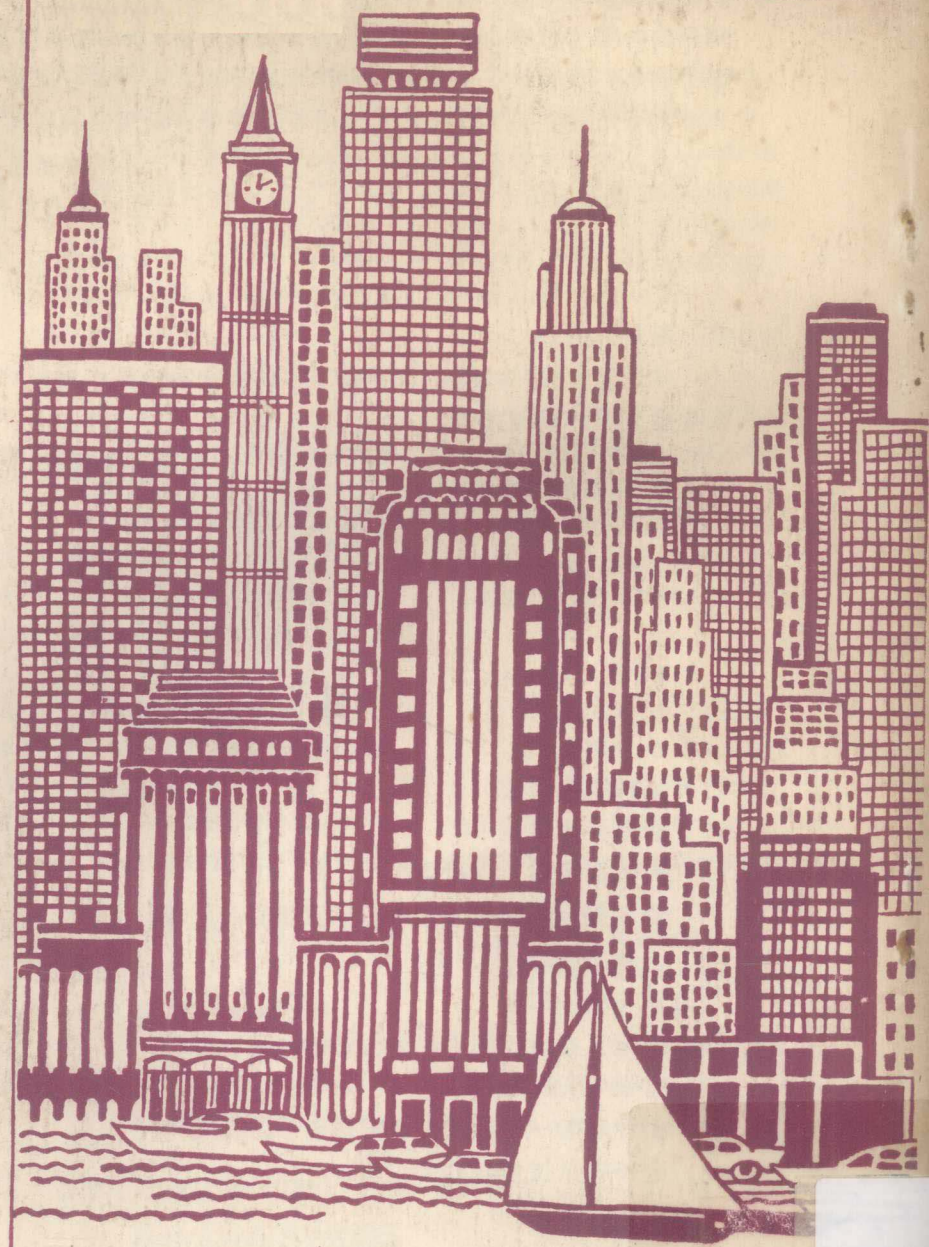
信息学（情报学）

台港及海外中文报刊资料专辑

第 1 辑



书目文献出版社

出版说明

由于我国“四化”建设和祖国统一事业的发展，广大科学研究人员，文化、教育工作者以及党、政有关领导机关，需要更多地了解台湾省、港澳地区的现状和学术研究动态。为此，本中心编辑《台港及海外中文报刊资料专辑》，委托书目文献出版社出版。

本专辑所收的资料，系按专题选编，照原报刊版面影印。对原报刊文章的内容和词句，一般不作改动（如有改动，当予注明），仅于每期编有目次，俾读者开卷即可明了本期所收的文章，以资查阅；必要时附“编后记”，对有关问题作必要的说明。

选材以是否具有学术研究和资料情报价值为标准。对于某些出于反动政治宣传目的，蓄意捏造、歪曲或进行人身攻击性的文章，以及渲染淫秽行为的文艺作品，概不收录。但由于社会制度和意识形态不同，有些作者所持的立场、观点、见解不免与我们迥异，甚至对立，或者出现某些带有诬蔑性的词句等等，对此，我们不急予置评，相信读者会予注意，能够鉴别。至于一些文中所言一九四九年以后之“我国”、“中华民国”、“中央”之类的文字，一望可知是指台湾省、国民党中央而言，不再一一注明，敬希读者阅读时注意。

为了统一装订规格，本专辑一律采取竖排版形式装订，对横排版亦按此形式处理，即封面倒装。

本专辑的编印，旨在为研究工作提供参考，限于内部发行。请各订阅单位和个人妥善管理，慎勿丢失。

北京图书馆文献信息服务中心

目　　次

（下转封三）

资讯与社会发展

信 息 学（情 报 学）（1）

——台港及海外中文报刊资料专辑（1986）

北京图书馆文献信息服务中心剪辑

书目文献出版社出版

（北京市文津街七号）

北京百善印刷厂印刷

新华书店北京发行所发行　　各地新华书店经售

787×1092毫米　1/16开本　5　印张　128　千字

1987年3月北京第1版　　1987年3月北京第1次印刷

印数1—4,000 册

统一书号：7201·101　定价：1.30 元

〔内部发行〕

專題

資訊科技展望

祁倫

自從政府將資訊科技（Information Science and Technology）列爲我國的重點科技，將資訊工業（Information Industry）列爲策略性工業後，政府的科技部門、各大專院校、研究機構、電腦廠商、大衆傳播媒體，莫不全力參與，國人也逐漸體認到電腦處理資訊的重要性而紛紛學習電腦及購置電腦，顯示出全民動員迎接即將全面來臨的資訊時代，爲我們的工農商業和衣食住行育樂等的邁向電腦化和自動化，興緻勃勃的各自投下自己的心力。

尤足欣慰的，海外中國人的爲求加速祖國順利邁進已開放國家之林，個別的或集體的提供了自己所學，貢獻出自己的才能而不計報酬。以「1984年北美華人學術研討會」對資訊科技與自動化（Automation）言便提出了下列項目的具體作法之寶貴建議——

⑴電腦輔助教學（Computer Aided Instruction）；

⑵電腦教育（Computer Science Education）；

⑶電腦網路（Computer Network）；

⑷電腦繪圖（Computer Graphics）；

⑸個人電腦與地域網路（Personal Computer and Local Area Network）；

⑹微處理機（Microprocessor）；

⑺記憶與邏輯技術（Memory and Logic Technology）；

⑻儲存技術（Storage Technology）；

⑼超大型積體電路技術（VLSI Technology）；

⑽設計自動化（Design Automation）；

⑾輸出輸入技術（Input/output Technology）；

⑿電腦輔助設計與製造（CAD/CAM/CAT（CAE）；

⒀機械人學——硬體與軟體（Robotics-Hardware and Software）；

⒁感應器（Sensors）；

⒂彈性製造系統（Flexible Manufacturing Systems）；

⒃整合製造系統（Integrated Manufacturing Systems）；

⒄自動製造系統（Automated Manufacturing Systems）；

國內資訊科技的研究

民國68年通過的「科學技術發展方案」，指定資訊科技爲重點科技，由行政院資訊發展推動小組，研訂有關政策與輔導措施，推動政府機關及公營事業實施自動化作業；協調國內各有關機構及業者推動硬體及軟體工業之發展；制訂資訊處理規範、中文配合標準；建立國內國際數據交換網路，促進國內資訊傳輸工業之發展；加强中小型電腦、週邊設備及軟體系統的研究並發展產製；簡化電腦資料及電子零件進出口的管制及手續；蒐集國外軟體發展趨勢等資料，協助國內軟體工業開發國外軟體市場；加强各級學校資訊教育，並辦理推廣教育與技職訓練（包括培育資訊師資，養成各級資訊工作人員的專長移轉訓練等）。

一、研究發展體系

國內資訊科技研究發展體系，在基本理論研究方面，係由中央研究院資訊科學研究所，及各大學院校配合工業發展長程目標進行之，各院校依特性作重點性分工。

在應用技術研究與產品原型結構，則由研究機構進行。譬如⑴工業技術研究院電子工業研究所從事微型、迷你型電腦與週邊設備硬體與軟體系統的發展，及電腦輔助設計與製造的研究；⑵資訊工業策進會的對軟體系統發展方法的研究、軟體工具的開發、管理資訊系統的發展、以及應用系統分析的研究；⑶交通部電信研究所則負責電腦與通信結合的研究；⑷中央研究院資訊研究所及各大學院校相關研究所的各就其特長方面的研究。

上述研究體系，迄今尚無協調各單位對資訊科技作有系統發展的正式機構，以致各單位的各自爲

政，彼此間的研究項目、研究成果、人才及設備等均無法有效溝通。

二、人才培育

經由學校教育、推廣教育、技職訓練的培育高、中級及基層資訊人才，就量而言，頗爲可觀；就質而言，則亟待提高。僅以學校教育來說，目前設有電腦及資訊研究所者，計有台大、清大、交大、成大、工業技術學院、中興、淡江、中央、中原共9所大學院校，前5校設有博士班，共計培育碩士以上資訊人才1,800人以上，目前研修博士及碩士學位者近1,000人。此外，在公私大學院校中，設有與電腦及資訊相關學系者有11所大學，2所學院及中央警官學校，共計畢業資訊人才近14,000人，目前在校學生超過5,000人；另有18所工專及5所商專，已畢業的電腦或資訊相關科組學生20,000人以上，在校學生約12,000人。

但是，大學院校及專科學校的資訊電子師資極爲欠缺：大學中專任教師每班平均僅2.08人，距教育部規定的每班4人相差很多；大學內專任教師中，講師以上者平均每班僅1.51人；大學內可擔任指導研究生的副教授以上師資，更少至平均每班僅0.94人；專科學校講師以上的專任教師，平均每班僅1.03人。而且，各校所擁有的教學用之電腦設備，至今仍以小型及其以下者居多。以如此嚴重缺乏的師資及簡陋的設備，便難以培育高素質的資訊人才。

三、延攬國外人才

爲配合研究發展與教學的需要，國科會特訂有「延攬國外人才回國服務」及「補助海外國人回國教學研究」處理要點兩種。前者主要爲：(1)聘請國際知名學者專家回國在研究機構或大學，以「特約講座」名義，指導國內急切需要的研究；(2)延聘國外技術專家，以「客座專家」名義，回國解決國內急切問題或訓練急需人才；(3)延聘國外執教學者，以「客座研究教授」名義，短期回國指導研究或傳授新學術。

但是，上述延攬國外人才回國服務的辦法，由於其他種種因素及欠缺整體性有計畫的安排，回國人數不多，即使利用海外學人休假時間輪流回國指導的可行計畫也未釐訂，加上海外學人一片熱忱的獻言與建議未能貫澈，所以延攬人才回國支援國內師資缺乏與指導研究的成效不彰。因此，國內資訊主管、系統分析師、應用程式師、系統程式師、硬體工程師等人才嚴重缺乏，資訊專業人才、資訊師資養成、資訊專業人員技術提升等教育訓練難以推展。

四、智慧型工作站

爲配合我國下一代電腦的發展滿足未來資訊處理需求，行政院國科會頃已決定投資3億元台幣，在今後5年內，推動包括電腦硬體系統、軟體工程、智慧型介面、專家系統、人工智慧、電腦網路、高階語言處理機、中文語音辨認系統、光纖區域網路、知識庫管理系統在內的「智慧型工作站」大型研究計畫，也就是美、日全力發展中的「第五代電腦」或稱「下一代電腦」，是舉世注目的大事。

展望國內此一大型研究計畫，筆者並不樂觀。因爲，除研究經費及參與人才與美、日有一大段距離外，整個基礎條件也很欠缺。譬如：微電腦及迷你（小型）電腦硬體技術與若干週邊設備硬體技術、電腦網路硬體技術迄今仍未完全掌握；大型電腦硬體的研究發展因需巨額投資尚待起步；國內大學院校間及研究機構間的電腦網路沒有建立；系統分析與設計方法以及相關規格標準等也有待建立；配合國際標準的中文（包括簡體字）電腦尚待開發；軟體工程技術及軟體工具發展基礎也未紮實；……在這情形下欲求順利發展智慧型工作站幾乎不可能！更何況，國內的資訊既欠缺又凌亂，如不速謀改善，及建立國內整體資訊系統，則國內的資訊科學研究便難望有所突破性成就。

國內資訊工業的回顧與展望

資訊工業是一種結合電腦與資訊的腦力與技術密集的工業，附加價值極高，應用範圍極廣，需要全民的參與，才能全面提高生產力、增進社會民生福利、以及加速國家現代化。以下除概述資訊工業的範圍及發展現況外，並就個人所見作一展望。

一、資訊工業的範圍及功用

結合電腦與資訊的資訊工業，涵蓋了(1)包括電腦硬體及軟體與其相關設備和零組件的生產銷售之「電腦業」；(2)包括應用軟體的設計、建制與維護

的「軟體工業」（Software industry）；⑶運用電腦及相關設備，提供資料處理服務的「資料處理服務業」（Data Processing Serice Industry）；⑷提供科技及情報等各類資訊服務的「資訊服務業」（Information Supply Service Industry）。

資訊工業又稱腦力密集工業，它極其快速擴大其用途，改善人民生活，提高文化水準，增强生產力，減省了人力、降低成本而品質不斷提高；它那能以極短時間從繁雜資料中找出所需資訊的「資訊檢覆」（Information Retrieval），及能從複雜現象中抽取單純資訊俾供所需的「圖形辨認」（Pattern Recognition）等功能，經由通信網路及資訊（電腦）網路，快捷而正確運用後所產生的「資訊社會」（Information Society）使資訊工業得以應用到人類生活及各種活動的每一部門，從工業自動化到家庭自動化！

二、我國資訊工業發展現況

因爲資訊工業直接關係國計民生，所以政府於民國 70 年選定我國策略性產業，獎勵與協助業者——

＊加强研究開發電腦製造及應用技術包括週邊設備。

＊協助引進技術及購買外國資訊有關設備及管理方法。

＊發展國內數據通信、開發數據電路交換式網路、分封式交換，以配合分散式處理與電腦網路發展趨勢的需求。

＊健全資訊設備租賃業的發展，減輕資訊設備使用者資金負擔。

＊積極發展高層次、高技術的半導體、電子、電訊等。

＊統籌規劃政府和民間各部門的整體管理資訊系統，加速推動各部門電腦與資訊的有效運用。

此外，經建會委托資訊工業策進會積極推展——

＊搜集資料，進行調查，向政府及工業界提供研究發展本國資訊工業之報告建議，協助政府擬訂短中長程發展計畫；並對政府、公共事業、工商業界提供服務，及建立其所需的電腦應用系統。

＊協助訓練電腦技術與管理人才；引進技術建立軟體設計能力；協助推動改善工業結構。

＊聯繫工業技術研究院推廣國內工業製造能力。

＊設立高級資訊人力訓練中心，並建立資訊人力資格檢定制度，劃一並提高資訊專業技術水準。

＊致力研究微電腦系統與技術，鼓勵投資製造終端機、ＥＰ表機、線式掃描繪圖機、光學閱讀機等。

＊統籌規劃大型軟體系統；成立資訊處理規範制定小組；推動研究軟體系統發展方法；國內外軟體市場調查；指定專責機構負責軟體的引進、改進、設計及推廣等資訊處理業之發展。

在政府領導及民間熱烈參與下，我國資訊工業發展頗爲快速、迄至筆者爲文，其重要成就計有——

＊業者數目：現有資訊工業製造廠商 176家（不含零件製造商），包括電腦及相關設備製造、週邊設備製造、資料處理、資訊服務業、軟體系統設計和資料登錄等。

＊資訊產品銷售：除內銷外，我國資訊產品外銷年成長極爲快速，1984年外銷金額幾超越紡織而躍居首位，但1985年起則呈現負成長。外銷主要爲電腦週邊設備如終端機（Terminal）、列表機（Printer）、磁碟機（Disk drive），其他爲零組件、微電腦、小型電腦、以及大型電腦零組件等。

＊軟體技術：已完成微電腦系列的監督程式、編校程式、連結程式、作業程式、組合程式、小型電腦系列的核心程式、系統指示、檔案系統、監督控制台式數種編譯程式、即將分工操作系統（用於小型電腦作爲工業控制應用的核心操作程式）等，及包括製造業、電腦輔助教學、貿易業、會計用、紡織業、校務用、工商用、商業用、醫療業、人事管理、家庭用等各類個人電腦中文套裝軟體等。

＊大型電子研究計畫：這是以積體電路電子材料與微處理機之設計、研製及應用爲主的計畫，刻由台大、交大、清大、成大四校合作進行中。

＊超大型積體電路：政府過去投資積體電路研究發展均達預期效果，頃又決定發展超大型積體電路，以强化國內半導體工業，結合半導體技術與其他工業以加速工業高級化創新特殊產品，提高產品競爭力與附加價值。

＊電腦通信網路：已由電信總局數據通信所裝

妥並擴大應用中，同時又據此擴展爲國際性電子數據交換網路，俾提供更爲快捷便利直接的電腦通信服務。

展望(結論)

未來資訊科技，必將走上將無線電、雷達、電話、電視、衛星與光纖通信、儀器、機械人、電腦等科技予以「整合」(Integrated)在一起；未來的資訊處理，是朝向「資訊遙控處理」(Information teleprocessing)，這是通信網路與電腦網路的大結合，人類將不論遠近而直接溝通及處理事務，這將影響人類的家庭與工作；未來工業生產必將全自動化，其他事務也將邁向自動化；未來資訊及產品與服務必將趨向個人化；各類的機械、工具、儀器等也將趨向聲控化(人類直接利用說話來操作)；家用電腦與家庭電腦化是必然趨勢；未來的電視機，必將配有鍵盤、微電腦、磁碟機以擔任娛樂、資訊終端機、資訊展示、尋取所需商情及科技等資訊與電讀的新聞和數學節目等；未來的資訊中心將如今日的電話亭，提供文字、圖形、聲音等資料；隨著掌上型計算器與掌上遊樂器的出現，未來將有更多掌上測量儀器、診斷器、教學器、以及與電腦通信網路連接在一起以獲取個人所需資訊；……

總之，未來資訊科技工業的發展，其觸角是全面的，影響是深遠的，這也就是所謂資訊時代。

面對此一必將到來的資訊時代，如何推動資訊科研及資訊工業的發展，有關部門必須速謀有效對策。以外，謹提出個人數點淺見——

＊設立全國性資訊科研的專業權力機構。

＊設立全國性資訊工業的專業權力機構。

＊籌訂整體計畫，分工合作避免浪費。

＊優先研究發展項目的短中長期目標之確定。

＊儘量縮短從研究發展到生產及開拓市場的時程。

＊研究成次與產品品質須不斷提高並力圖搶先推出。

＊政府的輔導方法及輔導重點之執行工作應再予加强。

＊政府應增撥研究經費，加速解決資訊師資、資訊高級人才、資訊專業人才的嚴重不足問題。

＊修改相關法令規章及制度以利資訊科技的發展。

＊資訊工業及資訊本身標準化須即制定並使於國際標準相配合，及成立全國性專業機構負責。

＊國內現存小型廠商應速謀合併爲中型並邁向大型化。

＊政府須加强投資軟體，並擬定具體可行的各種獎勵辦法與採購計畫。

＊政府應出面協調、輔導軟體業者，促進軟體業者分工合作以發揮各自所長，減少惡性競爭。

＊獎勵民間企業研究發展，設立研究發展基金。

＊訂定長期關稅調整時間表俾利工業投資。

＊成立專業機構調查國外市場、蒐集國外資料。

＊建立全國性完整的中間銷售網，避免仿冒及減少惡性競爭。

＊降低有關資訊產品貿買的關稅以加速國家資訊化。

＊擴大資訊週爲資訊月及國際性研討會以推廣觀念。

此外，經建會釐訂的資訊工業部門 10 年(至 1989 年)發展計畫的積極推動，及有關部門的密切配合與工商企業界的熱烈參與尤爲重要。如該計畫中所訂發展策略的——

＊在計算機製造業發展方面的(1)積極推動國內微型及迷你型電腦系統之發展；(2)鼓勵業者投資製造策略性產品；(3)政府採取投資獎勵配合措施。

＊在資訊處理業發展方面的(1)輔導國內資訊處理業的發展，以政府電腦作業委予承攬；(2)資訊處理規範工作小組蒐集並制訂軟體、硬體、資料與作業等規範；(3)推動研究軟體系統發展方法並將研究成果提供業者參考採用；(4)資訊工業技術與市場資訊服務中心的加强提供業者與使用者各類資訊服務；(5)鼓勵各專業機構引進、修改、設計與推廣套裝軟體，並立法保障其權益。

＊在財稅金融政策的配合方面種種措施之加强。

＊在人力與教育訓練方面尤須充實學校教育的資訊師資與設備，及增設資訊技術訓練中心以加速中、高級資訊人才的在職訓練。

果能如此，則我國的資訊科研、資訊工業、以及全面資訊化社會，便具有一個堅實的全面開展基礎了。

(原载：橡胶工业〔台〕1985 年 9 卷 10 期 33 — 36 页)

資訊系統安全政策簡析

工業技術研究院院部
樊 國 楨

一、前言

電子計算機是二十世紀最重要的發明，其與通訊的結合，將在這個世紀的末期和未來的二十一世紀使人類眞正感覺到他的震撼。過去，電子計算機只是專家和實驗室的專利品，隨著電子技術的爆炸性成長，它已經對工商活動產生了鉅大的影響，如何利用電子計算機改善我們的工作、降低成本、促進效率…使得它成爲未來工商環境中的希望泉源。在另一方面，人們也逐漸警覺到，電腦犯罪（ Computer Crime ）在這個眩目的計算機與通訊時代來臨時造成的新的威脅。

在近年來的廉價個人電腦（ Personal computer）的日益普及和可以利用遠地端末機，不需進入電腦室就能取用電腦資訊的數據通訊網路的設立，更使得電腦犯罪的問題益形迫切。譬如，現代電子計算機連線作業的影響力量已經擊潰了傳統的防止錯誤和舞弊發生的會計查帳稽核技術〔1〕。現在的電子計算機能夠同時處理許多工作及利用通訊設備可以讓使用者從遠地接通電腦分享其資源，因此，讓一些原本無權取得某些資訊的人，現在有更多的機會，故意或無意的取得資訊。這些均造成新的資訊安全與管理體制的複雜問題。

根據美國Business Week 雜誌〔1〕於1981年所公佈之資料顯示，美國每年的電腦犯罪，包括公開的與未公開的犯罪資料，所引起的財務損失可能達30億美元之多，相當於美國在1980年所有的銀行被搶劫（約 4 仟萬美元）總數的75倍以上，相當驚人。

上述電腦犯罪的一個主因是由於訊息之電子化。因爲訊息電子化後，當資料儲存於共用之媒體（ Medium ）時，容易爲電腦有關工作人員（ 如業務人員、經理、系統工程師、系統分析師、程式設計師、操作員、資料管制員等人）或連線（ On Line ） 之終端機（ 包括微電腦系統）使用者（ 包含合法與不合法）等人所擷取或更改；或者當工作人員利用有線電或無線電方式來傳遞訊息時，亦容易爲電腦犯罪者所擷取或更改。根據〔1〕知，當訊息在傳遞過程中，如果資料未經過安全之處理時，任何人只要購買約1000

美元之設備，包括一個無線電麥克風，一部AM－FM收音機，一個MODEM，與一部美國TI公司所生產的753型可印表式電腦終端機（Printing Computer Terminal）即可輕易獲得或更改所傳遞之電子訊息內容。這種新的犯罪方式已嚴重的影響到正常的工商運作，如何及時防制，已成爲資訊時代工商社會新的威脅及隱憂。

我們要怎樣的針對這些問題來設法解決，首先要有資訊系統安全政策，一般來說，政策（Policy）是一切管理作爲的原始依據；所謂政策，簡單的說，就是目標和原則；目標指引群體努力的方向，原則則規範管理的行爲。由於目前的電腦系統本身並未具備妥當的技術保護措施；同時，根據實務經驗的資料顯示，管理因素往往是資訊系統安全制度成功的關鍵所在〔2〕、〔3〕。資訊系統安全政策（Information System Security Policy）之重要性逐漸爲人們所肯定。

在本文之中，我們將從管理和技術的觀點，來討論電腦服務所遭受的威脅、資訊系統的弱點、管理部門的責任以及如何建立完整的資訊系統安全政策規畫。

二、電腦服務的威脅

要進行電腦安全規畫，首先要找出其所受的威脅。一般而言，這些威脅，大致可以分成六類：

1. 實體損毀。
2. 資訊損毀。
3. 妨礙電腦對他人的服務。
4. 偷用電腦的服務。
5. 偷取資訊。
6. 竄改資訊。

在1976年到1978年之中，義大利恐怖組織—赤軍旅（Red Brigade）在兩年之內，燒掉或炸掉了七家公司、兩所學校及一政府機構的電腦中心造成千萬美元以上的損失。我國財政部國貿局的電腦中心亦曾遭回祿之災。這些都是實體損毀的例子。

去年外交部電腦操作員塗銷一千餘件護照資料。1971年一家法國公司的職員因爲偷用電腦處理私人帳務，因而被解雇，兩年後的元月一日，這家公司的所有資式被這個職員所留下的一個木馬計（Tiojan Hourse）〔4〕程式自動銷毀，損失不訾，這些都是資訊損毀的例子。

我們很容易採取某些行動使得電腦無法運行，而使其他使用者受到妨礙；一般而言，造成系統故障（System Crash）；或是設計一個不斷要它去做非常耗時的工作，使得它的服務和回應變的拙劣而嚴重影響其效能均是簡單的工作。如何根據上述原則，運用其智慧與技巧，可以創造成無限多的變化，使人防不勝防。

1982年，美國某一學校職員因偷用學校電腦來貯存其私人飼養賽馬之資料被移送法

辦，這是典型的偷用電腦服務的例子。有趣的是此一職員因爲法官尚未找到任何美國禁止此種未經授權而使用電腦系統的法律，認定此一行動並非罪行也無須判刑。

去年台灣彰化銀行職員利用電腦連線機會幫朋友調頭寸。1979年到1981年之間，一位日本電腦公社的工程師，非法與北海道銀行之通信系統連線，偷取其自動存款機資料，複製在磁卡上，用以盜取他人之存款。這些均是偷取資訊的例子。

竄改資訊的例子更是比比皆是，1982年美國某大學學生在以一微電腦與學校之電腦系統連線後擅自更改自己的化學成績而被捕後，表示在同學之中利用微電腦偷窺成績檔案是極爲平常的行爲…。這項威脅的最大隱憂是往往沒有辦法分辨資料是否被改過了。

上述的六類威脅，從另一個角度來看又可以成〔5〕：

1 蓄意的威脅。

2 意外的威脅。

二類。

蓄意的威脅可以分爲下列幾種：

①偷窺（Browsing）：合法的使用者在未經授權的情況下想接觸資料、程式等。

②僞裝（Masquerading）：未經授權的使用者想要冒充經授權的使用者。

③線間介入（Between-Lines Entry）：當一侵入者和一認可的使用者在同一通信線路上，但該經認可的使用者的端末機是在靜止狀態時；藉著同一條通信線上特別加裝的端末機，侵入者能銷案（Sign-off）該經認可的使用者，而冒充他以取得所要的資訊。

④背肩介入（Piggy-back entry）：在與線間介入相類似的情況下，唯侵入者此時還想經由冒充認可的使用者與系統的對託裡，加入、改變、或刪掉某些資訊，甚至毀掉整個資料庫。

⑤愚弄（Spoofing）：使用者與電子計算機間的通信線路被攔截了，導至使用者被愚弄；他以爲自己是在和電子計算機交談，而事實上的對象却是侵入者；因此，給了侵入者許多資訊。

⑥暗門介入（Trapdoor Entry）：利用原本供系統本身，或是偵測修護用所特設的暗門，來取得資訊。

⑦開接攻擊（Indirect Attack）：包括修改從製造商處來的系統程式或文件，以及假造更新的資料等各種行爲。

⑧竊聽（Bugging and Wiretapping）：任何已知的竊聽方法都可以從電腦通信線上偷取資訊。

⑨員工：根據以往之資料，百分之九十以上的電腦犯罪，都是組織內部員工的行爲，所有合法的使用者、操作員、安全人員…等，都該被考慮爲潛在的安全威脅者。

至於意外的威脅又可以分成：

①硬體的失誤。

②軟體的失誤。

③使用者的失誤。

三種。我們在下一節，資訊系統的弱點中一併討論。

由本節的討論，我們可以認爲資訊系統安全的目標包含下列三項：

1. 防止天然或人爲的破壞資訊安全。
2. 防止非法利用資訊資源（即爲防止狹義的電腦犯罪）。
3. 防範因人爲疏忽或制度不健全所造成的錯誤處理。

而如何解決因訊息電子化而產生的僞造、背信、辨認、偸窺等四大問題，是遏止電腦犯罪的技術難題。

三、資訊系統的弱點

各個資訊系統的弱點，隨著時間、地區、行業、型態、所提供的服務，以及系統裡所有的資料的敏感度，而有所不同。在本節之中，我們僅就下列四方面來考慮：

1. 實體的考慮。
2. 硬體的考慮。
3. 作業的考慮。
4. 環境的考慮。

在一個資訊系統實體的考慮中，我們首先要瞭解那些資源是需要保護的，一般而言，在一個資訊系統之中，需要保護的資源包括下列七項：

1. 人員。
2. 電子計算機及其週邊設備（Computer and Peripheral Equipment）。
3. 輔助設備（Support Facilities）。
4. 通訊設備（Communication Equipment）。
5. 資料媒體（Data Media）。
6. 圖書（Libraries）。
7. 文書（Documentation）。

在分析各種需要保護的實體資源的同時，必須考慮到這些資源萬一遭受破壞，應變計畫是否妥當，復元的能力如何等問題。以上是在實體上的考慮；接著，我們對硬體加以考慮。

電子計算機現行的主要產品，大都不能保護資訊；其中尤以遠地電傳處理的輸入／輸出裝置爲然。第三代電子計算機引進了許多新的功能，譬如同時處理許多工作（

Concurrent Processing ），遠地端末機的使用等。爲了提供這些功能通常利用監督方式（ Supervisor Mode ）以及用者方式（ User Mode ）或是稱爲系統方式（ System Mode ）以及問題方式（ Problem Mode ）來達成其目的。在監督方式裡有些特別的指令可以更改貯存方面的保護措施；或是有些命令（ Commands ）能允許直接控制輸入／輸出裝置。因此，必須嚴防使用者進入監督方式裡，以避免其有機會故意的或無意的取得其原本無權取得的某些資訊或是任意支配資訊資源。至於記憶體的保護雖有一些方法，然而在應用上仍有其困難〔6〕。總結來說，資訊系統硬體安全上的顧慮還很多；同時，專家認爲單靠硬體並不足以達到完全的安全，必須和軟體合併起來考慮，才有希望。

目前市場上所有的電子計算軟體，在系統功能上都無法保證能達到一個可靠的程度；事實上是，能被鑽透的地方太多了，美國空軍1972年的一項報告裡，曾把這些攻擊手法分成七類〔5〕：

1. 暗中分享（ Implied Sharing ）。
2. 清理（ Scavenging ）。
3. 不完全的參數檢查（ Incomplete Parameter Checking ）。
4. 異步干擾（ Asynchronous Interrupt ）。
5. 木馬計（ Trojan Horse ）。
6. 秘密改碼（ Clandestive Code Change ）。
7. 異步攻擊（ Asynchronous Attack ）。

上述每一種方法都可能讓未經核准的人意外的或是蓄意的接觸到私人的、有獨占權的或是機密的資訊。至於存取控制（ Controlled Access ）、認證（ Identification ）、監視（ Surveillance ）等軟體安全觀念，至今還無法提供完整的功能。

最後，我們從環境上來考慮資訊系統安全的問題。對一個資訊系統中資料的偷窺、僞造等行爲，因其不必將某物的實體携走，即使是對受過專業訓練的人而言，如何蒐證及具體證明某些罪行曾經發生，實在是一大難題。資訊系統處理的資料，數量相當龐大而電磁濃縮之資料，又不爲內眼所能見，實難以人工處理方式重覆檢驗；在另一方面，犯罪的時間可能祇有十分之一秒，又可不留任何痕跡，造成電腦犯罪的犯罪黑數（Dark Figure of Crime）偏高。再加上有關法律條文並不周全，且處罰太輕，實不易收效。因此，有賴於教育來發揮功能，從小培養國民對偷窺、僞造、背信等電腦犯罪的羞恥心，期使社會提供良好的資訊系統的安全環境。在另一方面，利用各種在職訓練以加强科技倫理、灌輸職業道德觀念及資訊系統安全偵測技術來防範電腦犯罪的發生。

對資訊系統之實體、硬體、軟體和環境這四方面的考慮，就此告一段落。下面，我們將從管理的觀點來討論資訊系統安全政策的問題。

四、資訊系統的安全政策

一般而言，討論資訊系統安全政策規畫的問題有二個方式；其一是列出所有可能的威脅，並針對威脅提出對策；另一個方式是以資料爲中心，訂定一個有層次性、周延性保護措施。事實上這二個方式是一體的兩面；首先，我們看一下後者——資料安全的說明性定義〔7〕：

「所謂資料安全，是指對資料的保護以對抗意外或蓄意的將資料暴露給無權知道的人、或無權修改的人、或無權破壞的人。

整個資訊系統的安全政策應該植基於上述的目的之上。要達到這個目的，我們必須瞭解資訊系統可能存在的各種威脅以及其技術上、環境上的弱點才能擬定恰當的保護措施。接著，我們爲資訊系統安全政策下一個說明性的定義：

「所謂資訊系統安全政策，是指爲防範意外或人爲非法使用或破壞資訊資源，而加諸於資訊系統（電子計算機與通訊網路）硬體、軟體，及資料上之特定技術措施及管理程序。」

由以上的說明可以知道凡是爲了追求下述目的：

1. 防止天然或人爲破壞資訊資源。
2. 防止非法使用資訊資源。
3. 防範因人爲疏忽或制度不健全所造成之錯誤處理。

而實施之任何管理性或技術性措施，均屬於資訊系統安全之範圍。

一般而言，資訊系統安全政策的規畫就功能上而言，應該涵括下列五項：

1. 杜絕性（Deterrence）功能規畫：長期性地防制犯罪及錯誤發生之可能性的計畫，譬如人員素質的改良、訓練，授權制度的改進等。
2. 防護性（Prevention）功能規畫：即一般的傳統性安全防護措施，譬如警衛、通行碼驗對（Password Authentication）、限制度控制、密碼轉換等。
3. 偵測性（Detection）功能規畫：前面提到的杜絕性功能規畫及防護性功能規畫主要是在於防止電腦犯罪的發生；在另一方面，如何發掘電腦犯罪的存在，同時從事後的補救工作，也是資訊系統安全政策中很重要的一環。其主要目的，就是留下使用者所有活動的記錄（Logging），希望及時測知進行中之不法或有害活動，譬如監視系統（Surveillance）、電腦稽核（Computer Auditing）技術及制度的改進等。
4. 復元性（Recovery）功能規畫：此功能是指防範任何資訊系統損毀時之復元能力，如離址備份儲存（Off－Site Backup）、替代系統之安排、保險額度的訂定等。
5. 更正性（Correction）功能措施：一旦偵知錯誤發生、即須有適當的處理程序，能

迅速查明來源及範圍以更正錯誤，譬如稽核尋跡（Audit Trail），檢查碼(Error Checking Code）技術等。

在實際執行的時候，資訊系統安全政策的規畫，應該包涵下列六項：

1. 實體安全（Physical Security）：防範之重點在於天然災害及外來入侵者之防護、偵測與復原；實施的重點是：
   (1)資訊系統位址的選擇（Site Selection）。
   (2)防水、防火、防震、防熱、防盜、防濕等之建築設計（Building Design）。
   (3)通路的管制以及全天候預警系統。
   (4)災害處理程序（Disaster Plan）的規畫與準備。
2. 硬體安全（Hardware Security）：防範的重點在於利用硬體設備防護記憶媒體、週邊設備等資訊資源；實施的重點是：
   (1)電力保護及復元系統。
   (2)利用界限暫存器使用法（The use of bounds registers）、鎖及鑰匙使用法（The use of locks and keep）以及附加控制位元於記憶體法（The use of access control bits in memory）來保護實記憶媒體（Real memory）。
   (3)利用虛擬地址（Virtual address）轉換成絕對位置（Absolute Address）過程所要經過的地址轉換表（Address Translation table）來保護虛擬記憶媒體（Virtual memory）。
   (4)利用通行碼驗對、鑰匙卡（Keycard）等認證端末機及其操作者的設備。
   (5)利用錯誤檢查碼、微處理器等以維護輸出入通道（I／O Channel）傳輸的正確性。
3. 通訊傳輸安全（Telecommunication）：防範之重點在於資訊系統傳輸網路中所可能產生的錯誤、干擾、僞造、偸窺、辨認等之防護、偵測與更正；實施的重點是：
   (1)備用線路之安排。
   (2)一次密（One Time Chiper）系統，譬如美國國家標準局核定的數據保密標準（Data Encryption Standard）系統（晶片）的使用。
   (3)公開鑰密碼（Public Key Encryption）系統的使用。
   (4)通訊協定（Protocols）系統的使用。
   (5)數值簽章（Digital Signature）系統的使用。
4. 作業系統安全（Operating System Security）：防範之重點在於所有系統程式、應用程式及控制台操作，制度未經核准的人（意外的或蓄意的）接觸私人的、有獨占權的或是機密的資訊、程式的防護、偵測措施；實施的重點是：

(1)存取的管制（Access Control），這是指資訊系統對每一個使用者均僅在其所被批准的範圍內允許其取用系統裡的資訊和資源。

(2)獨立（Isolation）設計，意指使資訊系統裡的使用者、資訊、以及資源安排有序，以防止任何使用者非法之侵擾（Violation）。

(3)辨認設計，資訊系統一定要具有辨認各個程式，和目前在使用的以及被要求使用的資源的能力。這些資源能從想使用它的使用者、程式和相關的資料檔等來加以辨認；同時，執行那些使用者有取用的能力，那些使用者沒有取用的能力，以及他們能力的限制，譬如讀、寫、更新等）。

(4)監視系統，資訊系統對所有需要保護的資源上發生的一切活動，特別是所有違反安全的行動。都必須留下記載和供稽核的路徑；同時，根據問題的嚴重性來採取適當應變措施。

(5)應用系統之發展、上線以及維護均需經一定之程序。

5. 資料安全（Data Security）：防範的目的在於保障各類原始資料、資料檔及資料庫的完整無缺之防護、偵測、復元與更正；實施的重點是：

(1)輸入的管制（Input Controls），利用各種資料之完整性驗證方法，諸如編輯程序（Edit Routines）、工作完成後的複查（Completeness Checks）、檢查號碼等方法查核輸入資料的正確性。

(2)輸出的管制（Output Controls），利用授權矩陣（Authorization Matrix）、比較輸出的總數（Comparing Output Control）、例外情形報告（Exception Reporting）等方法管制、查核輸出資訊的合法性及正確性。

(3)復員及儲存媒體的管制，資料檔、應用程式、系統程式均應備份儲存於機房、當地的檔案室、遠地的檔案室；磁帶、磁碟及程式報表均應由專人管理，訂定取用程序以及廢品管制程序。

(4)利用分區控制（Partitioned Databases）、捨位控制（Rounding Controls）、隨機子檔（Random Subfiles）、監視威脅（Threat Monitoring）等技術來保護資料檔案中的隱私權（Privacy），唯此問題牽涉甚廣，訖今仍無定論〔8〕、〔9〕。

6. 行政安全（Administrative Security）：利用管理制度、人事政策等行政措施，進行全面性的資訊系統安全的杜絕、防護、偵測、復元與更正工作；實施的重點是：

(1)人員安全制度，擬定人員任用、工作輪調、教育訓練、離職檢查等制度以提高人員安全素質；同時，建立授權原則（集權或分權）及僅知政策（The Need－to－know Policy）的觀念、範圍及制度訂定。在另一方面執行工作分離政策，諸如

程式設計師不得兼任操作工作等，以便互相牽制。

(2)處理的管制（Processing Controls）：利用案卷計數（Record Counting）、序列檢查（Sequence Checks ）、雙人控制（Dual Control）、更正程序等制度來確保資訊系統的安全。

(3)程序上的管制（Procedural Controls）：建立認定資訊系統安全標準的程序以及各個實體、硬體、通訊傳輸、作業系統、資料等安全需求水準認定的程序以確保資訊系統的安全水準。

(4)建立資訊系統營運記錄制度，運用系統文件（Documentation）、操作記錄（Log）間接佐證資訊系統的安全性並做爲資訊系統維護、更新的依據。

7. 稽核安全（Audit Security ）：由於資訊系統的資料處理機能已集中於一部門，無法要求「縱的獨立」，另一方面又因自動轉帳、自動收付等功能的普及也無法冀求「橫的獨立」；因此，在資訊系統之中處處存在著「相互牽制機能之結合」現象，如何建立新的稽核制度以及資訊系統安全稽核制度以杜絕、防護、偵測等功能來確保整個資訊系統的安全；實施的重點是：

(1)風險分析（Risk Analysis）。

(2)安全稽核（Security Audit）之執行。

(3)應變計畫（Contingency Plans）的訂定。

(4)成本效益分析（Cost and Benefit Analysis）。

綜觀前述，資訊系統安全政策的製定，應包含以下四點：

1. 設定安全目標。
2. 訂定安全計畫。
3. 設定執行程序。
4. 訂定控制方法。

至於詳細的行政事項可以參考日本政府主管經濟事務的通產省於1977年4月發表的「電子計算機系統安全對策基準」及日本公認會計師公會1980年12月8日發表的「EDP系統內部控制質詢書」〔10〕。

五、結論

資訊系統安全問題的重要性，隨著作業型態的改變，自動化的程度，已有與日俱增的趨勢；同時，其並非科技所能解決的問題。因爲，目前的電子計算機與通訊設備的本身，並未具備妥當的技術保護措施；所以，管理因素才是其成敗的關鍵。如何由管理部門充分的注意、協調、規劃、執行、評估而後經由認知、參與、制定、實施、稽核資訊系統安全政策計畫，才是確保資訊系統安全的基石。

参考文献

〔1〕 Business Week, "Information Processing, The Spreading Danger of Computer Crime", Business Week, April 20, (1981).

〔2〕 Chambers, A.D., "Computer Auditing ", Pitman Books Limited, (1981).

〔3〕 Parker, D.B., "Computer Security Management", Reston Publishing Company Inc., (1981).

〔4〕 Denning, D.E.B., "Cryptography and Data Security", Addison-Wesley Publishing Company, (1982).

〔5〕 黃台陽，"從行政與技術觀點看電腦安全"，電腦季刊，第十五卷，第二期，(1981)。

〔6〕 Hsiao, D.K. et al., "Computer Security", Academic Prss, (1980).

〔7〕 Martin, J., "Security, Accuracy and Privacy in Computer System", Prentice-Hall Inc., (1973).

〔8〕 Ullman, J.D., "Principles of Database Systems", 2nd ed. Computer Science Press, (1982).

〔9〕 Hoffman, L.J., "Modern Methods for Computer Security and Privacy, Prentice-Hall, Englewood Cliffs, (1977).

〔10〕 葉國興等譯，電子資料處理系統之內部控制與稽核，財團法人金融人員研究訓練中心，(1983)。

（原载：电脑季刊〔台〕1985 年 19 卷 3 / 4 期 36 — 45 页）