled Tasks)等。以下逐項分述其可於案件中提供之資訊：

- 登錄檔(Registry)：Windows 登錄檔紀錄系統與使用者之設定值，以便提升使用者之使用經驗。但也因此對使用者之行為留下了許多可追溯之紀錄[6]。
- Prefetch Files：Prefetching 是 Windows 為了提高程式反應速度，而於將程式執行期間可能需要之資料先行搬移至特定位置之功能。
- 事件日誌：事件日誌功能與 Windows 之稽核設定極為相關，意即不同的稽核設定將有不同的事件日誌產生[7]。事件日誌系統不僅可以依稽核設定對眾多系統事件進行記錄[8]，而事件內容資訊亦可供數位證據分析之用。
- Hibernation Files：此種檔案主要為記憶體資料之壓縮，通常出現於筆記型電腦之 Windows 系統中，故 Hibernation Files 含有許多過去特定時間點之系統狀態資訊[7]。
- 排程工作：此為 Windows 提供使用者可自行排程自動執行程式之功能。但此功能之使用需具有系統管理員之權限方可，且排程之工作將以 System 之特殊權限執行。亦因此可能有部分部惡意程式或行為將透過此功能實作。因此，排程工作工作之 Job 檔與日誌(Scheduled Tasks Log)可提供系統之運行時間資訊，亦有助於數位證據分析之用。
- 系統還原點：屬於 Windows 環境之特有功能，相關檔案亦有助於數位鑑識人員對過去特定時間點之系統狀態(包括：登錄檔、系統檔案)等之比較與檢視。

4. UNIX/Linux 作業系統分析：Linux 雖可以支援多種檔案系統，包括 Ext2、Ext3、ReiserFS、XFS、JFS**錯誤! 找不到參照來源。**等。但其仍以 Ext2 與 Ext3 為主要使用之檔案系統；而 UNIX 系統所使用之檔案系統亦不一而足，如：UFS、ZFS、JFS、HFS、HFS+、XFS、ODS-5 等。各檔案系統之設計略有不同，先以較常見之檔案系統資訊說明如下表。

表 2 Linux 檔案系統提供資訊

檔案系統	Ext2	Ext3
提供資訊	➢ 最後寫入時間 ➢ 最後掛載時間與掛載點 ➢ 磁碟區塊(Block)之 inode 編號 ➢ 物件權限(包含使用者、群組) ➢ 物件變更、存取、刪除時間 ➢ inode 變更時間	➢ 最後寫入時間 ➢ 最後掛載時間與掛載點 ➢ 磁碟區塊(Block)之 inode 編號 ➢ 物件權限(包含使用者、群組) ➢ 物件變更、存取、刪除時間 ➢ inode 變更時間、資料 ➢ 檔案變更之資料

Ext2/Ext3 與 Windows 之檔案系統不同之處為，當資料被寫入磁碟區塊時，磁碟區塊未被資料寫入之部分皆會以 0 填入。因此在 Ext2/Ext3 檔案系統中，無法像 Windows 之檔案系統一般可藉由磁碟區塊未被資料寫入之部分重組資訊。

在 Linux 檔案系統之上，亦有許多檔案可以協助數位證據分析，如：passwd 檔、group 檔、shadow 檔、使用者活動紀錄、系統日誌(Syslog)、排程工作、Shell 紀錄等。以下便就此些檔案說明其可提供之資訊：

- passwd 檔：雖然其名稱意思為 password 之縮寫，但實際上該檔案並無儲存密碼之雜湊值，僅具有帳號與使用者目錄等相關資訊。
- group 檔：此檔與 passwd 檔相似，只是儲存帳號所屬群組之訊息。
- shadow 檔：shadow 檔才是使用者密碼之雜湊值儲存處，包含使用者密碼設置相關資訊。
- 使用者活動紀錄：使用者活動紀錄包含 utmp、wtmp、lastlog 主要紀錄使用者之登出/入系統之時間與狀態。
- 系統日誌：Linux 作業系統在不同之服務下會留下許多不同之日誌，關於系統發生事件之稽核軌跡皆有助於數位鑑識分析[9]。
- 排程工作：如 Windows 作業系統所提及，此項功能常為惡意程式所利用，若鑑識分析之方向為惡意程式，則排程工作之檔案應被詳細檢視。

5.網路行為分析：

現今網路上之通訊行為已非常多樣，但除卻需要專屬應用程式之方式外(如：Skype)，大部分之網路行為皆透過瀏覽器或電子郵件居多。

- 瀏覽器：由於現今雲端技術之盛行，所有服務皆以實作在網頁上以供使用者方便存取。瀏覽器記錄可以提供使用者上網行為之紀錄，藉以推測使用者之意圖與動機。
- 電子郵件：通常提供資訊除了電子郵件之內文與附件外、其所寄出之時間、收件者、自動完成使用者信箱、通訊錄皆為可以提供分析標的。

（二）數位證據呈現

由於閱讀報告之人可能不具備相關技術背景，故數位證據之呈現中亦應包括技術術語之定義與技術之簡介。若需具一定背景概念方能了解呈現報告時，也應加入背景概念之說明[10]。以下依 Brad Garnett 之舉例[11]說明呈現之要點：

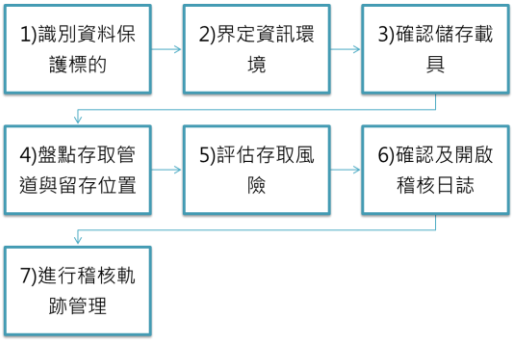
1.概述/案件簡述：概述數位證據之來源、案件起源與欲以數位鑑識找尋之資訊。此部分亦可能涉及到部分證據監管鏈之描述、數位證據之初始狀態為何。
2.鑑識擷取與檢驗準備：主要是針對數位證據之擷取與保存之步驟描述。換言之，此部分即是描述收到數位證據之開始與擷取之結束。另外為求後續可再次驗證，亦應附上數位證據之雜湊值。若可行，可以照片闡明此部分之步驟描述。

3.發現與報告(鑑識分析)：此部分應提及所使用到之工具、步驟以及在各步驟中所發現之資訊。若可行，亦可以提供報告中使用到之圖片、文件之超連結，以便檢視。
4.結論：經過數位鑑識分析後，所得到針對欲找尋之資訊之結論為何。

肆、 因應個資法施行之數位鑑識作業程序規劃

一、事前之數位資料留存作業程序

為能確保各類事件發生後，組織能夠提供有力的數位證據於法庭攻防上取得優勢，本研究歸納前述之探討，提出一套事前留存之作業程序，讓組織可逐步完備稽核日誌的留存，其步驟如圖 1 所示：



（一）識別資料保護標的

確認稽核軌跡留存的第一步，即是識別組織內的資料保護標的，一般而言，企業所定義資料保護標的包含客戶、員工與廠商之個人資料、設計圖、配方、程式碼與組織內的規範文件等…，保護標的文件之定義會依組織營運內容有所不同。盤點的方式可用組織業務流程圖為參考，查看其各單位日常執行的業務中，有哪些資料保護標的。

（二）界定資訊環境

此步驟我們界定所有盤查的範圍，可以以組織內的網路架構圖做為參考依據，劃分出所有保護標的文件可能移動的區域，做為盤點的範圍。舉例來說，盤點的範圍可能包含對外連線之 DMZ 區、OA 區及 Server 區中的各套系統，以及在網段上的各項設備，如防火牆、網站應用程式防火牆（Web Application Firewall，WAF）、路由器（Router）、資料外洩防護（Data Leakage Prevention，DLP）與入侵防禦系統（Intrusion Prevention System，IPS）等等…。

（三）資料保護標的儲存之載具

完成範圍劃分之後，以組織中各部門的業務為基準，確認哪些業務與所定義的資料保護標的有關，從業務流程中找出可能蒐集、處理或利用到的保護標的文件，並且確認該資料保護標的所儲存的載具。以銀行業開戶業務而言，櫃檯人員把客戶所填寫的開戶申請單資料輸入於開戶系統中，並從開戶系統中匯出每日開戶客戶的資料到作業電腦中，做為報表的使用，以這個例子而言，我們盤點到二個與資料保護標的相關項目，包含開戶申請單的資料儲存於開戶系統的資料庫中，與每日開戶報表，儲存於作業電腦中。

（四）盤點存取管道與留存位置

釐清所有資料保護標的與所儲存的載具之後，以資料保護標的所儲存的載具為起點，確認資料保護標的任何可能被存取的「管道」，並盤點這些可取存的「管道」上有哪些「位置」可留存相關的存取記錄，也就是說在以任何方式存取資料保護標的的同時，可以從哪些位置找到「蛛絲馬跡」。這裡所指的「位置」係根據資料保護標的之載具特質與可存取管道的不同，可記錄日誌（Log）的位置也有所不同，此處無法一一列舉，下表僅列出目前於存取管道上較常見可留存日誌的位置。

表 3 各層面日誌留存之位置

層面	留存位置	層面	留存位置
營運流程/端點行為	➢ IM 軟體控管 ➢ 卸除式儲存設備存取控管 ➢ 防毒軟體 ➢ 外部網路連線行為控管 ➢ 非法軟體安全控管	作業系統	➢ Windows ➢ Linux ➢ AIX ➢ Solaris ➢ HP-UX ➢ AS/400
資料庫系統	➢ Oracle ➢ SQL Server ➢ Sybase	應用系統	➢ 客戶管理系統 ➢ 員工考勤系統
其它相關伺服器	➢ WebSphere 網頁伺服器 ➢ Apache 網頁伺服器 ➢ IIS 網頁伺服器 ➢ FTP 伺服器 ➢ 檔案伺服器 ➢ 郵件伺服器	網路環境/資安設備	➢ 防火牆（Firewalls） ➢ 路由器（Router） ➢ 網路應用防火牆(WAF) ➢ 入侵防禦系統（IPS） ➢ 無線網路管理
實體環境	➢ 錄影監控系統（CCTV） ➢ 機房門禁系統		

（五）進行存取管道風險評估

繼上一步驟盤點出所有可留存日誌的位置，組織可依保護標的文件發生事件的衝擊以及可能性，評估優先開啟稽核日誌的留存。風險評估的方式，可依資料保護標的造成事件的衝擊程度（Impact）與發生機率（Likelihood）來評估，其公式如下：

風險=衝擊程度x發生機率

衝擊程度是依資料保護標的的重要性來評估，越重要的資料，若發生事件對組織的衝擊就越高，發生機率是依資料保護標的控管上的強度或組織對於安全管理規範落實的程度來評估，下表列出依衝擊程度及發生機率所評估出的風險：

表 4 風險評估表

衝擊 / 可能性	高	中	低
高	大	大	中
中	大	中	小
低	中	小	小

經過此步驟可優先挑選風險較大的資料保護標的，開啟各位置稽核日誌的留存，並依風險的大小逐一進行留存。

（六）確認及開啟稽核日誌

對於高風險的資料保護標的，根據存取管道上可留存日誌的位置，進行確認各項目日誌留存的狀況，並與下表留存事件做差異分析進行開啟稽核日誌的留存：

表 5 各層面日誌之留存事件

層面	**留存事件**
應用系統（AP）	➢ 使用者帳號登入成功/失敗或登出 ➢ 使用者帳號權限異動 ➢ 使用者針對機敏資料(含個人資料)之存取行為(包含新增、修改、刪除、查詢、產製報表匯出或下載及列印等)
作業系統（OS）	➢ 使用者帳號登入成功/失敗或登出 ➢ 使用者帳號權限異動 ➢ 系統檔案設定異動(如稽核原則設定組態檔案被變更)

	➢ 特權帳號行為 ➢ 切換使用者(如 Unix-Like 系統中之權限轉換紀錄) ➢ 重要檔案變更軌跡
資料庫 (DB)	➢ 使用者帳號登入成功/失敗或登出 ➢ 使用者帳號權限異動 ➢ 特權帳號行為 ➢ 資料庫權限異動行為(DCL) ➢ 資料庫資料調查行為(DQL) ➢ 資料庫資料變更行為(DML) ➢ 資料庫資料定義行為(DDL)
網路相關設備	➢ 登入登出成功/失敗紀錄 ➢ 帳號權限異動紀錄 ➢ 網路連線成功及失敗紀錄 ➢ 網路流量監控紀錄 ➢ 系統組態及規則設定異動紀錄 ➢ 違反規則之警示紀錄
其它 IT 相關設備	➢ 使用者帳號登入成功/失敗或登出 ➢ 使用者帳號權限異動 ➢ 特權帳號行為 ➢ 安全規則或設定異動

其中每一項留存事件，應包括人、事、時、地與物之內容，例如：一個完整的人員登入事件記錄，需包含人員之帳號、來源主機 IP 位址、來源主機名稱、登入時間、目的主機 IP 與目的主機名稱資訊，建議參考文獻[12]需包含的內容以下表所示：

表 6 個別事件之留存內容與面向

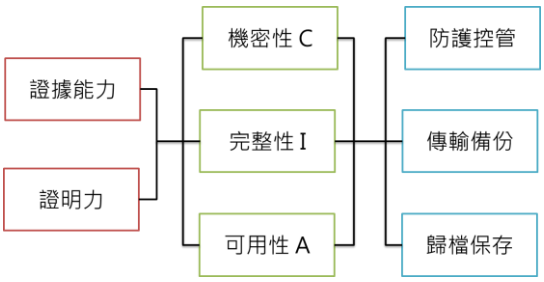
人	**事**	**時**	**地**	**物**
➢ 來源主機名稱 ➢ 來源主機 IP ➢ 帳號	➢ 事件類型 ➢ 執行指令 ➢ 使用程式	➢ 時間 ➢ 日期	➢ 目的主機名稱 ➢ 目的主機 IP ➢ 資料所在	➢ 存取筆數 ➢ 存取檔案/物件 ➢ 回傳結果

（七）進行稽核軌跡管理

數位證據在法庭，講求「證據能力」與「證明力」，所謂證據能力是指，作為證據的資格，而證明力是指能夠證明的程度。為求其達到證據能力的資格，從以下三個原則

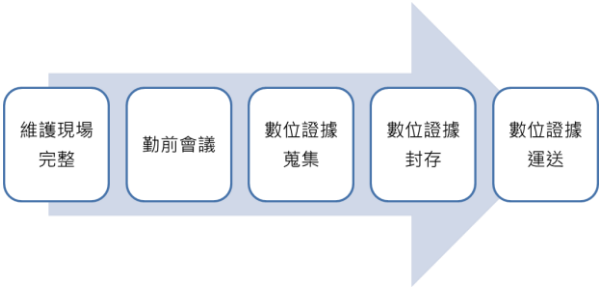
進行稽核日誌的管理[13]：保護標的的機密性（Confidentiality）、完整性（Integrity）與可用性（Availability），對於保護標的機密性及完整性而言，宜考量將組織內之稽核軌跡統一管理，導至後方日誌伺服器（Log Server），需確認傳輸管道之安全性，與日誌伺服器之權限管理。

而完整性的特性在於保證稽核軌跡在傳輸、儲存、分析及備檔的過程中不會被竄改，因此在於進行備檔的同時，利用雜湊函數（如：MD5 或 SHA1 等…）計算稽核軌跡之雜湊值，也是證明其完整性之重要步驟之一。而可用性（Availability）主要在於強調，需要調閱稽核軌跡報表或其原始檔（Raw data）時，能否即時、正確以及完整的呈現，此特性考量到本身其伺服器的效能、回溯的速度及儲存能力，而定期將備檔的資料取出讀取，並計算其雜湊值比較之前所計算的數值是否相等，也是確保其可用性和完整性的重要程序，其稽核軌跡管理之要點，如圖 2 所表示。



二、事發之數位證據保全作業程序

由前述探討的能力審核方法可知，本研究提出事件發生後，民間組織可自行執行之證據保全作業程序建議，其程序分為五個階段，如圖 3 所示：



（一）維護現場完整

1. 應設置暫時現場管制人員：
   - 確保涉及個資外洩事件之目標系統設備附近僅相關人員得進出管制現場、接觸目標設備並記錄進出之原因。

- 在事件應變人員進行數位證據保全之前應保持目標設備之原始狀態，如：本為開機則保持開機。
- 由現場管制人員對現場現況與目標設備現況進行記錄。
- 對設備負責人員之程序動作予以記錄。
-

2. 移除網路之判斷
    - 由於部分事件肇因於網路攻擊或惡意程式之連線。若遇有明顯刪除證據之行為則應考量是否移除網路。部分系統可能因其重要性而無法即時移除網路。可徵詢系統管理人員是否有備援機制以暫時移除目標設備之網路。
    - 若無法即時移除網路，仍應了解是否可以對該網路封包進行側錄。以備日後了解該網路輸出/入對目標設備之影響為何。

（二）勤前會議

1. 前置作業：應先對出勤使用之鑑識設備清點並確認其功能正常。
2. 案件資訊說明：
    - 確認本次現場數位證據保存主要方向及任務。
    - 本次事件資訊提示：包括事件類型、事件相關日期及時間、數位證據可能類型及其蒐集、封存及運送要求、相關紀錄填寫重點提示。
3. 人員任務分工：應至少包含現場管制、記錄攝影、鑑識作業三種職責

（三）數位證據蒐集

1. 維護現場完整
2. 記錄現場與目標設備現況
3. 資料蒐集 – 揮發性資料
    - 如相關標的設備處於開機狀態下，現場鑑識人員應使用現場數位證據蒐集工具取得揮發性資料。
    - 應確保現場鑑識人員具備一定專業能力，且對於所採取的每一個動作都必須能解釋其動機、目的與關聯性。
    - 應透過執行現場數位證據蒐集工具方式取代人為直接對目標系統進行操作作業。
    - 揮發性資料蒐集完畢後，應透過現場數位證據蒐集工具產生其對應之雜湊運算值。並對每一項揮發性資料給予證據編號。
    - 攝影紀錄人員應對揮發性資料蒐集之步驟進行完整記錄。

- 將所蒐集之揮發性資料進行證據封存。

2. 資料蒐集 -邏輯性資料蒐集
   - 除揮發性資料之蒐集外，尚應取得目標系統之事件相關邏輯性資料。
   - 針對防火牆設備、入侵偵測或防禦設備等其他相關設備，應匯出相關稽核日誌檔案。現場鑑識人員應將其存放於現場數位證據蒐集工具內。
   - 應透過執行現場數位證據蒐集工具方式來代替人為直接至系統進行操作作業。
   - 邏輯性資料蒐集完畢後，應透過現場數位證據蒐集工具產生其對應之雜湊值並紀錄或儲存之。
   - 現場鑑識人員應將其邏輯性資料蒐集過程詳細記錄，以供後續查證蒐集程序。
   - 應確保現場鑑識人員具備一定專業能力，且對於所採取的每一個動作都必須能解釋其動機、目的與關聯性。
   - 攝影記錄人員應以錄影或拍照方式記錄邏輯性資料蒐集之步驟。
   - 將邏輯性數位證據資料進行證據封存。
3. 電腦設備或儲存媒體蒐集
   - 標的設備有儲存媒體或有其他外接式儲存媒體存在時，現場鑑識人員應將之取出儲存媒體並攜回。
   - 無法取出其儲存媒體時，現場鑑識人員應攜回完整標的電腦設備。
   - 如須將標的設備進行拆卸並將其儲存媒體取出時，攝影記錄人員須針對儲存媒體拆卸及取出過程進行拍攝。
   - 現場鑑識人員應將其數位證據蒐集結果詳細記錄。
   - 所攜回之電腦設備或儲存媒體須依數位證據封存程序進行證據封存。
4. 現場製作儲存媒體複本
   - 如系統於可關機情況下並可取出其儲存媒體，但不能將其儲存媒體攜出時，應直接於現場透過儲存媒體複製設備進行儲存媒體複本製作作業。
   - 現場以製作儲存媒體複本為主，待攜回儲存媒體複本後再於鑑識分析環境內進行證據映像檔製作。
   - 如須將標的設備進行拆卸並將其儲存媒體取出時，攝影記錄人員須針對儲存媒體拆卸及取出過程進行拍攝。
   - 攝影記錄人員應以錄影或拍照方式記錄儲存媒體複本製作之步驟。
   - 儲存媒體複本製作完畢後，應計算其對應之雜湊值。
   - 應將媒體複本所儲存媒體種類、廠牌、型號、序號及儲存容量等相關資訊及儲存媒體複本製作結果紀錄。
   - 所製作之儲存媒體複本須依數位證據封存程序進行辦理。

（四）數位證據封存

1. 現場鑑識人員應確實清點要攜回之數位證據項目及數量。對每一項數位證據皆應維護其「證據監管鏈」，所有經手證據之人員皆應填寫。
2. 攝影記錄人員應將要封存之數位證據及其所紀錄之資訊進行拍攝。
3. 數位證據封存步驟：
    - 現場鑑識人員應將所有數位證據以防靜電之方式密封並註明密封日期、時間及現場鑑識人員。
    - 每一項數位證據皆應於封存之材料表面標示證據相關資訊。
    - 每一項數位證據之運送包裝(如：防靜電袋或其他容器)上亦應密封並註明密封日期、時間及現場鑑識人員。並附以證據監管鏈相關表格以便維護「證據監管鏈」。
4. 數位證據封存時，應防止數位證據被彎曲、對折或其它造成損壞之情況。

（五）數位證據運送

1. 數位證據運送重點
    - 應保持數位證據遠離磁場，如無線電發射設備、揚聲器等。
    - 應注意溫度與濕度之變化，勿將數位證據放置於高溫或直接日照強光等熱源下。
    - 應避免遭液體潑灑或接觸。
    - 應避免運送過程中發生重大衝擊與震動。
2. 證據監管鏈要求
    - 應符合證據監管鏈要求：每件數位證據運送過程中，無被篡改等不當行為發生之可能性，證據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相關表單，包含交件人、收件人、日期時間及目的等資訊。
    - 現場鑑識人員應填寫證據監管鏈相關表單，並將表單附於證據運送包裝上。
    - 應確認數位證據運送過程中皆全程進行監看作業。

三、事後之數位證據分析與呈現作業程序

（一）數位證據分析

在個人資料侵害事件中，可能透過許多途徑造成侵害之發生，如：電子郵件外洩資料、木馬程式入侵盜竊資訊、網頁上傳外洩個人資料。而不同之途徑在電腦設備中所留

下之紀錄亦有所不同。以下建議，尚未了解案件之侵害途徑可用下述功能先行實作：

1. 資料回復：將標記未配置之空間、已刪除之分割磁區中將資料回復為原本之資料形式。
2. 關鍵字搜尋：以與案件有關之關鍵字對目前可識別之資料進行搜尋，如：被外洩個資之資料內容(姓名、身份證字號等)、可疑網址等其他可能線索。
3. 簽章分析：針對可能隱藏線索之檔案類型、內容進行比對。如：欲檢驗是否有惡意軟體植入以 System 權限執行之工作排程，則搜索 JOB 檔是否存在。此類技術利用比對檔案標頭或雜湊值以比對檔案類型，若對於被修改副檔名以隱藏之檔案仍能有效比對。
4. 檔案分析：另外針對不同之個人資料侵害途徑可能都會留下不同之紀錄。值得一提的是「網路行為」因為經常是數位證據分析的一項重要標的。故目前市面上或開放原始碼社群中亦有以此功能為主之分析軟體。其他針對不同資料類型之分析功能尚有：記憶體分析、事件日誌分析、登錄檔分析、惡意軟體分析。
5. 時間序分析：最後，在各項證據之發現下，最重要之資訊之一為「時間點」。不同的時間點可串連為一時間線。故亦有「時間線分析」之功能可協助調查。

（二）數位證據呈現

由於數位證據呈現主要之目的在於：客觀陳述經數位鑑識分析所得到之客觀事實及其結論。故內容應力求詳細與客觀，但結論應以簡明扼要地敘述重點，故建議以如下為數位證據呈現之架構：

1. 案件資訊簡述：描述案件之概況與數位證據在案件中之定位為何。
2. 鑑識需求：描述欲自數位證據中鑑識之資訊與欲證明之事實為何。
3. 證據描述：數位證據在送至分析人員時之狀態描述。
4. 名詞定義與背景概念：定義與描述報告中出現之技術名詞與其他應具備之背景概念。
5. 資料擷取：描述將資料自證據中擷取出之步驟與技術為何。
6. 鑑識分析工具：描述於鑑識分析步驟中所使用到之鑑識分析工具。
7. 鑑識分析發現：描述各鑑識分析之步驟與於步驟中發現之資訊。
8. 結論：將鑑識分析發現中所發現之資訊統整並陳述統整後之結論，對鑑識需求進行回覆。
9. 附件：若有需要額外參考之文件可置於此部分。

伍、結論

一、結論

個人資料保護法之施行對我國各種組織單位影響甚鉅，為能有效因應相關之遵法要求，唯有適用作業程序之建立，得以協助民間單位組織做好個人資料保護，並將風險與損失降至最低。依據本研究報告之動機，針對「事前之資料保存機制」、「事發之證據保全機制」、「事後之證據分析與呈現機制」三方面進行研究，達成之目的如下：

1. 在事前之資料保存方面，分析國際組織提出之稽核日誌保存管理方式與實務作法，提供適用於各類組織單位的數位資料留存作業程序。
2. 在事發之證據保全方面，探究現行國際標準與公信單位提出之現場證據保全指引，研擬適用於各類組織單位的數位證據保全作業程序。
3. 在事後之證據分析與呈現方面，縱理國際知名學者之各方觀點，制定適用於各類組織單位的數位證據分析與呈現作業程序。

二、建議

本研究所提出之三階段作業程序，建議可作為日後民間組織實施個人資料保護機制之一環，首先可協助組織建立數位證據良好環境，在日後無論是個資侵害抑或是他種資料危害事件，都能透過有效的事前資料留存，以提供豐富的調查資源。此外，在組織欲自行養成數位鑑識調查能力時，可透過證據保全作業程序達成初步的建置，而藉由證據分析與呈現作業程序可輔助鑑識團隊之能量提昇。

參考文獻

[1] 葉奇鑫、李相臣，“淺談個人資料保護法民事賠償責任及數位鑑識相關問題”，司法新聲第 101 期第 3 篇，2012 年，頁 33~49。
[2] Federal Emergency Management Agency(FEMA), “National Urban Search and Rescue Response System Field Operations Guide”, 2003.
[3] National Institute of Standard and Technology(NIST), ”Guide to Computer Security Log Management”, 2006.
[4] National Institute of Justice, “Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition”, April 2008.
[5] Association of Chief Police Officers, “Good Practice Guide for Digital Evidence”,

March 2012.

[6] L. W. Wong, "Forensic Analysis of the Windows Registry", http://www.forensicfocus.com/downloads/forensic-analysis-windows-registry.pdf.

[7] Harlan Carvey, "*Windows Forensic Analysis Toolkit*", Syngress, 2012.

[8] Kaveesh Dashora, Deepak Singh Tomar and J.L. Rana, "A Practical Approach for Evidence Gatheing in Windows Environment", *International Journal of Computer Applications*, vol 5, no. 10, Aug. 2010.

[9] Cory Altheide and Harlan Carvey, "*Digital Forensics with Open Source Tools*", Syngress, 2011.

[10] National Institute of Justice, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement", Apr. 2004.

[11] Brad Garnett, "Intro to Report Writing for Digital Forensics", SANS Blog, 2010, http://computer-forensics.sans.org/blog/2010/08/25/intro-report-writing-digital-forensics.

[12] EPC153-10v1, "*The Use of Audit Trails in Security Systems: Guidelines for European Banks"*, Aug. 2010.

[13] ISO 15489, "*Information and documentation – Records Management – Part 1: General"*, 2001.