從「ISO17799」的導入論國軍資訊資產控管—以後備司令部為例

Discuss the Nation troop's information property control by ISO17799 implemention-Take the Reserve Headquarters as the example

林明武 上校 (Ming-Wu, Lin)
國防大學管理學院教官兼隊長

夏鈞浩 中校 (Chun-Hao, Shia)
後備904旅營長

提　　要

一、資訊安全(Information Security; IS)管理已是當今不可忽視的管理議題，其主要精神在於辨識出組織的重要資訊資產及其所面臨的威脅，並在資源有效地分配下，規劃合理控管措施，使得風險降至可接受範圍，這是一個風險管理的過程，管理重點應放在組織機密資料的保護，而非所有資訊資產存取的管道上，因爲如此將造成國軍的成本浪費並模糊失焦，近年來層出不窮的資安事件，多爲缺乏上述風險管理機制所致。

二、本研究依據ISO17799資訊安全管理作業要點，針對單位情形和特性進行規劃建議，從數個資安事件的檢討，思考國軍在資訊安全管理上的不足。

三、研究中試圖歸納資訊資產在分類與控管上的重點，同時依據國際標準ISO17799的規範及目前部分機構所採用的資訊資產分類與控管的方法，規劃可供單位採行之建議方案。

關鍵詞：資訊安全、資訊資產、分類與控管、ISO17799

Abstract

1. Information, as further to the energy after a new strategic resources, operational procedures and even influence the war ended in a tie, the first thing. Therefore produce to information warfare Revolution of Military Affairs.
2. In the face of the future of information warfare, in order to get information superiority, message security is more and more important, because the message security is an essential element of information warfare.
3. For the sake of a limited budget, to highly profitable investment do message security, we study cryptography and information hiding.

Keywords: Information warfare, And information superiority, Information security, cryptography, Information hiding

壹、前　　言

資訊環境自90年代從封閉走向開放，資訊成本急遽下降及使用介面便利的雙重效益，讓國軍各單位逐漸增加資訊設備的添購；隨著資訊科技的進步，帶動資訊系統的使用，進而改變了各項參謀業務的處理流程，單位對資訊系統的依賴程度也大幅提高。

雖然資訊數位化帶來許多管理上的方便性，但安全問題也開始備受挑戰；當單位正在享受資訊系統帶來的種種利益時，有心人士也正鑽研資訊系統的弱點，以便進行攻擊；此現象在網際網路及電子社群盛行後，更加猖狂；另外，由於部分國軍幹部對重要資訊欠缺應有的保護或不當使用，而造成資安違規洩密及影響國軍聲譽之案件層出不窮。有鑑於此，相關的管理、技術議題因應而生；然而，國軍需要的是一個全面有系統的管理，任何片面的加強都是枉然。

近年來國內外連續不斷的出現程度不同的資訊安全事件，這些事件不僅僅是簡單的資訊系統癱瘓的問題，其直接後果是導致巨大的經濟損失，還造成了不良的社會影響。

以下列舉近期國內外較大的軍事資訊安全事件，每一個事件都備受矚目，有的甚至是該國近年來最大宗的案件。本研究對於各個事件的報導資訊予以分析彙整如表1：

由於資訊環境的改變，使得資訊安全管

表1　資訊安全事件彙整

時　　間	事　　由	發　生　國　家
2005年3月	衡山指揮所遭木馬程式入侵。	中華民國
2005年8月	電展室莊姓少校洩密。	中華民國
2006年3月	我駐外館電腦遭木馬程式入侵。	中華民國
2007年3月	自衛隊中士拷貝檔案夾藏神盾艦機密資料。	日本
2007年1月	國軍博勝案資料外洩。	中華民國
2007年3月	漢光演習資料外洩。	中華民國
2007年11月	軍訓教官個人資料外洩。	中華民國
2009年10月	網際電子認證資料及機密外洩。	南韓

衡山指揮所遭木馬程式入侵（2005年3月）[1]	
外洩資料內容	漢光21號兵棋推演相關內容。
外洩管道	透過第三國與巴基斯坦入侵。
外洩資料流向	中國。
後續發展	1. 該名軍官除進行隔離與修補漏洞、更新病毒碼與掃毒等措施外，並立刻發出緊急通報。因發現的地點是在國軍最高指揮中心衡指所，軍方馬上由通資次長室綜合處處長柴○○、資電作戰指揮部指揮官崔○○等人員組成「○331事件」專案小組調查。 2. 專案小組曾發現目標區分別在聯一人事、聯二情報以及聯三作戰三個營區內。經專案小組分別到3個營區進行清查，結果發現只是個「跳板」，目標區又轉到左營軍區、臺北軍聞社文化營區、國防大學等營區，最後確認是中國網軍由第三國與巴基斯坦入侵。 3. 強化衡指所內部電腦漏洞修補與隔離機制。

1〈中國木馬破我軍中樞〉，《蘋果日報》，http://tw.nextmedia.com/applenews/article/art_id/2209584/IssueID/20051118，檢索日期：2009年11月17日。

電展室莊姓少校洩密（2005年8月）[2]	
外洩資料內容	電展室通訊參數等情報資料。
外洩管道	下載資料後，違規攜出營外共計6次。
外洩資料流向	由莊員交由退役人員帶到中國販售圖利。
後續發展	1. 案件經高等軍事法院審理後宣判，依違反洩漏軍事機密等罪名，判處莊○○無期徒刑並褫奪公權終身，爲近年來涉共諜案判刑最重者。至於黃○○部分，尚待高等法院審判。 2. 加強儲存媒體管控機制，封鎖資料外洩管道。

我駐外館電腦遭木馬程式入侵（2006年3月）[3]	
外洩資料內容	公務處理相關內容
外洩管道	由網際網路連線至一般電腦，再經由一般電腦與公務電腦連線時植入木馬。
外洩資料流向	中國。
後續發展	1. 國家安全局駐洛杉磯美西站主任資○○少將違規使用電腦，將公務電腦與一般電腦連線使用，遭中國網軍入侵；無獨有偶，我國駐外一百多個外館電腦，同時間也遭中國網軍入侵，並被植入木馬程式；情治高層懷疑中國網軍是從資○○的電腦知道外交部駐外單位的聯絡網址與密碼，才順利入侵外交部外館的電腦。 2. 資員身爲地區主管，嚴重違反保密規定，被調回進入訓練中心的「職能訓練組」，接受內部調查。 3. 外交部要求外館全面將處理公文及上網用的電腦分開，避免再遭入侵。

自衛隊中士拷貝檔案夾藏神盾艦機密資料（2007年3月）[4]	
外洩資料內容	美軍神盾艦作戰參數資料。
外洩管道	日本海上自衛隊中士，向同袍拷貝色情圖片，不知其中夾帶美國神盾艦的機密資料。
外洩資料流向	自衛隊中士個人電腦。
後續發展	該中士否認洩密，稱只是向同袍拷貝色情圖片，不知其中夾帶機密資料。由於美日間訂有秘密保護法，由美國提供的武器等相關情報均屬最高機密，因此日本政府現正積極追查洩露管道。

國軍博勝案資料外洩（2007年1月）[5]	
外洩資料內容	「博勝案」相關資料。
外洩管道	國防部資電作戰指揮部梁姓中校擅自將「博勝案」機密資料備份帶回家存檔，資料遭中國藉木馬程式竊取。
外洩資料流向	中國。
後續發展	1. 美國軍方派美國在臺協會官員向國防部表達嚴重關切，害怕連美國太平洋司令部的通資狀況也讓中國了解。 2. 相關人員均遭調查並依外洩資料機密等級，按照國家機密保護法辦理懲處。

2《聯合報》，2005年6月20日，A8。

3〈中國網軍攻陷我百外館〉，《蘋果日報》，http://tw.nextmedia.com/applenews/article/art_id/2597314/IssueID/20060510，檢索日期：2009年11月17日。

4《聯合報》，2007年4月6日，A17。

5《聯合報》，2007年4月12日，A8。

漢光演習資料外洩（2007年3月）[6]	
外洩資料內容	國軍漢光演習兵推資料。
外洩管道	公務家辦且家中電腦已遭植入木馬程式。
外洩資料流向	中國。
後續發展	1. 相關人員均遭調查並依外洩資料機密等級，按照國家機密保護法辦理懲處。 2. 國防大學加強資安管控措施，避免再有類似案件肇生。

軍訓教官個人資料外洩（2007年11月）[7]	
外洩資料內容	全國軍訓教官的個人姓名、軍階、手機、家中電話、身分證字號、住址等。
外洩管道	新竹縣軍訓聯絡分處官員筆記型電腦裝有FOXY共享軟體，上網時造成資料外洩。
外洩資料流向	臺灣。
後續發展	1. 教育部中部辦公室軍訓科長證實，洩密事件是新竹縣軍訓聯絡分處官員便宜行事的作業疏失，因該員筆記型電腦裝有共享軟體，上網時造成資料外洩，軍訓處兩周前已檢討懲處。 2. 事發後軍訓處通知美國Google總公司，將全球網頁上的暫存記憶檔全部清除，Google公司也相當配合，目前網路上已看不到這些機密資料。他強調，洩露的資料只侷限在新竹縣市，應未擴展到全國。

網際電子認證資料及機密外洩（2009年10月）[8]	
外洩資料內容	韓國國立環境科學院管理的700 家有害化學物質製造企業和機構的相關資訊、化學物質和天氣資訊近1,350件。
外洩管道	陸軍第三軍司令部某上校將該電子認證書儲存到電腦，後來用該電腦上網訪問網站時，感染到駭客植入的蠕蟲病毒，電子認證書因此被盜取。
外洩資料流向	第三國（不排除來自北韓）。
後續發展	1. 軍方昨天透露，陸軍第三軍司令部上網進入國立環境科學院建立的「化學物質事故應對資訊系統」時所必須使用的電子認證書，今年3月5日被駭客盜取，導致環境科學院的部分資料外洩。 2. 環境部表示，目前爲止，相關企業和機構並沒有出現資訊被盜取的案例。

資料來源：本研究整理。

理越來越重要，大多數國家與組織皆已意識到這個問題；再加上一次比一次更駭人的資訊安全事件，驅使各國加快腳步進行資訊安全管理。然而，因為過於求好心切，以及不願意投入足夠的資源，而忽略了在資訊安全管理領域相當重要的基礎工作。也就是應如何下手，才能使得投入有限的資源後，能有效達成資訊安全控管的目的。

對於民間企業資訊安全管理系統導入的探討，通常都是強調並著重於對資訊資產的風險評估及選擇如何控管，例如有委外需求的組織，就制訂一份委外管理辦法；但少有

6 同註5。

7〈教官個資網路看光光〉，《蘋果日報》，http://tw.nextmedia.com/applenews/article/art_id/3954822/IssueID/20071102，檢索日期：2009年11月17日。

8〈南韓軍隊上網，國家機密外洩〉，《中央社新聞》，檢索日期：2009年10月18日。

針對如何有效辨識資訊資產方法，及針對不同處理及使用之控管的探討。組織在初始進行ISO17799(ISO, 2005)所要求的「應列出並維持一分重要資訊資產的清單」時，所面臨的困擾是可以想見的。另一方面，基於組織資料的機密性，雖然有許多顧問公司，但大部分的企業仍期望由內部同仁自行建置資訊安全管理系統。

本研究依據ISO17799對組織建置資訊安全管理系統之建議，以個案單位的環境與需求，蒐集相關資訊，歸納整理出對單位未來建置資訊安全管理系統的建議與參考。

本研究的目的為提供單位在建置資訊安全管理系統(Information Security Management System; ISMS)時，對於資訊資產分類與控管的工作，有一務實的做法可供參考，減少未來摸索的時間，增加建置的效益。

為達上述目的，本研究探討以下問題：

一、資訊資產等級之變動性。

二、資訊資產分類等級決定的方法。

三、資訊資產分類與控管作法。

組織的資訊資產包含甚廣，大致上可歸納出實體類、軟體類及管理類3種，舉例如表2。本研究之範圍包含資訊安全管理及管理類資訊資產的分類與控管做法探討。

因資訊資產包含的類別較廣，故本研究僅針對國軍容易忽略的管理類資產為研究內容。

本研究係依據ISO17799國際標準組織對資訊安全管理制度之要求，並參考國內外機構對資訊資產分類及控管作法，規劃對單位在管理資訊資產分類及控管之建議。

貳、文獻探討

隨著資訊科技應用重要程度的日益提高，資訊安全控管，已成為實現資訊科技應用目的的必要任務；本章節藉由相關文獻探討，從資訊安全對組織的影響、ISO17799的條文規範、國際及國內資訊安全發展的現況等，做深入的探討分析。

一、資訊安全管理議題的演進

㈠資訊之定義

資訊安全管理議題之標的即為資訊，而資訊的定義為何？以下分別為教育部《國語辭典》與ISO17799對資訊所下的定義。

1.教育部《國語辭典》的定義如下：

電腦上指對使用者有用之資料和訊息的總稱，以別於未經過處理的資料。

2.ISO17799中對於「資訊」的定義是[9]：

⑴資訊，是現代企業組織的資產之

表2　資訊資產類別

類別	說明
實體類資產	泛指資訊安全範圍內的實體環境及電子設備。例如機房、辦公室、個人電腦、筆記型電腦、PDA、電腦主機、不斷電系統等。
軟體類資產	泛指組織所使用的資訊系統及作業系統。例如用兵後勤管理系統、公文處理系統、門禁管理系統、作業系統等。
管理類資產	泛指組織的管理資訊（形式不拘），例如人員基本資料、兵籍資料、採購資料、會議紀錄、內部呈核紀錄、電子郵件、傳眞、各類型判斷與計畫等。

資料來源：本研究整理。

9 ISO/IEC 17799 News, Asian Edition, March, 2005.

一，正如同有形資產（廠房、設備），對組織而言是具有價值的，因而需要妥善保護。

⑵資訊，會以各種不同型態存在，無論是紙本、電子檔、以網路進行資料交換的電子型態，甚至是人與人的對話交談都屬於資訊的範圍及種類。

⑶資訊，不論以何種型態存在，以何種方式儲存，都應該要被加以妥善保護。ISO17799其結構為：資訊安全範圍，風險審查與風險管理、資訊安全政策、資訊安全管理架構、資訊安全管理系統維護與審查。

保護資訊資產之安全，已成為當今數位空間的共識，亦為民主法制國家、社會與人民必備之素養。[10]

㈡資訊安全的定義

自90年代從封閉走向開放，網際網路的竄起，快速改變了企業的經營模式。電子化的營運模式隨之而起，而內外部所溝通的「資訊」逐漸成為重要的核心。因此從單純的「資訊」衍生「資訊安全」的議題，進而衍生到「資訊安全管理」的議題；我們可以從表3發現上述演進的過程。

表3　資訊安全的定義

年代	出處	資訊安全定義
1984	IBM [11]	對資訊資產的有意或意外之情形下，未經授權的公開、修改、破壞或使失效等等之行爲的保護。
1992	黃亮宇 [12]	就是把管理程序和安全防護技術應用於電腦的硬體、軟體和數據（或資料）上，以確保儲存中或傳遞中的數據（或資料）免除他人有意或無意的讀取、增刪或修改。
1997	Parker [13]	資訊安全的全貌就是對於有關個人或組織在使用所有關於說的、印行的及自動化記錄等情事的保護；及保護資訊的產生、處理過程、傳遞、儲存、使用、展示及控制等來源。
2000	Laudon and Laudon	資訊安全是指用來防止非法存取、竄改、偷竊和對資訊系統造成傷害的一些政策、程序和方法。藉由一些技術和工具來保護硬體、軟體、通訊網路和資料，以提升資料的安全性。
2000	吳琮璠、謝清佳	在網路分散環境中，運用一些控制機制對資源存取提供保護能力，以防止未經合法授權的使用者，入侵網路使用資源與破壞系統合作。其中控制機制包含技術，管理及組織文化層面（人事安全、實體安全、網路通訊安全、系統軟體安全、應用軟體與資料安全及電腦作業安全）。
2001	資策會	資訊安全的範圍涵蓋下列三個主題： 1.「網路安全」(Network Security)，乃指企業或組織實際運作的資訊系統與網路的安全防護，其所訴求的重點是實際運作的資訊系統本身的安全防護，其所訴求的重點是實際運作的資訊系統本身的安全防護，如存取控制、入侵偵測等議題。 2.「應用安全」(Application Security)，乃指合法客戶在授權範圍內的資料加密與身分認證等機制，其所訴求的重點是資料本身的加密機制與身分認證，透過認證中心Certificate Authority (CA)，做爲統一標準的認證單位，在應用

10 樊國楨、徐鈺宗、楊仲英、李孝詩，「美國聯邦政府資訊安全管理系統稽核作業與相關標準初探」，2004年10月。

11 IBM, IBM Data Security Support Programs, 1984.

12 黃亮宇，《資訊安全規劃與管理》，松岡電腦叢書，臺北，1992年。

13 Parker D.B.,“Information Security in a Nutshell,” Information Systems Security, Spring, 1997.

		上包含虛擬私有網路Virtual Private Network(VPN)及公開金鑰基礎建設Public key Infrastructure (PKI)等安全機制。 3.「資訊安全管理系統」(ISMS)，其乃指企業全方位觀念的資訊安全推動，包括如資訊安全政策，人員、實體與環境的安全、電腦與網路管理、系統存取控制、系統開發與維護、業務永續運作規劃、政策法規遵行等。
2003	朱延智[14]	資訊安全是企業安全之母，在數位時代沒有資訊安全，就等於整個企業是建築在脆弱的基礎上，是經不起考驗的。企業面臨資訊安全方面的挑戰，包含病毒攻擊、駭客入侵等的威脅。
2005	ISO/IEC17799 : 2005[15]	1. 確保資訊資產達成以下的特性 機密性(Confidentiality)： 確保資訊的存取或作業皆經授權。 完整性(Integrity)： 確保資訊與處理方式的正確性與完整性。 可用性(Availablity)： 確保獲得授權的使用者在有需要時，可以取得資訊及資源。 2. 藉由防範資訊資產遭受各種安全威脅，以達到企業持續經營，企業損失減至最小，投資報酬率及商機增至最大。
2007	國家標準 CNS27002[16]	使資訊不受廣泛的威脅之保護，以確保營運持續性、降低營運風險至最低、得到最豐厚的投資報酬率及最大商機。

資料來源：本研究整理，部分摘自盧興義，2004年[17]。

資訊安全管理系統(Information Security Management System, ISMS)的定義是，運用系統方法對組織敏感資訊進行管理，涉及到人、程序和資訊技術系統(BSI)。資訊安全管理系統之標的在於：「從確保資訊資源的合法存取，到在所有可能遭受資訊攻擊之階段，提供完整、未中斷的資訊系統運行」。

㈢全球資訊安全事件

根據賽門鐵克公司統計，2007年收到的惡意程式威脅數量多達711,912件，這個數值是2006年的6倍，更是2002年的110倍。（如圖1）

另外從圖2可明顯看出全球經回報的資訊安全事件，自1997年開始向上攀升，尤以1998年至1999年的164%的成長率為最高，同時自1997年至2002年已成長38倍之多。

資訊安全事件如此快速的增加，突顯出整個資訊環境的改變後，所衍生的管理議題尚未被充分注意，導致資訊安全事件發生的可能性居高不下，亦即企業管理的風險相對升高。

㈣推行資訊安全的障礙

資訊安全管理議題雖已被重視，但資訊安全事件的成長量，顯示仍有許多企業尚未成功有效地推行資訊安全管理制度，而主要無法落實的原因有缺乏專職人員、知識及訓練與經費不足（如圖3及表4）

二、各國資安管理現況

14 朱延智，《企業危機管理(Business Crisis Management)》（臺北：五南，第二版，2003年）。

15 同註9。

16 資訊安全管理標準(ISMS)-CNS 27002標準介紹，經濟部標準檢驗局。

17 盧興義，《危機管理在資訊安全上之研究—以防範「組織內部人員不當竊取」為例》（大葉大學事業經營研究所碩士論文，2004年）。

㈠全球資訊安全市場

研究機構臺灣IDC[18]預估，全球市場2010年將成長至15,000億美元，從資料顯示2003年的資安市場規模已超過140億美元，2008年更成長至421億美元，為2003年的3倍。（如圖4）

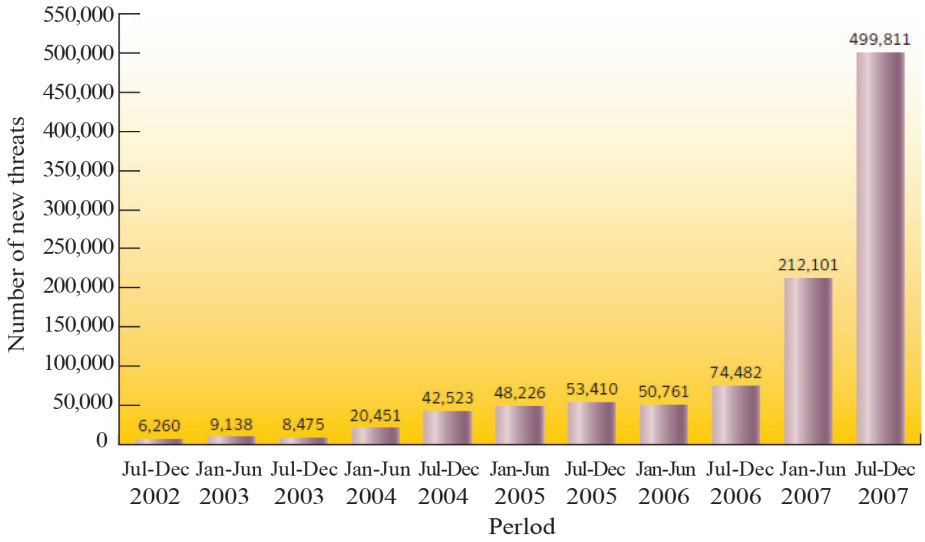

圖1　2008惡意程式威脅報告數量統計圖

資料來源：賽門鐵克公司[19]。

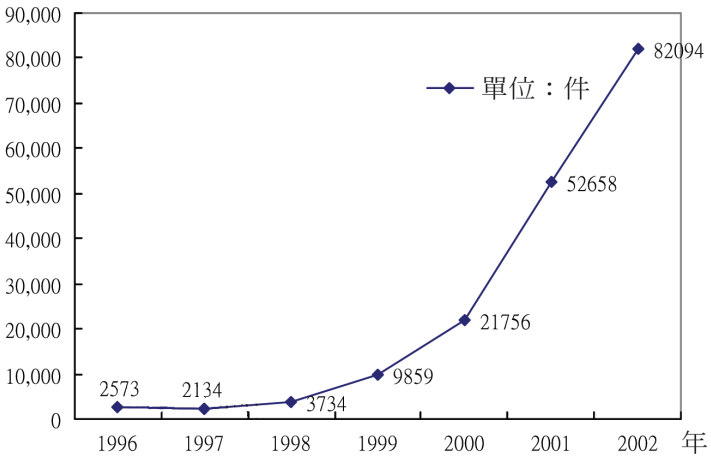

圖2　全球經回報的資安事件

資料來源：CERT/CC，資策會MIC整理，2003年2月[20]。

㈡國際標準規範ISO17799

ISO17799是從BS7799發展而來，BS7799是BSI（The British Standards Institution，英國標準協會）邀集業界相關領導廠商，為共同追求國際性品質的資訊安全管理系統所共同開發而成，可適用於各種產業與組織，是一個包含了各面向的企業資訊安全管理標準。

國際標準組織(International Organization for Standardization, ISO)於2000年底為提供一套能供全球依循的資訊安全控管標準，乃將BSI所制定的BS7799「資訊安全管理實務準則」的第一部分納入世界標準，

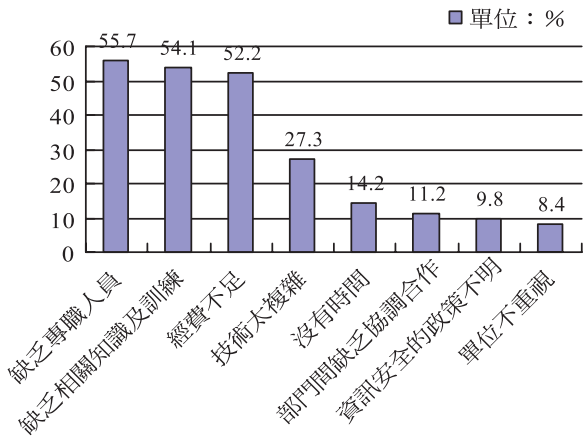

圖3　落實資訊安全的障礙（整體）

資料來源：資策會MIC整理，2002年12月。

18 臺灣IDC（國際數據資訊），http://www.idc.com.tw/about/detail.jsp?id=ODQ=，<Accessed, Dec/2009>。
19 賽門鐵克公司，whitepaper_internet_security_threat_report_xiii_04-2008.en-us, p46。
20 因資安數量事件統計於2009年後即屬於機密，故引用2003年資策會統計數據。

表4　落實資訊安全的障礙（依行業別區分）

	政府單位	金融業	製造業	服務業	醫療機構
缺乏專業人員	61.3	56.8	41.0	20.0	72.2
缺乏相關知識及訓練	60.7	50.0	36.5	30.0	52.8
經費不足	61.3	29.6	43.6	18.0	58.3
技術太複雜	30.3	27.3	23.1	14.0	25.0
沒有時間	15.8	6.8	12.8	4.0	25.0
部門間缺乏協調合作	10.0	15.9	12.8	10.0	16.7
資訊安全的政策不明	11.3	4.6	15.4	8.0	0.0
單位不重視	7.1	9.1	15.4	2.0	19.4

資料來源：資策會MIC，2002年12月。

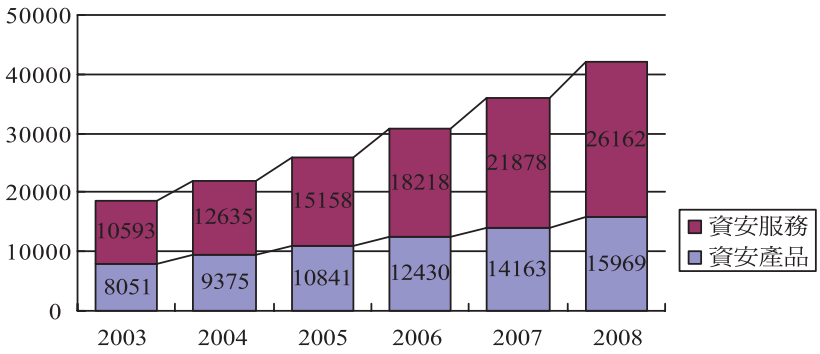

圖4　2003-2008年全球資安市場規模

資料來源：IDC，資策會MIC整理。

編號為：ISO/IEC 17799: 2000 (Information Technology-Code of practice for information security management)—資訊安全管理作業要點，包括領先企業提出的相關指導和建議。根據美國標準和技術國家機構(The National Institute of Standards and Technology's; NIST's)對ISO 17799的詮釋：「ISO/IEC 17799是個實施要則(code of practice)，提供了資訊安全管理的指導綱要(guidelines)和內發性指引(voluntary directions)。其針對在工作領域上重要的各項前引(initiating)、導入(implementing)或維護(maintaining)提供了高質、通用的敘述，在企業組織內的資訊安全管理。這文件目前並不能涵蓋所有的重要區域但仍持續更新中」。

2005年，國際標準組織從整體架構調整、條款呈現方式、調整控管措施結構安排、調整控制目標與控制措施之分類與從屬關係、考慮適用範圍修改條款用字、因應新的IT技術增加新控制措施及因應網際網路的趨勢修改控制措施用語等方向進行改版。改版後的內容為ISO17799: 2005包括了11大管理要項（如圖5）、38個執行目標與135種管制方法，可針對個別組織的實際「需求(Need)」，提出需要執行的「控制項目(Security Controls)」，提供資訊安全控制措施說明，做為建立ISMS (Information Security Management System)控制措施的參考。[21]

21 同註9。

圖5　ISO17799的11大管理要項

其認證標準的方法則為ISO27001:2005，包括組織資訊安全管理系統建立、實施和維護的要求，為資訊安全管理系統的評估基準。

㈢全球資訊安全認證與評鑑情況

全球截至2010年1月通過國際標準組織認證的情況如表5，從各國通過認證數來看，在日本、英國及印度等國家取得國際標準的認同較明顯，而其他國家則相對較不顯著。

美國自2000年起，開始資訊安全評鑑工作，並規劃確實可行之認證和認證過程方法。由於美國另外訂定自己的規範NIST800-100，[22]使得表5中，美國的ISO認證數偏低。

資訊安全管理系統導入後，尚需依PDCA的模式進行週期性持續的管理，而稽核是維持與改善資訊安全管理系統有效性之關鍵，因此稽核的相關議題仍然持續被關切。[23]

㈣國內目前概況

管理雜誌2004年2月的封面主題，以相當令人震驚的標題「不重視資訊安全，不配當主管」，提醒主管應正視資訊安全的相關問題；[24]資安人2009年5月也提到「部會首長應重視資訊應用、資訊安全」，而除了重視之外，還應有行動實踐。[25]

行政院於2001年正式設立國家資通安全會報，肩負起政府資通安全防護工作的推動，在第一期(2001～2005) 4年中，已針對

22 NIST Special Publication 800-100 Information Security Handbook: A Guide for Managers, P.94.

23 盧興義、徐鈺宗、楊仲英、李孝詩，「美國聯邦政府資訊安全管理系統稽核作業與相關標準初探」，2004年10月。

24 楊迺仁，「不重視資訊安全、不配當主管」，管理雜誌，2003年，第356期。

25 何依玟，「部會首長應重視資訊應用、資訊安全」，資安人63期，2009年5月。