從美國「聯邦風險與授權管理計畫」看我國促進政府部門導入雲端運算之策略與機制

刊登期別 2013年09月04日

從美國「聯邦風險與授權管理計畫」看我國促進政府部門導入雲端運算之策略與機制

科技法律研究所
2013年07月03日

資訊科技的發展，從早期「超級電腦/大型電腦」、近期「個人電腦」，到即將邁入以超大規模數量電腦主機虛擬集結的「雲端運算」時代。雲端運算將電腦集中運用，未來電腦運算設施就像是水、電；資料儲存與應用就像是銀行，只要連上網路就可以使用，不必各自投資發展。因此，「雲端運算」未來將成為每個國家的重要基礎建設。

將雲端運算列為重要的產業發展重心，已是各國的趨勢，而運用雲端運算所帶來的效益，如節省經費、提升效率等，亦為普遍地承認，再加上公部門相較於民間，其擁有較多的經費及資源來進行雲端運算的導入，而藉由公部門導入雲端運算，可以帶動雲端運算產業的發展以及雲端運算應用的普及化。因此，各國均皆致力於促進公部門導入雲端運算。

然而，在雲端運算帶來龐大經濟效益的同時，伴隨而來的，是新的資訊管理議題，雲端安全防護聯盟（Cloud Security Alliance, CSA）提出了雲端運算可能遭遇的九大安全威脅 ：

一、資料外洩（Data Breaches）
二、資料遺失（Data Loss）
三、帳號被駭（Account Hijacking）
四、不安全的APIs程式（Insecure APIs）
五、拒絕服務（Denial of Service）
六、惡意的內部人員（Malicious Insiders）
七、濫用雲端服務（Abuse of Cloud Services）
八、審慎評鑑不足（Insufficient Due Diligence）
九、共享環境議題（Shared Technology Issues）

面對前述的安全威脅，政府部門在考量導入雲端服務時，首先面對的就是要探討如何在導入雲端運算後仍能維持資訊安全的強度，以及政府部門要從何尋找符合其需求的業者。

壹、事件摘要

美國政府在2010年12月發表了25項聯邦IT轉型重點政策，其中一項核心的政策便是「雲優先政策」（cloud first policy）。根據「雲優先政策」，聯邦機構必須在三個月內找出三項轉移到雲端的政府服務，並且要在一年內導入其中一項。

然而，此種新型態的雲端運算服務為聯邦機構帶來資安管理的新挑戰，傳統由各機關分頭洽談所導入資訊系統與應用規格之方法，並實施個別的資訊安全需求與政策的作法，對服務商而言，其所提供的相同服務，在各機關導入時，卻必須將受各個機關的審查，造成各機關投入過多的資源

在審查程序上，導致政府資源的浪費，不但耗費時間、審查重複，且無法達到建構妥善操作程序的效果。

2012年6月6日，聯邦政府總務管理局（General Service Administration, GSA）宣布「聯邦風險與授權管理計畫」（Federal Risk and Authorization Management Program,以下稱FedRAMP）開始正式運作，GSA並表示，「FedRAMP」的正式運作，將解決美國政府在雲端產品及服務需求上，因各自導入之標準不一致所導致的系統相容性問題、重複投資浪費，並可降低各政府機關自行進行風險評估及管理相關系統所耗費的人力、金錢成本。預估該計畫可為美國政府節省高達40%的預算及費用，預期效益相當可觀。

「FedRAMP」的目的是要為全國政府機關針對雲端產品與服務的風險評估、授權管理以及持續監控等標準作業規範，建立一套可遵循之依據。未來所有雲端產品的服務提供者，都必須遵守及達到該計畫的標準規範，才能為美國政府機關提供雲端產品及服務。

貳、重點說明

「聯邦風險與授權管理計畫」主要由預算與管理辦公室（Office of Management and Budget, OMB）負責組織預算與管理；聯邦資訊長（the Federal Chief Information Officer，CIO）負責跨部門的整合；國土安全部(Department of Homeland Security, DHS)負責網際網路的監控與分析；總務管理局(General Services Administration, GSA) 則建立FedRAMP之架構與程序，並成立計畫管理辦公室（ Program Management Office，PMO）負責FedRAMP之操作與管理；以及國家科技研究所(National Institute of Science and Technology, NIST)負責提供技術分析與標準；最後由國防部(Department of Defense, DoD) 、國土安全部、總務管理局，組成共同授權委員會（Joint Authorization Board, JAB），負責對服務提供者的授權與定期檢視。

FedRAMP制度的精神在於「作一次並重複使用」（Do once ,Use Many Times），同一內容的雲端服務，透過FedRAMP，僅須經過一次的評估與授權，即得被多個機關所採用。早期各機關重複檢驗同一廠商的同一服務之安全性，造成資源浪費的問題，將可獲得解決。當其他機關欲採用雲端服務時，可透過FedRAMP，免去再一次的評估與驗證。

FedRAMP主要由第三方評估機構、對服務提供者的評估、以及持續監督與授權等三個部份所構成，簡單介紹如下：

一、第三方評估機構的認證

FedRAMP的特殊之處，在於雲端服務提供者應由通過FedRAMP認證的第三方評估機構（3PAO）來進行審查，而第三方評估機構欲通過認證，除了要符合FedRAMP的需求外，還必須具備雲端資訊系統的評估能力、備妥安全評估計畫、以及安全評估報告等，另外亦同時引進了ISO/IEC17020作為評估機構的資格。其認證程序如下：

（一）申請檢視

機構首先必須符合ISO/IEC 17020 檢驗機構的品質與技術能力，並且自行檢視FedRAMP網站上的申請表，自行檢視是否合乎要求，然後決定是否提出申請。

（二）完成要求

機構須分別完成申請表所要求的系統安全計畫（system security plan, SSP）、系統評估計畫（system assessment plan, SAP）、安全評估報告（security assessment report, SAR）。於完成後向計畫管理辦公室提出申請。

（三）審查

在接受申請後，總務管理局會與ISO網路安全專家共同組成「專家審查委員會」（Expert Review Board , ERB），審查該申請。

（四）決議

審查完畢後，FedRAMP計畫管理辦公室（PMO）會檢視ERB的意見，決議是否通過該申請。

於通過申請後，該機構將會被列入FedRAMP官方網站（www.FedRAMP.gov）的第三方評估機構名單，目前為止，陸續已有十五個機構通過共同授權委員會的授權，日後得對雲端服務商進行評估。

二、對雲端服務提供者的評估

在「聯邦風險與授權管理計畫」的機制設計中，政府機關或雲端服務提供者任一方，皆可提出申請（Request）啟動雲端服務的安全性評估（Security Assessment）程序，此程序中共有四個主要階段：

（一）提出申請

在申請人將所須文件初步填寫完畢之後，計畫管理辦公室（PMO）即會指派資訊系統安全官（Information Systems Security Officer, ISSO）進行指導，使之得進行安全控制、出具必要文件、並實施安全測試。之後，PMO會與雲端服務提供者簽署協議，並要求相關機關實施對雲端服務系統的安全性測試。

（二）檔案安全控管

雲端服務提供者必須作成系統安全計畫（System Security Plan, SSP），表明安全控制之實施方法，及其相關文件如IT系統永續計畫（IT Contingency Plan）、隱私衝擊調查（Privacy Impact Questionnaire），並送交ISSO進行審查，再由雲端服務提供者就對審查意見予以回覆之後，由ISSO將案件送至共同授權委員會（Joint Authorization Board, JAB）進行審查，以確認所提交的SSP安全措施符合雲端系統所需。

（三）進行安全測試

服務提供者與第三方評估機構（Third Party Assessment Organization, 3PAO）簽約，且由PMO約集雲端服務提供者與3PAO，確認雙方對於安全測試實施的期待與時程，再由3PAO獨立進行該雲端系統測試，並完成安全評估報告（Security Assessment Report, SAR），闡述評估結果並確認所暴露的風險。雲端服務提供者針對此評估結果，作成行動與查核點報告（Plan of Action & Milestones (POA&M)），以提出矯正弱點與殘餘風險（residual risks）的措施、資源與時程規劃。

雲端服務提供者再將前述SAR與POA&M提交予PMO，由JAB決定是否接受該弱點及其修正計畫，或者提出修正建議。倘若JAB可接受該弱點及其他因應措施，則由ISSO通知雲端服務提供者即將進入安全評估的最後階段。

（四）完成安全評估

雲端服務提供者將所有安全控制相關文件彙成單一的安全評估方案，並提出證明將確實執行其安全控制措施。由JAB檢視此方案，並作出最終決定是否授予「附條件之授權」（Provisional Authorization）。得到此授權的雲端服務提供者名單，將會被列在FedRAMP官方網站上。倘若雲端服務提供者未獲得此授權，PMO會指導如何進行重新申請。

三、持續的評估與授權

持續的評估與授權（ongoing Assessment and Authorization, A&A）通常也被稱為持續監控（Continuous Monitoring），在FedRAMP中第三個也是最後一個流程，透過持續的評估與授權機制，來確保雲端服務提供者持續的安全性授權。其中包含了三個主要層面：

（一）操作的能見度

操作能見度的目標，是藉由自動化的方式來減少政府機構在監督作業上的行政耗費。亦即雲端服務提供者透過自動化的資料提供、定期提交具體控制的證據文件、以及年度自我認證報告等安全控制措施來說明操作的能見度，而不必政府機構另行要求。

（二）變更控制程序

雲端服務提供者更新她們的系統是常有的事，此處的變更控制程序並非針對例行性的維修或變更，而是要求若有發生影響臨時性授權或的顯著變更時，服務提供者必須提供此種具衝擊性變更的有效資訊，使FedRAMP得以評估此變更的影響與衝擊。

（三）事件回應

事件回應方面聚焦於新風險和漏洞的因應，服務提供者在發現影響授權的新風險或漏洞時，應向機構說明其針對保持系統安全的因應對策與作法。

參、事件評析

在各國紛紛投入雲端運算的推動熱潮中，我國也不能在此項產業推動中缺席。2010年4月，行政院科技顧問組（現已改組為行政院科技會報）責成經濟部，研擬「雲端運算產業發展方案」；2011年5月，行政院研究發展考核委員會亦公布了「第四階段電子化政府計畫」，在內部運作管理面向，將運用新興雲端運算技術推動以全國性的政府雲端應用服務，減少機關重複開發成本，並達成節能減碳效果。

雲端的安全問題，無論在私人企業或政府部門，均為選擇導入雲端服務的第一要務，「第四階段電子化政府計畫」中亦指出第四階段電子化政府將以雲端資安防護推動為重點，運用雲端運算技術，創新資安服務價值，確保政府資通安全防護。

然而，在服務提供者的安全性方面，我國並沒有像美國FedRAMP計畫般適度地提供服務提供者的安全性保證。對此，我國可借鏡各國的作法，適度的以透過公正第三方機構驗證，來消除雲端服務安全性的疑惑，並推動一個公開的平台，將通過驗證的廠商公布出來，提供公部門甚至私人企業作選擇，不僅可免去同一服務廠商不斷重複驗證的麻煩，亦可削減選擇上的難題，並藉此發展雲端資安技術與推動雲端產業，使我國的雲端環境能夠更臻成熟。

郭俊仁 編譯整理

上稿時間：2013年09月

推薦文章