

DLP 採用的五個關鍵因素

資料外洩防護產品大解剖

作者：博格科技 周世雄

刊登於 RUN!PC 雜誌 (2008 年 12 月)

本文重點

作者整理歷經五年來參予即時讀寫加密、數位版權管理等資料外洩防護產品設計的經驗，和歸納近百家客戶的需求與導入所需考慮的重點，與讀者分享熱門的資料外洩防護產品能夠被廣泛地採用的關鍵因素，並分析各種資料外洩防護產品的優缺點、適用範圍、選購注意事項。

資料外洩防護上所面臨的挑戰

近年來，重大的資料外洩事件不斷地發生，加上防毒公司搶著併購 DLP 公司的消息炒熱了新聞，資料外洩防護 (DLP) 愈來愈熱門，成為今年最受矚目的資訊安全產品。

「資料外洩防護」簡稱「DLP」，DLP 為「Data Loss Prevention」、或「Data Leakage Prevention」的縮寫。

市場上陸續推出了林林總總的資料外洩防護 (DLP) 產品，嘗試解決企業於機密資料外洩防護上所面臨的挑戰，包括：

- ◇ 防範作者：文件的作者、編輯者洩漏公司的機密資訊。
- ◇ 防範駭客：駭客、木馬入侵竊取公司機密資訊。
- ◇ 防範設備遺失：筆記本電腦、隨身碟等設備遺失，洩漏設備內的機密資訊。
- ◇ 防範離職員工：離職員工帶走公司的重要資料，洩漏機密資訊。

以確保透過 Email、Web、MSN、隨身碟、列印、照相等方式不會洩漏公司的機密文件。

DLP 產品被廣泛地採用的五個關鍵因素

「安全」與「方便」，的確是資訊安全產品難以取捨的兩難，許多公司導入早期推出的資料外洩防護 (DLP) 產品後，雖然「安全」，但是不「方便」，造成使用者反彈、怨聲不斷，最後被迫只得縮小使用規模，限制只使用於一、兩個少數部門。

資料外洩防護 (DLP) 產品，到底是否能夠於企業內部被廣泛地採用呢？還是只能侷限於少數部門使用呢？

而能夠被廣泛地採用的主要關鍵因素在那裡呢？

若要導入一個可於企業內部被廣泛地採用的資料外洩防護 (DLP) 產品，除了「**安全性**」為最基本的考

量外，筆者認為「**改變使用者的習慣**」，與「**犧牲電腦的使用功能**」是造成使用者怨聲載道的主要原因，因此必須基於「**不改變使用者的習慣**」，與「**不犧牲電腦的使用功能**」的兩個原則下，針對「**所有檔案格式**」的機密文件自動進行保護措施。

是否很「**容易佈署導入**」也很重要，「**需要制定複雜的企業權限政策**」、「**需要預先進行文件的分級**」、與「**使用者反彈**」是造成企業猶豫不決採購遲緩的主因。

因為若需要先制定複雜的企業權限政策，才可以佈署，則往往需要找內部許多部門開好幾個月的會議，才能協調出企業可以接受的權限政策；而若需要預先進行文件的分級，才可以導入，則需要不斷耗費大量的人力，針對每一個新產生的文件進行分級的工作。

因此，資料外洩防護（DLP）產品能夠被廣泛地採用的主要關鍵因素有五個，即：

1. **安全性**。
2. **不改變使用者的習慣**。
3. **不犧牲電腦的使用功能**。
4. **保護所有檔案格式**。
5. **容易佈署導入**。

資料外洩防護（DLP）產品分析

廣義的資料外洩防護（DLP）於市場上主要的產品，有檔案控管（File Protection）、週邊控管（I/O Protection）、和網路控管（Lan Protection）等三種類型，而其中檔案控管（File Protection）又包括即時讀寫加解密、數位版權管理（DRM）等兩種產品：

1. **檔案控管（File Protection）：**

甲、**即時讀寫加解密**：於讀寫時自動進行文件加密和解密操作，從而達到保護文件的目的。

乙、**數位版權管理（DRM）**：發佈前將機密文件加密，開啟檔案時必須取得使用授權，傳給別人無法開啟。

2. **週邊控管（I/O Protection）**：針對用戶端電腦的輸出入、與儲存裝置等週邊硬體，進行限制（禁用、不可寫）、記錄（USB、列印）。

3. **網路控管（Lan Protection）**：使用網路控管軟體對流經網路的email、MSN、Skype、http、ftp等通訊進行限制，或對電子郵件或網路進行側錄、監控、記錄。

詳細說明如下：

解剖即時讀寫加解密產品

即時讀寫加解密產品，於以前仍舊不成熟，時常造成用戶電腦不穩定或當機，甚至毀損檔案。到了今年，即時讀寫加解密技術已漸臻成熟，有的也可於 Windows Vista 操作系統下穩定地運作。

即時讀寫加解密產品，技術門檻極高，需要設計驅動層（Driver Layer）程式，為 kernel-mode driver，採用「即時讀寫加解密」技術，針對所有檔案格式的受保護文件，於讀寫時自動進行文件加密和解密操作，從而達到保護文件的目的。

「即時讀寫加解密」是指用戶在操作過程中，不改變對文件的開啟或關閉習慣，不改變檔案名稱，不須額外操作，整個加密（解密）操作過程是自動完成的。請參考下圖：



即時讀寫加解密技術，直接運行於 Windows 作業系統的核心（kernel）中，接管檔案系統，自動識別什麼文件需要進行加密、解密操作，哪些不需要，將文件資料以密文形式儲存在硬碟機等儲存設備上，當需要讀寫該加密文件時，進行解密，使得系統在授權情況下可以即時地以明文形式讀該加密文件的資料。

即時讀寫加解密產品，不需要限制儲存裝置、輸入出裝置、網路、Email、MSN 的使用功能，因為檔案儲存時就處於加密狀態，即使外洩也無法開啟。

即時讀寫加解密產品，不需先制定企業權限政策，不需先進行文件的分級，即可佈署導入。

有的即時讀寫加解密產品廠商所提供保護的檔案格式有數量上的限制（100 或 10 種），有的產品則可以保護「所有」的檔案格式，突破的地方為可以「自行增加」新的檔案格式，而不需要找原廠額外花時花錢處理，這是選購時必須注意的地方。

即時讀寫加解密產品，因文件本身已經加密，安全性最高，而且「不改變使用者的習慣、不犧牲電腦的使用功能」，若產品穩定成熟，可期待成為很好的資料外洩防護（DLP）解決方案。

解剖數位版權管理（DRM）產品

近年來熱門的「數位版權管理」（Digital Rights Management，簡稱 DRM）產品，主要是因為微軟公司於 2003 年 11 月，推出 DRM 所需要的「微軟 DRM 的平台」，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 Office 2003/2007、MOSS 2007 產品整合了 DRM 的功能，而微軟公司的新產品也陸續地支援 RMS 功能，譬如 Windows Vista 內建 RMS Client，Windows Server 2008 內建 RMS Server 2.0。

另外，Adobe 公司也推出 DRM 功能的 LiveCycle ES 產品，保護 PDF 格式的安全。

數位版權管理（DRM）產品解決的是，有權限瀏覽機密資料的員工，無法再發佈洩漏給別人，限制其使用範圍與有效時間，並解決人員異動與權限異動頻繁問題，譬如離職後無法開啟電腦機密文件，請參考下圖：



數位版權管理 (DRM) 產品，第一次開啟加密文件時必須連線到授權伺服器先取得使用者授權，所以若使用者將加密文件複製到其他的電腦、或外洩給別人，該加密文件將因無法從授權伺服器取得使用者授權，而無法開啟。

數位版權管理 (DRM) 產品，因限制使用者的複製、編輯、列印、抓錄畫面等行為，可以有效地確保機密文件「發佈後」的安全，可防範一般使用者盜取公司機密文件。

但是因文件的作者（或者擁有編輯權限的使用者），可將開啟檔案的資料複製到其他檔案或 email 而外洩，仍可盜取機密文件，因此無法防範於「**發佈前**」文件的作者、編輯者盜取公司的機密文件。

若檔案集中於檔案伺服器（或企業入口網站）管理，若加上於伺服器自動加密的功能，則不需改變使用者的習慣；若檔案不集中管理，作者需設定權限，文件才受保護，故需稍微改變使用者的習慣。

需要注意的是，筆者有一個慘痛的經驗，若採用 Office 2003/2007 IRM 保護格式，需要於 File Server、SharePoint 自動加密時，若加密時於伺服器不斷地開啟 Microsoft Office 軟體，將會造成不穩定的大問題。

解決這個問題，需要研究 Office 2003/2007 的 IRM 保護格式，程式直接完成加密的動作，不需要開啟 Microsoft Office 軟體。

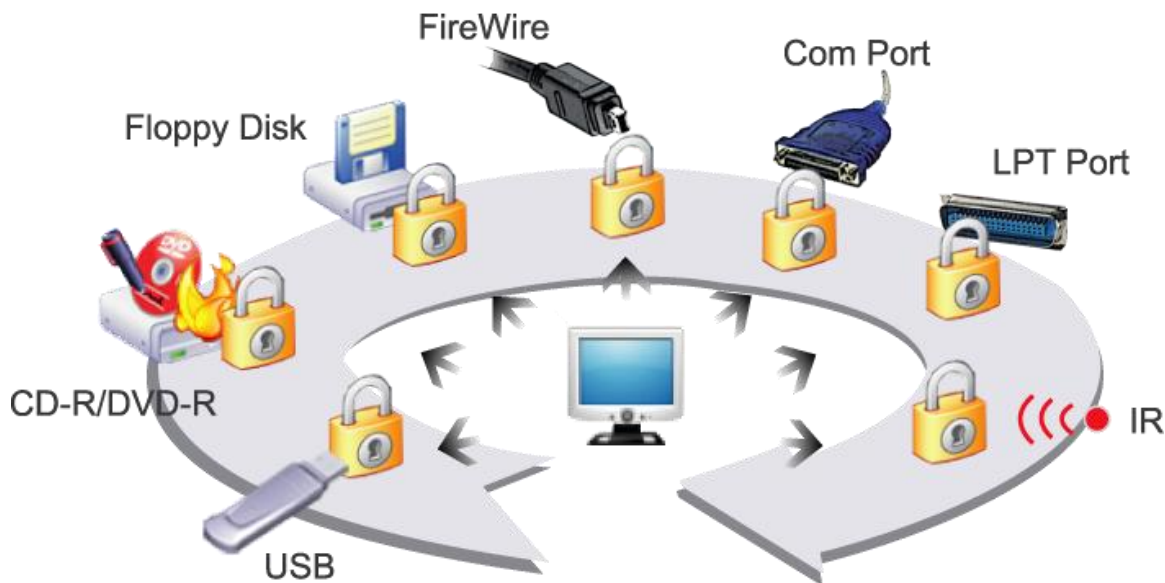
數位版權管理 (DRM) 產品，最大的問題為保護的檔案格式「極有限」，因為若原應用軟體未支援 DRM 功能，則每一個應用軟體的每一個版本都必須開發一個特定的外掛 (plug-in) 程式，來控制複製、編輯、列印的功能，而且很可能仍有安全漏洞。

解剖週邊控管 (I/O Protection) 產品

週邊控管 (I/O Protection) 產品，可中央控管所有用戶端電腦的儲存裝置、與輸出入裝置，如 USB 埠、磁碟機、隨身碟、外接硬碟、燒錄機或印表機，是否禁用、或者僅可讀不可寫，以確保內部機密資料被安全地保護，不致於藉這些裝置出入口而流出。

可控制用戶端電腦的硬體包括儲存裝置（軟式磁碟機、光碟機/燒錄器、隨身碟/隨身硬碟/讀卡機等）、

輸出入裝置（USB port、COM port、LPT port、1394 port、紅外線port等），請參考下圖：



週邊控管（I/O Protection）產品，優點為不需要對機密文件本身進行保護措施。

但是，需犧牲儲存裝置、輸入出裝置的電腦使用功能，譬如限制使用者無法使用 USB 隨身碟、燒錄光碟等，也需要改變了使用者對儲存裝置、輸入出裝置的使用習慣。

因此，週邊控管（I/O Protection）產品的最大問題，為違反了「不改變使用者的習慣」與「不犧牲電腦的使用功能」之兩個原則，並需要注意是否每一種儲存裝置、輸入出裝置是否都可以圍堵得到，遺漏的週邊會造成安全漏洞。

筆者個人強烈認為週邊控管（I/O Protection）為違反人性的產品，這是個當資料外洩防護技術未成熟時期的過渡產物，一旦其他資料外洩防護的技術成熟，勢必被淘汰出局。

解剖網路控管（Lan Protection）產品

網路控管（Lan Protection）產品，使用網路控管軟體對流經網路的資料進行側錄、監控、記錄，或加予限制，請參考下圖：



另外由防毒軟體公司併購 DLP 公司所推出的產品，也可歸類屬於網路控管（Lan Protection），針對機密資料先進行特徵分析，尋找出企業內部需要保護資料的特徵，並於使用者端安裝端點程式，或由網路、開道端來監控，可限制網路功能或用戶端電腦的儲存裝置與輸出入裝置，以阻止員工存取、外洩企業內部的機密資料，或監控員工的機密資料存取記錄。

網路控管（Lan Protection）產品，優點為不需要對機密文件本身進行保護措施。

需要注意的是若不限制網路、Email、MSN 不能傳送檔案、Skype 等功能，則只能事後稽核但是不能即時阻止洩密；若要即時阻止洩密，則需要限制使用，會「犧牲電腦的使用功能」，也改變了使用者的對網路的習慣。

另外，是否所有網路功能是否都可以管控得到，譬如 web email 等，若管控不到會造成安全漏洞。所以，網路控管（Lan Protection）產品，適合於事後稽核，較不強調可以即時阻止洩密，適合於側錄、監控、記錄網路的資料。

那種 DLP 產品能夠被廣泛地採用？

以五個關鍵因素，分析即時讀寫加解密、數位版權管理、週邊控管、網路控管等四種資料外洩防護（DLP）產品，是否能夠被廣泛地採用，首先以「安全性」關鍵因素，比較如下表：

DLP 產品	安全性
即時讀寫加解密	安全性較高：檔案本身已經加密保護。對一般使用者與作者都安全。
數位版權管理	對一般使用者安全，對作者不安全：檔案本身已經加密保護。對作者而言，可將開啟檔案的資料複製到其他檔案或email而外洩，故不安全。
週邊控管	若並非每一種儲存裝置、輸入出裝置都圍堵到，會造成安全漏洞。
網路控管	若管控不到所有的網路功能會造成安全漏洞。

而以「不改變使用者的習慣」關鍵因素，比較如下表：

DLP 產品	不改變使用者的習慣
即時讀寫加解密	不需改變使用者的習慣：儲存時自動加密，開啟時自動解密。
數位版權管理	集中管理不需改變使用者的習慣：若檔案集中管理，可於伺服器自動加密的功能，則不需改變使用者的習慣。 若檔案不集中管理，作者需設定權限，需稍微改變使用者的習慣。
週邊控管	需改變使用者的習慣：限制儲存裝置、輸入出裝置的使用。
網路控管	若犧牲網路的使用功能，則需改變使用者的習慣。

再以「不犧牲電腦的使用功能」關鍵因素，比較如下表：

DLP 產品	不犧牲電腦的使用功能
即時讀寫加解密	不需犧牲電腦的使用功能：不需限制儲存裝置、輸入出裝置、網路、Email、MSN 的使用功能，即使外洩無法開啟。
數位版權管理	不需犧牲電腦的使用功能：即使外洩無法開啟。
週邊控管	需犧牲電腦的使用功能，譬如限制使用者無法使用USB隨身碟、燒錄光碟等。
網路控管	若要即時阻止洩密，則需要限制網路功能，會「犧牲電腦的使用功能」。若只事後稽核不即時阻止洩密，則不需犧牲電腦的使用功能。

續以「保護所有檔案格式」關鍵因素，比較如下表：

DLP產品	保護所有檔案格式
即時讀寫加解密	保護「所有」的檔案格式。
數位版權管理	保護「有限」的檔案格式。
週邊控管	保護「所有」的檔案格式。
網路控管	保護「所有」的檔案格式。

考慮「容易佈署導入」關鍵因素，比較如下表：

DLP產品	容易佈署導入
即時讀寫加解密	容易佈署導入：不需先制定企業權限政策，不需先進行文件的分級，即可佈署導入。
數位版權管理	需先制定企業權限政策。
週邊控管	容易佈署導入，但是容易造成使用者反彈、怨聲不斷。
網路控管	側錄產品較容易佈署導入，可即時阻止洩密的產品需先制定企業權限政策。

結論

歸納以上的分析，將各種資料外洩防護（DLP）產品的優缺點，比較分析列表如下：

DLP產品	優點	缺點
即時讀寫加解密	符合「安全性、不改變使用者的習慣、不犧牲電腦的使用功能、保護所有檔案格式、容易佈署導入」五個關鍵因素。	若設計不良，可能造成用戶電腦不穩定或當機，甚至毀損檔案。
數位版權管理	微軟Office 2003/2007、Windows Vista、MOSS 2007、Windows Server 2003/2008等產品整合了DRM的功能。	保護的檔案格式有限。
週邊控管	不需要對機密文件本身進行保護措施。	需要圍堵到所有的儲存裝置、輸入出裝置。 犧牲電腦的使用功能。 改變使用者的習慣。
網路控管	不需要對機密文件本身進行保護措施。	需要監控到所有的網路功能。 若要即時阻止洩密，則會犧牲電腦的使用功能，並改變使用者的習慣。

最後，將各種資料外洩防護（DLP）產品的適用範圍、與選購注意事項，歸納列表如下，供大家參考：

DLP產品	適用範圍	選購注意事項
-------	------	--------

即時讀寫加解密	可防範一般使用者、與作者。 適用於保護CAD/CAM繪圖軟體、 程式設計、Video/Audio檔案。	是否僅保護有限（100或10種）的檔案格式， 並限定特定的版本，無法「自行增加」新的檔 案格式。 是否造成用戶電腦不穩定，檔案毀損。
數位版權管理	可防範一般使用者，但是不能防範 作者，適用於保護「發佈後」文件。 可集中於檔案伺服器（或企業入口 網站）管理，於伺服器自動加密。	建議僅使用於Office、PDF檔案的保護，使用 Office 2003/2007內建的IRM功能較安全。 若原應用軟體未支援DRM功能，極有可能有 安全漏洞。 若採用Office IRM保護格式於File Server、 SharePoint統一加密時，不能於伺服器開啟 Microsoft Office軟體，肯定有不穩定問題。
週邊控管	適用企業內部少數部門採用。 違反人性、漏洞較多，需要檢討是 否為過渡時期的產物。	儲存裝置、輸入出裝置的安全漏洞。
網路控管	適合只事後稽核較不強調可以即時 阻止洩密，適合於側錄、監控、記 錄網路資料。	需要即時阻止洩密，或只要事後稽核。 網路的安全漏洞。

作者介紹 周世雄 JackChou@borg.com.tw

專長為「從新技術當中創造藍海市場」，累積 17 本電腦書的著作經驗，和微軟公司 TechEd 等近百場研討會的教學經驗，以及資料外洩防護、商業流程管理等軟體設計的實戰經驗，從蘋果二號玩到 Web-based、.NET，有二十幾年電腦研發與行銷的工作經驗，現任職於「博格科技」公司總經理。