

## 企業需求與適用情境

# 一探數位版權管理全貌

5年來，在與微軟公司共同推廣數位版權管理(DRM)的幾十場研討會與客戶拜訪經驗當中，看到了客戶對DRM產品的需求與期待，筆者將5年來數百家企業的DRM導入經驗與需求，做一個總檢討，與讀者分享DRM的動作原理，並分析DRM的微軟相關產品、企業需求與其適用範圍。

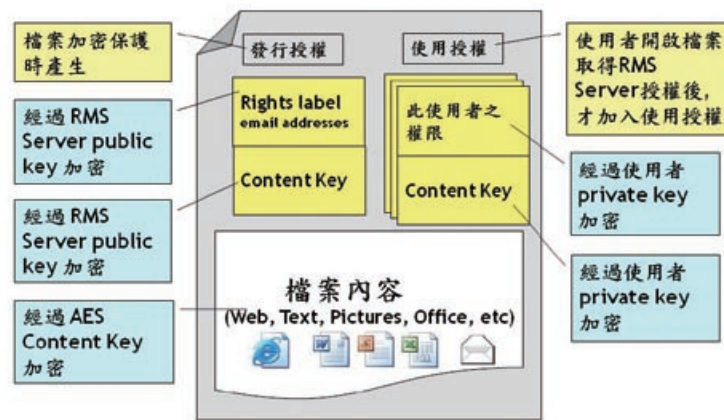
作/博格科技總經理周世雄

今年的熱門話題－「資料外洩防護」，簡稱「DLP」，為Data Loss Prevention的縮寫，也有人稱為Data Leakage Prevention。

DLP解決方案之一為「數位版權管理」(Digital Rights Management ,DRM)，企業用的數位版權管理叫做E-DRM(Enterprise Digital Rights Management)，2004年起開始由微軟公司炒熱。

將具有DRM保護的文件轉給別人，別人也無法開啓，其主要關鍵點在於：「開啓文件必須連線到授權伺服器先取得授權」，因此，盜取內部機密資料的人，將因無法連線到授權伺服器取得授權，而無法開啓文件。

DRM的動作原理，為有權限的使用者，當開啓具有DRM保護的加密文件時，第一次需要連線到授權伺服器取得授權，若有權限則會產生



DRM保護文件的格式。

一個使用授權(End User License ,EUL)。

EUL存放於DRM保護文件的表頭或一個檔案當中，一個使用者於一個文件有一個專用的EUL，因使用此使用者之非對稱式public key加密content key，即使傳給別人亦無法使用。

每一個開啓的加密文件都會產生一個個別的EUL，這個EUL是依照文件、電腦與使用者而異的，即換一個文件、電腦或使用者，就需要再

連線到授權伺服器取得授權。

因此，將加密保護的文件外洩給別人，別人將無法取得授權伺服器的使用者授權，而無法開啓文件。

### 微軟的DRM相關產品

微軟公司於2003年11月，推出DRM所需要的「微軟DRM平臺」，包括Office IRM(Information Rights Management)與Windows RMS(Rights Management Services) (授權伺服器)等產品與技術。

為使用這些DRM技術，Windows XP可安裝RMS Client 1.0 SP2，Windows Vista則內建RMS Client；授權伺服器方面，Windows Server 2003可安裝RMS Server 1.0 SP2，而Windows Server 2008則內建了RMS Server 2.0。

當初，讓使用者昇級到Microsoft Office 2003的新版本，最明顯的誘因是因為Office 2003整合了Office IRM技術，讓作者可以設定權限。Office 2007也繼續支援此功能。

而微軟的企業入口網SharePoint產品(WSS 3.0、MOSS 2007)，也整合了DRM的功能，於下載Office檔案時自動加密。

### DRM的企業需求

5年來，洽談了近百家的客戶，筆者歸納企業對於DRM的需求與具體的做法：

**需求：集中管理的機密文件，企業需要有自動加密的功能**

**做法：**譬如將機密文件放置到檔案伺服器(File Server)、企業入口網站(SharePoint)時，自動加密保護文件。

此需求的解決辦法為需要加密時，使用

程式開啓Word、Excel、PowerPoint檔案，呼叫Office物件模型(Object Model)，即可達成。但是經過幾個客戶的導入後，結果怨聲不斷，原因為加密時伺服器不斷地開啓Microsoft Office軟體而造成不穩定的問題發生。

為了解決這個問題，具體的做法為需要研究Office 2003/2007 IRM的保護格式，不開啓Office軟體，即可完成加解密的動作。

**需求：於企業入口網站(SharePoint)，企業需要更彈性的文件保護功能**

**做法：**當企業導入微軟公司的SharePoint產品WSS 2.0/3.0、SPS 2003/MOSS 2007時，企業需要更彈性的文件保護功能，譬如(1)可設定公司內部的權限政策(Policy)：像是機密、極機密等，解決之道為整合RMS的「權限原則範本」功能，讓權限管理員可以挑選資料夾所套用的權限政策。(2)可以保護其他的檔案格式：除了Microsoft Office外，也可以保護PDF、Text、JPG等檔案格式。

具體的做法為整合SharePoint與RMS的技術。

**需求：企業需要更安全的文件保護功能**

**做法：**安全性方面，企業需要照相保護(加上螢幕、列印動態浮水印以嚇阻與稽核)、抓圖保護(保護不會透過螢幕截取的方式外洩出去)等功能。

為了安全考量，當Office 2003、Office 2007僅具讀取權限時，整個文件是鎖住的，無法加上動態的浮水印。

具體的做法為使用Hook技術以提供照相保護、抓圖保護的功能。

## DRM的適用範圍

根據我們多年來的導入經驗，並沒有一種DLP產品就能夠滿足企業對機密文件保護的所有需求，DRM當然也有其適用的範圍。

### (一) 企業需要防範作者盜取公司機密文件

DRM技術，主要的防範對象是一般使用者，而非作者。對僅具讀取權限的一般使用者而言，因限制應用軟體的複製、列印、抓錄畫面等功能，可以防範一般使用者盜取企業的機密文件。

為什麼DRM無法防範「作者」呢？因為當開啓文件時，文件的作者、或擁有編輯權限者，可以將畫面資料複製到電子郵件或其他檔案，仍可外洩盜取機密文件，因此無法防範作者、編輯者盜取企業的機密文件。

若要防範「作者」盜取公司機密文件，具體的做法為採用「即時讀寫加解密」技術，文件儲存時自動加密保護，開啓時自動解密。為了達到保護但是不犧牲好用的複製功能，提供「單向複製」的功能，即採用複製或拖曳的方式，受保護的文件無法將內容複製至未受保護的文件，但是未受保護的文件可複製至受保護的文件。

### (二) 企業需要保護更多的檔案格式

DRM產品無法保護許多的檔案格式。為什麼呢？因為DRM產品需於開啓文件後控制複製、編輯、列印、程式存取的功能，包括選單、工具列按鈕、快速鍵等。

但是，自從微軟公司的RMS推出以來，只有微軟公司自家的Word、Excel、PowerPoint、Outlook 2003/2007應用軟體架構於其RMS，其他應用軟體的原廠都未支援微軟

公司的RMS。

因此，若應用軟體原未提供DRM的功能，則必須於每一個應用軟體（與每一個版本）都提供一個特定的外掛(plug-in)程式，來控制限制複製、編輯、列印、程式存取的功能，需要使用Hook技術控制其選單、工具列按鈕、快速鍵的動作。

若要控制AutoCAD應用軟體，則需要於每一個版本各提供一個外掛程式，即使做得出來，很可能仍有未控制到的安全漏洞。

由於微軟Office 2003/2007、Windows Vista、MOSS 2007、Windows Server 2003/2008等產品整合了DRM的功能，根據我們的經驗，建議僅使用DRM於Microsoft Office、Arobat PDF檔案的保護。

Microsoft Office保護則建議直接採用Office 2003/2007內建的IRM功能較安全，因為IRM/RMS保護的Office檔案迄今還尚未被破解，而Office外掛程式則容易有安全漏洞的疑慮。

要解決保護更多檔案格式的需求，具體的做法為採用「即時讀寫加解密」技術，可以保護所有的檔案格式。

總結來說，數位版權管理(DRM)產品，適用於保護Word、Excel、PowerPoint、Outlook 2003/2007、PDF文件，以及會放置於資訊分享、資訊管理系統的機密文件。DRM適合防範一般使用者，但是不適合防範作者盜取機密文件。即時讀寫加解密產品，則適合於保護CAD/CAM 繪圖軟體、程式設計、Video/Audio 檔案，適合防範「作者」盜取機密文件。