警政資通安全現況分析及管理政策之研究

Analysis of present situation and study on Policy of Police Information Security Management System in Taiwan

王俊雄
內政部警政署專員
secudet@npa.gov.tw
林宜隆
中央警察大學資管所教授
paul@sun4.cpu.edu.tw

摘 要

本研究經由蒐集 ISO/IEC 17799:2000(BS7799 PART I)等國際資通安全規範及警政資通安全管理規定等文獻，並以「文獻資料分析法」交叉比對、分析，比較現行警察資通安全管理規定與 ISO/IEC 17799:2000(BS7799 PART I)等國際資通安全規範之異同及缺失，再以「問卷調查法」測量各級警察機關資通安全設備、電腦及網路使用情形、資通安全管理、資通安全觀念及資通安全事故發生情形等警察資通安全現況，發現警政資通系統存在「警察資通組織不佳」、「資通安全設備不足」、「電腦及網路使用待推廣」、「警察資通安全現況堪虞」、「資通安全管理欠落實」、「資通安全觀念待宣導」及「警察資通安全規範待修訂」等缺失，並提出「遵循警察任務需求，明訂政策分段執行」、「健全警察資通組織，強化資通安全編組」、「確認資產風險評估，定期清查分類標示」、「辦理人員忠誠考核，落實訓練追蹤督考」、「控制資通設備環境，防護資通設備安全」、「確保通訊安全快速，提昇資訊網絡安全」、「使用技術協助管理，存取控制嚴格便利」、「運用安全科技產品，支援維護系統安全」、「律定危機處理程序，持續演練檢討修正」、「嚴禁違反法規命令，獨立內部稽核偵防」等警政資通安全管理政策芻議。

關鍵詞：資通安全、警政資訊、ISO17799-1:2000、BS7799

Abstract

In this paper, we use the method of literature review to collect many documents like ISO/IEC 17799:2000 (BS7799PART I) and the regulations of police information security management system in Taiwan and compare the difference between them in order to find the faults of police information security management system in Taiwan..

Basing on the differences and faults, we use the method of survey research to measure the present situation of police information security management system in Taiwan. According to the analysis of those answers of survey, there are six main problems such as bad information security organization, not enough information security equipment, few information security training for policemen, dangerous present situation of information security, not workable information security management system, mistaken information security concepts, simpler regulations. Final, we propose ten policies for police information security management system to solve the problems.

Keywords: information security, police information system, ISO/IEC 17799:2000, BS7799

1.前言

1.1 研究動機與目的

在資通安全領域中，有效的安全管理模式向為專家學者研究之重心之一，尤其在 BS7799 及 ISO17799：2000 等國際資通安全規範通過，並廣為各界接受後，資訊安全管理更受到實務單位之重視，我國警察組織龐大，員警人數眾多，分布區域遍布全國各角落，經手之勤業務頗為繁雜，且與人民權益關係密切，對於所保管相關資訊之安全頗值特別重視，警政單位電腦資料外洩(合法取得、非法使用)、刑事警察局淹水案等資通安全事故，不僅損及政府之威信，更嚴重損害人民之權利，亦證明警察資訊安全管理之機制尚有改進之空間，本研究乃期望檢討警察資通安全管理之現況缺失，並參考國際資通安全規範內容，研擬警政資通安全管理政策，以供實務單位參考，本研究之目的分述如下：

1. 比較現行警察資通安全管理規定與 ISO/IEC 17799:2000(BS7799 PART I)等國際資通安全規範之異同及缺失。
2. 調查警察資通安全現況及缺失。
3. 綜合前述分析，研擬「警政資通安全管理政策」。

1.2.研究範圍

資通安全範疇可略分為技術面及管理面，舉凡密碼學演算法之設計、改良、創新，或是防毒軟體、入侵偵測系統、防火牆等軟硬體設備之推陳出新，或是國際資通安全規範之研究訂定等構面，均是專家、學者或業界研究之重點，相關研究主題既深且廣，難以兼容並顧，本研究之主題為「警政資通安全管理政策」，研究範圍分述如下：

1.2.1 以管理面為主，技術面為輔

本研究以資通安全政策、組織、資產、人員、環境、危機及法治等管理面為主，並以 ISO/IEC 17799:2000(BS7799 PART I)為探討依據，有關通訊作業、存取控制、系統維護等技術層面，則僅就相關部分說明，未能深入探討。

1.2.2 以政策面為主，執行面為輔

本研究以探討警政資通安全管理政策為主，尤其將探討重點置於高階政策(High Level Policy)，再佐以低階政策(Low Level Policy)說明，有關執行程序、計畫或細部執行規定等執行層面，限於篇幅無法探討。

1.2.3 以 ISO/IEC 17799:2000(BS7799 PART I)為探討主軸

國際資通安全管理規範因適用對象不同，而紛由不同國際組織訂定後頒行，其規範之重點亦因需求不同而有所差異，例如金融機構的稽核作業，多遵循 COBIT 之規定，本研究以 ISO/IEC 17799:2000(BS7799 PART I)的十大控制項目、三十六個控制目標及一二七項控制方法為探討主軸，其他國際規範或有類以規定，限於研究期程及經費，難以全部加以討論。

1.3 研究方法

1.3.1 文獻資料分析法[1]

本研究採用「文獻資料分析法」，以蒐集國際資通訊安全規範、我國資通安全管理政策及警政資通安全管理規定等相關之中外書籍、期刊、論文及網際網路等文獻資料，深入研究、歸納、比較及分析。

1.3.2 問卷調查法[2]

本研究以「問卷調查法」，根據「內政部警政署電子計算機作業保密安全實施規定」之資通安全規定內容，擬定問卷二頁四十六題，對全國各警察機關各級警察同仁及在中央警察大學二技、警察專科學校進修班進修之現職員警，隨機抽樣調查，期望能測量出各級警察機關資通安全設備、電腦及網路使用情形、資通安全管理、資通安全觀念及資通安全事故發生情形等警察資通安全現況。

1.4 研究流程

本研究研究流程如圖 1。

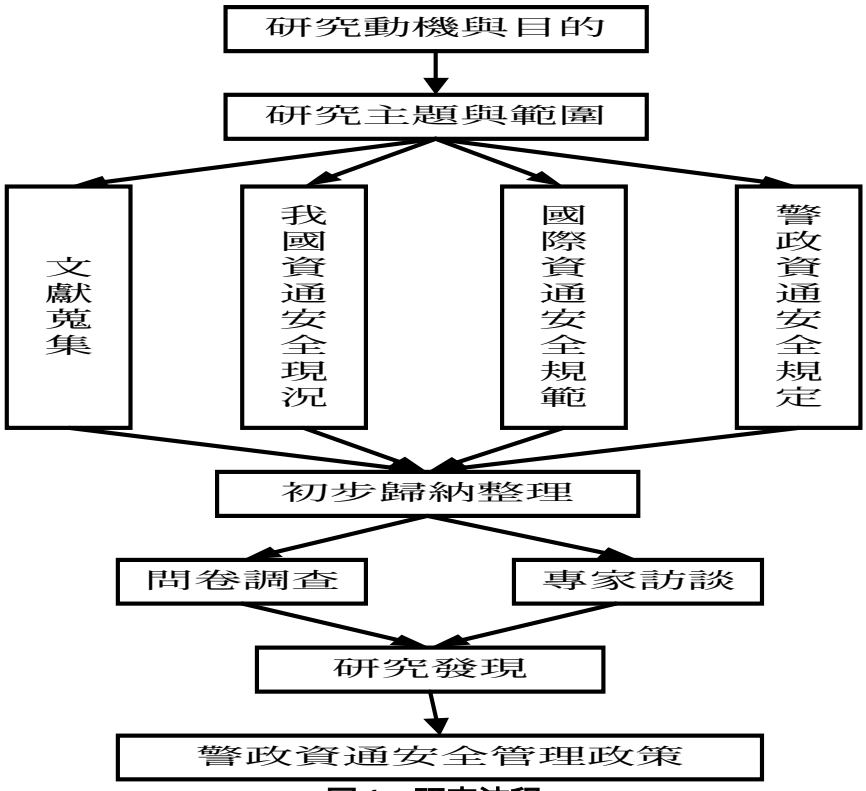

圖 1：研究流程

2.國際資通安全管理規範概況

所謂標準就是經由大多數國家或團體認定，供一般或重複使用，以提供各項活動或其結果有關的規則、指導綱要或特性所建立之文件，國際標準組織(International Organization for Standardization，簡稱 ISO)為目前全球最受認定的標準制定組織，該組織所制定或討論中之資通訊安全標準約可分為「資訊安全產品標準」、「資訊安全管理驗證標準」、「軟體處理評估標準」及「資訊安全管理認證程序標準」等四類，計有 ISO/IEC 15408-2，15408-3，17799-1，13335-1，13335-2，13335-3，13335-4，15504-1~7，15026，12207，13569 等，此外尚有其他國際標準組織所訂之資通訊安全標準如 BS7799、EA7/03，COBIT 等[3]。

「ISO/IEC 17799:2000 (BS7799 PART I)」的全名是「Information Security Management-Part 1: Code of Practice for Information Security Management」，是一個由英國 BSI（British Standards Online）在 1995 年二月所提出、1999 年五月修訂，為目前國際上最知名的安全規範，而且其 PART I 於 2000 年 12 月，也已被 ISO 接納成為標準 ISO/IEC 17799:2000。它廣泛地涵蓋了所有的安全議題，是一個非常詳盡甚至有些複雜的資訊安全標準[4][5]。其內容計分為安全政策、安全組織、資　分類及控制、人員安全、實際及環境安全、通訊與作業管理、存取控制、系統開發及維護、業務持續運作管理[6]、符合性等十大管理要項，卅六個執行目標及一二七項管制方法[7]。

3.警政資通安全管理機制檢討

內政部警政署為維護資通安全，在建置警政資訊系統之初即研訂「內政部警政署電子計算機作業保密安全實施規定」一種，於七十六年六月頒行，並依系統之擴大建置而多次增修，於八十九年十月修訂後其內容計分為總則、一般規定、實施要領、考核與獎懲及附則等五章十節四十三款，其內容雖已包含依據、目的、適用範圍、保密安全原則、權責劃分、人員管理、資料處理、維修作業、場地管理及物料管理等範疇，但因該規定係依專屬系統為防護標的，規範內容頗為簡略，對網際網路之開放環境而言，更顯不足，亟需重新修訂，謹就「內政部警政署電子計算機作業保密安全實施規定」內容與 ISO 17799-1：2000 內容比較如表 1，並就現行警政資通安全管理機制之優、缺點，彙述如下：

表 1、保密安全實施規定與 ISO 17799：2000 內容比較

內容	ISO 17799:2000		內政部警政署電子計算機作業保密安全實施規定	
	執行目標數（36）	管制方法數（127）	款數（43）	款目
安全政策	1	2	11	1002,1003,2001-2007, 5002-5003
安全組織	3	10	6	2008-2013
資分類及控制	2	3	1	3014
人員安全	3	10	4	3001-3004
實際及環境安全	3	13	11	3009-3013,3015-3020
通訊與作業管理	7	24	1	3005
存取控制	8	31	1	3006
系統開發及維護	5	18	2	3007-3008
業務持續運作管理	1	5	0	
符合性	3	11	6	1001,4001-4004,5001

說明：本表內容以 ISO17799:2000 之十大管理要項為內容分類依據。

3.1 優點

1. 警政機關在七十六年間即訂定資通安全規範頒行，並依環境變化多次檢討修訂，使龐大的警政體系，在維護警政單位資通安全時有所遵循。
2. 現有規範內容分為總則、一般規定、實施要領、考核與獎懲及附則等五章十節四十三款，其內容包含依據、目的、適用範圍、保密安全原則、權責劃分、人員管

理、資料處理、維修作業、場地管理及物料管理等範疇，除在業務持續運作管理方面未加規定外，內容尚稱完整。

3.2 缺點

1. 現行規定條文內容過於簡略，不夠深入嚴密。
2. 現行規定偏重於實體及環境安全部分，其他範圍明顯不足。
3. 未對業務持續運作管理方面加以規定。
4. 欠缺全般性資通安全管理政策及指導。
5. 執行管制及督導考核機制厥如。

4. 警察資通安全現況調查

4.1 調查經過

本研究為深入瞭解各級警察人員使用電腦的行為、經驗、期望及現行資通安全管理規定執行情形，乃以問卷調查方式，對各級警察機關各級官警、中央警察大學二技同學設計及警察專科學校進修班同學實施調查，計回收有效問卷 1618 份，調查執行過程簡述如下：

1 調查範圍

針對全國各級警察單位現職警察同仁使用電腦之情形，以探索電腦設備現況、使用電腦現況、使用電腦經驗、資通安全管理現況及及人別資料等相關因素間之關係。

2.調查對象

本調查以全國各級警察單位現職警察同仁為對象，含蓋各縣市、各種專業警察，各年齡層，各種階級及內、外勤同仁，亦包括在中央警察大學及警察專科學校進修之現職警察同仁。

3.問卷設計

本調查所用問卷係依據「內政部警政署電子計算機作業保密安全實施規定」之資通安全規定項目設計，擬定問卷二頁四十六題，經由中央警察大學資管所研究生五名，警政署資訊室同仁五名、保防室同仁五名及新竹縣警察局、保一總隊等基層同仁十五名，合計三十名實施前測後、再經討論、修正後定案。

4.抽樣方法

本調查抽樣方式如下：

(1)全國各警察機關各級警察同仁

由中央警察大學以九十一年四月十一日(九一)資管第一０九號函(如附錄三)，將問卷函送至全國二十五縣市警察局各二十份(實際寄出各四十份)，請求各縣市警察局協助辦理調查，共計寄出 1000 份問卷，經多次透過公、私情誼催收，共回收 910 份。

(2)中央警察大學二技同學

經由中央警察大學總隊部之協助，以隨機抽樣方式對二技同學實施調查，共計發出回卷 500 份，回收 451 份。

(3)警察專科學校進修班同學

經由警察專科學校大隊部之協助，以隨機抽樣方式對進修班同學實施調查，共

計發出回卷 500 份，回收 427 份。

本調查共計發出問卷 2000 份，回收問卷 1788 份(89.4%)，其中有效問卷 1618 份(80.9%)，其中極少數問卷有單題未答(Missing Valid)情事，但因其數量極少，本研究在統計時逕予忽略。

5 資料分析方法

本研究所收集資料，以 SPSS For Windows 10.0 版進行資料處理與分析，使用統計方法包括：

(1)次數分配及百分比

利用次數分配計算填答者之各項填答情形，以了解受測者基本資料、電腦設備現況、使用電腦現況、使用電腦經驗及資通安全管理現況等項分佈情形。

(2)信度分析

以 Cronbach's Alpha 係數考驗量表之內部一致性。一般而言，信度係數超過.70，都是可以被接受。

(3)效度分析

因本調查係依據「內政部警政署電子計算機作業保密安全實施規定」之各項規定設計，尚無完整理論架構支持，惟本問卷業經三十位各級警察同仁前測後定稿，應具表面效度。

(4)獨立樣本 T 檢定

對回收自學校之資料與與全部之資料逐題作樣本差異性分析，以研判有無系統偏誤之情事。

(5)Pearson 積差相關分析

檢測用 Pearson 積差相關檢驗受測者基本資料、電腦設備現況與使用電腦現況、使用電腦經驗及資通安全管理現況之關係。

4.2 調查結果

4.2.1.不符資通安全要求項目分析

綜合本節對電腦設備現況、使用電腦現況、使用電腦經驗及資通安全管理現況等項分析，調查結果尚不符資通安全要求者計 29 項，其中屬「資通安全管理不當」者計 15 項(佔 51.7%)，「資通安全設備不足」者計 3 項(佔 10.4%)，「資通安全教育訓練不足」者計 11 項(佔 37.9%)，茲彙整如表 2。

4.2.2 調查結果與人別資料相關性分析

綜合本節對使用電腦現況、使用電腦經驗及資通安全管理現況等項分析，調查結果與受調查者基本資料相關性分析如表 3。

5.研究發現

5.1 資通安全設備不足

資通安全設備是確保資通安全之基礎，種類、價格及設置因任務需求、網路架構而有所不同，本研究僅就基層警察同仁可理解，且能接觸的不斷電設備、上網設備、電子郵件設備及檔案加密設備等最基礎部分實施問卷調查，由下列調查得知警察資通

安全設備亟待購配：

1.未提供電子郵件設備者 42.2%。

2.無檔案加密設備者達 55%，其中有 30.8%認為工作本有此需求。

3.無不斷電設備者達 51%。

表 2 調查結果不符資通安全要求統計

調查項目	調查結果	對資通安全之影響
一、電腦設備現況		
電子郵件共用帳號	26.3	資通安全管理不當
可在單位外收發郵件	16.5	資通安全管理不當
無檔案加密設備	55.0	資通安全設備不足
無不斷電設備	51.0	資通安全設備不足
二、使用電腦現況		
電子郵件無加密習慣	58.9	資通安全教育訓練不足
無檔案加密習慣	54.8	資通安全教育訓練不足
三、使用電腦經驗		
認為密碼無幫助	16.8	資通安全教育訓練不足
認為密碼使用不便	58.3	資通安全教育訓練不足
認為應可自行安裝軟體系統	31.6	資通安全教育訓練不足
認為單位電腦設備不安全	31.8	資通安全教育訓練不足
認為單位電腦檔案不安全	63.2	資通安全教育訓練不足
認為自已應負電腦安全責任	6	資通安全教育訓練不足
四、資通安全管理現況		
電力中斷情事	70.3	資通安全管理不當
電腦病毒發作	63.8	資通安全管理不當
天災情事	47.3	資通安全管理不當
設備或資料遺失情事	31.4	資通安全管理不當
無防毒軟體設備	17.7	資通安全設備不足
未定期更新病毒碼	41.7	資通安全管理不當
單位規定自由選擇是否使用密碼	38.8	資通安全管理不當
單位不要求定期更改密碼	19.6	資通安全管理不當
未定期更改密碼	57.4	資通安全教育訓練不足
單位無不良密碼管理	71.6	資通安全管理不當
單位允許自行安裝軟體	22.3	資通安全管理不當
定期檢查電腦硬體設備	43.8	資通安全管理不當
定期檢查電腦軟體設備	40.1	資通安全管理不當
定期檢查電腦連線設備	40.7	資通安全管理不當
不能確定單位有無資通安全規定	54.9	資通安全教育訓練不足
單位無資通安全規定	9.4	資通安全管理不當
未學過資通安全課程	67.2	資通安全教育訓練不足

5.2 電腦及網路使用待推廣

警察職司國家安全及社會安寧，且單位遍布全國，成員眾多，指管通勤是達成此

一目標的重要命脈，有效的通信更是警察機關與警察機關，行政機關及人民的交流基礎，以達通訊快速，資源共享的目標，而新興的網路科技更是最佳的利器，可是由下列調查結果發現，警察對網路使用亟待推廣：

1.有 58%不知傳送資料的 NN 系統，合計 84%未使用過此作業系統，僅有 1.1%對此系統使用頻頻。

2.僅有 53.7%經常或頻繁使用網際網路，但有 96%認為網際網路有助於公務推動。

3.有 19.4%未使用電子郵件，僅 39.9%經常或頻繁使用，47.1%從未使用電子郵件傳送公務資料，僅 19.7%經常或頻繁使用電子郵件傳送公務資料，但有 88.3%認為電子郵件有助於公務推動。

4.在電腦使用方面仍停留在文書處理上(64%經常或頻繁使用，96%認為有助於公務推動)，但使用電腦處理大量資料(35.8%經常或頻繁使用，95.7%認為有助於公務推動)或編寫程式(7%經常或頻繁使用)方面則亟待推動。

表 3 調查結果與受調查者基本資料相關性分

調 查 項 目	年齡	年資	學歷	官階	職務	性質	性別	單位
公務查詢情形		正相關	負相關	負相關	正相關	負相關	負相關	負相關
使用ＮＮ系統情形	正相關			正相關	負相關			
使用網際網路情形			正相關	正相關	負相關	正相關	正相關	正相關
網路有無幫助		正相關	正相關		負相關	正相關		
使用電子郵件情形	負相關	負相關	正相關	正相關	負相關	正相關	正相關	正相關
電子郵件傳送公務情形		負相關	正相關	正相關	負相關	正相關	正相關	正相關
電子郵件加密情形	正相關	正相關	負相關					
電子郵件有無幫助		正相關	正相關	正相關	負相關	正相關		
電腦處理文書情形			正相關	正相關	負相關	正相關	正相關	
文書處理有無幫助	正相關	正相關	正相關	正相關	負相關	正相關		
電腦處理大量資料情形			正相關	正相關	負相關	正相關	正相關	
處理大量資料有無幫助	正相關	正相關	正相關	正相關	負相關	正相關		
電腦編寫程式情形		負相關						
檔案加密習慣			負相關					
檔案加密設備								
密碼有無幫助								
密碼有無不便				負相關		負相關	負相關	負相關
安裝軟體系統期望					正相關			
單位電腦設備安全度自評				負相關	正相關			
單位電腦檔案安全度自評	正相關						正相關	正相關
電腦安全責任歸屬			正相關	正相關	負相關	正相關		正相關
單位資通安全規定瞭解情形	正相關		正相關	正相關	負相關	正相關		
資通安全教育情形		負相關			負相關	正相關	正相關	負相關

5.3 警察資通安全現況堪虞

由下列調查結果發現，警察機關資通安全現況堪虞：

1.在 49%置有不斷電設備下，仍有 70.3%受測者受電力中斷事故困擾。

2.在 82.2%置有防毒軟體設備下，仍有 63.8%受測者受電腦病毒事故困擾。
3.有 47.3%受測者曾因天災而影響資通安全。
4.有 31.4%曾發生電腦設備或檔案遺失情事，

5.4資通安全管理欠落實

內政部警政署雖已訂頒「內政部警政署電子計算機作業保密安全實施規定」，並於七十六年六月頒行，姑且不論其內容是否合於國際資通安全規範，如能有效執行亦將有助於警察資通安全之推昇，可是由下列調查結果發現，各級警察機關對本項規定之執行尚欠落實：

1. 僅 40.5%置有防毒軟體且定期更新　毒碼。
2. 有 38.8%電腦無密碼保護，另 19.6%電腦放任使用者自行決定是否使用密碼保護。
3. 57.4%密碼未定期更改。
4. 71.6%單位未對不良密碼實施管理。
5. 尚有 22.3%使用者可在公家電腦上自行安裝軟體。
6. 僅 43.8%定期檢查電腦設備，40.1%定期檢查電腦中之軟體，40.7%定期檢查電腦連線設備。
7. 有 54.9%受測者不能確定單位有無資通安全管理規定，另 9.4%確定該單位設有此一規定。
8. 67.2%未受過資通安全教育或訓練。

5.5 資通安全觀念待宣導

資通安全觀念是推動資通安全的原動力，但由下列調查結果發現，警察人員對資通安全仍有許多錯誤的觀念：

1. 58.9%受測者無電子郵件加密習慣，54.8%無檔案加密習慣。
2. 16.8%認為密碼無任何幫助，58.3%認為密碼非常或稍有不便。
3. 31.6%認為應允許在公家電腦自行安裝軟體。
4. 有 31.8%認為單位電腦設備不安全，另有 44.6%無法評估是否安全。
5. 有 63.2%認為電腦檔案有被侵害之可能，另有 24.7%無法評估是否安全。
6. 對資通安全應由誰負之問題上，63.3%認為應由資訊人員負責，22.3%選擇廠商，僅有 6%認為應自行負責。

5.6 警察資通安全規範待修訂

由保密安全實施規定與 ISO/IEC 17799:2000(BS7799 PART I)內容比較(如表１)及優缺點分析中，不難發現，「內政部警政署電子計算機作業保密安全實施規定」不論在質與量上，均無法達到國際規範的要求，為有效推動警察資通安全管理之工作，亟需修訂現有資通安全規定，並依據人力、物力及財力情形，研訂配套計畫逐年推動，方能有效執行。

6.警政資通安全管理政策芻議(代結論)

ISO/IEC 17799:2000(BS7799 PART I)以 127 個控制方法，建構嚴謹的資訊安全管理系

統，其中部分控制方法在「內政部警政署電子計算機作業保密安全實施規定」中並未提及，本研究亦未在實證調查中深入探討，惟為擬定完整、明確的警政資通安全管理政策，本文乃依照 ISO/IEC 17799:2000(BS7799 PART I)的十大控制目標之結構，並參考前述各章之文獻探討、實證調查及研究發現，擬定警政資通安全管理政策(高階政策)10 條 160 字如下，

6.1 遵循警察任務需求，明訂政策分段執行

管理階層應制定一個明確的安全政策方向，並透過在整個組織中發佈和維護資訊安全政策，表明自己對資訊安全的支持和保護責任。發展警政資通系統的目的，係為全國各級警察機關及同仁服務，以提昇警察工作之效能，其政策自應遵循「維持公共秩序，保護社會安全，防止一切危害，促進人民福利」之警察任務[8]，資通安全管理政策亦應遵循(警察資通安全政策關係如圖 2)，另為使建置警政資通安全管理系統之計畫確實可行，可參酌本研究所得 ISO/IEC 17799:2000(BS7799 PART I)之 127 項控制方法執行優先順序，配合預算及人力分年實施，本節應包括下列低階政策：

1．資訊安全政策應文件化，並公告週知。

2．資訊安全政策應依人、事、時、地、物等因素變化，定期或隨時重新審查、評估、修訂。

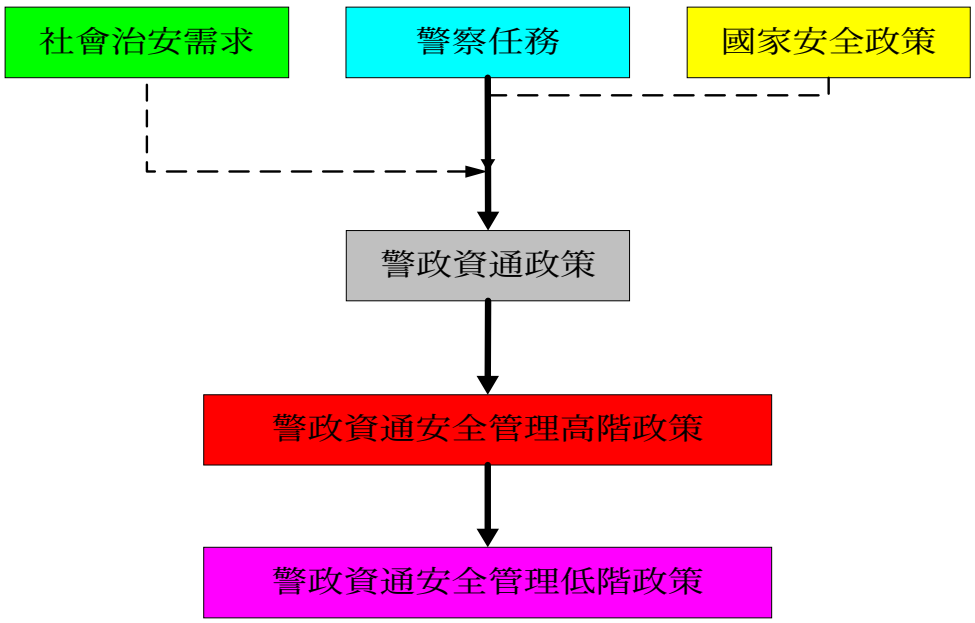

圖 2 警察政策與資通安全政策關係

6.2 健全警察資通組織，強化資通安全編組

為增強警政資訊系統安全能量，如僅於現行編制中增置安全部門，除需增加龐大人力外，並不能解決現有警政資訊組織頭重腳輕、人力不足且分散、警政通訊與資訊單位分立等缺失，故為達到警政資通安全之目的，本節應包括下列低階政策：

1.健全警察資通組織

警察資訊單位編制宜調整如下(如圖 3)：

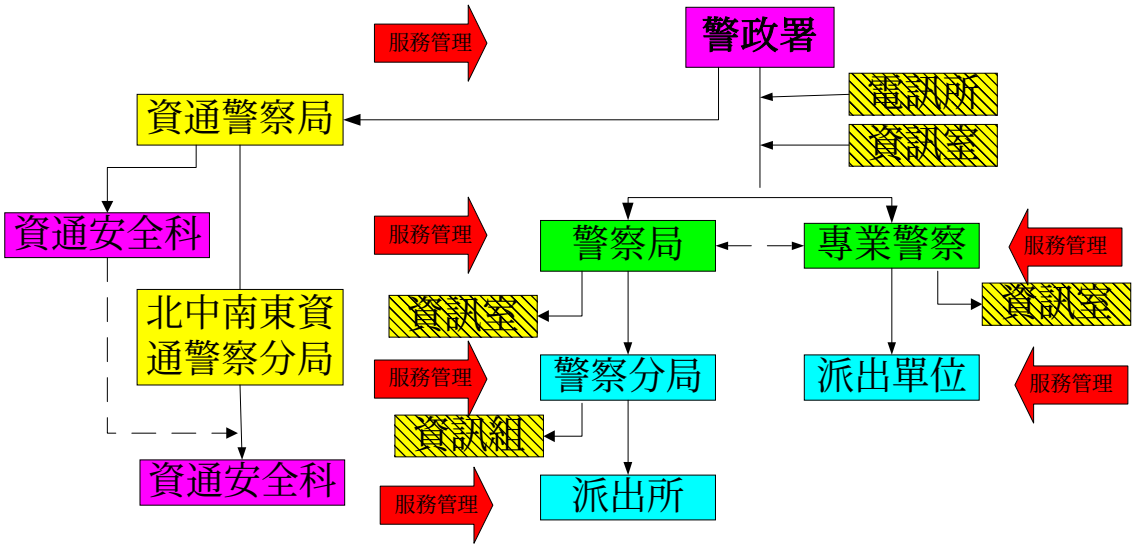

圖 3 警察資通安全組織整合架構

(1)警政署資訊室與警察電訊所合併為「警察資通局」，辦理全國警政資通事宜，並在其內設置專責資通安全部門，辦理資通安全事宜。

(2)在全國分北中南東四區，分設「警察資通分局」，辦理轄內各警察單位資通工作，並在其內設置專責資通安全部門，辦理資通安全事宜。

(3)裁撤各警察局、警察分局及專業警察單位資訊編組，人員調整至警察資通分局集中辦事。

2. 增置資通安全單位及管理資訊安全委員會。

6.3 確認資產風險評估，定期清查分類標示

透過清查資產的價值、弱點及威脅，對警察各類資通訊資產進行風險評估，確認風險之所在，以移訂定安全管理對策，本節應包括下列低階政策：

1.確認資產風險評估，維持對於組織織資產的適切保護，確認資　的保管責任

2.明定資產風險評估之程序，對資訊分類，指明其需要、優先順序和保護級別。

6.4 辦理人員忠誠考核，落實訓練追蹤督考

忠誠考核的目的，乃在降低因人員錯誤、偷竊、詐騙或不當使用設施所造成的風險，而落實訓練的目的，係為確保員工了解資訊安全的威脅及顧慮，並且具備在其日常工作過程中支持組支織資訊安全政策的能力，並安全及失效事件所造成的損害降到最低，並監督這些事件以從中學習。本節應包括下列低階政策：

1. 對新員工應充分進行篩選，特別是對於從事敏感工作的員工更是如此，在聘僱階段，就應該說明安全責任，將其寫入合約，並在雇用期間進行監督。

2. 所有員工和使用資訊處理設施的第三方使用者都應簽署保密協定。

3. 應對使用者進行安全步驟和正確使用資訊處理設備的訓練，將可能的安全風險降到最低。

4. 明訂安全事件、安全弱點、軟體失效事件的通報程序、責任及獎懲規定。

6.5 控制資通設備環境，防護資通設備安全

控制資通設備環境的目的乃在防止對警察資通設備所在地及資訊未授權的進入與存取、破壞及干擾，預防資　遺失、而防護資通設備安全係為預防對警察資通設備破壞或損失，並確保警政資通系統運作不遭受干擾，由研究發現中得知當前各級警察機關資通安全設備不足，且未能有效管理以使其發揮應有之功能，在 49%置有不斷電設備下，仍有 70.3%受測者受電力中斷事故困擾即是一例，故內政部警政署應爭取年度預算或專案經費，大幅購配資通安全設備，並培訓優秀管理幹部，以有效提昇警察機關資通安全能量。本節應包括下列低階政策：

1. 應明確劃分安全區域，進行實體進出管制，並對辦公處所及設備進行必要之保護。
2. 應保證警察資通設備免受安全方面的威脅和環境的危害。
3. 遵照「僅知原則」防止將資訊和資訊處理設備暴露給未經授權的人，或被未經授權的人修改或偷竊。

6.6 確保通訊安全快速，提昇資訊網絡安全

運用電腦及網路來提昇警察工作效率已是不容置疑的方向，由研究發現中得知警察單位使用電腦及網路之情形尚不普及，現有設備尚未發揮應有之功能，內政部警政署應在施政計畫中，將警政電腦及網路化訂為最重要施政目標，以有效提高警察工作效率。本條政策的目的在確保正確與安全地操作資訊處理設備，且將系統失效的風險降至最低，並保護軟體和資訊的完整性、確保網路中資訊之安全性、儲存媒體的處理與安全及資訊和軟體交換的安全。

6.7 使用技術協助管理，存取控制嚴格便利

存取控制的目的乃在防上未經授權之存取，警察機關偏布全國各地，人員眾多，在本研究實證調查中，業已發現密碼管理不良、自行安裝軟體等管理缺失，為達前述目的，應先明訂存取控館政策，使用先進的系統管理技術，對使用者存取管理、使用者責任、網路存取控制、作業系統存取控制、應用程式存取控制、系統存取和使用的監察、可移動式電腦運算及電腦通訊遠距工作等進行有效的管理控制，並確保存取的便利性，已是必然的趨勢。

6.8 運用安全科技產品，支援維護系統安全

本條政策之目的乃在保證安全機制內建於資訊系統之中，以防止應用系統中使用者資料的遭受遺失、修改或不當使用，並確資訊的安全性、真實性或完整性，以確保系統檔案、維護應用系統軟體和資訊的安全性。

6.9 律定危機處理程序，持續演練檢討修正

本條政策之目的乃在防止業務活動中斷，確保重要業務流程不受重大故障和災難的影響。在本研究中發現目前警政資通訊安全管理機制中，並不存在危機處理與復原之計畫，本項工作應與資產評估結合，以最適切之計畫對各類資產採取適當的保護和復原措施。本研究謹將辦理警察資通訊資　鑑別、分類，落實危機管理與復原機制程序彙整如圖 4，並說明如下：

1.資通資產普查。

資產鑑別乃為對現有資通資　，經由清查之程序來確認資產、換言之即是要確定「牛肉」在何處。

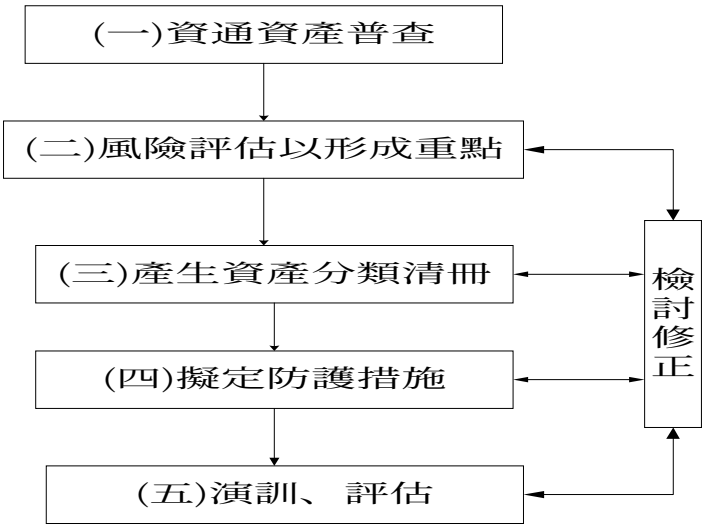

圖 4 資通資產鑑別、分類、管理程序

2 風險評估。

對各項資產因人、事、時、地、物等因素所產生之危害，進行風險評估，排定危機等級及類別，以確定安全重點何在，以集中有限行政資源運用。

3 資產分類，產生清冊。

分類之目的乃在保證資　得到適當的保護，其方法係對資　分類，指明其需要、優先順序和保護級別，因為資　的敏感程度和關鍵程度各不相同，例如有些資　需要加強保護或進行特別對待。國家可以使用資訊分類系統定義合適的保護級別，並解釋對特別處理手段的需要。

根據資　分類之結果，彙整資產清冊，也就是將成果文件化，其目的乃在幫助國家確保對資　實施有效的保護，也可以用於其他商業目的，如資　狀況、金融保險等（資　評估)。編輯資　清單的過程是資　評估的一個重要過程。

4 擬定危機管理及復原計畫(因應措施)。

資通安全專責機構可利用以上資訊，指導、管制各資產主管單位根據資　的重要性和價值，擬定相應級別的保護措施。

5 演訓評估

在因應措施擬定後，應經過教育訓練之方法，使各級參與人員明瞭危害之來源及應變之道，而且必須透過假設狀況之反復推演練習，以評估因應措施之可行性。

本節應包括下列低階政策：

1. 應該實施業務持續運作管理程序，預防和恢復控制相結合，將災難和安全故障（可能是由於自然災害、事故、設備故障和蓄意破壞等引起）造成的影響降低到可以接受的基準。
2. 應該分析災難、安全故障和服務損失的後果。制定和實施應急計劃，確保能夠在要求的時間內恢復業務流程。
3. 業務持續運作管理應該採用控制措施，確定和降低風險，限制破壞性事件造成

的後果，確保重要操作及時恢復。

6.10 嚴禁違反法規命令，獨立內部稽核偵防

本條政策之目的乃在確定警政資通系統不違反刑法、民法、成文法、法規或合約義務以及任何安全要求，並保證系統符合組織的安全政策和標準，且最大限度地提高有效性，最大程度地減少系統稽核過程的干幹擾和對系統稽核過程的干預。本節應包括下列低階政策：

1. 資訊系統的設計、操作、使用和管理要依據成文法、法規或合約安全的要求。
2. 應該根據適當的安全政策進行此類評審，還應該對技術平臺和資訊系統是否符合安全實施標準進行稽核。
3. 在系統稽核過程中，應該採取適當的控制措施保障作業系統和稽核工具的安全，同時還要求採取保護措施保障稽核工具的完整性，防止濫用。

參考文獻

1. William G. Zikmund, Business Research Methods, USA, The Dryden Press Harcourt Brace College Publishers, 1997.
2. 葉至誠、葉立誠合著、研究方法與論文寫作，台北市、商鼎文化出版社，民國八十八年二月，p74-81。
3. 魏忠華、樊國楨、黃淙澤、徐士坦，資訊安全管理系統相關標準芻議/電腦稽核第七期，台北市、中華民國電腦稽核協會，民國 90 年 10 月。
4. http://www.secureonline.com.tw/sol_main_t06-1a.asp?id=117，(accessed 90 年 11 月 23 日)。
5. 林勤經、樊國楨、方仁威，「資訊安全認證與電子化網路社會」、資訊安全論壇創刊號、台北、鈺松國際、2001 年。
6. 樊國楨、林宜隆、王俊雄，資通訊安全危機事件處理機制芻議，第十一屆全國資訊安全會議論文集，民國 90 年 5 月，p117。
7. http://www.secureonline.com.tw/sol_main_t06-1a.asp?id=117，(accessed 90 年 11 月 23 日)。
8. 內政部警政署編印，警察實用法令(90 年版)，P35。