東海大學企業管理學系碩士班

碩士論文

員工的工作情境相關態度與其遵循資訊安全政策之關聯性研究

An Empirical Study of the Effects of Organization Commitment and Job Satisfaction on Information Security Policy Compliance

指導教授： 張榮庭 博士

吳祉芸 博士

研究生： 劉昊雯 撰

中 華 民 國 一 百 年 七 月

論文題目：員工的工作情境相關態度與其遵循資訊安全政策之關聯性研究

指導教授： 張榮庭 博士
吳祉芸 博士
研究生： 劉昊雯

摘要

企業仰賴資訊系統與資訊科技來處理日常生活與工作的比重日漸增加，面臨資訊風險與資訊威脅的程度也隨之提升。過去資訊方面的相關研究，大多將心力放注在維護企業的資訊系統安全以及提出相對因應的策略，但最近漸漸發現員工的工作相關情境態度與組織資訊系統安全之間具有關聯性。

在本研究，將員工對資訊安全政策措施的行為意圖分為程序性控制措施的遵循意圖與技術性控制措施的採用意圖，探討工作滿意度、組織承諾和資安措施的態度這三項變數對員工行為意圖之影響，並且進一步比較三種態度對員工行為意圖的影響程度。

本研究採問卷調查法，利用滾雪球抽樣方式蒐集樣本資料，研究對象以需要仰賴電腦來完成大部份工作的員工為問卷主要發放對象，不限制產業以及部門。研究結果發現，資安措施的態度及組織承諾對員工遵循程序性措施的意圖與採用技術性措施的意圖有正向影響；工作滿意度對程序性措施的遵循意圖有正向影響。在員工的三種態度中，以資安措施的態度對資訊安全政策措施之行為意圖最具影響力。

相對於過去研究聚焦於資訊系統安全的因應措施與員工對資安措施的態度，本研究加入組織行為的工作滿意度與組織承諾兩項重要態度變數，並分別就資安政策中的程序性控制措施與技術性控制措施納入考量，希冀能幫助學術界與實務界對於資訊安全政策之遵循意圖與採用意圖的前因理解更臻完整。

關鍵字：資訊安全政策、資訊安全措施的態度、工作滿意度、組織承諾

Thesis：An Empirical Study of the Effects of Organization Commitment and Job Satisfaction on Information Security Policy Compliance

Advisor： Dr. Chang, Jung-Ting
Dr. Wu, Chih-Yun
Student： Liou, Hao-Wun

Abstract

Employees rely on information system and technologies to deal with daily work increasingly, and the issue of information security rise up as well. Most of past research focused on how to maintain information system security and propose some countermeasures. However, the interrelatedness between job-related attitudes and information systems was proposed recently.

We separate information security policies as compliance of information security policy and adoption of information security policy in this current work, and test and compare the effect of job satisfaction, organizational commitment and the attitude toward information security policy.

Data was collected from survey questionnaire by snowball sampling. The respondents should rely on computer for work from different industries and departments. The results showed that attitude toward to information security policy and organizational commitment were positively related to employee's behavioral intention, and job satisfaction were positively related to employee's compliance of information security policy. Overall speakin, the attitude toward to information security policy exerted greater effect on employee behavioral intention.

Keyword：Information security policy, attitude toward information security policy, job satisfaction, organizational commitment.

‘

謝誌

在研究所的這兩年時間真的過地相當快，彷彿才剛考上研究所，考慮該選哪一間學校，一轉眼之間，已經完成論文，即將踏出校門，邁向人生的另一條道路。這兩年之間，發生了許多事，包含歡笑、喜悅、生氣、悲傷，非常感謝陪伴在我身邊的每個人，這兩年來所經歷的每一件事，也讓我的個性更趨於成熟圓滑。

由於過去非企管相關科系的背景，讓我剛開始撰寫論文時曾經遇到許多瓶頸，感謝指導教授張榮庭老師與吳祉芸老師的悉心指導，謝謝榮庭老師不時的督促與叮嚀，讓我的論文能夠順利如期完成，謝謝榮庭老師總是不厭其煩地教導我；也要謝謝祉芸老師，感謝老師在我每一次遇到瓶頸時，總是能夠給予適時的幫助與提點，感謝老師在學業上與生活上的幫助。能夠在東海大學企研所遇到兩位老師，並且成為您們的學生，真的讓我感到莫大的榮幸與開心，很喜歡每次與您們 meeting 後的閒聊，老師不僅在課業上指導，也是我人生的導師，真的非常感謝您們。同時，也很感謝口試委員鄭菲菲老師、吳金山老師、應鳴雄老師能夠在論文口試時，不吝指正及給予建議，使得我的論文能夠更趨完善，在此再度謝謝老師。

謝謝我的好搭擋明琳，碩士班的生活有了妳，讓我們的生活多了許多歡笑，也讓枯燥的報告變的不再那麼討厭；謝謝振維，總是在我需要幫助時伸出援手；感謝大轉在我低潮時給我的關心；謝謝欣愉每次上量化時都幫我佔位子，能夠跟妳在同一個師門，讓我很珍惜這個緣份，相信妳一定會比我更出色；感謝寶貝熊的每一位好朋友，認識你們之後，讓我覺得以後很難再遇到像你們這麼好的老闆與同事了!感謝筱娟不論在大學或研究所時，總是幫我許多忙，真的麻煩妳超級多的!謝謝玲誼、曉穎、小關、肥滋滋、大支學長、大雄、小英你們的幫忙與關心，讓我更有動力向前邁進；謝謝淑華助教與倩華助教的幫忙，才能讓口試當天能順利圓滿結束；感謝每一位幫我填問卷的人，因為有你們的協助，才能使這本論文得以順利完成。

親愛的爸爸，雖然此時你已無法在我身邊看我取得碩士文憑，但我相信你在天上一定保佑著我們家的每個人，在此我要向你說一聲謝謝，謝謝你一直為這個家庭付出，你是一位偉大的父親，將今日的榮耀與您分享。感謝我的家人，謝謝你們包容我的任性，以及在撰寫論文時給予的幫助，因為有你們在身邊，才能讓我無後顧之憂的完成學業。最後，感謝一直陪在身邊的粉飾太平輝，在我讀研究所的這兩年真是辛苦你了，你知道的，一切盡在不言中。

要感謝的人真的很多，再次感謝在我生命中陪伴與關心過我的每一位朋友，謝謝你們的幫助，感謝大家！

劉昊雯 謹 識

於東海大學企業管理學系

2011 年 8 月

目錄

表目錄

圖目錄

第一章　緒論

隨著電腦的普及，人們生活中的日常活動與電腦愈來愈密不可分，尤其是公司的作業流程大部分需要仰賴電腦來完成工作。但是，對電腦的依賴度越大，也顯示了若公司電腦受到攻擊時，會使得公司資料有可能被洩漏，造成作業停擺，更嚴重地，甚至影響到公司的營運，這凸顯了資訊安全防護的重要性。接下來，會先介紹目前企業的電腦使用情形以及本研究的研究背景與動機及研究目的。

第一節　研究背景與動機

根據行政院主計處電子資料處理中心編印的「民國 98 年電腦應用概況報告」，直至 98 年底，我國個人電腦設置數達 1,215.8 萬台，其中家庭部門為 734 萬台，占 60.37％，政府機關企業學校有 481.8 萬台，占 39.63％，平均每千人擁有 525.9 台。表 1-1 為民國 94 年到 98 年的個人電腦變動數量，綜析民國 98 年底各機構使用個人電腦之普及率為 73.32％，其中政府行政機關、公營事業機構、公立研究機構等電腦設置比率均達 100.00％，民間企業則為 72.97％最低。由上述數據顯示，電腦已經越來越普及，人們在家中或公司時使用電腦來處理工作的比重相當大。

對電腦的依賴性越高，即表示暴露在資訊安全風險下的機率也隨著增加。根據行政院主計處直至民國 98 年底的統計資料，台灣私人企業共有 483,173 家，然而，民國 98 年受到資訊安全事件攻擊的公司就有 171,959 家，佔私人企業的 35.59％，比例高達三分之一！組織遭遇資訊安全事件外部攻擊以電腦病毒入侵佔大多數，其餘的依序為阻斷式攻擊(Distributed Denial of Service，DDoS)、被植入後門程式、資料遭竊或破壞、網頁被置換以及其它攻擊等，公司的重要資訊與機密文件可能就會在受到攻擊時遺失或被竊取，如果不建置完善的資訊安全防範措施，公司將暴露在很高的風險之下，嚴重地將影響到公司經營。

表 1-1　台灣個人電腦設置及使用概況

項目	94 年	95 年	96 年	97 年	98 年
個人電腦數					
家庭	5,621,369	6,149,480	6,464,956	6,816,476	7,340,414
機關、企業及學校	4,131,356	4,265,805	4,832,544	4,903,882	4,818,303
普及率					
家庭	63.09	66.09	67.11	69.24	70.48
機關、企業及學校	75.80	75.80	76.90	73.90	73.32

單位：台；%

資料來源：行政院主計處電子處理資料中心

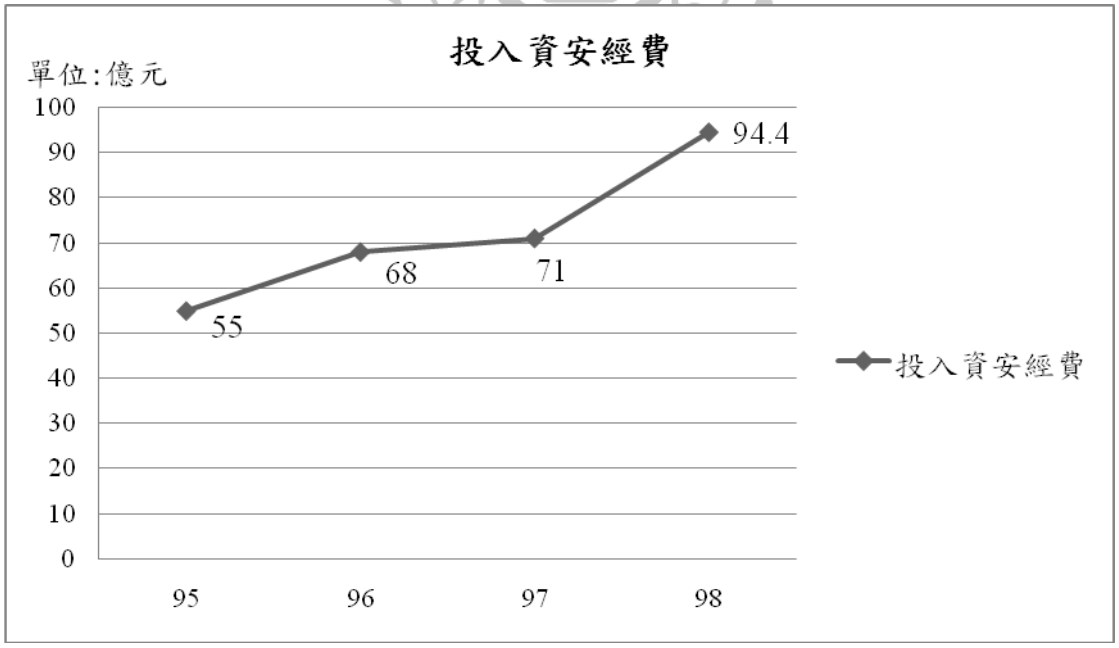

圖 1-1　95 年到 98 年台灣企業投入的資安經費

資料來源：行政院主計處電子處理資料中心

圖 1-1 是根據行政院主計處所統計的台灣各企業機關自 95 年到 98 年所投入的資安經費。95 年投入資安經費共 55 億元，96 年投入資安經費共 68 億元，97 年投入資安經費共 71.5 億，98 年投入資安總經費共 94.4 億元，投入的資安經費隨著時間逐漸增加，由此可看出對組織的資訊安全重視程度也是日益漸增。投入單位以一般民間企業投入的資安經費佔最高，民國 98 年一般民間企業所投入的資訊安全經費為 67.89 億。

企業過去使用紙本記錄與管理公司各項資料的情況已漸漸減少，現在的資料儲存與管理大多已電子化，資訊的傳播也愈趨發達及快速。自從電腦普及化後，資訊安全風險管理也是被廣為探討的領域，如果組織能夠找到降低或趨避風險的方法，那麼就能降低因為資訊安全所造成的損失。

過去的資訊安全相關研究大多專注在資訊安全的技術面，提出許多資訊安全的衡量標準及系統工具，但在管理層面的研究甚少(李東峰與林子銘,2001；Pahnila et al., 2007)。但現在發現，那些被授權可使用特定資訊系統或資訊設施的員工，往往給組織帶來很大的問題，因為這些員工忽視(ignore)、錯誤(mistakes)和惡意的(deliberate)行為會造成資訊系統安全的損害(Durgin, 2007；Lee and Lee, 2002；Lee et al., 2003)。組織內部遭受的資訊安全威脅有很大的一部分是由於人為因素破壞所造成，根據 CSI(Computer Security Institute) 2009 年的報導，組織內部職員利用公司網路上網或收發私人信件導致被攻擊的比例高達 30%，例如：上色情網站或非法接收未授權軟體。個人未經授權或經由特殊權力而取得公司資訊的比例也有 15%，上述皆顯示組織內部遭受員工攻擊的程度相當地高，而員工攻擊又分為惡意與非惡意攻擊，離職時故意將公司的機密文件攜帶散播出去即屬於惡意攻擊的一類；非惡意攻擊是指未受過電腦訓練的使用者與員工，這些使用者不清楚各種電腦安全的威脅，以致增加公司面臨的資訊安全風險(Information Security Risks)。圖 1-2、圖 1-3 分別為員工惡意攻擊與非惡意攻擊造成組織內部財物損失的比例，員工非惡意攻擊所造成的財損(65.8%)竟比員工惡意攻擊造成

的財損(43.2%)要來的高。另外，CSI 發現有 43.4%的公司，只撥出該年度資訊安全預算其中的 1%來提升員工的資訊安全教育，顯示了這些公司對員工的資訊安全相關知識的建立較不重視。

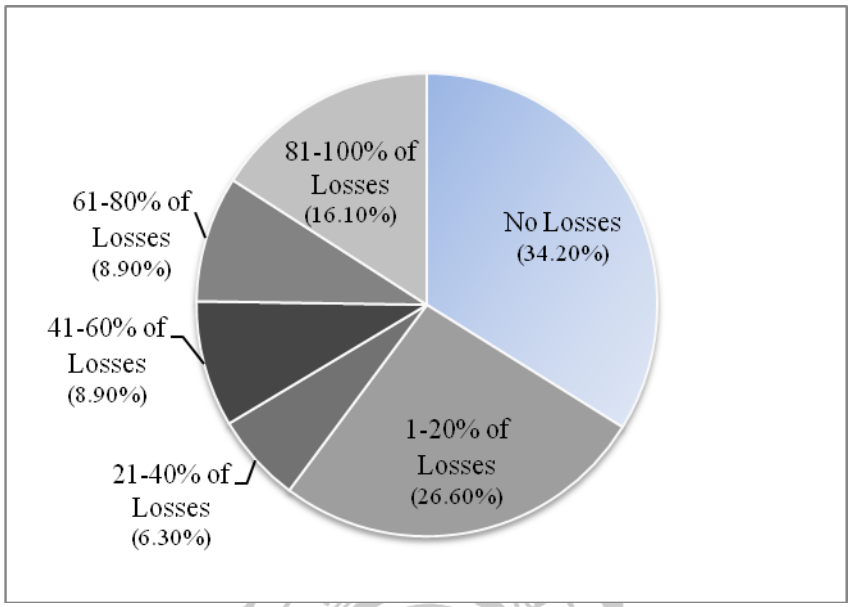

圖 1-2　員工非惡意攻擊造成的損失

資料來源：Computer Security Institute

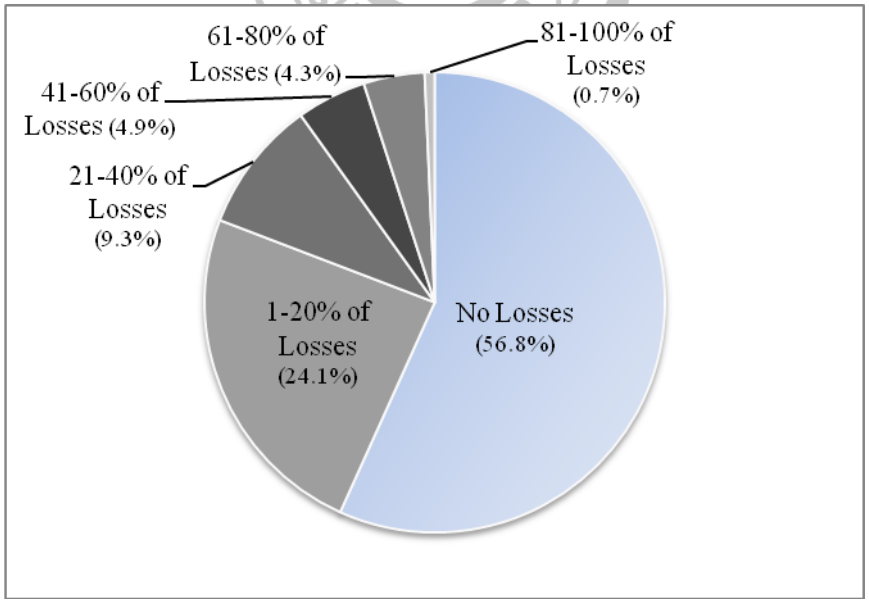

圖 1-3　員工惡意攻擊所造成的損失

資料來源：Computer Security Institute

由上述的資料顯示，除了公司的教育訓練、獎懲、員工本身對資訊安全政策的知識等因素會影響員工遵循程序性的控制措施與採用技術性的控制措施之外，員工對於工作帶來的滿足程度及其對公司的忠誠度，似乎也是有可能影響員工對資訊安全政策的行為意圖。工作滿意度(Job Satisfaction)與組織承諾(Organizational Commitment)為組織行為學(Organizational Behavior)兩項重要的態度變數，屬於工作情境相關變數，為員工對於自己的工作與組織的正反面態度。員工對工作的滿足程度越高，對工作也具有較正面的態度；Wiener(1982)認為組織承諾屬於一種內化的規範性壓力(internalized normative pressure)，可達到組織的目標和利益，員工對於自己的工作與組織具有較正面的態度，也能夠幫助組織有較好的績效成果(Randall, 1987)。

第二節　研究目的

除了建立員工對資訊系統安全的相關知識，員工對組織的正反面態度似乎也是影響員工行為意圖相當重要的因素，過去認為員工只要做好份內的事情與達成任務，就是一個好員工。如果員工跟組織的人相處的很好，讓大家工作氣氛很愉快；在同事面臨突發的狀況時，願意自動地幫助其他同事而不求回報，這些都是具有組織公民行為(Organizational Citizenship Behaviors)的員工所具備的特色。根據過去的研究(Organ and Ryan, 1995; Podsakoff et al., 2000; Williams and Anderson, 1991)，組織承諾與工作滿意度對組織公民行為具有正向且顯著的影響，也就是說，具有組織承諾與工作滿意度的員工他表現出組織公民行為的程度也會比較高。

隨著電腦普及程度越來越高，組織所面對的資訊系統的風險程度也相對的提高，在組織內部使用電腦來工作的員工相當地多，例如在過去工作時，公司的相關資訊或機密文件大多是以紙本型式存在，放置在安全的環境中保管；但是現在的資訊大多電子化，員工離職時將公司的機密文件攜出這種情形更是時有所聞。

大多數的組織花費大量的時間與資源，來預防、建立和監控組織內部的資訊系統安全。不過許多員工經常會做出故意違反組織內部資訊安全的決策，這是因為他們想要能夠更快速方便地執行他們的工作或增加他們自己的產出(Greene and D'Arcy, 2010)，這顯示了組織內部的員工表現出的違反行為可能是造成資訊系統安全事件的部分原因。因此，近來某些學者開始由行為面的角度去探討組織資訊安全措施(Bulgurcu et al., 2010)。

根據「理性行為理論(Theory of Reasoned Action)」(Fishbein and Ajzen, 1975)與「計劃行為理論(Theory of Planned Behavior)」(Ajzen, 1985, 1991)，個人態度會影響行為意圖，而行為意圖影響個人表現的行為。過去研究發現，員工對資訊安全措施的信念及態度會影響其對資訊安全措施的行為意圖(Yeh and Chang,

2007；Chang, 2010；Bulgurcu et al., 2010；Anderson and Agarwal, 2010)，因此，我們想要了解，員工除了資訊安全措施的態度會影響員工的對資訊安全政策的行為意圖外，另外，欲探討組織行為的兩項重要工作情境相關態度變數，「工作滿意度」與「組織承諾」對員工資訊安全政策的行為意圖之影響性。

另一方面，組織的資訊安全政策包含技術性與程序性的資訊安全控制措施。Straub and Nance(1990)認為有效的資訊安全應兼顧技術性與程序性的資訊安全控制措施。技術性的資訊安全控制措施包含預防性及處罰性的控制措施，例如：防毒軟體、防火牆、入侵偵測系統以及資訊安全相關軟硬體的建置或採用。程序性的資訊安全控制措施是指遵守資訊安全政策所規範的程序或規則，例如：系統當機的緊急應變程序、機密資訊分類方式、密碼編制規則、遵守組織所訂定的資訊安全相關命令、遵守相關法律與法規、按照時程更新系統與防毒軟體、在資訊安全事件發生時，按照組織規定的通報程序儘速通報。員工對資訊安全政策中的技術性及程序性的控制措施應有不同的行為意圖，故本研究擬出此研究的主要研究目的如下：

1. 瞭解員工對資訊安全政策的態度，對程序性控制措施的遵循意圖或技術性控制措施的採用意圖之影響。
2. 瞭解工作情境的相關態度：工作滿意度與組織承諾這兩項態度對員工程序性控制措施遵循意圖與技術性控制措施的採用意圖之影響。
3. 探討影響員工遵循程序性控制措施或採用技術性控制措施意圖的關鍵態度：在本研究中，三種態度變數對員工資訊安全措施遵循或採用意圖的影響，包含工作滿意度、組織承諾兩種工作情境相關態度以及員工的資訊安全措施態度，欲了解哪種態度對員工的程序性控制措施的遵循意圖與技術性控制措施的採用意圖影響最關鍵。

第三節　研究流程

本研究由具有初步想法構思到論文完成，可分為下列七個階段，如圖 1-4 所示：

一、　確認研究方向與主題

首先，先確認研究的方向與主題，主要與指導老師討論具有可探究性且尚未被研究的議題，並針對該主題的過去相關資料先做初步的了解與閱讀，藉由與老師的多次討論以及過去文獻中獲得啟發，最後確認研究題目。

二、　相關文獻探討研究

蒐集欲研究的主題過去文獻與相關資料，進行歸納與整理，每一項研究的論點基礎皆依據過去研究者的結果與實證而衍伸出來，回顧過去文獻除了了解欲研究主題相關的理論之外，另外，可產生進一步的想法啟發，提供穩固的立論基礎。

三、　建立研究假設與假說

根據文獻的回顧，提出研究的假設與假說，根據過去文獻做為假說的立論基礎，提出可能的假設與推導。

四、　問卷設計

提出研究假說之後，進行問卷設計。本研究採用問卷發放方式進行量化研究，問卷的設計是根據過去該領域的代表學者的研究問項而來。

五、　發放問卷

選定合適的研究對象發放問卷。

六、　問卷分析驗證

問卷回收後，進行信度驗證與因素分析，將資料進一步彙整與分析，看各構念之間的關係，並加以探討。

七、　結論與建議

由收集到的資料來驗證本研究的假說及假設，說明資料所呈現的發現與意涵，最後提出結論與後續的研究建議。

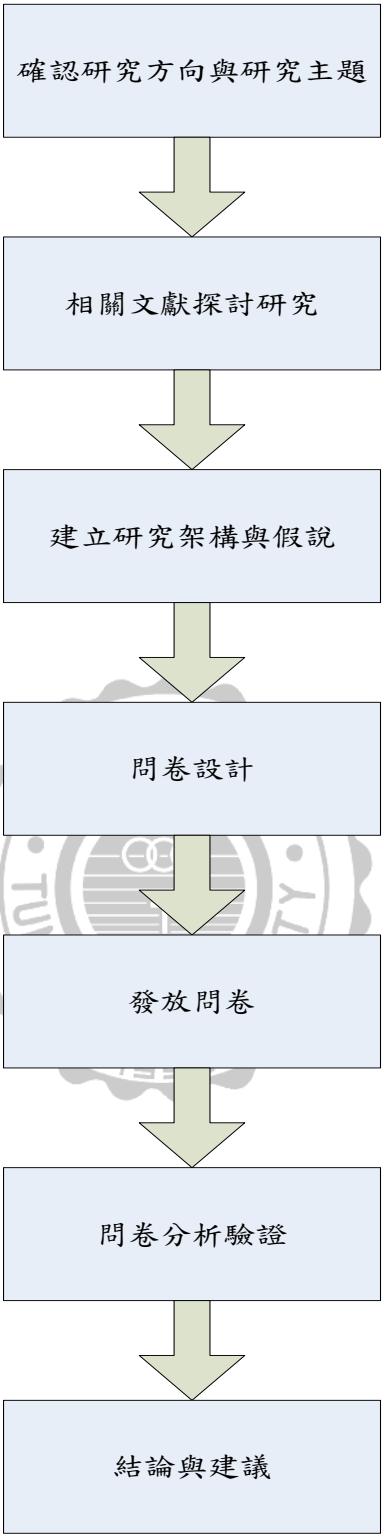

圖 1-4　研究流程圖

第二章　文獻探討

本章將針對資訊安全、工作滿意度和組織承諾等議題，蒐集整理過去的相關文獻及書籍資料，作為本研究的推導立論基礎，接下來，第一節先探討資訊系統安全(Information System Security)的定義與分類，第二節為資訊安全政策的分類，分為兩部份：第一部分為程序性的控制措施，第二部分為技術性的控制措施，第三節探討組織公民行為(Organizational Citizenship Behavior)的定義與理論基礎、第四節為工作情境相關態度的理論基礎與定義、第五節為資訊安全措施之遵循意圖及採用意圖。

第一節　資訊系統安全

隨著科技的蓬勃發展與進步，電腦在工作上扮演的比重日漸增多，我們的工作從文書處理、聯絡客戶、保存重要資訊甚至於維持公司的持續營運都與資訊安全有關，組織內部資訊安全部門負責的不只是防止駭客入侵與偵測病毒如此簡單而已，凡事與組織資訊有關的有形或無形的資訊，都應該受到妥善的保護與保存，即使要被銷毀時，也應該在安全且不被洩漏的環境中處理。

一、資訊系統安全定義

美國國家資訊系統安全詞彙(CNSS,2006)認為「資訊系統安全(information systems security)」是透過「資訊安全措施(security countermeasures)」來保護資訊系統的各個組成元素，偵測潛在的威脅並對抗，確保資訊在傳輸、儲存、處理時不被未授權者修改或存取。CNS 27002, X 6040，將資訊系統安全定義為：「資訊之機密性(confidentiality)、完整性(integrity)及可用性(availability)的保存；此外，亦能涉及如鑑別性(discriminative)、可歸責性(accountability)、不可否認性(nonrepudiation)與可靠度(reliability)等性質。」資訊的機密性是資訊不可揭露給未經授權的個人、個體或過程；完整性則是要保持資訊的準確度(accuracy)和完

全性(completeness)；而可用性為通過授權的個體可以使用及存取該資訊。

資訊系統應保護的主要元素有「硬體」、「軟體」、「資料」及「資訊服務」，這些元素具有不同的資訊風險(Straub and Nance, 1990)。Rainer et al., (1991) 將「資訊風險 (Information Risk)」定義為資訊系統相關資產的弱點 (vulnerability) 受到資訊威脅 (threats) 攻擊，造成資訊資產負面的衝擊。資訊(Information)的儲存方式可以紙本文件的有形方式收藏；也可使用電腦、磁片、DVD 或任何電子型式的無形方式保存。而 Gerber and von Solms (2005) 強調資訊風險分析時，必須同時兼顧有形(tangible)及無形(intangible)兩種資訊資產。

CNS 27002, X 6040 提出「資訊安全是使資訊不受各種廣泛的威脅之保護，以確保公司持續營運、將營運風險降至最低、得到最豐厚的投資報酬率及最大商機。」因此，當重大資訊被竊取或流出，可能會對組織的經營造成不可挽回的影響，當組織內資訊受到破壞時，公司應該要有明確的參考標準來回應問題及補救措施，才能使公司的營運快速回復正常。

Posthumus and von Solms (2004) 將資訊威脅分為「自然災害」、「技術問題」、及「人為因素」三種來源，而 White et al. (1996)歸納所有可能威脅，來自「內部安全(Internal security)」(系統面的安全)及「外部安全(External security)」(非系統面的安全)。自然災害像是地震、水災等重大突發事件；外部的威脅包含外來的駭客、病毒等惡意程式的攻擊；內部威脅包含電腦的相關硬體損害、協力廠商或員工的破壞、內部網路病毒的傳播等，如圖 2-1 所示。因此，資訊系統安全措施防止組織內部資訊系統受到天然災害與人為的破壞，降低營運風險並讓公司持續營運。

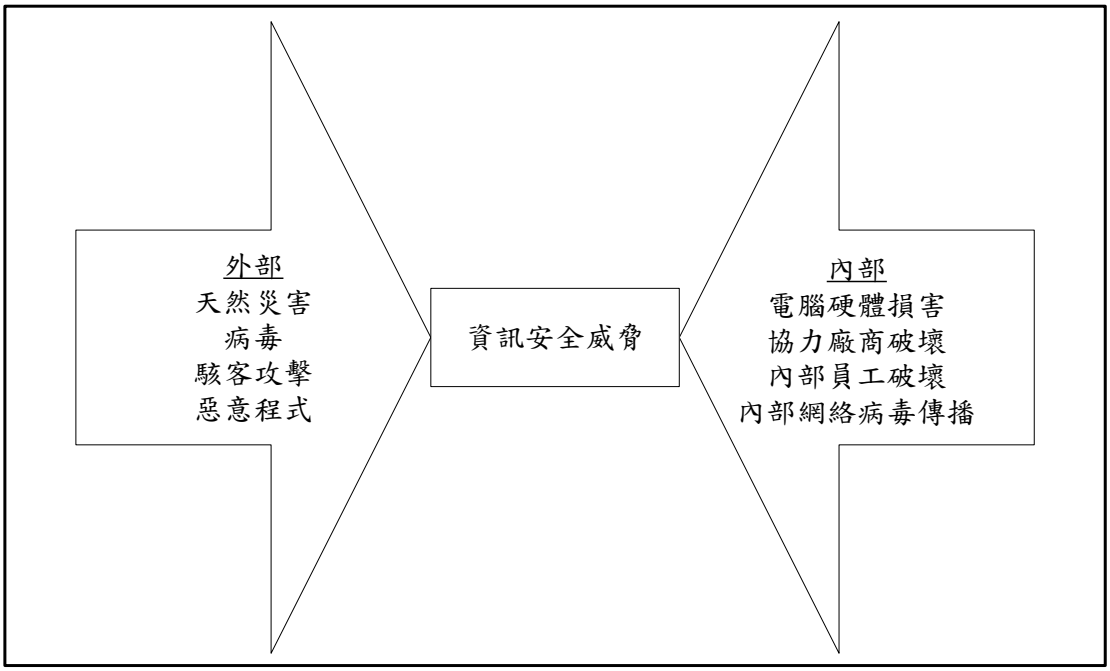

圖 2-1　資訊安全威脅來源

資料來源：本研究整理自台南大學資通安全防護網

二、BS7799 介紹

資訊系統的保存不只是硬體與軟體保護好即可，保護、使用資訊的相關人員與存取環境也都相當地重要，組織需要資訊安全措施來因應可能的資訊安全威脅，學術界、實務界提出許多衡量標準與解決資訊安全問題的方法，這些方法可以是預防性(preventive)或遏制性(deterrent)的措施(Straub, 1990; Straub and Nance, 1990; Forcht, 1994; Kankanhalli et al., 2003)。根據 Kankanhalli et al. (2003)研究，預防性措施如使用進階存取控制(advanced access control)、入侵偵測系統(IDS)、防火牆(firewall)、監視設施(surveillance mechanisms)等，以預防未授權者的入侵；而遏制性措施則屬被動性及管理性措施，如制定資安政策、教育使用者合法及非法的資源使用、定期及不定期的資安稽查。

BS7799 資訊安全管理系統(Information Security Management Systems，ISMS)是目前國際上許多公司採用的資訊安全管理標準，由英國標準協會(British Standards Institution，BSI)在 1995 年提出，希望提供明確建立、運作、監視、審

查、維持、及改進資訊安全管理系統(Information Security Management System, ISMS)的方式，使用規劃－執行－檢查－行動(Plan－Do－Check－Action, PDCA)循環模式，來建置所有 ISMS 的過程。包含 10 項衡量資訊安全的構面，分別為：安全政策(security policy)，組織資訊安全(organizing information security)，資產管理(asset management)，人力資源安全(human resources security)，實體與環境安全(physical and environmental security)，通信與作業管理(communications and operations management)，存取控制(access control)，資訊系統獲取、開發及維護(information systems acquisition, development and maintenance)，營運持續管理(business continuity management)，遵循性(compliance)等明確定義資訊安全管理系統的各項需求。經國際標準化組織(ISO)正式通過成為 ISO 27001:2005 資訊安全管理系統要求標準，為目前國際公認最完整之資訊安全管理標準。

BS7799包含兩部分，第一部分為BS7799-1， 1995年由BSI提出，為資訊安全管理的作業要點，為實務解(core of practice)，性質屬於參考文件，提供作業方式的指引，公司可以照該要點來實施，加強公司資訊安全程度，但是不能做為評鑑或驗證的標準。在2000年時，BS 7799-1通過ISO的審查，為ISO/IEC 17799: 2000，並在2005年再次審訂，為ISO/IEC 27002: 2005。2000年時，國內也將BS 7799-1納為國家標準，為CNS 17799, X6040。

第二部分是BS 7799-2，在2002年時首度提出，為資訊安全管理系統要求，給予組織驗證資訊安全，可做為評鑑和認證標準。之後BS 7799-2也發展為ISO27001：2005。國內的CNS 17800即是由BS 7799-2發展而來。BS 7799-2:2002發展成 ISO 27001:2005後，衡量資訊安全的構面由10項增加為11項，多了資訊安全事故管理(Information Security Incident Management)的衡量構面。控制作業也從36項增加至39項，原本有127項控管方法，也增加至133項(Societe Generale de Surveillance，SGS)。這十一項安全控制項目，可分為資訊安全政策的程序性控制措施與技術性控制措施。圖2-2為BS7799的發展流程：

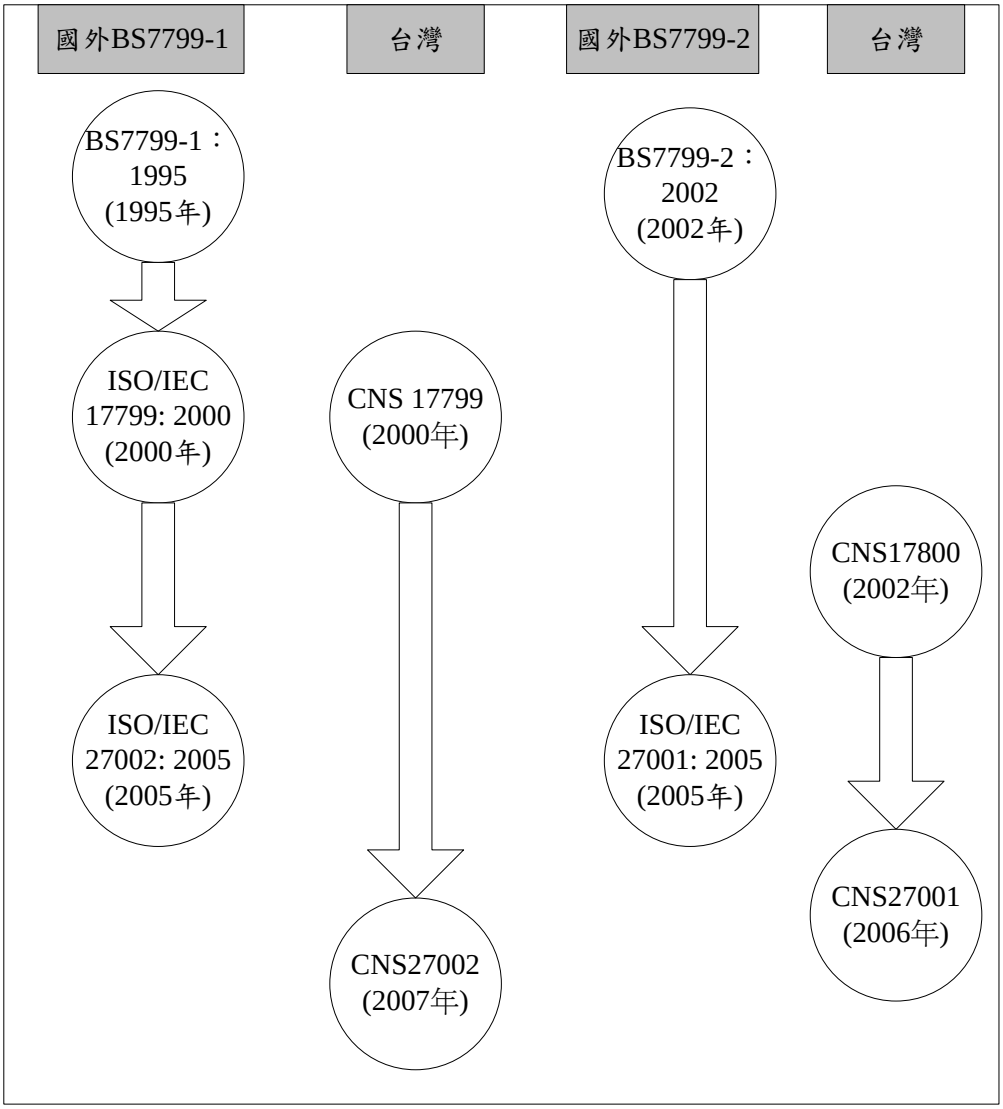

圖 2-2　BS7799 發展流程

資料來源：本研究整理

過去研究證實，在財務或金融相關產業會有較高的資訊需求，且資訊需求較大的產業也會較重視資訊安全(葉桂珍與張榮庭, 2006；Yeh and chang, 2007)，BS7799 大多用在金融業、保險業、高科技產業等擁有許多個人資料及高度機密資訊的產業，因這些產業有較高的資訊需求，有較高的資訊安全威脅，因此在國內已經有許多銀行導入 BS7799，來評鑑該公司的資訊安全。

第二節　資訊安全政策措施

由上一節資訊系統安全文獻探討可知，有效的資訊安全措施必須包含技術面與程序面的安全措施(Chang and Yeh, 2006)。Herath and Rao(2009)也提到，組織的日常活動仰賴資訊技術來完成，要達到組織資訊安全不能只從資訊技術單方面做起，還必須由政策(police)、步驟(procedure)、組織文化(organization culture)和個人在資訊安全中扮演的角色(the role individuals play in security)等非正式控制機制做起。接下來，本節將介紹資訊安全政策措施的定義與分類，再介紹資訊安全政策措施的相關理論。

一、資訊安全政策

有效資訊系統安全(Information System Security Effectiveness)應該包含系統面及非系統面的安全措施(Madnick, 1978)。資訊系統安全不應該只是技術面考量(Posthumus and von Solms, 2004; Chang and Yeh, 2006)。資訊安全政策定義為組織為保護該公司的資訊、資料、電腦相關設備、網路等重要資訊的機密性、完整性與可用性而訂定的相關法律或法規(BS7799)。資訊安全政策內有許多要遵行的措施，分為兩部分，一部分屬於程序性控制措施的遵循，另一部分屬於技術性控制措施的採用：

(一) 程序性控制措施的遵循（Compliance of Information Security Measures）

程序性控制措施的遵循是指員工願意維護組織的資訊系統安全，遵守組織訂定的資訊安全相關政策、程序、法令，例如員工願意遵照資訊安全政策所規範的程序或規則，避免違反任何法律、法令、法規或契約義務。

許多學者提出不同的立論觀點來解釋員工與資訊安全措施的關聯性，Herath and Rao(2009)提出員工自身的保護動機與嚇阻效果可以讓員工願意遵循公司的資安政策。Bulgurcu et al.(2010)以實證研究的方式，以計劃行為理論(Theory of Planed Behavior)與理性選擇理論(Rational Choice Theory)為立論基礎，發現除了

員工的資訊安全知覺(information security awareness)會影響態度(attitude)，態度還受到「遵循的利益」、「遵循的成本」、以及「不遵循的成本」三個角度影響，「遵循的利益」受到個體所感覺到的好處、安全性、及薪酬三個構面影響；「遵循的成本」是指遵守資訊安全政策而需要付出的成本，例如：遵守資訊安全的處理程序，導致需要更多時間來完成工作；而「不遵循的成本」由個體感覺到的成本、資產脆弱性、以及處罰所影響；而態度、規範信念(normative beliefs)、與遵循的自我效能(self-efficacy to comply)都會影響資訊安全政策的遵循意圖。Pahnila et al.以正增強與負增強的角度提出員工遵循資訊安全政策的原因，發現資訊的品質對員工實際的遵循(actual compliance)有顯著影響；威脅評價(threat appraisal)與促進條件(facilitating conditions)對員工的遵循態度(attitude toward compliance)有顯著影響；但發現制裁(sanction)與獎酬對員工遵循資訊安全政策的意圖無顯著影響。

(二) 技術性控制措施的採用（Adoption of Information Security Measures）

技術性控制措施的採用是指員工願意維護組織資訊系統的安全而去採用技術性的資訊安全措施，例如在電腦中裝設防毒軟體、防火牆、入侵偵測系統以及資訊安全相關軟硬體。

關於技術性控制措施，過去有許多學者提出可能影響員工對資訊安全措施的採用性，Chenoweth et al.(2009)提出，過去大部分科技採用模式都只專注在該項科技有幫助的角度來探討採用性，他們以保護動機理論來解釋員工願意採用保護科技(protective technology)的原因，研究結果發現知覺弱點(perceived vulnerability)、知覺嚴重性(perceived severity)、員工的回應效能(response efficacy)、回應成本(response cost)這四項會對技術性控制措施採用意圖有影響，但在此研究中，自我效能對於技術性控制措施的採用意圖無顯著影響。Lee and Kozar(2008)利用實證研究方式調查反間諜程式(anti-spyware)軟體的採用，以創新擴散理論(innovation diffusion theory)、計劃行為理論與資訊科技的倫理(ethic)與道德(morality)為該研究的理論基礎，結果發現，計劃行為理論的態度、主觀規範

(subjective norm)、與知覺行為控制(perceived behavioral control)對技術性控制措施的採用意圖皆有顯著影響，責任的推諉(denial of responsibility)也會對技術性控制措施的採用意圖有影響。

由資訊安全政策的程序性控制措施的遵循和技術性控制措施的採用相關文獻可知，理性行為理論、計劃行為理論、創新擴散理論、分解式計劃行為模式、科技接受模式會影響員工對於程序性控制措施的遵循與技術性控制措施的採用，將於以下分別介紹：

二、行為意圖相關理論

(一)理性行為理論(Theory of Reasoned Action，TRA)

根據 Fishbein and Ajzen(1975)提出的理性行為理論(Theory of Reasoned Action，TRA)，他們假設人為理性的前提之下，該思考是具有系統性地，並認為個人的行為表現會受到行為意圖的影響，個人的行為意圖決定於態度，行為信念是個人態度的前置因素，如圖 2-3 所示：

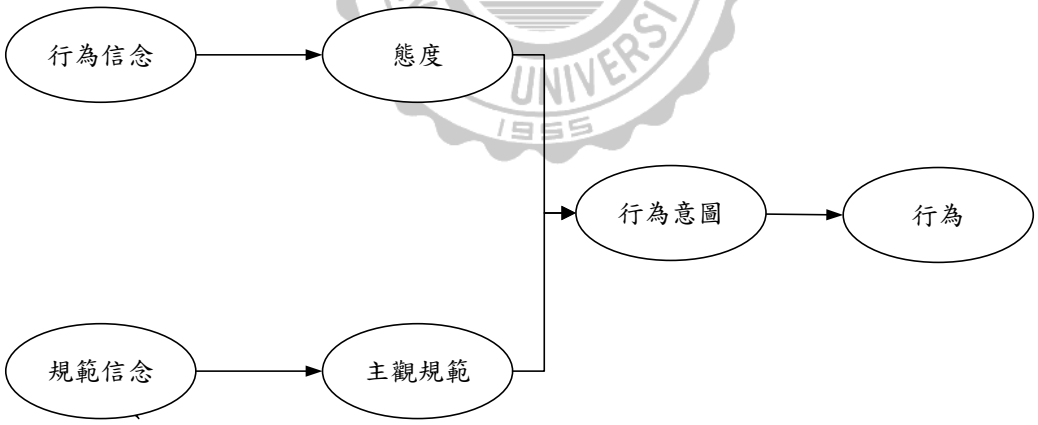

圖 2-3　理性行為理論

資料來源：Fishbein and Ajzen(1975)

(二) 計劃行為理論(Theory of Planned Behavior，TPB)

Ajzen(1985,1991)又根據理性行為理論提出計劃行為理論(Theory of Planned Behavior，TPB)，如圖 2-4，與理性行為理論不同的是，在計劃行為理論中，增加了知覺行為控制這項變數，來影響個人的行為意圖，即考慮個人主觀知覺對某特定行為控制的受限情況，此因素不但能夠透過行為意圖影響行為，也能夠直接影響行為。因此，計劃行為理論是個人的行為決定於行為意圖，態度、主觀規範與知覺行為控制會影響行為意圖，同時這三項因素之間也會互相影響。

以上這兩項理論為態度、行為意圖和行為之間的關係提供了良好的解釋，被廣泛應用於資訊科技的領域，包含員工遵循程序性控制措施的部分(Pahnila et al., 2007)。

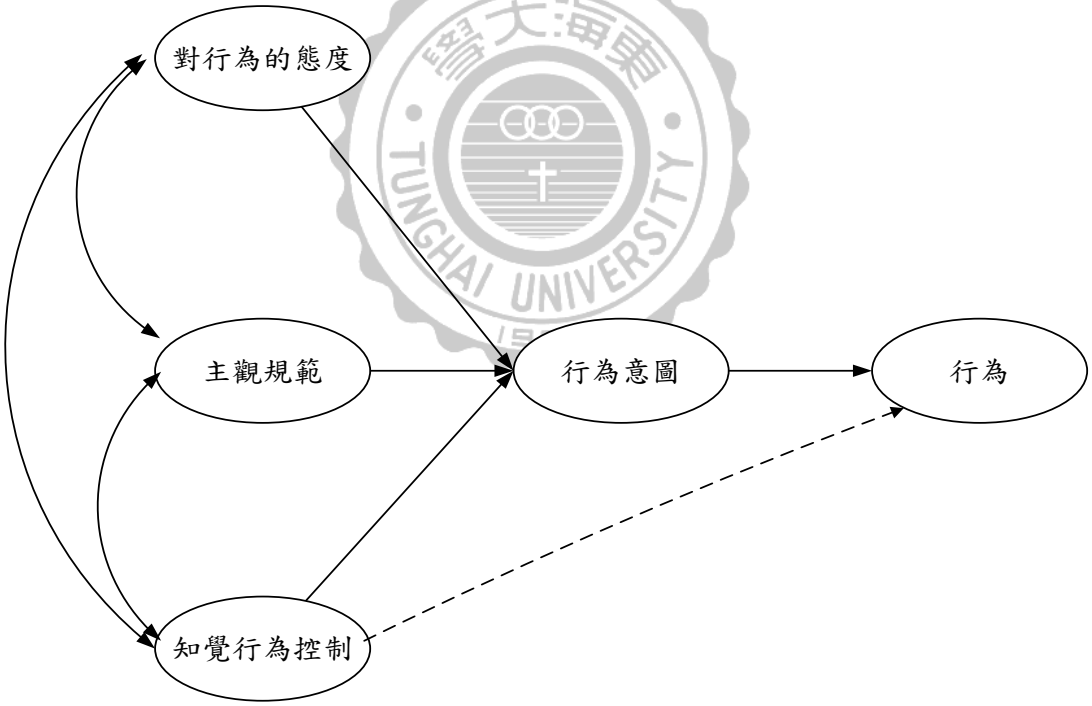

圖 2-4　計劃行為理論

資料來源：Ajzen(1985,1991)

(三) 創新擴散理論(Diffusion of Innovation)

由 Rogers (1983)提出，「創新(innovation)」是一個觀念、做法或事物被某個

人或某個團體認為「新的」時，這項觀念、做法或事物就是一種創新，創新的事物具有相容性(compatibility)、複雜性(complexity)、可試驗性(trialability)、可觀察性(observability)與相對優勢(relative advantage)五大特徵。「擴散(diffusion)」是指創新事物透過特定溝通管道，經由時間的流逝在某個社會體系中的成員之間互相傳播。傳統「創新擴散」研究典範(paradigm)提到潛在採用者的創新特質(personal characteristics)會影響他是否採用該創新科技；另外，也有提到一項創新科技採用包含認知(awareness)、說服(persuasion)、決策(decision)、執行(implementation)、確認(confirmation)這五個階段。潛在採用者先對該「創新科技」有初步的瞭解，然後進一步勸說自己並決策與採用，最後比較使用結果與預期的差距。「創新擴散理論」假設一個「創新科技」被採用的過程是一連串不確定的降低及資訊的匯集，透過採用者的社會化過程，將創新科技的特質與功能的透過特定溝通管道傳遞給潛在的使用者，經由使用的預期結果來評估對此創新科技的採用行為。簡而言之，一項創新科技的被採用的原因包含採用者個人特質(individual user characteristics)(Brancheau and Wetherbe, 1990; Agarwal and Prasad, 1998a, 1998b; Agarwal and Karahhanna, 2000)、創新科技的資訊來源與溝通管道(information sources and communication channels) (Nilikanta and Scammell, 1990)、創新科技本身特質(innovation characteristics) (Hoffer and Alexander, 1992; Moore, 1987)。

(四) 分解式計劃行為模式(Decomposed TPB, DTPB)

由 Taylor and Todd(1995)提出分解式計劃行為模式(Decomposed TPB, DTPB)」，結合 Fishbein and Ajzen(1975)的「理性行為模式（TAM）」、Ajzen(1985,1991) 提出的「計劃行為理論(TPB)」兩種模型，以及創新擴散理論的特性(Rogers, 1983)，將「計劃行為理論」中「態度」、「主觀規範」、及「知覺行為控制」三個構念因素分解。

在「分解式計劃行為模式」中，愈高的「知覺到的相對優勢(perceived relative advantages)」和「適合性(compatibility)」以及愈低的「複雜性(complexity)」將個

人對某科技的使用有更正向的「態度」;個人的「主觀規範」會受到「同儕(peers)」、「上司(superiors)」、及「下屬(subordinates)」這三個重要結構關係的社會壓力，而產生符合他們所期望的行為意圖。就「控制信念」構念，依 Ajzen (1985, 1991) 被分解成個體內部之「自我效能(Self-efficacy)」及外部的「資源便利性 (Resource Facilitating Condition)」兩個結構。「自我效能」意謂個體主觀知覺使用科技的能力(ability)，較高的自我能效能將會有較高的採用意圖；而「資源便利性」包含時間、資金資源，及科技能力(Technology Capability)，愈多時間及資金資源和愈高的科技能力，將有較高的採用意圖，分解式計劃行為模式如圖 2-5 所示：

分解式計劃行為模式用來了解使用者採用資訊科技的行為，比起科技採用模式多了主觀規範、電腦自我效能等因素，對評估影響員工採用資訊科技的因素更準確。

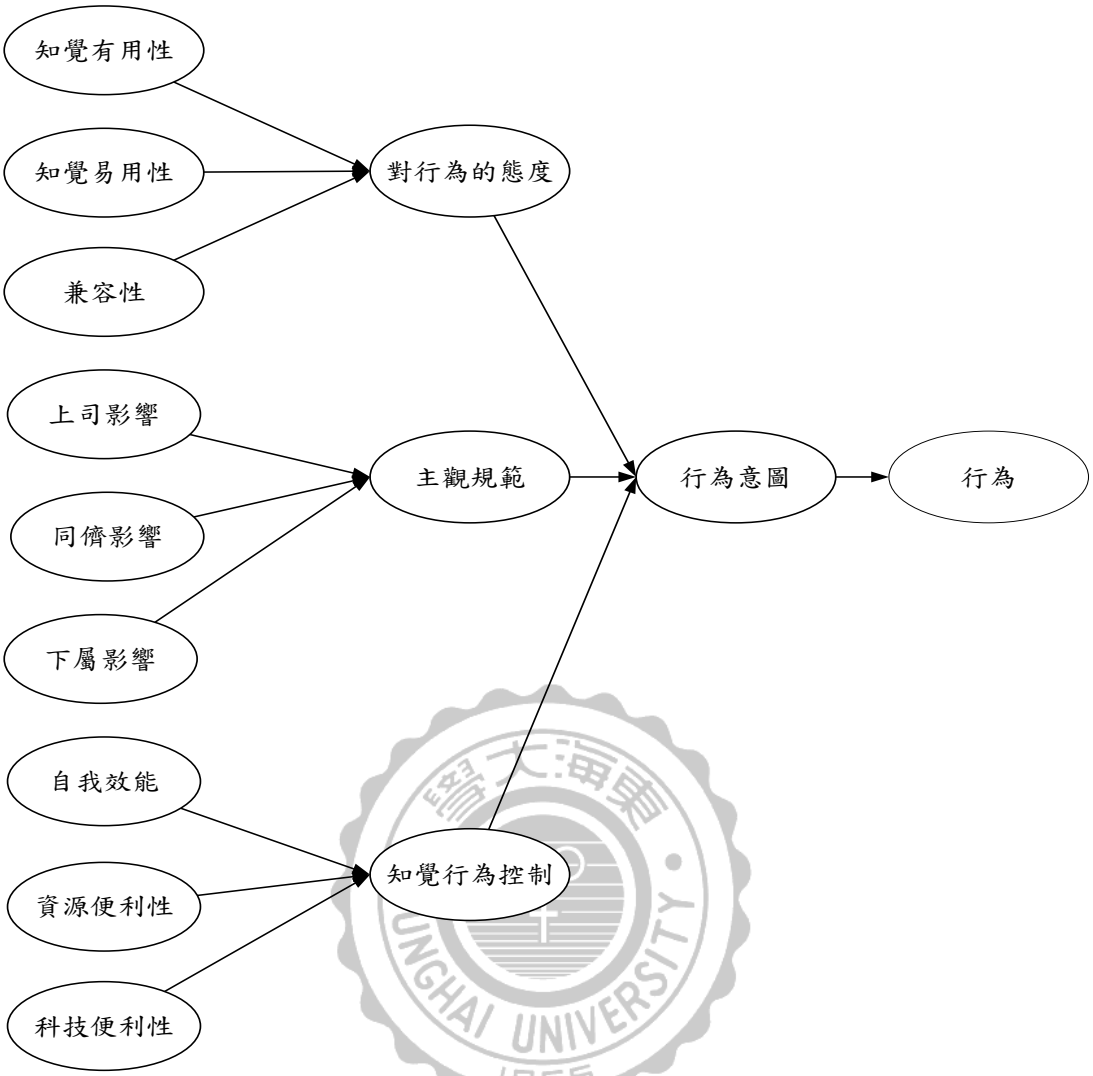

圖 2-5　分解式計劃行為模式

(五) 科技接受模式(Technology Acceptance Model，TAM)

由 Davis 在 1989 年提出，科技接受模式是根據 Fishbein and Ajzen(1975)的理性行為理論發展而來，在提出該理論之前，過去的研究沒能有一個明確衡量使用者對於系統的接受度。Davis 提出知覺有用性(Perceived Usefulness)與知覺易用性(Perceived Ease of Use)這兩個因素，認為這兩項因素對於資訊科技(Information Technology，IT)的接受程度有很大的影響，如圖 2-6 所示，知覺有用性可定義為潛在使用者相信使用一個特定的新科技可以提升自己的工作績效;知覺易用性則為潛在使用者感覺學習一項特定新科技的容易程度(Davis, 1989)。研究結果發現，第一，知覺易用性會影響知覺有用性換言之，個人覺得學一項新科技很容易，

則會增加個人對該項新科技的知覺有用性。第二，知覺有用性比知覺易用性更重要，當個人覺得一項新科技有用，比感覺這項新科技容易學習更願意接受。

若使用者感覺到新科技的易用性或有用性，則會願意去學習該項新科技，抱持正面的態度。

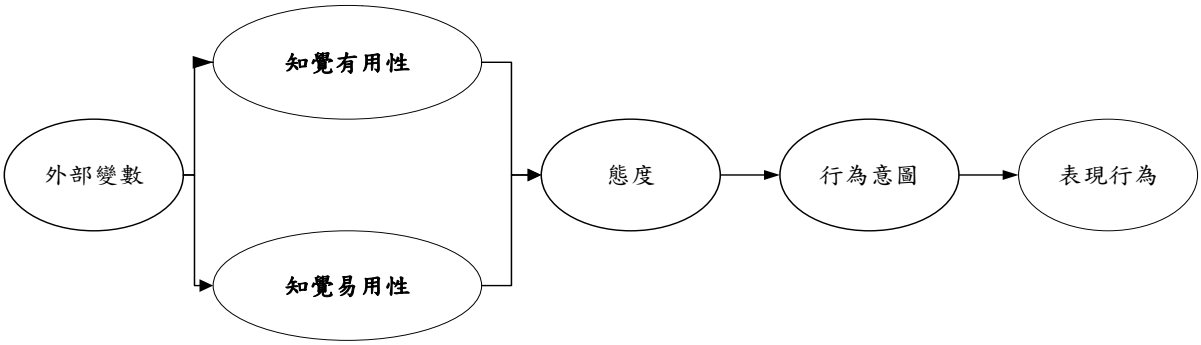

圖 2-6　科技接受模式

三、影響執行資訊安全措施的意圖之重要因素

(一) 自我效能(Self Efficacy)

為社會認知理論(Social Cognitive Theory，SCT)中的概念(Bandura, 1986)，最早由 Bandura(1977)提出，屬於一種信念，他認為每個人具有一套認知系統，此系統對新任務有評估與解釋的過程，自我效能可定義為個人對於自己具備的能力是否能夠達成某特定任務的信念，這項信念可以激勵人完成目標。

Bandura 提出效能的運轉機制，他認為人會受到預期效能(efficacy expectations)的影響而表現出行為，也就是說，個人表現的行為是透過評估自己的能力與知識，是否有能力可達成該任務，在這過程中，也會評估表現的行為可能帶來的預期結果(outcome expectations)，最後得到結果。如圖 2-7。

Bandura 提出自我效能不只是個人具備的能力與成就表現等個人因素，還會受到外在環境的影響，因此，自我效能是這三項因素交互作用後的結果，經此機制所產生的個人自信心會決定動機的高低，因此，自我效能會因任務、事件的不同而有所差異。

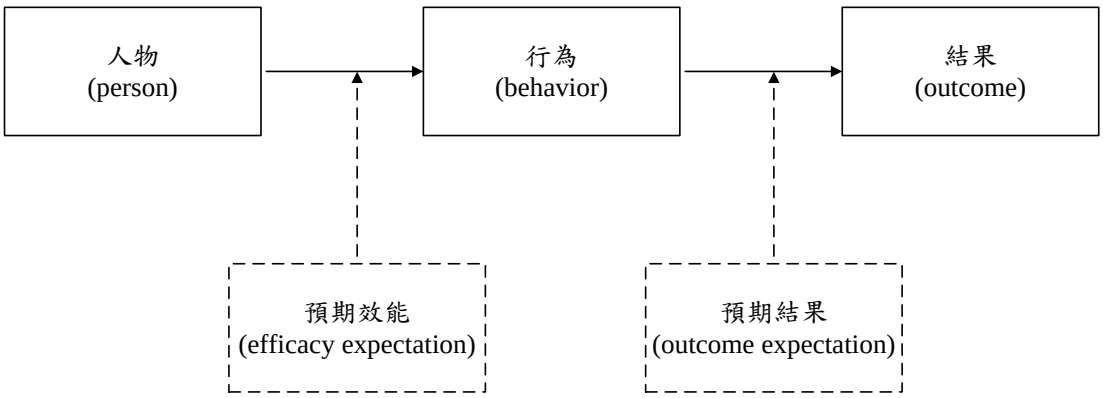

圖 2-7　預期效能與預期結果影響自我效能

資料來源：Bandura(1977)

(二) 主觀規範(Subjective Norm)

最早是由 Fishbein and Ajzen(1975)在理性行為理論(Theory of Reasoned Action，TRA)中提出，將主觀規範定義為個人感受到周遭人給予的期望行為造成的社會壓力，而決定去做或不做某個行為，這些社會壓力通常是來自於對個人有影響的重要人士，1995 年 Taylor and Todd 將科技接受模式與計劃行為理論結合，提出分解式計劃行為理論，提到主觀規範會受到上司和同儕的影響。

(三) 對資訊安全措施的態度(Attitude to Information Security Measures)

最早由 Fishbein and Ajzen(1975)在理性行為模式與計劃行為理論(Ajzen,1985/1991)提出，態度會影響行為意圖，進而影響個人的行為表現。對某行為的態度可定義為個人對於採取該行為時表現出的正面或負面的評價。影響個人對於某行為抱持正面或負面的態度的前置因素很多，茲說明如下：

1. 自我效能

過去許多的研究發現，在公司中自我效能愈高的員工，會對資訊安全政策有正面的態度(Anderson and Agarwal, 2010; Herath and Rao, 2009; Johnston and Warkentin,2010)。

2. 資訊安全知覺(Information Security Awareness)

員工的資訊安全知覺在資訊安全的管理中是非常重要的一部分(Cavusoglu et

al., 2009)，員工遵循程序性控制措施或採用技術性控制措施得到的好處、需要付出的成本及不遵循程序性控制措施或不採用技術性控制措施時必須付出的成本這三項因素都會影響員工對於資訊安全措施的態度(Bulgurcu et al., 2010)。

第三節　工作情境相關態度

在公司內，員工對於公司發佈的政策命令會隨著個人的信念而展現出不同的態度，根據 Fishbein and Ajzen(1975)提出的理性行為理論(Theory of Reasoned Action，TRA)，他們假設人為理性的前提之下，該思考是具有系統性地，並認為個人的行為表現會受到行為意圖的影響，個人的行為意圖決定於態度，行為信念是個人態度的前置因素，如圖 2-2 所示。

既然行為是由行為意圖而來，而行為意圖又是由個人的態度所產生的，在此節針對可能影響員工執行資訊安全的行為意圖之態度變數：(1)工作滿意度(2)組織承諾和(3)工作滿意度和組織承諾與組織公民行為的關係進行文獻回顧，分別說明如下：

一、工作滿意度

(一)工作滿意度的起源與概念性定義

工作滿意度(Job Satisfaction)又稱為員工滿意度(Employee Satisfaction)，顧名思義，是衡量員工對於自己的工作之滿意程度，其衡量的範圍不單是工作本身，也包含了工作相關環境、人際關係、工作自主性等，此議題過去在組織行為領域方面被廣泛地研究。

在 1930 年以前(吳定等人, 2010)，當時的環境動盪不安，人們謀生不易。而當時的員工薪資高低決定於他的產出數量，因此，在當時許多學者提出了許多能夠提高員工的生產數量的方法，像是科學管理學派的泰勒(Taylor)、管理程序學派的費堯(Fayol)…等，他們提倡利用獎金做為誘因來提高生產力；或是將工作分割，再專業分工，使每位員工的動作簡單化，增加生產效率，這個時期稱為傳統理論時期，著重在生產效率與產量上，而忽略了員工的心理層面，把員工當為生產的機器。

1930 年以後，行為科學的興起，進入另一個新的階段(吳定等人，2010)，霍

桑實驗研究的提出，開始讓大家重視到員工的心理層面。霍桑實驗(Hawthorne Experiments)為西方電氣公司與美國國家科學會研究委員會(National Research Council of the National Academy of Science)合作，原本研究工廠內的照明度與工人生產效率間的關係，，但發現照明度減低，工人的生產力反而增加，無法將照明度與工人的生產力找出明顯的關聯性，之後由哈佛大學教授 Mayo、Roethlisberger、西方電氣公司的 Dickson 以及另一間學校的 Whitehead 一起共同參與此實驗，實驗部分包含三項內容，分別為：(1)繼電器裝配工作實驗(Relay Assembly Test Room Experiment)(2)面談計畫(Interview Program)(3)配電器捲線作業觀察(Bank Wring Observation Room)，自 1929 年開始研究，一直到 1932 年結束(Mayo,1971)。霍桑實驗開啟了後世管理學者對員工內心層次的注意，也發現到員工的生產力除了受到薪資的影響之外，還會受到心理因素與非正式群體(informal groups)的影響，這是最早注意到員工的心理層面與滿足程度的實驗。

工作滿意度最早由 Hoppock(1935)提出，定義為「員工在工作時，於生理上與心理上兩方面對工作環境與工作本質的滿意程度。」Vroom(1964)將工作滿意度定義為「員工對於自己在工作岡位上所扮演的角色的感受與情感反應。」Locke(1976)認為工作滿意度為多個面向組成，定義為「個人評估自己的工作和工作經驗產生正向或快樂的情緒反應。」Spector(1997)認為工作滿意度是「員工藉由許多面向來評斷自己是否喜歡該工作。」許士軍(1991)將工作滿意度定義為「一位工作者對於其工作所具有的感覺或情感性反應。」

(二)工作滿意度相關理論

自工作滿意度提出之後，許多學者紛紛提出影響員工工作滿足的理論，研究者將與工作滿意度相關的理論整理如下表 2-2 所示：

表 2-1　工作滿意度相關理論

理論	提出者	定義
1. 馬斯洛需求理論 (Hierarchy of Needs Theory)	Maslow, 1943,1954	馬斯洛以穆萊(Murray,1938)提出的「先位」和階層觀念，將人的需求分為五個階層，由低→高依序為：生理、安全、社會、尊敬與個人實現這五個階層，並主張人在低階層需求得到滿足後才會追求更高階層的需求。
2. 雙因子理論 (Two-Factor Theory)	Herzberg, Mausner & Snyderman,1959	工作情況分為「激勵」與「保建」因子。 「保健因子」包含：公司政策、技術監督、公司內部人際關係、薪資、工作保障、個人生活、工作環境與地位。 「激勵因子」包含：成就、器重、升遷、工作本身、成長可能性、責任。 Herzberg et al.(1959)他們認為「保健因子」的存在，不一定能使員工感到滿足，但不存在，則會感到不滿足；而「激勵因子」的存在，可讓人感到滿足，若不存在則不會使人感到不滿足。
3. 公平理論 (Equity Theory)	Adams,1963	Adams(1963)認為公平是指人們處於一種「交換關係」(Exchange Relationships)情況中，人在一方面付出代價，稱為「投入」；而另一方面也有得到收獲，稱為「結果」。在「投入」和「結果」之間構成比率，若比率相等，則此時人會感覺最滿足。

資料來源：研究者整理自許士軍「管理學」(1991)

(三)工作滿意度衡量量表

在組織行為領域中，有許多學者發展了衡量工作滿意度的問卷，但衡量的方向也都各有自己的論述，目前尚無能將所有與工作滿意度相關的因素都納入問卷之中，Spector(1997) 在 Measurement of human service staff satisfaction: Development of the Job Satisfaction Survey 一書中，將自己提出的工作滿意度調查(The Job Satisfaction Survey，JSS)與其他學者的量表說明與比較。在此篇研究中，將較多學者選擇使用的量表分別介紹如下：

1、工作滿意度調查(The Job Satisfaction Survey，JSS)

由 Spector(1985)提出，工作滿意度調查的衡量面向包含薪酬(pay)、晉升(promotion)、監督 (supervision)、額外福利(fringe benefits)、績效獎酬(contingent rewards)、工作情境(operating conditions)、同事(coworkers)、工作本質(nature of work)以及溝通(communication)九個構面，每個構面以四個問項來衡量，共 36 個問項，包含正負問項，每一個問項給 1~6 分，1 分表示非常不滿意， 6 分表示非常滿意，以此類推，總分會介於 36 分~216 分之間。

2、工作描述指標(The Job Descriptive Index，JDI)

由 Smith et al.,(1969)一起編製而成，衡量的構面為工作(work)、 薪酬(pay)、晉升(promotion)、監督 (supervision)以及同事(coworkers)五個構面的滿意度，整份問卷包含 72 題問項，工作、監督和同事的題項各 18 題，薪酬與晉升的題項各 9 題，而每個問項的回答包含「是」、「不確定」、「否」這三個選項。

3、明尼蘇達滿意度問卷(Minnesota Satisfaction Questionnaire，MSQ)

由 Weiss et al. (1969)編製而成，此問卷被許多研究者廣泛使用。問卷分為長式與短式，由 20 個構面衡量工作滿意度，長式問卷每構面皆有五個題項來衡量，總共 100 題；短式問卷有 20 題，使用最能代表該構面的問項來衡量，一問項代表一構面。這 20 個構面衡量工作外在滿意度與內在滿意度，外在滿意度關注的是工作本身，像工作環境、薪資；內在滿意度關注的是員工對於工作的內心感受。

二、組織承諾

(一)組織承諾定義

組織承諾(Organizational Commitment)又被稱為「組織歸屬感」、「組織忠誠」，過去許多學者對組織承諾提出不同的定義，Porter et al.(1974)認為組織承諾是個人認同自己屬於組織的一份子，且願意為組織的目標而努力。Steers(1977)將組織承諾定義為個人對於某一組織的認同感與投入程度。Mowday et al.(1982)將組織承諾定義為個人對特定組織的認同和投入。Morrow(1983)認為組織承諾是個人深信該組織所訂定的目標與價值，並有強烈的接受度。Robbins(1998)認為是個人認同特定組織及組織目標，並希望能維持組織成員的身分。總括來說，具有組織承諾的員工能夠認同組織的目標，且願意付出心力來達成組織的目標，對組織有強烈的認同感與歸屬感。

(二)組織承諾相關理論

1、Steers 組織承諾前因後果模式

由Steers(1977)提出的組織承諾模式，將其分為前因(antecedents)與後果(outcomes)。前因部分屬於自變項(independent variable)，預測組織承諾的程度高低，包含個人特質、工作特性與工作經驗，個人特質像是教育水準、年齡，工作特性包含是否具有挑戰性、工作的回饋程度等工作屬性，工作經驗則是指組織的可靠程度及組織對員工的重視程度；後果部分屬依變項(dependent variable)，包含出席率(attendance)、留職意願(desire to remain)與工作績效(job performance)三項。

2、Mowday、Porter and Steers 組織承諾因後果理論模式

由Mowday et al.(1982)提出，他們認為組織承諾的前因變項有4項，分別為：個人特徵、角色特徵、結構性特徵與工作經驗，個人特徵為個人的年齡、教育程度等個人資料；角色特徵像是工作範圍及挑戰性、角色衝突、及角色混淆等；結構性特徵包括組織規模、控制幅度(span of control)、正式化(formalization)、分權

程度、及決策參與程度等等，工作經驗結果變項：包括工作績效、年資、缺勤、怠工及離職、組織可依賴性(organizal dependability)、個人重要性、期望程度、群體規範等等。後果變項則包括：工作績效、留職意向、留職願望、出席及留職。

(三)組織承諾量表

1、組織承諾量表(Organization Commitment Questionnaire, OCQ)

由 Porter, Steer 和 Boulian(1979)發展出的組織承諾量表(OCQ)，是目前最被廣泛使用的組織承諾量表，測量組織成員在態度與實際行動上的投入程度，衡量面向包含「對組織的認同與接受度」、「願意為組織投入心力的意願」、「離職傾向」三個面向。組織承諾量表分為長式與短式版本，長式短本包含 15 題項，短式版本包含 9 題項，刪除的 6 題項為測量離職意項，本研究選擇組織承諾量表的長版本為問卷來源。

2、Allen and Meyer 的組織承諾量表

Allen and Meyer (l990)制訂的組織承諾量表包含三部分，分別為情感性承諾(affective)、持續性承諾(continuance)和規範性承諾(normative)，每個部分包含8 題問項，共 24 題。情感性承諾是組織成員出於自願希望繼續留在組織服務；持續性承諾為有關離開組織可能付出的成本之認知，使成員想繼續留在組織中的承諾，通常員工想離開原有的組織時，會由兩方面來決定對組織的持續性承諾，第一，衡量外在就業環境的工作機會，第二，若離開公司，需要付出的成本有多少；規範性承諾是指對組織的忠誠，在員工心中產生想報答組織的想法。

(四)組織承諾與員工遵循或採用資訊安全政策措施之關係

員工對組織的承諾與其採行之組織安全行為應有密切關係(Herath and Rao, 2009)。若員工具備組織承諾，會反應在公民行為上。過去文獻提到，當組織成員的組織承諾高，他們比較不會讓組織的系統處於有風險的狀態，也不會做一些適得其反的電腦行為。例如，使用組織系統去瀏覽網頁、寄個人的信件及玩遊戲等(Herath and Rao, 2009; Stanton et al., 2003)。因此，就組織的資訊安全而言，具

有較高組織承諾的員工，可能具備較高的安全意識及安全行為，同時較高的可能性達成組織期望的資訊安全目標。

三、工作滿意度和組織承諾與組織公民行為的關係

組織公民行為的涵義最早是由 Barnard (1938)所提出，他提出了在組織內工作的人「合作」的觀念。1978 年 Katz and Kahn 在 The Social Psychology of Organizations 一書中將組織中的正式角色行為劃分為角色內的行為(In-Role Behavior)和角色外的行為(Extra-Role Behavior)。角色內的行為即為個體必須完成該職務所包含的任務，而角色外的行為則是義務規範外的行為。Smith et al.(1983)提出組織公民行為此名詞後，由 Organ(1988)將組織公民行為定義為個體的自主行為能夠提升組織的效率及效能，這些自主行為的產生不要求任何條件且與組織的正式獎酬系統無關。依據 Katz and Kahn(1978)的說法，一個有效的組織運作，不只需要員工做好「份內」的事(In-Role Performance)，還有許多行為是既定義務規範以外的(Extra-Role Performance)。

Organ(1988)主張組織公民行為是組織維持永續生存所必需，具有組織公民行為之「盡職行為(Conscientiousness) 」特質的員工對於上司指派的任務，其所達成任務的結果績效比上司所期望的還要更好。Organ 更在文中詳盡闡述組織公民行為能將員工和組織達到最大的工作效率和生產力，進而提高組織的績效，例如：增加組織的銷售業績(Posdakoff and MacKenzie, 1994)、增加生產力及產品品質(Podsakoff and MacKenzie, 1997)、以及顧客服務的品質(Bell and Menguc, 2002)。 Yoon (2009) 研究發現「組織公民行為」是有助於「企業資源規劃(Enterprise Resource Planning，ERP)」系統的採用，由此可知組織公民行為有助於一項新科技的導入。

行為研究領域的文獻顯示，員工對組織及工作的態度被認為是「組織公民行為」的重要預測變數(Organ and Ryan, 1995; Podsakoff et al., 2000; Williams and Anderson, 1991)。Williams and Anderson (1991)提出「工作滿意度」為角色外行為

的良好預測者； Bateman and Organ (1983)也發現「工作滿意度」是最常被用來檢測組織公民行為的變項。當員工愈滿意其工作，及對其組織較高承諾，則其表現出的公民行為更明顯。另外，當組織內部具有較多公民行為時，將有助於組織的政策及規範的推行(George and Jones, 1997; Smith et al., 1983)。

第四節　資訊安全政策之遵循意圖及採用意圖

以前認為影響組織的資訊安全程度或潛在的威脅，大部分的人較不會想到與員工的表現行為有關(Bulgurcu et al., 2010)，組織大多採用的資訊安全防護措施以基本的科技技術或設備來減少風險以及確保資訊安全(Ernst and Young, 2008)，容易想到的基礎設備像是與資訊安全有直接相關的防火牆、硬體設備、防毒軟體等。Rogers(1975)表示如果個人對提出的建議採取適當的態度和行為即可以避免危險。Bulgurcu et al.(2010)提出員工願意遵循資訊安全的規範(Information Security Policy，ISP)是增加組織資訊安全的關鍵要素。

員工的資訊安全措施行為意圖可以大致分為兩方面：程序性控制措施的遵循意圖和技術性控制措施的採用意圖。程序性控制措施的遵循意圖包括對組織頒布的資訊安全命令、要求、法律、法規和法令的遵守；技術性控制措施的採用意圖是指員工願意維護組織資訊系統的安全而採用技術性控制措施。

由第二節的資訊安全政策措施可知，過去研究已證實態度、主觀規範、自我效能、知覺行為控制都會對個體的行為意圖造成影響，而組織行為學領域的研究指出，個體對工作及組織的態度是會影響個體是否會具備組織公民行為(Organizational Citizenship Behavior) (Organ and Ryan, 1995; Podsakoff et al., 2000; Williams and Anderson, 1991)，而且員工具備組織公民行為會改善組織的績效(Podsakoff et al., 2000)，也有助於組織的政策及規範的推行(George and Jones, 1997; Smith et al., 1983)。因此，當探討組織成員對組織資訊安全政策所規範的安控措施是否意圖採用技術性控制措施或遵循程序性控制措施，其對工作及組織的態度是不可忽略，因此，我們期望從三個態度，來探究「員工對程序性控制措施的遵循意圖與技術性的控制措施的採用意圖。」

第三章　研究方法

在此章，第一節為本研究的研究假設，第二節為研究架構的說明，第三小節說明本研究的問卷如何設計以及各構念的概念性定義，第四節為說明本研究愈發放的問卷對象與使用何種統計分式來分析資料。

第一節　研究假設

大部份的公司花很多時間及資源提供(provide)、建立(establish)與監控(monitor)組織的資訊安全政策，但若最終使用者不願意喜愛或瞭解公司的資訊安全政策，那麼公司投入在資訊安全政策的時間與金錢都會付諸一炬(Herath and Rao, 2009)，因此讓員工願意使用公司的資訊安全措施相當重要。Williams and Anderson(1991)指出，「組織承諾」對「組織公民行為」有顯著正向的影響，Smith et al. (1983)指出具有「組織公民行為」的員工較會遵循組織訂定的規範，且有更多工作角色以外的作為。Randall(1987)指出，如果員工對組織表現高度的承諾，那麼在工作上也會有較好的績效表現和任務完成度。Herath and Rao(2009)研究結果顯示，組織承諾對員工的程序性控制措施的遵循意圖有顯著影響。根據 Stanton et al.(2003)顯示組織承諾對於員工使用低技術(low skill)的資訊安全相關行為(security-related behaviors)有影響，低技術的資訊安全相關行為包含寫入密碼(write password)、上網瀏覽(personal web surfing)、收個人電子信件(personal e-mail)、接受使用資訊科技的訓練(acceptable use training)、遵循使用者規範等資訊安全政策(abide by acceptable use)，也就是說，具有組織承諾的員工，他們會比較願意遵守組織訂定的資訊安全規範與約束。

行為學派的研究者(Fishbein and Ajzen, 1975；Ajzen, 1985,1991)認為個人的行為意圖決定於本身的態度，而行為意圖再影響其表現的行為，根據上述學者所發

現的結果，本研究預期員工的「組織承諾」的態度，有助於員工有意願遵循程序性控制或採用技術性控制措施，因此本研究得出下列假說：

***H1*：組織承諾與資訊安全政策的行為意圖有正向關係。**

員工對資訊安全政策中的程序性控制措施及技術性控制措施應有不同的行為意圖，因此在本研究中，將員工對資訊安全政策的行為意圖分為兩種，分別為程序性控制措施的遵循意圖與技術性控制措施的採用意圖，組織承諾對這兩項意圖的假說分別為 H_{1a} 與 H_{1b}，組織承諾對員工的資訊安全政策之行為意圖研究架構如圖 3-1：

***H1a*：**組織承諾對資訊安全政策所規範之程序性控制措施的遵循意圖有正向關係。

***H1b*：**組織承諾對資訊安全政策所規範之技術性控制措施的採用意圖有正向關係。

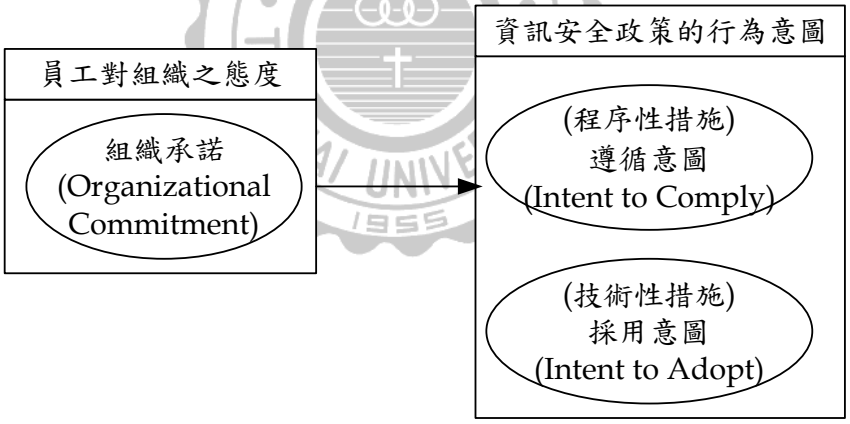

圖 3-1　員工之組織承諾與其資訊安全政策行為意圖之關係

行為學派研究者研究某項行為時，會先假設個體先有信念(belief)，綜合多個信念後轉變成個人的態度(attitude)，最後才產生個人表現出的行為(behavior) (Fishbein and Ajzen, 1975；Ajzen, 1985,1991)。因此，在探討員工採用技術性控制措施或遵循程序性控制措施時，不應直接從「組織公民行為」與「資訊安全措施之採用行為或遵循行為」兩項行為去探討因果關係，而建議由影響「組織公民行為」的態度面這項前置因素著手。

實證發現員工的工作態度被認為是「組織公民行為」的重要預測變數(Organ and Ryan, 1995; Podsakoff et al., 2000; Williams and Anderson, 1991)。這意謂員工愈滿意其工作,及對其組織較高承諾,則其表現出的公民行為更明顯。Yoon (2009)研究顯示「組織公民行為」有助於「企業資源規劃(Enterprise Resource Planning, ERP)」系統的採用，具有「組織公民行為」的員工更願意多付出額外的時間來學習使用 ERP 系統。George and Jones(1997)與 Smith et al.(1983)也發現當組織內部具有較多公民行為時，將有助於組織的政策及規範的推行。依此類推，本研究預期員工的「工作滿意度」的態度，有助於員工有意願遵循程序性控制或採用技術性控制措施，因此本研究得出下列假說：

***H2*：工作滿意度與資訊安全政策的行為意圖有正向關係。**

員工對資訊安全政策中的程序性的控制措施及技術性控制措施應有不同的行為意圖，因此在本研究中，將員工對資訊安全政策的行為意圖分為兩種，分別為程序性控制措施的遵循意圖與技術性控制措施的採用意圖,工作滿意度對這兩項意圖的假說分別為 H_{2a} 與 H_{2b}，工作滿意度對員工的資訊安全政策之行為意圖研究架構如圖 3-2：

***H2a*：**工作滿意度對資訊安全政策所規範之程序性控制措施的遵循意圖有正向關係。

***H2b*：**工作滿意度對資訊安全政策所規範之技術性控制措施的採用意圖有正向關係。

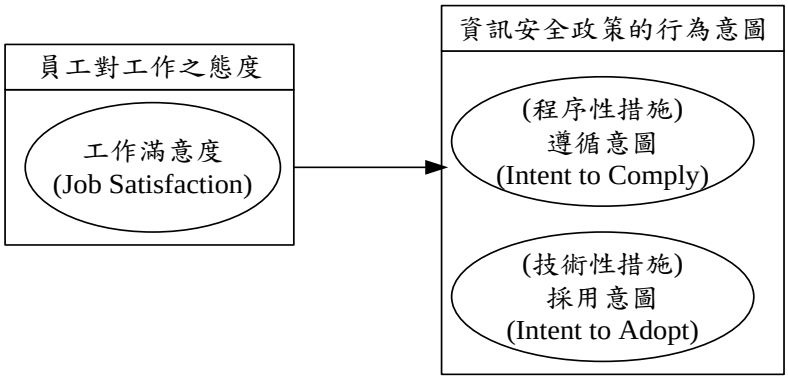

圖 3-2　員工之工作滿意度與其資訊安全政策行為意圖之關係

由理性行為模式(TRA)、計劃行為理論(TPB)可知，態度會影響行為意圖，行為意圖影響個人表現的行為。Bulgurcu et al.(2010)發現，除了資訊安全知覺(Information Security Awareness)會影響資訊安全遵循態度之外，還發現「遵循的成本」、「遵循的好處」和「不遵循的成本」也會影響員工的對資訊安全措施的態度，資訊安全措施的態度、主觀規範、自我效能對員工的遵循意圖也都呈現顯著。過去行為學派的研究者也發現，員工本身的態度會影響員工的程序性控制措施的遵循意圖(Pahnila et al., 2007；Lee and Lee, 2002)。Lee and Kozar(2008)研究發現，個人的態度會影響對反間諜程式(anti-spyware software)的技術性控制措施的採用意圖，對反間諜程式的態度會受到兼容性(compatibility)與相對優勢(Relative Advantage)的影響；Ajjan and Hartshorne(2008)發現學校教職員的態度會對 Web 2.0 的採用意圖有顯著影響。由上述的研究者可發現，個人的態度對於某項程序的頒布與一項技術的導入時，對員工程序性控制措施的遵循意圖與技術性控制措施的採用意圖有明顯影響。因此，本研究得出下列假說：

***H3*：資安措施的態度與資訊安全政策的行為意圖有正向關係。**

員工對資訊安全政策中的技術性及程序性的資訊安全控制措施應有不同的行為意圖，因此在本研究中，將員工對資安措施的行為意圖分為兩種，分別為程序性控制措施的遵循意圖與技術性控制措施的採用意圖，工作滿意度對這兩項意圖的假說分別為 H_{3a} 與 H_{3b}，資安措施的態度對員工的資訊安全政策之行為意圖研究架構如圖 3-3：

***H3a*：**資安措施的態度對資訊安全政策所規範之程序性控制措施的遵循意圖有正向關係。

***H3b*：**資安措施的態度對資訊安全政策所規範之技術性控制措施的採用意圖有正向關係。

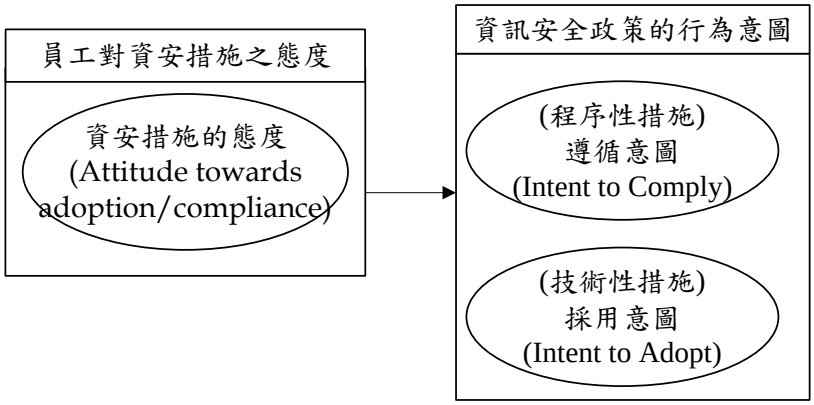

圖 3-3　員工之資安措施的態度與其資訊安全政策行為意圖之關係

Chan et al.(2005)研究中發現除了管理活動(Management Practices)和同事社會化(Coworker Socialization)對員工知覺到的資訊安全犯罪有影響，另外，同時也發現自我效能對於員工的資訊安全政策遵循行為具有正相關。Herath and Rao(2009)的研究結果也顯示，員工的資訊安全政策遵循意圖會受到自我效能、組織承諾、主觀規範和描述性規範(Descriptive Norm)的影響。Taylor and Todd（1995）提出的分解式計畫行為理論，「自我效能」會影響「知覺行為控制」，「知覺行為控制」進而影響個人的「行為意圖」。Johnston and Warkentin(2010)根據「保護動機理論」而提出「恐懼訴求理論(Fear Appeals Model，FAM)」來解釋資訊安全行為的採行。該理論認為「恐懼訴求」會增強「資安行為」的採行。發現「知覺威脅的嚴重性(Perceived Threat Severity)」會分別影響「反應措施效能(Response Efficacy)」及「自我效能(Self Efficacy)」，而後二者會影響個體執行資訊安全的行為意圖。根據過去研究者的研究結果，本研究得出下列假說：

***H4*：自我效能與資訊安全政策的行為意圖有正向關係。**

員工對資訊安全政策中的技術性及程序性的控制措施應有不同的行為意圖，因此在本研究中，將員工對資訊安全控制措施的行為意圖分為兩種，分別為程序性控制措施的遵循意圖與技術性控制措施的採用意圖，工作滿意度對這兩項意圖的假說分別為 H_{4a} 與 H_{4b}，自我效能對員工的資訊安全政策之行為意圖研究架構如圖 3-4：

H4a：自我效能對資訊安全政策所規範之程序性控制措施的遵循意圖有正向關係。

H4b：自我效能對資訊安全政策所規範之技術性控制措施的採用意圖有正向關係。

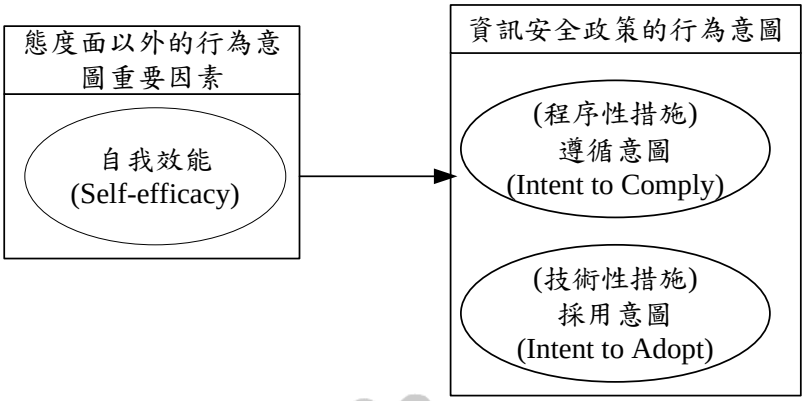

圖 3-4　員工之自我效能與其資訊安全政策行為意圖之關係

Pahnila et al.(2007)的研究結果顯示，態度、主觀規範、習慣會影響員工的遵循意圖。由 Lee and Kozar (2008)的研究結果發現，態度、主觀規範與知覺行為控制對於員工的採用反間諜程式的意圖有影響。Taylor and Todd (1995)提出的分解式計畫行為理論，發現個人的「主觀規範」會受到上司、同事、屬下等重要人士的期望行為造成的社會壓力而影響其行為意圖。Devaraj et al.(2008)發現在需要團隊合作的組織中，組織公民行為中的盡職行為(Conscientiousness)會調節主觀規範對個人使用一項科技的意圖，即是具有盡職行為特質的個人，會比較容易受到主觀規範的影響，進而影響其使用意圖(Intension to Use)。組織公民行為中盡職行為的定義是員工對於上司指派的任務，其所達成任務的結果績效比上司所期望的還要更好(Organ, 1988)。根據過去研究者的研究結果，本研究得出下列假說：

***H5*：主觀規範與資訊安全政策的行為意圖有正向關係。**

員工對資訊安全政策中的技術性及程序性的控制措施應有不同的行為意圖，因此在本研究中，將員工對資訊安全控制措施的行為意圖分為兩種，分別為程序性控制措施的遵循意圖與技術性控制措施的採用意圖，工作滿意度對這兩項

意圖的假說分別為 H_{5a} 與 H_{5b}，主觀規範對員工的資訊安全政策之行為意圖研究架構如圖 3-5：

H5a：主觀規範對資訊安全政策所規範之程序性控制措施的遵循意圖有正向關係。

H5b：主觀規範對資訊安全政策所規範之技術性控制措施的採用意圖有正向關係。

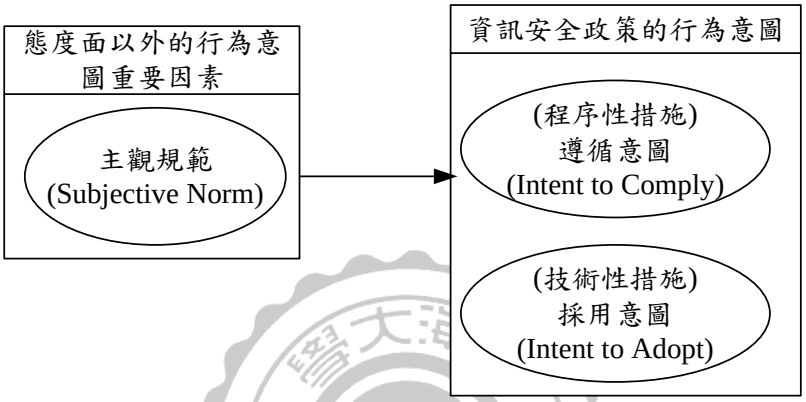

圖 3-5　員工之主觀規範與其資訊安全政策行為意圖之關係

第二節　研究架構

圖 3-6 為本研究的整體研究架構，欲探討員工對組織、工作、資訊安全措施這三種態度對員工資訊安全政策的程序性控制措施遵循意圖與技術性控制措施採用意圖之影響；以及自我效能、主觀規範兩個態度面以外的重要因素對員工資訊安全政策的程序性控制措施遵循意圖與技術性控制措施採用意圖之影響。

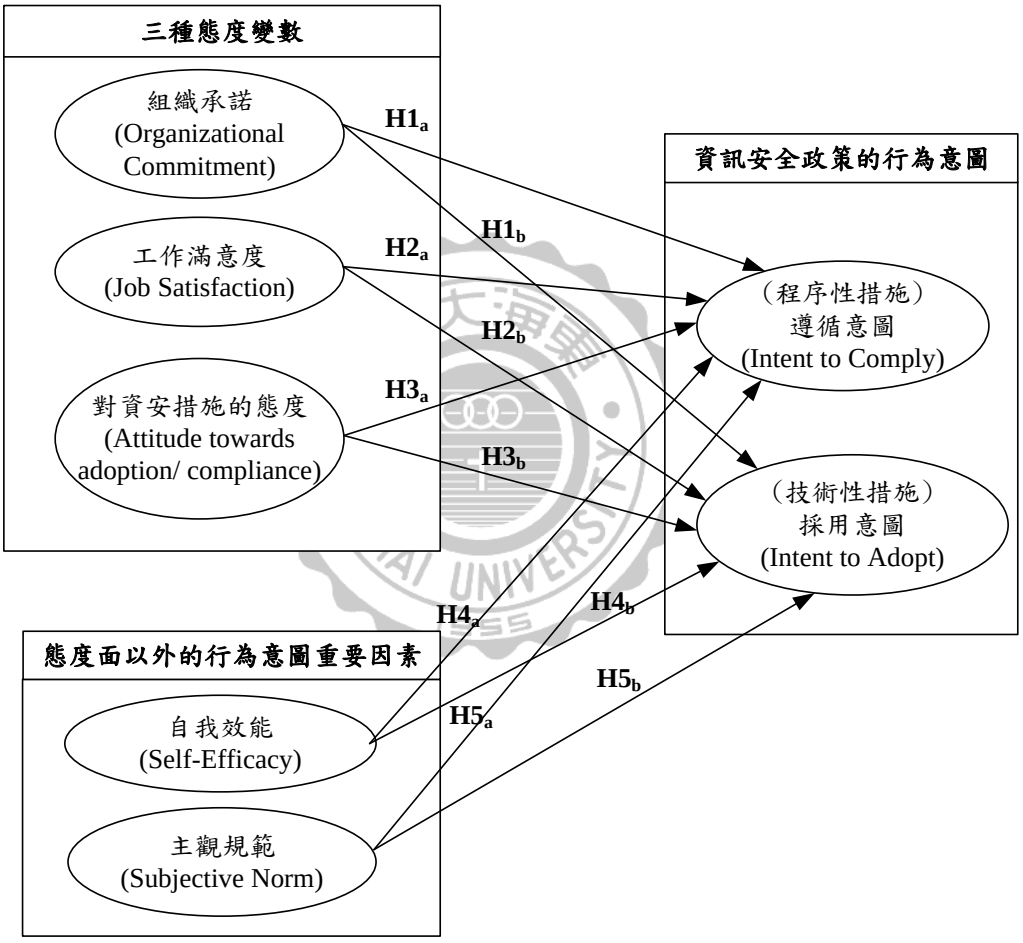

圖 3-6　研究架構

第三節　問卷設計與操作性定義

本研究使用的衡量工具，為過去許多學者引用及驗證過之量表，問卷由四部分所組成，此四部分為資訊安全、工作滿意度、組織承諾及個人資料，下列為各部份的操作性定義與衡量方式：

一、資訊系統安全

資訊系統安全部分共有 38 題問項，範圍包含員工對資訊安全措施的態度、技術性控制措施的採用意圖、程序性控制措施的遵循意圖、自我效能、主觀規範五大部分。

(一)操作性定義

態度是影響個人行為意圖的重要因素，根據計劃行為理論(Theory of Planed Behavior，TPB)，行為意圖決定於態度、主觀規範、知覺行為控制這三方面(Ajzen, 1991)。Davis(1989)提出的科技接受模式(Technology Acceptance Model，TAM)也有指出個人的行為意圖會受到知覺有用性(Perceived Usefulness)而影響，Bulgurcu et al.(2010)主張態度、主觀規範、遵循部分的自我效能(Self-Efficacy to Comply)皆會影響程序性控制措施的遵循意圖，本研究將此變數操作為員工對於資訊安全措施的正反向態度，員工個人在資訊安全領域的知識、技巧與執行能力，員工受到上司、同事、下屬或重要人士的影響這些變數都會影響到員工程序性控制措施的遵循意圖與技術性控制措施採用意圖。

(二)衡量方式

員工對資訊安全措施的態度有 9 題問項，本研究將此構念分為員工對技術性控制措施的態度、程序性控制措施的態度、員工對資訊安全措施的整體（包含技術性與程序性資訊安全控制措施）態度三個構面。自我效能有 14 題問項，此構念分為技術性的控制措施與程序性的控制措施二構面各 7 題。主觀規範有 6 題問

項，此構念分為技術性控制措施與程序性控制措施二構面各 3 題。程序性控制措施的遵循意圖有 3 題問項，技術性控制措施的採用意圖有 5 題問項。

表 3-1 是資訊安全變數的操作化彙整表，本研究衡量方式採用李克特(Likert's Scale)七點尺度量表，由「非常不同意」、「不同意」、「有點不同意」、「沒意見」、「有點同意」、「同意」、「非常同意」，依序給予 1~7 分，在員工對資訊安全措施的態度之構念，分數越高代表該員工對資訊安全措施的態度越正面。在員工的遵循意圖之構念，分數越高代表該員工愈有意願遵循組織的程序性控制措施。在採用意圖的構念，分數越高代表該員工愈有意願採用技術性控制措施。在自我效能的構念，分數越高代表該員工愈具有資訊安全措施需要的執行能力、知識或技巧。在主觀規範的構念，分數越高代表該員工愈容易受到上司、同事、下屬或重要人士的影響而去遵循程序性控制措施或採用技術性控制措施。

表 3-1　資訊安全變數操作化彙整表

構念	子構念	參考量表	問卷題項	衡量方式
資訊安全措施的態度	技術性控制措施的態度	Taylor and Todd(1995)	2~4	李克特七點量表 1：非常不同意 7：非常同意
	程序性控制措施的態度	Bulgurcu et al.,(2010)	5~8	
	對資訊安全措施的整體態度	Ajjan and Hartshorne(2008)	9~10	
自我效能	技術性控制措施	Bulgurcu et al.,(2010) Ajjan and Hartshorne(2008)	20、22、24、26、28、30、31	李克特七點量表 1：非常不同意 7：非常同意
	程序性控制措施		19、21、23、25、27、29、32	
主觀規範	技術性控制措施	Bulgurcu et al.,(2010)	34、36、38	李克特七點量表 1：非常不同意 7：非常同意
	程序性控制措施		33、35、37	
遵循意圖		Bulgurcu et al.,(2010)	11~13	李克特七點量表 1：非常不同意 7：非常同意
採用意圖		Taylor and Todd(1995)	14~16	李克特七點量表 1：非常不同意 7：非常同意
		Ajjan and Hartshorne(2008)	17~18	

資料來源：本研究整理

二、工作滿意度

(一)操作性定義

本研究的工作滿意度操作性定義為員工對工作各個層面的滿意程度，明尼蘇達滿意問卷(Minnesota Satisfaction Questionnaire，MSQ)包含 20 個衡量構面：工作活動(activity)、工作自立性(independence)、工作多樣性(variety)、社會地位(social status)、上司(human relations supervision)、科技的監督(technical supervision)、道德價值(moral values)、工作安全性(security)、社會服務(social service)、職權(authority)、能力使用(ability utilization)、公司政策和活動(company policies and

practices)、報酬(compensation)、升遷(advancement)、職責大小(responsibility)、創造性(creativity)、工作環境(working conditions)、同事(coworkers)、認同感(recognition)、成就(achievement)等構面，來衡量員工的工作滿意度。

(二)衡量方式

本研究的衡量工具採用由 Weiss et al.(1969)提出的明尼蘇達滿意問卷的短式版本問卷，共有 20 題問項，包含 20 個衡量構面，衡量方式採用李克特(Likert's Scale)七點尺度量表，由「非常不同意」、「不同意」、「有點不同意」、「沒意見」、「有點同意」、「同意」、「非常同意」，依序給予 1~7 分，分數越高，表示該員工對工作的滿意度愈高；反之，則愈不滿意。

三、組織承諾

(一)操作性定義

組織承諾為一種態度，Mowday et al.(1979)將組織承諾定義為個人認同該組織，並致力於達成組織的目標。在本研究中組織承諾為員工願意對組織付出更多心力與時間來完成組織所指派的任務，對組織有高度的認同，十分關注組織的未來發展。

(二)衡量方式

本研究使用 Mowday et al.(1979)所編製的組織承諾問卷(Organization Commitment Questionnaire，OCQ)，採用陳淑玲(2002)翻譯後的問卷內容，共 15 題問項，包含價值承諾、留職承諾與努力承諾三個構面。衡量方式採用李克特(Likert's Scale)七點尺度量表，由「非常不同意」、「不同意」、「有點不同意」、「沒意見」、「有點同意」、「同意」、「非常同意」，依序給予 1~7 分；問項 2、4、5、7、8、10 題為反向題，反向題則分別給予 7~1 分。

四、個人基本資料

包含受試者服務的產業、公司員工人數、員工於該公司的服務年資、員工於該產業的服務年資、部門、職位、性別、年齡與教育程度九項，茲說明如下：

產業別：本研究的產業分類是根據 2007 年出版的 Computer Crime and Security Survey(CSI)的產業分類方式，進行增減，分為顧問業、傳統製造業、醫療業、教育業、電子業、金融保險業、水電燃氣業、零售業、服務業、法律業、媒體通訊業、交通運輸業、資訊與高科技業、一般商業與貿易、政府機關、消費品產業、其他等十七項產業。

(一)公司員工人數:分為 50 人以下、51~100 人、101~200 人、201~500 人、501~1000 人、1001~2000 人、2001~5000 人、5001 人以上。

(二)員工於公司服務年資：分為 1~5 年、6~10 年、11~15 年、16~20 年、20 年以上。

(三)員工於產業服務年資：分為 1~5 年、6~10 年、11~15 年、16~20 年、20 年以上。

(四)部門：有生產作業、行銷企劃、人力資源、產品研發、財務會計、資訊部門、安全部門、業務部門、行政部門、採購單位、稽核部門、工程單位和其他部門。

(五)職位：分為主管、非主管兩類。

(六)性別：分為男性、女性。

(七)年齡：分為 20 歲以下、21~25 歲、26~30 歲、31~35 歲、36~40 歲 、41~45 歲、46~50 歲、51~55 歲、56~60 歲、61~65 歲。

(八)教育程度：分為國中及以下、高中(職)、專科、大學、碩士和博士。

本問卷衡量工具引用於各專家學者所驗證過的量表，並經過專家檢視問卷的表面效度，根據專家提供的建議將文字用字遣詞潤飾，所有問項皆予以保留，降低語意不清的可能導致的偏誤，修正後的問卷以電子檔及紙本方式發放填寫，問卷詳細內容如附錄一所示。

第四節　研究對象與資料分析方法

一、研究對象

本研究的資料收集以問卷調查的方式,研究對象以工作時需要藉以電腦來完成大部份工作的員工為問卷主要發放對象，不設限產業及公司規模。發放方式以滾雪球抽樣方式，透過已在工作的親友邀請同事幫忙填寫，填寫方式包含電子檔、紙本兩種型式，問卷發放日期由 2011 年 4 月 15 日開始，至 2011 年 5 月 15 日為止，為期一個月。

本研究共回收 223 份問卷，扣除填答內容不完整及填答有問題者 8 份問卷，有效問卷為 215 份，有效問卷之回收率為 96.4%。

二、資料分析方法

本研究使用統計軟體 SPSS 18.0 for Windows 為分析工具，透過敘述統計分析、信度分析、相關分析、階層式迴歸分析、集群分析等統計分析方法，進行研究假設的驗證並呈現研究結果：

(一)敘述統計分析(descriptive statistic)

經由敘述統計，分析基本的人口統計分佈，瞭解受測者的基本資料情形以次數分配與百分比來說明分布情況；瞭解各個構面的衡量狀況，以平均數與標準差來衡量之。

(二)信度(reliability)分析

本研究採用 Cronbach's α 來分析問卷問項的內部一致性，並使用總項相關係數(Item-to-total Correlations)來衡量分項對總項的相關係數，。

(三)相關分析(correlation analysis)

本研究使用 Pearson 相關係數(Pearson Coefficient of Correlation)檢定兩變項之間的關聯性，相關係數會介於＋1 與－1 之間，相關係數值越接近正負 1 時，表示兩變項之間的關聯越顯著，相關係數的絕對值範圍若在 0.1 以下為微弱或無

相關；0.1~0.39 為低度相關；0.4~0.69 為中度相關；0.7~0.99 為高度相關；1 為完全相關(邱皓政, 2003)。透過 Pearson 相關係數來檢驗資訊安全的態度之技術性控制措施、資訊安全的態度之程序性控制措施、資訊安全的態度之資安措施的整體態度、自我效能的技術性控制措施、自我效能的程序性控制措施、主觀規範的技術性控制措施、主觀規範的程序性控制措施、工作滿意度、組織承諾、遵循意圖、採用意圖等變數，兩兩之間的相關程度。

(四)階層式迴歸分析(hierarchical multiple regression)

本研究透過階層式迴歸分析方法，將控制變數與態度變數逐步納入迴歸方程式，透過多層次的迴歸來進行迴歸預測，檢驗控制變數與工作情境相關態度對員工遵循程序性控制措施意圖或採用技術性控制措施意圖的影響。

(五)集群分析(Cluster Analysis)

集群分析的目的主要是將具有某些共同特性者與以整合在同一群(吳萬益和林清河,2000)。本研究利用 K 平均數法將組織承諾及工作滿意度的填答狀況分為三群，K 平均數法是以 K 個中心值為中心，將個體中與中心點較接近者納入該群中，依各個體到各群中心點之距離遠近重新計算出各集群值之集結係數，持續重複計算，一直到中心點與個體不能在移動為止(吳萬益和林清河,2000)。

三、問卷前測

本研究所設計的問卷，由於是翻譯國外學者的問卷問項，因此在問卷正式發放以前，與指導教授討論後，並經過資訊安全專業人員與非資訊安全人員檢視問卷問項的內容，根據這些專家學者以及非資訊安全人員的意見，將問卷內容用字遣詞及語意不清的部分進行修正，減少填答者誤解或不理解問題的機率，降低可能導致的偏誤。

第四章　研究結果

本章的第一節為樣本的基本資料分析與敘述統計，了解受測者的分佈情形與填答狀況。第二節為樣本的信度分析，了解問卷題項是否具有一致性以及能否解釋該研究構念。第三節使用階層式迴歸分析方法與集群分析，來分析工作情境相關態度對員工程序性控制措施的遵循意圖或技術性控制措施的採用意圖是否有影響。

第一節　基本資料分析與敘述統計

一、受試者基本資料分析

將回收的 215 份有效樣本，依照填答者的作答，將受試者的基本資料分類，調查受試者服務的產業、服務單位之人數、於該公司的服務年資、於該產業的服務年資、服務單位的部門、職位、性別、年齡與教育程度等九項，如表 4-1 所示：

(一)產業：根據回收的樣本資料，傳統製造業、電子業、金融保險業、資訊與高科技產業等四產業皆各 30 筆左右樣本，共佔全部樣本的 55.4%。

(二)公司人數：調查的樣本之中，以公司人數少於 50 人與公司人數介於 201~500 人之中的公司為最多，各 37 筆，兩項共 74 筆資料，佔全部樣本 34.4%；其次是公司人數為 101~200 人，有 26 筆資料，佔 12.1%；公司人數為 501~1000 人的有 25 筆資料，佔 11.6%；公司人數介於 50~100 人、1001~2000 人以及 5000 人以上的各占 6%左右。

(三)於該公司服務年資：根據回收的有效樣本顯示，於該公司服務的年資以 1~5 年的佔大多數，共 138 筆，佔 64.2%；6~10 年的有 40 筆，佔 18.6%；11~15 年的有 20 筆，佔 9.3%；16~20 年的有 9 筆，佔 4.2%；服務年資 20 年以上的有 8 筆，佔 3.7%。

(四)於該產業服務年資：根據回收有效樣本顯示，於該產業服務的年資以 1~5 年

的資料筆數共 120 筆，佔 55.8%；服務年資 6~10 年的有 46 筆，佔 21.4%；11~15 年的有 28 筆，佔 13%；16~20 年的有 12 筆，佔 5.6%；於該產業服務 20 年以上的有 9 筆，佔 4.2%。

(五)服務部門：根據回收有效樣本顯示，填答者以業務部門為大多數，有 68 筆，佔 31.6%；其次為資訊部門，有 27 筆資料，佔 12.6%；勾選其它部門的有 19 筆，佔 8.8%，為其它部門的有包含銀行櫃檯行員、環境安全部門、警察單位、品管部門、創意設計部門、管理部門、老師等；行銷、研發、財會與行政部門各有 18 筆資料，各佔 8.4%；生產部門有 9 筆資料，佔 4.2%；採購與稽核部門各有 4 筆資料，佔 1.9%；人資部門有 1 筆資料，佔 0.5%。

(六)職位：：在職位方面，我們將職位分為主管和非主管，主管包含基層、中階與高階主管，根據回收的有效樣本顯示，填答者為主管的有 50 位，佔 23.3%；填答者為非主管的有 165 位，佔 76.7%。

(七)性別：根據回收的有效樣本顯示，填答者為男性的有 107 位，佔 49.8%；女性有 108 位，佔 50.2%，男女比例各佔一半。

(八)年齡：根據回收的有效樣本顯示，大部分的填答者年齡聚集在 21~45 歲之間，在這個年齡之間的資料共有 202 筆，佔全部樣本的 94.0%。

(九)教育程度：根據回收的有效樣本顯示，大部分填答者教育程度為大學，有 120 位，佔 55.8%；其次為碩士，有 65 位，佔 30.2%；專科畢業的有 21 位，佔 9.8%；高中畢業的有 7 位，佔 3.3%；博士畢業的有 2 位，佔 0.9%。

表 4-1　受試者基本資料分析

類別	人口統計變數	次數	百分比	累積百分比
產業	顧問業	2	0.9%	0.9%
	傳統製造業	29	13.0%	14.4%
	醫療業	15	7.0%	21.4%
	教育業	8	3.7%	25.1%
	電子業	30	14.0%	39.1%
	金融保險業	30	14.0%	53.0%
	水電燃氣業	1	0.5%	53.5%
	零售	2	0.9%	54.4%
	服務業	20	9.3%	63.7%
	媒體通訊	4	1.9%	65.6%
	交通運輸	2	0.9%	66.5%
	資訊與高科技	31	14.4%	80.9%
	一般商業與貿易	9	4.2%	85.1%
	政府機關	18	8.4%	93.5%
	消費品	11	5.1%	98.6%
	其他	3	1.4%	100.0%
公司人數	小於 50 人	37	17.2%	17.2%
	50~100 人	12	5.6%	22.8%
	101~200 人	26	12.1%	34.9%
	201~500 人	37	17.2%	52.1%
	501~1000 人	25	11.6%	63.7%
	1001~2000 人	13	6.0%	69.8%
	2001~5000 人	14	6.5%	76.3%
	5000 人以上	51	23.7%	100.0%
於該公司服務年資	1~5 年	138	64.2%	64.2%
	6~10 年	40	18.6%	82.8%
	11~15 年	20	9.3%	92.1%
	16~20 年	9	4.2%	96.3%
	20 年以上	8	3.7%	100.0%

類別	人口統計變數	次數	百分比	累積百分比
於該產業服務年資	1~5 年	120	55.8%	55.8%
	6~10 年	46	21.4%	77.2%
	11~15 年	28	13.0%	90.2%
	16~20 年	12	5.6%	95.8%
	20 年以上	9	4.2%	100.0%
服務部門	生產部門	9	4.2%	4.2%
	行銷部門	18	8.4%	12.6%
	人資部門	1	0.5%	13.0%
	研發部門	18	8.4%	21.4%
	財會部門	18	8.4%	29.8%
	資訊部門	27	12.6%	42.3%
	業務部門	68	31.6%	74.0%
	行政部門	18	8.4%	82.3%
	採購部門	4	1.9%	84.2%
	稽核部門	4	1.9%	86.0%
	工程部門	11	5.1%	91.2%
	其他部門	19	8.8%	100.0%
職位	主管	50	23.3%	23.3%
	非主管	165	76.7%	100.0%
性別	男性	107	49.8%	49.8%
	女性	108	50.2%	100.0%
年齡	21~25 歲	31	14.4%	14.4%
	26~30 歲	79	36.7%	51.2%
	31~35 歲	34	15.8%	67.0%
	36~40 歲	30	14.0%	80.9%
	41~45 歲	28	13.0%	94.0%
	46~50 歲	7	3.3%	97.2%
	51~55 歲	3	1.4%	98.6%
	56~60 歲	2	0.9%	99.5%
	61~65 歲	1	0.5%	100.0%
教育程度	高中	7	3.3%	3.3%
	專科	21	9.8%	13.0%
	大學	120	55.8%	68.8%
	碩士	65	30.2%	99.1%
	博士	2	0.9%	100.0%

資料來源：本研究整理

二、敘述統計分析

為了瞭解受試者服務的公司之資訊安全政策是否設立完善,於問項的第一題先詢問受試者認為自己服務的公司是否有明確完善的資訊安全政策或規範,經過敘述統計分析，如表 4-2 所示，得到的平均數為 5.84，高於平均 4，顯示出大部分填答者認為自己所服務的公司具有明確的資訊安全政策或規範。

表 4-2　公司資訊安全設置之描述統計分析

問項	樣本數	平均數	標準差
我們公司目前有明確的資訊安全政策或規範	214	5.84	1.3414

資料來源：本研究整理

表 4-3 是根據回收的有效樣本，將不同的研究構念分類後，利用 SPSS for Windows 18.0 統計套裝軟體分析工具所得到的結果，茲說明如下：

(一)資安措施態度：資訊安全措施的態度共有 9 題問項，前 3 題屬於技術性控制措施，在此部分平均數為 6.26；程序性控制措施有 4 題問項，平均數為 5.93；剩餘的 2 題則是在問項中皆有詢問到技術性控制措施與程序性控制措施,因考量到同時將這兩題都加入到技術性控制措施與程序性控制措施中會影響到平均值的正確性，因此將這 2 題歸納為另一部分，其平均數為 5.76。在資訊安全措施的態度此研究構念中，這三部分的填答都有在平均數 4 以上，顯示員工對於資訊安全措施有較正面的態度。

(二) 工作滿意度：工作滿意度共有 20 個題項，每題項皆代表一個構面，期平均數為 5.45，在平均數 4 以上，表示整體上看來填答的員工在組織中對於該工作有相當地認同程度。

(三) 組織承諾：組織承諾共有 15 個題項，組織承諾的平均數為 4.95，平均數為全部研究構念中最低的，但仍在平均數 4 以上，因此可看出在整體上填答的員工對服務的公司有相當程度的組織承諾。

(四) 自我效能：自我效能的題項共有 14 題，技術性控制措施與程序性控制措施的問項各佔 7 題，在技術性控制措施的問項，其平均數為 5.38；自我效能的程序

性控制措施的問項，平均數為 5.40，這兩部分的平均數相當地接近，皆有超過 4 以上，表示填答的員工認為自己具備在資訊安全方面的能力與知識。

(五) 主觀規範：主觀規範的題項共有 6 題，技術性控制措施與程序性控制措施的問項各佔 3 題，技術性控制措施的問項，其平均數為 5.77；而在程序性控制措施的問項，平均數為 5.75，兩部分的平均數相當地接近，皆有超過 4 以上，表示受測的員工認為自己會受到周遭重要人物的影響。

(六)遵循意圖與採用意圖：遵循意圖和採用意圖為此研究的依變項，遵循意圖的題項有 3 題，其平均數為 6.06；採用意圖的題項有 5 題，平均數為 5.91，皆在平均之上，可觀察到填答者對資訊安全措施有一定的行為意圖。

表 4-3　各研究構念之描述統計分析

研究構念	子構念	題數	樣本數	平均數	標準差
資安措施態度	技術性控制措施	3	215	6.26	0.7797
	程序性控制措施	4	215	5.93	0.8864
	資安措施整體態度	2	215	5.76	1.0195
工作滿意度		20	215	5.45	0.8235
組織承諾		15	215	4.95	0.8972
自我效能	技術性控制措施	7	215	5.38	0.9600
	程序性控制措施	7	215	5.40	0.9601
主觀規範	技術性控制措施	3	215	5.77	0.9576
	程序性控制措施	3	215	5.75	0.9703
遵循意圖		3	215	6.06	0.7614
採用意圖		5	214	5.91	0.8301

資料來源：本研究整理

第二節　信度分析

本研究的研究構念包含對資安措施的態度、工作滿意度、組織承諾、自我效能、主觀規範、遵循意圖和採用意圖七項，在對資訊安全措施的態度、自我效能與主觀規範這三個構念中，又分為技術性控制措施和程序性控制措施的這兩個子構面，資安措施的態度中有題項皆包含技術性控制措施和程序性控制措施，因此有資安措施整體態度的子構念。

信度是指測量結果的一致性(consistency)或穩定性(stability)，同一個量表給予受測者測試，該測驗分數的穩定性不會受到時間、地點的影響，而能維持前後一致的程度(邱皓政,2003)。本研究使用 Cronbach's α 來分析問卷子構念的內部一致性，α 值若大於 0.7 以上，屬於內部一致性良好；另外使用總項相關係數(Item-to-total Correlations)來衡量分項對總項的相關係數，而分項對總項相關係數須大於 0.5(吳萬益和林清河, 2000)，如表 4-4 所示，在資訊安全措施態度的三個子構念中，這三個子構念標準化的 Cronbach's α 分別為 0.86、0.90、0.80，代表其內部一致性達顯著水準，而分項對總項也達可用標準，代表這三項子構念非常良好。

在自我效能的兩個子構念中，其標準化的 Cronbach's α 分別為 0.91 與 0.92，代表其內部一致性達顯著水準，而分項對總項也達可用標準，代表這二項子構念非常良好。

在主觀規範的在自我效能的兩個子構念中，其標準化的 Cronbach's α 皆為 0.87，代表其內部一致性達顯著水準，而分項對總項也達可用標準，代表這二項子構念非常良好。

工作滿意度的標準化 Cronbach's α 為 0.94，代表其內部一致性達顯著水準，不過在分項對總項的相關係數中，工作滿意度的 1、3、9 題的數值分別為 0.459、0.465、0.444，雖未達 0.5，但仍在可接受的範圍之內。

組織承諾的標準化 Cronbach's α 為 0.93，代表其內部一致性達顯著水準，不過在分項對總項的相關係數中，組織承諾問項中的第 2、11 題的數值為 0.405、0.480，雖未達 0.5，但仍在可接受的範圍之內。

本研究的標準化後的 Cronbach's α 皆在 0.7 以上，而在分項對總項的相關係數中，大部分的分項對總項的相關係數皆大於 0.5，因此可判斷本研究的問卷具有不錯的信度。

表 4-4　本研究問項之內部一致性及分項對總項相關係數

構念	子構念	題項	Standardized Cronbach's α	Item-to-total correlations
資安措施的態度	技術性控制措施的態度	IS02	0.86	0.728
		IS03		0.774
		IS04		0.710
	程序性控制措施的態度	IS05	0.90	0.766
		IS06		0.726
		IS07		0.846
		IS08		0.800
	資安措施整體態度	IS09	0.80	0.670
		IS10		0.670
工作滿意度		JS01	0.94	0.459
		JS02		0.602
		JS03		0.465
		JS04		0.701
		JS05		0.700
		JS06		0.686
		JS07		0.537
		JS08		0.580
		JS09		0.444
		JS10		0.528
		JS11		0.720
		JS12		0.736
		JS13		0.684
		JS14		0.594
		JS15		0.726
		JS16		0.733
		JS17		0.728
		JS18		0.621
		JS19		0.660
		JS20		0.703
組織承諾		OC01	0.93	0.624
		OC02		0.405
		OC03		0.667
		OC04		0.685
		OC05		0.627
		OC06		0.728
		OC07		0.740
		OC08		0.610

構念	子構念	題項	Standardized Cronbach's α	Item-to-total correlations
組織承諾(續)		OC09		0.803
		OC10		0.603
		OC11	0.93(續)	0.480
		OC12		0.667
		OC13		0.757
		OC14		0.608
		OC15		0.683
自我效能	技術性控制措施	IS20		0.674
		IS22		0.771
		IS24		0.816
		IS26	0.91	0.646
		IS28		0.769
		IS30		0.765
		IS31		0.702
	程序性控制措施	IS19		0.674
		IS21		0.771
		IS23		0.816
		IS25	0.92	0.646
		IS27		0.769
		IS29		0.765
		IS32		0.732
主觀規範	技術性控制措施	IS34		0.706
		IS36	0.87	0.764
		IS38		0.785
	程序性控制措施	IS33		0.681
		IS35	0.87	0.789
		IS37		0.780
遵循意圖		IS11		0.842
		IS12	0.93	0.885
		IS13		0.849
採用意圖		IS14		0.622
		IS15		0.808
		IS16	0.92	0.839
		IS17		0.853
		IS18		0.716

資料來源：本研究整理

第三節　相關分析與階層式迴歸分析

本節探討資訊安全措施的程序性控制措施的遵循意圖與技術性控制措施的採用意圖是否會受到資安措施態度、工作滿意度、組織承諾、自我效能與主觀規範所影響，進行迴歸分析之前，先探討各構面之間相關程度。證實變項之間具有相關性之後，再利用階層式迴歸分析法，探討各變數與員工程序性控制措施的遵循意圖或技術性控制措施採用的意圖之關聯性。並將組織承諾與工作滿意度做集群分析(Cluster Analysis)。

一、相關分析

本研究利用 Pearson 相關係數檢定兩變項之間的關聯性，如表 4-5 所示，資訊安全措施的態度有三個子構念，自我效能有二個子構念，主觀規範有二個子構念，還包含工作滿意度、組織承諾、程序性控制措施的遵循意圖、技術性控制措施的採用意圖四個變項，共有 11 個變項。其中，程序性控制措施的遵循意圖與技術性控制措施的採用意圖為依變項，資訊安全措施的態度、自我效能、主觀規範、工作滿意度與組織承諾為自變項。

工作滿意度與資安措施的態度的三項子構念之間的相關係數依序為 0.415、0.410、0.383，在顯著水準為 P＜0.01 的情況下，由 Pearson 相關係數可看出工作滿意度與資安措施的態度之間均有顯著地正向關係。

組織承諾與與資安措施的態度的三項子構念之間的相關係數依序為 0.352、0.385、0.326，而組織承諾與工作滿意度的相關係數為 0.769，屬於高度相關，在顯著水準為 P＜0.01 的情況下，由 Pearson 相關係數可看出組織承諾與資安措施的態度，以及組織承諾與工作滿意度這兩項態度變數之間均有顯著地正向關係。

在遵循意圖部分，與資訊安全措施態度的三個子構念的相關程度分別為 0.641、0.687、0.703；與自我效能的二個子構念的相關程度分別為 0.573、0.553；與主觀規範的二個子構念的相關程度分別為 0.426、0.422；與工作滿意度的相關

程度為 0.416；與組織承諾的相關程度為 0.360，在顯著水準為 P＜0.01 的情況下，員工程序性控制措施的遵循意圖與各個自變數之間均有顯著地正向關係。

在採用意圖部分，與資訊安全措施態度的三個子構念的相關程度分別為 0.491、0.478、0.475；與自我效能的二個子構念的相關程度分別為 0.562、0.522；與主觀規範的二個子構念的相關程度分別為 0.383、0.350；與工作滿意度的相關程度為 0.350；與組織承諾的相關程度為 0.321，在顯著水準為 P＜0.01 的情況下，員工的採用意圖與各個自變數之間均有顯著地正向關係。

表 4-5　Pearson 相關分析

變項	平均數	標準差	1	2	3	4	5	6	7	8	9	10	11
1.資安措施態度之技術性控制措施	6.26	0.7796	1.000										
2.資安措施態度之程序性控制措施	5.93	0.8864	0.734**	1.000									
3.資安措施態度之資安措施整體態度	5.76	1.0195	0.644**	0.825**	1.000								
4.自我效能之技術性控制措施	5.38	0.9600	0.467**	0.541**	0.567**	1.000							
5.自我效能之程序性控制措施	5.40	0.9601	0.451**	0.524**	0.531**	0.967**	1.000						
6.主觀規範之技術性控制措施	5.77	0.9576	0.382**	0.476**	0.414**	0.491**	0.433**	1.000					
7.主觀規範之程序性控制措施	5.75	0.9703	0.352**	0.494**	0.427**	0.520**	0.499**	0.922**	1.000				
8.工作滿意度	5.45	0.8235	0.415**	0.410**	0.383**	0.513**	0.506**	0.320**	0.285**	1.000			
9.組織承諾	4.95	0.8972	0.352**	0.385**	0.326**	0.402**	0.415**	0.228**	0.213**	0.769**	1.000		
10.遵循意圖	6.06	0.7614	0.641**	0.687**	0.703**	0.573**	0.552**	0.426**	0.422**	0.416**	0.360**	1.000	
11.採用意圖	5.91	0.8301	0.491**	0.478**	0.475**	0.562**	0.522**	0.383**	0.350**	0.350**	0.321**	0.524**	1.000

** 顯著水準為P＜0.01時(雙尾)相關顯著

資料來源：本研究整理

二、階層式迴歸分析

(一)整體模式

本研究利用階層式迴歸分析方法，瞭解資訊安全措施的態度、工作滿意度和組織承諾等變數對員工的資訊安全措施行為意圖之影響，將遵循意圖和採用意圖合併計算出一個平均數，該平均數即為依變數，在此模式，不用將自我效能、主觀規範、對資訊安全措施的態度問項拆解成技術性控制措施與程序性控制措施，每一變數各計算出一平均數，為自變項。

在模式一為選入產業、部門、職位、自我效能與主觀規範五項變數，模式二選入工作滿意度變數，模式三將工作滿意度變數拿出，選入組織承諾，模式四將組織承諾變數拿出，選入資訊安全措施態度，模式五將產業、部門、職位這三項控制變數與自我效能、主觀規範、工作滿意度、組織承諾、資訊安全措施態度這五項自變數皆選入。模式二、三、四之間無階層式迴歸關係，模式二由模式一再選入工作滿意度，模式三由模式一再選入組織承諾，模式四由模式一再選入資訊安全措施的態度，模式五則是將三種態度變數皆選入。因此，模式一、二、五之間為階層式迴歸關係，模式一、三、五之間為階層式迴歸關係，模式一、四、五之間為階層式迴歸關係。

根據表 4-6，模式一當中的職位、自我效能與主觀規範均有顯著，自我效能的標準化 β 係數為 0.541，顯示在此模式，自我效能最能解釋員工資訊安全措施的行為意圖，模式一的 $F_{(5,209)}$=33.442，p-value =0.000，F 值達顯著，Adjusted R^2= 0.431。

模式二加入工作滿意度變數後，部門、職位、自我效能、主觀規範和工作滿意度均為顯著，自我效能為此模式中解釋力最高的變數，$F_{(6,208)}$=28.937，p-value =0.000，F 值達顯著，Adjusted R^2=0.439。

模式三將工作滿意度態度變數拿出，選入組織承諾態度變數，結果部門、職位、自我效能、主觀規範、組織承諾均為顯著，自我效能為此模式中解釋力最高的變數，$F_{(6,208)}$=29.754，p-value =0.000，F 值顯著，Adjusted R^2=0.446。

模式四將組織承諾態度變數拿出，選入資安措施的態度變數，結果產業、職位、自我效能、資安措施的態度均為顯著，資安措施的態度為此模式中解釋力最高的變數，$F_{(6,208)}$=46.560，p-value =0.000，F 值顯著，Adjusted R^2=0.561。

模式五將資訊安全措施的態度變數、工作滿意度與組織承諾所有態度變數都加入，結果產業、職位、自我效能與資訊安全措施的態度為顯著，$F_{(8,206)}$=30.202，p-value =0.000，F 值達顯著，Adjusted R^2=0.561。在所有態度變數接加入後，主觀規範、工作滿意度與組織承諾這三個變數變的不顯著。

由此結果看來，發現各態度對員工的資訊安全政策行為意圖會有影響，接下來將員工的行為意圖拆解成遵循意圖與採用意圖分開討論，看工作相關態度變數分別對兩種意圖的影響。

表 4-6　員工的三種態度對組織資訊安全政策行為意圖迴歸分析

	模式一	模式二	模式三	模式四	模式五
控制變項					
產業	0.057	0.072	0.075	0.095*	0.102**
部門	-0.070	-0.088†	-0.093†	-0.062	-0.074†
職位	-0.127**	-0.101*	-0.101*	-0.074†	-0.063
自變項					
自我效能	0.541***	0.480***	0.480***	0.339***	0.316***
主觀規範	0.163†	0.154**	0.158**	0.041	0.042
工作滿意度		0.127*			-0.004
組織承諾			0.151**		0.079
資訊安全措施態度				0.462***	0.446***
R^2	0.444	0.455	0.462	0.573	0.578
Adjusted R^2	0.431	0.439	0.446	0.561	0.561
F	33.442***	28.937***	29.754***	46.560***	30.202***

顯著水準 † P<0.1　* P<0.05　** P<0.01　*** P<0.001

資料來源：本研究整理

(二)工作滿意度對員工的技術性及程序性控制措施行為意圖之影響

將員工對資訊安全政策的行為意圖分成程序性控制措施的遵循意圖與技術性控制措施的採用意圖二個依變數來分析，並將自我效能、主觀規範這兩項變數的問項依技術性與程序性區分分別求得平均數，再加入工作滿意度工作相關態度變數平均數進行迴歸分析。

結果顯示，在程序性控制措施的遵循意圖中，$F_{(6,208)}$=19.935，p-value=0.000，F 值顯著，自我效能、主觀規範與工作滿意度三項變數為顯著，遵循意圖模式的 Adjusted R^2=0.347，整體解釋力為 34.7%；在技術性控制措施的採用意圖，$F_{(6,207)}$=19.869，p-value=0.000，F 值顯著，產業、職位、自我效能、與主觀規範四項變數為顯著，工作滿意度對員工技術性控制措施的採用意圖無看出明顯影

響，採用意圖模式的 Adjusted R^2=0.352，整體解釋力為 35.2%，如表 4-7。

自我效能與主觀規範同時對員工程序性控制措施的遵循意圖和技術性控制措施的採用意圖有影響，顯示在資訊安全方面擁有較多知識、技巧與能力的員工會比較願意採用技術性控制措施及遵守程序性控制措施；公司的上司、同事及下屬也是影響員工遵循程序性控制措施或採用技術性控制措施的重要影響變數；而只有產業、職位對員工的技術性控制措施的採用意圖有影響，換言之，員工服務的產業若本來就較重視資訊安全，那麼員工會更願意採用技術性控制措施；結果也顯示，為主管階級的員工，也會比一般員工更願意採用技術性控制措施。

由表 4-7 也可以發現，具有工作滿意度的員工會願意遵守公司訂定的程序性控制措施，但是具有工作滿意度的員工對採用技術性控制措施無明顯的影響，因為採用需要額外付出時間與心力學習如何使用技術性控制措施，遵循程序性資訊安全措施只需要遵守政策與命令，相較之下，遵守資訊安全程序性控制措施對於採用技術性控制措施要來的容易許多。

表 4-7　工作滿意度對技術性及程序性控制措施的行為意圖之迴歸分析

	遵循意圖	採用意圖
控制項		
產業	-0.004	0.109*
部門	-0.067	-0.083
職位	-0.065	-0.102†
自變項		
自我效能	0.373***	0.457***
主觀規範	0.184**	0.110†
工作滿意度	0.171*	0.081
R^2	0.365	0.365
Adjusted R^2	0.347	0.347
F	19.935***	19.869***

顯著水準 † P<0.1　* P<0.05　** P<0.01　*** P<0.001
資料來源：本研究整理

(三) 組織承諾對員工的技術性及程序性控制措施行為意圖之影響

組織承諾的迴歸分析操作方法與工作滿意度相同，先將員工對資訊安全政策的行為意圖分成程序性控制措施的遵循意圖與技術性控制措施的採用意圖二個依變數來分析，並將自我效能、主觀規範這兩項變數的問項依技術性與程序性區分分別求得平均數，再加組織承諾工作相關態度變數平均數進行迴歸分析。

得到的統計結果如表 4-8 所示，在員工的程序性控制措施之遵循意圖模式中，$F_{(6,208)}$=19.817，p-value=0.000，F 值顯著，自我效能、主觀規範與組織承諾三項變數為顯著，遵循意圖模式的 Adjusted R^2=0.345，整體解釋力為 34.5%；在技術性控制措施的採用意圖，$F_{(6,207)}$=20.562，p-value=0.000，F 值顯著，控制項的產業、部門、職位與自變項的自我效能、主觀規範與組織承諾六項變數都對員工的技術性控制措施的採用意圖有顯著影響，採用意圖模式的 Adjusted R^2=0.355，整體解釋力為 35.5%，自我效能在程序性控制措施的遵循意圖與技術性控制措施的採用意圖的模式中，為解釋力最強的變數。

員工服務的產業較重視資訊安全，那麼會增加員工採用技術性控制措施的意願；重視資訊安全的的部門會比其他部門的員工更願意採用技術性控制措施；員工為主管階級，較一般員工更願意採用技術性控制措施；具有組織承諾的員工會比不具有組織承諾的員工更願意遵循程序性控制措施與採用技術性控制措施。

表 4-8　組織承諾對技術性及程序性資訊安全措施的行為意圖之迴歸分析

	遵循意圖	採用意圖
控制項		
產業	-0.006	0.114*
部門	-0.067	-0.091†
職位	-0.074	-0.097†
自變項		
自我效能	0.393***	0.447***
主觀規範	0.190**	0.111†
組織承諾	0.154*	0.126*
R^2	0.364	0.373
Adjusted R^2	0.345	0.355
F	19.817***	20.562***

顯著水準 † P<0.1　* P<0.05　** P<0.01　*** P<0.001

資料來源：本研究整理

(四) 資安措施的態度對員工的技術性及程序性控制措施行為意圖之影響

資安措施的態度迴歸分析操作方法與工作滿意度、組織承諾相同，先將員工對資訊安全政策的行為意圖分成程序性控制措施的遵循意圖與技術性控制措施的採用意圖二個依變數分析，並將自我效能、主觀規範這兩項變數的問項依技術性控制措施與程序性控制措施區分，分別求得平均數，再加入資安措施的態度變數平均數進行迴歸分析。

如表 4-9 所示，根據迴歸分析結果，在員工的程序性控制措施之遵循意圖模

式中，$F_{(6,208)}$= 38.842，p-value=0.000，F 值顯著，自我效能、資安措施的態度此兩變數有顯著影響員工的程序性控制措施的遵循意圖，顯示出個人認為自己在資訊安全方面具有相當知識和能力的員工以及對資訊安全措施愈正向態度的員工，越願意遵循公司所頒布的程序性控制措施。遵循意圖模式的 Adjusted R^2=0.515，整體解釋力為 51.5%，在程序性控制措施的遵循意圖模式中，資安措施的態度為解釋力最強的變數，最能解釋該模式。

在技術性控制措施的採用意圖，$F_{(6,207)}$= 24.566，p-value=0.000，F 值顯著，控制項的產業、職位與自變項的自我效能、資安措施的態度等四項變數都對員工的技術性控制措施的採用意圖有顯著影響，顯示出員工願不願意去採用公司所要求的技術性控制措施與員工服務的產業、員工為主管、員工本身所具有的知識和能力與員工對資訊安全措施的正反面態度有關係，換言之，員工所服務的產業如果本來就比較重視資訊安全，會提升員工採用技術性控制措施的意願；員工為主管，會較一般員工更願意採用技術性控制措施；在資訊安全領域能力與知識較強的員工，越願意去採用技術性的措施；員工對資訊安全措施態度是正面的，員工會較願意採用公司所要求的技術性控制措施。技術性控制措施採用意圖的模式 Adjusted R^2=0.399，整體解釋力為 39.9%，自我效能在技術性控制措施的遵循意圖的模式中，為解釋力最強的變數。

表 4-9 資安措施的態度對技術性及程序性控制措施的行為意圖之迴歸分析

	遵循意圖	採用意圖
控制項		
產業	0.029	0.121*
部門	-0.035	-0.059
職位	-0.054	-0.088†
自變項		
自我效能	0.256***	0.394***
主觀規範	0.024	0.064
資安措施的態度	0.536***	0.273***
R^2	0.528	0.416
Adjusted R^2	0.515	0.399
F	38.842***	24.566***

顯著水準 † P<0.1　* P<0.05　** P<0.01　*** P<0.001

資料來源：本研究整理

三、非層次集群分析法(non-hierarchical methods)－K 平均數法(K－means methods)

藉由集群分析來看填答者對於組織承諾與工作滿意度是否有明顯的區別，集群分析的目地主要是將具有某些共同特性者與以整合在同一群(吳萬益和林清河,2000)。組織承諾的問項共有 15 題，本研究利用 K 平均數法將組織承諾的填答狀況分為三群，K 平均數法是以 K 個中心值為中心，將個體中與中心點較接近者納入該群中，依各個體到各群中心點之距離遠近重新計算出各集群值之集結係數，持續重複計算，一直到中心點與個體不能在移動為止(吳萬益和林清河,2000)。

表 4-10 為組織承諾與員工資訊安全政策的行為意圖之關聯性，將員工對組織的承諾高低分為三群，為組織承諾高(簡稱 1)、組織承諾中(簡稱 2)與組織承諾低(簡稱 3)，集群中心點各為 6.01、4.88、3.82，由這三集群來觀察組織承諾的分數高低對員工採用技術性控制措施的意圖與遵循程序性控制措施的意圖之影響，將組織承諾的集群分出後，再計算員工的採用意圖與遵循意圖分別於該集群的平均數，由平均數可看出，對組織較沒有歸屬感的員工，在採用與遵循資訊安全措施的意願也較低落；對組織有較高承諾的員工，也會比較願意採用與遵循公司的資訊安全措施。

技術性控制措施的採用意圖和程序性控制措施的遵循意圖平均數相比，發現程序性控制措施的遵循意圖的平均數在組織承諾高、中、低三集群皆高於技術性控制措施的採用意圖的平均數，可發現員工遵循程序性控制措施的意願比採用技術性控制措施要來的高。

將員工對技術性控制措施的採用意圖與程序性控制措施的遵循意圖各三個集群進行單因子變異數分析，利用 LSD 法比較集群之間的差異，分析結果發現，採用意圖的 $F_{(2,211)}$=12.452，p-value=0.000，F 值為顯著，組織承諾的三集群之間皆有顯著，組織承諾高的明顯大於組織承諾中的，組織承諾中的明顯大於組織承諾低的，組織承諾高的明顯大於組織承諾低的，這三集群對員工的技術性控制措施採用意圖有顯著影響；在遵循意圖部分，遵循意圖的 $F_{(2,212)}$=14.625，p-value=0.000，F 值為顯著；由統計結果可知，組織承諾高的與組織承諾中的員工，對於組織承諾低的員工有明顯較高的資訊安全政策遵循意圖。

表 4-10 組織承諾(X1)與資訊安全政策行為意圖(Y)之關聯性

組織承諾 (X1)		資訊安全政策行為意圖 (Y)	
集群	集群中心點	技術性控制措施採用意圖 (Y1)	程序性控制措施遵循意圖 (Y2)
組織承諾高(1) (N=65)	6.01	6.26	6.31
組織承諾中(2) (N=96)	4.88	5.88	6.14
組織承諾低(3) (N=54)	3.82	5.54	5.62
ANOVA 檢定結果	F 值	12.452***	14.625***
	LSD 多重比較	1>2(**) 2>3(**) 1>3(***)	1>3(***) 2>3(***)

顯著水準 †P<0.1 * P<0.05 ** P<0.01 *** P<0.001
資料來源：本研究整理

表 4-11 為工作滿意度與員工資訊安全政策的行為意圖之關聯性，將員工對工作的滿意程度分為三群，為工作滿意度高、工作滿意度中與工作滿意度低，各集群的中心點為 6.29、5.28、4.05，觀察員工的工作滿意度的高低對採用技術性控制措施的意圖與遵循程序性控制措施的意圖之影響。將工作滿意度的集群分出後，再計算採用意圖與遵循意圖於該集群的平均數，由表中可以看出，對工作滿意程度較低的員工，於採用與遵循資訊安全政策的意願也較低落；對工作較滿意的員工，也會比較願意遵循與採用公司的資訊安全政策。

技術性控制措施的採用意圖和程序性控制措施的遵循意圖平均數相比，發現程序性控制措施之遵循意圖在工作滿意度的高、中、低三集群之平均數，皆高於技術性控制措施的採用意圖的平均數，可發現員工遵循程序性控制措施的意願比採用技術性控制措施要來的高。

將員工對技術性控制措施的採用意圖與程序性控制措施的遵循意圖各三個集群進行單因子變異數分析，利用 LSD 法比較集群之間的差異，根據統計結果，技術性控制措施的採用意圖 $F_{(2,211)}=10.890$，p-value=0.000，F 值顯著，結果發現，工作滿意度高的對工作滿意度中與工作滿意度低的員工有明顯較高的技術性控制措施的採用意圖；在遵循意圖部分，遵循意圖的 $F_{(2,212)}=18.943$，p-value=0.000，F 值為顯著，工作滿意度三集群之間皆有明顯區別，顯示員工對工作的滿意程度會影響員工的程序性控制措施的遵循意圖。

表 4-11　工作滿意度(X2)與資訊安全政策行為意圖(Y)之關聯性

工作滿意度 (X2)		資訊安全政策行為意圖 (Y)	
集群	集群中心點	技術性控制措施採用意圖 (Y1)	程序性控制措施遵循意圖 (Y2)
工作滿意度高(1) (N=73)	6.29	6.25	6.44
工作滿意度中(2) (N=111)	5.28	5.78	5.94
工作滿意度低(3) (N=31)	4.05	5.58	5.60
ANOVA 檢定結果	F 值	10.890***	18.934***
	LSD 多重比較	(1)>(2)(***) (1)>(3)(***)	(1)>(2)(***) (2)>(3)(**) (1)>(3)(***)

顯著水準 †P<0.1　* P<0.05　** P<0.01　*** P<0.001

資料來源：本研究整理

第五章　結論與建議

在此章，將討論本研究的研究結果、研究貢獻與管理義涵，本研究在操作時所面臨的操作限制，並給予後續的研究者研究建議與方向。

第一節　研究結論

本研究的研究目的欲探討工作情境相關態度對員工遵循或採用資訊安全措施的影響程度，透過第四章的資料分析，得到的統計檢定結果彙整如表 5-1 所示：

表 5-1　研究假設檢定結果摘要表

研究假設	結果
H_{1a}：組織承諾對資訊安全政策所規範之程序性控制措施的遵循意圖有正向關係。	成立
H_{1b}：組織承諾對資訊安全政策所規範之技術性控制措施的採用意圖有正向關係。	成立
H_{2a}：工作滿意度對資訊安全政策所規範之程序性控制措施的遵循意圖有正向關係。	成立
H_{2b}：工作滿意度對資訊安全政策所規範之技術性控制措施的採用意圖有正向關係。	不成立
H_{3a}：資安措施的態度對資訊安全政策所規範之程序性控制措施的遵循意圖有正向關係。	成立
H_{3b}：資安措施的態度對資訊安全政策所規範之技術性控制措施的採用意圖有正向關係。	成立
H_{4a}：自我效能對資訊安全政策所規範之程序性控制措施的遵循意圖有正向關係。	成立
H_{4b}：自我效能對資訊安全政策所規範之技術性控制措施的採用意圖有正向關係。	成立
H_{5a}：主觀規範對資訊安全政策所規範之程序性控制措施的遵循意圖有正向關係。	成立
H_{5b}：主觀規範對資訊安全政策所規範之技術性控制措施的採用意圖有正向關係。	成立

資料來源：本研究整理

一、員工之組織承諾與其資訊安全政策行為意圖之關係

本研究結果顯示，組織承諾對資訊安全政策所規範之程序性控制措施的遵循意圖與技術性控制措施的採用意圖有正向關係。員工遵循資訊安全程序措施所付出的成本相較於採用技術性控制措施要來的低，也較簡單，根據集群分析的結果看來，組織承諾偏高的員工的確會比低組織承諾的員工願意遵循程序性的資訊安全措施。採用技術性的資訊安全措施需要員工多付出額外的心力與時間，對組織承諾較高的員工，才會比較願意去多為公司付出。

二、員工之工作滿意度與其資訊安全政策行為意圖之關係

本研究結果顯示，工作滿意度對資訊安全政策所規範之程序性控制措施的遵循意圖有正向關係，但對技術性控制措施的採用意圖無顯著影響。根據集群分析的結果，工作滿意度高的員工相較於對工作的滿意度中等或較低的員工願意遵循程序性控制措施。採用技術性的資訊安全措施需要員工多付出額外的心力與時間，由本研究的結果看來，具有工作滿意度能讓員工願意遵循程序性控制措施，但無法讓員工採用技術性控制措施。

三、員工之資安措施的態度與其資訊安全政策行為意圖之關係

本研究結果顯示，資訊安全措施的態度與員工遵循程序性控制措施的意圖與採用技術性控制措施的意圖有顯著影響，員工對資訊安全措施的態度愈趨正面，員工有更高意願去遵循程序性控制措施或採用技術性控制措施。

四、自我效能與其資訊安全政策行為意圖之關係

本研究結果顯示，自我效能對員工程序性控制措施的遵循意圖或技術性控制措施採用意圖有顯著影響，自我效能是員工本身自己所具備的個人技巧、知識與能力，對資訊安全領域具有相關知識能力的員工，會更願意去遵循公司所頒布的程序性資訊安全措施，也更願意去採用公司要求的技術性控制措施。

五、主觀規範與其資訊安全政策行為意圖之關係

員工對資訊安全政策的行為意圖會受到主觀規範的影響，主觀規範為員工的上司、同事、下屬或與公司相關的重要人士給予的期望行為而造成的社會壓力，因此，研究的檢定結果顯示出，員工對程序性控制措施的遵循意圖或技術性控制措施的採用意圖會受到公司內外部的重要人士的影響。

六、工作情境相關兩態度變數與其資訊安全政策行為意圖之關係

根據集群分析的結果，整體而言，不論是工作滿意度或組織承諾這兩項度變數的任一集群，其程序性控制措施的遵循意圖之平均數皆大於技術性控置措施的採用意圖之平均數，這顯示了員工不論組織承諾或工作滿意度高低，對於遵循程序性控制措施的意願都要比採用技術性控制措施的意願要來得高。

第二節　研究貢獻與管理義涵

一、研究貢獻

透過本研究結果，提出過去未被學者所關注的新發現，也提供後續的研究者有繼續探討的方向：

(一) 雖然過去研究證實組織行為相關變數會影響資訊科技的導入至組織中成功與否，也會影響到員工程序性控制措施的遵循意圖，但由本研究結果發現，加入資訊安全措施的態度變數後，工作滿意度與組織承諾的影響變的不顯著，除了個變數之間具有正相關性，導致資安措施態度加入後工作滿意度與組織承諾變的不顯著之外，另外也顯示出員工對資訊安全措施的態度會較另外兩項工作情境相關態度來的重要。

(二) 過去對程序性控制措施的遵循意圖與技術性控制措施的採用意圖研究大多專注在資訊安全相關的看法與對資安措施的態度上，而本研究加入組織行為的兩項重要態度變數後，能幫助學術界與實務界對於資訊安全控制措施的遵循意圖與執行意圖前因理解更完整。

(三) 發現工作滿意度與組織承諾這兩項工作情境相關態度變數，對遵循員工的程序性控制措施比採用技術性控制措施要來的更為願意去執行，顯示出公司在導入技術性控制措施時，需要更多的時間來讓員工願意採用技術性控制措施。

二、管理意涵

(一) 這篇研究將對資訊安全措施的態度、自我效能、主觀規範的題項分為程序性控制措施的遵循意圖與技術性控制措施的採用意圖，從結果中發現，組織承諾高的員工會比較願意去遵循程序性控制措施與採用技術性控制措施，採用技術性的控制措施比遵循程序性控制措施更需要付出時間與心力，這表示未來公司需要導入新的技術性控制措施時，可經由對組織較有歸屬感的員工來影響組織承諾較低的員工，使這些對組織較無歸屬感的員工也能遵循程序性控制措施與採用技術性控制措施。

(二) 由結果看出，資訊安全措施的態度對員工的遵循意圖與採用意圖皆有影響，組織承諾對員工的程序性控制措施的遵循意圖與技術性控制措施的採用意圖

有影響，工作滿意度會影響員工對程序性控制措施的遵循意圖。顯示出公司未來在推行資訊安全政策時，除了重視到組織對員工資訊安全政策的教育訓練之外，也需要重視到軟性態度的影響，像是組織環境的工作氣氛，員工對組織的歸屬感、員工對工作的滿意程度等因素，才能讓員工更願意為組織努力，更願意遵循程序性控制措施或採用技術性控制措施。

第三節　研究限制與後續研究建議

一、研究限制

本研究受到人力、時間、問卷發放方式等方面的限制，提供給未來後續的研究者參考並修正，使未來的研究者的研究能更趨完善，以下為本研究所受到的限制：

(一) 本研究的樣本來源多半是透過已在工作的親友幫忙，親友大多針對自己所工作的部門給予同事幫忙問卷的填寫，難以控制填答者的服務部門，因此同一公司的回收問卷會受限於單一部門，無法確定其他部門的狀況，因此此論文的類推性有限。

(二) 問卷發放是透過已在工作的親戚或同學來幫忙填寫，因此大部分的問卷年齡都集中在 30 歲以下，且職位大多為非主管，主管與一般員工對於資訊安全需要擔負的責任不同，所以填答方向不相同。

二、後續研究方向

(一) 因為主管與一般員工在資訊安全需要擔負的資訊安全責任程度不同，因此對資訊安全政策的態度與表現也會不同，若主管與一般員工的回收比例配置相當，那麼即可比較出主管與一般員工對於程序性控制措施與技術性控制措施的態度。

(二) 資訊安全部門與非資訊安全部門的專業能力程度不同，冀望能夠在各個部門收到的資料比例相同，以期能夠分析不同部門之比較。

參考文獻

英文部分

1. Anderson, C. L., & Agarwal, R. (2010). Particing Safe Computing: A Multimethod Empirica Examination of Home Computer User Security Behavioral Intentions.. *MIS Quarterly, 34*(3), 613-A615.
2. Agarwal, R. and Prasa, J. (1998a), "The antecedents and consequents of user perceptions in information technology adoption", Decision Support Systems, Vol. 22, No. 1, pp. 15–29.
3. Agarwal, R. and Prasa, J. (1998b), "A conceptual and operational definition of personal innovativeness in the domain of information technology", Information Systems Research, Vol. 9, No. 2, pp. 204–215.
4. Agarwal, R. and Karahanna, E. (2000), "Time Files When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage", MIS Quarterly, Vol. 24, No. 4, pp. 665–694.
5. Ajjan, H., & Hartshorne, R. (2008). Investigating faculty decisions to adopt Web 2.0 technologies: Theory and empirical tests. *The Internet and Higher Education, 11*(2), 71-80.
6. Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.
7. Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.
8. Allen, N. J., & Meyer, J. P. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. *Journal of occupational psychology, 63*(1), 1-18.
9. Anderson, C. L., & Agarwal, R. (2010). Particing Safe Computing: A Multimethod Empirica Examination of Home Computer User Security Behavioral Intentions. [Article]. *MIS Quarterly, 34*(3), 613-A615.
10. Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review, 84*(2), 191.
11. Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*: Prentice-Hall, Inc.
12. Bateman, T. S., and Organ, D. W. (1983). Job Satisfaction and the Good Soldier:

The Relationship Between Affect and Employee "Citizenship". *Academy of Management Journal, 26*(4), 587-595.

13. Bell, S., and Menguc, B. (2002). The employee-organization relationship, organizational citizenship behaviors, and superior service quality. Journal of Retailing 78(2), 131-146.
14. Brancheau, J. C., and Wetherbe, J. C. (1990), "The Adoption of Spreadsheet Software Testing innovation diffusion theory in the Context of End-User Computing", Information Systems Research, Vol. 1, No. 1, pp. 41–64.
15. Brown, K., & Mitchell, T. (1993). Organizational obstacles: Links with financial performance, customer satisfaction, and job satisfaction in a service environment. *Human Relations, 46*(6), 725.
16. Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548.
17. Cavusoglu, H., Cavusoglu, H., Son, J.-Y., and Benbasat, I. 2009."Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers," working paper,Sauder School of Business, University of British Columbia.
18. Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security. v1 i3*.
19. Chang, A.J.T. and Yeh, Q.J. (2006), "Coping With Systems Threats: A Study of the Adequacy of Security in Taiwan", The 3rd IEEE International Conference on Management of Innovation and Technology (ICMIT 2006), June, Singapore.
20. Chang, A. J.-T. (2010) Roles of perceived risk and usefulness in information system security adoption. The 5th IEEE International Conference on Management of Innovation and Technology (ICMIT 2010), Singapore.
21. Chenoweth, T., Minch, R., & Gattiker, T. (1899). Application of Protection Motivation Theory to Adoption of Protective Technologies. Paper presented at the 42nd Hawaii International Conference on System Science.
22. CNSS, National Information Assurance (IA) Glossary (CNSS Instruction No.4009), Committee on National Security Systems, Revised in June 2006, http://www.cnss.gov/instructions.html. [Cited July 5, 2006].

23. Cronbach, L. J., & Meehl, P. E. (1955). Construct validity in psychological tests. *Psychological Bulletin, 52*(4), 281.
24. Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.
25. Durgin, M. 2007. "Understanding the Importance of and Implementing Internal Security Measures," SANS Institute Reading Room (https://www2.sans.org/reading_room/whitepapers/policyissues/1901.php).
26. Ernst & Young. 2008. "Moving Beyond Compliance: Ernst &Young's 2008 Global Information Security Survey" (available online at http://www.ey.com/Publication/vwLUAssets/2008_Global_Information_Security_Survey_english/$FILE/2008_GISS_ingles.pdf).
27. Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research.* Reading, MA: Addison-Wesley.
28. Forcht, K.A. (1994), *Computer security management*. Danvers, MA: Boyd and Fraser.
29. George, J., and Jones, G. (1997). Organizational spontaneity in context. Human Performance 10(2), 153-170.
30. Gerber, M. and von Solms, R. (2005), "Management of risk in the information age", Computers & Security, Vol. 24, pp.16–30.
31. Greene, G. (2010). *Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance*.
32. Herath, T., & Rao, H. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.
33. Hoffer, J.A. and Alexander M.B. (1992), "The Diffusion of Database Machines", Data Base, Vol. 23, No.2, pp. 13-20.
34. Hoppock, R. (1935). *Job satisfaction.* New York: Harper.
35. Jahangir, N., Akbar, M. M., & Haq, M. (2004). organizational citizenship behavior:it's nature and antecedents. *BRAC University Journal, 1(2)*, 75-85.
36. Johnston, A., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly, 34*(1).
37. Katz, D., & Kahn, R. L. (1978). The social psychology of organizations (2d ed.): Wiley.

38. Kankanhalli, A., Teo, H.-H., Tan, B. C.Y. and Wei, K.-K. (2003), "An integrative study of information systems security effectiveness", *International Journal of Information Management*, Vol. 23, pp.139–154.
39. Lee, J., and Lee, Y. (2002). "A Holistic Model of Computer Abuse Within Organizations," *Information Management and Computer Security* (10:2/3), pp. 57-63.
40. Lee, S. M., Lee, S. G., and Yoo, S.(2003). "An Integrative Model of Computer Abuse based on Social Control and General Deterrence Theories," *Information and Management* (41:6), pp. 707-718.
41. Lee, Y., & Kozar, K. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management, 45*(2), 109-119.
42. Locke, E. A. (1976). The Nature and Causes of Job Satisfaction. *Handbook of industrial and organizational psychology (1990) Dunnette, MD; Hough, LM. Palo Alto, CA: Consulting Psychologists Press.*, 1319-1328.
43. Madnick, E.S. (1978), "Management Policies and Procedures Needed for Effective Computer Security", Sloan Management Review, Fall, pp.61–74.
44. Mayo, E. (1971). Hawthorne and the western electric company. *Organisation Theory*.
45. Moore, G.C. (1987), "End User Computing and Office Automation: A Diffusion of Innovations Perspective", Infor, Vol. 25 No. 3, pp.214–235.
46. Morrow, P. C. (1983). Concept redundancy in organizational research: The case of work commitment. *The Academy of Management Review, 8*(3), 486-500.
47. Mowday, R. T., Steers, R. M., & Porter, L. W. (1979). The measurement of organizational commitment* 1. *Journal of vocational behavior, 14*(2), 224-247.
48. Mowday, R. T., Porter, L. W., & Steers, R. M. (1982). *Employee-organization linkages: The psychology of commitment, absenteeism, and turnover*: Academic Press New York.
49. Mowday, R. (1998). Reflections on the study and relevance of organizational commitment. Human Resource Management Review, 8(4), 387-401.
50. Nilikanta, S. and Scammell, R.W. (1990), "The effects of information sources and communication channels on the diffusion of innovation on a data base development environment", Management Science, Vol. 36, No. 1, pp.24–40.

51. Organ, D. W. (1988). *Organizational citizenship behavior: The ''Good Soldier" syndrome.* MA: Lexington Books.
52. Organ, D., and Ryan, K. (1995). A meta analytic review of attitudinal and dispositional predictors of organizational citizenship behavior. Personnel Psychology 48(4), 775-802.
53. Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance*.
54. Podsakoff, P., and MacKenzie, S. (1994). Organizational citizenship behaviors and sales unit effectiveness. Journal of Marketing Research 31(3), 351-363.
55. Podsakoff, P., MacKenzie, S., Paine, J., and Bachrach, D. (2000). Organizational citizenship behaviors: A critical review of the theoretical and empirical literature and suggestions for future research. Journal of management 26(3), 513.
56. Porter, L. W., & Lawler, E. E. (1968). Managerial attitudes and performance. *Irwin, New Jersey*.
57. Porter, L., Steers, R., Mowday, R., & Boulian, P. (1974). Organizational commitment, job satisfaction, and turnover among psychiatric technicians. *Journal of Applied Psychology, 59*(5), 603-609.
58. Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646.
59. Rainer, R.K. Jr., Snyderr, C.A. and Carr, H.H. (1991), "Risk analysis for information technology", *Journal of Management Information Systems*, Vol. 8, No. 1, Summer, pp.192–197.
60. Randall, D. (1987). Commitment and the organization: The organization man revisited. Academy of management review 12(3), 460-471.
61. Richardson, R. L., & Institute, C. S. (2007). *CSI survey 2007: The 12th annual computer crime and security survey*: Computer Security Institute.
62. Robbins, S. P., & Langton, N. (1998). *Organizational behavior: Concepts, controversies, and applications*: Prentice Hall Upper Saddle River, New Jersey:.
63. Rogers, R. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology, 91*(1), 93-114.
64. Rogers, E.M. (1983), *Diffusion of Innovations*, 3rd ed., New York, NY: The Free Press.

65. Smith, P. C., Kendall, L. M., & Hulin, C. L. (1969). *The measurement of satisfaction in work and retirement.* Chicago:Rand McNally.
66. Smith, C. A., Organ, D. W., & Near, J. P. (1983). Organizational citizenship behavior: Its nature and antecedents. *Journal of Applied Psychology*, 68, 653-663.
67. Spector, P. E. (1985). Measurement of human service staff satisfaction: Development of the Job Satisfaction Survey. *American journal of community psychology, 13*(6), 693-713.
68. Spector, P. E. (1997). *Job satisfaction: Application, assessment, cause, and consequences* (Vol. 3): Sage Publications, Inc. Spector, P. E. (1997).
69. Stanton, J., Stam, K., Guzman, I., & Caledra, C. (2003). *Examining the linkage between organizational commitment and information security*. In *IEEE Systems, Man, and Cybernetics Conference* Washington DC,USA. ‘
70. Steers, R. M. (1977). Antecedents and outcomes of organizational commitment. *Administrative Science Quarterly, 22*(1), 46-56.
71. Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication, 800*, 30.
72. Straub Jr, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly*, 45-60.
73. Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research, 6*(2), 144-176.
74. Weiss, D. J., Dawis, R. V., & England, G. W. (1967). Manual for the Minnesota Satisfaction Questionnaire. *Minnesota Studies in Vocational Rehabilitation*.
75. White, G. B., Fisch, E. A. and Pooch, U.W. (1996), Computer system and network security, Boca Raton, FL: CRC Press.
76. Wiener, Y. (1982). Commitment in organizations: A normative view. Academy of management review 7(3), 418-428.
77. Williams, L., & Anderson, S. (1991). Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. *Journal of Management, 17*(3), 601.
78. Yeh, Q. J., & Chang, A. J. T. (2007). Threats and countermeasures for information system security: A cross-industry study. Information & Management, 44(5), 480-491.

中文部分

79. 經濟部標準檢驗局，資訊技術-安全技術-資訊安全管理系統-要求事項 CNS 27001,X6049，2006 年 6 月 16 日.
80. 經濟部標準檢驗局，資訊技術-安全技術-資訊安全管理之作業規範 CNS 27002, X6040，2007 年 10 月 24 日.
81. BSI 標準組織台灣官網 http://www.bsigroup.tw/zh-tw/.
82. Societe Generale de Surveillance(SGS)台灣檢驗科技股份有限公司台灣官網 http://www.tw.sgs.com/zh_tw/mini_site_iso27001_tw_1-1.
83. 行政院主計處，電腦應用概況報告 http://www.dgbas.gov.tw/ct.asp?xItem=28145&CtNode=5526&mp=1.
84. 許士軍(1991)，管理學，台北：東華書局.
85. 吳定, 張潤書, 陳德禹, 賴維堯, & 許立一 (Eds.). (2010). 行政學 (二版九刷 ed.): 國立空中大學.
86. 吳萬益、林清河(2000)，企業研究方法，台北：華泰書局。
87. 邱皓政(2003)量化研究與統計分析：SPSS 中文視窗版資料分析範例解析(二版三刷)，台北：五南出版社.
88. 陳淑玲. (2002). 影響新人類組織承諾相關因素之研究. 中華管理學報, 3(1), p.75-88.
89. 李東峰、林子銘(2001)，風險評估觀點的資訊安全規劃架構，台灣大學資訊管理學系第十二屆國際資訊管理學術研討會。
90. 葉桂珍、張榮庭 (2006)，企業之資訊安全策略與其產業別及資訊化程度關係探討，*資訊管理學報*，Vol. 13, No.2, pp. 113-144.

附錄一

您好！我是東海大學企業管理研究所碩士班學生，目前在張榮庭老師及吳祉芸老師的指導下，研究資訊安全管理相關議題，為使本研究能反映業界狀況，希望您協助填答本問卷，共計五頁。您的意見有助於我們了解員工對公司資訊安全政策的看法。

答案僅提供學術研究分析之用，不會外流。感謝您的協助，我們在此致上最誠摯的謝意與祝福！為表感謝，在收到填好之問卷後，我們將寄贈便利商店禮券一份致謝，謝謝您撥冗幫忙。

東海大學企業管理研究所

指導教授　張榮庭 博士
吳祉芸 博士

研究生　劉昊雯 敬上

第一部分　基本資料

1. 請問 貴公司產業別：□顧問業 □傳統製造業(包含食品、塑膠、紡織...等產業)
   □醫療業 □教育業 □電子業 □金融保險業 □水電燃氣業
   □零售業 □服務業 □法律業 □媒體通訊業 □交通運輸業
   □資訊與高科技業 □一般商業與貿易 □政府機關
   □消費品產業 □其他(請填寫)_____
2. 請問 貴公司員工人數約：□50 人以下 □51~100 人 □101~200 人 □201~500 人
   □501~1000 人 □1001~2000 人 □2001~5000 人 □5001 人以上
3. 請問您於 貴公司服務年資： □1~5 年 □6~10 年 □11~15 年 □16~20 年 □20 年以上
4. 請問您於現在產業服務年資：□1~5 年 □6~10 年 □11~15 年 □16~20 年 □20 年以上
5. 請問您服務的部門：□生產作業 □行銷企劃 □人力資源 □產品研發 □財務會計
   □資訊部門 □安全部門 □業務部門 □行政部門 □採購單位
   □稽核部門 □工程單位 □其他(請填寫)_____
6. 請問您的職位： □主管(包含基層、中階與高階主管) □非主管
7. 請問您的性別： □男性 □女性
8. 請問您的年齡： □20 歲以下 □21~25 歲 □26~30 歲 □31~35 歲 □36~40 歲
   □41~45 歲 □46~50 歲 □51~55 歲 □56~60 歲 □61~65 歲
9. 請問您的教育程度：□國中及以下 □高中(職)□專科 □大學 □碩士 □博士

第二部分 資訊安全

此部份將詢問您在組織中對於資訊安全相關措施的看法，題項中名詞意涵如下：

一、「資訊系統」包含電腦軟硬體以及周邊實體環境。

二、一般組織資訊安全政策所規範的安全措施分為兩種：

(1)**技術性的安全控制措施**：例如防毒軟體、防火牆、入侵偵測系統以及資訊安全相關軟硬體的建置或採用。

(2)**非技術性的安全控制措施**：資訊安全政策所規範的**程序或規則**，例如系統當機的緊急應變程序、機密資訊分類方式、密碼編制規則、遵守組織所訂定的資訊安全相關命令、遵守相關法律與法規、按照時程更新系統與防毒軟體、在資訊安全事件發生時，按照組織規定的通報程序儘速通報。

每家公司資訊安全政策寬嚴程度不一，若 貴公司目前無明確規範，請依題意之描述加以預想並填答。

請根據您同意程度，勾選**最符合者**

問　　項	非常不同意	不同意	有點不同意	沒意見	有點同意	同意	非常同意
1. 我們公司目前有明確的資訊安全政策或規範							
2. 採取**技術性的安全控制措施**來保護公司的資訊系統是好的。							
3. 採取公司所訂定的**技術性的安全控制措施**來保護公司的資訊系統是重要的。							
4. 我樂意採取**技術性的安全控制措施**來保護公司的電腦。							
5. 遵循公司訂定的資訊安全**程序或規則**是必要的。							
6. 遵循公司訂定的資訊安全**程序或規則**是重要的。							
7. 遵循公司訂定的資訊安全**程序或規則**對我的工作有好處。							
8. 遵循公司訂定的資訊安全**程序或規則**對我的工作有幫助。							
9. 公司訂定的資訊安全政策帶給我的好處多於壞處。							
10. 遵循或採用資訊安全措施是好的。							
11. 我打算遵守組織所要求的資訊安全**程序或規則**。							
12. 我打算依照組織所訂定的資訊安全**程序或規則**來保護公司的資訊和科技資源。							
13. 當我使用公司資訊資源時，我會執行組織訂定的資訊安全規範。							

問　　項	非常不同意	不同意	有點不同意	沒意見	有點同意	同意	非常同意
14. 我打算使用公司政策所規定的防毒軟體、防火牆...等**技術性安全控制措施**來保護資訊系統。							
15. 未來我很有可能使用**技術性安全控制措施**保護資訊系統。							
16. 我很確信未來我會採用**技術性安全控制措施**來保護資訊系統。							
17. 我計畫使用**技術性安全控制措施**。							
18. 未來我會把公司規定的**技術性安全控制措施**導入資訊系統中。							
19. 我具有必要的技能來遵循公司訂定的資訊安全**程序或規則**。							
20. 我具有必要的技能來採用公司所規範的**技術性安全控制措施**。							
21. 我具有足夠的知識來遵循公司訂定的資訊安全**程序或規則**。							
22. 我具有足夠的知識來採用公司所規範的**技術性安全控制措施**。							
23. 我具有必要的能力來遵循公司訂定的資訊安全**程序或規則**。							
24. 我具有必要的能力來採用公司所規範的**技術性安全控制措施**。							
25. 我在遵循公司訂定的資訊安全**程序或規則**時覺得很自在。							
26. 我在採用公司所規範的**技術性安全控制措施**時覺得很自在。							
27. 我在遵循公司訂定的資訊安全**程序或規則**時容易上手。							
28. 我在採用**技術性安全控制措施**時容易上手。							
29. 我擁有能力和知識去遵循公司訂定的資訊安全**程序或規則**。							
30. 我擁有能力和知識去採用公司所規範的**技術性安全控制措施**。							
31. 使用**技術性安全控制措施**完全在我的控制之中。							
32. 遵循公司訂定的資訊安全**程序或規則**完全在我的控制之中。							
33. 同事認為我應該遵循公司訂定的資訊安全**程序或規則**。							
34. 同事認為我應該採取**技術性的安全措施**來保護資訊系統。							
35. 主管認為我應該遵循公司訂定的資訊安全**程序或規則**。							
36. 主管認為我應該採取**技術性的安全措施**來保護資訊系統。							
37. 對我有影響的重要人物認為我應該遵循公司訂定的資訊安全**程序或規則**。							
38. 對我有影響的重要人物認為我應該採取**技術性的安全措施**保護電腦系統。							

第三部分　工作滿足

請根據您實際情形來決定同意程度，勾選**最符合者**

問　　項	非常不同意	不同意	有點不同意	沒意見	有點同意	同意	非常同意
1. 我認為我的工作負荷量是適當的。							
2. 公司讓我有機會獨當一面完成工作。							
3. 我的工作有機會接觸不同的事物。							
4. 我的工作讓我在公司中有機會成為一位出色的人物。							
5. 我的主管對待部屬的方式讓我滿意。							
6. 我對於主管制定決策的能力有信心。							
7. 做任何事情我能夠不違反我的道德原則。							
8. 我的公司提供我一個穩定的就業環境。							
9. 我的工作能夠讓我有機會與他人共事。							
10. 我的工作讓我有機會能夠指導別人該如何做。							
11. 我的工作讓我能夠有機會發揮才能完成工作。							
12. 我對公司執行的政策相當滿意。							
13. 我所做的工作份量與我所得到的報償讓我滿意。							
14. 我的工作職位有機會晉升。							
15. 我有足夠自由可運用自己的判斷能力。							
16. 我有機會可以用自己的方法來處理我的工作。							
17. 工作的環境讓我覺得舒適滿意。							
18. 我可以和同事相處融洽。							
19. 當我在工作上表現良好時，能夠得到大家的讚賞。							
20. 我能夠由現在從事的工作得到成就感。							

第四部分 組織承諾

請根據您實際情形來決定同意程度，勾選**最符合者**

問　　項	非常不同意	不同意	有點不同意	沒意見	有點同意	同意	非常同意
1. 我願意付出額外的努力以協助公司獲得成功。							
2. 只要公司性質相似，到別家去做也無所謂。							
3. 我很慶幸當年找工作時，選擇了這家公司。							
4. 繼續留在這個公司內，不會有什麼好處。							
5. 我經常不贊成公司內一些與員工有關的規定。							
6. 向別人提起自己是這家公司的一員時，感到很自傲。							
7. 我決定在這家公司做事，顯然是一件錯誤的事。							
8. 如果組織目前的情況有些許改變，我可能會離開這間公司。							
9. 我覺得我服務的公司是一個值得效勞的好公司。							
10. 我對於我所服務的公司沒有什麼忠誠可言。							
11. 為了繼續留在公司，我願意接受公司所指派的任何工作。							
12. 我感覺自己與公司所重視的事十分相近。							
13. 在這個公司之內做事能使我充分發揮自己的能力。							
14. 我十分關心公司的未來。							
15. 對我來說，這家公司是我所待過公司中最好的公司。							

請您再檢查一次是否**全部**填寫完畢，請**避免漏填任何一題，**

本問卷到此結束，非常感謝您的幫忙!