國立台東大學資訊管理學系
環境經濟資訊管理碩士在職專班
碩士論文

空軍人員資訊安全素養之評量與分析

研究生：鄭宇凱　撰
指導教授：謝昆霖　先生

中華民國九十八年六月

國立台東大學
學位論文考試委員審定書

系所別：資訊管理學系

本班 鄭宇凱 君

所提之論文 空軍人員資訊安全素養之評量與分析

業經本委員會通過合於 碩士學位論文 條件

論文學位考試委員會：

（學位考試委員會主席）

（指導教授）

論文學位考試日期： 98 年 6 月 22 日

國 立 台 東 大 學

博碩士論文電子檔案上網授權書

（提供授權人裝訂於紙本論文書名頁之次頁用）

本授權書所授權之論文為授權人在 國立臺東大學 資訊管理學系碩士班 _____組 97 學年度第 二 學期取得 碩士 學位之論文。

論文題目： 空軍人員資訊安全素養之評量與分析
指導教授： 謝昆霖先生

茲同意將授權人擁有著作權之上列論文全文（含摘要），非專屬、無償授權國家圖書館及本人畢業學校圖書館，不限地域、時間與次數，以微縮、光碟或其他各種數位化方式將上列論文重製，並得將數位化之上列論文及論文電子檔以上載網路方式，提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印。

1 讀者基非營利性質之線上檢索、閱覽、下載或列印上列論文，應依著作權法相關規定辦理。

授權人： 鄭宇凱
簽　名： 鄭宇凱　　中華民國 98 年 06 月 22 日

博碩士論文授權書

本授權書所授權之論文為本人在 國立臺東大學 環境經濟資訊管理 系(所)
組 97 學年度第 2 學期取得 碩 士學位之論文。

論文名稱：空軍人員資訊安全素養之評量與分析

本人具有著作財產權之論文全文資料，授權予下列單位：

同意	不同意	單　位
☑	☐	國家圖書館
☑	☐	本人畢業學校圖書館
☐	☑	與本人畢業學校圖書館簽訂合作協議之資料庫業者

得不限地域、時間與次數以微縮、光碟或其他各種數位化方式重製後散布發行或上載網站，藉由網路傳輸，提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印。

☐同意 ☑不同意 本人畢業學校圖書館基於學術傳播之目的，在上述範圍內得再授權第三人進行資料重製。

本論文為本人向經濟部智慧財產局申請專利(未申請者本條款請不予理會)的附件之一，申請文號為：_____，請將全文資料延後半年再公開。

公開時程

立即公開	一年後公開	二年後公開	三年後公開
			✓

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權為非專屬性發行權利。依本授權所為之收錄、重製、發行及學術研發利用均為無償。上述同意與不同意之欄位若未勾選，本人同意視同授權。

指導教授姓名：　　(親筆簽名)

研究生簽名：　　(親筆正楷)

學　　號：4396005　　(務必填寫)

日　　期：中華民國　98　年　06　月　22　日

1.本授權書 (得自 http: //www.lib.nttu.edu.tw/theses/ 下載) 請以黑筆撰寫並影印裝訂於書名頁之次頁。

2.依據 91 學年度第一學期一次教務會議決議:研究生畢業論文「至少需授權學校圖書館數位化，並至遲於三年後上載網路供各界使用及校內瀏覽。」

授權書版本:2008/05/29

誌謝辭

驪歌聲起，兩年的努力在此刻得到了肯定，過去的我從二技到研究所，一直都是過著半工半讀的生活，酸甜苦辣點滴在心頭，只為了達成自己設定的目標。當初，因為工作的關係輪調到了台東，心情其實很沮喪，破壞了原本既定的計畫，也因為工作的關係，碰觸了資訊這一塊，更讓我因禍得福，順利的考上研究所，內心無比激動，使我能完成遠程的學歷目標。

在論文寫作的過程中，我要特別感謝所有授課的教授，尤其王文清老師及鐘青萍老師，讓我打開眼界，清楚的了解一個完整的研究是要如何進行，特別是在我苦思論文題目的過程中，給了我很多心靈上的鼓勵與支持，協助我確定了論文的方向，在後續論文的研究中給予的指導更是珍貴，才讓研究得以順利進行；除了授課的教授外，最重要的還是我的指導教授謝昆霖老師，經由他的指導，更讓我清楚的聚焦在自己工作上的困境，進而產生了本篇研究主題，除了幫助我確定研究方法之外，更讓我在這個研究中，學習到自己永遠不會接觸的另一塊知識領域。

除了三位口考的指導教授之外，我也要一併感謝研究所的同學澤仁、鈞澤、振民、世泓、鎮屏、國芬、偉庭、雅真、俊宏，有你們的陪伴，讓研究所生涯充滿了歡樂色彩，還有父母的支持及表哥貴倫熱心的指導，感謝你們總是能夠在我遇到困難的時刻適時打氣和提醒，讓我更清楚自己努力的核心和重點，才能讓這篇論文得以順利完成，更希望這篇論文能對空軍提供研究之參考價值。

宇凱 謹誌

2009年6月23日

空軍人員資訊安全素養之分析與評量

作者： 鄭宇凱

國立台東大學 資訊管理學系環境經濟資訊管理碩士班

摘要

隨著電腦運用的普及與網際網路的蓬勃發展，已帶給人類急速而巨大的擊，也改變了人類生活模式。然而隨著資訊便利而來的則是令人擔憂的資訊安全題，因此，我們必須做好資訊安全防護措施，唯有在確保資訊安全之前提下享受資訊便利，才是面對資訊世紀來臨的正確態度，進而迎接未來更大的挑戰與衝擊。近幾年來，政府機關、軍事單位、學校及企業的入侵事件時有耳聞，而在新聞事件的背後，資料竊取所帶來的損失往往無可估計，尤其是軍中的資料，大多牽涉到限閱或機敏性的問題，所損及的不只是資料遭竊或金錢的損失，更嚴重的是危及整個國家的安全。在危機四伏的網路世界裡，網路犯罪案件層出不窮且逐年增加，顯現資訊安全防護工作的重要性。國軍肩負國防安全的第一線，軍事安全益形重要，因此，建構有效的資訊安全防護網，不僅是企業的重要課題，對於國軍單位更是不容忽視、勢在必行。

本研究主要在探討目前空軍人員資訊安全素養的現況，及其資訊安全素養與資訊違規認知兩者間之關係，進而提供空軍資訊業管部門研擬或修定相關政策之建議。本研究正式問卷共寄發 500 份，回收問卷 457 份，無效問卷 18 份，有效問卷共 439 份，有效問卷回收率為 87.80%。問卷資料以 SPSS 軟體工具，利用因素分析、專家檢核法、單因子變異數分析、多元回歸分析等統計方法，進行資料分析，研究結論如下：

（1）背景因素與資訊安全素養分析結果：年齡、教育程度、工作單位等因素，在資訊安全素養上，均有顯著差異。

（2）背景因素與資訊 違規認知分析結果：年齡、初次學習電腦時間、工作單位等，在資訊違規認知上，均有顯著差異。

（3）資訊安全素養與資訊違規認知分析結果：資訊安全素養與資 訊違規認知層面的積差相關分析達高度顯著相關。

關鍵詞：資訊安全、網路犯罪、網路安全、資訊安全素養

ABSTRACT

Along with the computer utilization popularization and the Internet vigorous development, has taken to the humanity rapidly and huge striking, also changed the humanity mode of life.However is the anxious information security topic which comes along with the information convenience, therefore, we must complete the information safe protective measure, only has in guarantees premise of under the information security to enjoy the information to be convenient, faces the correct manner which the information century approaches, then welcome future bigger challenge and impact.In the past few years network technology has become popular and pervasive, what was originally a single operation platform spanned into now an inter-net environment. But while it brings convenience it also brings up the network security problem. Within the past few years, network break-ins among government organizations, military units, schools, and business organizations are often heard, behind such incidents are data being stolen, causing huge amount of damage. This is a problem especially serious to the military units, where data are classified and limited to reading, The damage is not just data stolen or money lost, but something lot more serious endanger national security. Within this perilous network world, cybercrime increases year by year, showing the importance of network security. Military force holds responsibility of national security facing war at the front line, military security is therefore showing more importance each and every day. Because of this, the construction of an information security net is no longer an issue business organizationonly, but something that the military unit must not neglect but engage.

This research focus on analyzing the present information security literacy of military personnel man, and the relation between information security literacy and law-breaking recognition, which would provide suggestions for information security policy makings. The research totally 500 questionnaires are distributed and 457 are gathered. Deducting 18 invalid questionnaires, valid questionnaires amount to 439. The recall rate of valid questionnaires is 87.80%.We analyzed the data by using SPSS software system, with Factor Analysis, Experts' reviews, one-way ANOVA and Pearson Product-Moment Correlation. The conclusions are as follows:

(1) Analytic result between background and Information security Literacy recognition : Age, education level and unit all have significant effects.
(2) Analytic result between background and Information Law breaking recognition : Age, the first time of learning computer and unit all have significant effects.
(3) Product-Moment Correlation of Information security Literacy and Information Law breaking recognition reaches significant correlation.

Keywords: Information security, network crime, network security, information security accomplishment

目　　次

表目次

圖目次

一、緒論

隨著電腦運用的普及與網際網路的蓬勃發展，已帶給人類急速而巨大的衝擊，也改變了人類生活模式。然而隨著資訊便利而來的則是令人擔憂的資訊安全問題，因此，我們必須做好資訊安全防護措施，唯有在確保資訊安全之前提下享受資訊便利，才是面對資訊世紀來臨的正確態度，進而迎接未來更大的挑戰與衝擊。

資訊科技的快速發展，「數位化」已成為影響組織管理的一大革命性變革，隨著網際網路（Internet）與行動通訊（Mobile Communication）的快速成長，網路資訊安全問題一再浮現，但大部份造成資訊安全事件的原因都不是專業技術的層面，而是在人性面上出現漏洞所導致，不可否認，蓄意違規人員的專業素養，及用功認真的程度是遠高過於我們一般的資訊管理人員。若從技術層面討論資訊違規及駭客行為的防制，是明顯不足，有鑑於此，現階段國軍正不斷地積極推動「資安監控機制」精進作法，採取軍、民網路實體隔離政策，對於資訊違規部份，更是從嚴懲處，期能有效遏阻資訊違規事件發生，避免因人為疏失，造成單位損害或危及國家整體安全。但無論是預防或稽查資訊違規，除需有一套能在組織中推展的資訊安全管理機制外，更需藉由提昇組織內人員的資訊安全知識及警覺，來形成資訊安全的防護網，使得有心人士不再那麼容易的得逞，同時更提高了資訊違規的難度與成本，適時達到某種程度的資訊安全防護，以收具體成效。

1.1 研究背景與動機

根據台灣網路資訊中心最新的調查結果顯示（截至2009年1月初止），台灣地區上網人口已突破1580萬，共計有15,818,907人曾上網(整體人口0-100歲)，（如圖1.1）；12歲以上之上網人口有14,188,292人，上網比例為70.95%，比去年(97)增加了2.44%（如圖1.2），其中寬頻網路使用人數約為13,292,787，寬頻使用普及率為66.47%，與去年(97)63.37%呈現上升趨勢。（如圖1.3），而台灣地區可上網之戶數比例呈現穩定之趨勢，截至98年1月為止，共計有564萬戶可上網。（如圖1.4），台灣地區之家庭寬頻使用戶數比例呈現平緩穩定之趨勢，截至98年1月為止，共計有497萬

戶可上網。（如圖1.5）

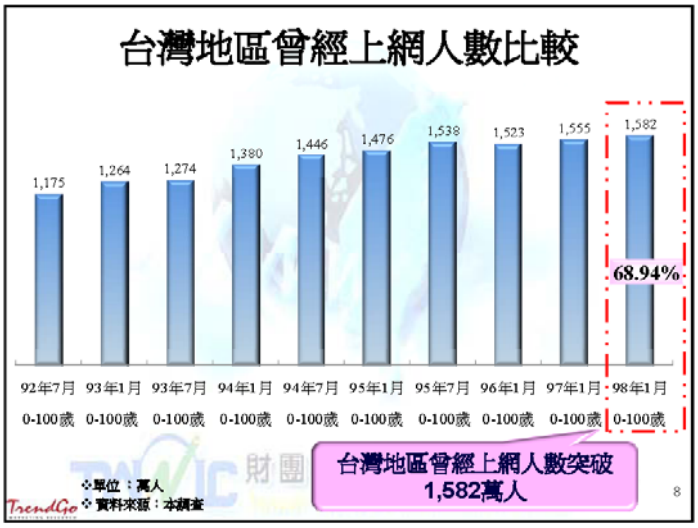

圖1.1 台灣地區曾經上網人數比較(單位：萬人)

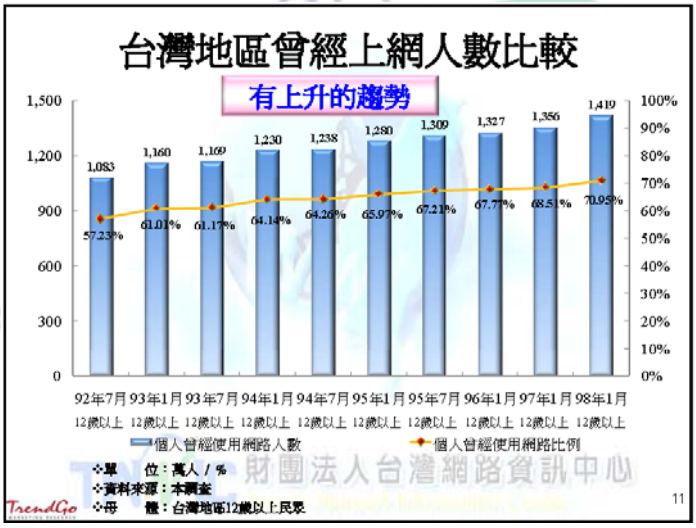

圖 1.2 台灣地區曾經上網人數比例(單位：萬人/%)

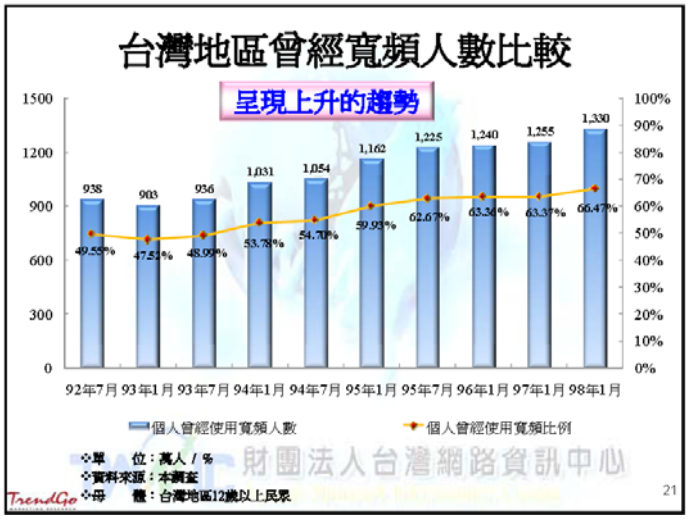

圖 1.3 台灣地區寬頻使用人數比較(單位：萬人/%)

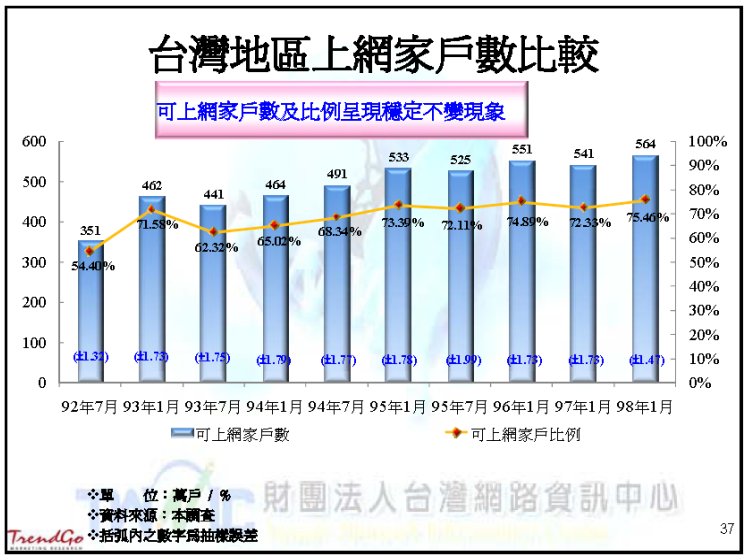

圖 1.4 台灣地區家庭上網戶數比較(單位：萬戶/%)

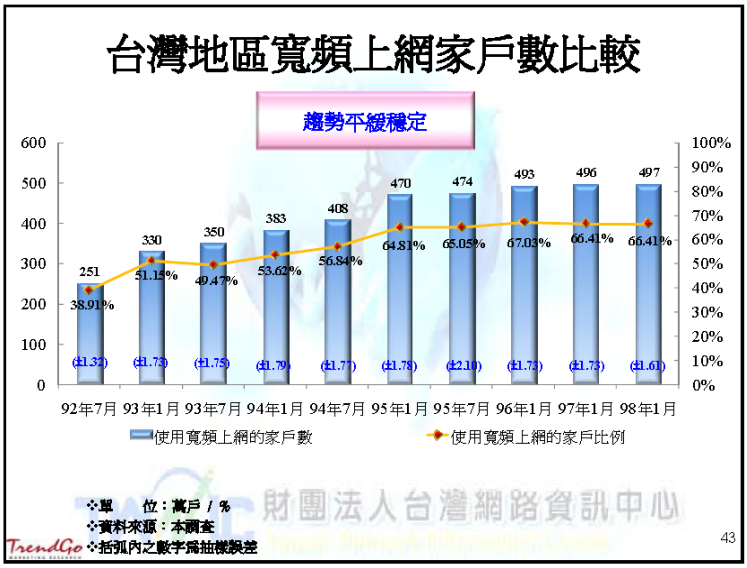

圖 1.5 台灣地區家庭寬頻使用戶數比較

台灣網路資訊中心，2009，“九十八年度台灣寬頻網路使用狀況調查摘要分析”，http://stat.twnic.net.tw。

根據上述調查報告顯示，我國國人網路基礎設備擁有度持續提升，上網與寬頻連網的戶數與人數穩定成長，不同年齡層的使用率亦逐漸提高，肯定台灣網路發展成效與國人資訊操作能力的普遍提升。值得注意的是，大多數民眾使用網路的習慣與服務內容雖無明顯改變，但是深化程度已反應網路對日常生活的影響加劇，顯示台灣地區上網及寬頻之人數/家戶數/寬頻使用戶數皆呈現穩定成長的趨勢。

另外，每半年統計一次光纖上網普及率超過1%的國家。於日前公佈2008年全球光纖上網普及率超過1%的國家數，可發現從2008前半年統計的14個國家已增加 到2008年底的20個。在全球光纖上網普及率排名方面，南韓普及率達44%，位居第1名，香港、日本分別以28%、27%緊追在後，台灣則以12%穩居第4名，此外本次的調查也首度

區分各國在FTTH及FTTB+LAN的普及率，進一步與2008年7月公佈的數據做比較如表1.1，台灣由7.7%上升至12%，短短半年便成長了4.3個百分點，僅次於韓國。此外，在光纖上網用戶數量排名上，日本共有1,320萬光纖上網的用戶，是全球最多光纖到府用戶的國家；美國市場則由於Verizon電信及地區性公司大力推廣光纖網路，用戶數也急遽成長，約605萬戶；其次則為中國大陸的596萬戶。顯見寬頻為全球家庭資訊取得的必備工具，網際網路其超越時間、空間限制的特性與優點，已成為21世紀不可或缺的傳輸媒體。

表1.1 全球光纖上網普及率前4名

表　全球光纖上網普及率前 4 名

	2008 年 7 月	2008 年 12 月
南韓	37%	44%
香港	27%	28%
日本	24%	27%
台灣	7.7%	12%

資料來源：FTTH Council（2008/7，2009/2）

資料整理：FIND（2009/2）

資料來源：III-IDEAS-FIND，2009，資策會創新應用服務研究所（IDEAS），
http://www.find.org.tw/find/home.aspx?page=news&id=5411

近年來隨著資訊網路科技的發達與盛行，多樣化的有線、無線通訊設備，帶給人們更便捷的生活，造就了 C2C(Consumer to Consumer electronic commerce)、B2C(Business to Consumer Electronic commerce)等電子商務的蓬勃發展，交易方式不再侷限於傳統的交易方法，使得網路漸漸成為人類生活中所不可或缺的傳輸工具，已經讓人們強烈感受到這股資訊流所帶來的便利與衝擊，然而電子交易的便捷同時提供犯罪者另一犯罪的途徑，相對延伸許多負面的問題，如最常見的網路駭客、網路誹謗、網路援交、網路詐欺、侵犯智慧財產權等，在在都說明了，網路的不當使用將會對社會造成相當程度的不良影響。

根據內政部警政署 97 年 1-10 月電腦網路犯罪發生數 22,111 件，較上年同期減少 2,981 件(-11.88%)，破獲數 17,565 件，較上年同期減少 165 件(-0.93%)，破獲率

79.44%，較上年同期增加 8.78 個百分點，呈現發生數減少、破獲率增加的情形，主要係警察機關加強偵查網路犯罪所致。如表 1.2。

表 1.2 97 年 1-10 月電腦網路犯罪概況

	發生數				破獲數			
	本期（件）	上期（件）	增減數（件）	增減率（%）	本期（件）	上期（件）	增減數（件）	增減率（%）
總計	22,111	25,092	-2,981	-11.88	17,565	17,730	-165	-0.93
詐欺	9,437	8,458	979	11.57	8,034	6,837	1,197	17.51
妨害電腦使用	3,519	5,878	-2,359	-40.13	722	607	115	18.95
一般妨害風化	2,864	1,036	1,828	176.45	2,864	1,033	1,831	177.25
違反兒童及少年性交易防制條例	2,646	5,353	-2,707	-50.57	2,646	5,353	-2,707	-50.57
智慧財產權	2,415	2,795	-380	-13.60	2,403	2,787	-384	-13.78
妨害名譽（信用）	566	531	35	6.59	329	276	53	19.20

資料來源：內政部警政署統計通報。

1.2 研究目的

國防二法自九十一年三月一日施行，我國國防體制正式邁入軍政、軍令一元化時代，在此同時，中共近年來挹注大量國防預算，處心積慮地對我國進行情蒐、電偵，不斷研發網路作戰能力，已對我國軍網路安全造成嚴重威脅，國軍為國防安全的第一線，倘若，國軍人員缺乏資訊安全素養，或資訊存取未配套縝密防護機制，而遭攻擊者竊取、竄改機密資訊，不論企業或國軍部隊，都將對組織造成無法彌補的傷害，網路的資訊安全勢將成為國軍邁向 E 化的重要關鍵。

近年來，在國軍人員共同努力下，相關資訊保密機制不斷地精進，使得國軍的資訊安全工作，已奠定一定的基礎，為建立國軍人員個人資訊安全防護觀念，強化國軍整體資訊安全，透過相關文獻探討與實證分析，期能達到下列之研究目的：

1. 瞭解空軍人員資訊安全素養的現況：

   藉由問卷調查瞭解空軍人員之資訊安全素養及其程度。

2. 探討空軍人員其不同背景變項在資訊安全素養及資訊違規認知之差異性：

   研究不同背景（年齡、階級、教育程度、初次學習電腦時間、電腦使用時間、工作單位）之空軍人員，其資訊安全素養與資訊違規認知是否存有差異。

3. 探討空軍人員資訊安全素養與資訊違規認知兩者間之關係：

透過研究調查結果，探討國軍人員資訊安全素養與資訊違規認知之關係，藉以瞭解如何加強查察，以避免類似案件再度發生。

4. 針對分析與研究結果提出建議，提供空軍人員、稽查單位擬定或修訂相關對策及後續研究之參考。

1.3 研究範圍與限制

1. 研究範圍

本研究係以南部地區某軍事單位之空軍人員為研究對象，涵蓋的範圍包括教學、訓練及後勤部隊等單位。

2. 研究限制

（1）對象受限：

因部份基層部隊官兵，平時專職戰備訓練任務，運用電腦作業時間並不多，為考量研究結果之適切性，因此排除上述人員。

（2）任務受限：

空軍人員任務區分幕僚、教學、訓練及部隊等單位，任務性質不同，上班時間相對亦有所不同，本研究受測對象以擔任教學與後勤支援任務之人員為主，因此，部份受試者在時空上將有所受限。

（3）研究方法受限：

本研究以問卷調查方式蒐整受試者資料，本研究僅能假設受試者均能發自內心，不受主觀因素、情緒、壓力或其它外力因素影響，而能據實以答。

（4）問卷內容受限：

本研究編製之問卷內容，雖參考相關文獻、國軍法令政策整理修定而來，但由於資訊安全素養與資訊違規認知領域範圍廣泛，且國軍相關作業規定有可能因考量其適用性或上級要求，而隨時修正調整，僅能以現行之法令政策作為參考依據，所以問卷內容可能無法一一涵蓋，恐有疏漏之處。

1.4 研究流程

本研究問卷以南部地區空軍某軍事單位之空軍人員為發放對象，再輔以SPSS軟體工具，進行資料分析。本研究流程如圖1.6所示，並依下列程序進行研究：

1. 確認研究方向：

依研究者工作背景有關的問題，及思考學術界、軍事單位所面臨或遭遇的問題，經

探討後研擬研究方向，並構思其可行性，以便進行實證研究。

2. 文獻探討與資料蒐集：

參考相關文獻與蒐集之資料，瞭解其它相關研究是否也遭遇類似之問題，或達成其相關之目標，以做為本研究之參考依據。

3. 擬定研究架構與方法：

參考相關文獻後，確立研究題項敘述與假設，以建立本研究之架構與方法。

4. 問卷設計：

參考相關文獻與法規政策，選定適當量表，以自編之「空軍人員資訊安全素養與資訊違規關係之研究」問卷，實施抽樣調查，問卷內容分為資訊安全素養與資訊違規認知兩大部份。

5. 實施問卷前測與修改：針對某軍事院校30名現職人員（含軍、士官、聘雇及文職人員）實施預試。為求量表之精確，本研究除依據預試問卷進行信度與效度之檢驗外，另以專家檢核方式，親自邀請兩位指導教授、一位專業教授與10位資訊專業軍官，針對預試問卷內容各題項逐一檢視後，作缺失修改與校正，並進行訪談工作。

6. 抽樣問卷調查：

本研究採樣時間為97年09月18日至98年03月23日，以某軍事院校空軍人員為研究對象，隨機抽取該單位之現職人員，以親自及委託發放方式實施抽樣問卷調查。

7. 資料整理與分析：

待全部問卷回收後，以SPSS for Windows 12.0 統計軟體，以卡方檢定、T檢定、單因子變異數分析等統計方法，進行資料分析。

8. 彙整研究結果：

根據統計分析結果進行檢定與假設驗證，最後依研究所得做出結論與建議，提供學術界或軍事單位擬定政策之參考。

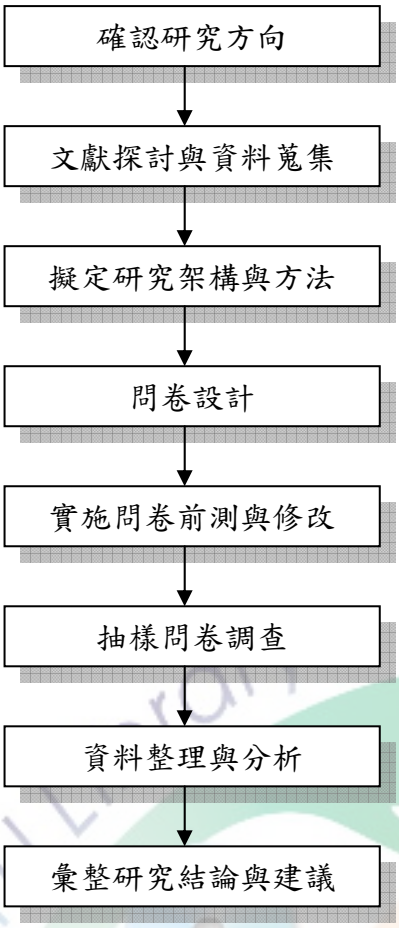
確認研究方向
文獻探討與資料蒐集
擬定研究架構與方法
問卷設計
實施問卷前測與修改
抽樣問卷調查
資料整理與分析
彙整研究結論與建議

圖 1.6　研究流程圖

二、文獻探討與理論基礎

從文獻中回顧發現，有關探討國軍人員資訊安全素養與資訊違規相關學術研究尚不多見，對於國軍人員資訊安全素養之研究仍處於起步階段，目前全國相關之研究有360篇：資訊安全素養2篇、資訊素養242篇、網路素養61篇、電腦素養55篇(全國碩博士論文網97年11月10日統計數據)，因此，關於這方面的議題實值得再進一步深入探討。本研究根據研究動機與目的，針對資訊安全、網路犯罪、資訊違規事件等作一完整性之介紹，並多方蒐集整理相關理論及研究，予以分析、歸納並找出適當的量表作驗證，以徹底了解資訊安全素養與資訊違規兩者間關係及其相互之影響。

2.1 資訊安全理論基礎

2.1.1 資訊安全的定義

由於政府對虛擬社會的大力推動以及商業界對電子商務交易需求的急迫性下，資訊安全的管理形成一個重要課題。隨著政府積極推動「e化台灣」、「e化政府」等計劃，許多政府單位的資訊都是透過資訊網路來發佈、交換或儲存，這些資訊一部分是公開資訊，提供使用者更便捷的服務，使政府行政更具效率，但是也有一部分可能包含著機密資訊、個人隱私資料、甚至是國防軍事機密佈署等。由於資訊網路本身的弱點，使得一些機密的、敏感性的資訊可能洩漏或資訊網路系統遭受入侵破壞，有鑑於此，行政院於九十年元月通過「建立我國通資訊基礎建設安全機制計畫」，成立「國家資通安全會報」並設立「國家資通安全應變中心」、「國家資通安全資訊中心」與「國家資通安全技術服務中心」來推動相關的電腦網路犯罪、危機的防範與防護相關工作。

BS 7799為英國標準協會 (The British Standards Institution, BSI) 所推動的資訊安全管理標準。它不僅已成為國際資訊安全管理的準則及規範（ISO 17799 及ISO 27001），更是各國政府單位和企業團體在資訊安全能力上的最佳證明，根據資訊安全管理系統國際標準ISO17799對資訊下的定義為：資訊（Information）意指以各種型態儲存的資料與知識，包括電子方式、文件方式---等，如同企業其他重要資產一樣，需要被妥善地保護。對「資訊安全」之界定上，Smith(1989)主張，任何電腦安全政策之廣義目標，必需能保護存於系統中資料之完整性（integrity）、可用性(availability)、與隱密性

(confidentiality)。其為資訊安全的基本要素（本質），示意如圖2.1。

圖2.1 資訊安全之界定示意圖

資料來源：Smith, M., 1989, “Computer Security-Threats,Vulnerabilities and Countermeasures”, formation Age,UK, pp.205-210.及本研究整理

資訊安全的基本要素（本質）：

(1)可用性－Availability

確保各項資訊資產能提供即時且正確的服務，以滿足使用者之需求。

(2)完整性－Integrity

將資訊資產依重要性分類，並提供適當的保護以確保資訊資產的完整性。

(3)機密性－ Confidentiality

適當的劃分資料的機密等級，並依其機密等級予以適當的規範及保護。

李志文（2003）指出，資訊安全可以說是目前最受矚目的資訊議題，由於網際網路的興盛，不論是政府、企業或個人，均與網路有密不可分的關係，也因此資訊安全的建置完善與否，其所帶來的影響將與日俱增。Simson and Gene(1991)認為，電腦系統能被使用者所倚賴，且其軟體運作表現如使用者所預期，則該系統便可稱之「安全」。江高飛（2000）等人指出，資訊安全包含了通訊安全與電腦安全，通訊安全是確保電腦的訊息（文件、資料、檔案），在傳輸時不於中途遭到竊取或被盜拷，其範圍不能僅限於網際網路的傳輸，還應包含一般方式的傳輸，電腦安全指的則是確保電腦能夠正常運作，資訊的儲存能無顧慮，不論是系統的操作、資料庫的儲存、病毒的防範等，其所謂的安全即是指確保事物的安全，事物指的是一個檔案、一封電郵、一個應用程式、一套系統等，至於安全性應包括下列五大項要素，分別為機密性、資料完整性、不可否認性、授權性、真實性等。

「資訊安全」的組成，其中包括「威脅」、「系統」及「對策」等三個軸向，「威脅」是針對「系統」所產生，而「對策」則用以保護「系統」免受「威脅」的傷害，示意如圖 2.2 所示。

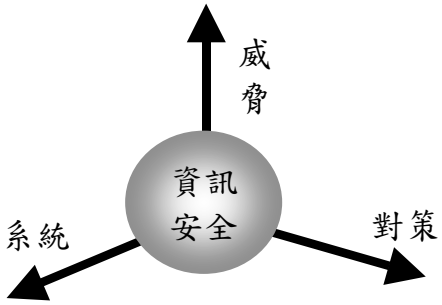

圖2.2 由威脅、系統、及對策所組成的「資訊安全」三軸模型

資料來源：張盛益、許美玲等譯，1995，“電腦安全的威脅與對策”，資訊工業策進會，簡介頁。

Karen（1992）等將資訊安全威脅造成的結果分為四類：1. 資訊遭阻斷（Interruption）、2. 資訊遭竄改（Modification）、3. 資訊遭攔截（Interception）、4. 資訊遭假冒（Fabrication）等。許瑩琪（2004）指出，資安威脅來源與類型包括有：情資蒐集、系統入侵、惡意程式、拒絕服務攻擊及偽冒欺騙等，茲分述如表 2.1。

表 2.1 資安威脅來源與分類一覽表

資安威脅來源與類型	
威脅來源	類型
情資蒐集	網路公開服務(如網頁、DNS Query、搜尋引擎等)
	網路掃描
	封包窺探
系統入侵	密碼設定不當(未設密碼、預設密碼或與帳號相同)
	不當的存取權限
	作業系統安全漏洞
	通信協定安全漏洞
拒絕服務攻擊	作業系統漏洞
	分散式阻絕服務攻擊
偽冒欺騙	向系統管理人員或使用者騙取密碼
	透過總機轉接至撥接門號

資料來源：許瑩琪，2004，“加強資訊安全之具體作為”，陸軍總部 93 年度通資安全巡迴講習，陸軍司令部，頁 10，及本研究整理。

2.1.2 資訊安全管理的要素

Ben Malisow（2004）指出，保護資料的安全並不是一件簡單的事，它需要各層次的相關管理來配合。與其他管理科學一樣，安全管理三要素是 People（人）、Process（流程）與 Technology（科技），因為事是由人做出來的，人事安全是所有安全當中非常重要的一環，企業或組織所擬定出來的安全政策，需仰

賴具備安全緊急意識的「人」去遵循；而企業若能掌握 Process 順暢，即可掌握 80% 以上的安全。如我們所知道的，在網路上傳送、接收與儲存等作業都可能致使資訊的洩漏，包含軟硬體設備，或是公司的員工，都有可能是洩密的管道，惡意使用者會想盡辦法透過不法途徑，利用合法使用者不良習慣所產生之漏洞，試圖越權存取資訊系統內的資訊。因此，欲使資訊安全無慮，防護工作並非僅是單純地依賴軟硬體輔助得以完成，而是需要多方面教育與習慣養成。

資訊安全涵蓋範圍相當廣，並非僅指網際網路，也絕非只是防火牆，因為資訊安全必須以人事、實體與環境安全為基礎，所有的科技都以協助安全管理政策為目的，否則科技只是一個產品。例如，當電腦為了資訊安全的緣故裝上防火牆，卻對其擺放位置不做適當防護，如何稱得上安全？有效推動資訊安全管理制度(ISMS)，包括 PDCA 過程模式，描述如下：

1. 計畫 Plan(訂立 ISMS 環境)：

   建立安全政策、目標、標的、過程及相關程序以管理風險與改進資訊安全，使結果與組織整體政策與目標一致。

2.執行 Do(實施與操作 ISMS)：

   安全政策、控制措施、過程與流程之實施與操作。

3. 考核 Check (監控與審查 ISMS)：

   依據政策、目標與實際經驗，以評鑑及測量(適當時)過程績效，並將結果回報給管理階層加以審查。

4. 檢討改進 Act (維持與改進 ISMS)：

   依據管理階層審查結果，採取矯正與預防措施，以達成持續改進資訊安全管理系統。相關示意圖如圖 2.3。

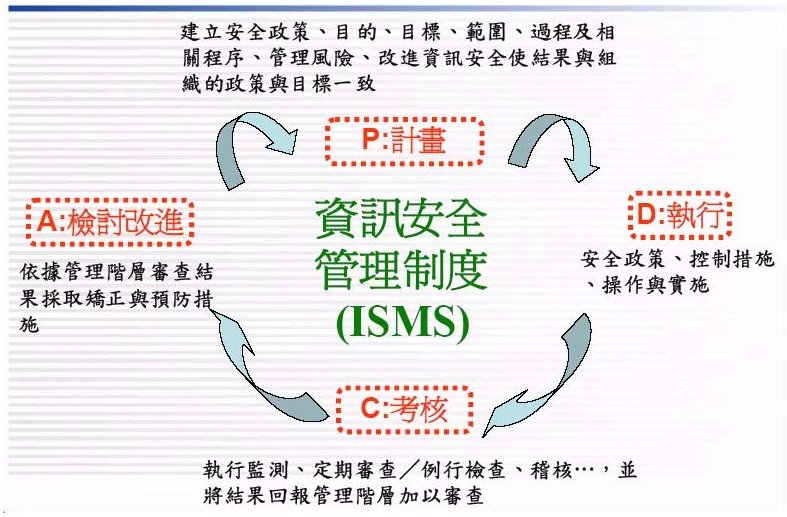

圖 2.3 PDCA 過程模式
資料來源：國家資通安全會報技術服務中心（ICST），2005，“由資安案例談資安防護”，9 月。

翁錳揮（2006）指出，因應資訊科技快速發展，通資系統將由資訊網路取代傳統通信，在「保密」與「時效」熟重下，各級應以「安全」為首要考量。我們必須要明白，「安全」是一段旅程，並非終點，資訊安全的目標在於保護資訊及其支援處理設備、系統和網路的機密性、完整性和可用性，不受到各種方式的威脅，使可能發生的事業損害降至最低，確保企業的永續經營，例如，程式設計師寫完程式必須向上級公開原始碼、企業 Data Center 必須進行資料異地備援...等等都是基於保護資訊安全的考量。

2.1.3 資訊安全之重要性

在軍事方面，中共雖然在傳統武力能量遠落於美國之後，但中共近年來已改變軍事戰略，以資訊攻擊效力取代武力的集結，尋求在戰略和戰鬥上獲得網路優勢，實值得我們加以戒慎警惕。以往在個人單機作業時代，使用者只要不隨意拷貝來路不明的檔案，即可確保電腦作業環境的安全，然而在網路及通訊環境蓬勃發展的時代，不管是瀏覽網頁、收發電子郵件、即時通訊或是資源分享等，只要沒有做好安全防護措施，電腦就可能遭到病毒、惡意程式、木馬後門程式…等的攻擊，危及到用戶電腦與資料的安全。在民間企業方面，根據美國電腦安全學院（Computer Security Institute

）與美國聯邦調查局（FBI）舊金山辦公室最新公佈的調查顯示，85%受訪企業的線上安全系統去年（2005）曾遭受滲透，35%的公司因類似入侵事件蒙受巨大損失，總金額高達三億七千七百萬美元。

2.2 資訊安全素養之相關研究

2.2.1 資訊素養之定義

一般而言，人類的「理解以及和外界做有意義溝通」所「需要的能力」，隨著時代的變遷而有所不同。外界的大環境若是文字世界，人要和文字世界溝通，最基本的便是要識字，在早期西方工業國家，一般民眾受教育的機會不多，若指有「素養」之人，即指具有識字能力之人，故早期的素養教育即教導民眾具有識字能力。Luke（1992）將素養定義為一套會隨著社會的文明科技而改變的策略與技術。李堅萍（1994）指出，一組人人都需要的基本能力（skills,abilities 或 competencies），因此，素養必須是某層次的能力、技能或技術的總和，而這組能力應具有基本的、人人必備的特性。「資訊素養」（information literacy）由「資訊」和「素養」組合而成。「素養」（literacy）為一般性的名詞，其內涵隨時代而有不同。「素養」（literacy）一詞原來指的是語文說、讀、寫的能力，「素養」亦可解釋為：「理解以及和外界做有意義溝通所需要的能力」。「資訊素養」便是指「在資訊時代個人所具備的一套技能，以學習以及和外界環境做溝通的基本技能」。Caissy(1992)指出素養是遠超過傳統的讀與寫的能力，素養包含著在不斷變遷的資訊社會環境中仍能存活的能力。

Doyle(1992)對資訊素養定義為：個人具有從龐大資源中蒐集、評估與利用資訊的能力。並認為凡是具有下列能力者為具資訊素養者：（1）能認識資訊的需求、（2）能認識正確性與完整性的資訊是做明智決定的基礎、（3）基於資訊需求來陳述問題、（4）確認資訊的潛在來源、（5）發展成功的搜尋策略、（6）利用電腦與其他科技獲取資訊資源、（7）評估資訊、（8）組織資訊予以利用、（9）整合新資訊在已有的知識架構與（10）以批判性思考與解決問題的觀點來利用資訊。素養也是用來描述人和外界溝通所需要的技能，Shelly(1996)認為資訊素養可分成內在與外顯能力，於內能思

考釐清問題所在、能分析所需的資訊，能正確解讀資訊、能分析、整合與組織有用的資訊。於外的能力包括知道資訊的來源所在，知道如何獲取資訊，能用合適的方式將組織與內化後的資訊呈現出來。其區別整理如表 2.2 所示。

表 2.2 資訊素養「內在」與「外顯」能力之區分

資　訊　素　養	
內　在	外　顯
＊能思考 ＊能釐清問題所在 ＊能分析所需要的資訊是什麼 ＊能正確解讀資訊 ＊能分析、合成、組織有用的資訊	＊知道資訊資源的所在 ＊知道如何獲取資訊 ＊能夠用合適的方式將組織及內化後的資訊呈現出來 ＊能利用資訊解決相關的問題

美國圖書館學會(American Library Association，簡稱 ALA)在 1989 年所提出的一份重要的歷史文件：「美國圖書館學會資訊素養委員會總結報告書」(The final report of the American Library Association Presi-dential Committee on Information Literacy)其對「資訊素養」的定義為：一個人具有能力知道何時需要資訊、且能有效的尋得、評估與使用所需要的資訊。最後成為一個學會如何學習的人，也就是為終身學習(lifelong learner)做好準備。換句話說，在日常生活中可察覺自己的資訊需求，並且有能力去處理，而這樣的能力必須經過學習才有。未來學大師 Alvin Toffler 曾說過：「所謂沒有資訊素養的人，在二十一世紀已不再是指那些不識字及不會寫的人們，而是指那些不能學習、不懂得學習、及不會持續學習的人們。」

Behrens(1994)認為，「資訊素養」是表示使用資訊、或者是擁有資訊知識的能力。McClure(1994)則認為資訊素養是由下列四種素養結合而成：（1）傳統識字素養(Traditional Literacy)、（2）媒體素養(Media Literacy)、（3）電腦素養(Computer Literacy)、與（4）網路素養(Network Literacy)。其關係如圖 2.4 所示。

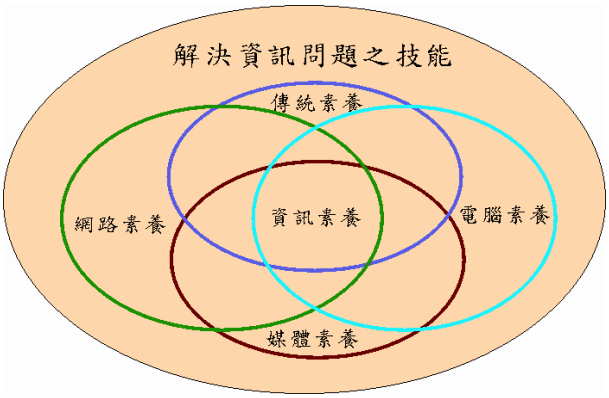

圖 2.4 資訊素養基本要素示意圖

資料來源：McClure, C. R., 1994, " Network literacy: A role of libraries? ", Information Technology and Libraries, 13(2), pp.117-118.及本研究整理

其中，他對電腦素養（ComputerLiteracy）所下定義為，使用電腦化完成一些基本工作的能力。而網路素養（NetworkLiteracy）指的是了解網路資源的價值，並能利用檢索工具在網路上尋取特定的資訊並加以處理、利用的能力。

國內對「資訊素養」一詞解釋，首見於李德竹（1994）在其主持國科會專案研究計畫「由資訊素養研究圖書館資訊服務之意義與內涵」中指出，培養國民具備瞭解資訊的價值、在需要資訊時能有效查詢、評估資訊、組織資訊與利用資訊。黃世雄(1996)認為，資訊素養是廿一世紀知識工作者必備的條件，其範圍涵括全球的資訊資源，資訊素養能力應界定在培養獲取資訊、解決問題、決策訂定以及評估資訊的能力。Luehrmann(1981)則指出，電腦素養是操作電腦的經驗與能力。吳正已與邱貴發（1996）認為，電腦素養應包括：（1）認識電腦、（2）應用電腦與（3）了解電腦與社會間的互動關係。網路素養依據陳雪華（1996）的定義包括：（1）網路之基本概念、（2）網際網路與台灣地區網路之源起、發展與現況、（3）網際網路之功能、（4）網路資源類型、（5）全球資訊網的介紹、（6）檢索資訊之比較與（7）檢索策略。

楊美華(1999)認為，「資訊素養」是指一個人知道何時需要資訊，並且具備找到資訊、評估資訊及有利用資訊能力的人，其目的是學習成為一位知道如何學習的人，而資訊技能的層次為：（一）對於資訊服務與資訊的認知；（二）了解資訊的結構；（三）具有分解資訊問題（需求）的能力；（四）懂得如何檢索資訊；（五）評估資訊；（六）管理資訊。郭麗玲(1999)認為，「資訊素養」是指蒐集、整理、評鑑及利用資訊的能力。

魏令芳（2002）指出，資訊素養是培養國民具備瞭解資訊的價值、在需要資訊時能有效查詢資訊、評估資訊、組織資訊和利用資訊。陳伯榆（2003）認為，全面提昇資訊安全的素養，將和提昇資訊素養一樣重要。綜合上述學者對資訊素養所作的定義整理如表2.3.1-2.3.2。

表 2.3.1 國內外學者對資訊素養所作的定義綜合整理表

國外研究者	定　義
Luke（1992）	將素養定義為一套會隨著社會的文明科技而改變的策略與技術。
Caissy(1992)	素養是遠超過傳統的讀與寫的能力，素養包含著在不斷變遷的資訊社會環境中仍能存活的能力。
Doyle(1992)	對資訊素養定義為個人具有從龐大資源中蒐集、評估與利用資訊的能力。
Behrens(1994)	認為「資訊素養」是表示使用資訊、或者是擁有資訊知識的能力。
McClure(1994)	認為資訊素養是由下列四種素養結合而成：（1）傳統識字素養(Traditional Literacy)、（2）媒體素養(Media Literacy)、（3）電腦素養(Computer Literacy)、與（4）網路素養(Network Literacy)。
Shelly(1996)	資訊素養可分成內在與外顯能力，於內能思考釐清問題所在、能分析所需的資訊，能正確解讀資訊、能分析、整合與組織有用的資訊。於外的能力包括知道資訊的來源所在，知道如何獲取資訊，能用合適的方式將組織與內化後的資訊呈現出來。
ALA	其對「資訊素養」的定義為：一個人具有能力知道何時需要資訊、且能有效的尋得、評估與使用所需要的資訊。
Alvin Toffler	所謂沒有資訊素養的人，在二十一世紀已不再是指那些不識字及不會寫的人們，而是指那些不能學習、不懂得學習、及不會持續學習的人們。
國內研究者	定　義
李德竹（1994）	培養國民具備瞭解資訊的價值、在需要資訊時能有效查詢、評估資訊、組織資訊與利用資訊。
李堅萍（1994）	素養為一組人人都需的基本能力（skills,abilities 或 competencies），因此，素養必須是某層次的能力、技能或技術的總和，而這組能力應具有基本的、人人必備的特性。

表 2.3.2 國內外學者對資訊素養所作的定義綜合整理表（續）

國內研究者	定　義
吳正已與邱貴發（1996）	認為電腦素養應包括：（1）認識電腦、（2）應用電腦與（3）了解電腦與社會間的互動關係。
陳雪華（1996）	網路素養的定義包括：（1）網路之基本概念、（2）網際網路與台灣地區網路之源起、發展與現況、（3）網際網路之功能、（4）網路資源類型、（5）全球資訊網的介紹、（6）檢索資訊之比較與（7）檢索策略。
郭麗玲（1999）	「資訊素養」是指蒐集、整理、評鑑及利用資訊的能力。
魏令芳（2002）	培養國民具備瞭解資訊的價值、在需要資訊時能有效查詢資訊、評估資訊、組織資訊和利用資訊。
陳伯榆（2003）	行為乃是個體表現於外，且能被直接觀察記錄或測量的動程。

資料來源：本研究彙整

2.2.2 資訊安全素養之定義

國內針對「資訊安全素養」一詞提出見解，首見於楊境恩（2004）在其碩士研究論文「國內警察人員資訊安全素養對資訊犯罪偵查能力影響之研究」中認為，「資訊安全素養」應指個人在具備操作資訊處理及傳播的工具與系統，包括電腦、媒體系統與網路的基本能力，為利用資訊與外界作資訊傳遞、共享、溝通與互動時所需的必備條件，且需體認資訊安全價值與力量，能判斷其正當性，並能瞭解資訊安全本質、管理的特性，熟悉尋求方法並具備評估解釋及綜合資訊安全的能力。其歸納「資訊安全素養」內涵應包括「資訊安全知識」、「資訊安全操作技能」、「資訊安全的應用、限制及影響」、「資訊安全倫理」等四個層面，其區別整理如表 2.4 所示。

表2.4 「資訊安全素養」層面之內涵

層　面	內容
資訊安全知識	包含資訊安全定義、名稱、功用和常用資訊安全術語等。
資訊安全操作技能	包含一些實際資訊安全操作的能力，如資料的存取與管理、密碼及權限使用等。
資訊安全的應用及影響	能利用資訊安全幫吾人解決電腦防護問題，並瞭解資訊安全的限制與對電腦安全的影響。
資訊安全倫理	使用電腦時，能遵守資訊安全法律與及倫理道德，不利用電腦做違背法律及社會道德規範的事情。

2.3 資訊違規與資訊犯罪研究理論基礎

2.3.1 資訊違規與資訊犯罪之定義

資訊違規乃指「違犯保密規定」，依據「國軍人員違犯保密規定行政懲處標準表」對其所作之定義為：違反國家機密保護法規，及「國軍保密實施規定」等有關保密之規定或命令，違成國防機密資訊有洩密顧慮，但未構成洩密者。其中，國軍人員在處理、保管國防機密資訊（即「國家機密」、「軍事機密」、「國防秘密」、「一般公務機密」），未善盡職責，致肇生洩密事件，洩密者依法偵辦，相關失職人員依照「國軍人員違犯保密規定行政懲處標準表」，依情節輕重檢討議處。

2.3.2 電腦犯罪、網路犯罪、資訊犯罪之定義

網路犯罪問題從歷史觀點而言係先從電腦犯罪(Computer Crime)漸演化而來，林山田(1984)認為，「電腦犯罪」乃指行為人濫用或破壞電腦而違犯具有電腦特質(Computer Property)的犯罪行為，所謂「電腦特質」則以行為的犯罪、追訴或審判是否需要電腦的專業知識為斷。林東茂（1996）指出，電腦犯罪係指「行為人濫用電腦或使用足以侵害電腦硬體或軟體的行為，而造成與電腦特質有關的犯罪」。凡利用電腦所具有的快速性、大量處理、隱匿性等電腦的特性而作為犯罪的工具就屬於電腦犯罪。在狹義上：網際網路犯罪是電腦犯罪的延伸，由人、電腦、資訊所構成，在廣義上：行為人所違犯故意或過失行為，需要透過電腦網路即稱為網路犯罪。Parker（1998）認為，電腦犯罪是一種罪犯會移用電腦科技知識所從事的犯罪。黃世銘、謝名冠（2001）指出，網路犯罪係由電腦犯罪逐漸演化而，二者關係密切，然而在意義上仍有所區別，因此，在探討資訊犯罪前需先探討電腦犯罪、網路犯罪二者之定義，再延伸至資訊犯罪。

「網路犯罪」係屬電腦犯罪之延伸，為電腦系統與通訊網路相結合之犯罪，但相較於電腦犯罪而言，更偏重於「網際網路」的應用，而係指具有網際網路特性的犯罪，亦即行為人所違犯之故意或過失的犯罪行為具有網際網路特性者，就實際應用而言，亦即犯罪者在犯罪過程中，需借助網際網路方能遂行其犯罪意圖之犯罪，國內網路犯罪之歷史追溯到1995年4月，港商愛普生公司電腦系統遭入侵案開始迄今，不但網路犯罪事件不斷的增加，不同型式的網路犯罪案件亦隨社會網際網路發展不斷增加，網路犯罪是一種新興電的犯罪型態，屬智慧型犯罪，依網際網路在犯罪中所扮演的角色

，警政署將網路犯罪分為以下三類：一、以網路空間作為犯罪場所；二、以(網際)網路為犯罪工具；三、以(網際)網路為犯罪客體。茲將網路犯罪分類分述如表2.5。

表2.5 網路犯罪之分類及其常見類型

分類標準	特點	常見型態	知悉程度	偵查難度
以網路空間為犯罪場所(被動)	被動性質，引誘吸引一般人進入	1. 網路色情 2. 網路援交 3. 販賣盜拷 4. 網路賭博 5. 網路遊戲 6. 販賣槍械 7. 教授製仿炸彈	高	低
以網路為犯罪工具(特定目標)	針對特定目標予以侵害性質，藉由網路作為犯罪工具	1. 網路恐嚇 2. 網路誹謗 3. 網路詐財	中	中
以網路為犯罪客體(為攻擊目標)	對網路或電腦系統的攻擊性或破壞性	1. 網路入侵（駭客） 2. 散播電腦病毒 3. 網路竄改 4. SQL Injection	低	高

資料來源：警政署，2007，http://www.internet-recordor.com.tw/crime.html。

另外，警政署網站（2007）指出，電腦網路犯罪案件，具有下列特性：

A. 散布迅速：網際網路具有無遠弗屆、迅速廣泛散布的特性，其影響極大。

B. 身分易藏：網際網路的來源網址可以假造，如阻斷服務攻擊極難追查。

C. 證據有限：電腦犯罪可能沒有現場、兇刀、血跡、槍彈、血衣等實体的跡證。網路犯罪留下的僅有數位化電磁紀錄並非如指紋、語音、ＤＮＡ等有個別性，如何提升數位化電磁紀錄的證明力實為一大挑戰。

D. 毀證容易：網路犯罪非但證據有限，且證據十分容易毀滅。例如，電腦內部駭客程式、不法取得之資料，祇要按下刪除鍵或執行格式化指令，即能瞬間銷毀證據。

E. 適法困難：民國八十六年十月立法院針對電腦犯罪通過修正刑法條文共計八條。然而電腦科技進步日新月異，現在修法解決的，只是過去面臨的問題；網路科技帶來的新問題，往往令立法及執法機構追趕不及。

F. 跨國管轄：網路世界不易分辨你我及疆界，在網路上漫遊世界輕而易舉，這也造成網路犯罪具有跨國管轄的特性。

G. 偵查不易：以上幾個特性致使網路犯罪不易偵查，甚至無法偵辦。各國法律與實務對於某些行為是否違法的判斷標準不同（如槍、賭、色情的認定），也使得跨國性網站的非法行為，造成在偵查上困難度。

馮震宇、劉志豪（1998）指出，就網路犯罪之犯罪型態分類可分為：一、網路服務提供型：如網路色情、利用網路發表不當言論、網路詐欺、利用網路煽惑他人犯罪、網路賭博等；二、入侵篡改、破壞資料類型:如利用網路無權侵入、利用網路入侵而篡改他人資料、利用網路散布病毒；三、其他侵害類型:如非法重製電腦程式或檔案、網址名稱與商標權之侵害等三類。內政部刑事警察局將犯罪類型概分為網路媒介及傳佈色情等八類，茲分述如表 2.6。

表 2.6 網路犯罪類型區分表

犯罪類型區分	
犯罪類型	內容
一、網路媒介及傳佈色情	一夜情交易中心、銷售色情光碟影片、聊天網站或其他方式進行援助交際、自拍、情色貼圖公然猥褻 散播情色資訊於網路聊天室間或公眾領域。
二、網路販賣違禁、管制物品、盜版光碟、贓物、侵犯他人著作權及商標權	例如：在網路上販賣 FM2、搖頭丸、毒品、其他禁藥、贓物、仿冒品、交易偽鈔賣槍、網路販賣盜版光碟：如俗稱泡麵或大補帖的盜版光碟、電影 VCD 或音樂 CD 等等。
三、教唆他人犯罪	例如：軍火教父、自殺手冊。
四、網路詐欺	例如：網路銷售商品，收錢沒送貨。
五、網路恐嚇	例如：網路千面人。
六、毀謗侮辱 妨害名譽(偽造文書)	例如：公佈電話、地址、公佈電子郵件帳號、散佈寫真、移植明星照片。
七、駭客侵入與散佈電腦病毒	例如：截取銀行帳號、密碼、截取其他個人隱私資料、金融犯罪、木馬程式窺伺資料、破壞或移植、駭客大戰散佈電腦病毒。
八、網路賭博	例如：在網路上架設網頁，並提供賭博網站之功能，連續公然煽惑不特定之人上網賭博財物犯罪。

林宜隆（2000）指出，資訊（網路）犯罪是電腦犯罪之延伸，為電腦系統與通訊網路相結合之犯罪，犯罪人在過程中必須籍助網際網路才能遂行其犯罪意圖之犯罪，其認為資訊犯罪相等於資訊網路犯罪、網路犯罪、網際網路犯罪及數位犯罪等。為考量公務機關的電腦系統被入侵，將造成國家機密外洩，有危及國家安全之虞，我國刑法於 2003 年 6 月修正時，特參考美國法律之規定，區別入侵政府之電腦系統與一般個人使用之電腦系統，對於入侵公務機關電腦或其相關設備的行為加重處罰。故刑法第 361 規定：「對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。」其次，就網路駭客進一步竊取資料的行為而言，除成立刑法第 359 條之無故取得電磁紀錄罪，依其資料內容是否涉及到國防機密，還可能成立刑法第 111 條或國家機密保護法第 34 條之刺探收集國防秘密罪。

2.3.3 國軍資訊違規相關法規

我國「國家機密保護法」於 2003 年 2 月 6 日公佈實施，該法中第 4 條將國家機密區分為「絕對機密」、「極機密」、「機密」三個等級，並在第 2 章中明確規範國家機密核定之權責、保密與解密之條件等。國防部為了配合國家機密保護法的制定與陸海空軍刑法第 78 條之規定，於同年 4 月 25 日修訂「軍事機密與國防秘密種類範圍等級劃分準則」，以處理軍事及國防機密。「通訊科技」與「網際網路」的精進與普及，除衝擊原有的國家限界外，也危及國家的整體安全。於此同時，國軍經歷多年的努力，已使軍隊邁入「資訊化」與「電子化」，有效提昇指揮管理與用兵作戰之效率；然而，資訊作業的便捷性，就像劍之雙刃，稍有不慎即可能為自己帶來莫大的傷害，而這也就是國防軍機維護，所必須面對的嚴峻挑戰。如何制止犯罪的發生，從人類有社會行為以來，一直都是值得討論議題。

另外，為解決國軍資訊保密安全之困境，國軍相關機構不斷地研謀精進措施，使國軍網路一旦遭受外來因素破壞或不當使用等緊急事故發生時，能迅速作必要之通報及緊急應變處置，並在最短時間回復正常運作，以降低該事故可能帶來之損害，促使國軍能真正成為「數位化」之國軍。本研究將參考國軍相關資訊安全管理標準，以作為問卷內容，國軍資訊安全相關管制規定與精進作法摘錄如下：

1.「個人電腦資訊安全防護作業規定」

為促使本軍人員瞭解資訊安全的重要性，以防止個人電腦遭入侵、竊取或破壞，有效維護個人資料及系統安全，以建立資訊安全一級防護概念，其內容包括：實體隔離政策、資料分級處理、個人電腦安全設定檢查等要項。

2.「國軍通資安全常見違規事件暨應行注意事項」

其內容包括：通信安全違規事件應注意事項如：密碼（語）本表暨通信密件管理、行動電話管制規定等計 14 要項；資訊安全違規事件應注意事項如：密級（含以上）資料儲存管制、資訊媒體稽核檢查、資訊系統與通資網路之設備存取管理、刑法修正條文等計 51 要項。

3.「電腦緊急應變處理實施計畫」

針對空軍資通系統、網路所發生之安全事件，提供早期預警、狀況處置程序，有效減低災損、快速復原，俾支援作戰。依「有效嚇阻、防衛固守」之作戰指導，及就各單位資訊系統、網路現況及可能之威脅與突發狀況，結合政策計畫、指揮管制、通報處理、研發諮詢及各單位 CERT 等分組，建立國軍電腦緊急應變處理機制，掌握遭受資訊攻擊或突發事件影響期間全般狀況及協調處理，以確保國軍通資安全，國軍電腦緊急應變（CERT）通報流程如圖 2.5 及國軍資通安全事件等級區分如表 2.7。

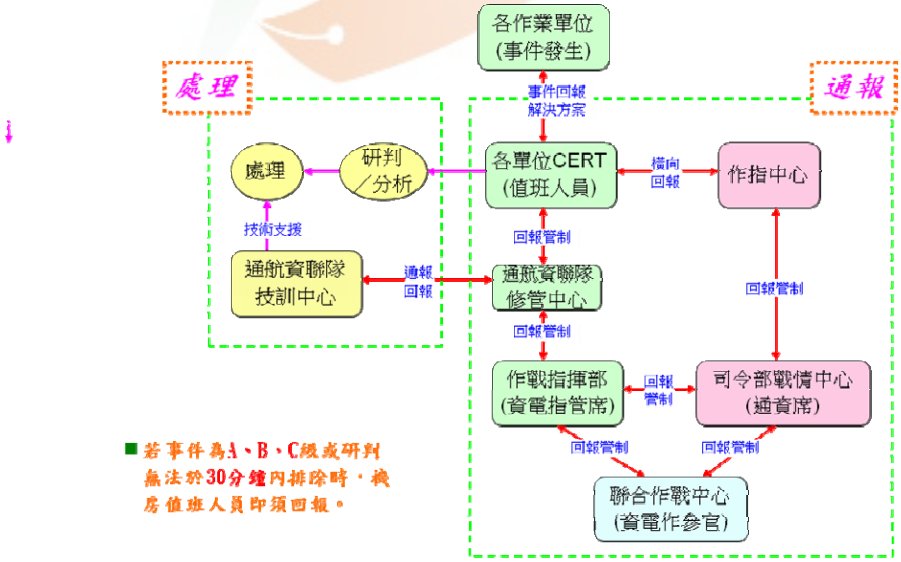

圖 2.5 國軍電腦緊急應變（CERT）通報及處理流程

資料來源：國防部通資次室，2007，“空軍資管作業執行現況”，空軍總部 96 年度通資安全巡迴講習，頁 45。

表 2.7 國軍資通安全事件等級

等級	狀況
A 級	影響國軍(公共) 安全、軍中(社會)秩序、國軍人員(人民)財產安全。
B 級	系統停頓，業務無法運作(影響情傳遞者) 。
C 級	業務中斷，影響系統效率。
D 級	業務短暫停頓，可立即修護。

資料來源：國防部通資次室，2007，“空軍資管作業執行現況”，
空軍總部 96 年度通資安全巡迴講習，頁 46。

4.「資訊網路安全監測作業實施規定」

有效落實「資安監控機制要求事項」為當前國軍重要政策，其置重點於陸軍連接國軍資訊主幹網路單位，實施系統偵測體檢、安全漏洞掃瞄及記錄分析檢討，採固定監測為主、機動監測為輔，不定期對連接國軍資訊網路單位，執行資訊安全「弱點掃瞄」作業，俾先期發掘問題及改進缺失，以杜絕資訊危安事件。其稽核項目包括：個人電腦權限管理、機密資料管理、防毒及漏洞修補、個人電腦保密設定、違反實體隔離、影響國軍安全、軍紀、軍譽等資訊作業行為。國軍資訊安全管控機制，示意如圖 2.6。

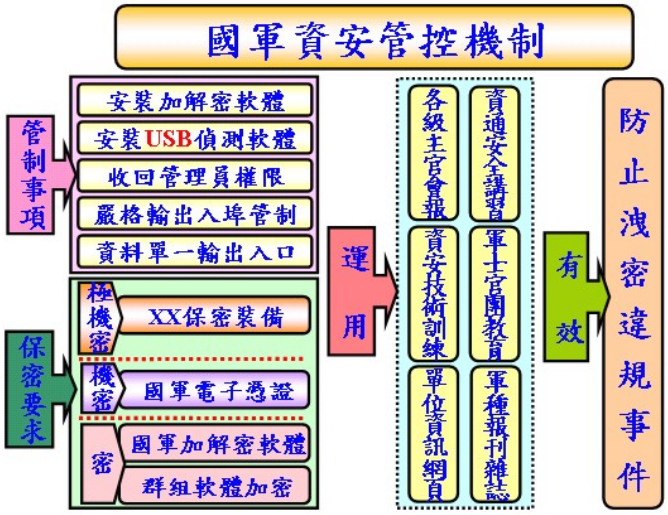

圖 2.6 國軍資訊安全管控機制

資料來源：許瑩琪，2004，“加強資訊安全之具體作為”，
陸軍總部 93 年度通資安全巡迴講習，陸軍司令部，頁 10，3 月 15 日。

5.「資訊設備及資訊儲存媒體管制規定」

藉嚴格限制單位公務用電腦「輸出（入）裝備」，俾防制機敏資訊洩密管道，以確保資料檔案管理安全。各類型公務用電腦（包括：桌上及筆記型）輸出（入）裝置均納入管制。其管制項目有：「軟碟機」、「燒錄器」、「USB」、「RS232」及「印表機」連接埠等電腦輸出（入）裝置，包括拆除「燒錄器」及「軟碟機」、移除「USB連接線」、安裝偵測軟體、資料交換(輸出/輸入）等管制規定。

6.「個人電腦輸出（入）裝置使用管制規定」

本規定之目的為落實單位及個人「資訊設備」、「資訊儲存媒體」管制，以防止設施器材遺損，內存公務資料、檔案、文件、圖像及機敏系統等洩（違）密，確保資訊安全，其管制項目有：裝備採購、管制識別標籤、器材、無線設備管制、網路實體隔離及相關違規懲處規定等要項。

7.「通資業務手冊密碼選取規則」

其目的為律定密碼選取規則要點，以強化電腦之保密機制，包括個人帳號及電腦各式密碼（包含作業系統上之使用者及管理者、開機密碼、BIOS 密碼等）作業規定。

8.「漢光００號演習」通資安全監察維護實施規定

為確保演習機密維護及演訓任務之遂行，每年定期修頒演習期間保密安全應行注意事項，包括：落實個人保密、保密作業紀律、復原階段之裝備與資料保管等要項。

9.「網路實體隔離及資訊設備庫存管理觀摩實施計畫」

藉由觀摩示範，統一國軍「網路實體隔離」、「資訊設備」及「資訊設備媒體」等管制作法，俾要求各相關單位落實辦理，以防杜肇生洩密事件。

茲將近年來國軍新頒資訊安全相關法規綜整如表 2.8（以空軍為例）：

表 2.8 空軍資訊安全相關法規綜整表

空軍資訊安全相關法規綜合整理一覽表	
頒佈日期	法　　規　　名　　稱
960117	Kerberos 版 USB 監控作業注意事項
960118	資通安全突擊檢查實施計畫
960306	軍民網網站管理作業規定
960504	CERT 作業規定

960621	國防科技工業機構資通安全輔檢實施計畫
960803	電腦輸出入裝置暨移動式儲存媒體使用管制規定
961120	出國人員資訊安全訓練實施計畫
961127	資安監控系統架測暨監控作業實施計畫
961207	網站資安檢測實施計畫
970110	資訊安全責任等級分級作業實施計畫
970926	資安合格簽證實施計畫
971030	資安違規人員講習實施計畫
971224	網站資安檢測實施計畫

資料來源：本研究整理。

2.4當前資安事件問題探討

資訊科技發達，不但帶給人類急速而巨大的衝擊，也改變了人類生活模式，然而隨著資訊科技所帶來的便利，也引發不少令人擔憂的資通安全問題。各類網路不安全事件的困擾與威脅層出不窮，例如：病毒蠕蟲、阻斷服務式攻擊、駭客入侵、網路釣魚、垃圾郵件及間諜軟體等各式各樣的威脅，如下圖2.7-2.8。

圖2.7 國軍資訊安全政策與事件宣導

圖2.8 國軍資訊安全政策與事件宣導

資料來源：國防部通資次室，2007，通資安全巡迴講習“資安政策與宣導”。

依據空軍通信航管資訊聯隊統計，97-98年各航資中隊違規情況統計表。如表2.9。

表 2.9 空軍航資中隊資安違規事件統計表

空軍航資中隊各單位 97-98 年度資安違規事件統計表												
區分	一中隊	二中隊	三中隊	四中隊	五中隊	六中隊	七中隊	八中隊	十中隊	十二中隊	台北大隊	合計
隨身碟造成系統誤判	3	1	1	2	0	2	1	4	0	0	1	15
誤插 USB 儲存媒體	0	1	7	1	1	0	0	6	1	0	1	18
硬碟變更	0	1	1	2	0	0	3	0	0	0	1	8
硬體誤判	0	6	1	5	0	0	1	0	0	0	1	14
合計	3	9	10	10	1	2	5	10	1	0	4	55
附記	資料時間：統計自 97 年 1 月 1 日起至 98 年 2 月 30 日止。											

資料來源：空軍通信航管資訊聯隊及本研究整理

三、研究方法

本研究根據前述之研究動機及目的，透過相關文獻的探討，建立研究架構及研究假設，進行問卷內容之設計與調查，資料的蒐集整理採用文獻探討、問卷調查法、訪問調查法、統計分析與專家檢核等方法，並依據國軍電腦緊急應變處理(CERT)實施計畫、資安監控機制作法、空軍人員違犯保密規定懲處標準表、資安督考實施計畫及資訊安全相關法規，另參考其他適用之量表，用以設計「空軍人員資訊安全素養與資訊違規認知關係之研究」調查問卷。

3.1研究架構

根據上述文獻探討，本研究以空軍人員之背景因素為自變項、資訊安全素養為依變項，探討空軍人員資訊安全素養的現況及分析比較其背景因素對資訊安全素養之影響及資訊安全素養與資訊違規認知兩者間之相互關係。本研究架構如圖3.1 。

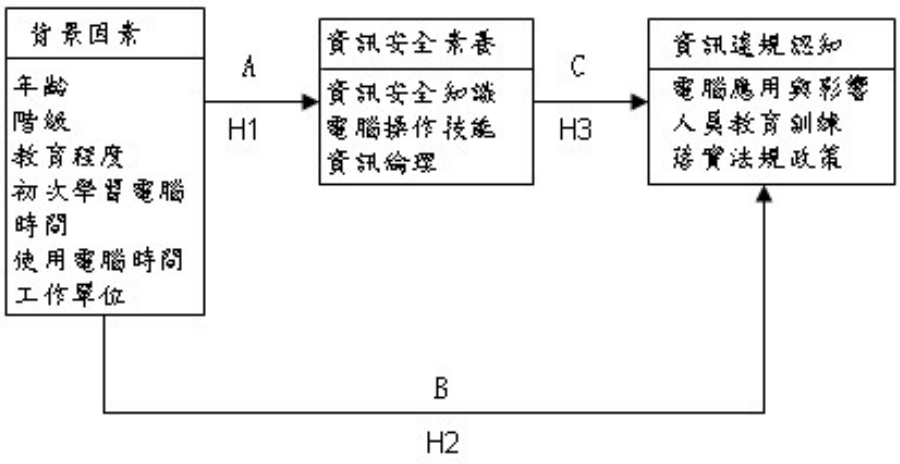

圖3.1 本研究架構圖

資料來源：本研究整理

路徑A：如圖3.1所示，旨在探討空軍人員背景因素與資訊安全素養的關係情形，以T檢定及單因子變異數分析（One-way ANOVA），來比較不同背景之空軍人員，其資訊安全素養的差異情形，找出哪些背景因素對資訊安全素養，有顯著影響。

路徑Ｂ：如圖3.1所示，旨在探討空軍人員背景因素與資訊違規認知的相關程度，以T檢定及單因子變異數分析，來比較不同背景之空軍人員，其資訊違規認知的差異情形，找出哪些背景因素對資訊違規認知，有顯著影響。

路徑Ｃ：如圖3.1所示，旨在探討空軍人員資訊安全素養與資訊違規認知彼此間的相關程度，以典型相關分析之統計方法，來比較其相互間密切之程度。

H1-H3：為假設1至假設3。

3.2研究假設

根據上述研究目的及研究架構，擬訂下列研究假設，進行相關假設檢定：

假設 1.：空軍人員背景之不同，在資訊安全素養上應無顯著之差異。

假設 1-1 空軍人員年齡之不同，在資訊安全素養上應無顯著之差異。

假設 1-2 空軍人員階級之不同，在資訊安全素養上應無顯著之差異。

假設 1-3 空軍人員教育程度之不同，在資訊安全素養上應無顯著之差異。

假設 1-4 空軍人員初次學習電腦時間之不同，在資訊安全素養上應無顯著之差異。

假設 1-5 空軍人員使用電腦時間之不同，在資訊安全素養上應無顯著之差異。

假設 1-6 空軍人員工作單位之不同，在資訊安全素養上應無顯著之差異。

假設 2.：空軍人員背景之不同，在資訊違規認知上應無顯著之差異。

假設 2-1 空軍人員年齡之不同，在資訊違規認知上應無顯著之差異。

假設 2-2 空軍人員階級之不同，在資訊違規認知上應無顯著之差異。

假設 2-3 空軍人員教育程度之不同，在資訊違規認知上應無顯著之差異。

假設 2-4 空軍人員初次學習電腦時間之不同，在資訊違規認知上應無顯著之差異。

假設 2-5 空軍人員使用電腦時間之不同，在資訊違規認知上應無顯著之差異。

假設 2-6 空軍人員工作單位之不同，在資訊違規認知件上應無顯著之差異。

假設 3.：空軍人員資訊安全素養之不同，在資訊違規認知上應無顯著之差異。

假設 3-1 空軍人員資訊安全知識之不同，在資訊違規認知上應無顯著之差異。

假設 3-2 空軍人員電腦操作技能之不同，在資訊違規認知上應無顯著之差異。

假設 3-3 空軍人員資訊倫理之不同，在資訊違規認知上應無顯著之差異。

3.3 研究變項定義與衡量

本研究為達研究目的，驗證研究假設，以自編之「空軍人員資訊安全素養與資訊違規認知關係之研究」調查問卷，作為問卷調查的研究工具，其內容共分為「個人背景」、「資訊安全素養」、「資訊違規認知」等三部分，各研究變項操作型定義及衡量方法分述如下：

3.3.1 基本資料

在基本資料部份，包括有員工個人背景屬性、使用電腦狀況、工作職務、教育訓練等部份。

一、其操作性定義分述如下：

1. 員工背景屬性：

本研究與個人背景有關的屬性，包括年齡、階級、教育程度等四個特徵。

2. 使用電腦狀況：

包含空軍人員之初次學習電腦的時間及平均每週使用電腦時間之長短。

3. 工作職務：

為空軍人員之工作環境狀況，包含教學、訓練與後勤部隊等單位。

二、衡量：

在人員屬性變項方面，其主要內容歸納為年齡、階級、教育程度等四項基本人口統計變數；在使用電腦狀況變項方面，其主要內容分別為初次學習電腦時間及平均每週使用電腦的時數。茲將問卷內容整理如表 3.1 所示。

表 3.1 個人背景之問卷內容

構　　面	題　　項
基本資料變　　項	1、年齡：□20 歲以下□21-29 歲□30-39 歲□40-49 歲□50 歲以上
	2、階級：□士兵□士官□尉級軍官□校級軍官□聘雇人員
	3、教育程度：□高中□專科□大學□研究所（含以上）
	4、初次學習電腦課程是何時： □高中以前□專科□大學□研究所□服役（工作）後□尚未學過
	5、平均每週使用電腦時數： □1 小時內□1-3 小時□3-6 小時□3-9 小時□9 小時以上
	6、工作單位：□幕僚單位□教學單位□訓練單位□部隊單位

資料來源：本研究整理

3.3.2 資訊安全素養

一、操作型定義：

資訊安全素養應指個人在具備操作資訊處理及傳播的工具與系統，包括電腦、媒體系統與網路的基本能力，為利用資訊與外界作資訊傳遞、共享、溝通與互動時所需的必備條件，且需體認資訊安全價值與力量，並能判斷其正當性，並能瞭解資訊安全本質、管理的特性，熟悉尋求方法並具備評估解釋及綜合資訊安全的能力。

二、衡量：

原則上是參考楊境恩(2004)的「國內警察人員資訊安全素養對資訊犯罪偵查能力影響之研究」調查問卷，與其之差異在於本問卷設計以空軍目前之資訊安全議題為主、空軍資訊安全相關法規及相關研究文獻，據以發展設計問卷題目。本研究歸納「資訊安全素養」內涵應包括「資訊安全知識」、「電腦操作技能」、「資訊倫理」等三個研究構面，其問項均為單選項目，採用 Likert 五點量表計分方式，以語意差異量表給予評等，其選項計分為「非常同意」5 分、「同意」4 分、「普通」3 分、「不同意」2 分、「非常不同意」1 分等。

1、資訊安全知識構面：

包含一些有關於資訊安全的功用和電腦上必備的保密知識、術語等。量表內容如表 3.2 所示。

表 3.2 資訊安全知識量表之問卷內容

衡量題項	選項及得分
1.我了解電腦密碼設定須符合複雜性原則(應含英文、數字及特殊符號至少 7 碼以上)。	5=非常同意 4=同意 3=普通 2=不同意 1=非常不同意
2.我了解電腦密碼，不可使用個人或眷屬生日、身分證字號、單位代號或有意義之英文字等來當作密碼。	
3.我了解設定好的電腦密碼，每季至少應更換乙次。	
4.我了解電腦應安裝最新「病毒碼」及「漏洞修補程式」。	
5.我了解不可以將密碼寫在電腦設備上，或告訴無關人員，以確保資料及系統安全。	
6.我了解電腦不可任意開啟「資源分享」功能，以防電腦遭受病毒感染。	
7.我了解發現不明來源之電子郵件，不可開啟郵件並應直接刪除。	
8.我了解應養成良好的習慣，不使用來歷不明的磁片、光碟片或軟體。	
9.我了解瀏覽色情網頁易遭電腦病毒或惡意程式感染。	
10.我了解電腦密碼長度要依規定超過 8 個字元。	

資料來源：本研究整理

2、電腦操作技能：

國軍人員所認知電腦在平時公務作業中的用途與相關操作的能力。量表內容如表 3.3 所示。

表 3.3 電腦操作技能量表之問卷內容

衡量題項	選項及得分
1.我有能力在公務電腦上安裝「國軍網路偵測軟體」。	5=非常同意 4=同意 3=普通 2=不同意 1=非常不同意
2.我有能力在公務電腦上設定「國軍保密警語畫面」及「國軍螢幕保護程式」。	
3.我有能力將重要公務資料，以「國軍檔案加解密軟體」設定加解密。	
4.我有能力安裝防毒軟體、更新病毒碼、漏洞修補程式及執行系統掃描。	
5.使用外來磁片或隨身碟時，我知道如何執行病毒掃描。	
6.我有能力安裝「國軍個人防火牆（BlackIce）」軟體，用以監測防阻不當網路入侵。	
7.當我的電腦感染病毒時，我有能力執行網路中斷，以避免造成大規模傳染。	
8.我有能力將電腦上重要資料加密儲存及備份。	
9.我有能力適時下載執行新病毒的清除工具，以維持系統正常運作。	
10.我有能力保護電腦資料，防止有意入侵人員竊取。	

資料來源：本研究整理

3、資訊倫理：

國軍人員在使用電腦時，所認知及恪遵的道德規約相關事項。量表內容如表 3.4 所示。

表 3.4 資訊倫理量表之問卷內容

衡量題項	選項及得分
1. 我了解不可任意安裝或使用非法軟體。	5=非常同意 4=同意 3=普通 2=不同意 1=非常不同意
2. 我了解不可在網路上散播違反善良風氣之暴力、色情等不當資訊。	
3. 我了解未經過合法授權，任意下載及轉寄(載)別人的著作，須同時受到民事及刑事的處罰。	
4. 我了解不可在網路上散播電腦病毒或惡意程式。	
5. 我了解使用具著作權的資訊時，應註明出處或徵得原作者的同意。	
6. 我了解應避免在網路公共討論區，指名道姓討論私人事務。	
7. 我了解未經查證或可疑的網路消息，不應再經由網路傳播出去。	
8. 我了解未經當事人同意，不應隨便將個人資料傳送給第三者	
9. 我了解不可隨意破解他人設定的電腦密碼。	
10. 我了解沒有經過合法授權，就把別人的著作放在網路上讓網友分享利用，那是一種不尊重著作權的網路盜版行為。	
11. 我了解在網路上公布軟體序號供別人使用，是種不合法的網路侵權行為。	
12. 我了解 USB 隨身碟規定由專人保管，不可私自使用。	

資料來源：本研究整理

3.3.3 資訊違規認知

一、操作型定義：

資訊違規即「違反保密規定」，係指違反國家機密保護法規，及「國軍保密實施規定」等有關保密之規定或命令，造成國防機密資訊有洩密顧慮，但未構成洩密者。

二、衡量：

原則上仍參考楊境恩(2004)的「國內警察人員資訊安全素養對資訊犯罪偵查能力影響之研究」調查問卷、國軍資訊安全相關法規及相關研究文獻，據以發展設計問

卷題目。本研究歸納「資訊違規認知」內涵應包括「電腦應用與影響」、「人員教育訓練」、「落實法規政策」等三個研究構面，其問項均為單選項目，採用李李克特（Likert）五點量表計分方式，以語意差異量表給予評等，其選項計分為「非常同意」5 分、「同意」4 分、「普通」3 分、「不同意」2 分、「非常不同意」1 分等。

1、電腦應用與影響：

係指電腦在公務傳輸、管制與應用上，對資訊安全可能發生之影響。量表內容如表 3.5 所示。

表 3.5 電腦應用與影響量表之問卷內容

衡量題項	選項及得分
1. 我了解全球資訊網站不可放置公務機敏資料，以防軍機外洩	5=非常同意 4=同意 3=普通 2=不同意 1=非常不同意
2. 我了解應用加解密技術，可以確保檔案傳輸的安全性。	
3. 我了解單位內必須做好資訊安全事件的通報機制，才能減少資安事件發生。	
4. 我了解經核准攜入營區之私人電腦及週邊設備應與辦公場所隔離，且不可混用。	
5. 我了解單位內連接「網際網路」之電腦，須指定專人管制及將連線紀錄備查。	
6. 我了解因公務需要使用資訊儲存媒體，應由資訊部門專責採購、管制及分發。	
7. 我了解單位購置之「資訊設備」及「儲存媒體」，應集中保管，以防止遺失或任意運用。	
8. 我了解電腦主機明顯處加貼「保密警語標籤」，並於機殼接合處粘貼「專用易碎標籤」，以防遭到破壞。	
9. 我了解資訊安全檢查，能有效發掘潛在問題，使官兵隨時養成良好保密習性。	
10. 我了解單位內電腦均須安裝「資安小幫手」。	

資料來源：本研究整理

2、人員教育訓練：

強化人員查核、人員管理及資訊法令宣教等，及其對資訊安全可能之影響。量表內容如表 3.6 所示。

表 3.6 人員教育訓練量表之問卷內容

衡量題項	選項及得分
1.我了解單位為做好資訊安全管理，必須要強調人員管理及資訊教育訓練。	5=非常同意 4=同意 3=普通 2=不同意 1=非常不同意
2.我了解定期接受資訊安全教育訓練，能有效降低及防範資訊違規事件發生。	
3.我了解資訊安全事項之宣導，能有效預防資訊系統遭受損害	
4.我了解電腦系統有中毒或異常現象，應即時通報系統管理者處置，以避免造成系統癱瘓。	
5.我了解落實「軍民網路實體隔離」政策，能有效避免軍機外洩事件發生。	
6.我了解個人未經核准，不得私設網站或提供各項網路資源服務。	
7.我了解資訊設備、媒體，應向保管人員辦理借用手續，才可使用。	
8.我了解資訊作業人員應定期接受安全查核，才可執行相關業務。	
9.我了解單位人員應定期實施資安教育訓練。	

資料來源：本研究整理

3、落實法規政策：

強調空軍人員對國軍資安法規之瞭解與相關限制，及其對資訊安全可能之影響。量表內容如表 3.7.1-3.7.2 所示。

表 3.7.1 落實法規政策量表之問卷內容

衡量題項	選項及得分
1.我了解各類型網路（國軍網路、戰情網路、情報與網際網路）均不得跨接混用。	5=非常同意 4=同意 3=普通 2=不同意 1=非常不同意
2.我了解屬於「密」級公務資料，須使用「國軍檔案加解密軟體」加密後才能在軍網上傳送。	
3.我了解不可將私人電腦及儲存媒體攜入營區使用。	
4.我了解電腦必須由單位保管人員收回系統管理者權限，以防遭他人安裝不當或非法軟體。	
5.我了解公務電腦必須設定輸出限制(關閉 USB 埠、光碟機、軟碟機等功能)，根絕輸出(入)源。	
6.我了解違反「網路實體隔離規定」將受「記大過並調職」之嚴厲處份。	
7.我了解違犯保密規定，其內容經查雖非屬國防機密資訊，但仍有影響保密軍紀或軍譽者，仍須受到處份。	

資料來源：本研究整理

表 3.7.2 落實法規政策量表之問卷內容（續）

衡量題項	選項及得分
8.我了解連接「網際網路」電腦，嚴禁用於處理單位公務資料	5=非常同意 4=同意 3=普通 2=不同意 1=非常不同意
9.我了解電腦業管人員離職或調職時，應先知會資訊部門撤換帳號、通行碼。	
10.我了解空軍人員違犯保密規定除當事人外，直屬一、二級主官（管）及該單保密軍官者應受連帶處份。	
11.我了解國軍人員因處理電腦資訊不當，如損及第三人權利等情事者，將依「刑法」、「陸海空軍刑法」、「電腦處理個人資料保護法」等相關法律偵辦。	
12.我了解須要求使用者對個人密碼盡保護及保密責任。	

資料來源：本研究整理

3.4預試

本問卷雖已參考相關法規、量表及研究文獻，但為求問卷調查結果能更加正確與嚴謹，將編製好之量表進行預試，以提高問卷的可行性。預試問卷在擬定初稿後，於民國 97 年 9 月 8 日利用某軍事學校莒光日資訊安全法令宣教時間，針對 30 名現職人員（含軍、士、官、聘雇及文職人員）進行預試。為求量表之精確，本研究除依據預試問卷進行信度與效度之檢驗外，另以專家檢核方式，親自邀請兩位指導教授、一位專業教授與 10 位資訊專業軍官，針對預試問卷內容各題項逐一檢視後，作語意修改與校正。

3.5建構正式問卷

配合本研究目的及專家意見，針對題目文字語意略作修改、增刪後，確認研究構面，完成正式問卷之建構（如附錄1），正式問卷包含資訊安全素養量表3個構面，題數共29題（如表3.8），資訊違規認知量表3個構面，題數共28題（如表3.9）。

表3.8 資訊安全素養之題數分配與題號摘要表

資訊安全素養構面	**題號分配**	**題數**
資訊安全知識	A1-A9	9
資訊安全操作技能	B1-B9	9
資訊倫理	C1-C11	11
總題數		**29**

表3.9 資訊違規認知之題數分配與題號摘要表

資訊違規認知構面	題號分配	題數
電腦應用與影響	D1-D9	9
人員教育訓練	E1-E8	8
落實法規政策	F1-F11	11
總題數		**28**

3.6 研究對象及抽樣方法

由於研究母群體龐大，礙於時間、人力及專業知識等因素考量，本研究屬地區性之研究，僅以空軍南部某軍事院校之現職人員為施測對象，問卷以親自送交及委託方式進行，採取「隨機取樣」方式進行抽樣問卷調查。

本研究採取問卷調查法為衡量方法，問卷依上述文獻探討中之理論基礎與學者之相關研究分析結果，找出合適問卷調查資料，進行實證資料蒐集。本研究採樣時間從97 年 09 月 18 日至 98 年 3 月 23 日，問卷共發送 500 份，回收 457 份，回收率達91.4%，其中不完整（資料不全或無效問卷）予以剔除計 18 份，共計有效樣本 439 份，有效回收率為 87.8%，各單位問卷發放及回收情形如表 3.10。

表 3.10 問卷發放及回收情形表

發放單位	發放份數	回收份數	回 收 率	有效份數	有效回收率
A 單位	**200**	**185**	**92.50%**	**175**	**87.50%**
B 單位	**200**	**187**	**93.50%**	**184**	**92.00%**
C 單位	**100**	**85**	**85.00%**	**80**	**80.00%**
合計	**500**	**457**	**91.40%**	**439**	**87.80%**

3.7 資料分析

本研究在調查問卷回收後，先將填答互相矛盾或太過一致之無效問卷剔除，隨即將有效問卷予以編碼，並彙整至資料庫中，所蒐集之資料以 SPSS for windows 12.0 統計軟體進行資料分析。依研究目的及變項性質選擇合適的統計方法，茲概述如下：

一、敘述性統計分析（Descriptive Statistics Analysis）

由於蒐集之資料均十分龐大，對於個別變數或因素進行描述性統計的方法，如何以簡單明白統計量數來描述說明各項變數與因素之平均值、標準差等，以了解各衡量

構面資料的特性，並針對不同屬性進行分析（邱皓政，2000）。藉由敘述性統計分析，以概括瞭解本研究之樣本結構，亦即有關樣本基本資料的分佈情形。本研究以求得各項基本資料之次數分配平均數及標準差，來分析比較國軍人員之背景特性。

二、因素分析（Factor Analysis）

藉由因素分析進行問卷項目構面縮減及適合度的檢定，利用其產生的因素負荷量來判斷個別項目與相對因素之關係。李順能（2005）指出，當因素設定為一個主成份時，各題目會顯示出其因素負荷量，若具有相當的同質性，則各題目會顯示一定水準的因素負荷量。一般研究中，是以 0.3 為界。Stevens（1992）提出因素數目考量與挑選的準則，選取特徵值大於 1 的因素，題項平均共通性（Commonality）最好在 0.6 以上。邱皓政（2000）指出，對建構效度之衡量，只要共通性相係數達 0.5 以上，即可視為高效度。

三、信度（reliability）與效度（validity）衡量

張紹勳（2000）從科學的觀點切入認為，一個良好的衡量工具應具備足夠的信度與效度。信度是指衡量工具的正確性與精確性。一般而言，一個具有信度的測量工具，必須在不同條件下都能獲得穩定的測量結果。葛樹人（1987）指出，Cronbach's α 係數為各種信度中較為嚴謹者，有時被稱為信度的低限，是目前採行最廣的指標。故以 Cronbach's α 值來測量問卷的內部一致性，若 Cronbach's α 係數值高，則顯示量表內各變項的相關性愈大，亦即其內部一致性愈一致性。Nunnally（1967）建議 Cronbach's α 係數要≧0.7 才屬於很可信的範圍，或至少要達到 0.5 以上方合乎信度要求。本研究以此建議來作為信度之衡量標準。

所謂效度則是指衡量工具能夠真正測出研究人員所想要衡量事務的程度。為瞭解本研究問項量表的信度情形，本研究乃參考相關文獻與法規政策之內容，另依據指導教授及實務專家根據各層面所包括之題項一一檢視修改提供修訂意見，確定各構面變項所涵蓋的題項後，先對各構面變項進行 Cronbach's α 信度係數分析，再逐題進行檢視，最後再以 SPSS 進行驗證性因素分析，以瞭解各構面變項與衡量題項間的內在一致性情形，及符合表面效度、內容效度及專家效度。

四、卡方檢定（Chi-Square.test）

檢測空軍人員使用電腦時間及初次學習電腦的時間是否因背景變項不同而有所差異；經檢定後，具有顯著的差異變項，則進一步透過交叉分析瞭解其差異情形。

五、獨立樣本（Independent Sample）T 檢定：

獨立樣本 T 檢定的目的在考驗兩個獨立母群體平均數差異的情形，若差異達到顯著水準，則代表兩個獨立母體彼此不同。在本研究中利用此方法，探討不同背景之空軍人員，在資訊安全素養及資訊違規認知方面之差異性。

六、單因子變異數分析（One-Way ANOVA）

在資料分析中，若要進行二組平均數的顯著考驗，以上述的獨立樣本 T 檢定最為適合，如果組別在三組以上，則必須使用單因子變異數分析法。在本研究中利用此方法，來探討不同背景之空軍人員，在資訊安全素養及資訊違規認知方面之差異；若達顯著，則以多重事後比較法，做進一步之分析比較，一般而言，當各組樣本數不同時，適用雪費法（Scheffe Mothod）來進行多重比較，以了解組群組之間的差異情形。

七、多元迴歸分析（Multiple Regression Analysis）

多元迴歸分析是同時以兩個以上的自變數對依變數進行迴歸，除了解之間相關及相關的方向與強度外，亦著重於利用自變數針對依數進行預測，自變數與依變數均須為計量變數，如果自變數為類別變數如來源國類別等時，則須先將變數轉換成「虛擬變數」（dummy variable），否則會違反線性關係的假定，而在 N 個類別的虛擬變項中，實際納入迴歸分析時只有 N-1 個，未經虛擬處裡的變數稱為參照組（reference group）。

四、實証分析

本章將根據回收資料運用適合之統計方法，並遵循本研究目的，將研究結果分為（1）基本資料敘述性統計分析；（2）各構面量表之因素及信度分析；（3）各構面量表之重視程度分析（次數分配）；（4）研究假說檢定結果；（5）小結等五個部份加以分析說明。

4.1 基本資料敘述性統計分析

本節將針對本研究空軍人員背景屬性中之年齡、階級、教育程度、初次學習電腦的時間、使用電腦時間及工作單位等變數分析說明。

個人背景變項之統計分析如表 4.1 所示。

一、年齡方面

20 歲以下為 30 人，佔 7.0%；21-29 歲為 263 人，比例最多，佔 60.0%；30-39 歲為 123 人，佔 28.0%；40-49 歲為 13 人，佔 3.0 %；50 歲以上為 10 人，佔 2.0%。空軍單位目前因應國家政經情勢發展及配合「人力精進案」之政策，國防人力運用之目標，朝以「量少」、「質精」的方向努力，人力狀況普遍趨向年輕化，經本研究樣本與母群體年齡特徵大致相符。

二、階級方面

士兵為 48 人，佔 11.0%；士官為 152 人，佔 35.0%；尉級軍官為 223 人，比例最多佔 50.0%；校級軍官為 11 人，佔 3.0%及聘雇人員為 5 人，比例最少，佔 1.0%。

三、教育程度方面

高中為 73 人，佔 17.0%；專科為 135 人，佔 31.0%；大學為 223 人，佔 50.0%；研究所為 8 人，比例最少，佔 2.0%。

四、初次學習電腦的時間方面

高中以前為 203 人，比例最多，佔 46.6%；專科為 120 人，佔 27.1%；大學為 70 人，佔 16.0%；工作後為 45 人，佔 10.1%及尚未學過為 1 人，比例最少，佔 0.2%。

五、每週使用電腦的時間方面

1 小時以內為 6 人，比例最少，佔 1.4%；1-3 小時為 26 人，佔 6.0%；3-6 小時為 68 人，佔 15.5%；6-9 小時為 86 人，佔 19.5%及 9 小時以上為 253 人，比例最多，佔 57.6%。

六、工作單位方面

部隊單位為 184 人，比例最多，佔 41.9%；訓練單位為 175 人，佔 39.9%及教學單位為 80 人，佔 18.2%。

表 4.1 背景變項統計分析表

背景屬性	類別	人數	比例	累計百分比
年齡	20 歲以下	30	7.0%	7.0%
	21-29 歲	263	60.0%	67.0%
	30-39 歲	123	28.0%	95.0%
	40-49 歲	13	3.0%	98.0%
	50 歲以上	10	2.0%	100.0%
階級	士兵	48	11.0%	11.0%
	士官	152	35.0%	46.0%
	尉級軍官	223	50.0%	96.0%
	校級軍官	11	3.0%	99.0%
	聘雇人員	5	1.0%	100.0%
教育程度	高中	73	17.0%	17.0%
	專科	135	31.0%	48.0%
	大學	223	50.0%	98.0%
	研究所	8	2.0%	100.0%
初次學習電腦時間	高中以前	203	46.6%	46.6%
	專科	120	27.1%	73.7%
	大學	70	16.0%	89.7%
	工作後	45	10.1%	99.8%
	尚未學過	1	0.2%	100.0%
使用電腦時間	1 小時	6	1.4%	1.4%
	1-3 小時	26	6.0%	7.4%
	3-6 小時	68	15.5%	22.9%
	6-9 小時	86	19.5%	42.4%
	9 小時以上	253	57.6%	100.0%
工作單位	教學單位	80	18.2%	18.2%
	訓練單位	175	39.9%	58.1%
	部隊單位	184	41.9%	100.0%

資料來源：本研究整理

4.2 各構面量表之因素及信度分析

本研究構面量表在「資訊安全素養」部份包括「資訊安全知識」、「電腦操作技能」、「資訊論理」等三個量表；在「資訊違規認知」部份包括「電腦應用與影響」、「人員教育訓練」、「落實法規政策」等三個量表。茲分別說明如下。

4.2.1 資訊安全知識部份

一、因素分析

利用主要成份分析（Principal Components）及最大變異數（Varimax）進行正交轉軸，藉以分析量表之因素結構與理論相符情形，因素分析時萃取特徵值大於 1，且旋轉後的因素負荷量（factor loading）之絕對值須大於 0.4，並採用題目與問卷中各量表之相關係數及其決斷值（critical ration）作為選題之參考。首先進行 Bartlett's 球體檢定，其檢定值為 1533.449（自由度為 36），達到顯著水準，顯示母群體的相關矩陣間有共同因素存在，且取樣適切性的 Kaiser-Meyer-Olkin（KMO）度量值達 0.788，表示問卷達到取樣適切性，顯示本研究抽樣資料適合進行因素分析，結果整理如表 4.2。

表 4.2 資訊安全知識的 KMO 與 Bartlett 檢定

Kaiser-Meyer-Olkin	取樣適切性量數	.788
Bartlett 球形檢定	近似卡方分配	1533.449
	自由度	36
	顯著性	.000

因素分析共計萃取出二個構面因素，其累積解釋變異量分別為 35.854%及 57.712%，各因素分析結果整理如表 4.3，其中包括因素代號、題項、因素負荷量、解釋變量及累積解釋變量等五項。

表 4.3 資訊安全知識量表因素分析

因素代號	題項	因素負荷量	解釋變異量%	累積解釋變異量%
因素一	2.我了解電腦密碼，不可使用個人或眷屬生日、身分證字號、單位代號或有意義之英文字等來當作密碼。	0.761	35.854	35.854
	3.我了解設定好的電腦密碼，每季至少應更換乙次。	0.878		
	4.我了解電腦應安裝最新「病毒碼」及「漏洞修補程式」	0.876		
	7.我了解發現不明來源之電子郵件，不可開啟郵件並應直接刪除。	0.745		
	8.我了解應養成良好的習慣，不使用來歷不明的磁片、光碟片或軟體。	0.699		
因素二	1. 我了解電腦密碼設定須符合複雜性原則(應含英文、數字及特殊符號至少七碼以上)。	0.429	21.858	57.712
	5.我了解不可以將密碼寫在電腦設備上，或告訴無關人員，以確保資料及系統安全。	0.762		
	6.我了解電腦不可任意開啟「資源分享」功能，以防電腦遭受病毒感染。	0.753		
	9.我了解瀏覽色情網頁易遭電腦病毒或惡意程式感染。	0.763		

二、信度分析

在因素分析完後，為進一步了解問卷的可靠性與有效性，則進行信度考驗分析。為確保因素構面之信度，針對萃取出的二個構面因素做檢定，並利用共同性（Commonality）來檢定建構效度，分析結果如表 4.4 所示。

表 4.4 資訊安全知識構面因素信度分析表

因素代號	題項	共同性	信度 Cronbach's α	整體信度
因素一	2.我了解電腦密碼，不可使用個人或眷屬生日、身分證字號、單位代號或有意義之英文字等來當作密碼。	0.593	0.8549	0.7520
	3.我了解設定好的電腦密碼，每季至少應更換乙次。	0.765		
	4.我了解電腦應安裝最新「病毒碼」及「漏洞修補程式」。	0.756		
	7.我了解發現不明來源之電子郵件，不可開啟郵件並應直接刪除。	0.572		
	8.我了解應養成良好的習慣，不使用來歷不明的磁片、光碟片或軟體。	0.507		
因素二	5.我了解不可以將密碼寫在電腦設備上，或告訴無關人員，以確保資料及系統安全。	0.590	0.6790	
	6.我了解電腦不可任意開啟「資源分享」功能，以防電腦遭受病毒感染。	0.573		
	9.我了解瀏覽色情網頁易遭電腦病毒或惡意程式感染。	0.627		

由表 4.4 得知，各構面整體信度為 0.7520，因素的信度 Cronbach's α 值均大於 0.6

，因此，每一資訊安全知識因素內的題項足以代表該因素構面，顯示本研究問卷的衡量項目具有一致性與穩定性。在資訊安全知識題項之共同性方面，題項之共同性皆大於 0.5，顯示此部份的問卷有相當高的建構效度。

4.2.2 電腦操作技能部份

一、因素分析：

利用主要成份分析（Principal Components）及最大變異數（Varimax）進行正交轉軸，藉以分析量表之因素結構與理論相符情形，因素分析時萃取特徵值大於 1，且旋轉後的因素負荷量（factor loading）之絕對值須大於 0.4，並採用題目與問卷中各量表之相關係數及其決斷值（critical ration）作為選題之參考。首先進行 Bartlett's 球體檢定，其檢定值為 1470.089（自由度為 36），達到顯著水準，顯示母群體的相關矩陣間有共同因素存在，且取樣適切性的 Kaiser-Meyer-Olkin（KMO）度量值達 0.886，表示問卷達到取樣適切性，顯示本研究抽樣資料適合進行因素分析，結果整理如表 4.5。

表 4.5 電腦操作技能的 KMO 與 Bartlett 檢定

Kaiser-Meyer-Olkin	取樣適切性量數	.886
Bartlett 球形檢定	近似卡方分配	1470.089
	自由度	36
	顯著性	.000

因素分析共計萃取出二個構面因素，其累積解釋變異量分別為 34.611%及 25.486%，各因素分析結果整理如表 4.6，其中包括因素代號、題項、因素負荷量、解釋變量及累積解釋變量等五項。

表 4.6 電腦操作技能量表因素分析

因素代號	題項	因素負荷量	解釋變異量%	累積解釋變異量%
因素一	1.我有能力在公務電腦上安裝「國軍網路偵測軟體（軍民網監控軟體）」。	0.801	34.611	60.097
	2. 我有能力在公務電腦上設定「國軍保密警語畫面」及「國軍螢幕保護程式」。	0.775		
	7.當我的電腦感染病毒時，我有能力執行網路中斷，以避免造成大規模傳染。	0.774		
	8.我有能力將電腦上重要資料加密儲存及備份。	0.788		
	9. 我有能力適時下載執行新病毒的清除工具，以維持系統正常運作。	0.785		
因素二	3. 我有能力將重要公務資料，以「國軍檔案加解密軟體」設定加解密。	0.756	25.486	
	4. 我有能力安裝防毒軟體、更新病毒碼、漏洞修補程式及執行系統掃描。	0.732		
	5.使用外來磁片或隨身碟時，我知道如何執行病毒掃描。	0.820		
	6.我有能力安裝「國軍個人防火牆（BlackIce）」軟體，用以監測防阻不當網路入侵。	0.688		

二、信度分析

在因素分析完後，為進一步了解問卷的可靠性與有效性，則進行信度考驗分析。為確保因素構面之信度，針對萃取出的二個構面因素做檢定，並利用共同性（Commonality）來檢定建構效度，分析結果如表 4.7 所示。

表 4.7 電腦操作技能構面因素信度分析表

因素代號	題項	共同性	信度 Cronbach's α	整體信度
因素一	1.我有能力在公務電腦上安裝「國軍網路偵測軟體（軍民網監控軟體）」。	0.652	0.8470	0.7818
	2. 我有能力在公務電腦上設定「國軍保密警語畫面」及「國軍螢幕保護程式」。	0.604		
	7.當我的電腦感染病毒時，我有能力執行網路中斷，以避免造成大規模傳染。	0.609		
	8.我有能力將電腦上重要資料加密儲存及備份。	0.623		
	9. 我有能力適時下載執行新病毒的清除工具，以維持系統正常運作。	0.633		
因素二	3. 我有能力將重要公務資料，以「國軍檔案加解密軟體」設定加解密。	0.585	0.7439	
	4. 我有能力安裝防毒軟體、更新病毒碼、漏洞修補程式及執行系統掃描。	0.536		
	5.使用外來磁片或隨身碟時，我知道如何執行病毒掃描。	0.694		
	6.我有能力安裝「國軍個人防火牆（BlackIce）」軟體，用以監測防阻不當網路入侵。	0.474		

由表 4.7 得知，各構面整體信度為 0.7818，因素的信度 Cronbach's α 值均大於 0.7，因此，每一電腦操作技能因素內的題項足以代表該因素構面，顯示本研究問卷的衡量項目具有一致性與穩定性。在電腦操作技能題項之共同性方面，題項之共同性皆大於 0.4，顯示此部份的問卷具有一定的建構效度。

4.2.3. 資訊倫理部份

一、因素分析：

利用主要成份分析（Principal Components）及最大變異數（Varimax）進行正交轉軸，藉以分析量表之因素結構與理論相符情形，因素分析時萃取特徵值大於 1，且旋轉後的因素負荷量（factor loading）之絕對值須大於 0.4，並採用題目與問卷中各量表之相關係數及其決斷值（critical ration）作為選題之參考。首先進行 Bartlett's 球體檢定，其檢定值為 1984.460（自由度為 36），達到顯著水準，顯示母群體的相關矩陣間有共同因素存在，且取樣適切性的 Kaiser-Meyer-Olkin（KMO）度量值達 0.868，表示問卷達到取樣適切性，顯示本研究抽樣資料適合進行因素分析，結果整理如表 4.8。

表 4.8 資訊倫理的 KMO 與 Bartlett 檢定

Kaiser-Meyer-Olkin	取樣適切性量數	.868
Bartlett 球形檢定	近似卡方分配	1984.460
	自由度	36
	顯著性	.000

因素分析共計萃取出二個構面因素，其累積解釋變異量分別為 50.318%及 18.782%，各因素分析結果整理如表 4.9，其中包括因素代號、題項、因素負荷量、解釋變量及累積解釋變量等五項。

表 4.9 資訊倫理量表因素分析

因素代號	題項	因素負荷量	解釋變異量%	累積解釋變異量%
因素一	1. 我了解不可任意安裝或使用非法軟體。	0.790	50.318	69.100
	2. 我了解不可在網路上散播違反善良風氣之暴力、色情等不當資訊。	0.787		
	3. 我了解未經過合法授權，任意下載及轉寄(載)別人的著作，須同時受到民事及刑事的處罰。	0.907		
	4. 我了解不可在網路上散播電腦病毒或惡意程式。	0.845		
	5. 我了解使用具著作權的資訊時，應註明出處或徵得原作者的同意。	0.755		
	6. 我了解應避免在網路公共討論區，指名道姓討論私人事務。	0.831		
	7. 我了解未經查證或可疑的網路消息，不應再經由網路傳播出去。	0.803		
	8. 我了解未經當事人同意，不應隨便將個人資料傳送給第三者。	0.907		
因素二	9. 我了解不可隨意破解他人設定的電腦密碼。	0.821	18.782	
	10. 我了解沒有經過合法授權，就把別人的著作放在網路上讓網友分享利用，那是一種不尊重著作權的網路盜版行為。	0.809		
	11. 我了解在網路上公布軟體序號供別人使用，是種不合法的網路侵權行為。	0.807		

二、信度分析

在因素分析完後，為進一步了解問卷的可靠性與有效性，則進行信度考驗分析。為確保因素構面之信度，針對萃取出的二個構面因素做檢定，並利用共同性（Commonality）來檢定建構效度，分析結果如表 4.10.1-4.10.2 所示。

表 4.10.1 資訊倫理構面因素信度分析

因素代號	題項	共同性	信度 Cronbach's α	整體信度
因素一	1. 我了解不可任意安裝或使用非法軟體。	0.639	0.9368	0.8729
	2. 我了解不可在網路上散播違反善良風氣之暴力、色情等不當資訊。	0.623		
	3. 我了解未經過合法授權，任意下載及轉寄(載)別人的著作，須同時受到民事及刑事的處罰。	0.825		
	4. 我了解不可在網路上散播電腦病毒或惡意程式。	0.723		

表 4.10.2 資訊倫理構面因素信度分析（續）

因素代號	題項	共同性	信度 Cronbach's α	整體信度
	5. 我了解使用具著作權的資訊時，應註明出處或徵得原作者的同意。	0.592		
	6. 我了解應避免在網路公共討論區，指名道姓討論私人事務。	0.703		
	7. 我了解未經查證或可疑的網路消息，不應再經由網路傳播出去。	0.821		
	8. 我了解未經當事人同意，不應隨便將個人資料傳送給第三者。	0.825		
因素二	9. 我了解不可隨意破解他人設定的電腦密碼。	0.678	0.7530	
	10. 我了解沒有經過合法授權，就把別人的著作放在網路上讓網友分享利用，那是一種不尊重著作權的網路盜版行為。	0.665		
	11. 我了解在網路上公布軟體序號供別人使用，是種不合法的網路侵權行為。	0.665		

由表 4.10 得知，各構面整體信度為 0.8729，因素的信度 Cronbach's α 值均大於 0.6，因此，每一資訊安全知識因素內的題項足以代表該因素構面，顯示本研究問卷的衡量項目具有一致性與穩定性。在資訊倫理題項之共同性方面，題項之共同性皆大於 0.5，顯示此部份的問卷有相當高的建構效度。

4.2.4. 電腦應用與影響部份

一、因素分析：

利用主要成份分析（Principal Components）及最大變異數（Varimax）進行正交轉軸，藉以分析量表之因素結構與理論相符情形，因素分析時萃取特徵值大於 1，且旋轉後的因素負荷量（factor loading）之絕對值須大於 0.4，並採用題目與問卷中各量表之相關係數及其決斷值（critical ration）作為選題之參考。首先進行 Bartlett's 球體檢定，其檢定值為 2483.911（自由度為 36），達到顯著水準，顯示母群體的相關矩陣間有共同因素存在，且取樣適切性的 Kaiser-Meyer-Olkin（KMO）度量值達 0.897，表示問卷達到取樣適切性，顯示本研究抽樣資料適合進行因素分析，結果整理如表 4.11。

表 4.11 電腦應用與影響的 KMO 與 Bartlett 檢定

Kaiser-Meyer-Olkin	取樣適切性量數	.897
Bartlett 球形檢定	近似卡方分配	2483.911
	自由度	36
	顯著性	.000

在本分量表中，在第一次因素分析時，共計萃取出二個構面因素，其累積解釋變異量分別為 54.072%及 11.704%，第二個構面因素部份，因其包含題項太少（僅為第 9 題），不適宜單獨構成一個因素，因此將它刪除後再進行第二次因素分析，各因素分析結果整理如表 4.12，其中包括因素代號、題項、因素負荷量、解釋變量及累積解釋變量等五項。

表 4.12 電腦應用與影響量表第一次因素分析

因素代號	題項	因素負荷量	解釋變異量%	累積解釋變異量%
因素一	1. 我了解全球資訊網站不可放置公務機敏資料，以防軍機外洩。	0.794	54.072	65.777
	2. 我了解應用加解密技術，可以確保檔案傳輸的安全性。	0.885		
	3. 我了解單位內必須做好資訊安全事件的通報機制，才能減少資安事件發生。	0.827		
	4. 我了解經核准攜入營區之私人電腦及週邊設備應與辦公場所隔離，且不可混用。	0.807		
	5. 我了解單位內連接「網際網路」之電腦，須指定專人管制及將連線紀錄備查。	0.813		
	6. 我了解因公務需要使用資訊儲存媒體，應由資訊部門專責採購、管制及分發。	0.848		
	7. 我了解單位購置之「資訊設備」及「儲存媒體」，應集中保管，以防止遺失或任意運用。	0.721		
	8. 我了解電腦主機明顯處加貼「保密警語標籤」，並於機殼接合處粘貼「專用易碎標籤」，以防遭到破壞。	0.462		
因素二	9. 我了解資訊安全檢查，能有效發掘潛在問題，使官兵隨時養成良好保密習性。	0.975	11.704	

第二次因素分析，Bartlett's 球體檢定值為 2457.525（自由度為 28），達到顯著水準，顯示母群體的相關矩陣間有共同因素存在，且取樣適切性的 Kaiser-Meyer-Olkin（

KMO）度量值達 0.901，表示問卷達到取樣適切性，顯示本研究抽樣資料適合進行因素分析，結果整理如表 4.13。

表 4.13 電腦應用與影響的 KMO 與 Bartlett 檢定

Kaiser-Meyer-Olkin	取樣適切性量數	.901
Bartlett 球形檢定	近似卡方分配	2457.525
	自由度	28
	顯著性	.000

進行第二次因素分析時，僅萃取出一個構面因素，其累積解釋變異量為 61.059%，各因素分析結果整理如表 4.14，其中包括因素代號、題項、因素負荷量、解釋變量及累積解釋變量等五項。

表 4.14 電腦應用與影響量表第二次因素分析

因素代號	題項	因素負荷量	解釋變異量%	累積解釋變異量%
因素一	1. 我了解全球資訊網站不可放置公務機敏資料，以防軍機外洩。	0.797	61.059	61.059
	2. 我了解應用加解密技術，可以確保檔案傳輸的安全性。	0.888		
	3. 我了解單位內必須做好資訊安全事件的通報機制，才能減少資安事件發生。	0.839		
	4. 我了解經核准攜入營區之私人電腦及週邊設備應與辦公場所隔離，且不可混用。	0.813		
	5. 我了解單位內連接「網際網路」之電腦，須指定專人管制及將連線紀錄備查。	0.803		
	6. 我了解因公務需要使用資訊儲存媒體，應由資訊部門專責採購、管制及分發。	0.854		
	7. 我了解單位購置之「資訊設備」及「儲存媒體」，應集中保管，以防止遺失或任意運用。	0.707		
	8. 我了解電腦主機明顯處加貼「保密警語標籤」，並於機殼接合處粘貼「專用易碎標籤」，以防遭到破壞。	0.470		

二、信度分析

在因素分析完後，為進一步了解問卷的可靠性與有效性，則進行信度考驗分析。為確保因素構面之信度，針對萃取出的單一因素做檢定，並利用共同性（Commonality

）來檢定建構效度，分析結果如表 4.15 所示。

表 4.15 電腦應用與影響構面因素信度分析

因素代號	題項	共同性	信度 Cronbach's α	整體信度
因素一	1. 我了解全球資訊網站不可放置公務機敏資料，以防軍機外洩。	0.636	0.9033	0.9033
	2. 我了解應用加解密技術，可以確保檔案傳輸的安全性。	0.789		
	3. 我了解單位內必須做好資訊安全事件的通報機制，才能減少資安事件發生。	0.703		
	4. 我了解經核准攜入營區之私人電腦及週邊設備應與辦公場所隔離，且不可混用。	0.661		
	5. 我了解單位內連接「網際網路」之電腦，須指定專人管制及將連線紀錄備查。	0.645		
	6. 我了解因公務需要使用資訊儲存媒體，應由資訊部門專責採購、管制及分發。	0.729		
	7. 我了解單位購置之「資訊設備」及「儲存媒體」，應集中保管，以防止遺失或任意運用。	0.500		
	8. 我了解電腦主機明顯處加貼「保密警語標籤」，並於機殼接合處粘貼「專用易碎標籤」，以防遭到破壞。	0.221		

由表 4.15 得知，本構面整體信度為 0.9033，因素的信度 Cronbach's α 值大於 0.9，因此，電腦應用與影響因素內的題項，足以代表該因素構面，顯示本研究問卷的衡量項目具有高度的一致性與穩定性。在電腦應用與影響題項之共同性方面，除第 8 題共同性稍顯低（0.221），較不具重要性外，其它題項之共同性皆大於 0.5，顯示此部份的問卷具有一定的建構效度。

4.2.5. 人員教育訓練部份

一、因素分析：

利用主要成份分析（Principal Components）及最大變異數（Varimax）進行正交轉軸，藉以分析量表之因素結構與理論相符情形，因素分析時萃取特徵值大於 1，且旋轉後的因素負荷量（factor loading）之絕對值須大於 0.4，並採用題目與問卷中各量表之相關係數及其決斷值（critical ration）作為選題之參考。首先進行 Bartlett's 球體檢定，其檢定值為 3483.511（自由度為 28），達到顯著水準，顯示母群體的相關矩陣間有

共同因素存在，且取樣適切性的 Kaiser-Meyer-Olkin（KMO）度量值達 0.769，表示問卷達到取樣適切性，顯示本研究抽樣資料適合進行因素分析，結果整理如表 4.16。

表 4.16 人員教育訓練的 KMO 與 Bartlett 檢定

Kaiser-Meyer-Olkin	取樣適切性量數	.769
Bartlett 球形檢定	近似卡方分配	3483.511
	自由度	28
	顯著性	.000

因素分析時，共計萃取出二個構面因素，其累積解釋變異量分別為 39.354%及 36.434%。第二個構面因素部份，因第 1 題因素負荷量太低（僅為 0.249），因此將它刪除後再進行第二次因素分析，各因素分析結果整理如表 4.17，其中包括因素代號、題項、因素負荷量、解釋變量及累積解釋變量等五項。

表 4.17 人員教育訓練量表因素分析

因素代號	題項	因素負荷量	解釋變異量%	累積解釋變異量%
因素一	4. 我了解電腦系統有中毒或異常現象，應即時通報系統管理者處置，以避免造成系統癱瘓。	0.797	39.354	75.788
	5. 我了解落實「軍民網路實體隔離」政策，能有效避免軍機外洩事件發生。	0.909		
	6. 我了解個人未經核准，不得私設網站或提供各項網路資源服務。	0.919		
	7. 我了解資訊設備、媒體，應向保管人員辦理借用手續，才可使用。	0.821		
因素二	1. 我了解單位為做好資訊安全管理，必須要強調人員管理及資訊教育訓練。	0.984	36.434	
	2. 我了解定期接受資訊安全教育訓練，能有效降低及防範資訊違規事件發生。	0.760		
	3. 我了解資訊安全事項之宣導，能有效預防資訊系統遭受損害。	0.767		
	8. 我了解資訊作業人員應定期接受安全查核，才可執行相關業務。	0.898		

二、信度分析

在因素分析完後，為進一步了解問卷的可靠性與有效性，則進行信度考驗分析。

為確保因素構面之信度，針對萃取出的單一因素做檢定，並利用共同性（Commonality）來檢定建構效度，分析結果如表 4.18 所示。

表 4.18 人員教育訓練構面因素信度分析

因素代號	題項	共同性	信度 Cronbach's α	整體信度
因素一	4. 我了解電腦系統有中毒或異常現象，應即時通報系統管理者處置，以避免造成系統癱瘓。	0.626	0.8984	0.8774
	5. 我了解落實「軍民網路實體隔離」政策，能有效避免軍機外洩事件發生。	0.857		
	6. 我了解個人未經核准，不得私設網站或提供各項網路資源服務。	0.885		
	7. 我了解資訊設備、媒體，應向保管人員辦理借用手續，才可使用。	0.707		
因素二	1. 我了解單位為做好資訊安全管理，必須要強調人員管理及資訊教育訓練。	0.806	0.8787	
	2. 我了解定期接受資訊安全教育訓練，能有效降低及防範資訊違規事件發生。	0.680		
	3. 我了解資訊安全事項之宣導，能有效預防資訊系統遭受損害。	0.682		
	8. 我了解資訊作業人員應定期接受安全查核，才可執行相關業務。	0.820		

由表 4.18 得知，本構面整體信度為 0.8774，因素的信度 Cronbach's α 值皆大於 0.8，因此，人員教育訓練因素內的題項，足以代表該因素構面，顯示本研究問卷的衡量項目具有高度的一致性與穩定性。在人員教育訓練題項之共同性方面，題項之共同性皆大於 0.5，顯示此部份的問卷具有一定的建構效度。

4.2.6. 落實法規政策部份

一、因素分析：

利用主要成份分析（Principal Components）及最大變異數（Varimax）進行正交轉軸，藉以分析量表之因素結構與理論相符情形，因素分析時萃取特徵值大於 1，且旋轉後的因素負荷量（factor loading）之絕對值須大於 0.4，並採用題目與問卷中各量表之相關係數及其決斷值（critical ration）作為選題之參考。首先進行 Bartlett's 球體檢定，其檢定值為 2329.128（自由度為 55），達到顯著水準，顯示母群體的相關矩陣間有共同因素存在，且取樣適切性的 Kaiser-Meyer-Olkin（KMO）度量值達 0.847，表示問

卷達到取樣適切性，顯示本研究抽樣資料適合進行因素分析，結果整理如表 4.19。

表 4.19 落實法規政策的 KMO 與 Bartlett 檢定

Kaiser-Meyer-Olkin	取樣適切性量數	.847
Bartlett 球形檢定	近似卡方分配	2329.128
	自由度	55
	顯著性	.000

在本分量表中，在第一次因素分析時，共計萃取出二個構面因素，其累積解釋變量分別為 34.470%、22.342%及 56.812%。第二個構面因素部份，因第 1 題因素負荷量太低（僅為 0.249），因此將它刪除後再進行第二次因素分析，各因素分析結果整理如表 4.20，其中包括因素代號、題項、因素負荷量、解釋變量及累積解釋變量等五項。

表 4.20 落實法規政策量表第一次因素分析

因素代號	題項	因素負荷量	解釋變異量%	累積解釋變異量%
因素一	5. 我了解公務電腦必須設定輸出限制(關閉 USB 埠、光碟機、軟碟機等功能)，根絕輸出(入)源。	0.793	34.470	56.812
	7. 我了解違犯保密規定，其內容經查雖非屬國防機密資訊，但仍有影響保密軍紀或軍譽者，仍須受到處份。	0.582		
	8. 我了解連接「網際網路」電腦，嚴禁用於處理單位公務資料。	0.873		
	9. 我了解電腦業管人員離職或調職時，應先知會資訊部門撤換帳號、通行碼。	0.824		
	10. 我了解空軍人員違犯保密規定除當事人外，直屬一、二級主官（管）及該單保密軍官者應受連帶處份。	0.814		
	11. 我了解空軍人員因處理電腦資訊不當，如損及第三人權利等情事者，將依「刑法」、「陸海空軍刑法」、「電腦處理個人資料保護法」等相關法律偵辦。	0.813		
因素二	1. 我了解各類型網路（國軍網路、戰情網路、情報與網際網路）均不得跨接混用。	0.249	22.342	
	2. 我了解屬於「密」級公務資料，須使用「國軍檔案加解密軟體」加密後才能在軍網上傳送。	0. 802		
	3. 我了解未經奉准，不可將私人電腦及儲存媒體攜入營區使用。	0.552		
	4. 我了解電腦必須由單位保管人員收回系統管理者權限，以防遭他人安裝不當或非法軟體。	0.773		
	6. 我了解違反「網路實體隔離規定」將受「記大過並調職」之嚴厲處份。	0.826		

第二次因素分析部份，Bartlett's 球體檢定值為 2295.731（自由度為 45），達到顯著水準，顯示母群體的相關矩陣間有共同因素存在，且取樣適切性的 Kaiser-Meyer-Olkin（KMO）度量值達 0.850，表示問卷達到取樣適切性，顯示本研究抽樣資料適合進行因素分析，結果整理如表 4.21。

表 4.21 落實法規政策的 KMO 與 Bartlett 檢定

Kaiser-Meyer-Olkin	取樣適切性量數	0.850
Bartlett 球形檢定	近似卡方分配	2295.731
	自由度	45
	顯著性	.000

進行第二次因素分析時，萃取出二個構面因素，其累積解釋變量分別為 38.188% 及 23.795%，各因素分析結果整理如表 4.22，其中包括因素代號、題項、因素負荷量、解釋變量及累積解釋變量等五項。

表 4.22 落實法規政策量表第二次因素分析

因素代號	題項	因素負荷量	解釋變異量%	累積解釋變異量%
因素一	5. 我了解公務電腦必須設定輸出限制(關閉 USB 埠、光碟機、軟碟機等功能)，根絕輸出(入)源。	0.797	38.188	61.983
	7. 我了解違犯保密規定，其內容經查雖非屬國防機密資訊，但仍有影響保密軍紀或軍譽者，仍須受到處份。	0.585		
	8. 我了解連接「網際網路」電腦，嚴禁用於處理單位公務資料。	0.877		
	9. 我了解電腦業管人員離職或調職時，應先知會資訊部門撤換帳號、通行碼。	0.828		
	10. 我了解空軍人員違犯保密規定除當事人外，直屬一、二級主官（管）及該單保密軍官者應受連帶處份。	0.817		
	11. 我了解國軍人員因處理電腦資訊不當，如損及第三人權利等情事者，將依「刑法」、「陸海空軍刑法」、「電腦處理個人資料保護法」等相關法律偵辦。	0.812		
因素二	2. 我了解屬於「密」級公務資料，須使用「國軍檔案加解密軟體」加密後才能在軍網上傳送。	0.801	23.795	
	3. 我了解未經奉准，不可將私人電腦及儲存媒體攜入營區使用。	0.544		
	4. 我了解電腦必須由單位保管人員收回系統管理者權限，以防遭他人安裝不當或非法軟體。	0.785		
	6. 我了解違反「網路實體隔離規定」將受「記大過並調職」之嚴厲處份。	0.827		

二、信度分析

在因素分析完後，為進一步了解問卷的可靠性與有效性，則進行信度考驗分析。為確保因素構面之信度，針對萃取出的二個構面因素做檢定，並利用共同性（Commonality）來檢定建構效度，分析結果如表 4.23 所示。

表 4.23 落實法規政策構面因素信度分析

因素代號	題項	共同性	信度 Cronbach's α	整體信度
因素一	5. 我了解公務電腦必須設定輸出限制(關閉 USB 埠、光碟機、軟碟機等功能)，根絕輸出(入)源。	0.671	0.8843	0.8282
	7. 我了解違犯保密規定，其內容經查雖非屬國防機密資訊，但仍有影響保密軍紀或軍譽者，仍須受到處份。	0.357		
	8. 我了解連接「網際網路」電腦，嚴禁用於處理單位公務資料。	0.803		
	9. 我了解電腦業管人員離職或調職時，應先知會資訊部門撤換帳號、通行碼。	0.715		
	10. 我了解空軍人員違犯保密規定除當事人外，直屬一、二級主官（管）及該單保密軍官者應受連帶處份。	0.693		
	11. 我了解空軍人員因處理電腦資訊不當，如損及第三人權利等情事者，將依「刑法」、「陸海空軍刑法」、「電腦處理個人資料保護法」等相關法律偵辦。	0.662		
因素二	2. 我了解屬於「密」級公務資料，須使用「國軍檔案加解密軟體」加密後才能在軍網上傳送。	0. 657	0.7441	
	3. 我了解未經奉准，不可將私人電腦及儲存媒體攜入營區使用。	0.303		
	4. 我了解電腦必須由單位保管人員收回系統管理者權限，以防遭他人安裝不當或非法軟體。	0.636		
	6. 我了解違反「網路實體隔離規定」將受「記大過並調職」之嚴厲處份。	0.702		

由表 4.23 得知，本構面整體信度為 0.8282，因素的信度 Cronbach's α 值大於 0.7，因此，落實法規政策因素內的題項，足以代表該因素構面，顯示本研究問卷的衡量項目具有高度的一致性與穩定性。在落實法規政策題項之共同性方面，除因素一的第 7 題（0.357）及因素二的第 3 題（0.303），其共同性稍顯低，較不具重要性外，其它題項之共同性皆大於 0.6，顯示此部份的問卷具有一定的建構效度。

綜合上述分析結果顯示，六個分量表的內部一致性 α 係數分別為 0.7520、0.7818

、0.8729、0.9033、0.8774 及 0.8282，其值均在 0.70 以上，信度係數均符合學者看法，具有高度的一致性及穩定性，因此，本研究量表應具有良好的信度與效度。

4.3 各構面量表之認知程度分析

本研究構面量表在「資訊安全素養」部份包括「資訊安全知識」、「電腦操作技能」、「資訊論理」等三個量表；在「資訊違規認知」部份包括「電腦應用與影響」、「人員教育訓練」、「落實法規政策」等三個量表。受測人員對研究構面的整體同意度，共分成 1-5 分，1 分表非常不同意；2 分表不同意；3 分表普通；4 分表同意；5 分表非常同意，以平均數 3 分加以區隔非常同意至非常不同意之次數分析，藉以瞭解受測人員對於各研究構面之認知程度，茲分別說明如下：

4.3.1 資訊安全素養量表次數分析

分析空軍人員其資訊安全素養之程度，在資訊安全知識、電腦操作技能及資訊倫理等構面，其每題平均值分別為 4.00、3.76 及 3.99，如表 4.24 所示。

在其三個構面中，以「資訊安全知識」的得分 4.00 為最高，而「電腦操作技能」的得分 3.76 為最低。顯示大部份空軍人員，其資訊安全素養在電腦實務的操作技能上需再進一步的加強。

表 4.24 資訊安全素養量表次數分析摘要表

構面	題項	最小值	最大值	平均數	每題平均數
資訊安全知識	9	9	45	36.02	4.00
電腦操作技能	9	9	45	33.83	3.76
資訊論理	11	11	55	43.73	3.99
資訊安全素養量表	29	29	145	113.58	3.92

資料來源：本研究整理

4.3.2 資訊違規認知量表次數分析

分析空軍人員對於資訊違規之認知程度，在電腦應用與影響、人員教育訓練及落實法規政策等構面，其每題平均值分別為 4.17、4.21 及 3.92，如表 4.25 所示。

在其三個構面中，以「人員教育訓練」的得分 4.21 為最高，而「落實法規政策」的得分 3.92 為最低。顯示大部份空軍人員之資訊違規之認知，對於空軍相關法規政策之落實仍有待加強。

表 4.25 資訊違規認知量表次數分析摘要表

構面	題項	最小值	最大值	平均數	每題平均數
電腦應用與影響	9	9	45	37.54	4.17
人員教育訓練	8	8	40	33.79	4.21
落實法規政策	11	11	55	43.05	3.92
資訊違規認知量表	28	28	140	114.38	4.10

資料來源：本研究整理

4.4 研究假說檢定結果

4.4.1 不同背景空軍人員初次學習電腦之獨立性分析

本節將以卡方檢定針對空軍人員屬性變項各構面因素進行分析，探討哪些背景變項會影響空軍人員初次學習電腦的時間。其中回收問卷中有關空軍人員「年齡」背景分類中的「40-49 歲」、「50 歲以上」；「階級」背景分類中的「聘雇人員」；「教育程度」變項分類中的「高中」、「研究所」等，因回收問卷個數太少，所以分別併入其他相關的分類中，經分析結果，背景變項除教育程度未達顯著水準外，餘均達顯著水準，表示空軍人員初次學習電腦的時間，會因為「年齡」、「階級」、「工作單位」之不同而有所差異，如表 4.26 所示。

表 4.26：人員屬性與初次學習電腦之分析

項目	卡方值	p 值	項目	卡方值	p 值
年齡	96.299**	.000	教育程度	4.932	.765
階級	24.547*	.002	工作單位	55.135**	.000

*p<.05　** p<.01

以下針對具顯著差異之變項，進行交叉分析比較，以了解其差異情形。茲分述如下：

（1）年齡方面：

因 20 歲以下、40-49 歲及 50 歲以上樣本數較少，故將 20 歲以下併入 21-29 歲；

40-49 歲及 50 歲以上併入 30-39 歲。年齡與初次學習電腦時間之交叉分析如表 4.27。

表 4.27 年齡與初次學習電腦時間交叉分析表

			初次學習電腦時間					
			高中以前	專科	大學	工作後	尚未學過	總和
年齡	21-29 歲（以下）	個數	133	70	50	39	1	293
		百分比	45.5%	23.8%	17.1%	13.3%	0.3%	100.0%
	30-39 歲（以上）	個數	30	14	37	65	0	146
		百分比	20.5%	9.6%	25.4%	44.5%	0%	100.0%

資料來源：本研究整理

由表 4.27 得知，21-29 歲（以下）階段中，在「高中以前」初次學習電腦者比例較高（45.5%），在 30-39 歲（以上）階段中，在「工作後」初次學習電腦者比例較高（44.5%），由此推論，在政府大力推行數位教學政策下，資訊教育都已普遍向下扎根，年輕一輩的空軍人員很早就有學習電腦的機會，但年齡層較高的空軍人員則是進入部隊服役工作後，受到近年來空軍部隊推行資訊數位化之影響，才對電腦有更一步的接觸。

（2）在階級方面：

因校級軍官及聘雇人員樣本數較少，因一般聘雇人員職等比照士兵階級，故將其分別納入尉級軍官及士兵階級一併統計。階級與初次學習電腦時間之交叉分析如表 4.28。

表 4.28 階級與初次學習電腦時間交叉分析表

			初次學習電腦時間					
			高中以前	專科	大學	工作後	尚未學過	總和
階級	士兵	個數	26	4	8	14	1	53
		百分比	49.1%	7.5%	15.1%	26.4%	1.9%	100.0%
	士官	個數	74	27	20	31	0	152
		百分比	48.7%	17.8%	13.2%	20.3%	0%	100.0%
	軍官	個數	116	51	42	25	0	234
		百分比	49.6%	21.8%	17.9%	10.7%	0%	100.0%

資料來源：本研究整理

由表 4.28 得知，在士兵、士官及軍官階級中，皆以「高中以前」初次學習電腦者分別為 49.1%、48.7%及 49.6%比例較高。由此推論，因目前空軍配合「人力精進案」及組織調整，人力狀況普遍趨向年輕化，其年齡層普遍較低，相對地，其學習電腦時間亦較早。

（3）在工作單位方面：

針對具顯著差異之變項，進行交叉分析比較，以了解其差異情形。工作單位與初次學習電腦時間交叉分析如表 4.29。

表 4.29 工作單位與初次學習電腦時間交叉分析表

			初次學習電腦時間					
			高中以前	專科	大學	工作後	尚未學過	總和
工作單位	教學單位	個數	42	20	11	7	0	80
		百分比	52.5%	25.0%	13.8%	8.7%	0%	100.0%
	訓練單位	個數	135	25	10	5	0	175
		百分比	77.1%	14.3%	5.8%	2.8%	0%	100.0%
	部隊單位	個數	138	23	19	4	0	184
		百分比	75.1%	12.5%	10.3%	2.1%	0%	100.0%

資料來源：本研究整理

由表 4.29 得知，在教學、訓練與部隊單位中，均以「高中以前」初次學習電腦者比例較高，分別為 52.5%、77.1%及 75.1%。由此推論，空軍人員不論其任務特性為何

，其初次學習電腦普遍都很早，顯示大部份空軍人員電腦方面皆應具有基本的操作能力。服役於教學、訓練與部隊單位之空軍人員，其雖於就學期間即接觸電腦，但由於平常忙於教學及部隊勤務，接觸電腦的機會相對較少，故每年定期辦理的空軍人員電腦鑑測，應將重點置於此類人員，使其除在平常忙於部隊勤務外，也能有更多學習電腦的機會，加強電腦方面的操作技能以習得一技之長。

4.4.2 不同背景國軍人員使用電腦時間之獨立性分析

本節將以卡方檢定針對空軍人員屬性變項各構面因素進行分析，探討哪些背景變項會影響空軍人員使用電腦的時間。其中回收問卷中有關空軍人員「年齡」背景分類中的「40-49 歲」、「50 歲以上」；「階級」背景分類中的「聘雇人員」；「教育程度」變項分類中的「高中」、「研究所」等，因回收問卷個數太少，所以分別併入其他相關的分類中，經分析結果，背景變項皆達顯著水準，表示空軍人員使用電腦的時間，會因為「年齡」、「階級」、「教育程度」、「工作單位」之不同而有所差異，如表 4.30 所示。

表 4.30：人員屬性與使用電腦時間之分析

項目	卡方值	p 值	項目	卡方值	p 值
年齡	60.482**	.000	教育程度	28.818**	.000
階級	81.413**	.000	工作單位	82.243**	.000

*p<.05　** p<.01

以下針對具顯著差異之變項，進行交叉分析比較，以了解其差異情形。茲分述如下：

（1）年齡方面：

因 20 歲以下、40-49 歲及 50 歲以上樣本數較少，故將 20 歲以下併入 21-29 歲；40-49 歲及 50 歲以上併入 30-39 歲，年齡與使用電腦時間交叉分析如表 4.31。

表 4.31 年齡與使用電腦時間交叉分析表

			每週使用電腦時間					
			1 小時	1-3 小時	3-6 小時	6-9 小時	9 小時以上	總和
年齡	21-29 歲（以下）	個數	9	20	43	69	152	293
		百分比	3.1%	6.8%	14.7%	23.5%	51.9%	100.0%
	30-39 歲（以上）	個數	5	7	4	9	121	146
		百分比	3.5%	4.8%	2.7%	6.2%	82.8%	100.0%

資料來源：本研究整理

由表 4.31 得知，21-29 歲（以下）及 30-39 歲（以上）階段中，均以「9 小時以上」比例較高，由此推論，空軍人員不同年齡層對網路的使用率均普遍提升，顯示空軍人員使用網路的習慣較以往有明顯不同，網路漸漸成為空軍人員不論工作上或生活中所不可或缺的傳輸工具。

（2）在階級方面：

因校級軍官及聘雇人員樣本數較少，因一般聘雇人員職等比照士兵階級，故將其分別納入尉級軍官及士兵階級一併統計。階級與使用電腦時間交叉分析如表 4.32。

表 4.32 階級與使用電腦時間交叉分析表

			每週使用電腦時間					
			1 小時	1-3 小時	3-6 小時	6-9 小時	9 小時以上	總和
階級	士兵	個數	2	3	9	6	33	53
		百分比	3.8%	5.6%	17.0%	11.3%	62.3%	100.0%
	士官	個數	0	2	5	19	126	152
		百分比	0%	1.3%	3.3%	12.5%	82.9%	100.0%
	軍官	個數	6	17	42	55	114	234
		百分比	2.6%	7.3%	17.9%	23.5%	48.7%	100.0%

資料來源：本研究整理

由表 4.32 得知，在士兵、士官及軍官階級中，每週使用電腦時間皆以「9 小時以上」，分別為 62.3%、82.9%及 48.7%比例較高。由此推論，空軍人員不論階級高低，對電腦的依賴程度都非常高。

（3）在教育程度方面：

因高中及研究所樣本數較少，故分別納入專科及大學一併統計，教育程度與使用電腦時間交叉分析如表 4.33。

表 4.33 教育程度與使用電腦時間交叉分析表

			每週使用電腦時間					
			1 小時	1-3 小時	3-6 小時	6-9 小時	9 小時以上	總和
教育程度	專科	個數	2	14	17	20	155	208
		百分比	1.0%	6.7%	8.2%	9.6%	74.5%	100.0%
	大學	個數	3	18	17	25	168	231
		百分比	1.3%	7.8%	7.4%	10.8%	72.7%	100.0%

資料來源：本研究整理

（4）在工作單位方面：

針對具顯著差異之變項，進行交叉分析比較，工作單位與使用電腦時間交叉分析如表 4.34。

表 4.34 工作單位與使用電腦時間交叉分析表

			每週使用電腦時間					
			1 小時	1-3 小時	3-6 小時	6-9 小時	9 小時以上	總和
工作單位	教學單位	個數	0	6	9	30	35	80
		百分比	0%	7.5%	11.3%	37.5%	43.7%	100.0%
	訓練單位	個數	1	5	26	46	97	175
		百分比	0.6%	2.9%	14.8%	26.3%	55.4%	100.0%
	部隊單位	個數	0	15	23	18	128	184
		百分比	0%	8.2%	12.5%	9.8%	69.5%	100.0%

資料來源：本研究整理

由表 4.34 得知，在教學、訓練與部隊單位中，均以「9 小時以上」分別為 43.7%、55.4%及 69.5%比例較高，但相較之下，教學單位在比例上明顯少了許多，由此推論，服役於訓練與部隊單位之空軍人員，工作期間舉凡在業務勤務或教學準備上都需使

用到電腦，接觸電腦的機會相對提高，而服役於教學單位之空軍人員，由於平常忙於教課，使用電腦的機會明顯減少。

4.5 空軍人員背景與資訊安全素養關係之分析

本節將針對空軍人員屬性變項對各構面因素以獨立樣本 T 檢定及單因子變異數分析，了解其差異情形，用以檢定本研究假說一：空軍人員背景之不同，在資訊安全素養上應有顯著之差異。

4.5.1 空軍人員年齡之不同，在資訊安全素養上之差異情形

使用獨立樣本 T 檢定，檢驗不同年齡在國軍人員資訊安全素養及其各層面的影響，其分析結果如表 4.35 所示。

表 4.35 年齡與資訊安全素養分析摘要表

構面	年齡	樣本數	平均數	標準差	T 值	P 值
資訊安全知識	21-29 歲（以下）	293	35.5805	5.0686	-3.152*	.002
	30-39 歲（以上）	146	37.1206	4.4360		
資訊操作技能	21-29 歲（以下）	293	33.1897	5.1874	-4.383**	.000
	30-39 歲（以上）	146	35.4326	4.9703		
資訊倫理	21-29 歲（以下）	293	43.0057	6.4325	-4.094**	.000
	30-39 歲（以上）	146	45.5674	5.8374		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4.35 得知，經由獨立樣本 T 檢定，不同年齡之空軍人員在資訊安全素養的相關因素分析中，以「年齡」為檢定變數，「資訊安全素養」之各構面為分組變數，因 20 歲以下、40-49 歲及 50 歲以上樣本數較少，故將 20 歲以下併入 21-29 歲；40-49 歲及 50 歲以上併入 30-39 歲，在顯著水準 0.05 的情況下，結果分析如下：

1.資訊安全知識構面分析結果：

達到顯著水準（P=.002），表示不同年齡之空軍人員在資訊安全素養之資訊安全知識因素上有顯著差異。

2. 資訊操作技能構面分析結果：

達到顯著水準（P=.000），表示不同年齡之空軍人員在資訊安全素養之資訊資訊操作技能因素上有顯著差異。

3.資訊倫理構面分析結果：

達到顯著水準（P=.000），表示不同年齡之空軍人員在資訊安全素養之資訊倫理因素上有顯著差異。

分析結果：

經由獨立樣本 T 檢定結果說明，在顯著水準 0.05 的情況下，結果證實【假設 1-1：空軍人員年齡之不同，在資訊安全素養上應有顯著之差異，研究假說成立】。

4.5.2 空軍人員階級之不同，在資訊安全素養上之差異情形

使用獨立樣本 T 檢定，檢驗不同階級在空軍人員資訊安全素養及其各層面的影響，因校級軍官及聘雇人員樣本數較少，因一般聘雇人員職等比照士兵階級，故將其分別納入尉級軍官及士兵階級一併統計。其分析結果如表 4.36 所示。

表 4.36　階級與資訊安全素養分析摘要表

構面	階級	樣本數	平均數	標準差	T 值	P 值
資訊安全知識	士官兵	205	36.1804	5.0277	.565	.572
	軍官	234	35.9220	4.8869		
資訊操作技能	士官兵	205	33.7835	5.4302	-.186	.856
	軍官	234	33.8712	5.0874		
資訊倫理	士官兵	205	43.5103	6.7787	-.659	.510
	軍官	234	43.8983	6.0892		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4.36 得知，經由獨立樣本 T 檢定，不同階級之空軍人員在資訊安全素養的相關因素分析中，以「階級」為自變項（因子），「資訊安全素養」為依變項，進行 T 檢定，因校級軍官及聘雇人員樣本數較少，故分別併入尉級軍官及士兵階級裡，區分為士官兵及軍官兩組，在顯著水準 0.05 的情況下，結果分析如下：

1.資訊安全知識構面分析結果：

未達到顯著水準（P=.572），表示不同階級之空軍人員在資訊安全素養之資訊安全知識因素上無顯著差異。

2. 資訊操作技能構面分析結果：

未達到顯著水準（P=.856），表示不同階級之空軍人員在資訊安全素養之資訊操作技能因素上無顯著差異。

3. 資訊倫理構面分析結果：

未達到顯著水準（P=.510），表示不同階級之空軍人員在資訊安全素養之資訊倫理因素上無顯著差異。

分析結果：

經由獨立樣本 T 檢定，在顯著水準 0.05 的情況下，結果證實【假說 1-2：空軍人員階級之不同，在資訊安全素養上應有顯著之差異，其研究假說不成立】。

4.5.3 空軍人員教育程度之不同，在資訊安全素養上之差異情形

使用 One-way ANOVA 檢驗不同教育程度在空軍人員資訊安全素養及其各層面的影響，其分析結果如表 4.37 所示。

表 4.37 教育程度與資訊安全素養分析摘要表

構面	教育程度	樣本數	平均數	標準差	F 值	P 值
資訊安全知識	高中	73	35.7121	5.3659	.316	.730
	專科	135	36.2741	5.4093		
	大學	231	35.9792	4.6102		
	整體	439	36.0245	4.9397		
資訊操作技能	高中	73	32.3788	5.9994	3.793*	.023
	專科	135	34.5259	5.5001		
	大學	231	33.8472	4.8328		
	整體	439	33.8364	5.2207		
資訊倫理	高中	73	42.7273	7.5275	2.023	.133
	專科	135	44.5556	6.5068		
	大學	231	43.5972	5.9812		
	整體	439	43.7444	6.3677		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4. 37 得知，經由 One-way ANOVA 檢定，不同教育程度之空軍人員在資訊安全素養的相關因素分析中，以「教育程度」為自變項（因子），「資訊安全素養」各構面為依變項，在顯著水準 0.05 的情況下，結果分析如下：

1.資訊安全知識構面分析結果：

未達到顯著水準（P=.730），表示不同教育程度之空軍人員在資訊安全素養之資訊安全知識因素上無顯著差異。

2. 資訊操作技能構面分析結果：

達到顯著水準（P=.023），表示不同教育程度之空軍人員在資訊安全素養之資訊操作技能因素上有顯著差異。

3. 資訊倫理構面分析結果：

未達到顯著水準（P=.133），表示不同教育程度之空軍人員在資訊安全素養之資訊倫理因素上無顯著差異。

分析結果：

經由單因子變異數分析檢定，在顯著水準 0.05 的情況下，假設 1-3 顯著，其結果證實空軍人員教育程度之不同，在資訊安全素養上應有顯著之差異，其研究假說部份成立。當變異數分析，顯示達顯著水準時，表示其可能有顯著差異存在，故再進行事後比較（Post Hoc comparison）分析，各構面因素多重比較 Scheffe 檢定結果如表 4.38 所示，並說明如下：

在「資訊操作技能」方面：教育程度為專科與高中作比較，其平均差異值為正數（2.1471），且達顯著水準（.023），顯示專科相較於高中，有較高的資訊操作技能，其與大學作比較，則無顯著差異。

表 4.38 教育程度在資訊安全素養各構面 Scheffe 檢定摘要表

依變數	(I) 初次修習	(J) 初次修習	平均差異 (I-J)	標準誤	顯著性
資訊安全知識	高中	專科	-.5620	.7430	.751
		大學	-.2670	.6751	.925
	專科	高中	.5620	.7430	.751
		大學	.2949	.5160	.849
	大學	高中	.2670	.6751	.925
		專科	-.2949	.5160	.849
資訊操作技能	高中	專科	-2.1471(*)	.7797	.023
		大學	-1.4684	.7084	.118
	專科	高中	2.1471(*)	.7797	.023
		大學	.6787	.5415	.456
	大學	高中	1.4684	.7084	.118
		專科	-.6787	.5415	.456
資訊倫理	高中	專科	-1.8283	.9544	.161
		大學	-.8699	.8672	.605
	專科	高中	1.8283	.9544	.161
		大學	.9583	.6628	.352
	大學	高中	.8699	.8672	.605
		專科	-.9583	.6628	.352

資料來源：本研究整理　註：*在.05 水準上的平均差異很顯著。

4.5.4 空軍人員初次學習電腦時間之不同，在資訊安全素養上之差異情形

使用 One-way ANOVA 檢驗不同階級在空軍人員資訊安全素養及其各層面的影響，其分析結果如表 4.39 所示。

表 4.39　初次學習電腦時間與資訊安全素養分析摘要表

構面	工作單位	樣本數	平均數	標準差	F 值	P 值
資訊安全知識	高中以前	203	35.7807	5.3330	.461	.765
	專科以後	120	36.1605	4.5729		
	大學以後	70	36.3857	4.6072		
	工作以後	45	36.4853	4.0574		
	尚未學過	1	34.0000	.		
	整體	439	36.0245	4.9397		

資訊操作技能	高中以前	203	33.6803	5.4494	1.360	.247
	專科以後	120	33.9259	4.8626		
	大學以後	70	33.3143	5.0806		
	工作以後	45	34.9706	4.7661		
	尚未學過	1	28.0000	.		
	整體	439	33.8364	5.2207		
資訊倫理	高中以前	203	43.4015	6.8253	1.246	.291
	專科以後	120	44.1852	5.9290		
	大學以後	70	43.3857	5.6473		
	工作以後	45	45.0294	5.5824		
	尚未學過	1	38.0000	.		
	整體	439	43.7444	6.3677		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4.39 得知，經由 One-way ANOVA 檢定，初次學習電腦時間不同之空軍人員在資訊安全素養的相關因素分析中，以「初次學習電腦時間」為自變項（因子），資訊安全素養各構面為依變項，進行 F 檢定，在顯著水準 0.05 的情況下，結果分析如下：

1.資訊安全知識構面分析結果：

未達到顯著水準（P=.765），表示空軍人員初次學習電腦時間之不同，在資訊安全素養之資訊安全知識因素上無顯著差異。

2. 資訊操作技能構面分析結果：

未達到顯著水準（P=.247），表示空軍人員初次學習電腦時間之不同，在資訊安全素養之資訊操作技能因素上無顯著差異。

3. 資訊倫理構面分析結果：

未達到顯著水準（P=.291），表示空軍人員初次學習電腦時間之不同，在資訊安全素養之資訊倫理因素上無顯著差異。

分析結果：

經由單因子變異數分析檢定，在顯著水準 0.05 的情況下，研究假設 1-4 不顯著，

，其它的結果一樣，故結果證實空軍人員初次學習電腦時間之不同，在資訊安全素養上應有顯著之差異，其研究假說不成立。

4.5.5 空軍人員使用電腦時間之不同，在資訊安全素養上之差異情形

使用 One-way ANOVA 檢驗不同階級在空軍人員資訊安全素養及其各層面的影響，其分析結果如表 4.40 所示。

表 4.40 使用電腦時間與資訊安全素養分析摘要表

構面	使用電腦時間	樣本數	平均數	標準差	F 值	P 值
資訊安全知識	1 小時	6	34.3846	4.3116	1.029	.391
	1-3 小時	26	35.0323	3.7637		
	3-6 小時	68	35.7424	4.5651		
	6-9 小時	86	35.8256	5.3954		
	9 小時以上	253	36.3242	5.0103		
	整體	439	36.0245	4.9397		
資訊操作技能	1 小時	6	33.5385	4.1153	1.026	.394
	1-3 小時	26	32.1290	4.1048		
	3-6 小時	68	33.0606	5.3490		
	6-9 小時	86	33.6163	5.2517		
	9 小時以上	253	34.2696	5.2985		
	整體	439	33.8364	5.2207		
資訊倫理	1 小時	6	42.7692	4.5489	1.757	.136
	1-3 小時	26	41.9355	5.7151		
	3-6 小時	68	43.4394	6.0514		
	6-9 小時	86	43.5000	6.6399		
	9 小時以上	253	44.1195	6.4810		
	整體	439	43.7444	6.3677		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4.40 得知，經由 One-way ANOVA 檢定，使用電腦時間不同之空軍人員在資訊安全素養的相關因素分析中，以「使用電腦時間」為自變項（因子），資訊安全素

養各構面為依變項，進行 F 檢定，在顯著水準 0.05 的情況下，結果分析如下：

1.資訊安全知識構面分析結果：

未達到顯著水準（P=.391），表示空軍人員使用電腦時間之不同，在資訊安全素養之資訊安全知識因素上無顯著差異。

2. 資訊操作技能構面分析結果：

未達到顯著水準（P=.394），表示空軍人員使用電腦時間之不同，在資訊安全素養之資訊操作技能因素上無顯著差異。

3. 資訊倫理構面分析結果：

未達到顯著水準（P=.136），表示空軍人員使用電腦時間之不同，在資訊安全素養之資訊倫理因素上無顯著差異。

分析結果：

經由單因子變異數分析檢定，在顯著水準 0.05 的情況下，結果證實【研究假設 1-5：空軍人員使用電腦時間之不同，在資訊安全素養上應有顯著之差異，其研究假說不成立。】

4.5.6 空軍人員工作單位之不同，在資訊安全素養上之差異情形

使用 One-way ANOVA 檢驗不同階級在空軍人員資訊安全素養及其各層面的影響，其分析結果如表 4.41 所示。

表 4.41 工作單位與資訊安全素養分析摘要表

構面	工作單位	樣本數	平均數	標準差	F 值	P 值
資訊安全知識	教學單位	80	3.2023	.8166	3.749*	.011
	訓練單位	175	3.2463	.7644		
	部隊單位	184	3.4773	.6682		
	整體	439	3.3134	.7490		
資訊操作技能	教學單位	80	4.3564	.6888	7.533**	.000
	訓練單位	175	4.2254	.7226		
	部隊單位	184	4.2343	.5925		
	整體	439	4.3182	.6702		

資訊倫理	教學單位	80	3.8434	.5684	6.317**	.000
	訓練單位	175	3.7902	.5771		
	部隊單位	184	3.8979	.5034		
	整體	439	3.8716	.5450		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4.41 得知，經由 One-way ANOVA 檢定，不同單位之空軍人員在資訊安全素養的相關因素分析中，以「工作單位」為自變項（因子），資訊安全素養為依變項，進行 F 檢定，在顯著水準 0.05 的情況下，結果分析如下：

1.資訊安全知識構面分析結果：

達到顯著水準（P=.011），表示不同工作單位之空軍人員在資訊安全素養之資訊安全知識因素上有顯著差異。

2. 資訊操作技能構面分析結果：

達到顯著水準（P=.000），表示不同工作單位之空軍人員在資訊安全素養之資訊操作技能因素上有顯著差異。

3. 資訊倫理構面分析結果：

達到顯著水準（P=.000），表示不同工作單位之空軍人員在資訊安全素養之資訊倫理因素上有顯著差異。

分析結果：

經由單因子變異數分析檢定，在顯著水準 0.05 的情況下，結果證實【研究假設 1-6：空軍人員工作單位之不同，在資訊安全素養上應有顯著之差異，其研究假說成立】。當變異數分析，顯示達顯著水準時，表示其可能有顯著差異存在，故再進行事後比較（Post Hoc comparison）分析，各構面因素多重比較 Scheffe 檢定結果如表 4.42 所示，並說明如下：

1. 在「資訊安全知識」方面：

部隊單位與訓練單位及教學單位做比較，其平均差異值為正數（.2750 及.2309），且達顯著水準（.019 及.023），顯示部隊單位較教學單位及訓練單位，有較高的資訊安全知識（部隊單位>教學單位>訓練單位），其與訓練單位分析比較結果則無明

顯差異。

2. 在「資訊操作技能」方面：

部隊單位與訓練單位及教學單位做比較，其平均差異值為正數（.1310 及.1220），且達顯著水準（.017 及.026），顯示部隊單位較教學單位及訓練單位，有較高的資訊操作技能（部隊單位>訓練單位>教學單位），其與訓練單位分析比較結果則無明顯差異。

3. 在「資訊倫理」方面：

部隊單位與教學單位及訓練單位做比較，其平均差異值為正數（.1276 及.1335），且達顯著水準（.011 及.023），顯示部隊單位較教學單位及訓練單位，有較高的資訊倫理觀念（部隊單位>訓練單位>教學單位），其與訓練單位分析比較結果則無明顯差異。

表 4.42 工作單位在資訊安全素養各構面 Scheffe 檢定摘要表

依變數	(I) 工作單位	(J) 工作單位	平均差異 (I-J)	標準誤	顯著性
資訊安全知識	訓練	教學	-4.4069E-02	8.779E-02	.969
		部隊	-.2750	.1029	.069
	教學	訓練	4.407E-02	8.779E-02	.969
		部隊	-.2309	9.091E-02	.093
	部隊	訓練	.2750(*)	.1029	.019
		教學	.2309(*)	9.091E-02	.023
資訊操作技能	訓練	教學	-.1220	7.767E-02	.616
		部隊	8.978E-03	9.104E-02	1.000
	教學	訓練	-.1310	7.767E-02	.417
		部隊	-8.9776E-03	8.043E-02	1.000
	部隊	訓練	.1310(*)	9.104E-02	. 017

		教學	.1220(*)	8.043E-02	.026
資訊倫理	訓練	教學	5.319E-02	6.338E-02	.872
		部隊	-5.4433E-02	7.430E-02	.911
	教學	訓練	-5.3190E-02	6.338E-02	.872
		部隊	-.1076	6.564E-02	.443
	部隊	訓練	.1335(*)	7.430E-02	.023
		教學	.1276(*)	6.564E-02	.011

資料來源：本研究整理　註：*在.05 水準上的平均差異很顯著。

4.5.7 空軍人員背景與資訊安全素養關係研究結果

綜合以上分析結果，本研究將空軍人員背景與資訊安全素養差異性檢定結果彙整如表 4.43。

表 4.43　空軍人員背景與資訊安全素養差異性檢定彙整表

構面	年齡	階級	教育程度	初次學習電腦時間	使用電腦時間	工作單位
資訊安全知識	T=-3.152**	T=.565	F=.316	F=.461	F=1.029	F=3.749*
	P=.002	P=.572	P=.730	P=.765	P=.391	P=.011
資訊操作技能	F=-4.383**	T =-.186	F=3.793*	F=1.360	F=1.026	F=7.533**
	P=.000	P=.856	P=.023	P=.247	P=.394	P=.000
資訊倫理	F=-4.094*	T =-.659	F=2.023	F=1.246	F=1.757	F=6.317**
	P=.000	P=.510	P=.133	P=.291	P=.136	P=.000

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4.43 分析結果得知：

1. 年齡方面，對於空軍人員之資訊安全素養而言，在資訊安全知識、資訊操作技能與資訊倫理構面上，均有顯著差異。
2. 階級方面，對於空軍人員之資訊安全素養而言，均無顯著差異。
3. 教育程度方面，對於空軍人員之資訊安全素養而言，除資訊操作技能構面上有顯著

差異外，其它並無顯著差異。

4.初次學習電腦時間方面，對於空軍人員之資訊安全素養而言，均無顯著差異。

5.使用電腦時間方面，對於空軍人員之資訊安全素養而言，均無顯著差異。

6.工作單位方面，對於空軍人員之資訊安全素養而言，在資訊安全知識、資訊操作技能與資訊倫理構面上，均有顯著差異。

4.6 空軍人員背景與資訊違規認知關係之分析

本節將針對空軍人員屬性變項對各構面因素以獨立樣本 T 檢定及單因子變異數做分析比較，以了解其差異情形，用以檢定本研究假說二。

4.6.1 空軍人員年齡之不同，在資訊違規認知上之差異情形

使用獨立樣本 T 檢定，分析不同年齡之空軍人員，在資訊違規認知及其各層面的影響，其分析結果如表 4.44 所示。

表 4.44　年齡與資訊違規認知分析摘要表

構面	年齡	樣本數	平均數	標準差	T 值	P 值
電腦應用與影響	21-29 歲（以下）	293	37.2586	5.0367	.148**	.072
	30-39 歲（以上）	146	38.1702	5.1491		
資訊教育訓練	21-29 歲（以下）	293	42.7816	6.0871	3.670**	.141
	30-39 歲（以上）	146	43.6596	5.6377		
落實法規政策	21-29 歲（以下）	293	33.3851	4.7291	1.378	.002
	30-39 歲（以上）	146	34.7943	4.3973		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4.44 得知，經由獨立樣本 T 檢定結果，不同年齡之空軍人員在資訊違規認知的相關因素分析中，以「資訊違規認知」各構面因素為檢定變數，以「年齡」為分組變數，因 20 歲以下、40-49 歲及 50 歲以上樣本數較少，故將 20 歲以下併入 21-29 歲；40-49 歲及 50 歲以上併入 30-39 歲，在顯著水準 0.05 的情況下，結果分析如下：

1.電腦應用與影響構面分析結果：

未達到顯著水準（P=.072），表示不同年齡之空軍人員在資訊違規認知上，在電腦應用與影響方面無顯著差異。

2. 資訊教育訓練構面分析結果：

未達到顯著水準（P=.141），表示不同年齡之空軍人員在資訊違規認知上，在資訊教育訓練方面無顯著差異。

3. 落實法規政策構面分析結果：

達到顯著水準（P=.002），表示不同年齡之空軍人員在資訊違規認知上，在落實法規政策方面有顯著差異。

分析結果：

經由獨立樣本 T 檢定，在顯著水準 0.05 的情況下，結果證實【研究假設 2-1：空軍人員年齡之不同，在資訊違規認知上應有顯著之差異】，其研究假說部份成立。

4.6.2 空軍人員階級之不同，在資訊違規認知上之差異情形

使用獨立樣本 T 檢定，檢驗不同階級之空軍人員，在資訊違規認知及其各層面的影響，其分析結果如表 4.45 所示。

表 4.45　階級與資訊違規認知分析摘要表

構面	階級	樣本數	平均數	標準差	T 值	P 值
電腦應用與影響	士官兵	205	37.4897	5.4108	1.400	.162
	軍官	234	37.5424	4.8611		
資訊教育訓練	士官兵	205	42.7577	6.1810	1.948	.052
	軍官	234	43.2169	5.8281		
落實法規政策	士官兵	205	33.7062	4.9548	1.374	.108
	軍官	234	33.8475	4.4896		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4.45 得知，經由獨立樣本 T 檢定，不同階級之空軍人員在資訊違規認知的相關因素分析中，以「資訊違規認知」各構面因素為檢定變數，「階級」為分組變數，進行 T 檢定，因校級軍官及聘雇人員樣本數較少，故分別併入尉級軍官及士兵階級裡，區分為士官兵及軍官兩組，在顯著水準 0.05 的情況下，結果分析如下：

1.電腦應用與影響構面分析結果：

未達到顯著水準（P=.162），表示不同階級之空軍人員就資訊違規認知上，在電腦應用與影響方面無顯著差異。

2. 資訊教育訓練構面分析結果：

未達到顯著水準（P=.052），表示不同階級之空軍人員就資訊違規認知上，在資訊教育訓練方面無顯著差異。

3. 落實法規政策構面分析結果：

未達到顯著水準（P=.108），表示不同階級之空軍人員就資訊違規認知上，在落實法規政策方面無顯著差異。

分析結果：

經由獨立樣本 T 檢定，在顯著水準 0.05 的情況下，結果證實【研究假設 2-2：空軍人員階級之不同，在資訊違規認知上應有顯著之差異】，其研究假說不成立。

4.6.3 空軍人員教育程度之不同，在資訊違規認知上之差異情形

使用 One-way ANOVA 檢驗不同教育程度之空軍人員，在資訊違規認知及其各層面的影響，其分析結果如表 4.46 所示。

表 4.46　教育程度與資訊違規認知分析摘要表

構面	教育程度	樣本數	平均數	標準差	F 值	P 值
電腦應用與影響	高中	73	37.6818	4.5881	.268	.765
	專科	135	37.8815	5.5826		
	大學	231	37.3160	4.9465		
	整體	439	37.5215	5.0809		
資訊教育訓練	高中	73	42.5758	6.0993	.286	.751
	專科	135	43.4667	6.3326		
	大學	231	42.9375	5.7687		
	整體	439	43.0348	5.9686		
落實法規政策	高中	73	34.1364	4.5060	.808	.446
	專科	135	33.9259	5.0144		
	大學	231	33.6493	4.5576		
	整體	439	33.7914	4.6753		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4.46 得知，經由 One-way ANOVA 檢定，不同教育程度之空軍人員在資訊違規認知的相關因素分析中，以「教育程度」為自變項（因子），「資訊違規認知」各構面因素為依變項，在顯著水準 0.05 的情況下，結果分析如下：

1.電腦應用與影響構面分析結果：

未達到顯著水準（P=.765），表示不同教育程度之空軍人員就資訊違規認知上，在電腦應用與影響方面無顯著差異。

2. 資訊教育訓練構面分析結果：

未達到顯著水準（P=.751），表示不同教育程度之空軍人員就資訊違規認知上，在資訊教育訓練方面無顯著差異。

3. 落實法規政策構面分析結果：

未達到顯著水準（P=.446），表示不同教育程度之空軍人員就資訊違規認知上，在落實法規政策方面無顯著差異。

分析結果：

經由單因子變異數分析檢定，在顯著水準 0.05 的情況下，結果證實【研究假設 2-3：空軍人員教育程度之不同，在資訊違規認知上應有顯著之差異】，其研究假說不成立。

4.6.4 空軍人員初次學習電腦時間之不同，在資訊違規認知上之差異情形

使用 One-way ANOVA 檢驗初次學習電腦時間不同之空軍人員，在資訊違規認知及其各層面的影響，其分析結果如表 4.47.1-4.47.2 所示。

表 4.47.1 初次學習電腦時間與資訊違規認知分析摘要表

構面	工作單位	樣本數	平均數	標準差	F 值	P 值
電腦應用與影響	高中以前	203	37.2751	5.1744	1.208	.306
	專科以後	120	37.7160	5.1192		
	大學以後	70	37.8143	4.8133		
	工作以後	45	37.9412	5.0190		
	整體	438	37.5215	5.0809		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

表 4.47.2 初次學習電腦時間與資訊違規認知分析摘要表（續）

構面	工作單位	樣本數	平均數	標準差	F 值	P 值
資訊教育訓練	高中以前	203	42.8922	5.8596	1.421	.236
	專科以後	120	43.2099	5.8816		
	大學以後	70	43.3000	7.0718		
	工作以後	45	43.1618	5.3827		
	整體	438	43.0348	5.9686		
落實法規政策	高中以前	203	33.4015	4.8046	1.496	.215
	專科以後	120	34.2716	4.9143		
	大學以後	70	34.1714	4.1910		
	工作以後	45	34.3529	4.3081		
	整體	438	33.7914	4.6753		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4.47.1-4.47.2 得知，經由 One-way ANOVA 檢定，初次學習電腦時間不同之空軍人員在資訊違規認知的相關因素分析中，以「初次學習電腦時間」為自變項（因子），資訊違規認知各構面因素為依變項，進行 F 檢定，在顯著水準 0.05 的情況下，結果分析如下：

1.電腦應用與影響構面分析結果：

未達到顯著水準（P=.306），表示初次學習電腦時間不同之空軍人員就資訊違規認知上，在電腦應用與影響方面無顯著差異。

2. 資訊教育訓練構面分析結果：

未達到顯著水準（P=.236），表示初次學習電腦時間不同之空軍人員就資訊違規認知上，在資訊教育訓練方面無顯著差異。

3. 落實法規政策構面分析結果：

未達到顯著水準（P=.215），表示初次學習電腦時間不同之空軍人員就資訊違規認知上，在落實法規政策方面無顯著差異。

分析結果：

經由單因子變異數分析檢定，在顯著水準 0.05 的情況下，結果證實【研究假設 2-4：空軍人員初次學習電腦時間之不同，在資訊違規認知上應有顯著之差異】，其研究假說不成立。

4.6.5 空軍人員使用電腦時間之不同，在資訊違規認知上之差異情形

使用 One-way ANOVA 檢驗使用電腦時間不同之空軍人員，在資訊違規認知及其各層面的影響，其分析結果如表 4.48 所示。

表 4.48 使用電腦時間與資訊違規認知分析摘要表

構面	使用電腦時間	樣本數	平均數	標準差	F 值	P 值
電腦應用與影響	1 小時	6	3.2385	.6436	3.202*	.013
	1-3 小時	26	3.1355	.5958		
	3-6 小時	68	3.1500	.7566		
	6-9 小時	86	3.2244	.9534		
	9 小時以上	253	3.4915	1.0065		
	整體	439	3.3691	.9465		
資訊教育訓練	1 小時	6	4.1868	.5196	.488	.745
	1-3 小時	26	4.1014	.5915		
	3-6 小時	68	4.2511	.5807		
	6-9 小時	86	4.2392	.6738		
	9 小時以上	253	4.2667	.6681		
	整體	439	4.2472	.6488		
落實法規政策	1 小時	6	4.2981	.4802	.707	.588
	1-3 小時	26	4.2379	.5695		
	3-6 小時	68	4.3617	.6225		
	6-9 小時	86	4.4230	.5826		
	9 小時以上	253	4.3200	.6389		
	整體	439	4.3379	.6187		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4.48 得知，經由 One-way ANOVA 檢定，使用電腦時間不同之國軍人員在資訊違規認知的相關因素分析中，以「使用電腦時間」為自變項（因子），資訊違規認知各構面因素為依變項，進行 F 檢定，在顯著水準 0.05 的情況下，結果分析如下：

1.電腦應用與影響構面分析結果：

達到顯著水準（P=.013），表示使用電腦時間不同之空軍人員就資訊違規認知上，

在電腦應用與影響方面有顯著差異。

2. 資訊教育訓練構面分析結果：

未達到顯著水準（P=.745），表示使用電腦時間不同之空軍人員就資訊違規認知上，在資訊教育訓練方面無顯著差異。

3. 落實法規政策構面分析結果：

未達到顯著水準（P=.588），表示使用電腦時間不同之空軍人員就資訊違規認知上，在落實法規政策方面無顯著差異。

分析結果：

經由單因子變異數分析檢定，在顯著水準 0.05 的情況下，結果証實【研究假設 2-5：空軍人員使用電腦時間之不同，在資訊違規認知上應有顯著之差異，其研究假說部份成立】。當變異數分析，顯示達顯著水準時，表示其可能有顯著差異存在，故再進行事後比較（Post Hoc comparison），各構面因素多重比較 Scheffe 檢定結果均無顯著差異。

4.6.6 空軍人員工作單位之不同，在資訊違規認知上之差異情形

使用 One-way ANOVA 檢驗不同工作單位之空軍人員，在資訊違規認知及其各層面的影響，其分析結果如表 4.49 所示。

表 4.49　工作單位與資訊違規認知分析摘要表

構面	工作單位	樣本數	平均數	標準差	F 值	P 值
電腦應用與影響	教學單位	80	37.4727	4.6545	5.134*	.002
	訓練單位	175	37.2585	5.4805		
	部隊單位	184	37.3030	5.1596		
	整體	439	37.5215	5.0809		
資訊教育訓練	教學單位	80	42.2818	5.8390	5.555*	.001
	訓練單位	175	42.5512	6.1893		
	部隊單位	184	43.8182	5.9733		
	整體	439	43.0348	5.9686		

落實法規政策	教學單位	80	33.5182	4.6130	1.516	.210
	訓練單位	175	33.5220	4.8835		
	部隊單位	184	33.5758	4.7425		
	整體	439	33.7914	4.6753		

資料來源：本研究整理　註：*：P<0.05　**：P<0.01

由表 4. 49 得知，經由 One-way ANOVA 檢定，不同工作單位之空軍人員在資訊違規認知的相關因素分析中，以「工作單位」為自變項（因子），資訊違規認知各構面因素為依變項，進行 F 檢定，在顯著水準 0.05 的情況下，結果分析如下：

1.電腦應用與影響構面分析結果：

達到顯著水準（P=.002），表示工作單位不同之空軍人員就資訊違規認知上，在電腦應用與影響方面有顯著差異。

2. 資訊教育訓練構面分析結果：

達到顯著水準（P=.001），表示工作單位不同之空軍人員就資訊違規認知上，在資訊教育訓練方面有顯著差異。

3. 落實法規政策構面分析結果：

未達到顯著水準（P=.210），表示工作單位不同之空軍人員就資訊違規認知上，在落實法規政策方面無顯著差異。

分析結果：

經由單因子變異數分析檢定，在顯著水準 0.05 的情況下，結果證實【研究假設 2-6：空軍人員工作單位之不同，在資訊違規認知上應有顯著之差異】，其研究假說部份成立。當變異數分析，顯示達顯著水準時，表示其可能有顯著差異存在，故再進行事後比較（Post Hoc comparison），各構面因素多重比較 Scheffe 檢定結果茲分述說明如下：

1. 在「電腦應用與影響」方面：

部隊單位與訓練單位及教學單位做比較，其平均差異值為正數（.5141 及.4365），達顯著水準（.004 及.008），顯示部隊單位相較於訓練單位及教學單位，在電腦應

用與影響方面有較高的認知。

2. 在「資訊教育訓練」方面：

部隊單位與訓練單位、教學單位做比較，其平均差異值為正數（.3551、.3207 及 .2891），達顯著水準（.004、.003 及.034），顯示部隊單位相較於其它單位，在資訊教育訓練方面有較高的認知。

3. 在「落實法規政策」方面：

由 Scheffe 檢定分析結果均無顯著差異。

4.6.7 空軍人員背景與資訊違規認知關係研究結果

綜合以上分析結果，本研究將空軍人員背景與資訊違規認知差異性檢定結果彙整如表 4.50。

表 4.50　空軍人員背景與資訊違規認知差異性檢定彙整表

構面	年齡	階級	教育程度	初次學習電腦時間	使用電腦時間	工作單位
電腦應用與影響	T=.148**	T=1.400	F=.268	F=1.208	F=3.202*	F=5.134*
	P=.000	P=.162	P=.765	P=.306	P=.013	P=.002
資訊教育訓練	T=3.670**	T =1.948	F=.286	F=1.421	F=.488	F=5.555*
	P=.000	P=.052	P=.751	P=.236	P=.745	P=.001
落實法規政策	T=1.378	T =2.374	F=.808	F=1.496	F=.707	F=1.516
	P=.169	P=.018	P=.446	P=.215	P=.588	P=.210

資料來源：本研究整理　*：P<0.05　**：P<0.01

由表 4.50 分析結果得知：

1. 年齡方面，對於空軍人員之資訊違規認知，在電腦應用與影響與資訊教育訓練構面有顯著差異。

2. 階級方面，對於空軍人員之資訊違規認知無顯著差異。

3. 教育程度方面，對於空軍人員之資訊違規認知無顯著差異。

4. 初次學習電腦時間方面，對於空軍人員之資訊違規認知無顯著差異。

5. 使用電腦時間方面，在電腦應用與影響構面有顯著差異。

6. 工作單位方面，對於空軍人員之資訊違規認知，在電腦應用與影響及資訊教育訓練構面有顯著差異。

4.7 空軍人員資訊安全素養與資訊違規認知關係之分析

本節以皮爾遜積差相關分析方法，檢定資訊安全素養與資訊違規認知兩者各構面間之關聯性。邱皓政（2000）指出，相關係數（Coefficient of Correlation）值是用以檢驗兩個變項線性關係之統計技術。由於相關係數為一標準化分數，其值不受變項特性之影響，介於-1 與+1 之間。相關係數值越接近正負 1 時，表示變項的關聯情形越明顯。1.00 或-1.00 之相關係數稱為完全正（負）相關，其相對應之意義如表 4.51 所示。

表 4.51 相關係數強度大小與其相對應之意義對照表

範圍	變項關聯程度
1.00	完全相關
0.70-0.99	高度相關
0.40-0.69	中度相關
0.10-0.39	低度相關
0.10 以下	微弱或無相關

4.7.1 空軍人員資訊安全素養與資訊違規認知之相關分析

針對空軍人員資訊安全素養與資訊違規認知層面的積差相關分析得知，兩者的相關係數為.770（顯著性為.000），以相關係數強度五分法標準來看，空軍人員資訊安全素養與資訊違規認知達高度顯著相關，同時驗証假設 3，顯示兩者間相互關係密切。

4.7.2 空軍人員資訊安全素養與資訊違規認知各構面之相關分析

經皮爾遜積差相關分析，空軍人員資訊安全素養與資訊違規認知各構面之相關係數為.439 到.786（顯著性均為.000），分析結果如表 4.52。

表 4.52 資訊安全素養與資訊違規認知各構面相關分析摘要表

構面		資訊違規認知			
		電腦應用與影響	資訊教育訓練	落實法規政策	整體
資訊安全素養	資訊安全知識	.570** (.000)	.768 ** (.000)	.439** (.000)	.674** (.000)
	資訊操作技能	.720** (.000)	.674** (.000)	.597** (.000)	.671** (.000)
	資訊安全倫理	.681** (.000)	.683** (.000)	.786** (.000)	.755** (.000)

資料來源：本研究整理 ** 在顯著水準為 0.01 時（雙尾），相關顯著。

由表 4.52 分析結果得知：

一、「資訊安全知識」與資訊違規認知整體層面積差相關值為.674，各構面的相關分析為.439到.768均呈顯著相關，因此，分析結果接受假說3-1。分述如下：

（1）資訊安全知識與電腦應用與影響之關係：兩者之相關係數為.570呈中度正相關。

（2）資訊安全知識與資訊教育訓練之關係：兩者之相關係數為.768呈高度正相關。

（3）資訊安全知識與落實法規政策之關係：兩者之相關係數為.439呈中度正相關。

二、「資訊操作技能」與資訊違規認知整體層面積差相關值為.671，各構面的相關分析為.674到.720均呈顯著相關，因此，分析結果接受假說3-2。分述如下：

（1）資訊操作技能與電腦應用與影響之關係：兩者之相關係數為.720呈高度正相關。

（2）資訊操作技能與資訊教育訓練之關係：兩者之相關係數為.674呈中度正相關。

（3）資訊操作技能與落實法規政策之關係：兩者之相關係數為.597呈中度正相關。

三、「資訊安全倫理」與資訊違規認知整體層面積差相關值為.755，各構面的相關分析為.681到.786均呈顯著相關，因此，分析結果接受假說3-3。分述如下：

（1）資訊安全倫理與電腦應用與影響之關係：兩者之相關係數為.681呈中度正相關。

（2）資訊安全倫理與資訊教育訓練之關係：兩者之相關係數為.683呈中度正相關。

（3）資訊安全倫理與落實法規政策之關係：兩者之相關係數為.786呈高度正相關。

4.8 小結

本節係根據以上檢定結果列表彙總整理，呈現顯著差異項目並加以說明。

一、空軍人員背景之不同，在資訊安全素養上應有顯著之差異，檢定結果整理如表4.53。

表4.53不同背景之資訊安全素養檢測結果

假說項目	假說內容	研究結果
假設1-1	空軍人員年齡之不同，在資訊安全素養上應有顯著之差異	成立
假設1-2	空軍人員階級之不同，在資訊安全素養上應有顯著之差異	不成立
假設1-3	空軍人員教育程度之不同，在資訊安全素養上應有顯著之差異	部分成立
假設1-4	空軍人員初次學習電腦時間之不同，在資訊安全素養上應有顯著之差異	不成立
假設1-5	空軍人員使用電腦時間之不同，在資訊安全素養上應有顯著之差異	不成立
假設1-6	空軍人員工作單位之不同，在資訊安全素養上應有顯著之差異	成立

資料來源：本研究整理

從4.5節研究數據分析，及空軍人員背景與資訊安全素養差異性檢定彙整表（表4.43）得知，空軍人員在不同的「階級」、「初次學習電腦時間」及「使用電腦時間」項目中，未達顯著差異；在不同的「教育程度」項目中，達部份顯著差異；在不同的「年齡」及「工作單位」達到顯著差異。

二、空軍人員背景之不同，在資訊違規認知上應有顯著之差異，其研究假說檢定結果整理如表4.54。

表4.54 不同背景之資訊違規認知各研究假說檢定結果

假說項目	假說內容	研究結果
假設2-1	空軍人員年齡之不同，在資訊違規認知上應有顯著之差異	部分成立
假設2-2	空軍人員階級之不同，在資訊違規認知上應有顯著之差異	不成立

假設2-3	空軍人員教育程度之不同，在資訊違規認知上應有顯著之差異	不成立
假設2-4	空軍人員初次學習電腦時間之不同，在資訊違規認知上應有顯著之差異	不成立
假設2-5	空軍人員使用電腦時間之不同，在資訊違規認知上應有顯著之差異	部分成立
假設2-6	空軍人員工作單位之不同，在資訊違規認知上應有顯著之差異	部分成立

資料來源：本研究整理

從4.6節研究數據分析，及空軍人員背景與資訊違規認知差異性檢定彙整表（表4.50）得知，空軍人員在不同的「階級」、「教育程度」及「初次學習電腦時間」項目中，未達顯著差異；在不同的「年齡」、「使用電腦時間」及「工作單位」項目中，達部份顯著差異。

三、空軍人員資訊安全素養之不同，在資訊違規認知上應有顯著之差異，檢定結果整理如表4.55。

表4.55 資訊安全素養與資訊違規認知相關性檢測結果

假說項目	假說內容	研究結果
假設3-1	空軍人員資訊安全知識之不同，在資訊違規認知上應有顯著之差異	成立
假設3-2	空軍人員電腦操作技能之不同，在資訊違規認知上應有顯著之差異	成立
假設3-3	空軍人員資訊倫理之不同，在資訊違規認知上應有顯著之差異	成立

資料來源：本研究整理

從4.7節研究數據分析，及資訊安全素養與資訊違規認知各構面相關分析摘要表（表4.52）得知，空軍人員資訊安全素養與資訊違規認知之「資訊安全知識」、「電腦操作技能」及「資訊倫理」各構面因素，均呈顯著相關，顯示空軍人員資訊安全素養之不同，在資訊違規認知上應有顯著之差異。

再經由多元迴歸分析，資訊倫理量表對資訊違規認知構面之迴歸分析方面，R平方為0.816，表示資訊違規對其平均值的變異，約有81.6%可以用資訊倫理的變異解釋，變異數檢定中，F檢定值為73.003，P=0.000<0.05，達顯著水準，表示資訊倫理迴

歸模式的效果顯著，標準化 Beta 值為正數，表示對資訊違規認知的影響是正向的，如表 4.56。

表4.56 資訊倫理量表對資訊違規認知之迴歸分析結果

自變數	R 平方	F 檢定	Beta	t 值
資訊倫理	0.816	73.003**	0.556	6.551**

依變數：資訊違規認知，**表示顯著水準P＜0.001

五、研究結論與建議

5.1 研究發現結論與建議

根據本研究發現，提出下列幾點結論與建議：

（1）空軍人員年齡之不同，在資訊安全素養上之差異比較結果，在資訊倫理構面分析有顯著差異，表示不同年齡之空軍人員，其在資訊利用的倫理議題上顯然有不一樣的價值觀。資訊安全的關鍵在於「人」、「制度」及「系統」，而資訊安全，人人有責，本人建議資訊相關部門應多加利用各項集會時機，加強不同年齡層對資訊法規之宣導，落實資通安全法制教育，進而提昇空軍人員資訊倫理素養。

（2）空軍人員工作單位之不同，在資訊安全素養上之差異比較結果，在「資訊安全知識」、「資訊操作技能」及「資訊倫理」等構面，均有顯著差異，顯然不同任務特性之空軍人員，其資訊安全之素養亦明顯不同。為貫徹國防部落實空軍各項資安政策指導，空軍各級單位均統一實施「空軍人員資安合格簽證」，藉由資安合格鑑測機制，使官、士、兵加強建立各資訊業務標準作業規範與工作認知。因此，本人建議資訊部門應同時配合辦理資訊安全教育課程，針對不同任務特性之空軍人員實施資安教育訓練，以提升其資訊作業能力與資訊安全素養。

（3）在資訊安全知識、電腦操作技能及資訊倫理等構面，以「資訊安全知識」的認知程度最高，而「電腦操作技能」的認知程度最低。顯示大部份空軍人員在電腦操作技能上，仍有待加強，因此空軍資訊相關部門應加強不同階層人員資訊作業能力之培養，避免因不閒電腦之操作，而產生資安事件，影響單位整體資訊作業安全。

（4）空軍人員資訊安全素養與資訊違規認知層面的積差相關分析得知，兩者達高度顯著相關，顯示兩者間關係密切且相互影響。研析國軍過去洩、違密案件中，不難發現，其主要原因多為官兵保密警覺性不足、法紀觀念淡薄及保密習性欠佳所致，唯有每一位官兵恪遵規定，資訊安全工作，方能有效運作。本人建議有效提升國軍人員資訊安全素養、強化「人」對「資訊安全素養」的認知及建立資訊安全

危機意識是刻不容緩的事，因為「人」是影響國軍資訊安全的核心，資訊安全的議題攸關國家存亡之事，成敗之間端繫於相關人員對資訊安全的認知是否落實。

（5）目前國軍資訊安全整備工作，係以貫徹資安管控機制作法、落實專碟專用及執行資安五蔬果為重點，相關部門若能建立資訊安全稽核量化作法，建立較專業、完善的稽查體制，提供資訊安全督導檢查及現況精進之參據，相信定能提高資訊違規事件查察成效，達到「零漏洞、零違紀、零缺失」之資訊安全作業要求，有效防範軍機外洩。

（6）資訊流量高度成長的時代，網路是彼此通連與交流的基本通路，資料安全隨著人們使用網路的頻繁而漸受重視，「E 化國軍」是我空軍積極倡導及推展的方向，因此，目前空軍單位每月均定期實施空軍人員資安合格鑑測，藉以提升空軍人員電腦基本操作能力，但並未訂定空軍人員資訊安全素養基本指標，如能明確將該指標一併納入，相信更能確保空軍人員資訊安全素養之提升。

（7）最後經由分析與研究結果發現，資訊倫理量表對資訊違規認知有顯著影響，顯示具有較高資訊倫理觀念的人員，較不易發生資訊違規事件。並提出一份空軍人員個人電腦資安自我督檢表如附錄 2 所示，藉此提供空軍人員、稽查單位擬定或修訂相關對策及後續研究之參考。

5.2 後續研究建議

1. 研究對象方面

礙於時間、人力及專業知識等因素考量，本研究難以從事大規模的研究，僅以空軍南部某軍事院校之現職人員為施測對象，建議未來的研究者可就不同地區之空軍人員進行調查，擴大調查的範圍，將其他軍種國軍人員加入探討，以求研究樣本數更具代表性。另外亦可分區進行個案比較性之探討，以研究各軍種間，國軍人員資訊安全素養現況及各構面之差異性。

2. 研究變項方面

不論政策面或實務上，其影響資訊安全之因素很多，未來的研究，可將更多相關

的變項或構面因素一併納入探討，針對量表內容的適切性作更進一步的研究與考量，以符合現行國軍資訊安全管制作法。

3.研究方法方面

本研究藉由問卷調查瞭解空軍人員資訊安全素養現況，及不同背景變項在資訊安全素養及資訊違規認知之差異性，僅能探討影響受試者行為與有關變項間之關係，或變項間的相關情形，較難了解空軍人員實際經驗或內心感受，故建議除量化資料蒐集外，應再輔以質性研究，例如將調查問卷加入建議事項、實地觀察或訪談等方式，採「質」與「量」相互印證比較，使研究結果更適切周延。

4.橫斷面與縱斷面研究並重

以研究時間點來看，本研究屬於橫斷面（cross-sectional）的研究方式，對於研究變項隨時間的變化（如工作環境變動、職缺任務的調整、人員受訓進修）等，未能長時間加以探究，後續研究者可以針對此方向從事跨時間點縱斷面研究（longitudinal study）。

參考文獻

中文部份

[1] E 網無涯，2009，http://pop3.tsjh.tpc.edu.tw/~ts-c/moral/crime.htm，淡水國中，1 月。

[2] 資策會 ACI-IDEA-FIND/經濟部工業局“電信平台應用發展推動計畫”：http://www.find.org.tw/find/home.aspx?page=many&id=133

[3] 日內瓦的世界經濟論壇，2009，“2007-2008 年全球資訊科技報告”，國科會國際合作簡訊網：http://stn.nsc.gov.tw/ view_detail.asp?doc_uid=0950412002&kind_no=A06，4 月。

[4] 文宣組，2006，“維護軍機防制洩密、保密安全你我有責”，忠誠報，國防部陸軍司令部，2 月 27 日。

[5] 台灣網路資訊中心，2009，“台灣寬頻網路使用狀況調查摘要分析”，http://stat.twnic.net.tw。

[6] 江高飛等編著，2002，計算機概論，志凌資訊，台北。

[7] 李志文，2003，“落實企業資安工作”，資訊與電腦，272 期，83 頁，3 月。

[8] 李堅萍，1994，國民中學科技素養教育課程現況之研究，國立台灣師範大學，教育研究所碩士論文。

[9] 李德竹、盧秀蘭，1994，由資訊素養研究圖書館資訊服務之意義與內涵，國科會專案研究計畫書，國立台灣大學，圖書館學系暨研究所。

[10]吳正己、邱貴發，1996，“資訊社國民的電腦素養教育”，社教雙月刊。

[11]林東茂，1996，危險與經濟刑法，五南圖書出版公司，台北。

[12]林宜隆，1998，“網路使用犯罪問題與防範對策之探討”，第三屆資訊管理學術暨警政資訊實務研討會，警察大學，5 月。

[13]林宜隆，1998，“網路使用犯罪問題與網路安全管理之探討”，中央警察大學學報，32 期，3 月。

[14]林宜隆，2000，“網路犯罪之案例分析”，中央警察大學學報，37 期，9 月。

[15]林宜隆，2000，“網際網路與犯罪問題之研究”，2 版，中央警察大學，桃園。

[16]林山田，1984，“電腦犯罪之研究”，政大法學評論，30 卷，頁 46-66。

[17]美國圖書館學會(American Library Association，簡稱 ALA)，1989，“美國圖書館學會資訊素養委員會總結報告書”。

[18]邱皓政，2000，量化研究與統計分析：SPSS 中文視窗版資料分析範例解析，五南出版社，台北。

[19]胡立人，張源滑，黃克東，1977，數字化中文字彙，系統出版社，台北。

[20]翁錳揮，2006，“資訊管理暨通資安全成效檢討與策進”，陸軍 94 年學用會報研討會，陸軍司令部，1 月。

[21]翁錳揮，2006，“當前通資安全政策指導”，陸軍 95 年度通資安全巡迴講習資料，陸軍司令部，頁 2，3 月 21 日。

[22]國防部陸軍總部，2004，個人電腦資訊安全防護作業規定，國防部陸軍總部，桃園。

[23]國防部陸軍總部，2004，國軍通資安全常見違規事件暨應行注意事項，國防部陸軍總部，桃園。

[24]國防部陸軍總部，2004，CERT 電腦緊急應變實施計劃，國防部陸軍總部，桃園。

[25]國防部陸軍總部，2004，資訊網路安全監測作業規定，國防部陸軍總部，桃園。

[26]國防部陸軍總部，2005，個人電腦輸出入裝置使用管制規定，國防部陸軍總部，桃園。

[27]國防部陸軍總部，2006，資訊設備及資訊儲存媒體管制規定，國防部陸軍總部，桃園。

[28]國防部陸軍總部，2006，修訂通資業務手冊密碼選取規則，國防部陸軍總部，桃園。

[29]國防部陸軍總部，2006，漢光ＯＯ號演習通資安全監察維護實施規定，國防部陸軍總部，桃園。

[30]國防部陸軍總部，2006，網路實體隔離及資訊設備庫存管理觀摩實施計畫，國防部陸軍總部，桃園。

[31]國家資通安全會報技術服務中心（ICST），2005，“由資安案例談資安防護”，9月。

[32]國防部總政治作戰局，2005，國軍人員違犯保密規定行政懲處標準表，國防部總政治作戰局，台北。

[33]黃毓怡，2006，“93-94 年警政署網路犯罪發破數統計調查”，內政部警政署服務信箱(電腦編號：951Z001871），4 月 13 日。

[34]黃世雄，1996，“資訊素養與圖書館使用教育”，高中圖書館館訊，14 期，頁 12-16。

[35]黃世銘、謝名冠，2001，“網路行為規範之研究”，台灣台北地方法院檢察署八十九年度研究報告，台灣台北地方法院檢察署印行。

[36]許瑩琪，2004，“加強資訊安全之具體作為”，陸軍總部 93 年度通資安全巡迴講習，陸軍司令部，頁 10，3 月 15 日。

[37]陳伯榆，2001，“Code Red 從癱瘓學術網路看校園網路主機管理問題”，台灣區學術網路研討會暨網路學習與繼續專業教育國際會議，10 月 24 日。

[38]陳雪華，1996，“網路資源與圖書館利用教育”，教學科技與媒體，25 期，頁 3-12。

[39]郭麗玲，1999，“學習社會中讀者終身學習的內容”，中國圖書館學會會報，61 期，頁 147-159，中國圖書館學會。

[40]張盛益、許美玲等譯，1995，“電腦安全的威脅與對策”，資訊工業策進會，簡介頁。

[41]馮震宇、劉志豪，1998，“我國網路犯罪類型及案例探討”，月旦法學雜誌，41 期，10 月。

[42]經濟部工業局，2009，“電信平台應用發展推動計畫”，資策會 ACI-IDEA-FIND：http://www.find.org.tw/find/home.aspx? page= many&id=133，5 月 20 日。

[43]楊境恩，2004，國內警察人員資訊安全素養對資訊犯罪偵查能力影響之研究，樹德科技大學，資訊管理研究所碩士論文。

[44]楊美華，1999，“由多元入學方案談圖書館資訊之運用”，全國高中圖書館主任業務研討會會議資料，頁 45-51，台北。

[45]葛樹人，1987，心理測驗學，桂冠出版社，台北。

[46]劉淑娟，1998，我國公共圖書館技術服務館員資訊素養之研究，淡江大學，碩士論文，6 月。

[47]魏令芳，2002，大學資訊素養之研究，國立台灣師範大學，圖書資訊學研究所碩士論文。

[48]警政署，2009，http://www.internet-recordor.com.tw/crime.html。

[49]蘇諼，1997，“談資訊素養與使用者導向的圖書館服務”，輔仁學誌—文學院之部，26 期，頁 152-153 ，6 月。

英文部份

[50]Behrens, Shirley J., 1994, A Conceptual Analysis and Historical Overview of Information Literacy, College and Research Libraries 55 : 4, pp.302-309.

[51] Caissy, Gail A. , 1992, “Curriculum for the Information Age Learning connections: Guidelines for media and technology programs. ” North Carolina Department of Public Instruction. Bob Etheridge, State Superintendent, pp.1.

[52] Doyle, Christina S.,1992, “Outcome measures for information literacy within the National educational Goals of 1990”, Final report to national forum on Information literacy, Summary of findings .

[53] Jelinek, F., 1968, Probabilistic information Theory, McGraw-Hill, New York.

[54] Karen, D.L., Houston, H.C., and Mellerrill, E.W., 1992, “Threates to

Information Systems: Today's Reality, Yesterday's Understanding.", MIS Quarterly, pp.173-186,.

[55] Luke, A.,1992, "Read and Critical literacy : Redefining the Great Debate.",ERIC ED345211.

[56] Luehrmann, Authur. , 1981, "Computer literacy-what should it be? Mathematics Teacher", 74(9), pp.682-686.

[57] McClure, C. R., 1994, "Network literacy: A role of libraries?", Information Technology and Libraries, 13(2), pp.117-118.

[58] Malisow Ben, 2004, "Valuing Secure Access to Personal Information.", http://www.securityfocus.com/infocus/1797, visited on 2006/6/8.

[59]Nunally J. C. , 1978, Psychometric Theory, New York: McGraw Hill.

[60] Parker, D. B., "Fighting Computer Crime.",Wiley Computer Publishing. pp.72,1998.

[61] Smith, M., 1989, "Computer Security-Threats, Vulnerabilities and Countermeasures", formation Age, UK, pp.205-210.

[62] Simson, G., and Gene, S., 1991, Practical UNIX Security, O, Reilly & Associates ,Inc.

[63]Shelly, G. B., Cashman, T.J., & Waggoner, G. A.,1996,Using computers: A gateway to information, Danvers, MA: Boyd & Fraser publishing company .

[64] Steven, J.,1992, Applied multivariate statistics for the social sciences (2nd ed.),New Jersey: Lawrence Erlbaum Associates, Hillsdale.

親愛的軍中同仁您好：

這是一份關於「空軍人員資訊安全素養」之研究，想請教您一些關於資訊安全的問題。問卷中您所回答之問題將成為本研究分析空軍人員資訊安全素養之重要資訊，有您寶貴的意見將使本研究更有其價值感與實質的意義。竭誠的感謝您！，謝謝您的協助，敬祝平安快樂！

台東大學環境經濟與資訊管理研究所
指導教授：謝昆霖 博士
研 究 生：鄭宇凱
E-mail：RS0923@hotmail.com

第一部分：基本資料

構　　面	題　　項
基本資料變　　項	1、年齡：□20 歲以下□21-29 歲□30-39 歲□40-49 歲□50 歲以上
	2、階級：□士兵□士官□尉級軍官□校級軍官□聘雇人員
	3、教育程度：□高中□專科□大學□研究所（含以上）
	4、初次學習電腦課程是何時： □高中以前□專科□大學□研究所□服役（工作）後□尚未學過
	5、平均每週使用電腦時數： □1 小時內□1-3 小時□3-6 小時□3-9 小時□9 小時以上
	6、工作單位：□幕僚單位□教學單位□訓練單位□部隊單位

第二部分：資訊安全知識量表

說明：每個題項均分為「非常同意」、「同意」、「普通」、「不同意」、「非常不同意」等五個選項。請就您的了解勾選最適的答案。

	非常同意	同意	普通	不同意	非常不同意
衡量題項	選項				
1. 我了解電腦密碼設定須符合複雜性原則(應含英文、數字及特殊符號至少8碼以上)。	□	□	□	□	□
2. 我了解電腦密碼，不可使用個人或眷屬生日、身分證字號、單位代號或有意義之英文字等來當作密碼。	□	□	□	□	□
3. 我了解設定好的電腦密碼，每季至少應更換乙次。	□	□	□	□	□
4. 我了解電腦應安裝最新「病毒碼」及「漏洞修補	□	□	□	□	□

程式」。					
5. 我了解不可以將密碼寫在電腦設備上，或告訴無關人員，以確保資料及系統安全。	□	□	□	□	□
6. 我了解電腦不可任意開啟「資源分享」功能，以防電腦遭受病毒感染。	□	□	□	□	□
7. 我了解發現不明來源之電子郵件，不可開啟郵件並應直接刪除。	□	□	□	□	□
8. 我了解應養成良好的習慣，不使用來歷不明的儲存媒體。	□	□	□	□	□
9. 我了解瀏覽色情網頁易遭電腦病毒或惡意程式感染。	□	□	□	□	□

第三部分：電腦操作技能量表

說明：每個題項均分為「非常同意」、「同意」、「普通」、「不同意」、「非常不同意」等五個選項。請就您的了解勾選最適的答案。

	非常同意	同意	普通	不同意	非常不同意
衡量題項	選項				
1. 我有能力在公務電腦上安裝「國軍網路偵測軟體（軍民網監控軟體）」。	□	□	□	□	□
2. 我有能力在公務電腦上設定「國軍保密警語畫面」及「國軍螢幕保護程式」。	□	□	□	□	□
3. 我有能力將重要公務資料，以「國軍檔案加解密軟體」設定加解密。	□	□	□	□	□
4. 我有能力安裝防毒軟體、更新病毒碼、漏洞修補程式及執行系統掃描。	□	□	□	□	□
5. 使用外來儲存媒體時，我知道如何執行病毒掃描。	□	□	□	□	□
6. 我有能力安裝「國軍個人防火牆（BlackIce）」軟體，用以監測防阻不當網路入侵。	□	□	□	□	□
7. 當我的電腦感染病毒時，我有能力執行網路中斷，以避免造成大規模傳染。	□	□	□	□	□
8. 我有能力將電腦上重要資料加密儲存及備份。	□	□	□	□	□
9. 我有能力適時下載執行新病毒的清除工具，以維持系統正常運作。	□	□	□	□	□

第四部分：資訊倫理量表

說明：每個題項均分為「非常同意」、「同意」、「普通」、「不同意」、「非常不同意」等五個選項。請就您的了解勾選最適的答案。

	非常同意	同意	普通	不同意	非常不同意
衡量題項	選項				
1. 我了解不可任意安裝或使用非法軟體。	□	□	□	□	□
2. 我了解不可在網路上散播違反善良風氣之暴力、色情等不當資訊。	□	□	□	□	□
3. 我了解未經過合法授權，任意下載及轉寄(載)別人的著作，須同時受到民事及刑事的處罰。	□	□	□	□	□
4. 我了解不可在網路上散播電腦病毒或惡意程式。	□	□	□	□	□
5. 我了解使用具著作權的資訊時，應註明出處或徵得原作者的同意。	□	□	□	□	□
6. 我了解應避免在網路公共討論區，指名道姓討論私人事務。	□	□	□	□	□
7. 我了解未經查證或可疑的網路消息，不應再經由網路傳播出去。	□	□	□	□	□
8. 我了解未經當事人同意，不應隨便將個人資料傳送給第三者	□	□	□	□	□
9. 我了解不可隨意破解他人設定的電腦密碼。	□	□	□	□	□
10. 我了解沒有經過合法授權，就把別人的著作放在網路上讓網友分享利用，那是一種不尊重著作權的網路盜版行為。	□	□	□	□	□
11. 我了解在網路上公布軟體序號供別人使用，是種不合法的網路侵權行為。	□	□	□	□	□

第五部分：電腦應用與影響量表

說明：每個題項均分為「非常同意」、「同意」、「普通」、「不同意」、「非常不同意」等五個選項。請就您的了解勾選最適的答案。

	非常同意	同意	普通	不同意	非常不同意
衡量題項	選項				
1. 我了解全球資訊網站不可放置公務機敏資料，以防軍機外洩	□	□	□	□	□
2. 我了解應用加解密技術，可以確保檔案傳輸的安全性。	□	□	□	□	□
3. 我了解單位內必須做好資訊安全事件的通報機制，才能減少資安事件發生。	□	□	□	□	□

4. 我了解經核准攜入營區之私人電腦及週邊設備應與辦公場所隔離，且不可混用。	□	□	□	□	□
5. 我了解單位內連接「網際網路」之電腦，須指定專人管制及將連線紀錄備查。	□	□	□	□	□
6. 我了解因公務需要使用資訊儲存媒體，應由資訊部門專責採購、管制及分發。	□	□	□	□	□
7. 我了解單位購置之「資訊設備」及「儲存媒體」，應集中保管，以防止遺失或任意運用。	□	□	□	□	□
8. 我了解電腦主機明顯處加貼「保密警語標籤」，並於機殼接合處粘貼「專用易碎標籤」，以防遭到破壞。	□	□	□	□	□
9. 我了解資訊安全檢查，能有效發掘潛在問題，使官兵隨時養成良好保密習性。	□	□	□	□	□

第六部分：人員教育訓練量表

說明：每個題項均分為「非常同意」、「同意」、「普通」、「不同意」、「非常不同意」等五個選項。請就您的了解勾選最適的答案。

	非常同意	同意	普通	不同意	非常不同意
衡量題項	選項				
1. 我了解單位為做好資訊安全管理，必須要強調人員管理及資訊教育訓練。	□	□	□	□	□
2. 我了解定期接受資訊安全教育訓練，能有效降低及防範資訊違規事件發生。	□	□	□	□	□
3. 我了解資訊安全事項之宣導，能有效預防資訊系統遭受損害	□	□	□	□	□
4. 我了解電腦系統有中毒或異常現象，應即時通報系統管理者處置，以避免造成系統癱瘓。	□	□	□	□	□
5. 我了解落實「軍民網路實體隔離」政策，能有效避免軍機外洩事件發生。	□	□	□	□	□
6. 我了解個人未經核准，不得私設網站或提供各項網路資源服務。	□	□	□	□	□
7. 我了解資訊設備、媒體，應向保管人員辦理借用手續，才可使用。	□	□	□	□	□
8. 我了解資訊作業人員應定期接受安全查核，才可執行相關業務。	□	□	□	□	□

第七部分：落實法規政策量表

說明：每個題項均分為「非常同意」、「同意」、「普通」、「不同意」、「非常不同意」等五個選項。請就您的了解勾選最適的答案。

	非常同意	同意	普通	不同意	非常不同意
衡量題項	選項				
1.我了解各類型網路（國軍網路、戰情網路、情報與網際網路）均不得跨接混用。	□	□	□	□	□
2.我了解屬於「密」級公務資料，須使用「國軍檔案加解密軟體」加密後才能在軍網上傳送。	□	□	□	□	□
3.我了解不可將私人電腦及儲存媒體攜入營區使用。	□	□	□	□	□
4.我了解電腦必須由單位保管人員收回系統管理者權限，以防遭他人安裝不當或非法軟體。	□	□	□	□	□
5.我了解公務電腦必須設定輸出限制(關閉USB埠、光碟機、軟碟機等功能)，根絕輸出(入)源。	□	□	□	□	□
6.我了解違反「網路實體隔離規定」將受「記大過並調職」之嚴厲處份。	□	□	□	□	□
7.我了解違犯保密規定，其內容經查雖非屬國防機密資訊，但仍有影響保密軍紀或軍譽者，仍須受到處份。	□	□	□	□	□
8.我了解連接「網際網路」電腦，嚴禁用於處理單位公務資料	□	□	□	□	□
9.我了解電腦業管人員離職或調職時，應先知會資訊部門撤換帳號、通行碼。	□	□	□	□	□
10.我了解國軍人員違犯保密規定除當事人外，直屬一、二級主官（管）及該單保密軍官者應受連帶處份。	□	□	□	□	□
11.我了解國軍人員因處理電腦資訊不當，如損及第三人權利等情事者，將依「刑法」、「陸海空軍刑法」、「電腦處理個人資料保護法」等相關法律偵辦。	□	□	□	□	□

問卷到此結束，謝謝您熱心的協助!

空軍人員個人電腦資安自我督檢表

附錄二

項次	督檢要項	執行情形		備考
部頒資安規定	資訊資產是否貼有識別標示?(演訓紅色、軍網綠色、民網黃色)	□是	□否	
	電腦是否依規定安裝資安管控軟體?	□是	□否	
	電腦是否全面安裝國軍加解密軟體?	□是	□否	
	USB、筆記型電腦是否依規定律定副主官或保密軍官保管?	□是	□否	
	電腦是否全面拆除燒錄器、軟碟機?	□是	□否	
實體隔離暨資料交換	各辦公處所是否繪製電腦配置圖?	□是	□否	
	檢查軍民網路是否有搭接、混用或誤差情事?	□是	□否	
	民網是否張貼黃色識別標籤並使用黃色網路線?	□是	□否	
	民網是否嚴禁儲存、處理公務資料?	□是	□否	
	民網地點是否遵守公開設置、集中收容原則?	□是	□否	
	是否建置資料交換檢疫區?	□是	□否	
	軍民網資料交換是否經權責長官核定?	□是	□否	
	是否建立網際網路使用管制登記簿?	□是	□否	
	USB 是否專碟專用?(演訓紅色、軍網綠色、民網黃色)	□是	□否	
	是否建立 USB、筆記型電腦借出/歸回管制登記簿?	□是	□否	
	USB 及筆記型電腦使用完畢是否將資料刪除?	□是	□否	
資通安全教育	是否定期實施資安教育訓練?	□是	□否	
	資安教育訓練未到人員是否實施補課?	□是	□否	
	人員是否瞭解資安須知卡內容及收視資安管控宣導短片?	□是	□否	
	人員是否瞭解違反資安作業懲處規定?	□是	□否	
	人員是否瞭解嚴禁公務家辦、無線上網、嚴禁使用照相手機等規定?	□是	□否	
	新進人員是否依規定實施 2 小時資安訓練?	□是	□否	
安全稽核	有無策頒年度資安稽核實施計畫及辦理評比?	□有	□無	
	有無實施無預警資安稽核?	□有	□無	
	資安稽核所見缺失是否發布並懲處失職人員?	□是	□否	

	稽核缺失有無實施複查作業?	□有	□無	
資訊資產	是否定期或不定期執行資訊資產清點暨檢查?	□是	□否	
	是否建立單位資訊設備帳籍資料?	□是	□否	
	資訊設備新購、汰除是否依據部頒配賦基準辦理?	□是	□否	
	各項資訊設備是否明確律定管理者與使用者權限?	□是	□否	