藉由電腦鑑識 (Computer Forensics) 進行企業風險管理

林佳瑩[1]

壹、導論 -IT 社會的發展與電腦鑑識
貳、電子資料證據的保全與調查
　一、Step1：不可隨意操作調查對象 PC
　二、Step2：應複製整個調查對象 PC 硬碟
　三、Step3：嘗試復原已刪除檔
　四、Step4：篩選出可作為證據之用的電子郵件
參、證據資料同一性的證明
肆、依不同目的運用電腦鑑識之案例
　一、內部違法行為之調查
　二、調查離職者的 PC
伍、藉由電腦鑑識進行風險管理

壹、導論－ IT 社會的發展與電腦鑑識

現代因ＩＴ技術發達，而得以更高速、大量且輕易儲存、傳送、重新寫入和刪除訊息，再加上還存在無法用肉眼所見的電子資料，因此在風險管理上已越來越困難。對於擁有特定電子資料的團體或個人而言，能正確且安全管理該資料至何種程度，儼然已成為重要課題。因此，

1. 為優比克股份有限公司科技法律諮詢顧問。(http://www.ubictw.com；megan_lin@ubictw.com；02-8752-3178)

用於保護電子資料的各種訊息安全技術便日益發達。然而，實際上要保護電子資料極為不易，要完全保護訊息甚至可說是不可能的任務。

基於以上結果，我們應假設資訊的不法使用一定會發生，因此必須採取相關對策。除了以往主流的防禦性安全對策，還必須擬定發生資料外洩等安全事件後的因應對策。

此外，若說在高度訊息化社會中，所發生的所有犯罪，皆透過各種形式，與數位設備息息相關，其實一點也不為過。因此，執法機關應將 PC 等數位設備，視同於指紋一般，是必須優先取得的重要證據。當今，透過數位設備所做出的犯罪行為，已從駭客蔓延到不具備ＩＴ知識的人們。舉例來說，過去曾發生調查具嫌疑的員工電腦內的郵件等資料，而掌握到企業粉飾決算、人員盜用公款等背信行為的證據，加以繩之以法的案例。

從風險管理的觀點來看，利用先進技術，一邊維持資料的證據性，一邊取得與分析高科技設備資料，以解決法律問題的電腦鑑識，突然備受矚目。

本文將介紹電腦鑑識的調查手法，並提出建議以幫助企業善加運用電腦鑑識。

貳、電子資料證據的保全與調查

在訴訟中，最可能被列為證據的電子資料就是電子郵件。其原因為，其通訊方式與電話通話相異，電子郵件直接收錄寄件人與收件人的溝通內容，因此容易列為證據。此外，電子郵件也是常被使用的日常溝通工具，一般而言被認為較能正確傳達寄件人的意思內容，因此也是電子郵件易被列為證據的理由之一。

以下將以電子郵件為例，具體說明以電子資料為證據並保全電子資料的方法、及針對被保全之電子資料的調查方法。

一、Step1：不可隨意操作調查對象 PC

要調查電子資料，就必須存取儲存資料的數位設備，然而若輕易進行存取，將有可能提高失去寶貴證據的危險性。電子資料的特徵在於，易失性高、容易竄改。

舉例來說，若隨意操作存放證據資料的 PC，將可能導致嫌疑人使用過 PC 的重要存取歷史紀錄被覆蓋。此外在 Windows 系統中，光只是打開 PC 電源，也會變更時間戳記 (time stamp)，因此無論是否故意，若隨意存取資料，即有讓重要證據消失的危險性。

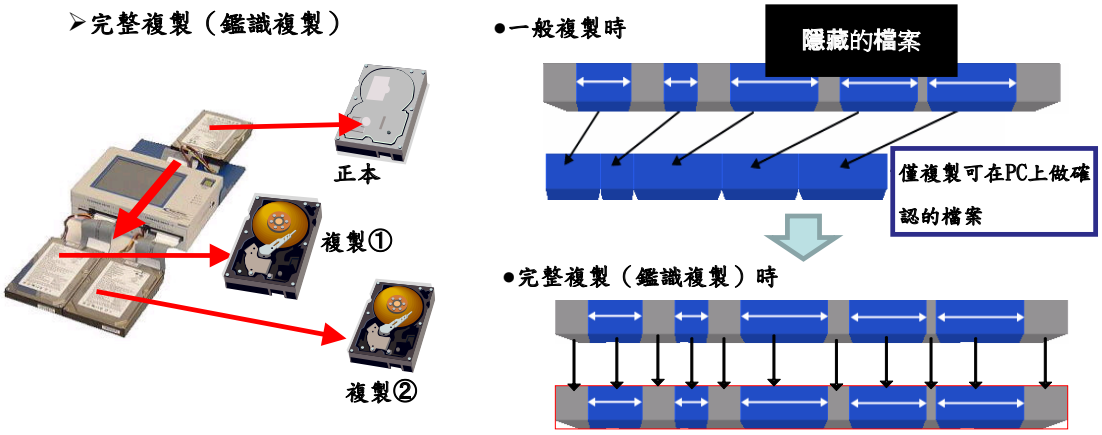
因此，操作電子資料時，必須處理得相當細膩。否則不僅是證據資料消失，連開始調查後的時間戳記的變更，都有可能被視為是調查者所執行的某些訊息操作。直接存取調查對象 PC，就好比是穿著鞋踏壞殺人事件現場的行為。

關於調查電子郵件方面，還有未讀取／已讀取郵件的問題。直接開啟電子郵件，以調查郵件內容時，在收件匣發現到重要證據郵件，此時嫌疑人是否已檢視該份郵件，便成為一大爭論點。倘若嫌疑人主張只接收郵件而未檢視內容，也就是在“未讀取”狀態時，若實際的資料在調查階段為“已讀取”，則要證明該郵件在調查前為“未讀取”或“已讀取”，是非常困難的事。

二、Step2：應複製整個調查對象 PC 硬碟

如 Step 1 所示，電子資料恐有容易損壞、或因不謹慎操作而覆蓋資料，導致破壞電子證據之虞，因此應避免直接調查內置於調查對象 PC 的硬碟，一般的步驟應先複製該硬碟，再針對複製物展開調查。這種建立複製的作業，即稱為證據保全作業。保全證據時，勢必要進行完整複製。所謂完整複製並不是只複製儲存資料的部分，而是針對每個磁區 (sector) 的 HDD 所有領域實施複製。嫌疑人有可能故意將資料隱藏在表面上未儲存資料

[示意圖]



（可調查包含刪除檔和隱藏檔在內的所有領域！！！）

之處、或者讓已刪除的資料存在於該處，因此該處很有可能存在列為證據的重要資料。

以證據保全作業工程而言，為了防止殘留資料干擾電子證據，都是完全刪除用來保全證據的硬碟內的殘留資料。此時，必須用具有「DoD 刪除」之稱的美國五角大廈等規格的刪除工具，事先完全刪除殘留資料。接下來，則用專用鑑識 (forensic) 工具，將調查對象 PC 硬碟，複製於已事先刪除殘留資料的證據保全硬碟上。通常，將 1 個調查對象硬碟複製成 2 份。 1 份用於儲存之用，另 1 份則用於分析。

三、Step3：嘗試復原已刪除檔

丟入垃圾桶後再進行「清空垃圾桶」作業，看似檔案已完全被刪除，但實際上仍被記錄於硬碟中。檔案管理訊息（檔名、時間戳記、屬性等）、和實際資料內容分別被記錄在不同的硬碟內部領域，光從垃圾桶刪除檔案，充其量只不過是將管理訊息中的屬性變更為「不存在」的旗幟罷了，對於實際資料部份並未進行變更。

若分析該管理訊息，即可強制將「不存在」的旗幟，恢復成「存在」，以復原看似已刪除的檔案。然而，一旦變更為「不存在」的旗幟，該資料內容的領域將依其他資料，而辨識為可再使用，因此一旦在該資料上再度重新改寫資料時，便無法再復原。

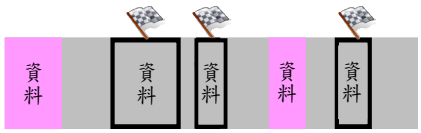
調查電子郵件時，最重要的是調查 WEB 郵件。因 Outlook 或 Lotus Notes 等公司內部電子郵件應用程式會在日誌 (log) 中留下記錄，可在公司內部透過監控以進行監視，因此企業內部若有不肖員工企圖洩漏資訊，可能不會使用公司內部電子郵件應用程式。但若使用 WEB 郵件，電子郵件不會被記錄於 PC 內的 Local 端，因此發現不法傳送郵件的可能性低，易於違法洩漏前述訊息。然而，WEB 郵件內容會暫時記錄於硬碟，因此將資料復原即可展開調查。

由於在硬碟上，是隨機記錄訊息，因此在已刪除的檔案之中，哪個檔案有無被覆蓋、可不可復原，都必須透過實際調查才能知道答案。然而，隨著時間的經過，PC 使用次數越來越多，勢必也將增加資料被覆蓋的風險，因此需調查 PC 時，盡早保全證據乃屬至關重要。

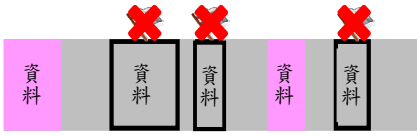
[示意圖]

➢資料的刪除與復原的架構（示意）

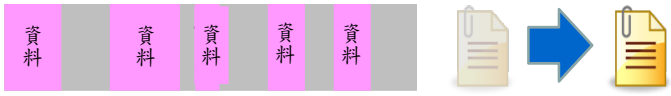
將欲刪除資料放入垃圾桶後，再清空垃圾桶・・・



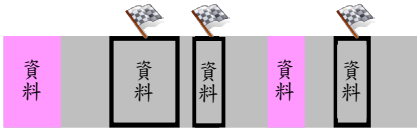
若檔案被標上「已刪除資料」的旗幟，將無法從畫面上看見該檔案。

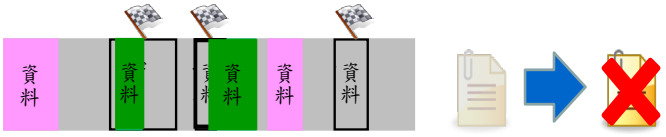


利用鑑識技術解除此旗幟後，便可重新存取檔案・・・



然而，這是以可以完美復原檔案為前提。





賦予刪除旗幟是指，「在此領域可寫入新資料」。

也就是說，當建立或儲存新資料時，可能會寫入已刪除的資料上。這就是檔案覆蓋。

一旦發生檔案覆蓋的情形，資料只能以不完整的型態復原、又或者無法再復原。

四、Step4：篩選出可作為證據之用的電子郵件

包含已復原的電子郵件在內，應從龐大的訊息中，鎖定可作為證據之用的郵件。以下記載數則電子郵件的調查方法。

（一）搜尋關鍵字 (Keyword Filtering)

搜尋關鍵字不僅適用於電子郵件，還可說是所有調查的基礎，是非常重要的調查方法。設定的關鍵字包含以人名、郵件信箱（網域資料）為首的所有相關調查內容的關鍵字。其中還包含“秘密”、“上次提到的”、“曝光”等關鍵字。

（二）藉由日期鎖定對象 (Date Filtering)

電子郵件中存在接收／傳送日期與時間等資料。調查時大多是依調查內容，篩選出應調查的期間，因此可利用電子郵件的傳送／接收日期與時間等資訊，鎖定調查對象的電子郵件。

（三）重複資料刪除技術 (Deduplication)

有不少案例調查對象並未侷限於１名，必須同時調查數名調查對象者的PC。此時，重複資料刪除技術可發揮作用。舉例來說，調查Ａ、Ｂ、Ｃ３名對象時，Ａ傳給Ｂ、Ｃ的電子郵件，有可能以相同電子郵件存在於Ｂ及Ｃ的PC內。若屬相同群組內的對象者，那麼即存在多份相同的電子郵件。此時，利用各電子郵件的ID、郵件標頭訊息（傳送／接收日期與時間、傳送者、收件人、主旨等），將這些相同電子郵件機械性的視為１個電子郵件，以進行處理後，便可省去瀏覽數次內容完全相同的電子郵件時間，以達成有效率的調查。

在此已介紹幾種電子郵件的調查方法，然而這些終究是對應應調查的電子郵件，賦予優先順位的篩選技術，要尋找可成為各調

查案件證據的電子郵件，畢竟還是要透過肉眼的調查。

參、證據資料同一性的證明

然而，為了分析，而複製整顆列為證據的原始硬碟之後，該如何證明複製的電子郵件，同於原始證據的電子郵件呢？

在電腦鑑識調查工程中，應隨時留意資料同一性的證明、和儲存持續性的證明。在美國司法部的指導方針中，便建議採用「雜湊函數 (hash function)」。雜湊函數在資料內容完全一致時，會算出相同值，但只要有 1 個文字不一樣，即算出不同值。因具有這種性質，因此也稱為指紋辨識（電子指紋）。

複製資料時，應確認原始檔與複製檔的雜湊函數為一致並記錄下來，之後在進行所有作業時，應檢查複製的雜湊函數是否變更。如此一來便可用數學角度證明，原始檔與複製檔乃屬完全相同的資料，且在調查與分析過程中，所有作為證據的複製資料皆未受到任何篡改。

此外，取得所有作業日誌 (log)，並記錄何人、何時，曾處理該證據資料，以作成嚴謹監護環（Chain of Custody），也是非常重要的作業。

肆、依不同目的運用電腦鑑識之案例

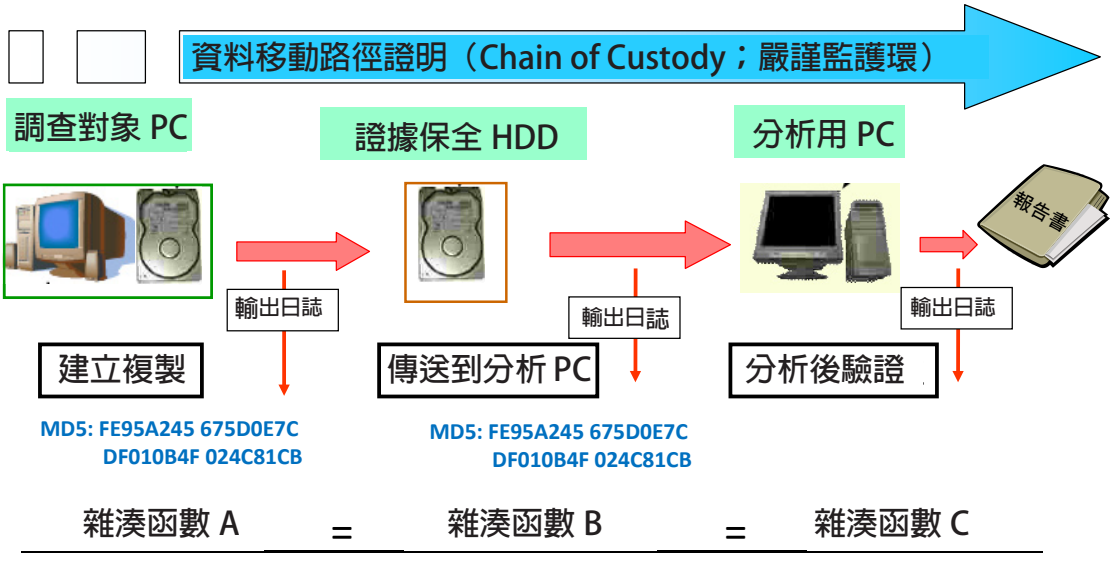
一、內部違法行為之調查

透過電腦鑑識，調查企業內部違法行為時，重點並不是以搜尋與分析電子資料為最終目的，而是以訴訟解決目前所調查的問題。換言之，一旦存取未授權檔案、或違法使用網路時，不僅能找到違法的直接證據，還能發現該員工違反就業規則等行為，例如該員工“在上班時間上網玩遊戲。”或“準備設立新公司。”等行為，皆能影響法官的心證，更是有利於訴訟的重要證據。

二、調查離職者的 PC

為了防止離職者所用的 PC 洩漏訊息，目前幾乎所有日本企業，皆在完全刪除該 PC 資料後，再廢棄或歸還 PC。然而，仍有不少

[示意圖]



證據資料同一性的證明（雜湊函數：藉由單向函數作確認）

受害企業是在離職者即將離職前，資料便被洩漏、破壞、刪除或竄改。因此，有些企業會將 PC 資料實施證據保全後，再進行刪除作業。據報告指出，實際上也有在發生事件後，因調查已實施證據保全的資料，而成功避免受害，或將受害情況控制在最小限度的案例。另一方面，因未實施證據保全，導致事件發生後毫無任何調查途徑，而讓犯罪者逍遙法外的案例也不少。

伍、藉由電腦鑑識進行風險管理

通常，企業裡的員工，大部分都是遵守法令與公司內部規定的守法者，然而這些人所做出的不正確行為，幾乎都是因疏忽與意外所致，此時可藉由內部控管的業務流程或內部管制，以防範未然。不容否認的是，企業裡也有可能存在一部分輕度不守法（瀏覽色情網頁、收發私人郵件、一時興起而存取機密資料等）的人。此時可針對這些人，透過 IT 安全系統，限制存取檔案、設定密碼、限制瀏覽網站、禁止傳送與接收 Web 郵件等方法加以抑止。

然而，即便是處於灰色地帶的輕微不守法的人，或遵守規則、工作認真的人，也有可能因壓力・機會・藉口（自我合理化）等舞弊三角，加上心中抱著應該不會被發現的僥倖念頭，而做出惡意的違法行為。事件回應的體制用於因應已發生的違法事件，因此企業應建立可視其需要採取訴訟予以因應的體制。如此一來，電腦鑑識便成為有效的手段。而且，若企業體制具有可實際執行訴訟的能力，以解決實際發生的違法事件，則可遏止懷著僥倖心態的惡意不法行為者執行非法行為，就結果而言，可說是具有相當大的嚇阻力量。

利用電腦鑑識監察 PC，以防發生內部不法行為的對策，具有極高的投資效益。這不僅可降低因個人資料外洩而導致的損失，還能防止技術資料等智慧財產的外洩，守護企業競爭力，獲得正當利益。

此外，判斷企業價值時，是從企業的成長程度及下行風險 (downside risk)2 個角度做判斷，特別是下行風險的降低，對於企業價值的提升具有相當大的貢獻。

要完全消弭內部不法行為、或涉入訴訟的風險並不容易，因此必須制定具體對策以控制損害，其中應包含針對風險擬定的風險控制計劃及危機管理，讓企業從這些風險中減輕損失，持續事業經營。企業確實秉持嚴禁內部出現不法行為的堅決態度、針對不法訴諸法律的態度、及擁有電腦鑑識體制以具體支援企業方針，可說是體質堅強的企業所不可欠缺的解決方案。

（作者為優比克股份有限公司科技法律諮詢顧問）

栗喉蜂虎 / 金門縣政府