DRM-機密文件保全防身術

數位版權管理（ Digital Rights Management，DRM）過去主要運用在遏止影音內容盜拷，近年來被視爲保全機密文件的有效解決方案。其原理是對音樂、文件與郵件等數位檔案進行統一的版權管理，包括修改、存取、傳遞等權限控管，以防止機密文件遭非法列印、複製、郵件轉寄及螢幕瀏覽等。根據 CSI/FBI 的調查顯示，2003 年全美智慧財產損失超過七千萬美元，而數年前國內台積電機密文件外流大陸，損失據傳高達十億元以上；除了文件外，組織或企業內部往往還潛藏許多外洩管道，這也突顯資產保護的重要性與 DRM 技術的價值所在。

DRM 技術包括使用者認證、版權產生、驗證、移轉與權限管理等，在「e-Taiwan」計畫下，政府與企業間網網相連，使有心人士有機可乘，而機密外洩事件亦時有所聞，因此在法令規範之外，企業組織必須練就文件保全防身術，始能確保機密檔案安全，以下僅就常見資料外洩管道討論 DRM 之運用。

一、機密文件被列印傳閱

在一般辦公室環境中，網路印表機是偷渡機密文件最佳管道，因爲不論是計畫、合約或其他重要電子文件，一經實體紙本列印後，即使該電子文件設有保密期限亦於事無補。因此「加密」是避免機密資訊遭竊取的主要防護技術，而加密亦是 DRM 軟體必備功能，其通常採客端（Client）與伺服器軟體相互搭配，當原創者加密文件時，終端程式就會將文件金鑰與使用政策儲存在文件檔頭，併同使用者資訊與金鑰上傳伺服器，而另一使用者欲開啓該文件，須通過身分驗證後始能依使用政策閱讀。此外，大多數 DRM 軟體亦具備禁止列印功能，並支援多種文書軟體格式，包括 Word、Excel、PDF、JPG 及動靜態網頁等，而更先進者尚可動態決定發行權限，並紀錄與稽核追蹤文件的存取、列印與閱讀時間等參數，管理者可巨細靡遺的檢視所有使用過程。

二、電子郵件轉寄偷渡

國內曾發生員工任意轉寄企業內部郵件而遭開除事件，如聯電董事長對內發布的公開信在數小時內傳遍同業，聯電經徹查後將參與「第一梯次」轉寄的十名

員工以「不務正業」名義開除。電子郵件釀禍的可能性不只來自內部，當企業與外部公司合作並以 e-mail 寄送重要資料同樣亦可能喪失對機密文件的控制權，透過郵件軟體的「轉寄」，幾分鐘內文件即一傳十、十傳百的擴散，企業組織無論事後如何補救，其成效均微乎其微。

因此每一種 DRM 軟體都有禁止非法轉寄郵件功能，只要事先設定寄送對象、權限與範圍，未經授權者無法轉寄，而如郵件已寄達第三者或遭竊取，亦可依事先設定的效期，逾時即無法開啓；又員工如將機密文件誤傳或傳送後發現內文有誤，亦可藉動態變更權限將已寄出或開啓的文件，有效的「回收」。

三、資料任意複製

現今社會變遷快速，員工異動率極高，因此攜離重要機密文件的行爲時有所聞。日前媒體披露國內五大銀行員工販賣消費者個人資料，導致全臺一半以上人口個人資料外洩，再度證明高價打造防火牆雖擋得了駭客卻難防家賊，畢竟資料複製的方法不勝枚舉，端視企業管理政策嚴謹與否，如文件存取控管鬆散，則惡意員工只需執行「複製 、貼上」即可將文件內容直接轉貼，而另存新檔或以隨身碟儲存，一次可偷渡大筆的機密資訊。同樣地，網頁內容亦可直接利用複製或列印剽竊，縱使網頁設限無法直接複製，使用者亦可以瀏覽器檢視原始碼完整的複製網頁。

因此最佳文件保全方式係根據管理政策設定文件存取權限，使用者須通過身分認證，再依文件敏感程度決定其權限。幾乎所有 DRM 產品都具備上述功能，唯一差異在其操作的不同，基本上都可針對不同層級使用者給予不同程度的授權。在安全政策保護下，DRM 不管文件身在何處，管理者可隨時更改其權限，即使已遭複製攜離，只要及時在開啓前改變權限，便無法一窺檔案中的機密。

四、螢幕或網頁畫面擷取

當員工瀏覽內部網路發現未經保護的機密文件，即使無法另存新檔或轉寄，只要按下「 Prinet Screen」，就可進行複製或列印，而網路上亦流傳多達數百種抓圖軟體免費下載，這些軟體均具備錄製螢幕畫面功能，甚至可紀錄使用者桌面的每一動作，因此 DRM 軟體均將保護螢幕畫面視爲重要功能，只要文件權限設

定爲「不允許複製」、「不允許修改」、「不允許列印」等三項條件同時成立，使用者就無法執行 Prinet Screen 功能。

五、網路芳鄰或遠端存取

利用網路芳鄰分享資料是網路的基本功能，惟如對資料夾權限設置不當，極易遭未授權的第三者複製而渾然不知；此外 Windows 作業系統或某些軟體均提供遠端協助、遠端桌面等功能，熟悉網路者亦可藉 PC anywhere 這類遠端控制軟體，輕易連上重要管理階層的個人電腦偷取機密資訊。因此欲享受網路傳播的便利，又要防止同一網域中不請自來的入侵者，最根本工作還是設定密碼保護機密檔案，但使用密碼亦有其遭破解的風險，而部署 DRM 則透過終端軟體與伺服器認證配合，不論何種形式的電子檔案，凡未經授權的操作行爲都無法成功，即便是遭到入侵，任何儲存、複製、列印或轉寄等行爲都會遭到攔截。

打擊文件偷渡的新選擇

DRM 是利用加密技術保護文件，對國內 IT 產業而言，其並非嶄新概念，多年前即有企業導入，近期因接連發生大型製造業、電信業與銀行內部洩密事件而再度受到重視。在市場方面，微軟推出 Office System2003 前，已有多種品牌包括網核資訊與寬華代理的 Mirage、力邁科技代理的 Authentica，以及本土廠商優碩資訊自行研發的 TrustView 等。

就技術觀點而言， DRM 的作法概分兩類；一是要求使用者每次開啓機密文件須連至伺服器下載解密金鑰，如此有利 MIS 人員執行嚴密的內容控管，Authentica 及 Mirage 即屬之；另一是允許使用者設定文件存取權限，一旦設定完成無論文件傳至何處均依其規則不必每次連上伺服器，使用上較爲方便，但不具動態管理能力，微軟的 IRM、TrustView 即屬此類。

在完整部署防火牆、打造入侵偵測系統之後，下一步我們該如何建構文件保全系統，確保機密資訊滴水不漏？而機密文件的存取、使用與權限管理政策又應如何設定？囿於「十個外來駭客對於機密資料造成的威脅，往往比不上一個內部低階員工外洩資料的殺傷力」之事實，政府機構或企業應由安全政策著手，建立管理稽核架構，而最重要的是在使用便利與管理目標間取得平衡點。

一、配合組織安全政策

DRM 管理單一文件的概念類似於網路安全政策中的身分認證與授權，基本上 DRM 可「給不同使用者予不同的存取權限」，因此成功部署 DRM 的前提是：配合組織安全政策，依據權限大小區分可修改、只能讀不能改、允許改不能刪除、只能讀及不得轉寄、複製或列印等權限。因此 MIS 人員存取權限大於員工，而以高層主管權限最大，若企業欲部署最嚴格的管理模式，則使用者每次存取均須連至伺服器取得密碼後才可讀取或修改文件。

二、建立管理稽核架構

標準的管理組織包括系統 /伺服器管理員、政策管理員、稽核人員與一般使用者等四種角色。在一個取得資訊管理標準 BS7799 認證的組織中，這四種角色應該隸屬不同單位：系統管理員交付 MIS 或 IT 經理擔任、政策管理員角色應是主管或部門主管扮演。爲避免上述二種人「監守自盜」，還需要建立監督角色，即由另一部門員工出任稽核員角色，一旦有人企圖或在無意中開啓已被保護的重要文件，稽核員將會接到系統發出的警報通知而能即時處置。

三、找出便利性與管理的平衡點

或許有人質疑部署 DRM 對各種電子檔案進行嚴密控管將會造成「綁架重要資訊」的副作用，且喪失靈活應用的能力。其實 DRM 的解決方案亟具彈性，一般而言單位越重視智慧財產則內部控管越嚴格，而多數 DRM 都提供從最嚴格到最放任的管理方式，以因應組織的需求可適時調整。

根據國際知名研究分析機構 METAGroup 的研究數據，未來兩年內 DRM 市場可成長十倍，亦即在 2006 年時，全球 2,000 家生產數位內容的企業中將有 20% 導入 DRM。經過本文闡述分析後，身處資安防護益顯重要的今日，您的組織是否已準備練就機密文件保全防身術—導入 DRM，來保護單位重要的資訊資產呢？有需求者不妨試試 DRM！

（本文作者爲吳文進先生）

（本文摘自行政院國軍退除役官兵輔導委員會政風處網頁）