雲報專欄：政府雲端資料中心之資安與維運系統設計

技術專家委員會
國立交通大學副校長林一平
中華電信股份有限公司博士陳元凱
中華電信數據分公司總經理鍾福貴
中華電信數據分公司處長鍾鳴
中華電信研究院所長梁冠雄

電子化政府(E-Government)是聯合國用以評估各國在資通訊科技及社會經濟發展的重要指標之一，同時也反應該國在資通訊科技的運用及人民數位素養的程度。我國自1996年起推動電子化政府以來，陸續完成第一階段政府網路基礎建設、第二階段政府網路應用推廣計畫及第三階段優質網路政府計畫，進入第四階段電子化政府計畫(101年至105年)，歷經多年建設成果，已實質地提升政府對民眾服務的行政效率及服務品質，同時獲得國際組織評比肯定。例如，世界經濟論壇(WEF) 2011-2012年資訊科技應用成果評比我國「政府資訊科技使用度」及「政府資訊科技整備度/效能」分別位居全球第3及第5名[1]。

隨著資通訊科技演進，我國電子化政府的推動也從早期的行政簡化、為民服務的目標，邁向以政府應用服務帶頭推動資通訊產業發展的領頭羊角色。例如，運用新興資通訊科技來促進數位經濟的發展，推動雲端運算即為當前要務。因此，歐、美、日等先進國家政府都積極投入雲端運算推動與發展，除了運用雲端運算的創新力量提供智慧化政府服務外，更重要的是促進產業轉型與發展。例如美國聯邦政府「Apps.gov」，歐盟「Euro Cloud」，日本「霞關雲(Kasumigaseki Cloud)」等計畫。

我國行政院於2010年4月公佈我國雲端運算發展推動策略，2012年8月修訂規劃以「推動民眾有感應用」、「建構創新應用開發能量」、「奠定系統軟體基礎」、「落實雲端基礎建設」和「發揮綠色節能效率」等五大策略，以「產值」和「價值」並重發展，規劃建置與民眾生活息息相關的十朵「有感雲」應用，包括「政府雲端資料中心基礎建設」、「交通雲」、「警政雲」、「防救災雲」、「教育雲」、…

等[2]。其中「政府雲端資料中心基礎建設」計畫即為至關重要的雲端運算基礎建設之一。

政府雲端資料中心基礎建設規劃

「政府雲端資料中心基礎建設」的設計考量除了必須滿足雲端運算的隨需即用(On-demand Self-service)、資源池(Resource Pooling)、寬頻接取(Broad Network Access)、彈性調度(Rapid Elasticity)及可量測管理(Measured Service)等五大特性，實務的營運面還需要一套簡易操作的營運管理系統及高安全等級的資安防護機制來滿足這些設計考量。中華電信公司自2010年啟動以「四大中心、一平台、一市集」為主軸的雲端運算策略布局以來，迄今累積建立了相當程度的雲端運算自主研發技術及維運能量(Know-how)，包括規劃、設計、建置、維運能力等(如圖1)。下面就針對「政府雲端資料中心基礎建設」的關鍵核心系統－資安防護及維運管理系統，做一簡要說明。

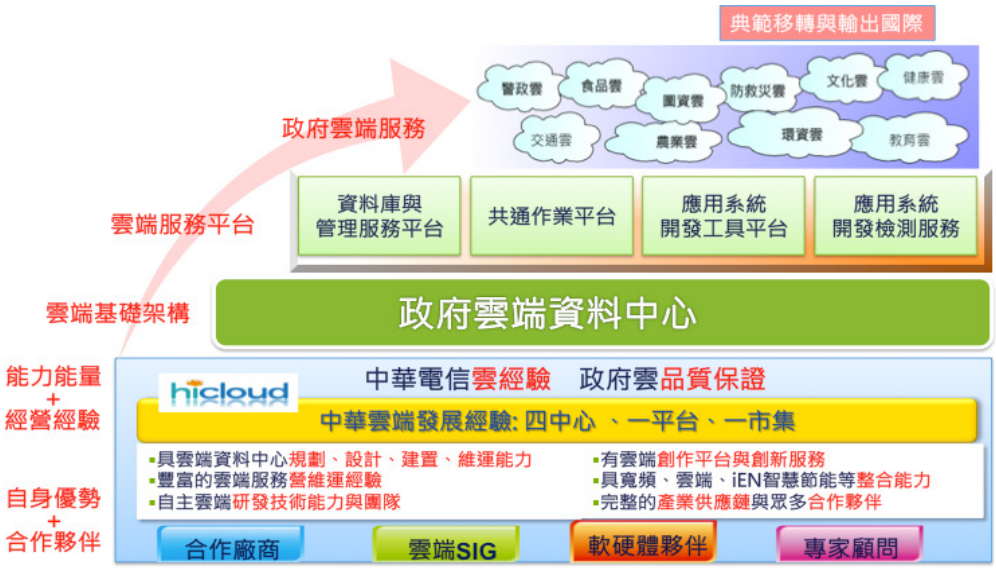

圖 1. 政府雲端運算資料中心規劃考量

雲端資料中心之資安防護

安全及信賴是使用任何服務的第一前提，政府相關應用牽涉機關秘密和民眾個資，必須具備高規格的資安防機制護。目前企業為因應各項資訊安全威脅，大量

建置防火牆(Firewall)、入侵偵測/防禦系統(Intrusion Detection/Prevention System, IDS/IPS)、網頁應用程式防火牆（Web Application Firewall, WAF）等安全防護防堵駭客攻擊。雲端運算係基植於資訊技術架構，無可避免地承襲以往的所有資安問題，同時雲端運算服務採用虛擬化技術與架構，所衍生的資安管理與攻擊防禦機制皆比以往傳統資安領域更為複雜。根據資策會產業情報研究所（Market Intelligence & Consulting Institute, MIC）在2010年7月所公布的企業使用雲端服務意向的調查結果顯示，高達38.7%的台灣大型企業認為使用雲端服務的最大疑慮是資訊安全問題。使用雲端服務的雲端用戶所關心的雲端資安考量包含：

- 放在雲端的資料會不會不見？會不會被竊取？是否有加密機制？退租後，雲端服務環境或儲存在雲端的資料是否會刪除？
- 從自己的電腦操作雲端設備或服務是否安全？
- 雲端服務是與他人共享資源，資料與資源會不會未經允許也被共享？
- 是否有其他鄰近租用人可以攻擊雲端主機或服務並取得我的資料？
- 有其他鄰近租用人可以利用封包監視工具（Packet sniffer）側錄網路封包？
- 如何確認租用雲端主機與服務的安全性？

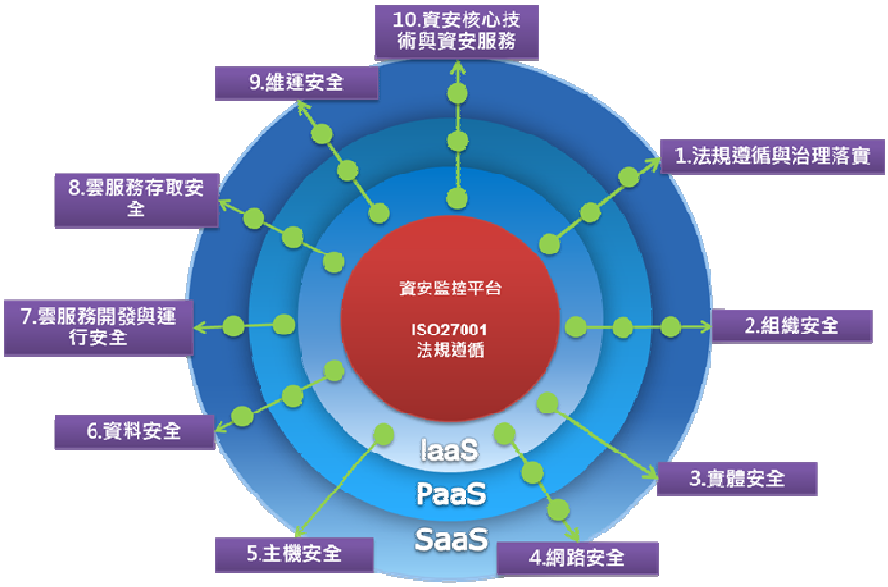

圖 2. 雲端十大資安主題

因此，在建置雲端運算資料中心時，雲端安全的全面考量與建置將是最重要的。以中華電信的雲端運算資料中心為例，設有專屬的資安艦隊，專責資安防護技術研發與營運，團隊成員皆具備多項資安專業證照，以建構堅強且具規模之資安技術研究與營運服務能力。同時針對雲端運算可能的安全考量歸納出十大主軸(如圖 2)及具體防護機制[3]：

1. 資安法規遵循與治理落實：本公司雲端機房除了導入 ITIL v3 服務管理流程，取得 ISO 9001、ISO 20000 國際級認證外，運作與資訊安全方面則通過 ISO 27001 及 OHSAS 18001 認證，確保客戶資料之安全性。未來更將計劃導入 SAS 70 Type II、PCI DSS 及取得 CSA（Cloud Security Alliance）安全認證。
2. 組織安全：導入多項國際級服務與資安專業認證，並定期邀請第三方公正認證單位重新檢驗確認其效力與實行。
3. 實體安全：採用具備援之高可用度系統架構設計，包含雙路由網路備援、設計電力備援、空調系統備援、多重部署/雙重偵測/雙層防護架構之消防系統、應用服務伺服器及網路設備完整備援等，同時配合 ISO 9001 與 ISO27001 專業認證確保管理制度的完備度。
4. 網路安全：包含建立 DDoS 分散式阻斷服務攻擊防護機制、防火牆和入侵偵測/防禦系統（IDS/IPS）等安全防護設備，主動杜絕駭客可能入侵的途徑並對惡意流量進行阻擋。
5. 主機安全：雲端運算的基礎設施皆建立於同一套硬體資源上之虛擬平台（Cloud host OS）上，因此虛擬平台的資安管理與防護便成為第一要務。相關機制包括虛擬層安全防護、作業系統安全措施、弱點掃描及滲透測試等。
6. 資料安全：除了針對儲存資料的異地備份機制外，為保護資料安全性及完整性，本公司使用最具信賴之公開金鑰基礎架構（Public Key Infrastructure, PKI）及 AES（Advanced Encryption Standard）加解密機制，對資料的傳輸提供加密保護，防止資料於傳輸的過程中被竊取；並採用即時加解密機制(On-the-fly encryption ,OTFE)與 AES 加解密機制，為資料的儲存提供加密保護。

7. 雲服務開發與運行安全：所有雲端服務程式檔案都必須經過簽章來防止系統檔案遭到竄改，並於上線前後定期進行主機及網站之弱點掃描與滲透測試。有關雲端服務之啟動與終止程序、改變防火牆之參數…等雲端服務功能的每個動作都必須經過認證與授權，確保運行安全。
8. 雲服務存取安全：為確認存取雲端服務的適當性及安全性，本公司採用多道式身分認證、服務存取管制、取記錄與稽核，並搭配通訊加密確保連線安全。例如典型的帳號/密碼機制搭配 hiNet 動態密碼鎖（hiNet OTP）、專利型手機一次性密碼（One Time Password, OTP）、hiKey、IC 卡認證等多重配套認證方式，以強化認證的安全性。
9. 維運安全：除了具備符合 ISO 27001 認證的營運持續運作管理程序及架構，提供雲端主機 7x24 全天候即時 SOC（Security Operation Center）等級之整體資安監控防護外，還必須具備緊急災難時的服務回復、資料備援等，以達成 99.9% 以上服務層級協議（Service Level Agreement, SLA），確保永續經營的要求。
10. 資安核心技術與資安服務：為因應日益頻繁的網路攻擊事件，本公司雲端運算資料中心採用先進的資安核心技術，包含 PKI 架構/金鑰管理、先進的資料與通訊加解密技術、雲端新興威脅防護以及整合式多元身份認證與授權機制，並設置專責的資安研究與服務專業團隊。其中，PKI 架構採用高信賴度之 RSA 2048-bit 高安全性金鑰，滿足訊息傳遞與交換過程之資料私密性、資料完整性、身分識別與不可否認性等資訊安全四大需求功能，並遵循業界先進標準的金鑰管理互通協定（Key Management Interoperability Protocol, KMIP）提供與其他系統互通性。除了上述核心資安技術基礎外，本公司電信研究院也針對雲端安全議題進行研究，並朝向五個面向：雲端核心安全、安全雲端儲存、雲端身份與存取管理(Identity and Access Management, IAM)、雲端 PKI 安全與雲端攻防，研發相對應的雲端安全防護技術。

雲端服務營維流程自動化

「雲端服務營維運管理系統」是雲端運算資料中心的核心系統，用以實現雲端運算服務的自動化與彈性化資源調度，降低營運與維運作業複雜度與成本，確

保服務品質並提升服務使用滿意度。為達到雲端運算資料中心營維流程自動化需求，中華電信研究院基植於多年研發電信級營維運管理系統(Operation Supporting System, OSS)之豐富經驗，依循 TM Forum Frameworx 和 SOCCI 技術規範[4][5]，自主研發國際級的「雲端服務營維運管理系統」。此「雲端服務營維運管理系統」的設計兼顧完整的營維流程(Business Process)、共通的營維資訊(Shared Information Data Model)、完善的營維功能(Operations Applications)及高彈性的系統整合架構(System Integration Architecture)等四大特色，同時具備模組化的彈性調整特性，以快速因應多變的環境(如圖 3)。

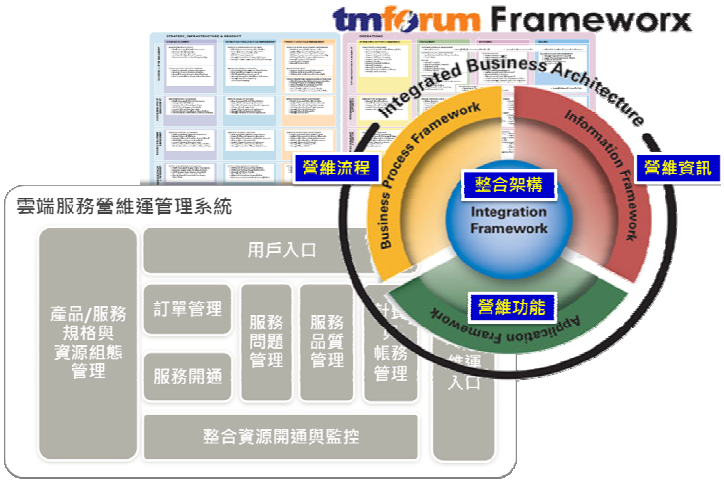

圖3. 雲端服務營維運管理系統遵循國際標準技術實現雲端服務營維流程自動化

圖4. 雲端服務營維運管理系統之系統架構

「雲端服務營維運管理系統」的功能包括業務支援(Operation Support & Readiness)、供裝(Fulfillment)、品保(Assurance)、帳務(Billing)等四大類 End-to-End 垂直整合的營維流程(Business Process)，並具備客戶管理、服務管理、資源管理等三大類水平分層管理功能，以單一系統串整四大營維流程，提供自動化管理功能，有效減低人工作業之複雜度及減少人工作業引發之錯誤，大幅減低維運成本(如圖 4)。雲端運算資料中心的資源包含運算、儲存及通訊等，因此「雲端服務營維運管理系統」結合了資訊技術(IT)與通信技術(CT)的維運管理能力，整合並管控包含運算、儲存、開發平台、應用服務及網路等多廠牌、多類型的實體與邏輯資源，並以彈性、高效益之資源池管理功能為基礎，實現雲端服務快速供裝、隨需即用、多類終端接取、服務自主管理、以量計價、資源彈性調整等重要特性，提供用戶無縫端對端(End to End)的多類型雲端服務。

雲端服務營維運管理系統重要核心能力包括：

- 多重網路架構、多機房實體與虛擬資源池整合管理機制
- 虛擬機資源池自動化管控機制
- 多類雲端產品動態上架管理機制
- 受理、訂單、供裝、帳務流程無縫式自動銜接
- 雲端運算服務快速供裝機制
- 支撐一站式自助申裝及多樣化隨選即用雲端服務
- 高彈性供裝流程引擎與資源指配最佳化技術
- 動態匯集服務使用量，快速處理大量使用紀錄，彈性計價
- 異質性網路/運算/貯存資源整合監控
- 跨機房/跨廠牌之資源監控與服務品質分析機制
- 申告自助服務與障礙標準處理流程

「雲端服務營維運管理系統」具備操作簡易、高品質、彈性擴充、高資源利用率等特性，可成功建構政府雲端運算資料中心的維運管理系統，強化資源整合共享，使政府各機構免去各自建立相關系統，大幅提高運作效率並避免重覆投資的浪費。此外，「雲端服務營維運管理系統」亦能夠應用於各類型雲端應用服務

營運，成為各種雲端服務的核心基礎，提供穩定的虛擬化環境，以及雲端創新應用服務開發，與同業共同建立多元共生之雲端生態系統(Cloud Ecosystem)。

結語

我國雲端運算發展已從技術研究、發展試驗，進展到實用推廣的階段。因此，政府相關雲端運算應用服務便具備示範引領的作用，具有鼓勵企業安心採用雲端運算技術的推動作用。「政府雲端資料中心基礎建設」為政府雲的重要建設之一，藉由中華電信公司自主研發的「雲端服務營維運管理系統」及高安全度的資安防護機制，將成功強化政府雲端資料中心的資源整合共享，大幅提高運作效率，滿足電子化政府多元化雲端運算應用服務的營運，同時也為我國雲端運算產業發展建立良好的典範成果。

參考資料

[1] 行政院研究發展考核委員會，http://www.rdec.gov.tw/
[2] 行政院科技會報辦公室，雲端運算應用與產業發展方案，2012年11月。
[3] 中華電信股份有限公司，中華電信雲端運算服務安全白皮書，2010年。
[4] TM Forum Frameworks，http://www.tmforum.org/TMForumFrameworx/1911/home.html
[5] “Service-Oriented Cloud Computing Infrastructure (SOCCI) Framework”, The Open Group, Dec. 2011.