從霧裡看花到撥雲見日－談雲端鑑識面臨之挑戰與因應之道

陳威棋／勤業眾信聯合會計師事務所企業風險管理經理

一、前言

近年來，隨著雲端運算快速發展，衍生出多樣而複雜的資訊安全與電腦犯罪議題；因而發生之法律糾紛及資訊安全問題時，使用者要如何因應及面對，更是目前雲端運算領域的熱門議題。本文將先說明「雲端鑑識」的定義，再探討目前雲端運算所面臨，包含技術、法律及管理等層面的相關挑戰，並重點說明國外雲端鑑識相關作業程序。

二、「雲端鑑識」之定義

電腦鑑識科學 (Computer Forensics Science) 一詞係西元 1991 年由國際電腦調查專家協會 (The International Association of Computer Investigative Specialists，IACIS) 首次提出，發展至今已逾二十年，從早期以電腦設備儲存媒體為鑑識目標，迄至目前已擴展為數位鑑識之多元概念。所謂「電腦鑑識」是指在法令規範下，利用科學驗證的方式調查數位證據，經由數位證據的還原、擷取及分析過程，還原事件原貌，以利事件偵查及作為法庭訟訴之依據。而「雲端鑑識」的定義 [參考文獻 1] 係指於雲端運算環境中，使用數位鑑識之作業方式，它包含技術層面、法律層面及管理層面的議題。

三、法律面之挑戰與建議

「雲端鑑識」於法律層面所帶來的衝擊與挑戰包含：跨國司法管轄權爭議、多層承租關係、服務水準協議及相關證據法則之要求等，分別說明如下：

(一) 跨國司法管轄權爭議

管轄權爭議為雲端鑑識調查的首要問題，由於法律上的「行為地」不易判斷，因而產生管轄權的議題；而資料所在位置將影響案件涉訟的起訴地點，也就是哪個法院具有管轄權。

以刑事案件來說，不論是被害人所在地、被告所在地、犯罪行為地或結果地的法院，皆有可能取得刑事案件的管轄權，而管轄權並不

具有排他效力，多數案件皆可能同時有數個法院可取得合法的管轄權。若案件涉及不同法院的管轄權，選擇哪一個法院起訴即屬於政策選擇的問題。

至於民事案件，當事人可能因為違反契約義務而提起民事爭訟，此類涉及當事人之間的私法爭議，管轄權問題通常較為複雜。因為資料之存取地點與實體主機之存放地點可能分屬不同地理區域，案件究竟應繫屬於哪一區的法院才符合法律及憲法要求？即使一旦擇定管轄法院後，法院應該選擇適用哪一個國家的法律，則是另一個重要議題。

（二）證據適用原則

1. 關聯性 (Relevance)

處理證據得否作為案件認定事實的基礎時，首要問題就是證據與案件事實是否具有關聯性？亦即法院若採納該證據，就表示該證據對法院心證有一定程度的影響力。因此，證據本身必須與本案事實有一定的關聯性。

2. 真實性 (Authenticity)

為證明證據是真實的，可能傳喚證人出庭作證，透過其專業知識證明證據未經竄改且具有真實性。以數位證據為例，證人出庭作證，必須詳細說明證據蒐集、存取及保存的過程是未經汙染的，才能以其證詞認定證據具有真實性。另，美國最高法院建立的「Daubert 標準」，主要是指法官必須擔任科學事實「守門員」的角色，排除不可靠的科學證據與專家證人證詞，避免該證據進入法庭不當誤導陪審團，也就是說專家證人的意見並不必然拘束法院，法院仍可自行判斷。就數位證據而言，縱使專家證人出庭作證說明蒐證過程一切合乎程序，所取得的證據具有真實性，法院仍可自行斟酌專家證人證詞之可信度，其認定事實不受專家證人證言所拘束。

關於儲存於雲端的資料究竟可否作為訴訟證據，亦即可否取得證據能力，作為判斷基礎事實的依據，基本上都環繞在數位證據是否具有「真實性」的認定上。提出證據的一方必須證明證據經過完善的證據保全及蒐集程序，若無法證明所蒐集取得的證據在蒐證鑑識過程中未經汙染而具有真實性，該證據自不得作為證據使用。為確保雲端鑑識資料之真實性，必須詳細說明由雲端服務提供者所提供的資料是可信賴的，且鑑識過程中證據未遭竄改等等。

3. 傳聞法則 (hearsay)

傳聞法則是指排除傳聞證據之使用的法則；而所謂傳聞證據則指陳述者不是在目前的審判或聽證程序中作出陳述，且當事人一方提出該陳述作為證據，以證明陳述中所聲稱的事項為真實。因傳聞證據可能有認知、記憶及表達錯誤的風險存在，因此排除傳聞證據之使用。

至於電磁紀錄是否屬傳聞證據，致受傳聞法則限制而排除其證據能力，則應視電磁紀錄本身之特性而定。例如：系統紀錄 (Log) 檔案係系統運算過程中所產生的機械性紀錄，並不涉及人類的陳述表達，因此不是傳聞證據，不受傳聞法則的限制。

發生異常事件時，如須取得儲存於雲端的紀錄，以供鑑識分析使用，雲端服務提供者通常會出具書面文件，說明所提供的電磁儲存資訊是真實的，而不會詳細敘述存取該電磁資訊的時間、蒐集過程等。這是業界常見的處理方式，該書面文件雖然符合傳聞的定義，但例外被允許使用。

4. **原始證據** (Original Evidence)

一般來說，除法律另有規定外，為證明檔案、紀錄或照片的內容，應提出證據之原本，這是美國聯邦證據法第 1002 條的規定，我國法律也要求證據提供者應提出原始證據，不可提出其衍生品，以符合直接審理的要求。

儲存於電腦或類似設備的數位證據，若能證明證據的複本與原本內容相同，且提出複本並不會造成當事人一方的不公平時，可例外允許提出複本作為證據。

由於儲存於雲端的資料很難復原以取得原始的證據，資料究竟是否為原始證據，又如何證明其真實性，確實為雲端鑑識之一大挑戰。

（三）服務水準協議 (Service Level Agreements，SLA)

雲端服務提供者及消費者間所產生的爭議問題，可經由服務水準協議 (Service Level Agreements，簡稱 SLA) 約定處理。在法律層面上，SLA 對於蒐集相關數位證據及資訊有其重要性，通常 SLA 會明載雲端服務提供者對消費者的義務，包含事件發生應如何處理、蒐集存取鑑識資料的程式、調查程式應如何進行、涉及多管轄權案件的管轄法院選擇等事項。

很多案件的被害人是雲端消費者，如果 SLA 未針對案件發生時如何處理或指出應提供消費者何種資料，則雲端服務提供者對於資料的提供實際上並無契約義務。由此足見，SLA 約定對使用雲端服務的消費者有一定的重要性。然而，SLA 效力僅存在於約定的雙方當事人之間，不會限制國家公權力介入的取證程序及對證據的要求。換言之，即使雲端服務提供者依據 SLA 約定沒有提供系統日誌檔案的義務，亦不可以此為由拒絕提供系統日誌檔案予國家司法單位。

（四）雲端的多層租賃關係

雲端服務之分享儲存空間可能產生多層租賃關係，其主要爭議有二：第一是令狀合法性的要求，簡單來說，事件發生後，若欲進行調查，不可恣意開啓強制處分 (如搜索) 程序，必須要有相當理由相信欲搜索的目標存有足以證明案件犯罪的證據，才可核發令狀進行搜索取證。

另一項爭議是調查時發現資料儲存位置有多位租用者，此時首先必須確認使用該資料的被告身分及資料的儲存位置。換言之，如果搜索票無法明確記載資料所在的位置，這樣的搜索行為是不合法的，而所搜索到的證據也被禁止使用，此即所謂「概括搜索票禁止原則」。為了避免概括搜索，搜索票必須明載與搜索目標範圍無關的地方，如此才可避免搜索過程中，不慎侵害其他租用者的權利或隱私。再者，搜索票亦須指出欲搜索目標資料的範圍，如有違反，可能導致所取得的證據不得使用之結果。

（五）難以確保數位證據的全面性

在雲端運算環境下，資訊大多儲存在雲端環境中，而非實體儲存媒體，即使使用者端也可能沒有完整的原始資料檔案，要全面蒐集完整的犯罪事實勢必存在一定難度，而數位證據的完整性與真實性如難以確保，將造成證據蒐集、封存與分析作業的困難。

四、技術與程序面之挑戰與建議

(一) 無法直接存取實體儲存媒體

依雲端運算的特性，資料集中放置於雲端主機，且分布於不同主機、地區或國家內。雲端運算環境與傳統電腦環境最大的差異是企業失去資料掌控權，因此進行數位鑑識作業時，數位證據的蒐集及擷取程序相對困難許多。傳統數位鑑識作業中，鑑識人員可完全控制目標主機相關證據 (例如：直接進行證物擷取及封存)；然而，在雲端運算環境中，對資料的控制權則因雲端服務運算模式 (如 IaaS － Infrastructure as a Service、PaaS － Platform as a Service 或 SaaS － Software as a Service) 之不同而有異，須依賴雲端服務供應商的協助，這也是雲端運算環境證據蒐集階段可能遭遇的瓶頸。

(二) 取得揮發性資料及日誌檔案的挑戰

揮發性資料係指電腦網路相關設備拔除電源或關機即消逝的數位資料內容。對於雲端運算模式如果沒有較高的掌控權，一旦雲端服務供應商關閉虛擬化主機，相關記憶體資料可能隨之遺失。針對揮發性資料的蒐集，IaaS 運算模式較具優勢，而 SaaS 與 PaaS 模式可能面臨前述相關問題。在日誌檔案方面，除非雲端運算服務商提供，否則 SaaS 模式可能無法取得任何系統紀錄；PaaS 模式雖可取得應用程式日誌，然而網路安全設備、資料庫或系統等日誌資料，仍須仰賴雲端運算服務商。

(三) 欠缺蒐證手段

目前的蒐證技術與手段，難以充分偵測與擷取雲端運算環境中的某些數位證據，例如：許多常見的雲端應用服務，是以虛擬專用網路存取方式進行，鑑識調查幾乎無法檢測。

(四) 數位證據監管鏈

於法庭呈現的證據是否符合證據監管鏈原則之要求是非常重要的，對於易被竄改或改變的證據，完善的證據監管鏈是必須的。自雲端取得數位證據可能比一般數位證據更容易遭竄改，證據監管鏈的要求應更加嚴格。其危機首見於雲端服務供應商，主因是部分數位證據可能由雲端服務供應商提交司法單位，調查取證及接觸數位證據的人員可能因蒐證程序有瑕疵而影響證據能力，實務執行上不易控制。因此，雲端服務供應商須善盡保存責任，所有取得的數位資料皆須檢驗其雜湊值，以確保證據於保存過程中未被修改。

五、國外雲端鑑識作業程序

國外對於雲端服務架構所提出的鑑識作業程序相關研究文獻，重點整理如表 1 所示。除針對不同雲端服務架構 (如 IaaS、PaaS、SaaS) 進行研究外，並可考量區分外勤人員蒐證程序及實驗室內部分析程序。相關研究經常參考 ISO/IEC 27037 [參考文獻 2] 之建議，以下探討其框架與鑑識原則。

針對傳統的數位鑑識調查標準如何套用於雲端服務環境，雲端安全聯盟 (Cloud Security Alliance, CSA) 特別提出「Mapping the Forensic Standard ISO/IEC 27037 to Cloud

表 1　國外雲端服務架構鑑識作業程序相關研究

相關文獻	相關文獻重點摘要說明
D. Birk, “Technical challenges of forensic investigations in cloud computing environments.” [參考文獻 3]	依據不同的雲端服務架構調整數位證據蒐集項目，由於對 PaaS 與 SaaS 環境的掌控權較差，建議探討系統設定資訊及日誌機制，於 IaaS 環境可透過揮發性資料 (Volatile Data)、映像檔快照 (Snapshots)、虛擬自我監控 (Virtual Introspection) 進行分析。
Lei, Yunting, and Yuyin Cui, “Research on Live Forensics in Cloud Environment.” [參考文獻 4]	主要依據 ISO/IEC 27037 之四步驟進行探討與建議： ・識別：在 SaaS、PaaS 或 IaaS 不同架構下的證據資料來源。 ・蒐集 (設備移送至他處)：若因法令要求而進行蒐集，通常只能由雲端服務提供者進行。 ・擷取 (潛在證據複本製作)：因雲端的多租戶特性，通常傾向僅做邏輯物件擷取，以免影響無關他方。 ・保存 (維持完整性)：使用證據監管鏈與傳統鑑識相同。 建議採用「雲端環境即時鑑識方法論」，即以虛擬機器 (Virtual Machine, VM) 映像檔為鑑識分析標的，透過虛擬化軟體層控制，使 State transition 得以完整保存，並於本地端重建 VM (Virtual Machine) 狀態。
de Oliveira, José Antonio Maurilio Milagre, and Marcelo Beltrão Caiado, “Cloud Forensics : Best Practice and challenges for process efficiency of investigations and digital forensics.” [參考文獻 5]	雲瑞環境鑑識作業主要分成以下階段與程序： ・識別：由 IPS (Intrusion Prevention System) 機制偵測事件，透過雲端服務供應商協助瞭解範圍，以及提供 snapshot、稽核檔或備份的可能性。 ・保存：由雲端服務供應商 (或其指派專家) 負責證據保存及建立證據監管鏈。 ・蒐集：建立遠端蒐集策略，或由雲端服務供應商 (或其指派專家) 負責萃取實體硬碟 / 磁區 /VM 鑑識映像檔，並提供 snapshot 檔案。 ・檢查與分析：與傳統鑑識分析程序無異。 ・呈現：再現性與重複性與傳統鑑識無異，雲端服務供應商應依約保存證據檔。
Josiah Dykstra, and Damien Riehl, “Forensic Collection of Electronic Evidence from Infrastructure-As-a-Service Cloud Computing.” [參考文獻 6]	以美國 Amazon EC2 平台為實例，確認現有數位鑑識工具可針對 IaaS 架構進行遠端擷取。由於雲端架構特殊，應考量各階層的信任度，鑑識人員針對各階層證據皆須檢驗與進行關連。調查人員可能進行主機的遠端鑑識，但執法單位可要求雲端服務供應商技術人員進行操作 (如搜尋、蒐集與取出等)。

Computing」，訂定識別、收集、獲得與保存數位證據的指南。對於負責數位證據識別、蒐集、擷取與保存作業的相關人員，包括數位證據第一線應變人員 (Digital Evidence First Responders，DEFR)、數位證據專家 (Digital Evidence Specialist，DES)、事件應變專家及鑑識實驗室管理者等，ISO/IEC 27037 可提供相關指引，但不應取代司法體系的特定要求，如數位證據在法庭上的證據能力、證明力、相關性及其他司法要求及認定。

ISO/IEC 27037 在資訊安全事件調查過程中，提供事件分析數位鑑識可依循的標準與指南，其特點分述於下：

(一) 現場處理注意事項

為保持現場完整，應設置現場管制負責人，管制現場進出與證據存取。除隔離嫌疑人員與現場的接觸外，應記錄現場環境與設備狀態，並管制設備現況與相關資訊。

(二) 角色與職責

ISO/IEC 27037 將涉及數位鑑識證據保全作業程序的人員分為兩種角色，一是數位證據一線應變人員，主要職責為數位證據的辨識、蒐集、擷取與保存，包含數位證據蒐集及擷取報告內容的編列、數位證據的保存及處理；二是數位證據鑑識專家，具備專業鑑識職能，可針對一線人員無法處理的情形 (例如：複雜的伺服器架構或磁碟陣列儲存裝置等)，提供技術性協助。

(三) 文件化要求

ISO/IEC 27037 要求詳細記錄操作動作、存取的資料名稱、螢幕顯示畫面、目標設備的廠牌、型號、規格等資訊，並建議可用攝影方式記錄之。

(四) 勤前會議

進行證據保全時，現場環境情況可能無法預料，必須先召開勤前會議，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。

(五) 證據蒐集及擷取優先

若電腦主機處於開機狀態，則非必要不應關閉，以避免揮發性資料 (例如：RAM、Cache RAM、Register、主機正在執行中的程序、網路連線與應用程式開啓通訊埠等) 可能因關閉主機而就此消逝無法回復。

(六) 證據封存、運送及儲存

證據進行封存時，應有明確的標示紀錄與阻隔防護性包裝；運送過程應處於受監管與保護的環境；最終的儲存地點應確保其實體防護安全。

(七) 謹慎處理原則 (Use reasonable care)

避免任何可能損毀數位證據的行為，數位證據第一線應變人員 (DEFR) 不應直接存取原始數位證據，除非人員具備相關能力，且使用可靠且經過驗證的程序，鑑識作業過程應避免破壞數位證據。

六、結語

雲端時代的來臨，帶來數位鑑識領域相關挑戰；雲端上的數位證據有其特殊性，不如實體主機存取資料的明確。若欲使用雲端上的數位證據作為認定案件事實的基礎，會面臨相關法律議題，例如雲端資料可能分別儲存於不同地點，甚至分屬不同國家，涉及跨國司法管轄權認定的問題。

本文針對雲端鑑識在法律、程序及技術等層面所遭遇的挑戰進行分析，探討雲端鑑識相關問題，這些都是應用新興科技必須克服的科技法律議題，不論是提供或使用雲端服務的企業及使用者，均應審慎評估及面對。

※ 參考文獻 / 資料來源：

1. Keyun Ruan, “Cloud forensics: An overview”, University College Dublin Centre for Cyber Crime Investigation.
2. ISO/IEC 27037 Information technology—Security techniques— Guidelines for identification, collection, acquisition and preservation of digital evidence, 2012.
3. D. Birk, “Technical challenges of forensic investigations in cloud computing environments”, in Workshop on Cryptography and Security in Clouds, January 2011.
4. Lei, Yunting, and Yuyin Cui, “Research on Live Forensics in Cloud Environment”, 2nd International Symposium on Computer, Communication, Control and Automation, Atlantis Press, 2013.
5. de Oliveira, José Antonio Maurilio Milagre, and Marcelo Beltrão Caiado, “ Cloud Forensics : Best Practice and challenges for process efficiency of investigations and digital forensics”, ICoFCS 2013.
6. Josiah Dykstra, and Damien Riehl, “Forensic Collection of Electronic Evidence from Infrastructure-As-a-Service Cloud Computing”, Richmond Journal of Law and Technology Vol. 19, 2012.

讀者心聲

首先，感謝您撥冗閱讀「財金資訊季刊」！

請您提供我們寶貴的意見或建議，給我們一個攜手共進的機會，我們將儘可能符合您的需求，也豐富季刊的內容，提升對您的服務。

敬請 不吝賜教，並請您將寶貴的意見或建議以電子郵件傳送至財金資訊公司管理部文書組張小姐 laura_chang@mail.fisc.com.tw。