

端點安全對企業採用桌面虛擬化技術的影響

應用 ISO 27001 與決策理論觀點

為例

李仁鐘¹ ²周維明

華梵大學資訊管理系 johnlee@hfu.edu.tw

華梵大學資訊管理系 chou5431@gmail.com

摘要

雲端運算的資源共享、彈性運用，快速佈署、集中管理等優勢，提供企業高可用性的資訊服務環境，當企業評估或導入雲端運算技術時，資訊安全上的風險同時也必需作好風險評估的管理，經相關文獻發現，探討雲端運算之研究多以基礎架構與商業服務為主，但探討雲端端點安全的領域較少，本研究以 ISO27001 所規範之安全控制措施為標準，提供企業採用桌面虛擬化技術的評估方向為目標，成立 3 組導向推論。

本研究以問卷調查法進行研究，經回收 208 份有效問卷進行分析，經驗證後本研究之信度與效度皆符合檢定標準，並以回歸分析法檢定其結果，經證明本研究所推導之 3 組導向推論均成立，即端點安全控制措施管理導向、端點安全控制措施操作導向、以及端點安全控制措施技術導向均對企業採用桌面虛擬化有正向顯著的影響，並提出相關管理意涵，以協助未來企業在採用桌面虛擬化決策之參考。

關鍵詞：ISO27001、雲端運算、桌面虛擬化

The Effects of Cloud Security on Enterprises to Adopt Desktop Virtualization Technology Applying the Standard of ISO 2700 and Organizational decision-making theory

Wei-Ming Chou¹ Zne-Jung Lee²

Department of Information Management, Hua Fan University

Correspondence: Wei-Ming Chou, (chou5431@gmail.com)

Abstract

The Study is according to Standard of ISO 27001 , this study examined the effect of cloud Security on enterprises to adopt desktop virtualization technology and based survey Internet survey method with the focus on company and Government units was adopted for data collection and 208 valid questionnaires were obtained. The data analysis shows that Information Security were the most powerful variable, according for almost 71% of the variance, and adopters' characteristics explains less than 1% of the variance. Of the 3 variables Oriented of Management、Action、Technology were significant predictors in adoption desktop virtualization. More detailed findings were discussed in the paper.

Keyword: ISO 27001、Cloud Computing、Desktop Virtualization

1. 緒論

經主計處調查顯示，99 年度全國個人電腦使用普及率為 73.34%，較 98 年底略增，其中政府行政機關、公營事業機構、公立學校、公立研究機構等均為 100.00%，民間企業為 73.01%，顯示一般辦公室自動化環境仍以使用桌上型個人電腦為大宗。在企業服務愈來愈依靠資訊系統的今日，傳統的個人電腦管理已面臨各種軟體上、硬體上以及人為使用不當的挑戰，為降低風險、提升競爭力，與落實法規的依循，無論政府單位或民間企業紛紛規劃及導入資訊安全管理系統(Information Security Management System, ISMS)，以政府單位為例，經本研究調查有 61.9%機構導入 ISMS，而其中又有 50.9%的機構已通過 ISMS(ISO27001)驗證(主計處 99)，顯示政府已逐步要求所屬單位建置 ISMS 系統，落實資安政策。

以虛擬化技術為基礎的雲端運算架構已逐漸成熟，並應用於各領域，而雲端運算的資安風險議題，也成為企業導入時評估的重點，而雲端服務供應商所發展的桌面虛擬化技術，以提供個人電腦資訊安全環境為說帖，受到多數企業的持續關注。經本研究蒐集發現，在眾多雲端相關的研究中，較少探討桌面虛擬化技術應用於資訊安全相關領域之議題，因此本研究以 ISO27001 標準之安全控制措施為研究動機，探討私有雲下的端點電腦設備安全控制措施對於企業採用桌面虛擬化技術的影響，為本研究的目的，以作為政府或企業各單位在建立私有雲，提升整體營運效益的參考。

2. 文獻探討

2.1 ISO 27001

ISO 27001 標準為提供一項建立、實施、操作、監控、審查、維護及改進資訊安全管理系統(Information Security Management System,ISMS)之模式，並採用“規劃—執行—檢查—行動(Plan-Do-Check-Act,PDCA)”過程模型，根基於戴明(Deming)品質循環，適用於建置所有 ISMS 過程。係依資訊安全要求與相關者期望為輸入，經由各必要之行動過程，產生符合要求與期望的資訊安全輸出的結果(經濟部標檢局，95)。

前身為英國標準協會 (BSI) 於1995年所訂定「BS 7799-1：1999」之國家標準，並提交國際標準組織進行微幅修改，國際標準組織於2000年審議成為ISO/IEC 17799國際標準，2005年6月15日ISO/IEC 17799:2005正式發行，之後由ISO/IEC 27002取代，而根基於ISO/IEC 17799:2005與BS 7799-2:1999之ISO/IEC 27001:2005於2005年10月15日正式發行，成為ISO/IEC 27000資訊服務管理系列標準之第一份標準。提供組織資訊安全管理系統建立、實施和維護具體要求，包含11個章節(Clauses)、39項控制目標(Control objectives)、133個控制措施(Control controls) (經濟部標檢局，95)

2.2 雲端運算(Cloud Computing)

雲端運算技術，並非是一個嶄新的技術，而是一種虛擬的空間概念，這個概念是由美國國家標準與技術研究所 (National Institute of Standards and Technology, NIST) 所定義規範出來(韓善民，2001);(Steve et al,2009)。依據美國國家標準和技術協會(National Institute of Standards and Technology, NIST)第 15 版的定義，認為雲端運算是一種能透夠

透過無所不在的網路，以便利且隨選所需(On Demand) 的方式存取共享式運算資源(如網路、伺服器、儲存設備、應用程式、服務)的運作模式，並以最小的管理成本進行快速配置與發佈運算資源(Mell & Grance, 2009)。

雲端運算的主要運用方式，係結合運用龐大電腦科技的運算技術，新研發出一種網路互動模式，這種網路互動的模式，也促使各IT (Information Technology) 業者，提供多樣的雲端服務平台(Michael, 2009)。因此可以從系統平台與應用服務兩個角度來解釋雲端運算，從系統面來看，雲端運算系統為可以依需求動態新增(Provision)、安裝、設定與移除伺服器的一種平台。雲端運算架構也能包含伺服器提供環境所需的其它計算資源，如：網路儲存群(SANs)、防火牆與其它網路設備等。從應用服務的角度來解釋，雲端應用服務代表利用大量的資料中心(Data Center)與強大的伺服器群來提供服務，並可直接透過網際網路連接，任何使用者只要有適當的連線能力與瀏覽器即可取得服務(Boss, Malladi et al. 2007)。

根據 Gartner 研究機構的研究，指出雲端運算代表商業模式的革新，影響到電子商務的發展，而各種對於『雲端運算』這個名詞的矛盾與混淆，代表它改變 IT 市場現狀的潛力。Gartner 將雲端運算定義為一種運算的模式，包含可大量擴充IT 提供相關的技術能力，利用網際網路的相關技術，包裝成一種服務來提供(as a service)給多個外在使用者(Stamford 2008)。

經相關文獻探討，本研究有關雲端運算之優點整理如下：(1) 可以降低企業的營運成本；(2) 可以提升企業的專職技術；(3) 可以達到節能的環保概念；(4) 可以彈性擴充的資源環境；(5) 可以縮短系統的建置時間；(6) 可以彈性調節的系統配置；(7) 可以整合應用的平台資源；(8) 可以作為平台的溝通橋樑(張益豐等，2009);(Foster et al,2008)；缺點包括：(1) 網路頻寬速率大小，造成網路存取速度的快慢；(2) 檔案資源共享機制，隱藏資料外洩防護的安全；(3) 硬體設備供應廠商，受限架構的差異，對雲端用戶會有不同的限制(江政哲等，2010)。

雲端運算的流行，引發許多學者對於其安全性的質疑，這些批評都可能成為推廣雲端運算架構上的阻力，以下整理目前各學者對於雲端運算在資安上的質疑：(Heiser and Nicolett 2008; Mansfield-Devine 2008; Stallman 2008) 當使用者利用網際網路存取雲端服務，傳統網路釣魚、DoS(Denial of Service)攻擊與跨站腳本攻擊(XSS)等常見的網路資安問題，都可能造成使用者遭受攻擊，並受到損失。尤其雲端服務常以網頁服務的形式出現，更容易成為駭客攻擊的目標，相較以往封閉式的環境而言，需承擔較高的風險。

依據雲端安全防護聯盟 (Cloud Security Alliance, CSA) 提出，雲端運算服務，可能會遭遇到七大資訊安全的問題，敘述如下：(1) 不法人士使用雲端運算技術，從事不法的資源服務；(2) 使用者操作介面與雲端運算服務，具有資訊安全的隱憂；(3) 企業內

部有心人士，不法取得雲端客戶的資源內容；(4) 雲端資料在共享的時候，可能造成資源分享錯誤或干擾的情形；(5) 當資料全部集中在雲端資源平台上時，可能導致資料外洩的問題；(6) 雲端客戶的帳號與密碼認證資料，被有心人士竄改或使用；(7) 未來可能發生的潛在風險問題(張念慈、彭秀琴，2010)等。

2.3 桌面虛擬化(Desktop Virtualization)

桌面虛擬化是虛擬化技術的一種，虛擬化是一種將電腦資源抽象的方法，透過這種方法，可以不受現實、地理位置或底層資源實體組態的限制，進而隱藏屬性和操作間的差異，讓使用者透過一種通用的方式來查看並維護資源。

桌面虛擬化是一種基於服務器的計算模型，並且借用了傳統的瘦客戶端 (Thin Client) 的模型，讓管理者與使用者能夠同時獲得兩種方式的優點：將所有桌面虛擬機在數據中心進行託管並統一管理；同時使用能夠獲得完整 PC 的使用體驗(維基百科)，經本研究整理，桌面虛擬化的分類與效益如表一與表二：

表一、桌面虛擬化分類

種類	技術	特性	產品
個人用	安裝在電腦原生的作業系統 (Host OS) 上，並建立相對應的虛擬磁碟檔案，以便建立虛擬機器 (VM)，進而安裝虛擬作業系統 (Guest OS)。利用 Hypervisor 來模擬處理器、硬碟、網路卡和顯示卡等元件，並透過這個中介層的轉換機制存取實體的硬體資源。	<ul style="list-style-type: none"> ● 架構簡單，較適合小規模部署。 ● 提供異質平臺與軟體測試的能力。 ● 對電腦的硬體規格要求較高，其中又以能支援 AMD-V 或 Intel VT 虛擬化技術的處理器效果較佳。 	Virtual PC Citrix XenClient VMware Workstation
企業級	集中式虛擬化桌面架構 (Virtual Desktop Infrastructure, VDI)		
	與常見的 Terminal Services 類似，將存放在伺服器端的虛擬機器畫面，利用遠端桌面協定傳送到前端的使用者電腦上，僅傳送虛擬機器的電腦畫面，以及個人端電腦的鍵盤、滑鼠等操作指令，因此頻寬的需要較少，對前端平臺的硬體等級要求也很低，適用精簡型電腦。	<ul style="list-style-type: none"> ● 初期建置成本較低。 ● 能重複利用相同的檔案內容 (例如作業系統)，僅需儲存個人化後的差異性資料，就可以同時傳送多個不同畫面至使用者電腦。 	微軟的遠端桌面服務 (Remote Desktop Services, RDS) Citrix XenDesktop VMware View

種類	技術	特性	產品
企業級	分散式虛擬化桌面架構(VDI)		
	前端平臺必須是具有儲存能力的個人電腦，並在使用伺服器派送虛擬機器給使用者操作時，該環境也一併保有原生的作業系統。	<ul style="list-style-type: none"> ●使用個人電腦的運算資源，因此可降低伺服器負擔。 ●初期必須先將所有的虛擬機器映像檔，逐一派送到使用者電腦中，因此部署時較需求網路頻寬。 ●集中化管理便於部署、修正、派送，或是升級虛擬機器映像檔。 ●可以變更使用者權限及安全性設定。 ●藉由集中儲存的映像檔，快速回復損毀的系統。 	微軟 MED-V (Microsoft Enterprise Desktop Virtualization) RHEV (Red Hat Enterprise Virtualization) VMware View

資料來源：iThome

表二：桌面虛擬化的效益

效益	說明
減少管理複雜性	企業級的桌面虛擬化解決方案採用集中式架構，前端使用者的作業系統、應用程式，以及個人設定檔等資料，統一儲存在資料中心 (Data Center) 的伺服器或儲存設備中，管理者可完全掌握使用者電腦的狀態，依實際需求製作各電腦的影像檔，配合網路傳送，提供端點個人電腦一致的服務，簡少實體電腦軟、硬體環境與使用者間依存度，增加資產管理的彈性。
解決應用程式相容性問題	面對作業系統不斷改版、升級，以及產品生命週期結束的挑戰，企業在導入新作業系統，或考慮延用舊系統時，必須解決的相容性問題。

效益	說明
強化資料安全	強制使用者將檔案存放在後端伺服器或儲存設備中，以防止有心人士複製或散布檔案。此外也可以透過虛擬機器的管理介面，來限制 USB 隨身碟或光碟機等周邊儲存裝置的使用原則。
延長設備使用壽命	桌面虛擬化對於前端使用者電腦的硬體規格要求較低，可以讓這些設備用更久。對於將運算資源集中在伺服器上的解決方案來說，精簡型電腦已經足以負擔顯示畫面和輸出入等基本操作需求，如果企業選擇保留舊有的桌上型電腦，也可以不買精簡型電腦，用現在的電腦直接做為前端使用平台。
維持系統持續運作	由於應用程式的資料檔案是獨立存放，和虛擬化服務使用的作業系統檔案、使用者個人電腦之間，可以完全切割，因此即使伺服器或個人電腦故障，只要用備援的伺服器來掛載資料檔，或是更換一臺新電腦，就可以讓使用者以原本的設定繼續工作。當然，資料集中化後，IT 人員要更能掌握伺服器及儲存設備的健康狀態，問題時，只要先排除硬體故障，就能利用這些映像檔來恢復正常資料，大幅減少維修時間並考慮建置備援機制。

資料來源：iThome

2.4 組織決策理論

2.4.1 組織決策行為

在眾多的研究中，組織決策的研究發現，在面對不確定性的決策情境時，組織決策會出現不同的決策階段中有不同的決策過程，例如前進、後退、跳越與重複的漸進式過程(Mintzberg et al., 1976)。組織決策，常需要在解決方案不清楚、行動可能結果也不明確的模糊情況下進行(Cyert et al,1956)，組織內的決策與社會互動關係，例如組織決策影響力、衝突與組織政治行為因素，都是成為組織決策的重要影響因素(Laudon and Loaudon 1998)。

組織決策行為模式，會因為組織對於決策議題的了解程度的差異，而有不同的結果(Nutt,1984)，(Hickson et al,1989)對於 150 個策略決策案例所進行的分析發現，決策者對於決策議題重要的認知程度，會影響組織的決策行為，並透過研究指出，組織內對於決策參與的程度，會因為企業不同的決策議題，有非常明顯的差異，因此可能在某些專業性的議題，會由特定的部門所組導，例如本研究針對虛擬化桌面的採用議題，就應由 IT 部門進行主導，因此在某些議題上，必須要透過政治互動過程或決策影響力的行使來進行。

以企業資訊安全控管的角度，乃至 ISO27001 標準的規範，資訊安全是不斷的推陳出新(Larsen,1999)，因此企業對資訊安全的風險評估，可能會受到決策者認知偏誤的影

響而有所不同，在缺乏明確資訊安全風險數據的情況下，風險管理決策模式在資訊安全控管決策上的適用性，可能會受到阻礙(Huber,1980)。

2.4.2 高階主管決策涉入的應響

高階主管的決策涉入程度，是指高階主管對於特定組織決策議題的態度及參與情形(Jarvenpaa and Ives, 1991)。由於組織結構是組織正式決策影響力的主要來源，高階主管代表了組織實質及與行事的權威。在組織決策的過程中，高階主管的決策影響力，遠高於其他的決策者(Pfeffer,1992)。取得高階主管對於特定決策議題的支持，是決策議題獲得組織正當性與資源投入承諾的重要關鍵(Dutton,1986)。

企業的資訊資源控管決策，可能會引發使用者部門及資訊部門立場的衝突(Cash et al,1992)，並且當企業內不同的部門對於決策的必要性及可行手段看法不同時，高階主管的涉入，有助於衝突的化解。如果高階主管態度不明，則可能激化組織衝突，使組織決策過程成為政治運作的戰場(Neilson,1972)。因此在短期而言高階主管的介入，是恢復組織程序的有效方法，但是，如果組織衝突的根源無法解決，則衝突仍將再起(Pondy,1968)。

從企業資訊安全控管決策的研究得知，高階主管對於企業資訊安全漏洞的態度，會對企業的資訊安全控管決策，產生重大的影響(Hoffer and Straub,1989)。由於不確定性，如果高階主管缺乏對資訊安全風險的遠見，則企業可能連資訊安全機制都無法運作(Straub and Welke, 1998)。因此從本研究的觀點來看，企業導入桌面虛擬化的因素，在高階主管高度的風險意識、積極的支持與涉入，有助於提高企業的資訊安全控管程度，保障資訊安全，因此在採用桌面虛擬化的過程中，對資訊安全的保障與控管程度越高，對於高階主管的採用意願就會越高，因此在端點安全的管理導向、操作與技術導向來思考虛擬化桌面的採用，其高階主管涉入程度越高，對企業採用意願也越高。

2.5 假設推導

從上述文獻探討可知，資訊安全的威脅是雲端運算應用重要的考量，因此企業在評估採用雲端運算應用時，安全性是影響企業是否採用的重要因素之一，雖然目前許多雲端運算服務供應商聲明已具備足夠的雲端運算資訊安全能力，然而企業採用雲端運算服務所面臨的資訊安全問題，會隨著企業採用的種類以及使用方式而有所不同。因此雲端運算服務供應商所提供的資訊安全等級是否能夠符合需求仍需經過企業自行評估才能確立，因此企業除了進行整體風險分析來確認相關資料與應用程式的重要性，以及可能發生的風險與衝擊，也必須對雲端服務進行整體性的風險評估。

本研究經相關文獻探討，發現雲端運算服務，在資訊安全考量有以下因素：資料的安全性(如：使用者存取管理、資料加密管理、資料傳輸管理、各用戶資料彼此間的隔

離、資料實際儲存位置)、雲端運算服務供應商法規遵循的可靠性(如：營運方式是否符合法規要求)、服務中斷時的回復能力(如：回復速度、回復程度)、對企業需求的支援能力(如：協助企業進行調查、雲端運算服務提供商之間的轉換)、永續經營(如：計劃中或意外導致的服務終止、終止服務後協助原用戶移轉服務的能力)。企業可搭配資訊安全等級的要求以及所處產業的相關法規，經延伸或修改上述項目以制定出符合該企業雲端資訊安全需求的風險評核表。在制定風險評核表時，企業必須清楚地了解採用雲端服務後工作流程的改變，發掘各環節可能發生的風險，以提高風險評核表的完整性與周延性(CSK, 2010)。

透過上述雲端安全聯盟的研究得知企業對於採用雲端運算，對於安全性整體評估是相當重要的，而 ISO27001 公認為最具權威的資訊安全技術管理標準，因此本研究採用 ISO 27001 標準，來探討資訊安全對企業採用桌面虛擬化技術的影響程度，本研究參考資策會 99 年度國家資通安全技術服務與防護管理委外服務案安全控制措施參考指引(V3.0)，以 ISO 27001 標準附錄 A 的 11 個章節(Clauses)為主分類，歸納個人電腦的安全控制措施如表三：

表三：個人電腦的安全控制措施

類別	主分類	描述
管理面	安全政策與程序	應訂定相關要點辦法以為遵循
	資訊安全的組織	內部與外部團體的使用與授權
	資訊系統獲取、開發及維護	電腦軟、硬體的規劃、建置、開發、驗收與維護的相關作業
	遵循性	應遵循政府相關法規或標準
操作面	資產管理	軟、硬體的資產清單 設備的管理與維護
	人力資源安全	使用者教育訓練
	實體與環境安全	實體設備的控管
	通訊與作業管理	資訊的完整性 媒體的管理
	資訊安全事故管理	資安事故的回報與分析
	營運持續管理	資料備份與回覆 服務不中斷
技術面	通訊與作業管理	系統與網路的防護
	存取控制	認證與鑑別 存取權限的控管 使用紀錄的稽核

資料來源：資策會

2.5.1 端點安全控制措施管理導向

透過表三文獻的探討可知，電腦設備安全控制措施類別之管理面而言，管理階層對資訊安全承諾的落實，對個人電腦使用者來說，可以增加對工作的信任度與共同維護資安的凝聚力；並作好對個人資料的保護，達到遵循政府法令的要求，降低個資外洩所導致的風險，因此本研究針對端點安全控制措施管理導向有以下推論，如表四：

表四：端點安全控制措施管理導向推論

H1	端點安全控制措施管理導向對桌面虛擬化採用有正向顯著的影響
	H1-1 個人電腦安全承諾越落實對桌面虛擬化採用的採用有正向顯著的影響
	H1-2 個人資料保護管控措施越好對桌面虛擬化採用的採用有正向顯著的影響

2.5.2 端點安全控制措施操作導向

端點電腦設備安全控制措施類別之操作面而言，個人電腦營運持續目標的達成，有助於維持企業整體的運作，達到服務不中斷的目標；而個人電腦的更新與移轉是企業發展經常面臨的問題，所花費的人力與時間的成本，應有效降低以避免影響日常作業之運行，因此本研究針對端點安全控制措施操作導向有以下推論，如表五：

表五：端點安全控制措施操作導向推論

H2	端點安全控制措施操作導向對桌面虛擬化採用有正向顯著的影響
	H2-1 個人電腦持續運作的目的越有保障對桌面虛擬化的採用有正向顯著的影響
	H2-2 個人電腦的更新與轉移越容易對桌面虛擬化的採用有正向顯著的影響

2.5.3 端點安全控制措施技術導向

就端點電腦設備安全控制措施類別之技術面而言，個人電腦應用軟體以及相關作業系統漏洞修補等測試作業，應與正常運作環境有所區隔，以免影響或發生風險；而USB等可攜式媒體，已成為個人電腦資料外洩或中毒的最大風險之一；對於使用者身份權限的管理，一直是傳統個人電腦的弱點，以符合工作內容的最小權限控管(Least Private)可以有效降低資安風險；依據ISMS作業運作模式，需定期施作個人電腦的稽核作業，透過桌面虛擬化集中控管的機制可有效執行，因此本研究針對端點安全控制措施技術導向有以下推論，如表六：

表六：端點安全控制措施技術導向推論

H3	端點安全控制措施技術導向對桌面虛擬化採用有正向顯著的影響
	H3-1 應用軟體安全的測試環境越好對桌面虛擬化的採用有正向顯著的影響
	H3-2 可移除式媒體的管控越好對桌面虛擬化的採用有正向顯著的影響

H3-3 使用者存取權限管理越簡化對桌面虛擬化的採用有正向顯著的影響
H3-4 電腦設備使用記錄之稽核越容易對桌面虛擬化的採用有正向顯著的影響

3. 研究方法

3.1 研究架構

本研究依據 ISO27001 標準，建立研究假說，並發展三個研究假設，來探討私有雲下的端點安全對於企業採用桌面虛擬化的影響，研究架構如圖 1 所示：

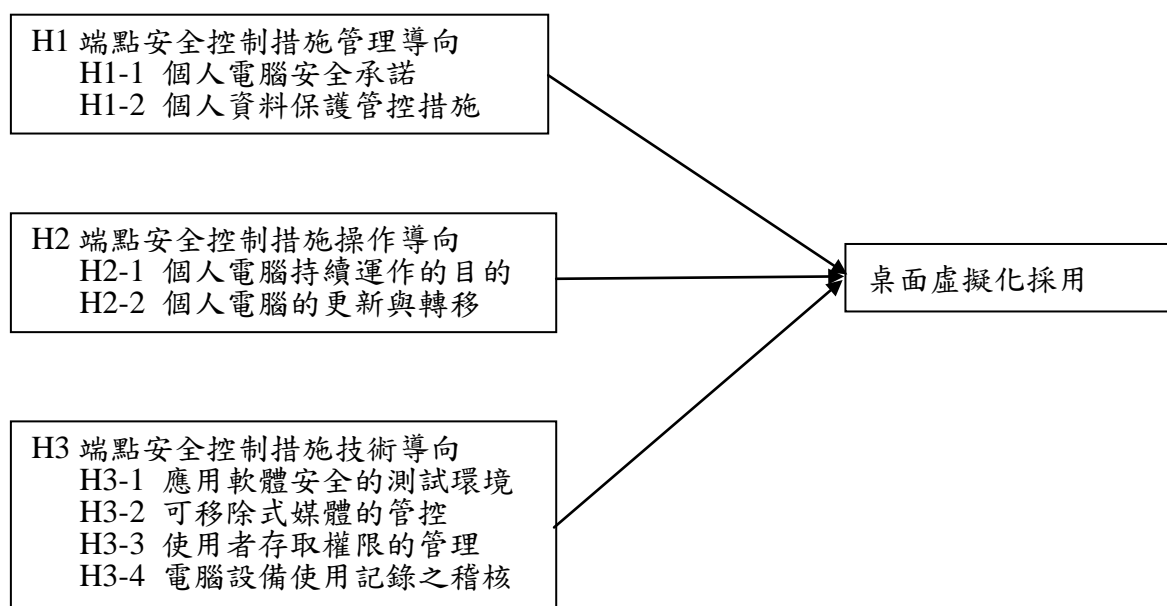


圖 1 研究架構

3.2 研究變數的操作型定義與問卷設計

本研究採用問卷調查法研究方式進行，並依據蒐集相關 ISO 27001 標準及文獻資料進行問卷的設計，以了解本研究假設推導之研究架構，(1) 端點安全控制措施管理導向對企業採用桌面虛擬化有正向之影響，(2) 端點安全控制措施操作導向對企業採用桌面虛擬化有正向之影響，(3) 端點安全控制措施技術導向對企業採用桌面虛擬化有正向之影響。先發展初期問卷並透過相關文獻探討，涵蓋個人變數之問題，分為管理面、操作面以及技術面 3 組分類，合計 28 題，並使用 Likert 五點尺度量表衡量，依同意的程度來衡量問項之關聯程度，從“非常不同意”至“非常同意”轉換為 1 分至 5 分，平均分數愈高者，代表關聯愈大，獲得多數受訪者的認同，並針對問題不清與合適性不良的問題進行刪改，再進行正式的問卷發放。

4. 結果與分析

4.1 樣本資料描述

本研究共針對政府機關、學校、資訊業、金融業發放網路問卷，共發放了 251 份問卷，經扣除部分問卷填答答案皆為同一選項之問卷及問項漏答之無效問卷計 43 份後，有效問卷合計 208 份，有效回收率為 82.8%，由於本研究樣本數取得不易，符合填答內

容之公司或人員又太過於嚴苛，因此問卷回收有相當的困難。在 208 份的問卷中，以資訊業之填答者為最多，佔問卷回收總數 32.7%，而服務單位人數 10~50 人的單位佔問卷回收總數的 31.3%；另外在工作性質的部分，以系統操作與維護者居多，佔本問卷總回收數的 36.1%；因此本研究之問卷發放對象以資訊領域相關為主，如表七。

表七：個人變數資料彙整

特徵項目	項目	數量	百分比
您的性別	男	122	58.7%
	女	86	41.3%
您的工作性質	資訊主管	31	14.9%
	資訊安全管理	38	18.3%
	系統操作與維護	75	36.1%
	程式撰寫 與開發	32	15.4%
	其他	32	15.4%
您從事資訊相關工作年資	1~3 年	19	9.1%
	3~5 年	50	24.0%
	5~10 年	83	39.9%
	10 年以上	56	26.9%
您服務單位的行業別	政府機關	38	18.3%
	學校	26	12.5%
	資訊業	68	32.7%
	金融業	10	4.8%
	其他	66	31.7%
您服務單位職員或學生人數	10~50 人	65	31.3%
	51~100 人	40	19.2%
	101~200 人	37	17.8%
	201~500 人	37	17.8%
	501 人以上	29	13.9%
單位年度資訊經費	100 萬以內	57	27.4%
	100~500 萬	45	21.6%
	500~1000 萬	55	26.4%
	1000~5000 萬	46	22.1%
	5000 萬以上	5	2.4%
單位導入 ISMS 現況	已導入	96	46.2%
	已規劃導入或建置中	68	32.7%
	未導入、未規劃	44	21.2%

單位導入 ISMS 的範圍	全單位	42	20.2%
	資訊中心	48	23.1%
	電腦機房	48	23.1%
	其他	70	33.7%
是否通過 ISO 27001 標準之驗證	是	64	30.8%
	否	144	69.2%
特徵項目	項目	數量	百分比
單位導入虛擬化技術現況	已導入	91	43.8%
	已規劃導入或建置中	85	40.9%
	未導入、未規劃	32	15.4%
導入(或欲導入)之虛擬化技術	基礎架構虛擬化 (例：網路、儲存設備)	32	15.4%
	系統虛擬化 (例：伺服器主機、桌面)	84	40.4%
	軟體虛擬化 (例：應用程式、高階語言)	3	1.4%
	其他 (含 2 種以上虛擬化技術結 合運用)	89	42.8%

資料來源：本研究整理

4.2 信度與效度分析

本研究問卷問項蒐集係依據 ISO 27001 標準，以及相關文獻發展而來，以 Likert 五點尺度量表設計出 28 題問項，本研究各構面之衡量結果與題項信度都達到了 α 值 0.7。另為探測本研究各構面的凝聚性，進行因素分析，經驗證整體信度係數(Reliability Coefficients),Cronbach Alpha(a)值均大於 0.7，且所有題項特徵值皆大於 1，顯示本問卷在同一衡量構面問項，具有內部一致性的可靠度。

本研究為使問卷量表與衡量工具能達到本研究目的，研究範圍與研究內容達到本研究衡量效度，量表發展過程中透過文獻探討，本研究前測 20 份問卷的結果，提高本研究之內容效度，各建構之單一構面信度 Cronbach α 係數皆大於 0.7，各個構面衡量題項之因素負荷量觀察值皆大於 0.5，可解釋之累積百分比皆大於 60% 以上，因此可探知衡量的效度情形良好，可推論本研究之結果與量表問項與理論邏輯有一致性相關程度的佐證。

4.3 研究假說檢定

本研究採用 Pearson 積差相關分析(Pearson Product-moment Correlation)來初步驗證假說。表八為各變數之相關係數，「端點安全控制措施管理導向」、「端點安全控制措施

操作導向」、「端點安全控制措施技術導向」與「桌面虛擬化技術的採用」間均存在顯著的正相關，因此符合本研究相關架設依據。

表八：端點安全控制措施管理導向、端點安全控制措施操作導向、端點安全控制措施技術導向與桌面虛擬化採用之相關分析

相關分析	端點安全控制措施管理導向	端點安全控制措施操作導向	端點安全控制措施技術導向	桌面虛擬化採用
端點安全控制措施管理導向	1			
端點安全控制措施操作導向	.771**	1		
端點安全控制措施技術導向	.663**	.681*	1	
桌面虛擬化採用	.210**	.211**	.440**	1

註：* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

本研究為求得變數間相互關聯的影響程度，使用簡單迴歸方法來具體判定影響程度，結果如表九至表十一所示。其中的杜克-華生氏值(Durbin-Watson, DW)，用來檢驗誤差項間是否存在線性相關，此值若接近 0，代表變數具有正向自我相關，若 DW 值接近 4 代表負向自我相關，若介於 1.5 到 2.5 間，即大略表示誤差項之間並無自我相關存在。由於本研究的 DW 值皆在 1.646~2.197 間，表示誤差項沒有存在線性相關。此外，自變數的允差(tolerance)與變異數膨脹值(variance-inflation factor, VIF)，可檢視變數間是否有共線性的問題，由於各迴歸模式之 VIF 值為 1.186~3.317 間，皆小於 5，且允差介於 0.302~0.843 間，皆大於 0.1，表示應可避免各變數間線性重合，故本研究之迴歸模式並沒有存在變數間線性重合的問題。

在表九迴歸式中，「端點安全控制措施之管理導向」、「個人電腦設備的安全承諾」、「個人資料保護的管控措施」皆對桌面虛擬化採用有顯著的影響，因此假說 H1 獲得支持，亦即端點安全控制措施之管理導向中的個人電腦設備的安全承諾、個人資料保護的管控措施，均會顯著正向影響企業對於桌面虛擬化技術的採用。

表九：端點安全控制措施之管理導向對桌面虛擬化採用之迴歸分析

依變數	自變數	迴歸係數	標準差	T 值	顯著性	R ²	F 值	DW	共線性統計量	
									允差	VIF
桌面虛擬化採用	個人電腦設備的安全承諾	.540	.046	9.456	.000***	.716	84.000 (.000)	1.949	.640	1.563
	個人資料保護的管控措施	.284	.080	3.550	.016*				.448	2.233

註：*p<0.05, **p<0.01, ***p<0.001

在表十迴歸式中，「端點安全控制措施之操作導向」、「個人電腦設備持續運作的目的」、「個人電腦設備的更新與移轉」皆對桌面虛擬化採用有顯著的影響，因此假說 H2 獲得支持，亦即端點安全控制措施之操作導向中的個人電腦設備持續運作的目的、個人電腦設備的更新與移轉，均會顯著正向影響企業對於桌面虛擬化技術的採用。

表十：端點安全控制措施之操作導向對桌面虛擬化採用之迴歸分析

依變數	自變數	迴歸係數	標準差	T 值	顯著性	R ²	F 值	DW	共線性統計量	
									允差	VIF
桌面虛擬化採用	個人電腦設備持續運作的目的	.116	.138	8.069	.000***	.681	84.510 (.000)	1.646	.843	1.186
	個人電腦設備的更新與移轉	.215	.283	7.597	.000***				.448	2.233

註：*p<0.05, **p<0.01, ***p<0.001

在表十一迴歸式中，「端點安全控制措施之技術導向」、「應用軟體安全的測試環境」、「可移除式媒體的控管」、「病毒碼的更新與派送」、「電腦設備使用紀錄之稽核作業」全部顯著正向影響企業對於桌面虛擬化技術的採用，因此研究假說 H3 獲得支持。

表十一：端點安全控制措施之技術面對桌面虛擬化採用之迴歸分析

依變數	自變數	迴歸係數	標準差	T 值	顯著性	R ²	F 值	DW	共線性統計量	
									允差	VIF
桌面 虛 擬 化 採 用	應用軟體安全的測試環境	.364	.092	3.966	.000***	.552	17.331 (.000)	2.197	.312	3.207
	可移除式媒體的控	.392	.074	5.284	.000***				.302	3.317
	使用者存取權限的管理	.266	.117	2.268	.025*				.324	1.341
	電腦設備使用紀錄之稽核	.522	.134	3.907	.000***				.472	2.210

註：*p<0.05, **p<0.01, ***p<0.001

5. 研究結果分析與討論

5.1 端點安全控制措施之管理導向對企業採用桌面虛擬化之影響

根據本研究之實證研究，端點安全控制措施對企業採用桌面虛擬化之影響是正向的，在本研究實證調查結果，端點安全控制措施導向之「個人電腦設備的安全承諾」與「個人資料保護的管控措施」，對於企業採用桌面虛擬化，有以下影響性，本研究試分別分析與討論之，如下述：

(1)、在個人電腦安全承諾部分：

企業時常為提升企業競爭力與企業營運績效，時常需要透過提升資訊科技來協助企業未來的經營效率，隨著雲端運算技術的興起，已逐漸改變企業對資訊科

技的角度與應用，傳統上，企業員工時常因工作所需，因而對於資訊產品設備的更新有其特殊的要求，在多數企業因考量員工工作效率的問題，時常配給一般員工單一個人電腦的使用，但資訊科技與資料處理在正向的成長下，時常有硬體設施不敷使用的狀況，同時若辦公室遭竊，也容易導致企業機密資料外洩，造成企業難以估算的損失。

隨著資訊科技的進步，企業若採用桌面虛擬化技術，如何確保個人電腦使用的安全，並保障人員工作的順暢，是一大重要的挑戰，也是本研究在研究企業虛擬化採用時一個重要的研究目的，經本研究發現，桌面虛擬化技術在雲端之應用上，不但能夠多重備份，同時使用者可不受設備限制於各端點電腦使用熟悉之工作環境，降低單一設備故障或被竊的風險等，對於電腦安全承諾更有保障因此更有助於企業採用，故未來服務提供者或企業導入者在個人電腦安全承諾上，能滿足使用者安全保障，對桌面虛擬化之採用更為有助益，故經本研究實證結果，桌面虛擬化應用於個人電腦安全承諾越落實對桌面虛擬化技術的採用有正向顯著的影響。

(2)、在個人資料保護的管控措施部份：

我國在 2010 年公告個資法案，對於個人資料保護的重要性尤為的重要，企業最重視的亦是商業資料的保護，也是 ISO 27001 標準最重視的一環，隨著雲端運算應用日趨火熱，資訊安全資訊保護一直是企業在導入雲技術時一個相當重要的考量，也是一般企業不願意使用公有雲的主要因素之一，故企業轉往採用私有雲的方式來佈署雲端運算服務，因此也對桌面虛擬化之應用帶來了契機。

桌面虛擬化不但能夠使企業集中管理使用者環境，同時透過使用者權限的控管更能保障資訊的安全，因此在個人資料以及企業資料的保護上逐漸受到企業的親暱，經本研究實證結果調查，企業在採用桌面虛擬化技術的同時對於個人資料保護與管理將更有效益，有助於企業採用桌面虛擬化技術之意願，故經本研究實證結果，桌面虛擬化應用於個人資料保護管控措施越好對桌面虛擬化技術的採用有正向顯著的影響。

5.2 端點安全控制措施之操作導向對企業採用桌面虛擬化之影響

(1)、在個人電腦設備持續運作的目的部份：

美國 911 事件，日本 311 地震等各種天災人禍所導致的資訊系統服務中斷事件層出不窮，如何在事件發生後有效降低企業資訊服務中斷的損失，已成必要面對的課題，傳統端點電腦設備的備份與回覆機制，需要使用者的配合落實，缺乏統一的管理與稽核，往往事倍功半，當企業運用桌面虛擬化技術集中管理，統一儲存，以及快速佈署的優勢，可有效降低使用者備份作業不確實的風險，提供企業決策者制定營運持續計劃時有利的運作策略，故經本研究實證結果，桌面虛擬化應用於個人電腦持續運作的目的越有保障對桌面虛擬化技術的採用有正向顯著

的影響。

(2)、在個人電腦設備的更新與移轉部份：

因應科技的進步、業務發展、與人事調動等需求，企業所屬個人電腦設備經常面臨各種軟、硬體的採購、更新、升級與報廢等異動管理，當使用者因新舊軟體版本不相容以及新作業環境不熟悉等因素，往往產生抗拒與排斥心理，進而影響業務的運作，經應用桌面虛擬化的影像檔技術，可在新系統下建置並運行一套原有舊系統的模擬環境，因此提升新舊系統的相容性，有助於電腦設備的更新與移轉，經研究實證結果，桌面虛擬化應用於個人電腦設備的更新與移轉越容易對桌面虛擬化技術的採用有正向顯著的影響。

5.3 端點安全控制措施之技術面對企業採用桌面虛擬化之影響

根據本研究之實證研究，「應用軟體安全的測試環境」、「設備可移除式媒體之控管」、「病毒碼的更新與派送」、「電腦設備使用記錄之稽核作業」，對於桌面虛擬化技採用，有以下影響性，本研究試分別分析與討論之，如下述：

(1)、在應用軟體安全的測試環境部份：

企業因業務發展需求，時常需要針對不同的應用程式進行佈署與安裝，傳統上常因為軟體佈署錯誤或新系統不穩定，造成 IT 人員額外的工作負擔，透過桌面虛擬化技術模擬環境的特性，提供安全的測試環境，能有效減少對實體系統環境的影響，並可縮短因影響所復原的時間，有助於資訊安全的提升，故本研究經實證發現桌面虛擬化應用於端點電腦設備軟體安全的測試環境越好對桌面虛擬化技術的採用有正向顯著的影響。

(2)、在設備可移除式媒體的控管部份：

可移除式媒體有其相容性及可攜性，已廣泛使用於一般個人電腦運作環境，但水可載舟亦可覆舟，可移除式媒體容易造成內部資訊的外流，亦是明顯的資訊安全急需管控的風險，透過桌面虛擬化技術搭配精簡型電腦的部署，鎖定或排除可移除式媒體的使用，更可透過權限設定主動控管使用者資料存取的行為，有助於資訊安全的提升，經本研究實證結果，桌面虛擬化應用於端點電腦設備可移除式媒體的管控越好對桌面虛擬化的採用有正向顯著的影響。

(3)、在使用者存取權限的管理部份：

在一對一使用者與專屬電腦的辦公環境裡，使用者身份的認證已是存取網路資源的第一步，卻不時發生帳號密碼被駭、被竊等情事發生，未經授權的存取，導致個人或企業的重大損失等事件，亦時有所聞。當現代化企業為提升競爭力，降低營運成本，走向雲端的網路服務的同時，使用者存取權限管理的問題更是一大挑戰，為此傳統使用者存取權的管理工作也愈加複雜化；經由桌面虛擬化集中管理的運用，管理者可以經事前依企業任務規劃，設定好對應的使用者存取權限模組，套用到所屬使用者桌面虛擬化映像檔，即可彈性且快速的派送給使用者，符合企業業務

發展與資安的需求，故經本研究實證結果，桌面虛擬化應用於端點電腦設備使用者存取權限的管理越簡化對桌面虛擬化的採用有正向顯著的影響。

(4)、在電腦設備使用記錄之稽核部份：

傳統上企業在進行電腦設備使用記錄稽核，大多採取人工稽核的作業，常受限於紀錄資料量龐雜且分散儲存的困擾，採用桌面虛擬化技術可透過集中管理的模式，可統一設定與查詢稽核紀錄，並加以保全，有助於提升端點電腦設備的稽核與監督，符合企業遵循個人資料保護法以及 ISO27001 的標準，故經本研究實證結果桌面虛擬化應用於電腦設備使用記錄之稽核作業越容易對桌面虛擬化的採用有正向顯著的影響。

6. 管理意涵與後續研究建議

6.1 管理意涵

本研究主要探討端點安全控制措施管理導向、端點安全控制措施操作導向、端點安全控制措施技術導向對企業採用桌面虛擬化技術的影響，並使用 ISO 27001 標準定義的安全控制措施規範進行研究，在有關雲端運算眾多的研究中，多半以技術導向及管理導向相關的議題來進行研究，隨著雲端運算的議題日趨的重要，企業對於雲端相關技術的投資也大幅的增長的前提，因此本研究針對於桌面虛擬化的採用來進行探討。

在眾多的研究中雲端運算的主題多半以討論企業內部主機架購與雲端運算之商業模式，但這樣的研究固然的重要，但都趨向於企業資訊科技底層之研究，本研究有鑑於此，故針對與使用者較有關連之桌面虛擬化進行探討，同時透過 ISO 27001 標準之控制面項關聯為學術構面，並透過問卷調查進行相關實質的研究，來探討桌面虛擬化採用之意願。

經本研究透過 ISO 27001 之標準，發現從安全控制措施管理導向、操作導向、技術導向均會對於企業採用桌面虛擬化產生影響，因此未來相關的系統服務商或解決方案提供商在進行桌面虛擬化商品的設計，皆是其必須考量的重點因素，同時更應該從使用者的角度來進行思考，並能從管理面向、操作面向與技術面向進行產品設計，更有助於提升企業採用桌面虛擬化的意願，對於企業用戶來說，雲端運算的發展，已日趨成熟，從已往的伺服器虛擬化的應用到現今由前端出發的桌面虛擬化，企業所關心的層面皆不相同，因此當企業在導入桌面虛擬化的同時，更應該要了解使用者的接受程度。

但從本研究的結果發現，企業採用桌面虛擬化所帶來管理、操作或技術導向的利益相當多，同時這些利益越加正向，對企業採用桌面虛擬化有很重要的影響，因此未來服務提供者與企業評估者，也能從此一角度出發，來增加企業對於桌面虛擬化有全方位思維的了解。

6.2 學術貢獻

本研究並有以下之學術貢獻：

- (1)、從使用者角度探討桌面虛擬化之應用。
- (2)、以 ISO 27001 標準來探討科技採用之影響性。
- (3)、驗正 ISO 27001 控制項是否能以問卷設計題項進行其他變數的衡量。

6.3 研究限制

- (1)、本研究因為卷取得不易，並國內企業採用桌面虛擬化之企業不易尋找，故本研究在問卷施測上已盡量排除，不適合之研究施測者，以確保研究資料的完正性。
- (2)、本研究主要以實務導向來探討本研究之主題，故因研討會篇幅員故，無法詳細在本文中說明。

6.4 後續研究

- (1)、本研究以 ISO 27001 控制項進行構面的產出，並以安全控制措施之管理面、操作面與技術面進行衡量，未來的研究者可加入 ISO 27001 其他相關的控制項來進行探討。
- (2)、本研究以 ISO 27001 控制項進行研究探討，並以資訊安全的角度出發，未來研究者可加入其他構面變項進行探討，來增加研究內容的豐富性與廣度。
- (3)、未來研究者可加入如創新擴散理論與科技接受模式之相關理論，來進行本研究之下一步驟，同時更以使用者知覺或使用者認知的角度，並研究使用者在使用桌面虛擬化後的滿意程度，進行後續的研究。

參考文獻

中文部分

- 1、主計處「99年電腦應用概況報告」，民100年9月。
- 2、主計處政府機關資訊通報271期，「政府機構資通安全執行概況調查」報告，民99年5月。
- 3、資策會，99年度國家資通安全技術服務與防護管理委外服務案安全控制措施參考指引(V3.0)，民99年12月。
- 4、江政哲、張迺貞，「初探雲端運算」，臺灣師範大學研討會論文集-2010海峽兩岸圖書資訊學學術研討會論文集B集，2010年。
- 5、張念慈、彭秀琴，「雲端運算下資訊安全之探討」，經建會管制考核處技術手冊，2010年。
- 6、張益豐、陳上元，「邁向代理者基礎的智慧化環境研究」，中華民國建築學會第二十一屆第一次建築研究成果發表會，2009年。
- 7、陳澄，2010年3月，「雲端策略：雲端運算與虛擬化技術」，天下雜誌股份有限公司。
- 8、經濟部標準檢驗局 CNS27001，資訊技術－安全技術－資訊安全管理之作業規範，X6049，民95年6月。
- 9、劉得民，「圖書館虛擬個人化服務的資安及隱私權問題探討」，中華民國圖書館協會

—雲端運算與行動技術在圖書館服務的應用研習，2010年。

10、韓善術，「我國資訊教育發展現況與展望」，資訊與教育雜誌，第7-12頁，2001年。

英文部分

- 11、A. Michael, F. Armando, G. Rean, A. D. Joseph, K. Randy, K. Andy, L. Gunho, P. David, R. Ariel, S. Ion, and Z. Matei, "Above the Cloud: A Berkeley View of Cloud Computing", February 10, 2009.
- 12、Boss, G., P. Malladi, et al. (2007). "Cloud Computing." From http://download.boulder.ibm.com/ibmdl/pub/software/dw/wes/hipods/Cloud_computing_wp_final_8Oct.pdf.
- 13、Cash, J.I., McFarlan, F.W., Mckenney, J.L., and Applegate, L.M., Corporate Information Systems Management:Text and Cases, Irwin:MA., 1992.
- 14、Cyert, R.M., Simon, H.A., and Trow, D.B., "Observation of a Business Decision," The Journal of Business, 1956, 29, 237-248".
- 15、Dutton, J.E., "Understanding Strategic Agenda BUILDING AND Its Implications for Managing Change," Scandinavian Journal of Management Studies, August 1986,3-21.
- 16、Gartner, I. (2008). "Gartner Says Contrasting Views on Cloud Computing Are Creating Confusion." from <http://gartner.com/it/page.jsp?id=766215>.
- 17、Heiser, J. and M. Nicolett. (2008). "Assessing the Security Risks of Cloud Computing ", from <http://www.gartner.com/DisplayDocument?id=685308>.
- 18、Hickson, D.J., Bulter, R.J. Cray, D., Mallory, G.R., and Wilson, D.C., "Desision and Organization - Process of Strategic Decision Making and Their Explanation," public Administration, 1989,67,373-390.
- 19、Hoffer, J.A., and Straub, D.W. Jr., "The 9 to 5 Underground: Are you policing computer Crimes?" Sloan Management Review, Summer 1989,35-43.
- 20、<http://www.digitimes.com.tw/tw/dt/n/shwnws.asp?CnlID=10&Cat=&Cat1=&id=168851#ixzz1aMKbi29G>.
- 21、<http://www.ithome.com.tw/itadm/article.php?c=56953&s=2>
- 22、<http://www.ithome.com.tw/itadm/article.php?c=56953&s=4>
- 23、Huber, G.P., Managerial Decision Making, Glenview, III: Scott, Foresman, 1980.
- 24、I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared", Grid Computing Environments Workshop, Nov, 2008.
- 25、Jarvenpaa, S.L. and Ives, B., "Executive Involvement and Participation in the Management of Information Technology," MIS QUARTERLY, 1991, 205-227.
- 26、Larsen, A.K., "Global Security Survey: Virus Attacks," July 12,1999, Informationweek, Accessed from <http://www.informationweek.com/743/security.htm>.
- 27、Laudon, K.C., and Laudon, j.p., Management Information Systems:New Approaches to Organization and Technology,Prentice Hall, USA:New Jersey,1998.

- 28、Mansfield-Devine, S. (2008). "Danger in the clouds " Network Security 2008(12):9-11.
- 29、Mell, P., & Grance, T. (2009). The nist definition of cloud computing. National Institute of Standards and Technology .
- 30、Mintzberg, H., Raisinghani, D., and Theoret, A., "The Structure of "Unstructured"Decision Process",Administrative Science Quarterly, June 1976, 21,246-275.
- 31、Neilson, E.H., "Understanding and Management Conflict,"in J.W. Lorsch and P.R. Lawrence Eds., Managing Group and Intergroup Relations, Homewood, iii:Irwin and Dorsey, 1972,329-343.
- 32、Nutt, P.C., "Types of Organizational Decision Process,"Administrative Science Quarterly, 1984,29,414-450.
- 33、Pfeffer, J., and Salancik, G.R., The External Control of Organization: A Resource Dependency Perspective, Happer and Row, New York,1978.
- 34、Pondy, L.R., "Organizational Conflict:Concepts and Models," Administrative Science Quarterly, 1968,12,296-320.
- 35、R. Steve, "New Service Offers Cloud Cracking for WPA", The Tech Herald, <http://www.thetechherald.com/article.php/200950/4906/New-service-offers-cloud-cracking-for-WPA>, 2009.
- 36、Security Concerns for Cloud Computing Global Knowledge Training LLC, 2010 march.
- 37、Stallman. (2008). "Stallman: Cloud computing is 'stupidity'." The Guardian.
- 38、Stamford. (2008). "Gartner Says Cloud Computing Will Be as Influential as E-business." Retrieved August, 2008, from <http://www.gartner.com/it/page.jsp?id=707508>.
- 39、Straub, D.W. Jr., and Welke, R.J. "Coping with Systems Risk: Security for Management Deciiion Making," MIS Quarterly, Decembr 1998,411-469.
- 40、Top Threats to Cloud Computing V1.0 cloud security alliance ,2010 march <http://www.cloudsecurityalliance.org/topthreats>