臺中市政府

九十六年度自行研究發展報告

開放式主機自動監控架構研究

服務單位：臺中市中山地政事務所

姓名：謝正嘉

研究日期：96.03～96.08

目　　錄

內 容 摘 要

在二十一世紀的今日，電腦作業已成為政府日常作業不可或缺的一環，而隨著電腦作業便利及效率伴隨而來的則是各式各樣的駭客攻擊、後門程式所帶來的機密外洩、內部使用人員非法使用電腦系統等資訊安全問題，嚴重的影響資訊系統的安全性。

主機為各政府單位資訊作業核心，也是資訊系統防護重點；綜觀目前各類資安設備系統，皆為各種理論繁複且操作無法簡單確認更改的系統，其運作方式不易為系統管理人員了解，加上資安系統極為價昂，現各機關經費拮据，並不容易購入該類系統，購入後操作困難又維修昂貴，令機關引入該類系統阻礙重重且難以確認成果。

上述資訊安全的重要性及導入方案的問題，本報告提出一個開放式主機自動監控架構，該系統架構有下列功能：有效減低系統管理人負擔、增加系統安全、改善操作困難之處、避免增加主機負荷、避免安全漏洞、可儲存主機運作軌跡。

為因應機關經費短缺及避免日後遭特定設備綁住，該系統需再符合可運用現有工具建置，建置經費低，不受限於特定軟體或設備，以開放式架構為基礎建置。

本研究以臺中市中山地政事務所（以下簡稱本所）為研究對象，在兼顧開放及自主兩大原則下進行探討，經由作業系統本身提供的各

類系統監督訊息，找出一套由系統管理人員主導並掌控的開放式主機自動監控架構；在完成架構建置後，依架構完成可監控伺服器硬碟的主機監控系統。

本研究一方面在主機安全工作上，減低系統管理人員的負擔讓系管人員有更多時間處理其餘業務及精進資訊技術，另一方面則更可進一步發現主機異常狀況，早期處理避免損壞擴大，使得電腦作業停頓，造成業務工作無法推行及民眾損失等各種問題。

圖表目錄

第一章 導論

1.1 研究動機

國內的土地買賣係屬登記制，每個縣市依地區大小及業務量不同設有一個至數個不等的地政事務所，負責轄區內土地交易買賣登記事宜；因土地資料繁多，地政事務所將土地資料全數存入電腦伺服器，相關作業不論是審查案件或是土地異動登記，都以電腦作業為主，藉以改善作業速度及提高為民服務效率，如何確保電腦資料正確便格外受到重視。

在電腦駭客盛行的年代，確保電腦資訊系統安全為系統管理人員的首要目標，電腦資訊系統現在面臨到內部使用者、外包廠商及來自網際網路等的攻擊威脅，如何針對伺服器加強安全工作，成為電腦從業人員的首要目標。

近年拜資訊安全觀念的普及，各項的電腦安全軟硬體如雨後春筍般由各電腦公司發展出來，但鑑於各項技術的進入門檻過高，其運作方式不易為系統管理人員了解，加上防護系統極為價昂，現各機關經費拮据，並不容易購入該類系統，購入後系統人員面臨到操作困難及維修昂貴問題，令機關引入該類系統阻礙重重。

身為系統管理人員負責系統，不禁令人思考有無解決方案即便宜又實用方案？一個開放式主機自動監控系統架構是否可行？

1.2 研究目的

伺服器主機為各政府單位資訊作業核心，是資訊防護重點工作，本研究希望能提出一個系統架構，擁有下列特點

1. 增加系統安全。
2. 改善操作困難之處：系統管理人員真正了解監控內容，系統易於操作，達成系統管理人員自主性目的。
3. 避免增加主機負荷：可視系統負荷予以調整監控資源及時間。
4. 避免安全漏洞：不可因該架構造成另外的系統防護的負擔。
5. 可運用現有工具：在不增加財政負擔下進行該架構。
6. 可以各類方式實作：不受限於特定軟體或設備，以開放式架構為基礎。
7. 有效減低系統管理人負擔：減少系管人員時時監控系統負擔。
8. 儲存主機運作歷史：以預估暨評量日後各項所需(磁碟空間、主機運作效能是否足夠？各類升級需求)。

1.3 研究範圍與限制

本研究以臺中市中山地政事務所（以下簡稱本所）為研究對象，藉由檢視主機設備相關文件及各種安全討論文獻，在兼顧開放及自主兩大原則下進行實行架構探討，找出一套由系統管理人員主導並掌控的開放式主機自動監控架構，以期符合「行政院及所屬各機關資訊安全管理要點」及「臺中市政府及所屬機關資訊安全管理要點」精神，落實資訊安全。本研究期望一方面在主機安全工作上，減低系統管理人員的負擔，另一方面則更可進一步發現主機異常狀況，早期處理避免損壞擴大，使得電腦作業停頓，造成業務工作無法推行及民眾損失等各種問題。

本篇研究係植基於系統基本程式產生的各類資訊檔案，藉由各資訊檔案所提

供訊息進行分析，若運作系統未提供該類文件，則架構需進行修正，改以其餘監督程式所產生資訊檔案進行分析；另外因系統管理人員需介入系統運作及調整，優點在於系管人員可增進系統了解，缺點則為在系統引入初期增加系管人員負擔，引發抗拒心理導致系統失敗風險提高。

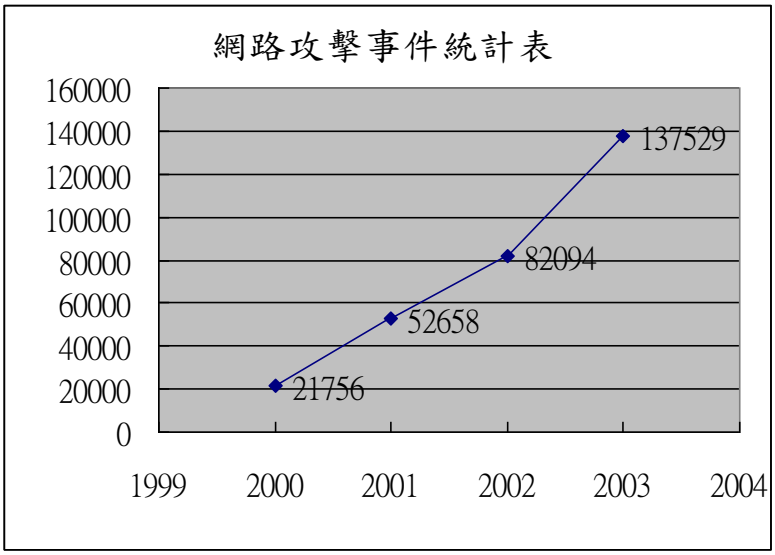
1.4 論文架構

在本篇論文的組織架構上，我們將在第二章資訊環境探討資訊安全問題的種類及風險來源、入侵偵測技術、資訊委外的趨勢及風險等問題及機關採取的資訊安全措施，第三章則提出本研究架構，介紹開放式主機自動監控架構系統模型；第四章則為研究結論與未來發展。

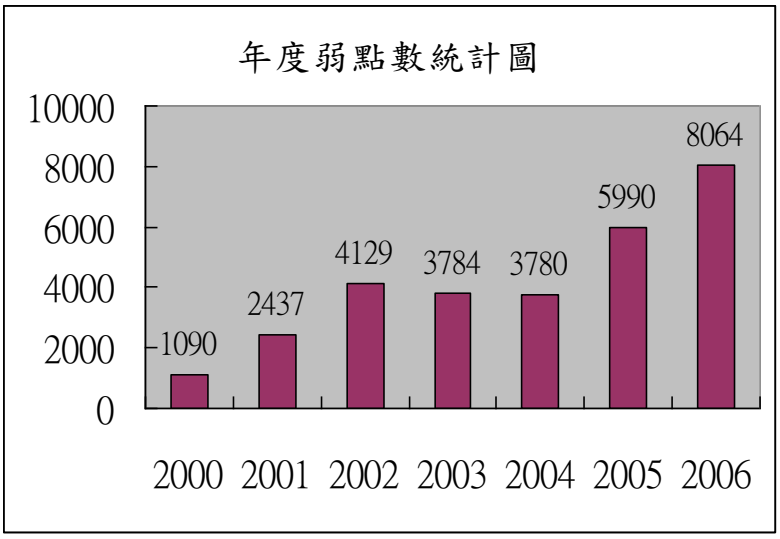
第二章資訊環境探討

2.1 資訊安全問題討論

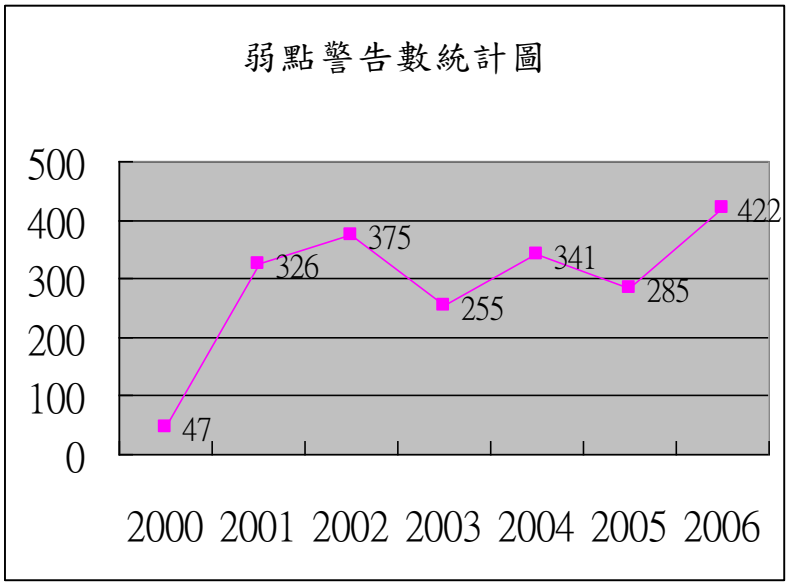
依據美國 cert 組織統計歷年發生攻擊事件[圖一]、系統弱點報告數據[圖二]及弱點警告數據[圖三]，可以發現在網際網路盛行的年代，隨著系統的更替及複雜化，各項系統弱點所造成的系統安全事件越來越多；在這樣的外在環境下，如何確保系統的安全及正常營運，成為各管理人員的首要任務，但系統的日趨複雜化、資訊技術日新月異及人力縮減所造成的影響，使得系管人員負擔沈重，間接的影響到資訊系統安全，也危害到組織的推展。



圖一



圖二



圖三

如上圖一所示的網路攻擊事件，在某一層面而言可謂是電腦犯罪或網路犯罪，依國內學者定義為「行為人濫用電腦或使用足以侵害電腦硬體或軟體行為，而造成與電腦特質有關的犯罪」或「犯罪行人濫用電腦，或足以破壞電腦系統正常運作之行為，而形成與電腦特質有

關之犯罪」；而網路駭客則泛指利用電腦技術，咨意進出他人資訊系統之人；此一行為則使網路駭客犯下「電腦犯罪」的行為，依系統管理人員角度而言，這些駭客的行為可視為入侵資訊系統的具體象徵。

本篇報告以防護角度為主，希望提出一種架構，透過自動監控系統希望達到系統安全目的，需先討論入侵者的可能行為及目前採用的入侵偵測技術及其優劣，以說明提出架構的歸類及其重要性、必需性。

2.2 入侵種類分析及偵測技術

入侵偵測觀念首見於 1980 年 James P. Anderson 所提出報告內，日後又有許多對入侵提出相關定義，如 Graham 所定義者「某人企圖進入或非法使用(misue)系統」即為入侵。入侵偵測則是使用各種方法發現入侵者，以期保障電腦系統安全。

若以入侵者進行入侵行為分類，可概分為內部人員及外部人員，其中內部人員若依電腦使用權限再細分則可分類出使用者及管理者兩類，其中以管理者情形最難處理。分述如下：

1. 系統外部入侵人員：該人員與資訊系統所屬的組織不相統屬，所需入侵技術門檻最高；因其對組織內部的相關架構不了解，加上接觸核心系統的必要資訊不明，如核心系統在何處？資訊系統相關資訊(作業系統版本？資料庫種類？系統種類？使用的程式語言？)並不明朗，皆需花費一段時間進行搜尋及了解，被發現入侵行為的風險度極高。

外部人員主要利用系統本身的漏洞進行入侵行為，例如作業

系統本身已知漏洞(如 Buffer Overflow 等)或是程式未完善的防護所形成的漏洞(如 SQL Injection 或是網頁位址的編碼，最佳範例為民國 92 年發生的花旗銀行網路申請信用卡資料外洩，即為程式漏洞所造成)進行入侵，取得管理者權限(作業系統管理者或是資料庫管理者)後，進行電腦犯罪行為。

2. 使用者：本身即為使用資訊系統組織的一份子，對於組織的資訊系統雖不甚了解，但有某種程度的認識，對於職務所使用的相關系統，擁有使用者的權限，所使用的電腦位於組織的各項防護設備(防火牆、入侵偵測系統)之後，比起系統外部入侵人員，所需技術門檻及需突破的限制皆少了許多。

越權使用者可能並非心存惡意，以進行系統破壞為目的。有時係希圖一時的方便，想要取得額外的權限或因好奇心驅使想要取得受到特殊保護的資料，凡此種種越權行為，在各組織中發生機率越來越高，也是內部入侵最為常見的入侵者

越權的內部使用者其主要的攻擊目標極為明確，只需找到主機的弱點或是利用各類網路監聽軟體擷取網路封包，進而獲取管理者帳號/密碼資訊後，即可順利進行入侵，以取得非法使用權限或是受保護資料。尤其在組織為了方便使用系統，疏忽了許多嚴格的驗證工作或是存取管制計畫，此一情況將更形嚴重。

3. 管理者：系統管理者係負責管理系統運作人員，擁有系統的最高權限，可以視情況進行程式、檔案等變更。除擁有系統變更權力外，更有著刪除或變更系統存取記錄權力，這使得系統管理者若發生瀆職問題時，比起一般使用者更難處理。

隨著職位異動，管理人員可能離職或是變動，若是管理人員心生不滿，可能產生竊取隱密性資訊的風險，就算是變更管理者帳號及密碼，亦可能因植入木馬程式所形成的後門，令已離開職位的管理者擁有不相當的權限，造成管理上的極大問題。

如何避免管理者造成的問題？建議由策略面設立管制措施：例如對管理工作進行不定時的稽核、設定程序或執行相關的批次命令時需經其他小組複核方可進行等等。

入侵偵測系統可以依使用技術及偵測方法分類，茲分述如下：

依系統所使用的入侵偵測技術是透過偵測已發現特徵值為主亦或是根據使用者日常行為建立行為模型為判斷基準，入侵偵測可歸納為下列三種模式：

(1.) Misuse intrusion detection system：建立特徵值進行偵測，特點是偵測速度快速，誤判率低，缺點是無法發現尚未建立特徵值的入侵行為。常見的使用方法包含了 Rule-based、Bayesian

Network、Finite State Machine 等三種。

(2.) Anomaly intrusion detection system：根據使用者日常行為建立個人模型，若使用行為超出該模型範圍，則視為入侵行為發生。此一方法的特點為可發現新型入侵行為模式；缺點為偵測行為方法及建立模型所耗費時間較久，誤報率(非入侵行為誤判為入侵行為)較高。常見的使用辦法為 Statistic Analysis、Neural Network 及 Data Mining 等方法。使用上皆需將資料進行量化以進行處理，也限制此一方法的應用，且因誤報率較高，在應用上常因誤報率高，令使用者輕忽訊息，導致偵測系統聊備一格，造成系統安全上的漏洞。

(3.) Hybrid and Mixed intrusion detection system：混合上列 Misuse 及 Anomaly 兩種方法,部份明確的入侵偵測行為採用 Misuse 偵測方法，再應用 Anomaly 方法以查覺新型的入侵行為，惟仍需選定一種方法為主，另一種為輔，特點是偵測效果較佳，惟成本及偵測時間較前兩種皆為高，在即時應用上有其先天限制。

若依入侵偵測系統所使用的判斷技術方法不同進行分類；入侵偵測系統系統應可歸納為分類系統的一種，換言之，凡是分類系統的技術皆可運用於入侵偵測系統，舉例各類偵測方法如后：

(1.) Statistic Analysis：運用各種不同的統計分析方法，建立系統運作情形及使用者日常行為頻率等，做為偵測方法。其重點在於收集資料建立個別電腦的正常行為模式，再將目前發生

事件與該模式相比較，相異過大則判定為異常，反之則為正常。

此一方法的成敗因素繫於正常行為模式(Normal Profile)的建立，而該模式的準確度則與取樣時間、空間的普遍性、監測機器特性(區域網路或網際網路)有關；實務上以分群方式進行區隔，如何將相似機器區分為一類，減少模式種類，降低模式空間，為本法的討論重心。

(2.) Neural Network：利用類神經網路的快速運算分類功能，可進行監督式或非監督式學習以建立網路模型，不論是用在 Misuse 或是 Anomaly 系統皆有其效用。

雖然在應用上，不論是 Misuse 及 Anomaly 皆可應用此一方法，但使用類神經的技術問題仍無法避免，包含訓練資料的取得、量化特徵值的過程、訓練時間較長、計算量大，有時會有重新訓練的必要性等。

使用類神經網路時，因其有著監督及非監督兩種模式，在應用範圍上寬廣許多，應用自我分類特性，進行資料分類觀察，找出其群聚特性，在減少設計模型時間上，有著明顯助益。

類神經系統建立模式完成後，在檢查結果(或是分類上)

都可達到快速運算的需求，在注重即時應用的入侵偵測/入侵防禦系統極為適合。

（3.）Rule-Based Analysis：Rule-base 主要用來表現專家的思考模式，因為人類的思考極為複雜，難以用演算法加以表示，但若以解決問題導向，採用 rule 型式建立專家系統以解決問題，成為一個可行辦法。應用在 IDS 時，建立系統安全的 Rule Base，據此判斷使用者行為是否符合已建立的 Rule，表示規則方法又可分為正面表列及負面表列兩種方式，在實際產品的應用上，Fire Wall 的規則列表在某一程度上即呈現此一情形。

（4.）Bayesian Network：使用貝氏網路架構圖表示出各類事件或行為的發生機率據以判斷入侵行為是否發生；Bayesian Network 重點在於各種偵查行為及特徵值的機率描述及其分佈情形是否清楚？能否以此表示出一個完整的貝氏網路架構圖？若無法形成網路架構，則代表偵測目標不適用此一方法進行偵測。

貝氏網路本身亦有推測機制的運用，也就是說可根推測機制，在各種條件符合的情形下進行 Anomaly 偵測，發現新的入侵行為。

（5.）Finite State Machine：利用有限狀態機來表示網路行為的狀態

轉換圖，定義出轉移條件，若是最後的狀態為入侵行為，則判斷這一次的偵測對象為一個入侵行為，反之則否。

一個有限狀態機一般包含有幾個要素：起始狀態、輸出狀態、狀態轉變函數及輸出函數等。如何將入侵行為轉變為狀態及轉變函數進行描述，影響到入侵偵測系統的成敗。

以 Finite State Machine 為主的入偵技術，較有名的有 STAT(State Transition Analysis Tool)，這是用來表示電腦受到攻擊時，各種狀態彼此間的描述工具。

若以 Finite State Machine 描述一個常見的資料庫入侵行為：查得受保護的主管薪水資料；查得全部門的薪水為一個狀態(S1)，再查除保護主管薪水資料外的薪水資料則為一個狀態轉換行為，到達資料庫入侵行為發生狀態(S2)。若是在一定時間內未發生查詢非主管薪水則為一安全狀態。

（6.）Data Mining：利用 Data Mining 技術找到網路行為記錄間的關連規則，例如使用者的上線時間，網路位址，呼叫程式等之間的關連性或是各類事件間的發生資料，由其中取得重要的關鍵資料後，找出其中的關連規則做為 IDS 的判斷依據。

以 Data Mining 進做為入侵偵測方法技術，其重點在發現各項特徵彼此間的關係，怎樣的特徵值意味著入侵行為將發

生。而 Data Mining 的成功與否在於如何選擇特徵值資料及各類門檻值設定，若是選錯特徵值，則發現與入侵行為真正相關的機率將降低，例如要找的是同一時間重複簽入的異常行為，其偵測特徵為來源電腦與相同的使用者與同一電腦不同使用者的簽入記錄，在一個使用固定 IP 或是浮動 IP 的網路，電腦位址是否可做為偵測特徵？或是該以電腦名稱進行偵測特徵碼？若是應用到新作業系統時，同一網卡可指定不同位址，則是否應以網卡編碼為偵測重點？凡此種種皆需進行了解及考慮，以期提高偵測效率。

Data Mining 在應用上主要著眼於眾多資料中發現重要規則，在即時性的入侵偵測中，速度是重要因素，也就是希望能將規則數降到必要性的最低程度，以期能即時發現入侵偵測行為加以阻斷，避免入侵行為的危害；Data Mining 係利用門檻值來進行產生規則數的控制；門檻值高，可以降低規則數，但有遺漏入侵行為的疑慮，門檻值低，雖可找到許多可疑的入侵行為，但耗掉的是大量運算及誤判正常行為成異常行為，常需因時因地制宜；但目前現有成品並不提供如此調整，一方面是應用困難(使用者要求高)，再來是與購買此一產品的市場需求相反。

（7.）Immune-Based System：為新一代的入侵偵測技術，其主要係模擬人體的免疫系統進行入侵偵測判斷的技術。人體的免疫運作是由大量平行的免疫細胞進行對病毒的防衛，表示免疫技術背後的意義是可進行大量而平行的複雜運算，在網路發展快速的現代，入侵 IDS 的運算需求日異升高，Immune-Based System 是一個可行的解決方案。

Immune-Based System 擁有許多單元，每一個單元都可學習新訊息，保留原有訊息及進行字元辨識工作，單元間並無關連，系統一開始亂數產生許多單元，再進行單元挑選後，各單元即自行運作；每一單元都有一個生存時間，隨著系統運作，有發現入侵行為者，其生存時間延長，若無，則生存時間到隨著消滅；利用此一方式進行淘汰，可使得系統能擁有許多可發現入侵行為的獨立單元，完成 IDS 的任務。

2.3 資訊系統委外發展情形

資訊系統委外為近年興起風潮，機關在人力、物力無法支應各項資訊系統日益擴大支出及兼顧資訊系統品質及活絡社會經濟要求下，逐漸興起資訊系統委外趨勢，在談到資訊安全議題，不可避免的必須談到這個層面所帶來的影響及其潛在風險。

首先由歷史層面觀看資訊委外，在民國 80 年代，有鑑於資訊發展的日新月異，開始興起一股資訊委外的風潮至今未衰，由掌理全國各機電腦審議輔導業務的單位：行政院主計處電子處理資料中心進行各項辦法要點的幕僚作業；經產官學界的多次討論後，行政院於民國 83 年公佈「各機關資訊作業委外服務實施要點」列出政府機關資訊作業委外服務工作重點與原則性規範；復於政府採購法施行後，於 88 年 5 月 27 日頒佈「機關委託資訊服務廠商評選及計費辦法」作為政府單位資訊委外的基準要點。

對政府機關而言，其主要工作項目為服務民眾，經管資料與民眾隱私息息相關，如以委外工作而言，茲以為首重資訊安全與機密維護為重，與一般企業對資訊委外所注重的重點：成本效益有所不同。

在自 88 年停止適用的「各機關資訊作業委外服務實施要點」內對資訊安全及機密維護特別獨立出一章進行規範(第五章)，包含重點項目計有四大重要項目：

1. 訂定具體安全需求，應載明於服務契約。

2. 應加強安全控管，必要時，應自行管理。

3. 建立管理制度，定期評估。

4. 確保資訊業務之持續運作。

復於 88 年依政府採購法訂定的「機關委託資訊服務廠商評選及計費辦法」則於第六條規定招標文件應載明資訊安全及機密維護需求、稽核作業需求及品質保證需求。比較 88 年廢止及新訂辦法，新辦法訂定範圍更為寬廣，另一方面則賦予招標單位更多的彈性，令招標單位需要付出更多的心力評估自我需求及修訂合約內容，以求達到資訊系統成功委外目標。

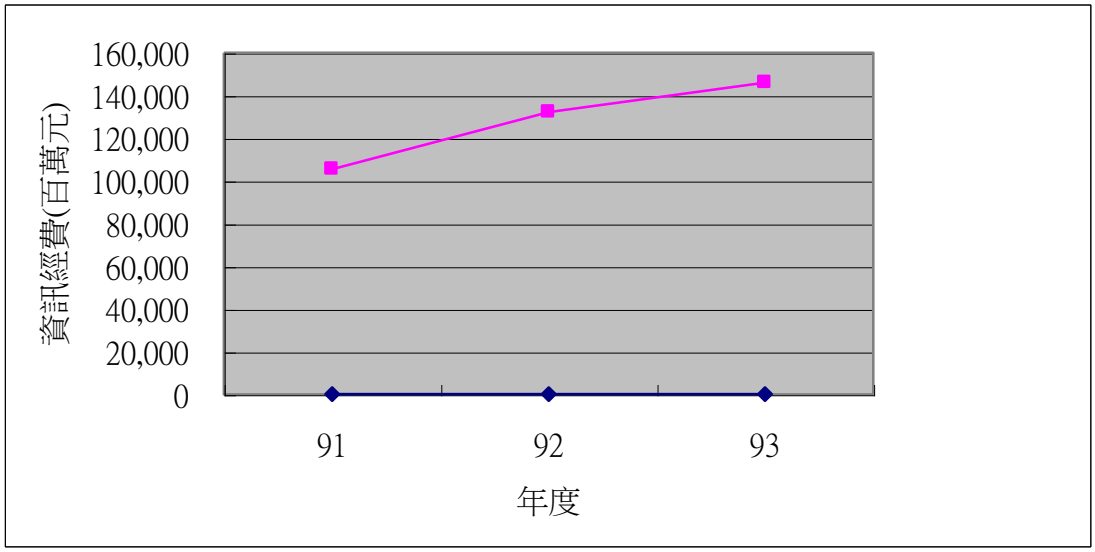
依據主計處 91 年至 93 年的電腦應用概況報告，其中資訊經費變化列示如表 1：

表 1 中華民國 91 年至 93 年資訊經費全年支出結構概況

單位：百萬元

年度	民間企業	政府行政機關	公營事業機構	公立學校	公立研究機構	私立學校	私立研究機構	合計
91	67,373	16,451	14,078	3,547	932	2,916	136	105,433
92	87,907	20,147	13,270	4,885	1,058	4,480	387	132,133
93	105,900	16,678	13,138	4,531	532	4,647	551	145,977

資料來源：行政院主計處電子處理資料中心



圖四 91 年至 93 年資訊經費支出趨勢圖

由圖 1 支出經費變化中，可以看出資訊支出經費逐年上昇，年增率分別為 25%及 10%，說明不論是在政府或是民間，資訊系統的使用皆是不可或缺，其投資金額若再考慮各種設備價格的降低情形，隱含的意義說明整個社會在電腦資訊應用上日趨迫切而不可或缺。

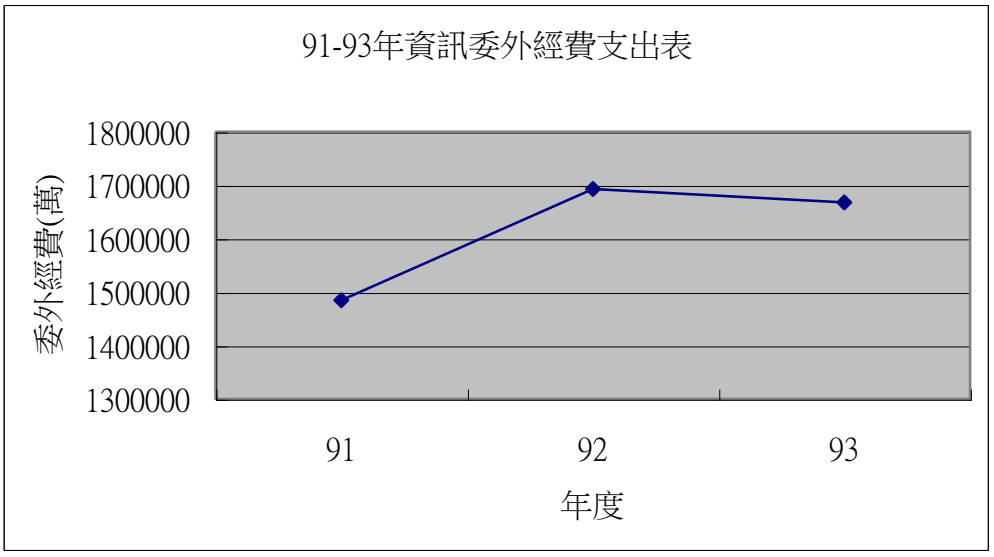
再觀察 91 年到 93 年的資訊委外支出經費(詳表 2)及趨勢圖(詳圖 2)如下：

表 2 中華民國 91 年至 93 年資訊委外全年支出結構概況

單位：萬元

年度	民營企業	政府行政機關	公營事業機構	公立學校	公立研究機構	私立學校	私立研究機構	合計
91	901,344	448,644	102,658	9,602	6,857	14,799	1,066	1,484,970
92	928,619	589,613	130,429	11,663	12,108	16,962	3,544	1,692,938
93	1,066,451	419,135	138,323	14,403	3,483	19,633	6,288	1,667,716

資料來源：行政院主計處電子處理資料中心



圖五 91-93 年資訊委外經費支出趨勢圖

其中 92 年比起 91 年的年增率約為 14%，而 93 年比起 92 年則減少了約 1%，探究 93 年較 92 年減少投資金額原因，係因政府行機關及公立研究機關資訊委外經費的縮減，民間企業成長率則仍有 14.85%，委外作業項目仍以軟體開發與維護為主，占委外總經費 52.91%。

在行政規範中既然無委外風險評估細節內容，由學術角度進行資訊委外風險評估則為另一切入資訊系委外的方式，以下由資訊委外的理論角度進行各類的探討，討論需注意的相關細節。

綜觀資訊系統的發展歷史，早期因電腦系統昂貴，企業以租用時間方式使用電腦系統，可視為資訊委外的起源，以另一說法可說資訊系統與委外是分不開的。到 1970 年代，資訊設備呈現某一程度的普及化，使各公司擁有自己的電腦設備，惟考慮到資訊系統需求的多樣性及發展性，大多以另一種較隱匿的委外方式進行資訊系統發展(購買軟體、進行專案開發)；近幾年由於網際網路的興起，加上全球性競爭的壓力下，企業將部份標準化業務以委外方式完成，資訊系統以資訊科技的發展迅速、資訊系統管理技術的困難性、資訊部門績效不明、資訊業界服務項目的提升等因素下，資訊系統委外成為企業處理資訊業務的方式之一。

企業將資訊系統委外的理由最主要有：1. 追求企業目標，2. 節省成本，3 重組財務，4. 提供資訊部門能力，5. 策略優勢等理由。Apte & Sobol 調查美國、日本及芬蘭等三個國家的資訊外包情形，發現設備維護、教育訓練、損害復原、資料輸入及系統整合是最常見的委外作業，但資訊部門名列前茅的公司，沒有一家將資訊部門全部委外，但有 77%的資訊部門將一項業務委外，主要的委外作業幾乎都是非核心、與公司主要政策無關的業務。

Looff etl.發現絕大部份公司採取委外作業行動的原因，起因高級主管下令裁減經費，導致資訊部門表現不如委外公司那樣有效率。 但無可避免的，委外作業仍有風險，企業需自行分析及評估其風險，以政府機關角度評估，掌管資訊與民眾息息相關，自民國 84 年 8 月 11 日公佈施行電腦處理個人資料保護法後，資訊委外風險性需再加上法律層面的考慮，令機關在進行資訊委外時更加小心謹慎。

委外作業風險可從以下幾種角度進行分析：

一. 管控角度

在委外作業最顯而易見的危機為「失控」；委託公司隨著委託時間的進行，逐漸發現無法掌握一切，加上委外廠商的員工並不歸屬委託公司管理，通常不直接向委託公司報告狀況及進度，進而衍生出服務品質失控、作業彈性不足、無

形費用(額外收費)、機密資訊洩露等問題，凡此種種皆賴一個良好的合約進行控制。

二. 潛在問題角度

資訊委外有一大誘因在於減少資訊支出費用及控制資訊支出，但若委託公司的使用者任意花費，擅自越過廠商由它處來獲取服務，將使資訊支出費用不減反增。科技不斷變動的影響，將使得長期合約潛藏作業費用有付出與收獲不相符的風險，每年付出的固定費用，卻無法享用到最新科技的便利性。

其他潛在風險包含在資訊委外後才發現資訊部門對公司的策略目標有其重要價值和貢獻，對公司的競爭策略將造成影響。企業未事先了解廠商在成本控制上非常嚴格，只有合約規定的服務才履行，使得服務水準與迅速反應並沒有實現，甚至比起原有資訊部門還糟糕。

事先未於合約中規範委外廠商需使用新科技及新設備，廠商使用過時的設備及服務，都將使得提升資訊能力目標未能達成等。

三. 特殊性角度

Michael Earl(1996)指出資訊系統的特殊性：科技不斷在超前，加上網際網路興起，科技走向更難預測，加上企業經營環境也更趨複雜，資訊系統在支持企業營運上更加困難。

企業資訊系統的應用與組織經驗息息相關，需要時間累積及實務經驗中學習，委外廠商需學習資訊科技和企業的配合，使得資訊委外存在另一種風險性。而科技的整體難以分割性，使得委外廠商的整合性需求更為殷切，難以分割軟體、硬體、網路等獨立運作，整體外包有其必要性。

四. 財務及協同運作角度

Clark 指出委外作業的風險通常會被一些忽略的事實或無法預知的變化，造成資訊系統的支出昇高；其可能發生的支出增加原因包含有調職員工的保險福利及退職金，軟體使用授權費用，交涉委外所花費的財力、精力及勞力等，最重要的是回收資訊系統所帶來的費用。

協同運作則因委外廠商與客戶的特質與行為所帶來的風險包含各自立場上的矛盾、依賴性，公司文化不同，營運能力不足及再次分包等問題。延伸出公司人員學習新應用的機會喪失及失去適應能力

綜合上述四種角度所帶來的風險性，企業唯有仔細評估、分析風險後，藉由選擇好的廠商，擬定良好合約避免相關風險。

我國政府機關受到採購法及現實環境影響，使得資訊委外更加困難重重，尤其以機關資訊若與民眾財產有關，如地政、稅務機關及金融機構(如銀行及集保公司)，其掌握資訊可說是金錢的代名詞，若是單純以合約規範，外包公司的資本額可能還比不上所掌握的資訊總額，若是遇到惡意廠商進行資料竄改，所造成的損失將難以估計，使得政府機關資訊委外的問題更為難解。

2.4 資訊系統安全措施

現各機關在對各資訊安全的對應方法，不外乎採購市面上各類產品：防火牆、入侵偵測系統、資料庫防護系統、防毒軟體等，若是經費充裕下，更可委外建構SOC系統，委由專業廠商隨時監控系統及網路狀況。

以上種種措施均賴各資訊人員依設備需求進行各種操作，相對而言資訊人員也需了解各項設備的運作細節以求達到安全目的，對資訊人員實為一大負擔。

尤其各項資訊安全設備，以專業知識而論，除了防火牆只需具備網路七層知識即可操作外，其餘不論是入侵偵測系統、資料庫防護系統、病毒系統及SOC系統，其所需知識皆需專家級人員方可實作。

機關內資訊人員實無此能力及時間了解各系統的運作細節，大都依廠商所教導的每日更新步驟按表操課，只能期待所選擇產品能發揮其宣稱作用，保障資訊系統安全。

第三章 研究架構

3.1 研究目標

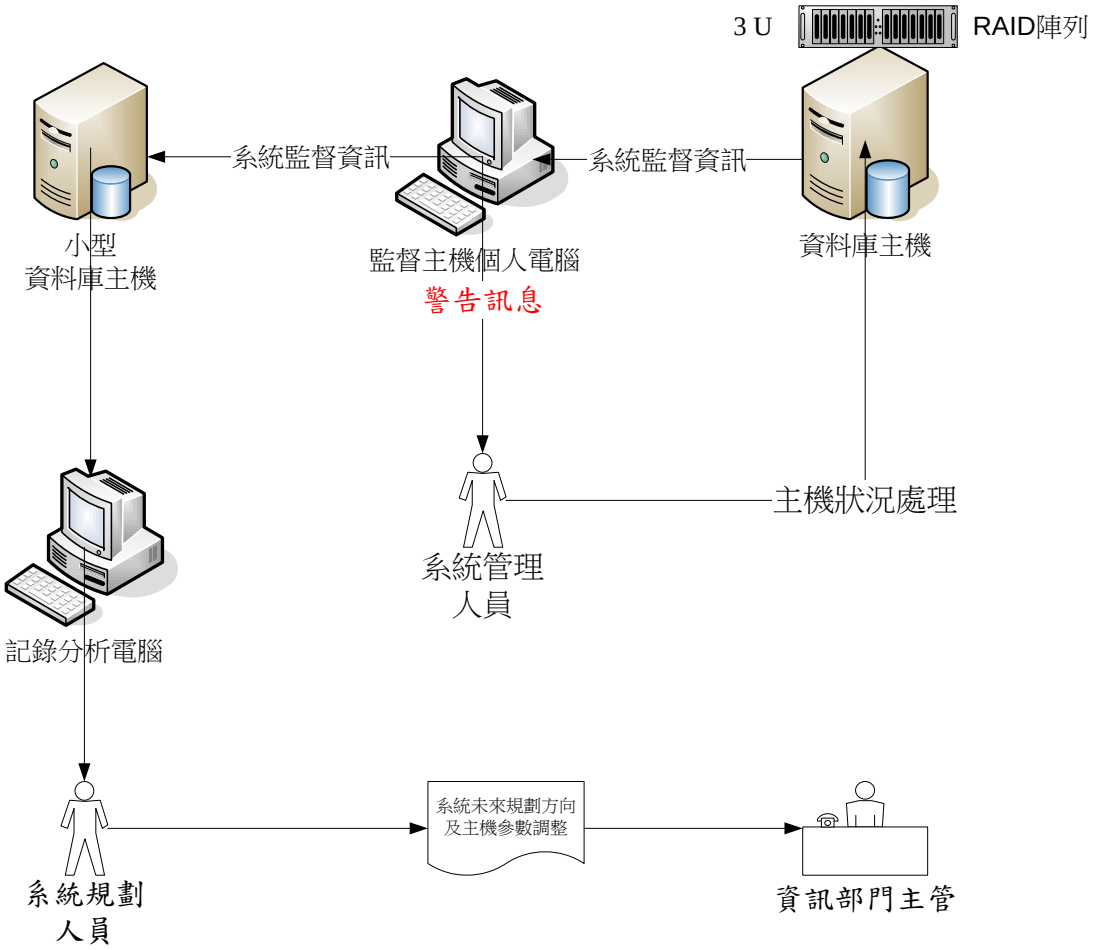
在經過第二章的討論後，資訊系統面臨到日趨複雜的各種攻擊行為、入侵技術的多變及資訊委外所帶來的新增風險，雖有各類入侵偵測防護技術及各種資安設備可供運用，但所需的費用高昂及資訊人員對設備無法充份掌握則是另一問題。

身為一個系統管理人員，了解經管系統的重要性，每每苦思有無妥善解決方法，屢屢向外求教，所獲得的多為購買各種產品，但限於經費及未知產品可為機關帶來多少可計算利益？加上機關使用系統由上級統一配發處理，應用程式與新一代技術的相容性亦成問題，無法使用最新技術處理一些已可解決問題，使得資訊安全總是一份揮之不去的隱憂。

在經過多年的思考後，回歸資訊安全原點，每日系管人員皆需進入主機查核相關資訊，利用主機本身提供監控程式進行檢查，那能不能由作業系統提供的資訊進行自動化分析？如此一來可達到省經費，而該類資訊又屬公開非隱私資訊，有各類文件可以參考，所獲得資訊亦為可信，實屬一可行政策，而且可達到由系統管理人員自主操作，不受限於廠商，歸納各項收集資料後，更可由中獲取系統未來所需擴充方向，實為一可行架構。

3.2 開放式主機自動監控架構模型

以研究目標為構想的架構列控如下：



圖六 開放式主機自動監控架構圖

開放式主機自動監控架構係以運作系統所具備系統資訊為主，由系統管理人員擇定系統監督資訊後，以監控主機系統運作。

3.3 開放式主機自動監控運作步驟

1. 由系統管理人員參考主機作業系統所提供資訊，擇定系統監

督訊息內容，並由系統人員於監督主機個人電腦內設定各項警告標準。

2. 定時由主機取得系統監督訊息內容。
3. 由監督主機個人電腦對系統監督資訊進行處理，依步驟 1 設定的警告標準與監督資訊進行比較，以決定是否對系統管理人員進行警示？若不需警示則跳到步驟 5。
4. 系統管理人員接到監督主機發出警告訊息後，即刻進入主機狀況處理程序，對主機進行處置。
5. 系統監督資訊存放於小型資料庫主機，以備日後分析。
6. 系統規劃人員(或是系統管理人員)由記錄分析電腦定期存取小型資料庫主機，了解各項系統資源使用變化及發生狀況頻率。
7. 系統規劃人員依記錄電腦分析結果產出系統未來擴增需求，作成系統未來規劃方向(汰機)及主機參數調整建議，送交資訊部門主管參考。

3.4 開放式主機自動監控運作實例

1. 系統管理人員擇定監督系統內硬碟使用狀況，系統人員於監督主機個人電腦內設定各項警告標準(如 15 分鐘內使用空間不可大於上次使用空間 5%)。
2. 定時由主機取得系統系統內硬碟使用狀況。
3. 由監督主機個人電腦對系統監督資訊進行處理，依步驟 1 設定的硬碟使用狀況警告標準與監督資訊進行比較，以決定是否對系統管理人員進行警示？若不需警示則跳到步驟 5。
4. 系統管理人員接到監督主機發出警告訊息後，即刻進入主機了解硬碟使用情形，為何在 15 分鐘內會有 5%使用空間？了解是否為一正常使用？或是暫時性情形？並對主機進行處置-擴大磁碟空間，以避免硬碟空間不足使系統無法運作。
5. 系統內硬碟使用狀況存放於小型資料庫主機，以備日後分析。
6. 系統規劃人員(或是系統管理人員)由記錄分析電腦定期存取小型資料庫主機，了解系統內硬碟使用狀況變化及發生狀況頻率。
7. 系統規劃人員依記錄電腦分析結果產出系統硬碟未來擴增需求，作成系統未來規劃方向(汰機)及主機參數調整建議

（包括監督主機標準是否更改？監督頻率(15 分鐘)及警告標準(大於 5%)），送交資訊部門主管參考。

3.5 開放式主機自動監控運作系統

以[3.4 開放式主機自動監控運作實例]為範本，實作系統如下：以開放可調式主機監督為系統設想架構，以減少系統管理人員負擔為主要目標，再則以其概念不受限主機型式及加深管理人員參與為主要目的。

以固定間隔時間(15 分鐘)查詢主機目前硬碟使用情形，並與上次記錄進行比較，若是單一目錄在間隔時間發生異常增長情形，則發出警訊，提示系統管理人員進行處理。

上圖為設定監控時間，其時間長短需考慮與主機的配合問題。一方面需考慮主機負荷，不可本末倒置，因監督系統運作導致系統運作發生效能問題。

上圖為發現硬碟空間異常增加訊息，以警告聲響及螢幕警示為主，此時系統人員即需進入主機，檢查為何/dev/hd1 發生異常增加狀況。

第四章 研究結論及未來發展

本篇研究報告探討因資訊技術突飛猛進而造成機關面臨到各種不同的資安問題挑戰，雖有各項資安設備可供機關購買，惟其引入價格高昂、使用操作門檻極高及效益難以評估使得機關面臨到的種種問題。

在以伺服器為重點防護區域的想法下，本報告提出一個可行的系統架構：開放式主機自動監控架構；以作業系統本身的各項監控程式為監控主體，將其輸出為系統監督資訊，由監控電腦進行收集及判斷是否有問題並通知系統管理人，並將歷次的訊息收集到資料庫內，做為日後系統規劃依據及系統調整參考。

此一系統架構可達到研究目的計有：增加系統安全、易於操作、達成系統管理人員自主性、避免增加主機負荷、避免安全漏洞、所需經費極少、以開放式架構為基礎可以各類方式實作、有效減低系統管理人負擔、可預估暨評量日後系統發展方向。

本報告依所提出架構實作監控系統，以監督伺服器硬碟使用情形為系統目的，並記錄伺服器硬碟使用情形，系統成效良好。

報告所提出架構係植基於系統管理人員對系統的熟悉度及了解程度，由系統人員選擇所需要的系統監督資訊並設定其警示條件，這是一件看似困難又不得不做之事，若是系統人員不了解經管系統運作

內容，便難以令架構發生效用。在此提出一個選擇方向供大家參考，監督系統資訊可概分為三類：

1. 為數字型態：如硬碟已使用率？檔案數？
2. 固定文字型態：如系統運作時該存在的程式，如以 oracle 資料庫而言，其 listener 程式必須存在，以供 client 端連接用，又如應用程式在伺服器端存在的運作程式皆屬此類。
3. 混合型態：為 1 及 2 的處理後的型態，如每一 oracle client 連接時，會在主機產生一個連接程式，其為文字型態訊息，而系統監督資訊則是要了解同一時間有多少連接？則需將文字型態進行處理成為數字型態資訊皆為此類。

分析上述三類資訊，第二種資訊最為清楚及明瞭，只需確認程式是否存在即可，而第一類及第三類資訊看似難以訂定警告，實可以利用觀察彙整系統運作歷史資料進行判斷，此亦為入侵偵測方法中的異常偵測方法，其原理為系統的各項運作在正常情況下，不應有過大變動情形產生，利用觀察彙整一段期間資料，自可發現應設的警告條件。以實作系統為例，地所單位應用程式在主機發生的硬碟變動值，在 15 分鐘內不可能大於 5%，若是其他單位的應用系統，若有多量報表暫存或運算暫存檔案，則有可能發生 15 分鐘內硬碟多於 5%情形發生，這些可由系統運作歷史資料決定，在有長期間的觀察資料佐證

下，可以有效的設定警告訊息的產生條件。

因受限於時間及資訊安全不應揭露太多系統運作內容情形下，報告到此告一段落，利用實作系統已證實報告所提架構為可行，所餘者為如何在兼顧安全及系統效能下，將系統監督資訊進行傳輸，凡此種種皆為個案調整，在此不便進行討論。未來發展方向則視系統管理人員對系統掌握度，在不影響系統效能下，將更多的系統運作資訊納入監督系統內，此一監督架構可系統管理人員主導進行，也可視為將要求系統管理人員需更多的成長，以備應付將來各項資安挑戰；另一方面則免除系管人員觀看系統運作資訊日常工作，讓系管人員能專注心力在更複雜業務與日新月異的資訊技術。

本報告實作系統係為採用 Rule Based 方式建構的 Anomaly intrusion detection system，Rule Based 係為最容易了解及實作的偵測技術，日後技術成熟後，亦可採用第二章其餘偵測技術加以輔助以加強系統安全性，惟可能導致費用增加，那又是另一個討論題目。

參考文獻

中文文獻

[1] Andrew Conry-Murray(2005)，「來算內部的安全威脅」，網路資訊，2005 年第 11 期，第 50-58 頁

[2] David Greenfield、「網路安全委外處理省麻煩」，網路資訊，2001 年第 9 期，第 132-138 頁

[3] Penny Lunt Crosman、「網路管理委外風潮吹不停」，網路資訊、2005 年第 5 期，第 115-121 頁

[4] 王旭正主編(2002), 資通安全專輯之四系統安全, 行政院國家科學委員會科學技術資料中心。

[5] 王岳忠，「全力偵測機而動的新威脅」，網路通訊，2003 年第 4 期，第 64-67 頁

[6] 行政院主計處，「各機關資訊作業委外服務實施(計費)要點【停止適用】」，民國 88 年停止適用。

[7] 行政院主計處，機關委託資訊服務廠商評選及計費辦法」，http://www.dgbas.gov.tw，民國 88 年。

[8] 行政院主計處電子處理資料中心 ，「91 年電腦應用概況報告」，http://www.dgbas.gov.tw，行政院主計處電子處理資料中心，民國 92 年。

[9]行政院主計處電子處理資料中心 ,「92 年電腦應用概況報告」, http://www.dgbas.gov.tw，行政院主計處電子處理資料中心，民國 93 年。

[10] 行政院主計處電子處理資料中心 ,「93 年電腦應用概況報告」, http://www.dgbas.gov.tw，行政院主計處電子處理資料中心，民國 94 年。

[11] 吳萬順總編(2005), 地政業務電化紀實, 內政部。

[13] 蔡甘子、「委外服務與資安管理」、網路通訊、2005 年第 4 期、第 17-22 頁

[14] 鄭義熙(2001)，政府資訊作業系統委外管理之研究-以國稅局資訊系統為例，義守大學，高雄。

[15] 賴妍帆、「網路、安全、弱點與風險管理」，網路通訊，2003 年第 3 期，第 44-46 頁

英文文獻

[16]D. Clarkjr. Thomas, W. Zmud Robert, E. McCray Gordon (1995), “The Outsourcing of Information Services: Transforming the Nature of Business in the Information Industry,” Journal of Information Technology(Routledge, Ltd.), DEC, Vol. 10, Issue 4, pp 221-237.

[17]D. L. Carter & A.J. Katz.(1996) "Trends and experiences in computer-related crime: Findings from a national study," The Annual Meeting of the Academy of Criminal Justice Sciences, Las Vegas, NV.

[18]E. Eugene Schultz(2002), "A framework for understanding and predicting insider attacks," Computer & Security, Vol. 21, No. 7,pp. 526-531.

[19]G. B. Magklaras and S.M. Funell(2002), "Insider Threat Prediction Tool: Evaluating the Probability of IT misuse," Computers & Security, Vol. 21, No. 1, pp. 62-73.

[20]James P. Anderson(1980), "Computer Security Threat Monitoring and Surveillance," Technical report, Fort Washington, Pennsylvania, April.

[21]Joseph S. Sherif, Tommy G. Dearmond, "Intrusion Detections: Systems and Models," Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises(WETICE'02), pp. 1-19

[22]Klepper Robert & Wendell O. Jones(1997), Outsourcing Information Technology, Systems & Services, Prentice Hall; 1st edition.

[23]Leon A. Delooff(1995), "Information systems outsourcing decision making: a framework, organizational theories and case studies," Journal of Information Technology (Routledge, Ltd.), Dec, Vol. 10, Issue. 4, pp. 281-297.

[24]M. Apte Uday and G. Sobol Marion, Tatsumi Shimada and Timo Saarinen, Timo SAlmela and Ari P. J. Vepsalainen(1997), "IS

outsourcing practices in the USA, Japan and Finland: a comparative study," Journal of Information Technology (Routledge, Ltd.), Dec, Vol. 12, Issue. 4, pp. 289-304.

[25]McHugh John, Christie Alan, and Allen Julia (2000), "Defending Yourself: The Role of Intrusion Detection Systems," IEEE Software, Vol. 17,pp. 42-51.

[26]Ozgur Depren, Murat Topallar, Emin Anarim, M. Kemall Ciliz(2005), "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," Expert Systems with Applications, Vol. 29, Issue 4, pp. 713-722.

[27]Robert Graham,FAQ:Network Intrusion Detection System, version 0.8.3, March 21,2000, http://www.robertgraham.com/ pubs/network-intrusion-detection.html.