構建國軍雲端資料中心資訊安全防護關鍵因子之初探

作者簡介

劉定衛上校，國防管理學院79年班、靜宜大學管理科學碩士、國立中央大學資訊管理博士；曾任資參官、研究教官、科長、主任教官、副組長，現任陸軍後勤指揮部後勤通資中心主任。

提要

一、網路攻擊已逐漸成為一種軍事武器，敵人可透過網路，癱瘓通訊、運輸、交通等重要基礎建設，進而影響國軍戰力。國防部刻正規劃建構符合國軍特性之雲端服務架構，整併現有機房為雲端資料中心及軍種資料中心，提供效率高及存活性強之資訊服務架構；故如何建立雲端資料中心之資訊安全防護措施，防止國防機密資訊外洩、網路遭破壞入侵以及資料遭竊取等網路攻擊情事，已成為攸關國家安全之重要議題。

二、本文以過往對資訊安全防護能力指標之研究論文為基礎，並參酌政府部門雲端資料中心所提供的資訊安全相關機制，提出國軍雲端資料中心在建構資訊安全防護作為時，必須思考的面向及關鍵因子，期能提供資通訊相關部門之決策參考。

三、經歸納與比較相關研究內容，本文初步提出國軍雲端資料中心的資訊安全

作為必須以「資訊安全設備」、「人員專業能力」及「資訊安全管理」3個面向為主軸，並透過落實執行各面向下的細部關鍵因子，包含「完善資安防護設備」、「提升資料加密機制」、「妥採備份備援措施」、「嚴密實體安全管控」、「遴選符資專業人員」、「培訓人員進階職能」、「落實資安威脅修補」及「維護資料存取安全」8項，以確保國軍雲端資料中心在運作時能安全無虞，提供穩定且高品質的資訊服務。

關鍵詞：雲端服務、雲端資料中心、網路資料中心、資訊安全、關鍵因子

前　言

在數位時代，企業進行電子化(e化)的過程中，電子資料安全儲存一直是重要的課題；隨著各類資訊系統發展，以及近年大數據相關應用不斷出現，除了提高企業競爭力，企業也思考如何能以創新的方式，在兼顧降低成本與提升效率的前提下，妥善管理企業營運資料，以支持企業永續經營。

為妥善保存企業營運資料，完善的網路設備與資訊安全相關設施是必須的，然而，若要自行建置與維護各項資通訊設備，對企業而言卻是一項沉重的負擔；所以，網路資料中心(Internet Data Center, IDC)就應運而生。所謂網路資料中心，是指一個大型的資訊及數據儲存中心，可提供企業e化時存取及管理資訊，有如資料的銀行。網路資料中心所提供的服務，首先為網路基本服務，包括提供企業用戶主機代管(Co-Location)、虛擬主機(Virtual Hosting)、機房共構與企業專線等服務；其次為網路加值服務，如網路管理與監控服務、防火牆、伺服器加速快取服務、網路流量分析、設施管理、網路健診、網管委外基本服務及防毒、防駭等安全管理服務。

建置網路資料中心的成本，對民間企業是一大負擔，對國軍而言亦是如此。國軍資訊人力與資源，在過去數年間歷經多階段的精簡，以往由各軍種分散建置資訊機房的模式，現階段已面臨管理人力不足以及運作效率欠佳等諸多課題，實有必要以集中建置方式，將人力與資源向上收攏，並將資訊資源置於關鍵節點，使資訊服務能有效支援各單位任務遂行。

這樣的概念在雲端科技出現後，有了解決方案。國防部自民國100年起，逐步推動雲端服務的建構，整併國軍現有資訊機房為雲端資料中心及軍種資料中心，

國軍資訊作業規劃由單點提供服務調整為作戰區導向之多點服務架構，資訊服務型態從過去各單位自行籌建、管理，調整為整體規劃發展，資訊服務由資料中心統籌提供，另規劃基礎建設、通用性服務、功能性服務、雲端資安及虛擬化5類服務。[1]

美國「2015年國家安全戰略」指出，網路空間安全威脅是當前國家安全、公共安全和經濟安全所面臨最為嚴重的挑戰之一。[2]就國家安全而言，網路攻擊手段可成為一種強大的軍事武器，敵人可透過網路，癱瘓通訊、運輸、交通等重要基礎建設，進而影響國軍部隊戰力，更可破壞國家金融交易網，水、電力設施及行動電話基地臺等民生基礎設施，造成社會秩序混亂，對任何國家的生存發展，均可構成嚴重威脅。透過趨勢科技2015年資訊安全總評報告，[3]可瞭解資安事件的影響程度因網路攻擊手法不斷翻新，使得威脅的深度及廣度持續增加，尤以數度發生之「重要資料外洩」最易造成社會大眾恐慌與不安，再加上遵行政院推動雲端產業政策[4]及物聯網(Internet of Things, IoT)的加速普及，使得原本的資安挑戰更加棘手。

為確保建構雲端服務的同時，亦能完善其安全性，美國國防資訊系統局(Defense Information Systems Agency, DISA)於2016年3月為美國國防部發展了「國防部雲端運算安全要求指引(Department of Defense Cloud Computing Security Requirements Guide)」，[5]其主要目的包括：「提供國防部及商業雲端服務提供者安全需求與指引，並要求雲端服務產品應納入『國防部雲端服務目錄』[6]中」、「建立國防部評估本身或其雲端服務提供者產品之安全狀態的基準」、「提供國防部官員使用與建置雲端服務時之要求與架構」、「提供國防部官員在使用雲端服務產品時之規劃與授權」以及「支持國防部將網站及應用程式從其內部網路及資料中心，遷移到較低成本的商業資訊服務」。

1 國防部，民國100年3月31日國通軟發字第1000000883號令頒「國軍雲端服務發展計畫」。

2 國防部，《中華民國104年國防報告書》(臺北：國防部，民國104年10月)，頁44。

3 趨勢科技，〈2015年資訊安全總評報告〉，http://www.trendmicro.tw/cloud-content/tw/pdfs/security-intelligence/reports/rpt-setting-the-stage.pdf，檢索日期：2017年4月30日。

4 行政院科技會報辦公室，〈雲端運算應用與產業發展方案〉，http://image.tca.org.tw/AD/EDM1011212094226/雲端運算應用與產業發展方案(核定本)101年11月.pdf，2017年4月30日。

5 Defense Information Systems Agency, Department of Defense Cloud Computing Security Requirements Guide, http://iasecontent.disa.mil/cloud/SRG/,2017年7月12日。

6 DoD Cloud Service Catalog, http://www.disa.mil/~/media/Files/DISA/Services/Cloud-Broker/AuthorizedCloudServicesCatalog.pdf, 2017年7月12日。

在「國防部雲端運算安全要求指引」中，所述及的安全要求(Security Requirements)計有18項：(1)國防部的安全控制政策；(2)法律相關注意事項；(3)持續性評估；(4)雲端服務提供者使用國防部公鑰基礎設施(PKI)相關事項；(5)政策、指引與操作限制；(6)實體設施和人員存取權限管理；(7)資料洩漏管理；(8)資料檢索及雲端服務中止使用的資料銷燬；(9)儲存媒體與硬體的再用與處置；(10)服務架構要求；(11)儲存於雲端的靜態資料加密；(12)資料備份；(13)承包商／任務合作夥伴對雲端服務產品的使用；(14)任務負責人在雲端服務的測試與發展；(15)埠口、協議、服務、管理和基於雲端的系統／應用程式之使用要求；(16)行動碼的獲得、傳輸與使用；(17)雲端系統／應用程式之註冊和連結核准；(18)供應鏈風險管理評估；(19)電子郵件保護要求事項。

國軍的雲端資料中心依網路實體隔離政策，將建置於軍網內部，雖未與外界網際網路連接，但並不代表絕無資訊安全的風險與挑戰。觀察國際各類資安事件與網路攻擊手法，震網(Stuxnet)蠕蟲即是攻擊實體隔離內網設備之最佳案例。[7]因此，國軍相關單位在建構雲端資料中心時，務必考量影響其資訊安全的相關因素，並預先採取防範措施，降低其面對的資訊安全風險。

本文旨在探討國軍雲端資料中心構建時，所須考量的資訊安全防護面向與關鍵性因子，由於國軍與民間企業之任務不同，其所構建的雲端資料中心因應特殊任務需求，將有不同的資訊安全考量因素。惟囿於現有研究文獻中，並未能搜尋到探討國軍雲端資料中心資訊安全相關之研究文獻，故本文首先回顧筆者於2015～2016年指導的兩篇碩士論文，分別從網路作戰及網路資料中心的角度，歸納出建置網路資料中心時必須考量的資訊安全防護指標，再從雲端服務與雲端安全的角度，探討這些防護指標對雲端資料中心資訊安全的影響，最後提出構建國軍雲端資料中心資訊安全防護的面向與關鍵因子，期能做為未來資通訊相關部門在建置雲端資料中心時，資訊安全相關作為之參考。

網路作戰觀點下的資訊安全防護指標

美軍在2012年發表的「聯戰準則3-13資訊作戰」(Information Operations, Joint Publication 3-13)中，闡釋「網路戰」區分為電腦網路攻擊(Computer Network Attack, CNA)、電腦網路防禦(Computer Network Defense, CND)及電腦網路利用

7　維基百科，〈震網〉，https://zh.wikipedia.org/wiki/震網，2017年4月30日。

(Computer Network Exploitation, CNE)三重指標任務；[8]國軍在相關資訊戰準則中，亦開宗明義闡述「資訊攻擊」、「資訊防護」及「資訊管理運用」。資訊攻擊包含指管攻擊、電子攻擊、網路攻擊、情報戰、心理戰、經濟資訊戰及其他資訊攻擊手段；資訊防護包含指管防護、電子防護、網路安全防護、情報蒐集、心理建設、經濟資訊防護及其他資訊防護手段；資訊管理運用則是運用指、管、通、情、監、偵系統與其他資訊系統，迅速獲得一切可供決策所需之資訊；資訊作戰即運用資訊科技蒐集、處理、傳輸與管理敵我雙方各項資訊與情報運用，以資訊分享與自動化機制，快速將大量繁雜之資訊轉換成重點情資。[9]

基於網路戰已成為未來極可能發生的情境，各先進國家無不把建立網路戰能力做為重要的建軍發展方向；林志章於2015年，以「國軍網路作戰部隊作戰能力評估指標之研究」為題，[10]透過專家問卷(Expert Questionnaire)調查，建立「4個構面、21項能力指標」的網路作戰能力評估指標，再運用層級分析法(Analytic Hierarchy Process, AHP)，[11]歸納並提出一套網路戰作戰能力指標 (如圖1)，各個構面及其所包含的指標說明如后：

一、網路攻擊構面

包含弱點掃瞄操作、作業系統操作、網路位址匿蹤、傀儡網布建及惡意程式編撰5個能力指標。

二、電腦防護構面

包含電腦鑑識操作、誘捕系統操作、網路封包分析、網路設備設定及資安設

8 Department of Defense, JP3-13 Information Operations (USA: DoD, 2012), http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf, 2017年4月30日。

9 國防部陸軍司令部，《陸軍資訊戰教則(試行本)》(龍潭：國防部陸軍司令部，民國95年)，頁1-3。

10 林志章，《國軍網路作戰部隊作戰能力評估指標之研究》(臺北市：國防大學管理學院資訊管理學系，西元2015年)。本篇為碩士學位論文，指導教授：蘇品長博士、劉定衛博士。

11 層級分析法(Analytic Hierarchy Process, AHP)為匹茲堡大學教授Thomas L. Saaty於1971年所發展，主要應用在不確定情況下及具有多數個評估準則的決策問題，目的是將複雜的問題予以系統化，並由不同層面進行層級分解，透過量化運算，找到脈絡再加以綜合評估。此方法可以將複雜的決策情境區分為數個小部分，再將這些小部分組織成為一個樹狀的層次結構，並彙整專家意見，以評估尺度針對每一個部分的相對重要性給予權重數值；其後建立成對比較矩陣，並求出特徵向量及特徵值，以該特徵向量代表每一層級中各部分的優先權，能提供決策者充分的決策資訊並組織有關決策的評選條件或標準(Criteria)、權重(Weight)和分析(Analysis)，且能減少決策錯誤的風險性。在操作流程中，首先是問題描述，而後判別影響要素及建立層級結構，並設計問卷項目，進而依問卷收集的數據資料找出各層級間決策屬性的相對重要性，再依此建立成對比較矩陣用以計算矩陣特徵值與特徵向量，所得出的數據經由一致性檢定及層級結構一致性檢定的回饋修正後，便可計算出各指標之權重以協助選出最適決策方案。

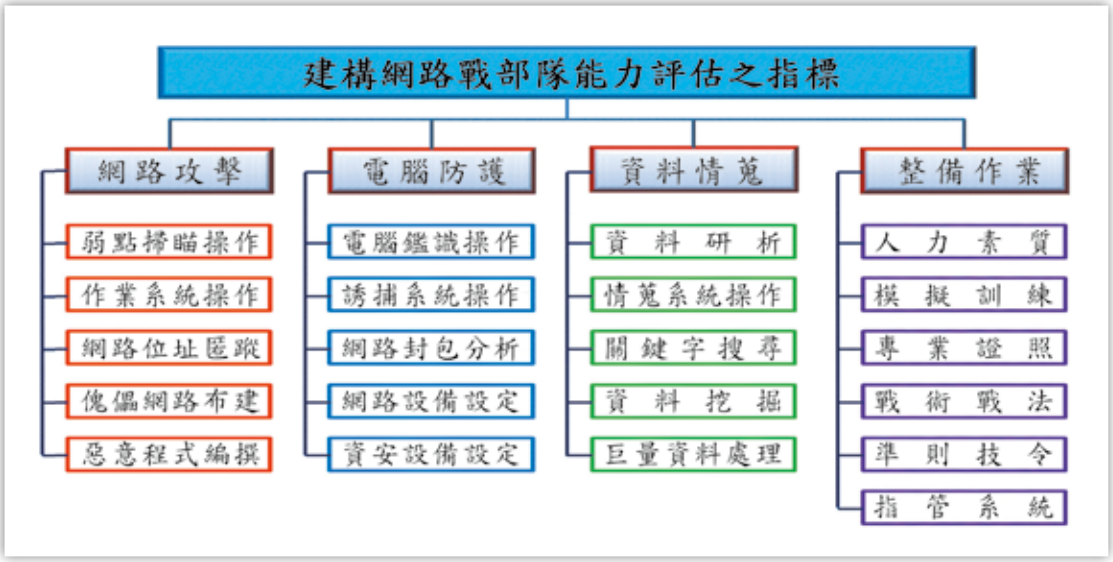

圖1　網路戰部隊作戰能力評估指標架構

資料來源：林志章，《國軍網路作戰部隊作戰能力評估指標之研究》(臺北市)，國防大學管理學院資訊管理學系，2015年碩士論文，頁53。

備設定5個能力指標。

三、資料情蒐構面

包含資料研析、情蒐系統操作、關鍵字搜尋、資料挖掘技術及巨量資料處理5個能力指標。

四、整備作業構面

包含人力素質、模擬訓練、專業證照、戰術戰法、準則技令及指管系統6個能力指標。

在前述構面中，有關「電腦防護」構面所包含的5個能力指標及其定義說明如后：

一、電腦鑑識操作

能運用電腦鑑識工具，對入侵者所留下的蛛絲馬跡進行各式的專業鑑識，以及撰寫資訊安全事件標準文件之作業能力。

二、誘捕系統操作

具備設定及操作虛擬化網路型誘捕系統之作業能力。

三、網路封包分析

具備分析惡意程式與駭客攻擊封包行為之作業能力。

四、網路安全設備設定

具備路由器安裝設定之技術能力。

五、資訊安全設備設定

具備入侵偵測系統操作及特徵碼更新，以及具備防火牆規則設定之作業能力。

上述構面及指標，經過AHP問卷對從事網路戰人員進行調查，並以Expert Choice 2000決策分析程式運算，獲得各評估要項之相對權重值，以進行分項要項之比較。在主要構面要項比值方面，資料

情蒐：0.55＞電腦防護：0.272＞網路攻擊：0.112＞整備作業：0.067(如圖2)；顯見在國軍網路戰人員的看法中，電腦防護較網路攻擊及整備作業更為重要。

若再針對「電腦防護」的各個指標分析，經由Expert Choice 2000程式運算結果，依比值次序為：網路封包分析：0.615＞電腦鑑識操作：0.18＞資訊安全設備設定：0.101＞誘捕系統操作：0.058＞網路安全設備設定：0.046，其中以「網路封包分析」為最優先(如圖3)。

網路或雲端資料中心的建立，首重資訊安全防護，林志章(2015)的研究雖然是以網路戰觀點出發，「電腦防護」僅是作戰能力的一部分，但其所整理出的指標與優序，對網路或雲端資料中心遂行資訊安全相關防護作為而言，仍可做為重要之參考依據。

網路資料中心的資訊安全防護指標

鑑於安全及信賴是使用任何服務的第一前提，[12]且資訊安全管理的目的在保護電腦資源，包括：硬體、軟體、資料、

圖2　網路戰部隊作戰能力評估各構面權重值配比

資料來源：林志章，《國軍網路作戰部隊作戰能力評估指標之研究》(臺北市)，國防大學管理學院資訊管理學系，2015年碩士論文，頁59。

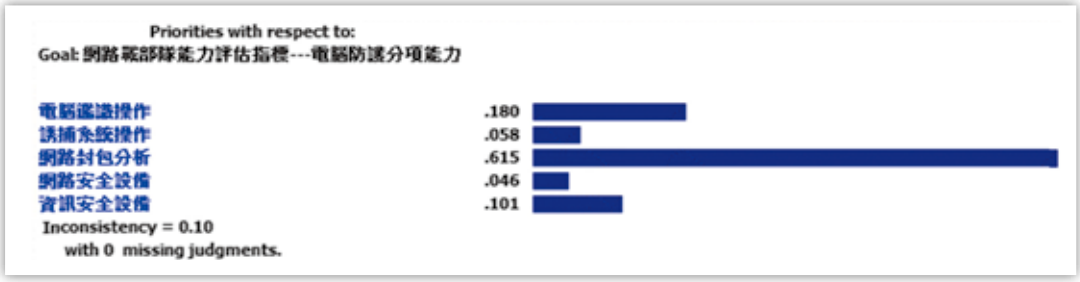

圖3　電腦防護分項能力指標權重統計及分析結果

資料來源：林志章，《國軍網路作戰部隊作戰能力評估指標之研究》(臺北市)，國防大學管理學院資訊管理學系，2015年碩士論文，頁65。

12　行政院科技顧問組，《2010資通安全政策白皮書》(臺北市：行政院，民國99年)，頁8。

程式及人員，以防止電腦資源被變更、破壞及未授權使用，為瞭解國軍網路資料中心資訊安全防護未來重點發展方向，朝重點建軍備戰，持續籌建可恃之國防資訊安全防護能力，吳世璋於2016年，以「網路資料中心資訊安全防護能力評估指標之研究」為題，並以「某國軍網路資料中心」為對象，[13]探討網路資料中心資訊安全防護能力評估指標，期望經由文獻探討及德爾菲法專家問卷所得結果，研訂國軍網路資料中心資訊安全防護各構面項目，運用AHP發展資訊安全防護各構面能力評估之衡量標準，再透過評估指標的建構，進而能夠獲得資訊安全防護能力的分析方法，奠定國軍優質資通作業根基，創造高效率及高安全性之資訊作業環境。

在吳世璋(2016)的研究中，首先透過專家問卷及訪談，訂定「網路資料中心資訊安全防護能力評估架構」，包含「管理程序」、「人員技術」以及「設備建置」3個構面，各構面分別有10、6及5個指標，總計有21個指標(如圖4)。各構面及指標之意義說明如后：

一、管理程序構面

本構面區分資產風險評鑑、使用者管理、防護管理、應變復原機制、稽核程序、存取控制規範、風險管理、網路實體隔離、儲存媒體管理及機房維運10個

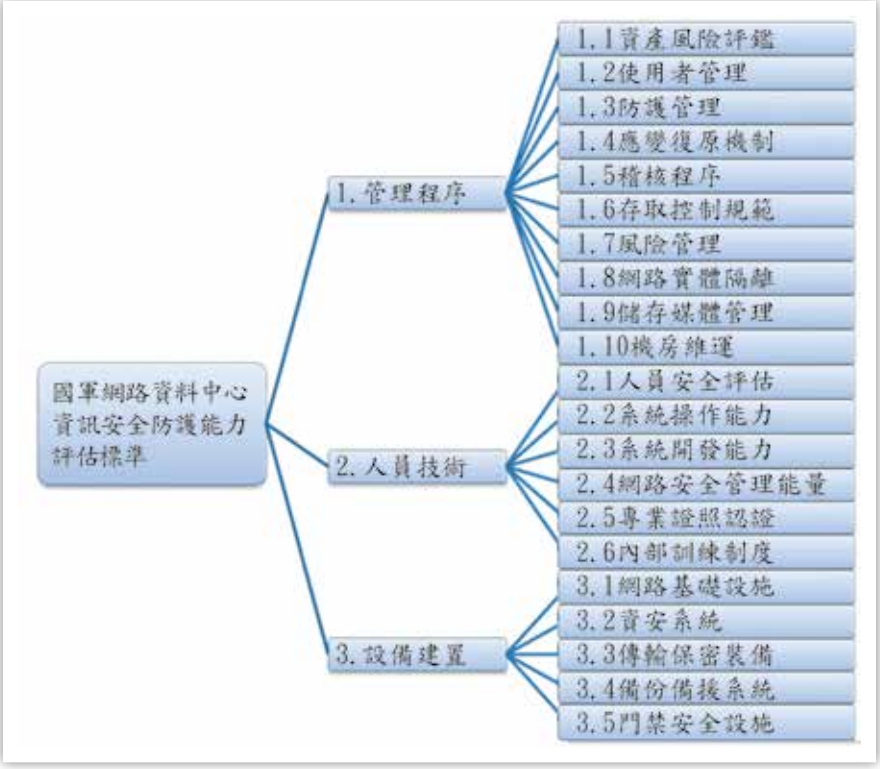

圖4　網路資料中心資訊安全防護能力指標架構

資料來源：吳世璋，《網路資料中心資訊安全防護能力評估指標之研究—以國軍某網路資料中心為例》(臺北市)，國防大學管理學院資訊管理學系，2016年碩士論文，頁47。

13　吳世璋，《網路資料中心資訊安全防護能力評估指標之研究—以國軍某網路資料中心為例》(臺北市：國防大學管理學院資訊管理學系，西元2016年)。本篇為碩士學位論文，指導教授：蘇品長博士、劉定衛博士。

項目。

(一)資產風險評鑑：為硬體、軟體、資料、人員、文件與週邊設備的鑑定，以釐清重要資訊資產的潛在風險。

(二)使用者管理：使用者登入時，正確記錄終端機及登入作業等相關資訊，以為後續系統監測使用者狀況，並可防止未被授權者任意變更他人的電腦設定及檔案內容。

(三)防護管理：參考惡意攻擊模式，使機房維管人員依程序落實資訊安全防護之管理作為。

(四)應變復原機制：對於各項足以造成服務中斷之風險，分析其成因及後果，訂定可行之應變與復原計畫。透過教育訓練、狀況演練及不斷修改，確保狀況發生時，能有效執行應變措施，將損害降低至可承受範圍，確保組織及資訊運作流程能在既定時間內重建及恢復運作。

(五)稽核程序：落實組織實施資訊安全防護的作為，藉以掌握組織資訊安全的可能缺失，適時執行矯正行動及追蹤確認。

(六)存取控制規範：建立機房維運人員對系統程式及資料存取之權限及範圍。

(七)風險管理：釐清資訊資產可能面臨的風險，進而加以控管，將風險降低至維運管理可承受的程度，確保業務運作持續無礙。

(八)網路實體隔離：國軍軍網、戰情、指管及情傳等網路，不得與網際網路及學術網路之電腦搭接或混用，並嚴禁與國軍各資通訊系統設備共用主機及裝設切換開關。

(九)儲存媒體管理：針對具有儲存、讀取或交換資訊能力之設備、轉存裝置，包括磁帶、磁碟(片)、光碟片等，明確定義可攜式設備的使用規範及使用者的相關權責。

(十)機房維運：資料檔案之備份、控管及電腦設備、機房之維護、安全控制。

二、人員技術構面

本構面區分人員安全評估、系統操作能力、系統開發能力、網路安全管理能量、專業證照取得及內部訓練制度6個項目。

(一)人員安全評估：工作職責須使用或處理機敏性資訊的人員，應經適當的安全評估與考核程序。

(二)系統操作能力：資訊安全事件大多是因人為操作錯誤而產生，強化人員對各系統設定及故障排除之操作能力，亦能降低事件發生機率。

(三)系統開發能力：開發人員須具備系統開發經驗或系統整合能力，以確保開發之系統符合資安防護要求。

(四)網路安全管理能量：在網路環境中，所運作的軟體、硬體、作業系統應受到適當的保護，避免因人為因素或自然災害遭受損壞，且可持續的運行或提

供服務。

(五)專業證照取得：透過資訊(安)專業證照取得，提升作業人員的技能與素養，精進人力資源品質，強化資安防護能量。

(六)內部訓練制度：灌輸資安觀念，教導工作技能，培育資訊(安)人力資源，使人員瞭解資安管制作法與應行注意事項，降低違規情事。

三、設備建置構面

本構面區分網路基礎設施、資安系統、傳輸保密裝備、備份備援系統及門禁安全設施5個項目。

(一)網路基礎設施：依區域網路、遠端存取及廣域網路等所需之各式網路規劃需求，建置相對應設備，並針對容量使用狀況，分析及找出可能危及系統安全的瓶頸，預先規劃補救措施，以滿足作業需求。

(二)資安系統：藉分析達成安全性的需求，針對所需控管之項目，建置相對的資安系統及設備。

(三)傳輸保密裝備：國防機密資訊傳輸必須使用政府權責主管機關核發或認可之保密裝備或加密技術。

(四)備份備援系統：為使單位業務能持續運作，應依單位需求建立資料備份及系統備援措施，以防止資料與系統損失(壞)，影響業務遂行。

(五)門禁安全設施：重要及機敏資訊處理設備應置於安全區域，並劃出安全防線，建置適當的安全檢查關卡及門禁保護，確保受到實體的嚴密保護，避免遭非授權人員非法存取、損害干擾。

在構面及指標建立後，透過AHP問卷對網路資料中心主管及作業人員進行調查，並以Expert Choice 2000程式運算，在主要構面方面，其權重以「設備建置(0.481)」為最重要，其次為「人員技術(0.320)」，最後則是「管理程序(0.199)」(如圖5)。透過AHP分析發現主要構面權重以「設備建置」占了48%，比重將近一半，此結果反映出國軍網路資料中心在資訊安全防護環境的建置上，受試者認為當有資安事件時，對於硬體的投資不管是電力、環控、消防、資訊設備及門禁設施等，都是為了保障機房所架裝的設備及儲存的資料，而且為達國軍網路資料中心資訊服務不中斷目標，構建穩定又可靠的網路基礎建設及嚴密的監控管理設備，亦是不可或缺。

有關各構面下的細部指標分析說明如后：

一、管理程序構面

對於「管理程序」構面議題下的指標，經問卷權重計算結果(如圖6)，顯示「儲存媒體管理(0.13)」指標為最重要，接著依序為「機房維運(0.124)」、「網路實體隔離(0.121)」、「應變復原機制(0.103)」、「稽核程序(0.1)」、「風險

圖5　網路資料中心資安防護能力主要構面分析結果

資料來源：吳世瑋，《網路資料中心資訊安全防護能力評估指標之研究—以國軍某網路資料中心為例》(臺北市)，國防大學管理學院資訊管理學系，2016年碩士論文，頁52。

管理(0.095)」、「存取控制規範(0.094)」、「使用者管理(0.079)」及「防護管理(0.079)」指標，最後則是「資產風險評鑑(0.075)」指標。

二、人員技術構面

對於「人員技術」構面議題下的指標，經問卷權重計算結果(如圖7)，顯示「網路安全管理能量(0.184)」指標為最重要，接著依序為「系統操作能力(0.181)」、「內部訓練制度(0.18)」、「專業證照認證(0.169)」及「系統開發能力(0.147)」指標，最後則是「人員安全評估(0.139)」指標。

三、設備建置構面

對於「設備建置」構面議題下的指標，經問卷權重計算結果(如圖8)，顯示「備份備援系統(0.235)」指標為最重要，接著依序為「傳輸保密裝備(0.214)」、「門禁安全設施(0.213)」及「資安系統(0.195)」指標，最後是「網路基礎設施(0.143)」指標。

四、整體權重分析

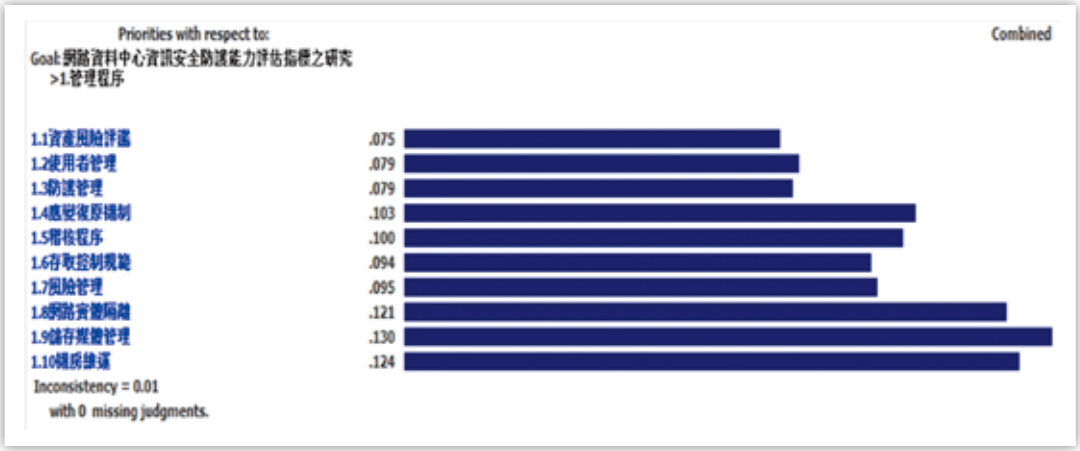

圖6　網路資料中心資安防護能力管理程序構面各項目計算結果

資料來源：吳世瑋，《網路資料中心資訊安全防護能力評估指標之研究—以國軍某網路資料中心為例》(臺北市)，國防大學管理學院資訊管理學系，2016年碩士論文，頁54。

圖7　網路資料中心資安防護能力人員技術構面項目計算結果

資料來源：吳世璋，《網路資料中心資訊安全防護能力評估指標之研究—以國軍某網路資料中心為例》(臺北市)，國防大學管理學院資訊管理學系，2016年碩士論文，頁56。

經由AHP所彙整的指標權重整體排序(如圖9)可以發現，在吳世璋(2016)對個案組織的研究，受試者認為「備份備援系統(0.113)」是絕對重要的評估項目，再來是「傳輸保密裝備(0.103)」及「門禁安全設施(0.103)」均占了10%，這也顯示了大多數受試者對於儲存資料的完整性及可用性的重視；另外針對資料的保密與機房的實體及環境安全也須同步加強管理，亦已成為現今資訊安全工作中不可或缺的重要環節。

另一方面，在整體權重排序中，對於各項管理程序在組織中均已依循上級管理單位所制訂之管理制度執行，並定期辦理稽核作業，所以對吳世璋(2016)研究之個案網路資料中心而言，在比重上也就沒這麼高。

網路資料中心與雲端資料中心之差異

行政院於民國106年1月9日訂定「行政院及所屬各機關資料中心設置作業要點

圖8　網路資料中心資安防護能力設備建置構面項目計算結果

資料來源：吳世璋，《網路資料中心資訊安全防護能力評估指標之研究—以國軍某網路資料中心為例》(臺北市)，國防大學管理學院資訊管理學系，2016年碩士論文，頁57。

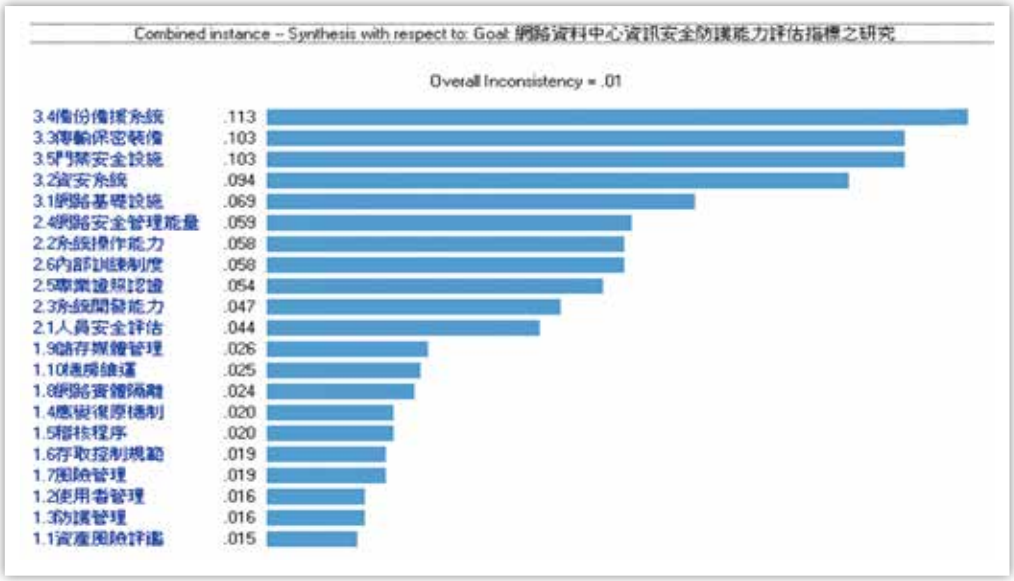

圖9　網路資料中心資安防護能力各構面項目整體權重排序

資料來源：吳世璋，《網路資料中心資訊安全防護能力評估指標之研究—以國軍某網路資料中心為例》(臺北市)，國防大學管理學院資訊管理學系，2016年碩士論文，頁60。

」，[14]其目的乃為提升行政院所屬各機關(構)資料中心運作效率及管理效能，打造穩健、彈性及綠能之資訊基礎建設，藉以提升電子化政府服務品質。作業要點適用對象雖然不包含國防部及其所屬機關(構)，但仍可做為國軍在建立相關資料中心時之參考。

該作業要點也揭示「資料中心」、「雲端資料中心」與「通訊機房」之定義，茲說明如后：

一、資料中心

指各機關為供資通訊系統正常運行所設置之基礎及備援設施，其主要設施包含運算伺服主機、儲存設備、網通設備、資安設備、環境控制設施及存放前述設施之實體空間。

二、雲端資料中心

指提供使用者隨需自助服務(On-demand Self-service)、多元網路存取(Broad Network Access)、多人共享資源池(Resource Pooling)、快速且彈性部署(Rapid Elasticity)及服務可量測(Measured Service)5項特性之資料中心。

三、通訊機房

指各機關為提供員工連結網際網路、內部使用之資訊服務及維持與資料中心網路通訊，所設置之小型資料中心，其設施僅限必要之網通設備、資安設備及提供機關在地專用資通訊服務運行所需之運算伺服主機。

就前述「資料中心」與「雲端資料中心」的定義而言，前者著重於資訊機房的基礎設施與備援管理，而後者則是著重於為了提供存取服務而進行的設備建置與

14　行政院國家發展委員會，民國106年1月 9日院授發資字第1051501757號函訂定「行政院及所屬各機關資料中心設置作業要點」。

資源部署，因此，兩者在資訊安全管理上注重的應有所不同。在2009年以前，大部分的雲端運算基礎架構是由通過資料中心傳送的可信賴服務和建立在伺服器的不同層次的虛擬化技術所組成的。人們可以在任何有提供網路基礎設施的地方使用這些服務，而「雲端」通常表現為對所有用戶運算需求的單一存取點。人們通常希望商業化的產品能夠滿足服務品質(Quality of Service, QoS)的要求，並且一般情況下要提供服務水準協定(Service Level Agreement, SLA)。[15]

雲端運算的安全性(Cloud Computing Security)，有時也簡稱為「雲端安全」(Cloud Security)，是一個演化自電腦安全、網路安全、甚至是更廣泛的資訊安全的子領域，而且還在持續發展中。雲端安全是指一套廣泛的政策、技術與被部署的控制方法，以用來保護資料、應用程式與雲端運算的基礎設施。雲端安全的面向可被歸結為「安全與隱私」、「規範遵循」以及「法律或契約議題」3大領域。[16]

一、安全與隱私

為了確保資料是安全的，不會被未授權的使用者存取，或單純地遺失，以及資料隱私是被保護的，雲端服務提供商必須致力於資料保護、身分管理、實體與個資安全、可用性、應用程式安全以及隱私等事項。

二、規範遵循

(一)關於資料的儲存與使用有眾多的規範，包括Payment Card Industry Data Security Standard (PCI DSS)、Health Insurance Portability and Accountability Act (HIPAA)、沙賓法案等。這些規範中有許多都需要定期的回報和稽核追蹤。雲端服務提供商必須協助他們的客戶可以適當地遵守這些規範。

(二)在商業連續性與資料復原方面，雲端服務提供商必須有商業連續性與資料復原計畫，以確保在發生災害或緊急情況的情況下可以繼續提供服務，並且可以復原任何遺失的資料。這些計畫必須和客戶分享並可讓客戶審視。

(三)在日誌與稽核追蹤方面，除了產生日誌與稽核追蹤，雲端服務提供商必須與客戶合作，只要客戶有需要，就必須確保這些日誌與稽核追蹤會被適當地保全、維護，並當有法庭調查的需要時能夠取用。

(四)在獨特的規範要求方面，除了順應客戶的需求，由雲端服務提供商負責維運的資料中心也可能要遵循規範的要求。

15 雲端運算，https://zh.wikipedia.org/wiki/雲端運算，2017年4月30日。

16 雲端運算的安全性，https://zh.wikipedia.org/wiki/雲端運算的安全性，2017年4月30日。

三、法律或契約議題

除了遵從前述列舉的安全和規範議題，雲端服務提供商和客戶依照責任來協商訂定條款(例如：當有資料遺失的事件發生時該如何協商解決)、智慧財產權與服務的終止(例如：何時會將資料和應用程式還給客戶)。公眾的紀錄，法律問題可能還包括公務機關對紀錄儲存的要求，許多中間機構必須依法使用特定的方式來儲存電子紀錄。這些可能是由立法單位或法律要求的機構所制定的規則和慣例，公眾在使用雲端運算和雲端儲存時，都必須要考慮到這些議題。

關於雲端資料中心必須提供的資訊安全機制，依據「電子化政府基礎建設網站」揭示的內容，計列出8項如下：[17]

(一)入侵偵測防禦系統：提供骨幹網路設備及網站面對網路攻擊時的防護。

(二)惡意黑名單阻擋：阻擋惡意網站及黑名單，隔絕內部主機向惡意主機連線。

(三)惡意活動偵測：偵測是否有主機受駭、進行惡意活動或擴散感染。

(四)防毒控管及主機防毒：提供虛擬主機所需之防毒軟體及病毒碼更新。

(五)主機及網站弱點掃瞄：每季對主機及網站進行弱點掃瞄，並提供弱點掃瞄報告。

(六)作業系統安全修正檔更新通知：定期連至Windows Update及CentOS網站檢查是否有新的作業系統安全修正檔案。

(七)服務監控及告警：提供服務異常監控及告警服務。

(八)不同用戶虛擬主機安全隔離：不因任何一個用戶之虛擬主機的資安漏洞或應用程式問題，影響到同一資料中心其他用戶存取服務之權利。

國軍雲端資料中心資訊安全防護關鍵因子

本節綜整林志章(2015)提出的「網路作戰部隊電腦防護能力指標」、吳世璋(2016)提出的「網路資料中心資訊安全防護能力指標」，以及電子化政府基礎建設網站所列出「雲端資料中心提供的資訊安全機制」(如表1)，並考量國軍網路環境現況，提出未來國軍在建立雲端資料中心時，有關資訊安全防護方面的關鍵因子，提供資通相關部門參考，俾能提高雲端資料中心建置後的安全度，也包含服務品質的穩定度。

在表1中，有關林志章(2015)所提出的指標計5項，並按其重要性依序排列，在吳世璋(2016)所提出的指標方面，其提

17 電子化政府基礎建設網站，http://www.service.gov.tw/qa_category_list_content.php?qc_id=11& qs_id=57& qd_id=565，2017年4月30日。

表1　資訊安全防護關鍵因子比較表

項次	林志章(2015)	吳世璋(2016)	雲端資料中心資安機制
1	網路封包分析	備份備援系統	入侵偵測防禦系統
2	電腦鑑識操作	傳輸保密裝備	惡意黑名單阻擋
3	資訊安全設備	門禁安全設施	惡意活動偵測
4	誘捕系統操作	資安系統	防毒控管及主機防毒
5	網路安全設備	網路基礎設施	主機及網站弱點掃瞄
6	--	網路安全管理能量	作業系統安全修正檔更新通知
7	--	系統操作能力	服務監控及告警
8	--	內部訓練制度	不同用戶虛擬主機安全隔離

資料來源：作者自行彙整。

出的指標計有21項，經考量其重要性，取前8項並按重要性依序列入，在雲端資料中心提供之資訊安全機制部分，則是依電子化政府基礎建設網站內容所列出的順序填入。

經比較林志章(2015)與吳世璋(2016)兩研究提出的指標，前者的目標係建構一套可衡量網路作戰部隊在各構面作戰能力的評估指標，以便分析其在攻擊、防護與情蒐等各面向之作戰能力，故資安防護僅是整體指標的一部分；而後者則是聚焦於網路資料中心，目的為在建構一個可靠、穩定、安全及高品質的資訊作業環境下，資訊安全防護的要求重點。因此，前者的指標主要是以「人員專業能力」為主(包括：網路封包分析、電腦鑑識操作及誘捕系統操作等3項能力)，「資訊安全設備」為輔(包括：資訊安全設備及網路安全設備等2項設備建置)；而後者的指標以「資訊安全設備」為主(包括：備份備援系統、傳輸保密裝備、門禁安全設施、資安系統及網路基礎設施等5項設備建置)，「人員專業能力」為輔(包括：網路安全管理能量、系統操作能力及內部訓練制度等3項能力)。雖然林志章(2015)與吳世璋(2016)兩研究對「人員專業能力」與「資訊安全設備」強調的優序不同，惟此兩類指標在建置網路資料中心時，皆為必須強調的基礎項目。

另一方面，在雲端資料中心資訊安全機制的分類上，8項機制可區分為「資訊安全設備」(包括：入侵偵測防禦系統、惡意活動偵測、防毒控管及主機防毒、主機及網站弱點掃瞄、作業系統安全修正檔更新通知等5項)及「資訊安全管理」(包括：惡意黑名單阻擋、服務監控及告警、不同用戶虛擬主機安全隔離等3項)等2類。再與林志章(2015)與吳世璋(2016)兩研究做比較，雲端資料中心資訊安全機制並不強調「人員專業能力」的指標，而強調「資訊安全管理」的能力。究其原因，筆者認為一般政府機關(尤其是民間企業)在建置資料中心時，招聘之人員應已具備一定之資訊安全專業能力，與國軍各單位

常以「先用後訓」方式，透過在職訓練培訓合格作業人員之方式有所不同；另雲端資料中心強調資訊安全管理能力，應與雲端資料中心必須提供使用者隨需自助服務、多元網路存取、多人共享資源池、快速且彈性部署及服務可量測等服務有關連，因為這些服務必須依靠作業人員運用其對資料中心的資訊安全與設備管理能力來達成。

值此國軍逐步推動雲端服務，亦將建置雲端資料中心，為建構具備資訊安全要求的雲端資料中心，筆者基於前述之探討，就「資訊安全設備」、「人員專業能力」及「資訊安全管理」3個面向的關鍵因子提出建議如下：

一、「資訊安全設備」面向

(一)完善資安防護設備：國軍建置之雲端資料中心，依其服務對象，係建置於與網際網路實體隔離之軍網，實體隔離雖能隔離來自網際網路之威脅，然而，網際網路上的惡意程式仍可能透過資料交換而進入軍網，造成對雲端資料中心的危害。因此，資訊安全防護設備的建置仍是防護作為之基礎。現階段，各單位於營區網路對外閘口均會裝設網路防火牆、入侵偵測與防禦系統，也透過目錄服務派送作業系統修補程式及防毒軟體病毒碼更新檔；未來，在建置雲端資料中心過程中，應逐步將現有的資安防護觀念與設備部署策略，轉化為符合雲端服務的架構，也就是「雲端資安」，例如：在網路主幹檢查及過濾惡意封包，提升應變制變之時效，並降低使用單位(人員)遭入侵之風險；將現有防毒機制調整為雲端防毒架構，提升防範電腦病毒之時效，並降低使用單位(人員)管理負荷。

(二)提升資料加密機制：軍事資料儲存與傳輸首重保密，故資料加密演算法及傳輸保密設備的建置均為建置雲端資料中心時，必須納入考量的項目。現階段，軍網個人電腦所採用的檔案加解密軟體為中科院研發之「FileSecure V1.200」，雖專屬於軍網內部使用，惟面對未來更多可能的資安威脅，加上推動雲端服務後，資料的儲存安全將有更高的要求標準，故在建構雲端資料中心的同時，檔案加解密軟體必須與時俱進，確保其密碼演算法安全強度足以對抗惡意的破解行為。此外，在雲端服務架構下，雲(雲端資料中心)與端(使用者)間的資料傳輸頻次將更高，故資料傳輸的加密措施尤應建置，以提升傳輸安全，防範竊聽與封包側錄；目前，網際網路安全資料傳輸的方法首推TLS(Transport Layer Security)協定，未來，可運用現有國軍電子憑證的機制，核發TLS憑證，使軍網內各端點與雲端資料中心間可建立資料傳輸的加密通道，確保傳輸安全。

(三)妥採備份備援措施：備份與備援系統(機制)的妥當設計，是實現資訊服務持續不中斷之基礎，也是資訊機房營運不

可忽略的項目。現階段，各單位的業務資料儲存與資訊伺服器設備，及其資料備份與系統備援，主要是建置於單位內部，囿於人力與成本，鮮少有設置於異地之能力；未來，在國防部及各軍種分別設置雲端資料中心或軍種資料中心後，應利用雲端架構的優勢，實現跨單位、跨軍種及跨地域之資料備份與系統備援作為，以提高平時資訊服務的可靠度，並確保作戰時資訊系統的高存活率，有效支援作戰任務。

(四)嚴密實體安全管控：實體安全方面，雲端資料中心必須有效防護外來的威脅，故門禁安全設施，包含警衛派遣、警監設備、以及資料中心出入口門禁管制，均應相互搭配與規劃設計，確保實體設備的安全性。目前，各單位資訊機房主要採用傳統的識別工具，做為人員進出之身分辨識與管制手段，如：磁卡、無線射頻識別(Radio Frequency Identification, RFID)，其冒用與偽造風險較高；未來，因應雲端資料中心較高的安全性要求，可規劃導入生物特徵識別機制，如：指紋、虹膜，以精確識別進出人員身分。

二、「人員專業能力」面向

(一)遴選符資專業人員：人員素質是雲端資料中心運作良窳之關鍵，惟符資專業人員之獲得並非易事，學校教育主要在培養基礎學能，而維運資料中心的經驗，尤其是網路管理及系統管理能力，則必須在基礎學能上，持續的累積實務方能有所成，故如何遴選及留住此等人員，是建構雲端資料中心時必須思考的。現階段，國軍資訊人員的進、訓、用、退，其監管不如其他兵科嚴密，亦無明確的人才交流機制，故人員在軍旅發展上時有受限之情事，也間接導致人才流失。未來，在建置與維運雲端資料中心時，主責單位同時要考量人員之獲得與培育管道，建立人才資料庫並做有效之經管，使符資人員能長留久用。

(二)培訓人員進階職能：由於資訊科技進展快速，持續提升人員專業職能，是確保維運雲端資料中心能力可時俱進之關鍵。過往，各單位分別以其有限的訓練資源，規劃所屬人員的持續訓練課程，或以學校教育方式，使人員獲取更高的學歷(資)，未來，應以營運雲端資料中心所需之能力為依據，並以符資專業人員為對象，區分「機房管理」及「資安管理」兩個維度，整體規劃持續訓練課程，逐步提升人員的進階職能，而在其接受深造教育時，亦應結合理論與實務，課予研究課題，俾能學以致用。

三、「資訊安全管理」面向

(一)落實資安威脅修補：資安管理作為的落實，也是確保雲端資料中心運作順遂之基礎，尤其是各端點執行狀況若不落實，將成為整體系統中最弱的一環。目前，舉凡惡意網站黑名單的阻擋、各種系統修補程式及防毒系統病毒碼的派送，均有

律定相關機制，也應按標準作業程序及規定執行，惟各單位資訊人員在執行這些作業後，其上級單位並無確切的稽核機制，可確保及時依規定完成，將導致用戶端的資安組態不一致，從而肇生漏洞；未來，應配合雲端服務的架構與資源，設計端點資安防護的稽核機制，確保整體防護作為的完整性。

(二)維護資料存取安全：由於雲端資料中心係提供各軍種(單位)使用，故有關資料存取的安全性必須妥慎規劃，包括虛擬主機服務對象的律定、資料存取符合使用者權限及資料庫儲存內容的管理，也應涵蓋軍網與民網資料交換的管理。在過往各自建置資訊機房及虛擬化程度不高的年代，較無此等安全議題。未來，在建置雲端資料中心及高度虛擬化的狀態下，尤應透過明確的政策制定，輔以適切的權限管控，維護資料存取的安全。

結　　語

本文旨在探討國軍雲端資料中心構建時，有關資訊安全防護必須考量的因子。經過比較林志章(2015)及吳世璋(2016)對資訊安全防護能力指標的研究，再參酌政府部門對雲端資料中心所提供的資訊安全機制，初步擬定國軍雲端資料中心的資安防護作為必須以「資訊安全設備」、「人員專業能力」及「資訊安全管理」3個面向為主軸，透過落實執行各主軸下必須執行的工作，以確保雲端資料中心在運作時能安全無虞。此外，國軍整體的網路架構與品質，亦應依據雲端服務之需求適時檢討調整與提升，畢竟穩定與明確的網路架構是資訊安全管理之基礎，也是確保「雲」(雲端資料中心)與「端」(使用者)之間能順暢連結，使用者能獲取雲端服務之根基。

國軍各層級資訊部門在歷經多次組織精簡後，人力已大幅裁減，為能提供穩定且可靠的資訊服務，將有限的資訊資源往上收攏，並以現有網路資料中心為基礎，構建未來的雲端資料中心，將成為必然之趨勢。另由於資訊安全的威脅日趨嚴峻，國軍的資訊服務雖然主要建構在實體隔離的軍網，但並不代表就完全能隔絕來自網際網路的威脅，必須有嚴密的管理機制方能達成。本文依據既有的文獻資料，初步提出國軍在建構雲端資料中心時，資訊安全防護的重要考量因子，包括「完善資安防護設備」、「提升資料加密機制」、「妥採備份備援措施」、「嚴密實體安全管控」、「遴選符資專業人員」、「培訓人員進階職能」、「落實資安威脅修補」及「維護資料存取安全」8項，可提供主責之資通訊部門擬定政策與規劃實務作為的參考，亦可做為未來進一步發展細部控制目標與控制措施之基礎。