

資料外洩防護 (DLP) 導入經驗分享

此文章由 [中華軟協](#) 發表於 2008 年 12 月 2 日 下午 15:48

作者：博格科技 周世雄 總經理

刊登於 中華民國資訊軟體協會 e 化部落 <http://eblog.cisanet.org.tw/post/20081202dlp.aspx>

五年來，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，我們投入資料外洩防護 (DLP) 產品的研發工作。本文將五年來數百家企業的 DRM 導入經驗與需求，與讀者分享。

數位版權管理 (DRM)

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

資料外洩防護 (DLP) 解決方案之一為「數位版權管理」(Digital Rights Management，簡稱 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。

將具有數位版權管理 (DRM) 保護的文件轉給別人，別人也無法開啟，其主要關鍵點在於：「開啟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，而無法開啟文件。

微軟的數位版權管理 (DRM) 相關產品

微軟公司於 2003 年 11 月，推出數位版權管理所需要的「微軟 DRM 平台」，包括 Office IRM (Information Rights Management)、與 Windows RMS (Rights Management Services) (授權伺服器) 等產品與技術。



(微軟 DRM 平台)

應用軟體方面，微軟公司的 Office 2003、Office 2007 整合了 Office IRM 技術，其中 Word、Excel、PowerPoint 檔案讓作者可以設定是否可以讀取、列印、複製、到期日、程式存取、需要每次連線等權限；而 Outlook 則提供讓作者可以設定郵件是否不可轉寄的功能。

企業入口網站方面，微軟公司的 SharePoint 產品 WSS 3.0、MOSS 2007 整合了 DRM 的功能，根據資料夾的 Access Control List (ACL) 權限設定，於下載 Word、Excel、PowerPoint 檔案時自動加密，僅提供是否可以讀取、列印、複製等權限。

作業系統方面，微軟公司的 Windows XP 需要安裝 RMS Client 1.0 SP2，Windows Vista 則內建 RMS Client；而授權伺服器方面，Windows Server 2003 需要另外安裝 RMS Server 1.0 SP2，Windows Server 2008 則內建了 RMS Server 2.0。

數位版權管理 (DRM) 的企業需求

五年來，洽談了近百家的客戶，我們解決了企業對於數位版權管理 (DRM) 的許多需求，譬如：

一、集中管理的機密文件，企業需要有自動加密的功能：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。

當我們接到這個需求時，原本以為不會太困難，方法為當要加密時，只要使用程式開啟 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，原因為加密時於伺服器不斷地開啟 Microsoft Office 軟體，造成不穩定的大問題。

為了解決這個問題，我們研究了 Office 2003/2007 IRM 保護格式，不需要開啟 Office 軟體，即可完成加解密的動作，客戶導入後，滿意度大幅度地提升。

二、於企業入口網站 (SharePoint)，企業需要更彈性的的文件保護功能。

當企業導入微軟公司的 SharePoint 產品 WSS 2.0/3.0、SPS 2003/MOSS 2007 時，企業需要更彈性的的文件保護功能，譬如：

1. 可設定公司內部的權限政策 (Policy)：譬如機密、極機密等，解決之道為整合 RMS 的「權限原則範本」功能，讓權限管理者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。
3. SharePoint 下載的加密文件可以傳給其他有權限的使用者：雖然 WSS 3.0、MOSS 2007 於下載文件時會依照此使用者於 ACL 的權限自動加密，但是只會加上此使用者的權限，因此無法傳給別人，其他使用者必須到 SharePoint 下載加上其權限的文件。

三、企業需要更安全的文件保護功能。

安全性方面，企業需要照相保護、抓圖保護等功能：

1. 抓圖保護：可以保護所有應用軟體的內容不會透過螢幕截取 (包括 print screen 鍵) 的方式外洩出去，需要防止多種螢幕截取影像、圖片的軟體截取受保護檔案的螢幕內容。

2. **照相、列印保護**：自動加上螢幕、列印動態浮水印以嚇阻與稽核，「自動加上螢幕浮水印」的保護功能，可以針對透過照相方式外洩機密文件的行為達到稽核與嚇阻的目的。開啟文件時，於應用軟體動態地於螢幕自動加上開啟者的 Email、電腦與開啟日期時間之浮水印。

為了安全考量，當 Office 2003、Office 2007 於僅具讀取權限時，整個文件是鎖住的，無法加上動態的浮水印，我們曾經吃盡了苦頭，最後使用獨特 Hook 技術提供了浮水印的功能，還申請了發明專利。

四、企業需要將「系統管理」與「權限管理」兩個角色分離：譬如資訊部門則負責系統的建置維護，而各部門自行管理設定機密文件的權限。

這個需求十分重要，因為資訊部門並不需要負責變動頻繁的權限設定，大幅度降低工作負荷，而各部門於新增加資料夾、變更資料夾權限等的時候，也可以快速地變更成所需要的設定，不需要等待資訊部門。

五、將機密文件給外部使用者，企業需也有保護功能。

外部使用者不需連線到公司伺服器，即可開啟文件，譬如限制過期日、開啟次數、開啟幾次後自動刪除，並加上浮水印、密碼保護等。

結語

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。DRM 產品，也不容易保護許多的檔案格式。要解決這個需求，比較合適的是「即時讀寫加解密」產品，可以保護所有的檔案格式。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。

作者小檔案

作者周世雄，現為博格科技總經理，從蘋果二號玩到 Web-based、.NET，將二十幾年電腦研發與行銷的工作經驗，以及十年來累積數百家企業的 DLP、BPM 導入經驗與需求，歸納出有助於企業解決資料外洩防護與商業流程管理等問題的想法，以及產品。

榮獲經濟部【新創事業獎】、【創新研究獎】、【卓越 SBIR 產業貢獻獎】、台大創新育成中心【績優廠商獎】等政府獎項，以及 Microsoft【合作夥伴服務英雄獎】、【服務領導有方獎】、【Best IW Solution Partner Award】、【Windows Vista 應用軟體金像獎】、【Microsoft Office System 解決方案獎】等獎項，連絡 Email：JackChou@borg.com.tw