清流月刊中華民國一百零二年二月號

電子化的病歷已是一個趨勢，醫院將無法置身其外；唯有事先萬全準備，才能確保病患的個人資料不致外洩。

電子病歷的安全防護

◎魯明德

美國研究機構Ponemon Institute LLC對80家美國醫療機構進行訪查後，於去（2012）年12月發布了一份對病人隱私及個人資料之安全防護所做的研究報告。報告中顯示：有高達94%的醫療機構在過去兩年內曾經發生病患資料遺失或遭竊取的事故，有將近一半（45%）的受訪醫療機構在兩年內發生５次以上資料遺失或遭竊取的事故。而最常遭竊或遺失的資料，是病患的保險紀錄和病歷。

常見的事故發生原因包含硬體設備遺失、員工或第三方使用者操作失當、員工監守自盜，以及駭客入侵等。超過50%的受訪機構表示自身並沒有偵測或監控資料是否遺失或外洩的能量，致使全美醫療體系在一年中，因資安事件所遭受的財務損失即達70億美元。

美國雖然是科技大國，各項科技均領先群雄，且資訊科技的發展亦為世界翹楚，然而，從研究資料中卻發現：美國醫療機構的資訊安全防護竟是如此不堪一擊。國內目前雖未見到相關研究，但是，他山之石可以攻錯，見到別人的缺失，我們可以引以為鑑。

資訊安全的標的可分為有形與無形兩種，以前述案例而言，有形的標的包括資訊設備、紙本的病歷等看得到的東西；無形的標的則如電子病歷等儲存在電磁媒體中的資料。由於網路的發達，資訊共享已是一種常態，因此，電子病歷已是一種無法可擋的趨勢。既然是時代的潮流，不能走回頭路，所以就必須針對它的安全性做全面的規劃。

對於網路伺服器的安全，雖可透過防火牆加以保護，惟駭客的手法日益增強，正所謂道高一尺、魔高一丈；而電子病歷又是個人資料保護法所保護的標的，因此對於個人資料的保護，不能全部仰賴防火牆。

我們既然無法完全防止駭客入侵資料庫竊取機密文件，就要想辦法讓駭客入侵後，所竊取的文件無法看懂，因此，對於電子病歷的資料，可以採用加密方式處理。

首先針對醫生、護士、藥劑師及行政人員，給予不同權限的憑證，依權限授予不同的功能，例如醫生可以讀、寫病歷，藥劑師就只能看到處方；醫生在看診後，把病人的病情記錄在電子病歷上，在存檔時，即以他的憑證把檔案加密，同時留下簽章紀錄。經過加密後的檔案，即使被駭客入侵竊取，或是員工監守自盜，縱使拿到檔案，但因沒有解密金鑰，打開檔案後，看到的都是亂碼，所以就算防火牆擋不住駭客，資料被偷走，拿到的資料也是有字天書，讓人看不懂，即可達到保密的目的。而透過電子簽章的方式，讓每個修改過病歷的人，都用他自己的憑證，經由特定的加密演算法，記錄修改的時間及人員，如此一來就可避免人為竄改資料的情事發生。

其次，也要防止具有權限的人員，濫用權限竊取資訊。例如有讀取權限的工作人員，利用其合法權限，把電子病歷列印後流出。所以在設定權限時，可以限制列印的功能，讓一般人員無法列印病歷，以防止合法人員的危安事件。為避免因電腦遺失造成電子病歷資料外洩的風險，在規劃電子病歷系統時，即應考量設置檔案伺服器（File Server），將電子病歷集中存放在機房的資料庫中；而機房除了專人管理外，也要有門禁管制措施，記錄每日之進出人員及進出時間，並避免閒雜人等隨意進出，造成危安事件。

除此之外，電子化的病歷，最怕的是資料損壞、遺失，因此，對於電子病歷還是要每天做備份（Backup），以避免因為資料庫?損而造成資料遺失，損及病人權益。又備份不能只做一份，醫院也應有異地備援（Remote Backup）的觀念，要在不同的地方也儲存備份，以防自己的機房遭到意外時，還有另一份資料可以用。

電子化企業已是一個趨勢，醫院也無法置身其外；面對資訊科技的進步，電子病歷已是無可避免，唯有事先妥慎規劃及萬全準備，才能確保病患的個人資料不外洩。

（作者為科技大學資訊管理系講師）

▲Top

真正影響雲端發展的關鍵並非技術與服務項目的多寡，而是資訊安全上的保障，能否讓使用者放心使用。

雲端與資安交互的火花—雲端資安效應初探

◎樊晉源

雲端科技近年來已成為國際通訊及科技市場上重點發展的領域，包括Google、Amazon、IBM、Microsoft等大廠，甚至是各國政府組織，均積極投入大量資源發展相關技術與產業，未來人們就能以低成本、高效率的方式，快速連結到網際網路上處理資訊資料，進而根據個人或公司的需求，發展資訊服務平台並快速地部署在網路上供顧客使用。但是，到底什麼是「雲端」？又分享在雲端上的資訊是否能保護我們的隱私，讓我們在便利使用各項資訊應用的過程中，不至於擔心「雲」會讓我們個人或企業的重要資料曝露在不安全的環境中，而讓不法之徒有機可乘？這是目前許多人最想確認與了解的課題。

本篇文章首先期望從雲端架構進行探討，讓讀者了解雲端如何服務大眾，進一步從中點出資訊安全議題，並提出此類資訊問題該如何解決；最後希望給大家省思，當進步的科技帶來幸福的果實讓大眾享用時，相對而言大眾所能保有的隱私是否也逐漸降低？這兩者間是否有一平衡機制？身為個人該如何防範？

探討雲端架構之前勢必要解釋何謂「雲端」？基本上所謂的「雲端」，其實就是泛指「網路」，會稱為雲端是因為早期工程師繪製網路示意圖時，習慣用「雲」來代表網路，因此雲端科技簡單而言，可說是網路科技之延續。坦白說，雲端科技並不是一項創新的科技，因為其概念及技術均來自於更早期的「分散式運算」（Distributed Computing）以及「網格運算」（Grid Computing）這兩種概念，但不同於此兩種運算技術，故雲端科技可簡稱為此兩者之整合應用與服務。原本此兩種技術受限於硬體及軟體，所能服務之對象均有限，但透過整合兩者的優勢與特長，雲端運算能讓更多人享受到分散式及網格運算技術的強大效益，同時，也伴生及結合出更多更新的應用概念與新興技術。

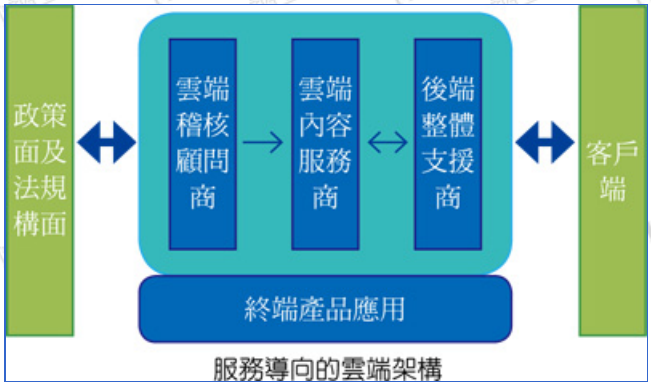
而雲端到底包含哪些架構？這些架構需要如何定義？這個問題最早是由CSA（Cloud Security Alliance）在2009年發表的報告中，以服務的角度切入雲端並進一步區分為三大類，即IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）與SaaS（Software as a Service）。從各類服務的內容與特質來看，三種服務分別針對基礎設施（硬體、網路連線）、系統平台（系統環境、開發工具）、應用系統（軟體、服務平台）作為雲端架構的檢視；並進一步從中針對雲端技術如何支援此三種服務進行討論。

隨著雲端科技越趨火熱，市場上相關的應用相繼出籠，單純從CSA提出的服務架構來看雲端發展，也變得有些不足。因此，許多專家學者紛紛提出自己的雲端應用架構。我們認為，應該將支援輔助的角色含括進來共同討論，才能算是完整的雲端服務架構。所以，架構的核心仍然是CSA的三層服務類型，而相關服務的提供者就稱為雲端內容服務商，協助設計、規劃與布建的提供者稱為稽核顧問商，尚包括其他周邊的支援性產品提供者。在稽核顧問商這部分，必須隨時關注各國相關政策與法令規章，這會影響到雲端服務商在服務架構上的設計要求；這部分也會連帶影響雲端應用系統與服務平台關於設計開發規範與營運管理的要求，進而影響後端其他支援性產品的開發與設計。

至於資訊安全在這一架構中，到底扮演何種角色？若從服務的角度切入，那麼資訊安全的需求勢必成為最被關注的問題。尤其在內容服務商這部分，對任何一個選擇雲端作為解決方案的個人或企業，資訊安全一定是其最為擔心的問題；畢竟，資料都存在「雲」上，廠商怎麼保證其實體資料不會遭受駭客、敵對廠商之竊取與入侵？因此，雲端必須加重其資訊安全之重要性。至於如何規劃布建出一個符合需求的雲端資訊安全架構與環境，則是雲端與資訊安全廠商必須積極努力的課題。

現階段ISO27001針對資訊安全構面，已有詳盡的管理規範，從硬體、軟體，甚至接觸者，均有稽核時應注意的重點與要求。但這是否已足夠應付雲端服務可能遭遇的資訊安全問題？其實，整個雲端資訊的安全，必須從內容服務加以拓展出去，針對各種可能出現的資訊安全狀況進行分析，並進一步思考制定適當的法規；稽核顧問商也應重新思考如何加進法規，進行一系列雲端內容商的認證；同理，支援商也必須符合技術及法規規範，提出相對應之服務、軟體或設備。

概括而言，真正影響雲端發展之問題，並不是技術與服務項目的多寡，恐怕還是資訊安全上的保障與相關技術，是否足以讓使用者在享受方便之資訊服務的同時，能安心使用，達到「免於恐懼的自由」，這將是雲端與資安廠商最應注重的問題。



服務導向的雲端架構

（作者為國家實驗研究院科技政策研究與資訊中心副研究員）

▲Top