解析雲端運算有關認驗證機制與資安標準發展

解析雲端運算有關認驗證機制與資安標準發展

科技法律研究所
2013年12月04日

壹、前言

2013上半年度報載「新北市成為全球首個雲端安全認證之政府機構」[1]，新北市政府獲得國際組織雲端安全聯盟(Cloud Security Alliance, CSA)評定為全球第一個通過「雲端安全開放式認證架構」之政府機構，獲頒「2013雲端安全耀星獎」（2013 Cloud Security STAR Award），該獎項一向是頒發給在雲端運用與安全上具有重要貢獻及示範作用之國際企業，今年度除了頒發給旗下擁有年營業額高達1200億台幣「淘寶網」的阿里巴巴集團外，首度將獎項頒發給政府組織。究竟何謂雲端認證，其背景、精神與機制運作為何？本文以雲端運算相關資訊安全標準的推動為主題，並介紹幾個具有指標性的驗證機制，以使讀者能瞭解雲端運算環境中的資安議題及相關機制的運作。

資訊安全向來是雲端運算服務中最重要的議題之一，各國推展雲端運算產業之際，會以提出指引或指導原則方式作為參考基準，讓產業有相關的資訊安全依循標準。另一方面，相關的產業團體也會進行促成資訊安全標準形成的活動，直至資訊安全相關作法或基準的討論成熟之後，則可能研提至國際組織討論制定相關標準。

貳、雲端運算資訊安全之控制依循

雲端運算的資訊安全風險，可從政策與組織、技術與法律層面來觀察[2]，涉及層面相當廣泛，包括雲端使用者實質控制能力的弱化、雲端服務資訊格式與平台未互通所導致的閉鎖效應（Lock-in）、以及雲端服務提供者內部控管不善...等，都是可能發生的實質資安問題 。

在雲端運算產業甫推動之初，各先進國以提出指引的方式，作為產業輔導的基礎，並強化使用者對雲端運算的基本認知，並以「分析雲端運算特色及特有風險」及「尋求適於雲端運算的資訊安全標準」為重心。

一、ENISA「資訊安全確保架構」[3]

歐盟網路與資訊安全機關（European Network and Information Security Agency, ENISA）於2009年提出「資訊安全確保架構」，以ISO 27001/2與BS25999標準、及最佳實務運作原則為參考基準，參考之依據主要是與雲端運算服務提供者及受委託第三方（Third party outsourcers）有關之控制項。其後也會再參考其他的標準如SP800-53，試圖提出更完善的資訊安全確保架構。

值得注意的是，其對於雲端服務提供者與使用者之間的法律上的責任分配（Division of Liability）有詳細說明：在資訊內容合法性部分，尤其是在資訊內容有無取得合法授權，應由載入或輸入資訊的使用者全權負責；而雲端服務提供者得依法律規定主張責任免除。而當法律課與保護特定資訊的義務時，例如個人資料保護相關規範，基本上應由使用者與服務提供者分別對其可得控制部分，進行適當的謹慎性調查（Due Diligence, DD）[4]。

雲端環境中服務提供者與使用者雙方得以實質掌握的資訊層，則決定了各自應負責的範圍與界限。

在IaaS（Infrastructure as a Service）模式中，就雲端環境中服務提供者與使用者雙方應負責之項目，服務提供者無從知悉在使用者虛擬實體（Virtual Instance）中運作的應用程式（Application）。應用程式、平台及在服務提供者基礎架構上的虛擬伺服器，概由使用者所完全主控，因此使用者必須負責保護所佈署的應用程式之安全性。實務上的情形則多由服務提供者協助或指導關於資訊安全保護的方式與步驟[5]。

在PaaS（Platform as a Service）模式中，通常由雲端服務提供者負責平台軟體層（Platform Software Stack）的資訊安全，相對而言，便使得使用者難以知悉其所採行的資訊安全措施。

在SaaS（Software as a Service）模式中，雲端服務提供者所能掌控的資訊層已包含至提供予使用者所使用的應用程式（Entire Suite of Application），因此該等應用程式之資訊安全通常由服務提供者所負責。此時，使用者應瞭解服務提供者提供哪些管理控制功能、存取權限，且該存取權限控制有無客製化的選項。

二、CSA「雲端資訊安全控制架構」[6]

CSA於2010年提出「雲端資訊安全控制架構」（Cloud Controls Matrix, CCM），目的在於指導服務提供者關於資訊安全的基礎原則、同時讓使用者可以有評估服務提供者整體資訊安全風險的依循。此「雲端資訊安全控制架構」，係依循CSA另一份指引「雲端運算關鍵領域指引第二版」[7]中的十三個領域（Domain）而來，著重於雲端運算架構本身、雲端環境中之治理、雲端環境中之操作。另外CCM亦將其控制項與其他與特定產業相關的資訊安全要求加以對照，例如COBIT與PCI DSS等資訊安全標準[8]。在雲端運算之國際標準尚未正式出爐之前，CSA提出的CCM，十分完整而具備豐富的參考價值。

舉例而言，資訊治理（Data Governance）控制目標中，就資訊之委託關係（Stewardship），即要求應由雲端服務提供者來確認其委託的責任與形式。在回復力（Resiliency）控制目標中，要求服務提供者與使用者雙方皆應備置管理計畫（Management Program），應有與業務繼續性與災害復原相關的政策、方法與流程，以將損害發生所造成的危害控制在可接受的範圍內，且回復力管理計畫亦應使相關的組織知悉，以使能在事故發生時即時因應。

三、日本經產省「運用雲端服務之資訊安全管理指導原則」[9]

日本經濟產業省於2011年提出「運用雲端服務之資訊安全管理指導原則」，此指導原則之目的是期待藉由資訊安全管理以及資訊安全監督，來強化服務提供者與使用者間的信賴關係。本指導原則的適用範圍，主要是針對機關、組織內部核心資訊資產而委託由外部雲端服務提供者進行處理或管理之情形，其資訊安全的管理議題；其指導原則之依據是以JISQ27002（日本的國家標準）作為基礎，再就雲端運算的特性設想出最理想的資訊環境、責任配置等。

舉例而言，在JISQ27002中關於資訊備份（Backup）之規定，為資訊以及軟體（Software）應遵循一定的備份方針，並能定期取得與進行演練；意即備份之目的在於讓重要的資料與軟體，能在災害或設備故障發生之後確實復原，因此應有適當可資備份之設施，並應考量將備份措施與程度的明確化、備份範圍與頻率能符合組織對於業務繼續性的需求、且對於儲存備份資料之儲存媒體亦應有妥善的管理措施、並應定期實施演練以確認復原程序之有效與效率。對照於雲端運算環境，使用者應主動確認雲端環境中所處理之資訊、軟體或軟體設定其備份的必要性；而雲端服務提供者亦應提供使用者關於備份方法的相關訊息[10]。

參、針對雲端運算之認證與登錄機制

一、CSA雲端安全知識認證

CSA所推出的「雲端安全知識認證」（Certificate of Cloud Security Knowledge, CCSK），是全球第一張雲端安全知識認證，用以表示通過測驗的人員對於雲端運算具備特定領域的知識，並不代表該人員通過專業資格驗證（Accreditation）；此認證不能用來代替其他與資訊安全稽核或治理領域的相關認證[11]。CSA與歐盟ENISA合作進行此認證機制的發展，因此認證主要的測試內容是依據CSA的「CSA雲端運算關鍵領域指引2.1版（英文版）」與ENISA「雲端運算優勢、風險與資訊安全建議」這兩份文件。此兩份文件採用較為概略的觀念指導方式，供讀者得以認知如何評估雲端運算可能產生的資訊安全風險，並採取可能的因應措施。

二、CSA雲端安全登錄機制

由CSA所推出的「雲端安全登錄」機制（CSA Security, Trust & Assurance Registry, STAR），設置一開放網站平台，採取鼓勵雲端服務提供者自主自願登錄的方式，就其提供雲端服務之資訊安全措施進行自我評估（Self Assessment），並宣示已遵循CSA的最佳實務（Best Practices）；登錄的雲端服務提供者可透過下述兩種方式提出報告，以表示其遵循狀態。

(一)認知評價計畫（Consensus Assessments Initiative）[12]：此計畫以產業實務可接受的方式模擬使用者可能之提問，再由服務提供者針對這些模擬提問來回答（提問內容在IaaS、PaaS與SaaS服務模式中有所不同），藉此，由服務提供者完整揭示使用者所關心的資訊安全議題。

(二)雲端資訊安全控制架構（CCM）：由服務提供者依循CCM的資訊安全控制項目及其指導，實踐相關的政策、措施或程序，再揭示其遵循報告。

資安事故的確實可能使政府機關蒙受莫大損失，美國南卡羅萊納州稅務局（South Carolina Department of Revenue）2012年發生駭客攻擊事件，州政府花費約2000萬美元收拾殘局，其中1200萬美元用來作為市民身份被竊後的信用活動監控，其他則用來發送被害通知、資安強化措施、及建立數位鑑識團隊、資安顧問。

另一方面，使用者也可以到此平台審閱服務提供者的資訊安全措施，促進使用者實施謹慎性調查（Due Diligence）的便利性並累積較好的採購經驗。

三、日本-安全・信賴性資訊開示認定制度

由日本一般財團法人多媒體振興協會（一般財団法人マルチメディア振興センター）所建置的資訊公開驗證制度[13]（安全・信頼性に係る情報開示認定制度），提出一套有關服務提供者從事雲端服務應公開之資訊的標準，要求有意申請驗證的業者需依標準揭示特定項目資訊，並由認證機關審查其揭示資訊真偽與否，若審查結果通過，將發予「證書」與「驗證標章」。

此機制始於2008年，主要針對ASP與SaaS業者，至2012年8月已擴大實施至IaaS業者、PaaS業者與資料中心業者。

肆、雲端運算資訊安全國際標準之形成

現國際標準化組織（International Organization for Standardization, ISO）目前正研擬有關雲端運算領域的資訊安全標準。ISO/IEC 27017（草案）[14]係針對雲端運算之資訊安全要素的指導規範，而ISO/IEC 27018（草案）[15]則特別針對雲端運算的隱私議題，尤其是個人資料保護；兩者皆根基於ISO/IEC 27002的標準之上，再依據雲端運算的特色加入相應的控制目標（Control Objectives）。

[1]http://www.ntpc.gov.tw/web/News?command=showDetail&postId=277657 (最後瀏覽日:2013/11/20)

[2]European Network and Information Security Agency [ENISA], Cloud Computing: Benefits, Risks and Recommendations for Information Security 53-59 (2009).

[3]ENISA, Cloud Computing-Information Assurance Framework (2009), available at http://www.enisa.europa.eu/activities/risk-

management/files/deliverables/cloud-computing-information-assurance-framework .

[4]ENISA, Cloud Computing-Information Assurance Framework 7-8 (2009).

[5]ENISA, Cloud Computing-Information Assurance Framework 10 (2009).

[6]CSA, Cloud Controls Matrix (2011), https://cloudsecurityalliance.org/research/ccm/ (last visited Nov. 20, 2013).

[7]CSA, CSA Guidance For Critical Areas of Focus in Cloud Computing v2 (2009), available at https://cloudsecurityalliance.org/research/security-guidance/#_v2. (last visited Nov. 20, 2013).

[8]https://cloudsecurityalliance.org/research/ccm/ (last visited Nov. 20, 2013).

[9]日本経済産業省，クラウドサービスの利用のための情報セキュリティマネジメントガイドライン（2011），http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html，（最後瀏覽日：2013/11/20）。

[10]日本経済産業省，〈クラウドサービスの利用のための情報セキュリティマネジメントガイドライン〉，頁36（2011）年。

[11]https://cloudsecurityalliance.org/education/ccsk/faq/（最後瀏覽日：2013/11/20）。

[12]https://cloudsecurityalliance.org/research/cai/（最後瀏覽日：2013/11/20）。

[13]http://www.fmmc.or.jp/asp-nintei/index.html（最後瀏覽日：2013/11/20）。

[14]Information technology - Security techniques- Security in cloud computing (DRAFT), http://www.iso27001security.com/html/27017.html (last visited Nov. 20, 2013).

[15]ISO/IEC 27018- Information technology -Security techniques -Code of practice for data protection, controls for public cloud computing services (DRAFT), http://www.iso27001security.com/html/27018.html (last visited Nov. 20, 2013).

本文為「經濟部產業技術司科技專案成果」

張乃文
主任 編譯整理

上稿時間：2013年12月

推薦文章