同一公司兩次轉換企業防毒軟體服務之個案研究- 詮釋主義的觀點

A Case Study of an Enterprise Switching Antivirus Software- from an Interpretivist Perspective

侯正裕

Avus C,Y. Hou

摘要

商業活動依賴網路的程度越深，企業對資訊安全的要求也就越高。在這樣的需求下，企業防毒軟體便成企業資訊安全首要的必備方案。本研究剖析一家台灣中型企業經歷兩次防毒軟體的轉換過程。第一次的轉換結果並未成功，而在兩年後的第二次轉換中成功轉換。本研究觀察並紀錄這這兩次的轉換決策的過程，再提出研究命題，提供需要轉換防毒軟體的企業及供應商提供建議。防毒軟體供應商應特別注意其客戶的合約期限。在期限之前藉由增加相關行銷活動來維持客戶續用其防毒產品及服務。並發現曾經嘗試轉換防毒軟體但失敗的公司，會進行一些調整活動，並持續進行轉換的可行性分析，有這種特徵出現的企業，其轉換的機率更高。

關鍵字：企業防毒軟體服務、資訊安全、詮釋主義、服務轉換

ABSTRACT

Business application of Internet has matured. This maturity promotes the development of various business models based on the Internet. However, as enterprises depend more on the Internet, so as their demand for information security, to which corporate antivirus software is the primary solution. Because enterprises have different perceptions on the validity of a corporate antivirus package, when they are not satisfied with a given product, the most direct solution would be switching to a new service provider. The business model of antivirus software provision that based on regular contract extension also guarantees an opportunity for enterprises to adopt different products when the previous contract is due.

The research studies the process of a medium-sized Taiwanese enterprise which experienced antivirus software switching twice. The first switching was not successful, but the upgrading of software and alternation of structure had helped the enterprise to meet its information security needs. Two years afterwards, the second switching, which was also rendered by the same decision-making process, was successful. Adopting a philosophical perspective of interprevitism, the research observes and documents the decision-making process of these two switches, and provides reference for enterprises in need of antivirus software switching.

In addition to the analysis of switching processes, the research also provides suggestions to antivirus software providers. The research found that before the service contract is due, clients have an opportunity to switch to a new service provider. Therefore, antivirus software providers should pay special attention at the end of the contract period, and offer promotions so that clients would extend contracts. The research also expands the result of Hou and Chern's study (2007) and found that enterprises that have seen switching failures would initiate some adjustment steps to accommodate its information security needs until the operation is stabilized. These adjustments include continuously evaluating products of other service providers, and analyzing the feasibility of switching. Enterprises that adopted these moves are more likely to switch in the future.

Keywords：Corporate antivirus software; information security; interprevitism; service switching

侯正裕 崑山科技大學資訊管理系講師

一、緒論

資訊科技(Information Technology, IT)進步的現代社會，使用電腦系統來進行辦公室自動化及業務處理已成為企業行政的主要工具，同僚之間藉由網路協同合作，進而完成商業功能。研究指出企業使用 IT 會帶來潛在的風險，依賴 IT 資源較深的公司承受的風險也較高 (王凱 2003)。例如企業在倚靠網際網路來協助商業功能，隨之而來的電腦病毒議題同時也帶來了資訊安全威脅的風險。這些電腦病毒的攻擊讓企業的功能在極短的時間癱瘓，付出高昂的回復成本(陳至哲 2002)。例如 Blaster 病毒，在短短五天之內就造成全球的感染，根據 CSI 在 2005 年的調查顯示，美國企業因為資訊安全所造成的損失高達一億三千萬美元，其中由電腦病毒造成的損失最高 (CSI Survey, 2005)。

在對抗電腦病毒威脅上，多數企業首先安裝防毒軟體以為因應，因而創造了防毒軟體廠商的商機。眾多廠商競相投入提供多樣的防毒軟體產品供企業選擇(Burke and Brian 2007)。防毒軟體可以建立一道基礎防線，提高安全的程度，降低資訊安全威脅的風險。然而，研究結果顯示縱使企業在防毒軟體的安裝率近乎 100%，仍然無法完全防止電腦病毒的攻擊，在面對新型態電腦病毒的創新攻擊模式及經由 Internet 的快速擴散讓大多數企業防不勝防 (Keller and Powell 2005)。此外，不同品牌的防毒軟體效能不同，使得的有效性也有所差異。一旦負責掌控企業資訊安全的軟體失效，則企業會陷於危機狀態，癱瘓商業功能造成企業極大的損失。這個狀態必須等資訊安全問題得到排除之後，公司才能重新運作。這個零合的特性(zero-sum)讓資訊安全軟體與其他企業應用軟體有極大的不同，也就是企業在病毒爆發的時候，資訊系統是完全無法運行。因此，在選擇符合企業資訊安全架構及有效的防毒軟體的上是相當重要的。最後，現行的技術無法在同一部電腦安裝兩套防毒軟體以增加保護，這種軟體互斥特性，也讓企業防毒軟體的轉換研究就有其必要性，且符合轉換行為的定義(Keaveney 2001)。

防毒軟體必須定期更新病毒碼以保持其有效性，最新定義的病毒碼可以讓防毒軟體能夠辨認最新的病毒並加以攔截進而刪除威脅。這種需要定期更新的特性讓防毒軟體的廠商更像是一種服務產業：對企業提供病毒碼及更新的掃毒引擎來防制電腦病毒的服務，而非單純的資訊產品。而防毒軟體的年度續約購買制度也類似服務業廠商的經營模式，每年向客戶收取固定的費用以支付這一整年的病毒碼更新服務。因為這些特性，本研究從服務轉換觀點來分析防毒軟體的轉換應該是適當的。關於服務轉換研究主要出現於行銷學域，Keaveney (1995) 以關鍵事件法(critical incidents method)研究為何消費者轉換服務供應商。她發現核心服務失敗、服務遭遇過程失敗、服務人員對服務失效的回復失當、不方便、競爭、道德問題、價格、甚至服務供應商結束營運均會造成消費者轉換行為，該研究並衍生出後續多樣性的討論(Keaveney 2001；Kim et al. 2006)。由於資訊安全是近年來重視的研究議題，而著力於資訊安全產品的轉換探討非常缺乏，僅有 Hou and Chern (2007)曾經提出以經濟面之轉換成本影響防毒軟體轉換議題。該研究顯示因為防毒軟體的資產特用性低，意味著轉換行為產生的轉換成本並不高，企業唯一要故慮的只有安裝防毒軟體的用戶端的多寡，因為重新安裝用戶端軟體的人工成本佔轉換過程中最高的成本。然而該研究並未後續探討這些轉換失敗的廠商的持續行動，因而啟發了本研究再進行的必要性。本研究的貢獻有下列 3 點。首先，我們的研究延續了 Hou and Chern (2007)的研究，持續探討並深入了解防毒軟體服務轉換失敗廠商的後續行動。第二，探討對資安產品不滿意的前置因素，以供資安產品供應商參考。第三，提供有關企業資安產品的轉換決策過程，供實務界參考。

本文後續內容如下。第二節進行相關文獻探討；第三節說明研究方法；第四節描述個案及轉換過程；第五節分析個案結果；最後於第六節提出簡短的結論，供研究者及實務界作為後續工作的參考。

二、文獻探討

2.1 防毒軟體產業

Kaspersky (2005) 對防毒軟體的分類，依據其年營收的高低及市場的佔有率，將防毒廠商分成三大群：領導廠商、二線廠商、及其它廠商。領導廠商有三家：Symantec, Trend Micro與McAfee，其防毒軟體及防毒架構也為大多數企業用戶採用，因此這三家廠商的舉動均對整個市場造成影響。二線廠商的產品大多集中於其母國銷售，少部分銷往國際市場並獲得客戶的青睞，例如來自英國的Sophos及俄國的Kaspersky都屬此類。其它廠商則是一些只營運於其所屬國家的防毒軟體，如南韓的VI Robot (Kaspersky 2005)。

企業版防毒軟體的營業額是逐年的攀升，根據IDC的調查顯示在2005年市場總營業額已經超越了個人版的年銷售總額(Burke and Brian 2007)。升高的原因是在企業環境中需要統一佈署的架構來應付網際空間中多樣化的威脅，企業不得不在其疆界之內構築一道安全的圍牆。這些多樣化的威脅除了以往的電腦病毒之外，近幾年的間諜軟體、垃圾郵件、釣魚軟體等，都給予防毒供應商成長的利基。而因應這新增的威脅，作為安全圍牆的防毒軟體的功能也愈加越多，例如McAfee，便提供企業可以依據通訊埠(by ports)去限制企業電腦的網路通訊，以增加網路安全及中央控管的彈性。而在這競爭激烈的市場中，近年來各家廠商的策略也出現分歧。例如Trend Micro開始專注於防毒為核心資訊委外服務，不僅是提供企業用戶防毒軟體，也提供資訊安全的相關服務，例如在企業受到電腦病毒疫情氾濫後會派技術人員前往提供解決方案，資安委外的顧問服務等，藉以轉換薄利的軟體出售到高利潤的服務市場當中。而Symantec 則認為防毒工作只是資訊安全的一環，任何防毒軟體均有其不足。因此除了做好目前的防毒工作之外，一旦企業陷入癱瘓時，要如何在最短的時間內做到災後復原。因此，在既有的防毒功能之外，還提供備份的功能，以確保災後復原的有效性。

2.2 服務轉換

在轉換行為意圖的研究主要可以分成三個主要的方向，1.以過程模型(process models)來探討顧客對服務的轉換(Roos 1999)；2.比較服務持續者與轉換者之間的不同(Keaveney 2001)；3. 探討影響顧客的轉換因素。最末的這個方向也是最多學者著力的觀點。先前的研在消費者轉換涵蓋許多的領域，例如修車業及髮廊， Keaveney (1995) 就以關鍵事件法(critical incidents method)研究為何消費者轉換服務供應商。她發現核心服務失敗、服務遭遇過程失敗、服務人員對服務失效的應對失當、不方便、競爭、道德問題、價格、甚至服務供應商結束營運均會造成消費者轉換行為。 Bansal and Taylor(1999) 則發展一個認知模型(cognitive models)檢視消費者的轉換。

先前研究顯示滿意度高的客戶對服務提供者的忠誠度也較高，不容易轉換到其他競爭者的品牌及產品。反之；低滿意度會讓客戶有高的機率轉換到其他競爭者的產品或品牌(Fornell 1992)。然而，研究也顯示高滿意度的客戶仍然可能轉換其服務，只是機率較低滿意度的客戶為低。是故，滿意度的高低對轉換行為並絕對的因果關係。而Fornell (1992) 建議廠商有兩種策略來防止客戶的轉換：攻擊策略及防守策略。在攻擊策略則是以高市場佔有率，藉由網路效應 (network effect)來吸引更多的顧客。而防守策略上主要可以藉由轉換障礙(switching barriers)來阻止客戶的轉換行為，例如高轉換成本。許多研究顯示轉換成本不僅直接影響消費者的轉換或再購，且也是影響消費者轉換及再購決策的一個干擾變數 2002)。(Anderson et al., 1994; Gwinner, 1998; Jones et al.,

三、研究方法

在研究涉及高度敏感議題時，以大量郵寄問卷填答法來收集資料是不適當的，因為企業通常不會願意將敏感性資料經由問卷調查的方式提供給外部人員，造成公司的損害。資訊安全議題的研究亦屬上述的類型，因而增加資訊安全研究的困難度，甚而或有研究失敗的可能 (Kotulic and Clark 2004)。 而本研究亦屬此類，其過程中會涉及高敏感議題或許對企業商譽有所影響，因此研究對象是否願意配合研究進行，便相當重要。Kotulic and Clark (2004)曾建議研究者，在從事資訊安全議題研究時，可以考慮以個案研究法來進行深入的瞭解，以便獲取翔實的真相。其次，研

究對象對於研究員本身的信任也相當重要。先前研究者便與此企業有緊密的關係，該企業同意配合學術計畫讓研究者獲得翔實的資料，以作為日後資訊安全教案。此外，雙方並簽訂防制資訊揭露協定以保護個案公司；並且在作者投稿之前，個案公司已經先行研讀本研究結果，藉以了解揭露的程度並對研究結果進行確認。

除了研究者深入場域資料收集的方式採取個案情境之外，本研究輔以訪談法及次級資料來源。由研究者親至被研究單位進行面對面訪談，以期獲得一手資料以進行分析研究。訪談方式由研究者提出問題請被研究對象回答，問題均於訪談一週前以電子郵件寄給受訪者。其職位分別為CIO、網路管理人員、及資訊安全人員，受訪者皆負責組織電腦病毒管理並有參與採購防毒軟體決策的權力，故本研究的資料相當具有可信度。在次級資料收集方面，本研究獲得兩次採購記錄，內部評估報告等，以作為判准的依據。資料的分析以特徵出現方式為主，如果理論預設的情況在被研究對象出現，則宣稱具有理論複現，支持理論的觀點。

個案研究法可以是深入瞭解研究對象進而能建立理論的詮釋主義觀點(Eisenhardt 1989)。或者，先提出理論假設並比較研究對象結果來驗證理論的解釋能力，屬於實徵的個案研究觀點(Yin 1994)。這兩種方式都有學者使用，但其背後的思維建築在卻是在迥異的哲學觀之上。詮釋研究進行是一種循環的過程：詮釋由「本文(context)文字的解釋→部分(part)瞭解→全文瞭解→再回頭來看本文→部分…」如此形成循環圈，以達到全然瞭解的過程(Klein and Myers 1999)。也就是說，要瞭解全部必須要先從部份開始，而每一個部份都是彼此互相依存、互為相關(interrelationships)。這是其它principle的根源，為詮釋研究必須要達到的根本要求。詮釋主義主張以全然了解的方式來闡述研究事件的完整脈絡及事件的歷史背景，進而建立理論命題。Klein and Myers (1999) 曾提出七點原則(principle)指引研究者利用詮釋主義的觀點進行研究。1.情境(contextualization)：對研究對象的背景脈絡要能全然瞭解。2. 研究者與參與研究者的互動3. 抽象與一般性：從研究的抽象層次到一般性 4.合理性：排除研究者先入為主的觀念 5. 詮釋的多樣性：從不同觀點來進行詮釋，而非單一個論點。例如用多樣來源的資料收集方式，藉以修正偏誤(bias) 6. 懷疑(suspicion)：希望研究者能批判自己的研究，解放自己而得到全然不同的瞭解 7. 所有的原則並非獨立條件而是彼此相互依存，期望研究者以整體(whole)的點來觀察這些個別的原則。

在一個新議題浮現之時，利用實徵的方法恐無法了解問題真正的發生原因及本質。而資訊安全軟體的轉換(防毒軟體為其一)，便是屬於此一新興的議題。此時，以不預設立場的詮釋主義觀點來瞭解問題的全貌，將有助於探索問題發生的原因與本質，以便解釋。

四、個案背景與轉換過程

4.1 個案簡介

A 企業

A企業為大型教育訓練機構有約350名教職員工，2500名學員。2006年在整個企業擁有1000台以上的PC電腦 (包含行政網路及教育訓練教室)，及約50部伺服器在不同的作業系統上運作，包含AIX 400, Sun Solaris, Linux, FreeBSD, Windows 2000, 2003 Server 等。而A企業的網路環境非常複雜，其擁有對外300Mbps的大頻寬及包含ATM，Giga Ethernet，Fast Ethernet，Wireless 等的網路架構，並且在某些企業環境提供員工認證無線上網，其組織龐大而且文化相當自由。

A企業受制於母公司的資訊系統支援及採購規章限制，某些重要的資訊系統由母公司的資訊部進行系統開發，再轉由A企業使用及維護。必要時由母公司進行遠端程式修改維護及異地備源，故A企業對母企業有E1網路專線連接。在營運設備採購方面，由A企業提出採購需求及規範，交由母企業的採購部辦理，以增強成本控管，杜絕與廠商勾結等採購弊端的發生。然而，母企業資訊部對於非核心的資訊系統及應用程式並沒有強制的統一，也就是說，並不會強制A企業採用相同的資訊應用軟體。例如，在防毒產品方面，並沒有強制必須與母企業一致。故A企業

有自主權可以決定其防毒軟體的品牌及服務支援供應商。

4.2 第一次轉換

4.2.1 轉換動機

因為對原有防毒軟體核心功能不滿意而引發轉換動機。A企業一開始使用 S牌 8.0企業版防毒軟體，因為Nimda, Blaster, MyDoom 等接連幾次的全球性電腦病毒攻擊，S牌都無法有效防禦，企業內已中毒的電腦透過高速的網路連接快速的再感染其它電腦，使災情如滾雪球般擴大。每次處理均讓IT人員疲於奔命並耗費大量的時間與人力成本，用戶端對IT單位抱怨連連。所以A企業是不滿意 S牌的防毒效能而誘發轉換的動機。其次是廠商在售出軟體之後並無進行相關的售後服務。任由A企業在病毒來襲時孤軍奮戰，即使A企業向經銷商尋求援助，也經常沒有任何的回應或是拖延。因此引發A公司轉換的動機，時間則是在防毒軟體合約到期前的3個月。

4.2.2 第一次轉換過程

在A企業在防毒軟體轉換的過程中，決定轉換至哪一品牌的防毒軟體是考慮市場上領導品牌進行評估選擇，就是在市場上為S牌的競爭者P品牌。兩品牌防毒軟體的聲譽在市場上不相上下。然而，A企業尋找合格的經銷商的過程中，花費2個月的時間所接觸的兩家P品牌供應商都不能符合A企業的需求，因為A企業的資訊安全主管認為供應商規模太小不足以應付A企業大型企業的需求。然而在供應商的觀點則認為，他們有足夠的能力承擔A企業的系統建置，是A企業的主管多慮了。這顯示雙方互信基礎不足，而供應商又不願意花時間與資安主管建立信任關係，讓彼此的交易產生了阻礙。

在預算執行截止的時間逼近及防毒合約到期的雙重壓力下，A企業回頭找了S品牌的代理商尋求問題解決的可能。S牌的供應商以很快速度回應了A企業的要求，幫助A企業安裝新版的防毒軟體 ”X9.0” 測試，“X9.0”的新功能「用戶端郵件收件掃瞄」正好是A企業資訊安全架構上缺乏且迫切需要的功能，符合A企業資訊安全的需求。甚而，在此次的安裝中，供應商提供並安裝S牌郵件閘道掃瞄伺服器供A企業免費試用，而S品牌的代理商規模較大，有許多大型企業的成功建置經驗，並銷售防毒軟體服務給予A企業的母公司，也讓A企業的資訊安全主管放心不少，提高了其信任度。而這樣快速的反應及關係，讓A企業忘卻了先前S牌防毒軟體核心功能不佳的印象。

4.2.3 第一次轉換結果

感受到轉換到新系統的不確定性，決策就不易達成。A企業 CISO在比較過後，決定繼續購買S牌防毒軟體服務1年，並升級到X9.0版本。於是提出了採購規範來進行採購，因為 CISO已經決定要使用 S牌的企業防毒軟體，所以採購規格主要是以 S牌的產品規格來開立，並提交母公司採購部進行採購。

4.3 第二次轉換

4.3.1 第二次轉換動機

S品牌的軟體漏洞，引發A企業的第二次轉換動機。由於S牌10.0版本有系統漏洞，這會造成用戶端的系統受到入侵而不斷的重新開關機，進而導致使用者電腦系統的不穩定。這些因素讓A企業的IS人員疲於奔命，甚至在一開始原因未明的時候，還花很多時間作故障排除而不得其解。直到A企業的網路管理人員參加一次外部研討會時，赫然發現是導因於S品牌防毒軟體的漏洞是影響到用戶端電腦不正常問題的原因，於是通知資訊安全人員此一現象，並在實際測試中獲得證實。之後，A企業向S牌供應商尋求協助，然而供應商的消極拖延的態度讓A企業的對S品牌的滿意度降至低點，於是在合約即將到期之前，決定更換防毒軟體。

4.3.2 第二次轉換過程

A企業於是開始評估防毒軟體轉換，以決定轉換哪一品牌的防毒軟體。有三家公司被考慮：P牌，M牌，K牌。於是A企業進行一系列的測試與評估。而原本S牌則因為服務品質太差，在一開始就被排除考慮名單之外。

A企業首先要求各廠牌銷售團隊進行簡報。P品牌以到場服務客戶的病毒問題為訴求，強調不僅是單純的軟體銷售，而是包含了防毒業務委外的服務方式。M牌提供優秀的中央控管功能，

強調在中央控管的機制下，可以針對用戶端進行通訊埠的限制，藉此類似防火牆的功能來進一步達到病毒的防禦。K品牌是市場上的明星公司，強調非常高的病毒偵測率。在聽過三家供應商的簡報之後，A企業的CIO，網路管理人員，資訊安全人員開始進行一連串的評估。

M牌及P牌皆受到A企業青睞。M牌優秀的中央控管能力及不需病毒 patch 程式，僅需防毒軟體本身的更新就是新的解毒程式是一種在防毒機制上創新的作法，能有效的降低企業對防毒軟體的維護成本。P牌則是因為創新的服務功能將企業防毒的業務部分委外而受到A企業的注目，然而因為包含委外服務，其價格也最高。而K牌雖然防毒效能優秀具有口碑，但沒有大型企業的使用實績，受不確定性的因素影響，A企業並不敢貿然嘗試。最後，M牌的銷售經理與A企業的CIO素有淵源，而且價格也最低。就此，A企業將防毒軟體付諸母公司的採購中部進行採購。

4.2.3 第二次轉換結果

在三家公司當中，M牌提供非常大的折扣，以低價格來贏得A企業的合約。在採購規章規定，除非使用部門有特別原因陳述且經由採購審核組同意，否則經由使用部門確認之後，就會由最低價的廠商得標該採購案。而 M牌的產品因為大幅折扣的關係，是本採購案件中最報價最低的，理所當然由 M牌得標。

A企業於是開始進行整個企業的防毒軟體轉換。A企業的組織環境是分散式的，擁有五個教學研究部門及單一的行政單位來提供內部研發單位及客戶的服務，這讓A企業可用平行轉換與階段轉換的方式來進行防毒軟體的轉換。在全面轉換用戶端的過程中，A企業排定每個部門以一天的時間進行轉換，從S牌防毒軟體到M牌防毒軟體。M牌的供應商並且提供人力支援來幫助A企業進行轉換。此外，M牌軟體有專門的移除程式可將S牌的防毒軟體移除並自動安裝M牌產品，一個滑鼠按鍵就完成所有程序，相當簡易而方便。經由這種簡易的程序，讓A企業較具電腦使用技能的部分員工也能夠自行安裝用戶端防毒軟體而減少轉換過程中的人工成本。A企業用戶端全數的防毒轉換共經歷了三週，Table 1顯示M公司轉換的兩種不同防毒軟體的硬體需求，而Table 2顯示了新舊廠商在轉換過程承諾提供的支援及價格。

Table1 M個案轉換之軟硬體需求

	S牌	M牌
伺服器硬體需求	● 64 MB RAM ；111 MB available disk space	● Intel Pentium II 300MHz processor or equivalent ● 128MB of RMM ● 300MB of disk space
伺服器軟體平台需求	● Win2000ProfessionMl 以上支援 IIS Server 版本即可. ● Web server: Microsoft IIS Server.	● Windows NT series (SP 6a), 以上支援 IIS Server 版本即可 ● Web server: MS IIS Server. ● Apache Web Server 2.0 or later.

Table2 新舊廠商在轉換過程承諾提供A企業的支援及價格

	S牌	M牌
軟體版本	X9.0	最新版
測試期限	1個月	1個月
採購價格	NT$800000	NT$450000
教育訓練	有	有
用戶端免費安裝	有	有

五、結果

本章節就個案兩次轉換過程及結果進行分析。在此歸納前後兩次轉換的差異，經過分析後分類出下列幾個因素。

人員特質-資訊人員的人格特質

A企業從四年內經歷了二次的企業防毒軟體轉換，涉及了長時間的演變。雖然結果不同，但是人員的特質卻是不可以忽略的因素。

第一次的轉換中，資訊安全主管扮演了非常重要的角色，A企業的採購文化為業務負責人佔有較大的採購決定權，因為該軟體採購後將由業務負責人使用。所以資訊安全主管在防毒軟體的採購中佔有重要的位置。第一次轉換因為資訊安全主管對 P牌的供應商皆無法信任，對轉換結果有很高的不確定性，在此不確定的影響之下對轉換的成功就會有所影響。因此，否決P牌的產品而續用S牌，轉換結果為失敗。

第二次的轉換中，不僅資訊安全主管已經換人。網路管理人員，CIO也已經一併更換。在第二次轉換過程中，A企業原先的資訊人員都已經離職。僅有原先網路組組長留任並升級為資訊部門經理(CIO)，其餘都是新人且是經理親自面試的嫡系人馬。可以說決策人員全面的更換，當然評估軟體轉換的面向也會不一樣，進而做出不同的決策。

藉由Hou and Chern (2007)針對四家公司以轉換成本高低來影響防毒軟體轉換的研究結果顯示，因為防毒軟體的資產特用性相當低，為相當標準化的一項軟體產品，意味著企業受制於防毒軟體的特殊性資產投資很低，轉換行為產生的轉換成本並不高。而企業唯一要考慮的只有用戶端的多寡，因為轉換行為涉及重新安裝用戶端軟體的人工成本。用戶端越多，轉換過程中的安裝成本較高。意即，企業防毒軟體的轉換成成本與用戶端的多寡呈現正向關係。藉由上述研究結果來分析A企業個案，本研究認為在第一次轉換過程中，資安主管顧慮太多，喪失了轉換的契機。使A企業需要面臨再一次轉換的過程及成本花費。而第二次轉換因為資訊安全主管的行事風格明快，因此轉換相當順利。因此，綜合以上論述，本研究提出下列命題：

Proposition1：資訊安全主管的人格特質對防毒軟體轉換的決策有影響。

對軟體效能及供應商服務的不滿意

誘發兩次轉換的原因都是因為對軟體的效能不滿意。第一次是因為Nimda, Blaster等病毒的爆發時S牌無法有效阻攔，第二次則是因為S牌10.0企業版防毒軟體的漏洞而影響到用戶端。但本研究在訪談結果顯示：「經銷商的漠不關心態度，是造成第二次轉換的主要因素」。

Nimda, Blaster 病毒造成全球性的電腦病毒疫情，防毒軟體供應商無法提供及時的防護而造成客戶的損失及不便。照理供應商應該注意到客戶服務，藉由各種管道表示關懷及提供解決方案。然而，經銷商及防毒軟體供應商的漠不關心，任由A企業自行摸索處理的態度讓資安主管的滿意度大幅下降。甚至還必須用到P牌的掃毒程式來進行補救的動作，更讓這種情勢雪上加霜。

而S牌 10.0企業版防毒軟體的漏洞，理應由經銷商主動提醒客戶及提供修補程式漏洞的服務；然而，經銷商對A企業的諮詢要求拖延甚至毫無回應的處理態度更讓A企業的滿意度降至低點。A企業網管人員在接受訪談時表示，擔任安全防線守門員的防毒軟體有漏洞已經是無法令人接受的事實，經銷商掩蓋事實真相的態度更令人不解及心寒。讓A企業在二次評估防毒軟體轉換之前，直接剔除掉S牌的候選資格。

本研究所得到的轉換因素與Keaveney (1995)所提出的結果相互印證。除了主要服務失效以外，員工的服務處理失效是造成客戶轉換的一大因素。這兩個類型分別對服務業轉換中佔居首位及第二的位置。

因此，綜合以上論述，本研究提出下列命題：

Proposition2：防毒軟體核心效能及供應商售後服務態度，兩者會影響客戶的續用意願。

信任因素

二線防毒軟體廠商通常沒有在企業評估中勝出的機會。在第一次轉換企業曾評估Panda及Sophos等廠牌軟體，第二次曾評估Kaspersky。

但這些二線廠商都沒有勝出的機會，到最後階段都僅有領導廠商才有機會被考慮。分析其可能因素為，防毒軟體是資訊安全產品，涉及安全議題的產品都有信任的因素浮現。而商譽愈佳，市場佔有率愈高的廠商越能得到客戶的信任。綜合以上論述，本研究提出下列命題：

Proposition3：企業選擇防毒軟體會因為信任因素選擇領導廠商的品牌，二線廠商難有勝出的機會。

轉換時機-合約到期之時

綜觀兩次的轉換時機，本研究發現A企業在意圖轉換的時機，都是在防毒軟體即將到期之前，其防毒軟體合約以一年一簽或兩年一簽為基準。防毒軟體因為具有低資產特用性的關係，對客戶而言要考慮的只是用戶端的多寡是否影響到人為轉換成本，因為重新安裝防毒軟體耗費人力成本往往是資訊部門首先面臨的問題(Hou and Chern, 2007)。故用戶端越多的企業，面臨的轉換人為成本愈高。資訊部門在追求穩定度的前提下，會有多一事不如少一事的心態，故不會貿然的進行轉換行動。因此，綜合以上論述，本研究提出下列命題：

Proposition4：防毒廠商應特別注意客戶的合約期限，並可在期限截止之前藉由加強行銷活動關懷客戶，防止客戶轉換防毒軟體。

六、結論

本研究檢視單一個案兩次轉換企業防毒軟體的過程，以不預設立場的詮釋主義觀點，親涉場域中探討兩次轉換過程的異同。其結果可幫助實務界評估資訊安全轉換的企業，在此個案尋找異同點，以作為資訊安全產品轉換決策的參考：要與原有經銷商續約或是轉換。而在學術貢獻上，釐出資安產品不滿意的前置因素，及考慮點可供後續的研究者發展後續定量的研究分析。

研究結果發現企業資訊安全人員並無法精確評估防毒軟體的效能，在此情境下，IT人員偏好在領導品牌或防毒軟體市占率進行選用，因此信任因素相當重要。然而價格仍然是企業採用前會考慮的因素，在客戶以價格為衡量因子的情況之下，壓低價格求售的領導廠商之產品有較佳的出線機會，然而這也壓縮了廠商能夠獲利的空間，而陷入價格競爭。

一般而言防毒廠商的經銷商對企業用戶的支援不夠，讓企業多半自行架構及解決防毒問題而甚少依賴供應商，這樣的情況造成企業幾無忠誠度可言，因為供應商沒有建立轉換障礙。研究結果發現供應商並沒有建立轉換成本來鎖住客戶(customer lock-in)進而抑制買方的轉換，建議防毒軟體廠商可在建立轉換障礙上思考相對應策略，留住買方。最後，轉換的動機起源於效能不佳造成使用者不滿意軟體效能，本研究建議防毒業者在行銷策略之外，應著重本身產品技術的核心能力，乃是確保產業地位的核心資源。

本研究雖力求嚴謹，但仍有其限制。首先，研究個案為中大型企業，其結果可能無法一般化到其他型企業，如小型企業。因為多數小型企業並沒有分工精細的資訊部門及複雜的網路架構，因此將本研究結果概化到小企業時，需審慎的考量案例的狀況。然而本個案的網路複雜程度及系統考量均較中小型企業來的縝密，因此研究結果仍有其參考的價值。其次，本研究的對象為單一個案，建議後續的研究者能以多個案的方式來進行研究並加以比較，來延伸研究的結果。

參考文獻

1. Anderson, E.W. and Sullivan, M.W. “The antecedents and consequence of customer satisfaction for firms.” Marketing Science (12:2), 1993, pp. 125-143.
2. Bansal, H. S. and Taylor, S. F. “The Service Provider Switching Model SPSM: A Model of Consumer Switching Behavior in the Services Industry.” Journal of Service Research (22:2), 1999, pp.200-218.
3. Burke and Brian. (2007). Worldwide Antivirus 2004-2008 Forecast and 2003 Vendor Shares. Internet Data Center Reporting, IDC #31737, accessed 2009/11/7.
4. Chen and Hitt. (2002). Switching Cost and Brand Loyalty in Electronic Markets: Evidence From on-line Retail Brokers. PhD dissertation, University of Pennsylvania.
5. Eisenhardt, K. M. “Building theories from case study research.” The Academy of Management Review (14: 4), 1989, pp. 532-550.
6. Fornell, C.A. and Larcker, D. “Evaluating structural equations models with unobservable variables and measurement error.” Journal of Marketing Research (18:1), 1981, pp. 39-50.
7. Gordon, M. et al. “CSI/FBI Computer Crime and Security Survey”, CSI, 2005.
8. Gwinner, K.P. “Relational benefits in service industries: The customer’s perspective.” Journal of Academy of Marketing Science (26:2), 1998, pp. 101-114.
9. Hou, C.Y. and Chern, C.C. The effect of switching costs for corporate antivirus package switching decision, in Proceedings of Pacific Asia Conference in Information System (PACIS 2007); Auckland, New Zealand.
10. Jones, M.A., Mothersbaugh, D.L. and Beatty, S.E. “Why customers stay: measuring the underlying dimensions of services switching costs and managing their differential strategic outcomes.” Journal of Business Research (55:6), 2002, pp. 441-450.
11. Kaspersky, E. (2005). The contemporary Antivirus industry and its problems. http://www.viruslist.com/en/analysis?pubid=174405517, accessed 2009/11/7
12. Keaveney, S.M. “Customer switching behavior in online services: An exploratory study of the role of selected attitudinal, behavioral, and demographic factors.” Journal of the Academy of Marketing Science (29:4), 2001, pp. 374-390.
13. Keaveney, S.M. “Customer switching behavior in service industries: an exploratory study.” Journal of Marketing (59:2), 1995, pp. 71-82.
14. Keller, S. and Powell, A. “Information Security Threats and Practices in Small Business”, Information System Management (22:2), 2005, pp.7-19.
15. Kim, G., Shin, B. and Lee, H.G. “A study of factors that affect user intentions toward email service switching.” Information & Management (43:7), 2006, pp. 884-93.
16. Klein. and Myers. “A set of principles for conducting and evaluating interpretive filed studies in information system.” MIS Quarterly (23:1), 1999, pp. 67-91.
17. Klemperer, P. “Market with Consumer Switching Cost.” The Quality Journal of Economics, May 1987, pp.375-394.
18. Kotulic, A. and Clark, S. “Why there aren’t more information security research studies ?” Information & Management, (41:5), 2004, pp.597-607.
19. Ross, C., Orr, E.S., Sisic, M., Arseneault, J.M., Simmering, M.G. and Orr, R.R. “Personality and motivations associated with Facebook use.” Computers in Human Behavior (25:2), 2009, pp. 578-586.

20. Williamson, O.E. (1985). The economic instructions of capitalism, Free Press.
21. Yin, R.K. (1994). Case study research: Design and Method. 2nd edition, Sage Publication.
22. 王凱，「由 McAfee 重新佈局台灣防毒市場談起」，MIC，2003，<http://mic.iii.org.tw/intelligence/reports>
23. 陳至哲，「我國資通安全產業發展趨勢及市場應用需求分析」，MIC，2002，<http://mic.iii.org.tw/intelligence/search/pop/show_reports>