情報顧問

Advisory & Intelligence Service Program

產 業 研 究 報 告

Software and Services

強化設計資產保護－以加密追蹤防止 3D 設計資料外流

前言

對設計製造業而言，各種類之 3D 設計檔案、資料可說是公司最貴重的資產。如何方能確保此種重要的無形資產不外洩，乃是至關重要的問題。若是您對僅以 ID 及密碼限制登入權限、爲檔案加上密碼等傳統資料保密方式感到不安，本文中將介紹保障資料安全的最新方法，讓資料保密更爲周全。

原作：中山 力（日經 BP）

編審：曾維真、龔俊光

Document Code: CDOC20080710011
MIC Publication Date: July 2008
Check out Nikkei BP on the Internet!
http://consult.nikkeibp.co.jp
Check out MIC on the Internet!
http://mic.iii.org.tw/intelligence

目錄

頁次

圖目錄

頁次

2007 年 3 月時，爆發了汽車零件廠商工程師因違法攜出設計資料而遭到逮捕的事件。在這個事件中，該名具有登入資料庫權限之技術人員，於公司內以筆記型電腦下載資料後，將之帶回住處。雖然公司方面認爲該技術人員有將資訊洩漏給競爭對手之嫌疑，但由於嫌疑犯已將 HDD 等儲存媒體破壞，因此無法確認事情真僞，無法追究其刑事責任。

由於 CAD 等 IT 工具日漸普及，使設計資料不但可透過網路於轉眼間傳輸至遠方，同時也容易進行複製。

由於一分設計資料將逐漸跨越公司之間的隔閡，遍及設計、生產製程的每個環節，因此，如何確保 3D 資料的安全性將成爲今後首要之務。此外，若是涵蓋外型、尺寸規格、屬性等細部資料之 3D 圖面也開始廣爲流通時，一旦資料外洩，造成的損害也將更爲龐大。

設計資料堪稱是製造業的智慧財產。保護設計資料免於不法利用，是保持競爭力不可或缺的要素。現行對策包括「利用 ID 及密碼限制登入權限」、「經由網路傳輸或儲存於記錄媒體時，進行加密處理」等。

然而，欲將獲得之資料實際運用於業務方面時，仍需將先前經過加密處理的資料復原（解密）。但是，密碼解除後便有可能將資料複製儲存，進而將之轉交給外部人士。即使採用禁止寫入 USB 隨身碟或透過網路監視資料傳輸等方法，若是如前述事件般，將原本的儲存媒體直接帶走時，資料仍會外流。一旦資料外流，幾乎不可能成功將之徹底回收（圖一）。

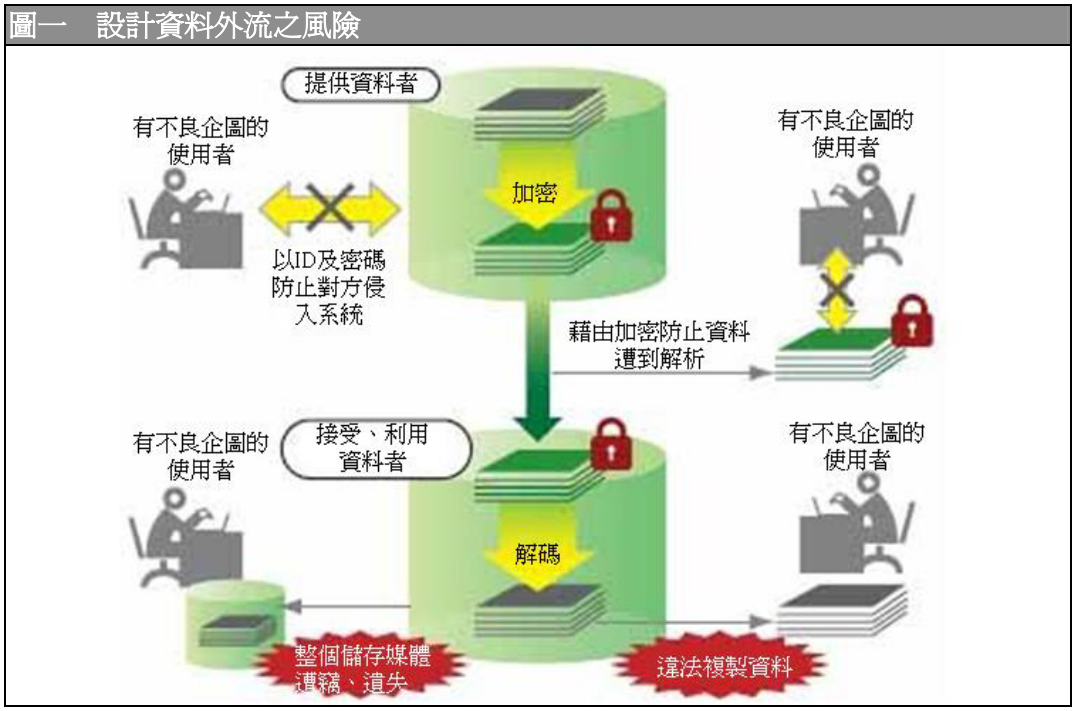
某些公司採取使用者無法將資料保存於自己所用電腦之「Thin Client」方式以防止弊端。如此一來，即使整台電腦遭竊，資料也不至外洩。

雖然已有對應 Thin Client 的 3D CAD 程式出現，但由於 Thin Client 基本上較適合小範圍少數利用者的狀況，因此仍有其極限。除必須事先導入 Thin Client 用之相關程式外，若是處理業務過程中需要時常收發檔案時，則相關程序也必須隨之進行調整。

是否已有一方面能夠維持在電子郵件中附加檔案、郵寄儲存媒體等現行傳遞資訊方式，同時仍可提高資訊安全性的方

法？近來，這方面最受矚目的技術非「DRM（Digital Right Management，數位版權管理）」莫屬。透過這項技術，即使在交付檔案後仍可變更使用權，也能夠將可能遭到不法利用的資料全部變更爲無法使用的狀態。另外，此項技術還具有能夠防止相關人員誤用設計變更前之舊資料的優點。

圖一　設計資料外流之風險



圖說：即使製作時予以嚴密管理，於實際運用時仍然必須面對諸如處於可用狀態的設計資料之複製、儲存媒體失竊等檔案外洩之危機
資料來源：NikkeiBP，資策會 MIC 整理，2008 年 6 月

小型 3D 資料加密

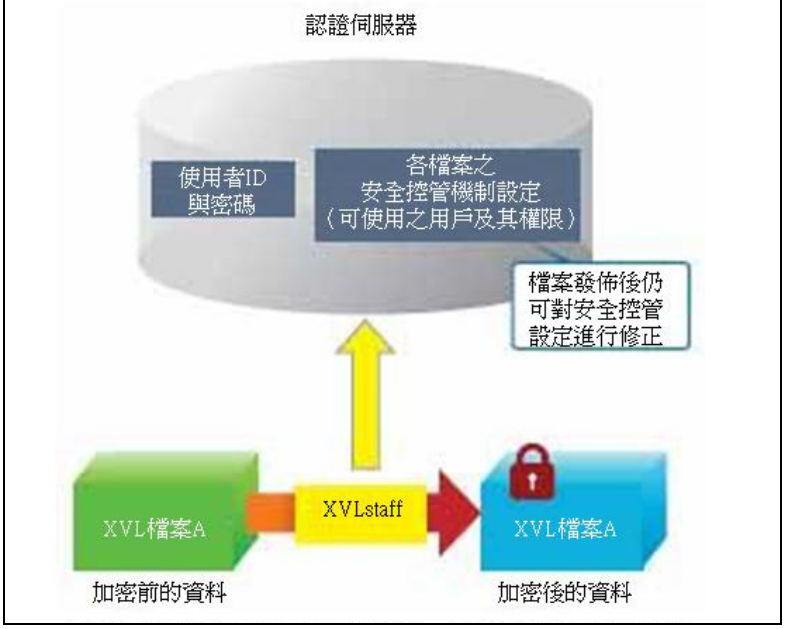
3D CAD 程式的價格昂貴，這也是 3D 資料不法利用問題至今仍未造成嚴重問題的原因之一。「必須先付出數百萬日圓購入 3D CAD 程式後才能讀取資料」，此門檻本身便可稱之爲一種防範機制。

然而，對於爲使 3D 資料能更廣爲流通、更受各界活用而日漸普及的小型 3D 資料，則可能藉由利用某些只利用觀看功能時不需付費的工具程式等方法，以較低的成本導入。因此，顧慮到不法流出的問題，部分廠商開始於發布小型 3D 資料時採取較爲慎重的態度。

開發出一種小型 3D 檔案格式「XVL」，總公司位於東京的 Lattice Technology 也將這點納入了考量。因此，該公司與 Hitachi Software Engineering（日立軟體工程，以下簡稱日立軟體）開始合作進行使 XVL 檔案能夠適用 DRM 之開發工作。爲使該程式可使用 DRM，必須用到美國 Adobe System 的「Adobe LiveCycle Right Management ES」之功能。

LiveCycle Right Management ES 原本是爲 PDF 檔而開發之程式（預定於 2008 年夏季時開始支援 Microsoft Office 檔案），因此，日立軟體接受 Adobe 提供 SDK（程式開發套件），開發出具有對應 XVL 檔案機能之程式「XVLstaff」。XVLstaff 除可將檔案進行加密處理外，還具有可以設定哪些使用者能進行何種操作的「安全控管機制」。使用者的資訊（ID、密碼）及各 XVL 檔案之安全控管機制資訊都儲存於認證伺服器之中。

圖二　XVL 資料的安全設定

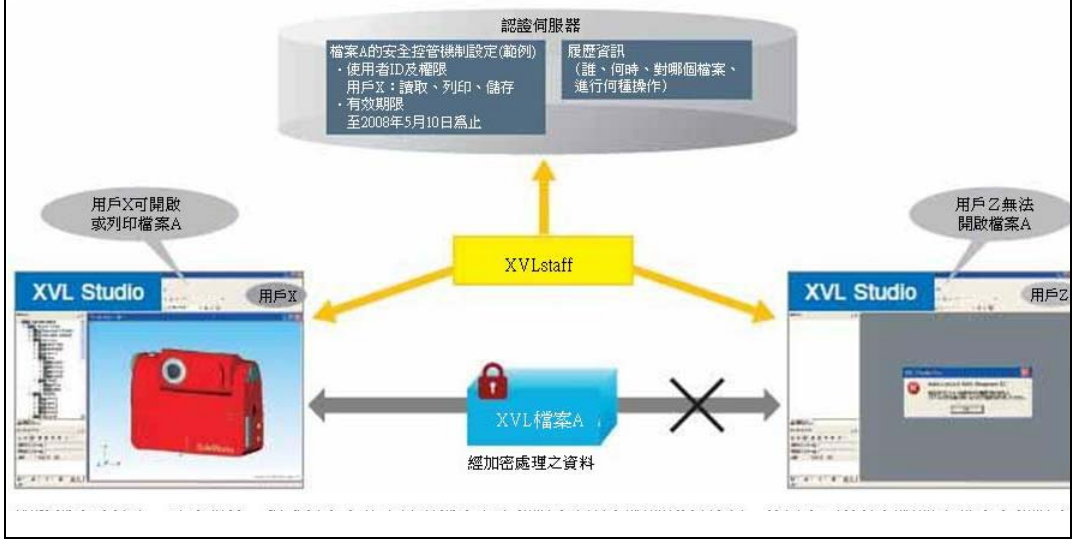


圖說：XVLStaff 可使 XVL 資料進行加密處理，並將安全控管機制資訊寫入伺服器。管理者可進行「哪位用戶獲准進行何種操作」、「檔案有效期間至何時爲止」之類的設定，這些設定於檔案發佈後仍可變更

資料來源：NikkeiBP，資策會 MIC 整理，2008 年 6 月

經過 XVLstaff 進行加密處理的 XVL 檔案，只能以 XVL 編輯工具程式「XVL Studio」開啓，且開啓時需輸入使用者的 ID 與密碼。XVL Studio 會將檔案及使用者資訊反映給認證伺服器，由伺服器進行「該使用者是否可開啓該檔案」、「能夠對該檔案進行何種操作」等判斷。

圖三　如何利用經過加密處理的 XVL 資料



圖說：開啓檔案時輸入 ID 及密碼後，程式便會向負責管理檔案登入權限之認證伺服器進行確認。使用者可依據伺服器內設定之權限來運用檔案
資料來源：NikkeiBP，資策會 MIC 整理，2008 年 6 月

由於採用此種機制，因此不必在每次變更某個 XVL 檔案之安全控管機制後，都必須再次進行加密處理，即使於資料發佈後亦然。此外，因爲能夠收集到「誰」「何時」「做了什麼」的履歷記錄，對事後追蹤也有所助益。

可使用免費程式進行瀏覽

雖然現在尚未出現實際導入 XVLstaff 的企業，但日立軟體表示已開始進行接近實際應用狀況之相關測試。該公司指出：「許多感到僅將資料加密或以密碼鎖定仍不夠周全之企業用戶，已開始詢問相關價格等資訊」。

在用戶所提出的詢問中，「希望接受資料者能夠使用免費瀏覽程式」的需求佔相當高比例。小型 3D 資料原本的誕生目

的之一，就是爲了擴大流通範圍，雖說 XVL Studio 之價格低於 3D CAD 程式，但使用者仍不希望因此而增加所有來往客戶及相關部門之負擔。

雖然目前已有可瀏覽 XVL 檔案的免費程式「XVL Player」，但該程式尚無法開啓經 XVLstaff 加密之 XVL 檔案。日立軟體表示，該公司「正在評估不久的將來可利用 XLV Player 的構想」。

另一方面，總公司位於名古屋的 Data Design 已於 2008 年 5 月推出的「SpinFire Protect」（美國 Actify 公司），則採取接收資料者所使用的瀏覽程式免費之方案。該程式可對應 Actify 的 3D 工具程式「SpinFire」之專用檔案格式「.3D」，並且透過與美國 AirZip 公司技術合作方式導入 DRM。

該程式對.3D 檔案進行加密處理，設定安全控管機制之程式介面與 Windows 的 Explorer 類似。以右鍵點選開啓位於主機或網路上之.3D 格式檔案後，便可對各使用者進行「閱覽」、「列印」、「解密」、「變更權限」等相關權限設定，並將加密後的檔案以「.azs」格式儲存。此外，該程式也可將相關檔案放入特定資料夾後，採用觸發（Trigger）方式進行批次處理（圖四）。

開啓.azs 檔案需要專用程式，若是該主機尚未安裝所需程式，雙擊.azs 檔案後便會自動從伺服器下載所需程式。輸入 ID 及密碼後，瀏覽程式會將資料回傳認證伺服器，使用者此時便可依照被設定之權限來閱覽檔案。

SpinFire Protect 也能防止畫面遭到擷取。該瀏覽程式無法在已啓動畫面擷取程式的狀態下運作，且「Print Screen」鍵也無法使用。另外，雖然.azs 檔案可以嵌入 PDF 或 Word、Excel 等非 3D 資料檔案內，但由於這些檔案也需經由瀏覽程式才能顯示，因此可適用相同的安全控管機制。

圖四 「SpinFire Protect」的畫面

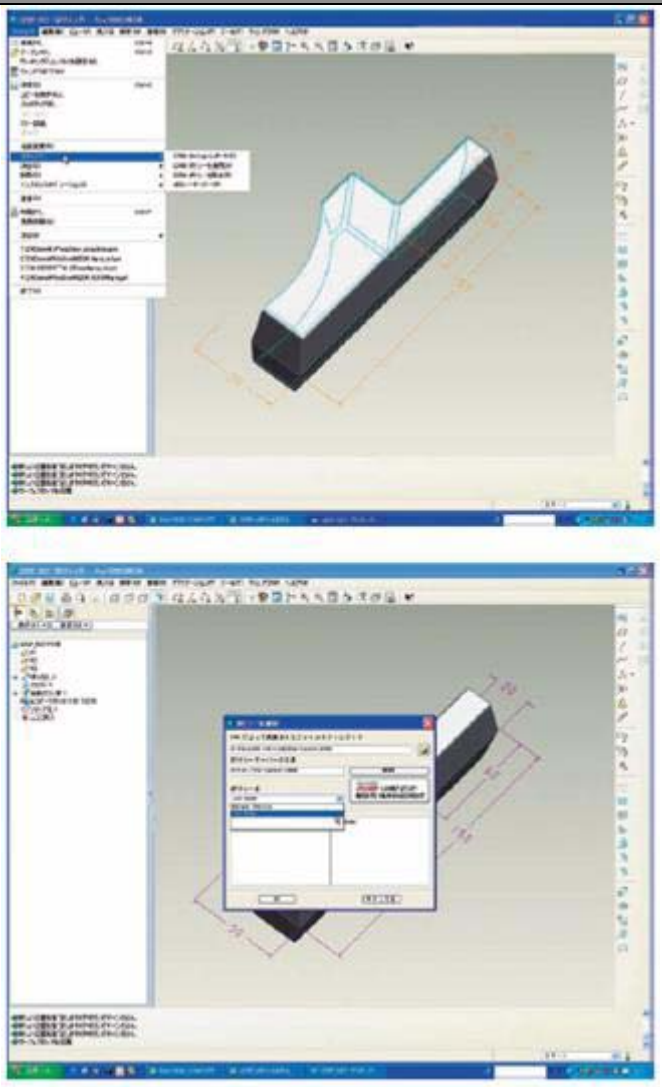
圖說：在近似 Explorer 的畫面中選取檔案、設定權限。在權限設定畫面中，除可針對各用戶或團體分別設定其權限外，也能夠設定有效期限
資料來源：NikkeiBP，資策會 MIC 整理，2008 年 6 月

使 DRM 適用於 3D CAD

除小型 3D 資料外，也開始出現將 DRM 運用於 3D CAD 原始檔案之趨勢。美國 PTC 公司於 2008 年 1 月推出的「Pro／ENGINEER Wildfire」最新版本 4.0 版中，新增了「Pro／ENGINEER Right Management Extension（以下簡稱 RMX）」的選項。它與 XVLstaff 同樣利用由 Adobe 提供的 LiveCycle Right Management ES 之 SDK 進行開發。

安裝 RMX 後，便可將 Pro／ENGINEER 本身進行加密。此外，欲開啓已經加密的 Pro／ENGINEER 原始檔案時，雖不需要用到 RMX，但程式版本須爲最新版（4.0）。RMX 的認證機制等基本架構與 XVLstaff 相同，但在權限種類上略有差異。

圖五　「Pro／ENGINEER」的安全設定

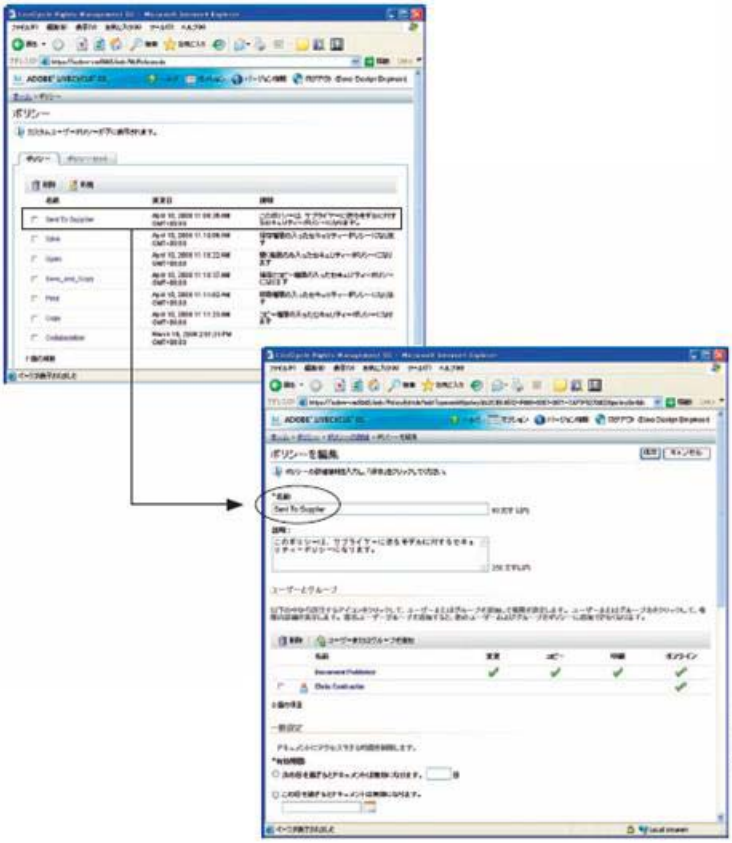


圖說：在檔案選單中的安全設定項目下，選擇「適用 DRM 機制」後便可連結認證伺服器。輸入 ID 及密碼後，即可選擇欲進行之安全設定

資料來源：NikkeiBP，資策會 MIC 整理，2008 年 6 月

目前，RMX 除最低程度的「開啓」權限外，另有「列印」、「複製」、「變更」、「離線」等 4 種權限可供選擇。其中「複製」項目可將資料儲存爲不具修改紀錄等之 Shape Data（中介檔案格式），「變更」則可修改物件外形並另存新檔。以複製方式儲存之檔案，因未經加密處理，故需多加注意，變更後儲存之檔案則能夠直接沿用原有之安全控管機制設定。

圖六　編輯「Pro／ENGINEER」的安全設定



圖說：可事先依照不同用途，設定要賦予各使用者何種權利。舉例來說，在下方的畫面中列出的就是「適合協力廠商之設定」的內容
資料來源：NikkeiBP，資策會 MIC 整理，2008 年 6 月

舉例來說，取得產品之 3D 檔案後，於設計鑄模等情形時，可能會出現需要參考部分原有資料，將資料翻轉以便運用的狀況。即使此時只用到初期 Shape Data 的一部分，但只要其中仍包含任何與成品外形（設計）有關的資訊，便應盡量避免發生資料違法外流的狀況。

使用經 RMX 保護的資料進行作業時，即使主機內僅留下些許參考用原始資料，安全控管機制也仍會繼續運作。如此可使接收資料者於運用時不致遭受過大阻礙，同時也能確保資訊安全。

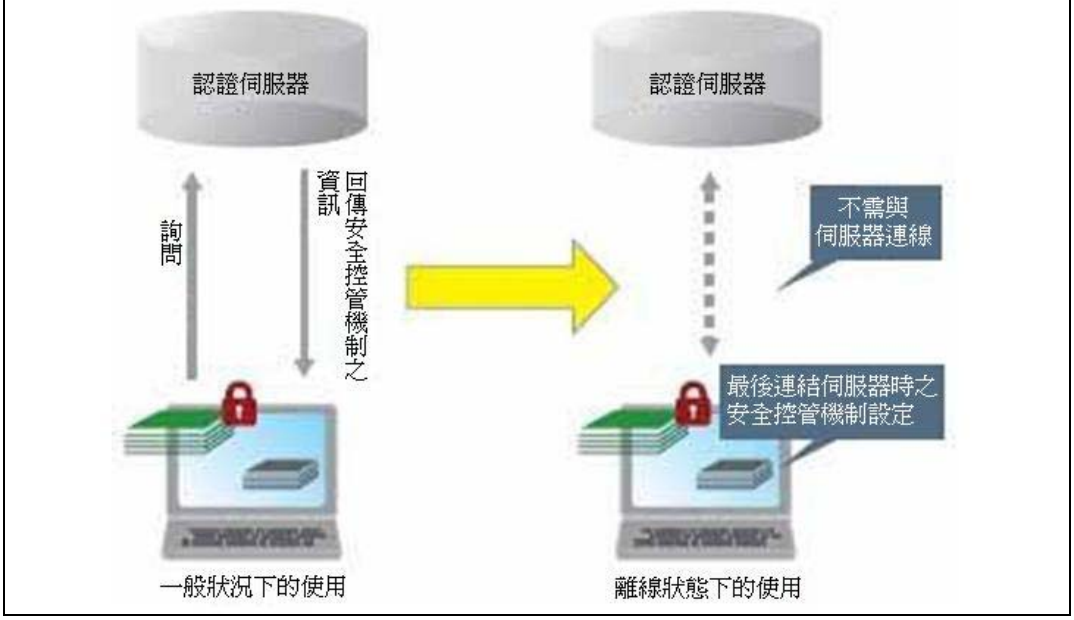
今後，PTC 預定對 Pro／ENGINEER 的模組操作進行可設定更詳細權限之相關調整。另外，該公司也正在進行將 DRM 機能整合進旗下之檔案管理工具程式「Windchill」，以及付費瀏覽程式「Product View」對應 RMX 之計畫。

離線時亦可使用

除「提供接收資料者免費瀏覽程式」之外，預定導入相關程式還包括「於離線狀態下亦可進行操作」，這一點是基於使用者的強烈期望。例如使用筆記型電腦，在公司以外的地點進行討論之類的情況下，開啓加密檔案時仍必須隨時與認證伺服器保持連線，可能會對業務造成妨礙。

雖說於離線狀態下利用資料之行爲與 DRM 原始目的「隨時讓安全控管機制保持在最新狀態」有些許相違之處，但這次介紹的 3 種產品都具有可在離線狀態下使用的功能。不過，這 3 種產品也必須在初次開啓檔案時，使主機與認證伺服器保持連線狀態。之後即使未連上網路，也可開啓 3D 資料。

圖七　離線狀態時的使用



圖說：初次使用時仍然必須先與認證伺服器連線，以確認安全控管機制設定，若是獲准於離線狀態下使用時，則第 2 次之後即可在未連結伺服器的情況下開啓檔案
資料來源：NikkeiBP，資策會 MIC 整理，2008 年 6 月

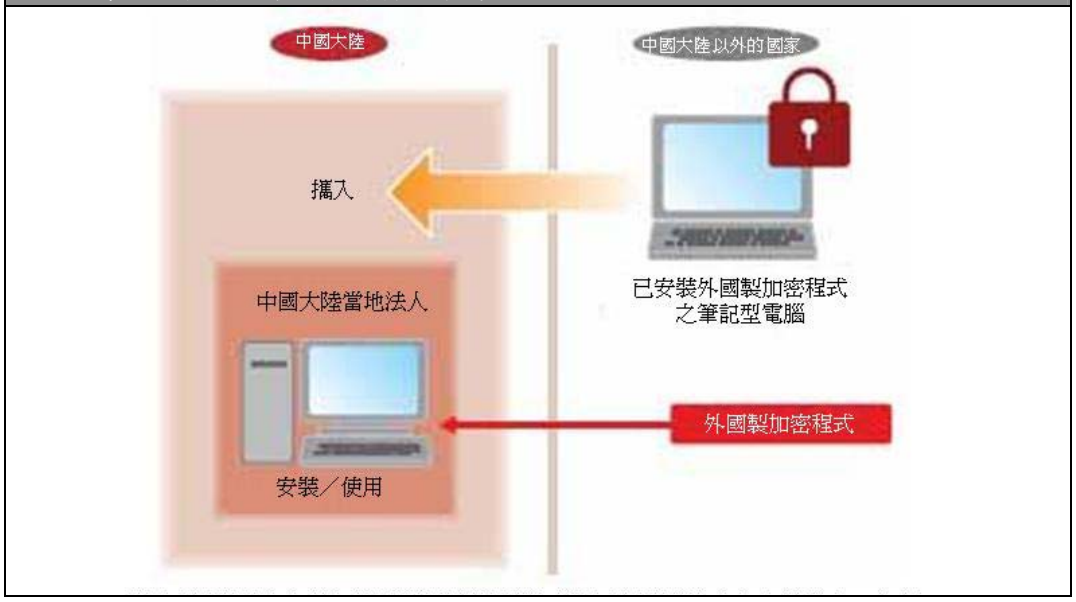
使用離線操作機能時，安全控管機制設定將保持在最後連結認證伺服器時之狀態。也就是說，即使某位用戶於離線狀態下進行作業時，其安全控管權限有所變動，改變後之設定也無法立即適用於該用戶。在一般使用狀態下，主機會定期與認證伺服器進行通信，下載最新的安全控管機制設定。

因此，對於離線狀態下的操作設有使用期限，藉此避免用戶持續使用舊的安全控管機制設定。另外，由於安全控管機制設定會被寫入工具程式之內，所以若只將資料轉移到其他電腦，仍舊無法在離線狀態下使用。

中國大陸對加密程式的限制

在使用加密程式時，必須考慮到中國大陸的狀況。中國大陸對於在其境內銷售、使用其他國家開發的加密程式之事設有相關限制。實際上，曾經發生過日本技術人員未經許可，便擅自攜帶裝有加密程式之筆記型電腦入境，導致電腦遭到沒收的事件。

圖八　中國大陸對於使用加密程式之限制



圖說：除中國大陸法人之桌上型電腦欲使用外國製（非中國大陸製）之加密程式時，需要申請外，由日本派遣前往大陸者所攜帶之筆記型電腦中裝有加密程式時，亦須進行申請
資料來源：NikkeiBP，資策會 MIC 整理，2008 年 6 月

每個需要用到加密程式的使用者，都必須於事先向中國大陸當局（國家暗號管理局）申請許可。然而，申請內容之調查及相關資料填寫等手續均頗爲繁複。有鑑於此，大塚商會於 2007 年 2 月開始推出協助日本人申請於中國大陸使用加密產品之「輕鬆利用密碼產品套裝」代辦服務。「我們與中國大

陸的律師事務所合作，掌握了相關規定及法令解釋後之微妙變化等訊息。近來詢問相關事宜者數量有急速增加的趨勢」大塚商會人員表示。

舉例來說，總公司設於日本大阪市，中國大陸分公司已於 2007 年 11 月開始運作的 SCAS（Sumika Chemical Analysis Service，住化分析）中心，當初爲降低中國大陸方面業務資料違法外流的風險而計畫導入加密程式。然而，該公司直到 2007 年春季時才得知必須先進行前述的許可申請之事。該公司人員表示：「我們判斷，靠公司方面自行處理多半來不及完成手續，因此選擇了代辦服務」。

運用 DRM 技術之產品，由於並非單純的加密程式，因此，中國大陸方面的因應方法也會依公司的情況而有所不同。以 XVLstaff 爲例，日立軟體對於評估是否應當導入該程式之用戶提供了以下的建議：「關於加密的部分，請將伺服器設置於日本。XVL Studio 雖具備可與伺服器連線，開啓加密之 XVL 檔案的功能，但其主要機能仍爲編輯 XVL 檔案，並非加密程式。」實際上，在中國大陸也能買到 XVL Studio。

另一方面，針對 SpinFire Protect，Data Design 則發表了「AirZip 的產品已於中國大陸開始銷售，使用相同技術的 SpinFire Protect 並不會成爲受限制的對象」之言論。雖然在中國大陸可以購得 Pro／ENGINEER，但安裝附加套件後，Pro／ENGINEER 本身便會追加加密機能。關於此種狀況下是否必須進行申請，總公司位於東京的 PTC Japan 僅以「現在仍在洽詢中」作爲回應。

發行所	財團法人資訊工業策進會 資訊市場情報中心 MIC
地址	台北市 106 敦化南路二段 216 號 19 樓
電話	+886-2-2735-6070
傳真	+886-2-2732-1353
全球資訊網	http：// mic.iii.org.tw
會員服務專線	+886-2-2378-2306
會員傳真專線	+886-2-2732-8943
E-mail	members@iii.org.tw
AISP 會員網站	http://mic.iii.org.tw/intelligence

由於產業變動快速，並不保證上述報告於未來仍維持正確與完整，引用時請注意發佈日期，及立論之假設或當時情境。