

## 面對雲端環境上的訊息風險，企業該如何因應此衝擊？

Openfind 產品經理 廖享進

隨著 Google 在去年初宣布於台灣啟動「雲端運算」學術計畫，「雲端運算」這個聽來帶點浪漫色彩的科技名詞立時席捲各大媒體版面，但根據 MIC 在 2010 年 7 月公佈的最新一份企業使用雲端服務意向所做的調查結果顯示，目前在台灣的大型企業中，仍然有 44.2% 的企業表示對雲端服務供應商不熟悉，特別是台灣本土廠商多不在大型企業較熟悉的雲端運算服務供應商名單中；同時，也有高達 38.7% 的台灣大型企業認為使用雲端環境的最大疑慮，是資訊安全問題。

隨著專業媒體與廠商的大量推廣和說明，大部分人目前對雲端解決方案的認識已經逐漸成熟，也開始進入相關產業的成長起飛期；但相較於相關雲端解決方案的廠商不斷推薦雲端服務的「隨選即用」、「隨著需求、負荷動態成長」、「負載平衡」、「降低成本」等特性時，卻鮮少有人去提出在雲端環境下，需要注意的資訊安全問題。

在 2009 年時，美國電子隱私資訊中心 (Electronic Privacy Information Center, EPIC) 曾訴請聯邦貿易委員會 (Federal Trade Commission, FTC)，調查 Google 的雲端運算服務 (Cloud Computing Services) 是否有足夠的安全及隱私保護，原因陳述在 EPIC 的訴願狀中：「近來的報告顯示，Google 沒有充分保護所取得的秘密資訊；因此希望負責消保業務的 FTC 能調查 Google 雲端服務，以確定隱私及安全措施是否足夠。」

事實上，在許多雲端環境的名人訪談中，多半都能嗅到大家在推廣、說明雲端環境為企業帶來的好處之時，均會語帶保留地提醒大家重視雲端服務廠商的隱私與資訊安全政策，是否完善。歐洲新一代自由主義(聯合報，民國 98 年 9 月 7 日 A16)曾經說過：「自由遭襲現象絕對是廿一世紀人類社會最嚴重的大問題。一般人無法容忍有人闖進住宅，在他們的書桌前東翻西找，卻可以默默忍受政府及一些機構在網路上截取他們的私人資料。」原因就是因為不管個人或企業，在享受雲端環境帶來的便利之時，很容易會因為服務易取易得，不需要思考自行維運的許多安全問題，因此而忽略掉許多資訊安全政策上應該要注意的重大議題，例如資料外洩、訊息追蹤稽核等問題。

因此，企業在思考自己需要什麼樣的雲端服務之前，應先檢視自我的資訊安全政策是否完備，即使因為相關需求而選擇或者轉移自建服務到雲端環境時，更應該思考相關的資料保護措施是否完備，以及廠商是否有提供相關的解決方案，供企業在雲端環境時，仍能追蹤並稽核訊息的動向、內容。

國內知名軟體廠商於 2010 年的 Openfind Solution Day 中提出「Message Assurance」(訊息保全)概念，就是提醒企業在進入雲端環境前，一定要注意自身的訊息解決方案是否從資料的傳遞、保存階段，完整考慮到相關的隱私法規(如台灣的個人資料保護法)與風險預防政策，

包括訊息是否均能被追蹤、前稽核(資料外洩)、後稽核(事後舉證)，並能安全的負荷巨量訊息的成長。對企業來說，將自身維運已久的訊息解決方案推上雲端，已經不是問題，有太多的專業廠商已經可以解決技術上或者架構上的難題，但走上雲端之後，意味著企業的訊息系統面臨的風險更加複雜化，以往在內網不會遭遇到的資安攻擊或風險，可能都在走上雲端之後立刻遭受挑戰。即使企業使用「內部私有雲」的方式進行雲端架構的部署，仍會面臨內賊難防，而且資料還放在同一個籃子裡，單一資安事件就有可能流洩全企業訊息資訊，風險更加巨大的問題。

訊息保全(Message Assurance)的概念來自於資訊保全(Information Assurance)；資訊保全最早的概念起源於 CIA Triad 資訊安全三要素，該份模型定義了資訊運用的保密性(confidentiality)、完整性(integrity)和可用性(availability)；隨後在 2010 年 4 月，由美國國防部的國家安全系統委員會(Committee on National Security Systems)發表的 CNSS Instruction No. 4009 中，正式完整地描述了 Information Assurance 的多項特性，包括可用性(availability)、完整性(integrity)、身份認證(authentication)、保密性(confidentiality)和不可否認性(non-repudiation)。對一般企業來說，要作到完整的資訊保全，任務非常繁重，但檢視企業對網際網路應用最頻繁的兩個面向 – Email 和 Web，注意最基本的訊息保全則是刻不容緩的課題。

如果在走向雲端之前，對企業內部資訊系統的訊息控管政策就已經面臨許多風險，雲端環境的快速部署、強大運算能力等特性將會使這些風險以數倍速度成長並散播；這跟網際網路興起後，相關的資安風險數量也比單機電腦時代多了數千甚至數萬倍是一樣的道理。一個能穩定快速散播資訊訊息的環境，一定也會將相關的威脅以相對等的速度散播，唯有在步上雲端前就重視訊息保全，同時在選擇相關雲端服務時，注意該服務是否具備訊息保全的特性，提供服務的環境是否也具備訊息保全的相關資安工具和政策，這才是最基本的雲端安全之道。

## 郵件雲端解決方案 – Message Assurance

- 郵件管理、防護安全、歸檔搜尋、訊息檢測

