資訊安全的關鍵還是在人，制度與系統都只是輔助管理的工具。

資訊環境的安全考量

◎魯明德

個人資料保護法自今（2012）年 10 月開始實施後，公司與個人都開始注意各種資料的安全管理。小潘公司的業務人員在外面不小心遺失了公務用的筆記型電腦，公司知道後，立即進行危機處理，要求資訊部門配合擬訂管制措施，防止機密資料的外洩，以免造成個人資料外洩。

小潘接到指令後感到納悶，個人資料保護不是人力資源部跟業務部的事嗎？跟資訊部門有什麼關係？小潘就把這個疑問提出來請教老師，司馬特老師喝一口美味的焦糖瑪琪朵後，沒有直接回答這個問題，反而笑著跟小潘講了一個故事。

日本電信 NTT 集團的 NTT Data 公司，是日本規模最大的系統整合業之一，2003 年 12 月，有一名派遣員工的筆記型電腦遭竊，導致相關的業務資料外流；2005 年 5 月，又有一名員工遺失 USB 隨身碟，也造成大量員工資料外洩。在得知資料外洩事件後，NTT Data 公司立刻通知各部門主管，並由總經理級和經理級主管組成事後調查委員會，負責進行內部調查，以了解員工外洩資料當天的詳細經過與外洩資料的內容和範圍，最後再提出外部因應措施。

小潘聽了這個故事後恍然大悟，企業在電子化後，所有重要的資料都存放在電腦內，所以，資訊安全就成為首要工作。於是又提出他的問題：既然公司的資料都存在電腦裏，要防止資料外洩就要從源頭著手，資料可能的外洩途徑有那些？

司馬特老師，繼續說道，一般常見的資料外洩管道可分為兩大類，第一類是透過行動裝置，另一類則是內部網路。行動裝置範圍廣泛，除了我們常用的筆記型電腦、iPad、智慧型手機等可上網的裝置外，還包

括行動儲存媒體，如行動硬碟、隨身碟等。使用行動裝置造成資料的外洩管道有五種：

一、儲存媒體外洩：由於目前儲存媒體容量非常大，因此，有心人士很容易透過各式儲存媒體，將公司的機密資料下載攜出，包括個人資料、研發資料、業務資料等。

二、列印外洩：公司因資源有限，往往都是整個辦公室共用印表機，如果列印出來的機密資料，沒有馬上去拿，很可能會被有心人士拿走，造成機密資料外洩。

三、透過網路服務如 FTP 或電子郵件等管道外洩：機密資料被有心人士利用 FTP 站臺或電子郵件方式傳出，或者放在 FTP 站臺而被入侵、竊取，造成機密資料外洩。

四、透過外接式裝置外洩：大量要攜帶的資料，往往存放在外接式硬碟中，如果沒有妥善保存，就會發生如 NTT data 公司類似的情形。

五、病毒入侵感染導致資料外洩：因使用者疏忽，致使病毒入侵，造成機密資料外洩。

至於透過公司內部網路外洩機密資料的管道則更多，除了包括上述五種以外，還有可能因為資訊流通的需求而導致資訊設備濫用，或是使用個人筆記型電腦處理公務，因筆記型電腦遺失或遭竊而外洩機密資料；另外，伺服器也有可能被入侵而使機密資料外洩。

小潘聽完司馬特老師的分析，發現機密資料外洩的管道還真多，實在是防不勝防，於是想到有沒有可能利用坊間的資安產品來協助管制？而這些產品應該具備什麼功能才能滿足需求？

司馬特老師喝口咖啡接著說，除了利用制度防止機密資料外洩外，以資安產品協助管制也是一種方法，但坊間產品眾多，在選擇時，除了考慮軟體版本、產品概念、防備對象、支援語系和作業系統支援度等基本項目外，還要特別針對控管、審核、監看、管理等功能進行評估。

控管除了包括對儲存裝置控管、硬體部分加密功能、HTTP 上傳控管、FTP 上下傳控管、離線控管、USB 指定使用等項目外，還有對使用者執行特定程式或瀏覽特定網頁時會執行的控管條件，如檔案列印、網頁列印、使用鍵盤、滑鼠拖曳、剪貼簿等。

審核則是對特殊需求的暫時開放，如瀏覽網頁、檔案列印，在審核確認檔案內容後，可暫時同意放行。

監看包括紀錄和警告，例如 HTTP 上傳操作紀錄、FTP 上傳下載操作紀錄、PrintScreen 紀錄、管理者操作紀錄、檔案寫出紀錄、寫出資料的備份、軟硬體異動紀錄等。

管理包括檢視軟體管理標準、遠端技術、報表功能、使用者管理、管理者管理等，例如管理者管理可採用指紋辨識系統來協助。

最後，司馬特老師還是語重心長地告訴小潘，資訊安全的關鍵還是在人，制度與系統都是輔助管理的工具，如果人沒有意識到資訊安全對組織的重要，就會有防不勝防的危機出現。所以，要維護資訊安全，教育訓練是不可忽視的一環。