東海大學
資訊工程與科學研究所

碩士論文

網路安全威脅分析與防制策略

Network Security Analysis and Defense Strategies

指導教授：呂芳懌博士
研 究 生：蘇　俊　維

中華民國九十二年八月

誌謝

工作數年後再返回校園，讓我更加珍惜這三年的研究學習與養成過程。首先，特別感謝恩師呂芳懌教授的指導，才得以從摸索、探索到研究網路安全的知識、技術與學理，培養組織管理、解決問題及口頭表達的能力，並且學習到寫作論文的技巧與組織架構的方法。此外，老師對做研究一絲不苟、實事求是的嚴謹態度，讓學生著實受益良多，更是現代年輕學子所應效仿的。在論文審查與口試期間，承蒙林宜隆教授、林熙禎教授、連志誠教授與張文貴教授等所給予寶貴的意見與指導，讓論文結構與內容更加嚴謹與充實，在此致上最誠摯的謝意。

其次，在校求學過程中，由衷感謝許玟斌教授與溫嘉憲教授的啓蒙，使學生能養成獨立思考的能力與通曉做學問的方法，俾使在研究領域上能更深一層的透析與瞭解，並養成樂觀進取的態度與性格。同時也要感謝實驗室所有同學，包括義樺、政瑋、真真、嘉鴻、清健、子逸、品璁、仁傑、耀中、國煒等的關懷與鼓勵，在這互動的學習環境下，所學的不祇是專業，更能相互學習、分享與成長，讓我留下許多美好的回憶。

最後，要感謝在背後默默支持我的家人，我的母親盧蘭君女士與兄長蘇俊源、蘇俊揚等，在多年的求學生涯給予我最大的精神支持與幫助，謹以此論文，獻給我最摯愛的家人。

摘要

在建構安全的網路系統上，一般的入侵偵測僅著重在網路的異常行爲分析，如要提昇網路的安全層級，還應該針對網路的各種攻擊方式，做全面性的分析與防制，並訂定出合適的網路存取機制與監控方法。本論文首先探討入侵者如何利用網路的特性，擷取傳輸封包與竊聽密碼，與如何利用不當的存取控制，取得控管權限與系統資訊等。其次，研究入侵者如何利用不被監控的網路封包與不易檢測的隱藏通道建立後門、種植木馬，竊取系統資訊，與如何利用 TCP/IP 通訊協定的疏漏，經由 IP 封包欺騙或 TCP 序號猜測，劫持 TCP 連線以入侵系統。接著分析入侵者如何利用人爲管理疏失與系統設定上的漏洞，取得系統帳號／密碼與使用權限，並探討入侵者如何利用 Windows、Unix 系統現有的安全漏洞，竊取或破壞系統資源；之後研究入侵者如何利用不易被察覺的偵測技術，掃瞄網路缺陷及漏洞，擷取網路設施的資訊，最後探討網路入侵步驟與入侵趨勢，並提供網管人員制訂安全管理機制時的準則以及防制措施，使入侵攻擊與資訊竊取的困難度提昇，以有效提昇組織內部的網路安全。

關鍵字：網路安全、網路管理、入侵偵測

Abstract

An Intrusion detection system (IDS) generally focuses on the analysis and detection of network anomalies. In fact, all the messages that might threaten a network system and the behaviors of improper network accesses are those should be analyzed when one tries to detect network attacks. In order to improve security degree of a network, we should analyze all kinds of network threats and establish a proper access and monitoring mechanism. In this paper, we first study how intruders gather network packets or obtain illegal access authority by hacking network drawbacks. Second, we discuss how intruders use rarely monitored packets and tunnel to build backdoors for stealing information from information systems, and the way they perform connection hijacking by using spoofing IP and TCP sequence number surmise. Third, how intruders obtain system accounts through security weakness of an operation system is stated. Forth, we describe how hackers make use of undetectable methods to scan network systems to avoid detection by some security mechanism. Finally, we study intrusion procedures and trends, and provide suggestions for network administrator to set up a safer network environment. The purposes are to increase the difficulties of intrusion and illegal accesses to network facilities so as network security can be dramatically improved.

Keywords：Network security、Network management、Intrusion detection

目錄

圖目錄

表目錄

第1章 緒論

1.1 研究動機

隨著網路應用技術與服務的日漸成熟，現今的網路的入侵／攻擊行爲，與往昔僅僅單純的破壞網站或使系統服務中斷已有很大的不同。入侵者可以透過網路，利用木馬程式、系統設計缺失或網路協定的疏漏等問題等，發展出許多複雜又多樣化的入侵攻擊手法，不但隱藏了攻擊來源，又能成功地入侵系統主機以竊取機密資料、篡改文件與破壞系統，攻擊成功的機率與破壞力也大幅地提昇，使得安全防制更加困難。

美國著名入口網站雅虎（Yahoo！）在 2000 年 2 月遭到駭客以「阻絕服務」（Denial of Service，DoS）方式攻擊，對網站伺服主機傳送大量封包，使其窮於應付連線要求，耗竭系統資源，導致負荷過重而癱瘓，無法服務數百萬的網路使用者，時間長達三小時。之後，包括四大熱門網站，拍賣網站 eBay.com、購物網站 Amazone.com、Buy.com 及美國有線電視新聞網網站 CNN.com 等，亦遭受到 DoS 攻擊，損失達數百萬美元。另外，在 2001 年 4 月中美撞機事件，所引爆的中美網路駭客大戰，根據 CERT 統計[1]，當時遭到攻擊的作業平台中，Windows based 占 71%，Unix based 占 21%，其他 8%。對於層出不窮的駭客入侵攻擊事件，除了系統／軟體本身設計上的缺失，尚有內部人員不當的存取與不當的存取管理，這些問題的起因，大都是網管人員忽略網路安全的重要性所致。

針對網路系統所存在的安全問題，本論文將研究駭客在入侵網路的過程中，常用到的各項技術及工具，包括如何掃瞄系統弱點、辨認系統型態、擷取存取權限、甚至開啓後門等，並對網路所面臨的安全威脅做一分析；另一方面，我們將從系統入侵者的威脅及系統弱點的角度，建立一套有效的安全機制，並歸納出一些網路安全防禦的基本原則，避免入侵者盜用系統資源、竊取機密資料及防範駭客的惡意攻擊等，俾提昇網路入侵的困難度及降低入侵事件的損害。

1.2 研究範圍

本研究係從資訊科技的角度，分析與探討在 TCP/IP 協定架構下，所面臨網路的威

脅與存取監控所面對的問題，圖 1-1 所示爲本研究之研究架構。

1. 在網路安全威脅方面，從技術層面分析網路架構上各項安全威脅，包括網路設施在設計上的缺失及缺陷、通訊協定的問題、作業系統的缺失等，並研究各種網路入侵和攻擊的案例，探討相關文獻，瞭解入侵者如何尋找網路系統安全最薄弱的地方？使用哪些手法攻擊系統？使用哪些掃瞄技術偵測系統？及在入侵系統後的行爲？進而分析網路架構所存在的各項缺陷／缺失，目的是讓網管人員在架構及管理網路時，能夠採取適切的保護措施來保護系統資源與網路通訊的安全。

2. 在入侵偵測方面，從駭客入侵網路的手法探索偵測技術，包括掃瞄技術、駭客行爲等，研究駭客常用掃瞄技術的原理、入侵網路系統的流程、及瞭解入侵／攻擊手法的趨勢，目的是提昇網管人員在技術層次的控管與改善，以制定入侵偵測的防制方法。

3. 在網路存取監控方面，從管理層面控管上述缺失，包括網路的監控項目與地點、網路防火牆、入侵偵測、存取控制等，研究目前現有之網路監控、入侵偵測與存取控制等機制，在面對目前可能的入侵／攻擊行爲，如何偵測可疑的攻擊封包？如何偵測異常的網路連線？如何監測可能的入侵行爲？如何適當地使用防火牆防範不法的存取？並提出適當的防範方法與行政管理原則，目的在加強監控網路內部未經授權的服務與安全較薄弱的節點，以建構安全的傳輸與存取環境，保護網路與系統的安全。

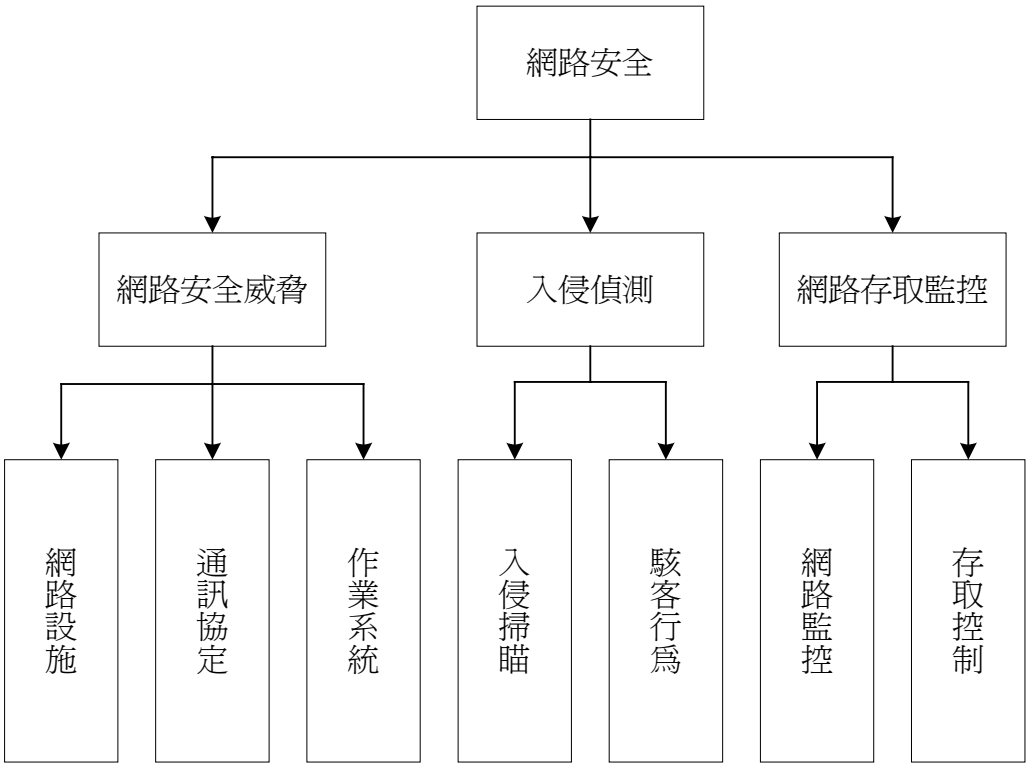

圖 1-1　研究架構

1.3 研究流程

本研究依據「網路安全威脅」與「網路安全防制」二大方向，進行文獻蒐集、探討與分析，包括有文獻蒐集、案例研究、入侵攻擊手法研究、網路安全威脅分析、網路安全理論探索與研究、入侵偵測技術研究、防禦策略／技術研究、網路監控技術研究等，經由分析歸納與整理，而獲致結論與建議。研究流程如圖 1-2。

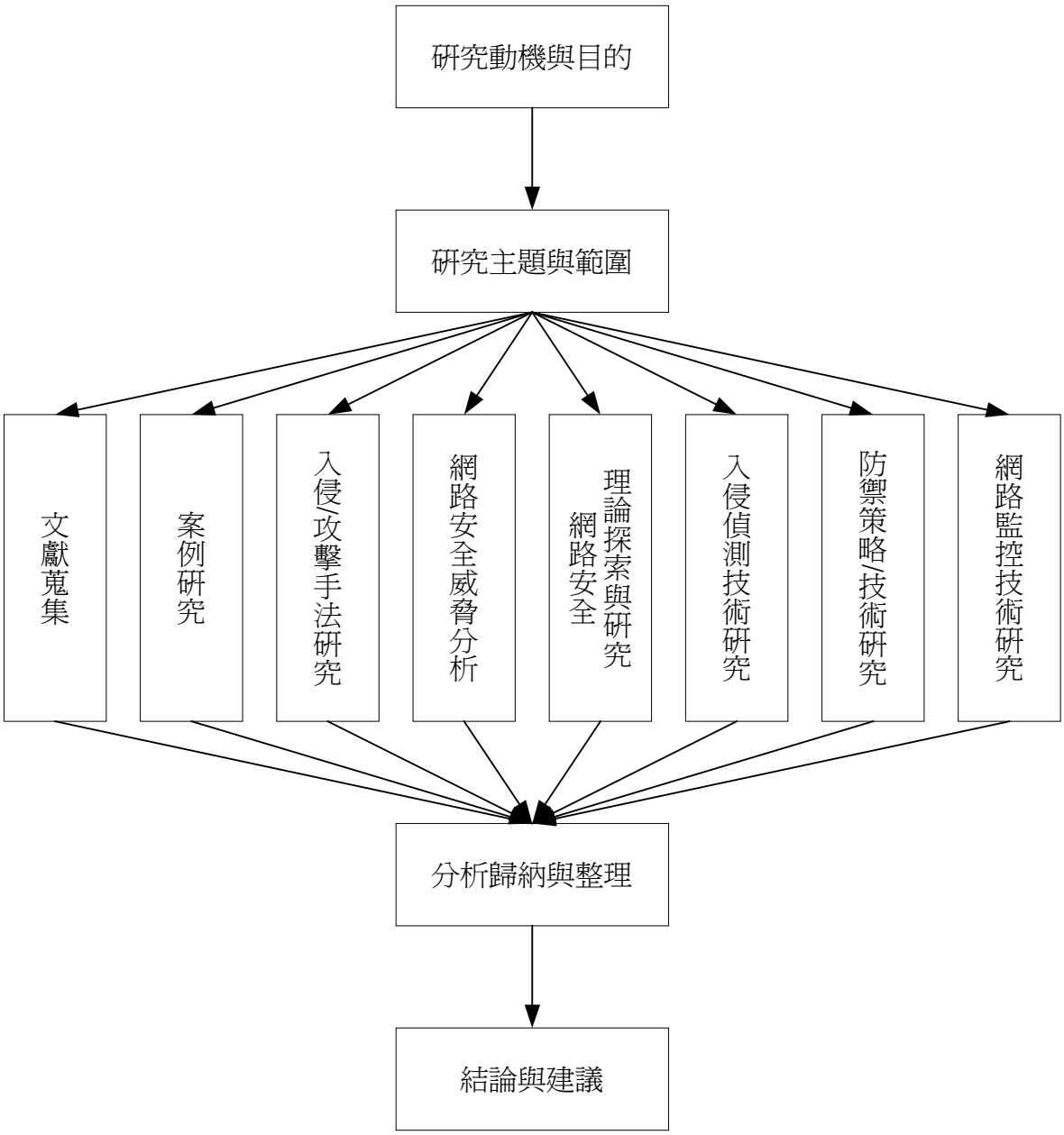

圖 1-2　研究流程圖

1.4 章節結構

本論文共分成五個章節：第二章介紹各項研究背景知識；第三章探討網路的各種漏洞，並闡述網路入侵者的入侵步驟、入侵趨勢及掃瞄技術等；第四章從網路監控的角度分析任何可能的攻擊行為或異常之處，並探究如何監控網路內部未經授權的服務與安全

較薄弱的節點，提出適當的調整安全管理方式及安全策略。第五章爲本論文之結論，並提出未來研究方向，以供後續研究參考。

第2章 文獻探討

2.1 駭客之定義

所謂電腦駭客（Hacker）原始的定義[2, 3, 4]是敍述具有“技術專才”或“有志解決問題及超越極限之人”。是指致力於促進科技隨手可得，而有崇高理想的人，或是意欲創造美好事務，並藉著科技的力量來幫助他人的人。也就是現今立身於電腦業且醉心於科技的運用，來解決問題並創造解決方案的人。然而由於一般大眾媒體的引用不當，使其喪失原有的意義，今天駭客的意義是指利用電腦以非法的手段與方法，未經授權逕行進出他人電腦系統，或使用高超技術進行不法行爲的電腦玩家，又稱爲快客（Cracker）。而今，電腦系統的管理人員爲了防範駭客的入侵或破壞行爲，必須以網路安全設備阻擋未經授權或非法的入侵或攻擊行爲，這些設備包括網路防火牆、入侵偵測系統等，當然，一旦遭到入侵，追蹤駭客的系統也是重要的嚇阻力量之一。

2.2 入侵攻擊手法

藉由瞭解駭客或入侵者的入侵／攻擊手法，有助於提昇管理人員在網路安全的應變能力，保障系統資源安全，以下分別敍述各種入侵攻擊手法[5, 6]：

2.2.1 DoS 攻擊

阻絕服務（Denial of Service，DoS）攻擊，是藉由大量的封包或 TCP/IP 協定的疏漏，消耗網路的頻寬或耗竭系統資源，例如，CPU、Process、Memory 等，阻撓系統或網路運作。可分爲：

1. 傳輸層攻擊

攻擊者利用 TCP/IP 傳輸層（Transport Layer）的封包，例如，TCP、UDP 等，攻擊目標主機，包括：

(1) TCP SYN flood DoS

攻擊者 A 是利用 TCP 連線三階段確認（Three-Way Handshake）的機制的疏漏，以每秒送出數千個 TCP SYN 封包至目標主機 T 請求（Request）連線，T 收到 A 的連線請求後，會回覆 SYN/ACK 封包確認，但 A 並不理會，使得 T 在 SYN Queue 中累積過多的等待（Waiting）回覆確認，而耗盡 CPU 時間、記憶體等，而造成 T 無法繼續提供服務。

(2) UDP flood DoS

UDP flood DoS 攻擊又稱爲 Fraggle 攻擊，攻擊者透過僞造來源的 UDP 封包，送到目標網域的廣播位址（Broadcast IP），讓該網域內的所有主機回應 echo 封包至目標主機 T，產生擴大效應的資料流，使得 T 忙於回應，造成網路壅塞或使 T 之 CPU 負荷過重無法提供服務。即使該網域的 echo 回應功能被關閉，路由器仍會產生 ICMP（type 3, Destination Unreachable）封包，一樣達到 DoS 消耗頻寬的效果。

2. 網路層攻擊

攻擊者利用 TCP/IP 網路層（Network Layer）的封包，例如，IP、ICMP、IGMP 等，攻擊目標主機，包括：

(1) Ping Flood DoS

攻擊者 A 藉由傳送大量的 ICMP echo 封包至目標主機 T，以耗盡 T 的網路頻寬。

(2) Ping of Death

攻擊者利用 TCP/IP 協定的疏漏，對目標主機 T 發送過長的 Ping 封包（例如，超過 65535 Bytes。而乙太網路封包最大傳輸單元（Maximum Transmission Unit，MTU）有 1518 Bytes 的上限，若沒有做好資料長度的限制時，過長的資料覆蓋到 T 的其它部份資料或系統，有可能會造成 T 發生錯誤而當機。

2.2.2 DDoS 攻擊

分散式阻絕服務（Distributed DoS，DDoS）攻擊是攻擊者 A 從遠端遙控許多傀儡主機 F，再下達攻擊指令給 F，導致 T 無法提供正常服務。攻擊類型如下：

1. TFN DDoS

Tribe Flood Network（TFN）[7]是針對 UNIX 作業系統的 DDoS 攻擊工具，攻擊者 A 會入侵許多傀儡主機 F，當 A 對 F 下達攻擊指令時，F 會對目標主機 T 送出大量的封包（例如，SYN、UDP、ICMP、Smurf 等）攻擊，造成 T 無法提供服務。

2. TFN 2K DDoS

TFN 2K 是 TFN 的更新版本，它允許使用隨機的連接埠，還支援加密功能，而且可以在 SYN、UDP、ICMP、Smurf 這些攻擊型態之間隨機變換，使網路設施（例如，路由器、網路防火牆、目標主機等）與入侵偵測系統，無法有效偵測／監控防範，造成網路頻寬癱瘓或系統資源耗竭。

3. Trin00 DDoS

攻擊者 A 藉由 UDP 封包入侵許多傀儡主機 F，在 F 植入木馬 Trin00 Daemon，該木馬受控於 A 的 Trin00 Master，當 A 對 F 下達攻擊指令時，F 會對目標主機 T 送出大量的 UDP 封包攻擊，並不斷改變目的地埠號，造成 T 產生大量 ICMP Port Unreachable 訊息，使 T 無法正常提供服務。

4. Stacheldraht

Stacheldraht 是綜合 TFN 與 Trin00 的特性，增加攻擊者 A 與傀儡主機 F 之間 telnet 加密連線，及提供 TCP 與 ICMP echo reply 兩種封包，讓 A 與 F 之間溝通更直接，對系統造成的威脅也更大。

2.3 入侵偵測系統

雖然入侵偵測系統已發展相當時日，但是，大部份的人卻對於它的研發與研究歷史

不瞭解，而導致一再地犯相同的錯誤，浪費許多時間在解決不重要的問題上。我們提出幾個較具代表性的入侵偵測系統，以前瞻的角度描述入侵偵測的歷史。以下分述之：

2.3.1 NSM

在 1990 年由加州大學 Davis 分校所發展 NSM（Network System Monitor），是第一個把網路流量（Network Traffics）當成主要資料來源的入侵偵測系統[8]。它在 SUN UNIX 工作站上執行，而主要功能如下：

1. 把 Ethernet 網卡切入錯亂模式（Promiscuous Mode）。亦即可以監控不屬於該機器的網路封包，聽取該網段所有的網路流量。

2. 分析封包的通訊協定，以擷取更多封包的特徵。

3. 採用矩陣式（Matrix-Based）的方法分析這些特徵。

NSM 的架構正代表了當時大多數商業產品的架構，在入侵偵測領域是一個相當重要的里程碑，是第一個嘗試將入侵偵測用在異質性網路環境的系統。

2.3.2 DIDS

在 1991 年由 Snapp 提出 DIDS（Distribute Intrusion Detection System），是第一套整合主機式和網路式的入侵偵測系統，它的原始觀念是採取中央控制的技巧[9]。該系統點出了一個問題。首先，在複雜而且廣大的網路環境裡，要追蹤網路使用者和檔案是很困難的工作。這項功能非常重要，主要有兩個因素：

1. 入侵者總是在網路系統間來回穿梭，藉此隱藏真實的身份和地點。實際上某些入侵者還會發動分散式的攻擊，而每個攻擊階段都影響不同的系統。

2. 要發現誰是入侵者是一件很麻煩的事，必須要蒐集證據，然後交給執法者來施以適當的刑罰。

其次，我們怎麼知道在系統不同層級的資料和發生的事件扯上關係，而這些資訊可

以讓我們看到它們是如何影響整個系統的。DIDS 採用了一種方法，他藉由六個階層的入侵偵測模式和資料做關聯，而每個階層都呈現出轉換的效果。

2.3.3 MIDAS

在 1998 年由美國國家電腦安全中心（National Computer Security Center, NCSN）所發展 MIDAS（Multics Intrusion Detection and Alerting System），是第一個能監控網際網路存取環境的入侵偵測系統[10]。目的是監控 NCSC 的 Dockmaster 系統，這是一部 Honeywell DPS 8/70 的機器，上面執行高階安全的 Multics 作業系統。利用從系統所蒐集的資訊擴充成日誌稽核資料，這些資料被組織起來重建成交談專檔（Session Profile），再與正常行爲的使用者專檔作比較。MIDAS 在當時就像入侵偵測專家系統（Intrusion Detection Expert System, IDES）[11]，與其他系統一樣，採用混合式的分析策略，結合統計的異常偵測方法（Anomaly Detection），並配合規則式（Rule-Based）的專家系統。這個統計和規則式分析的部分是用 LISP 所寫，並在 Symbolics 工作站上執行。MIDAS 在 1989 年上線，持續監控 Dockmaster 直到 1990 年代中期。

2.4 TCP 三階段確認

TCP 傳輸協定[12]提供連線導向、可信賴的傳輸服務，在客戶端（Client）與伺服端（Server）雙方在進行通訊之前，必須先透過 TCP 三階段連線（TCP Three-Way Handshake）機制（如圖 2-1）建立連結，以設定傳輸資訊狀態的初始值，例如，Socket、Sequence Number、Window Sizes 等；但是終止連線時，必須使用四個階段（如圖 2-2），因爲 TCP 是全雙工連線，亦即在連線中的 Client 端停止輸出，但是仍可以接收來自 Server 端資料的能力，此特性亦稱 TCP 半關閉（half-close）。下面將分別敍述連線的建立與終止步驟：

1. TCP 連線的建立

   (1) Client 端會向 Server 端送出一個 SYN 封包，含有初始序號 isn1（Initial Sequence Number）及 Server 端的連接埠（Port）的連線請求（Request）。

(2) Server 端接收到 Client 端的連線請求後，則會回應一個含有初始序號 isn2 與確認序號 M（M=isn1+1）的 SYN/ACK 封包確認。

(3) Client 端收到 Server 端的回覆封包（即 SYN/ACK）後，則回覆含有序號 N（N=isn2+1）的 ACK 封包確認連線。

透過此三個階段，建立 Client 端與 Server 端的連線，我們稱爲三階段連線，亦稱三向握手。之後的封包之序號，以遞增的方式增加。

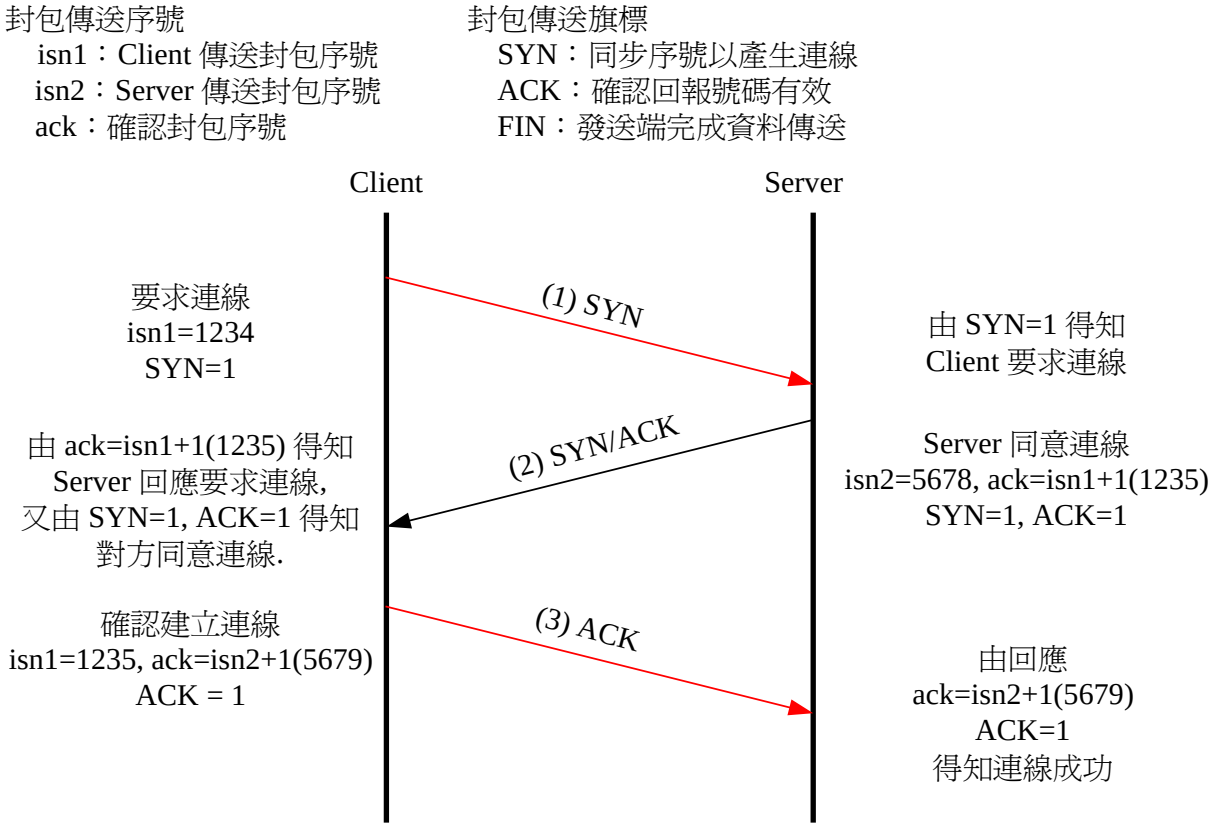

圖 2-1　TCP 三階段建立連線之程序

2. TCP 連線的終止

(1) Client 端會向 Server 端送出一個 FIN 封包，含有初始序號 isn1 及 Server 連接埠的終止連線要求，同時開始等待 Server 端同意終止連線。

(2) Server 端收到終止連線要求後，則會回應一個含有序號 M（M=isn1+1）的 ACK 封包，告知 Client 端已收到終止要求。

(3) Server 端同時會傳送檔案結尾（EOF）符號給它本機 Server 端的應用程式，關

閉此應用程式，並送出一個含有序號 isn2 的 FIN 封包，同意終止連線，

(4) Client 端則回覆含有序號 N（N=isn2+1）的 ACK 封包確認終止連線。

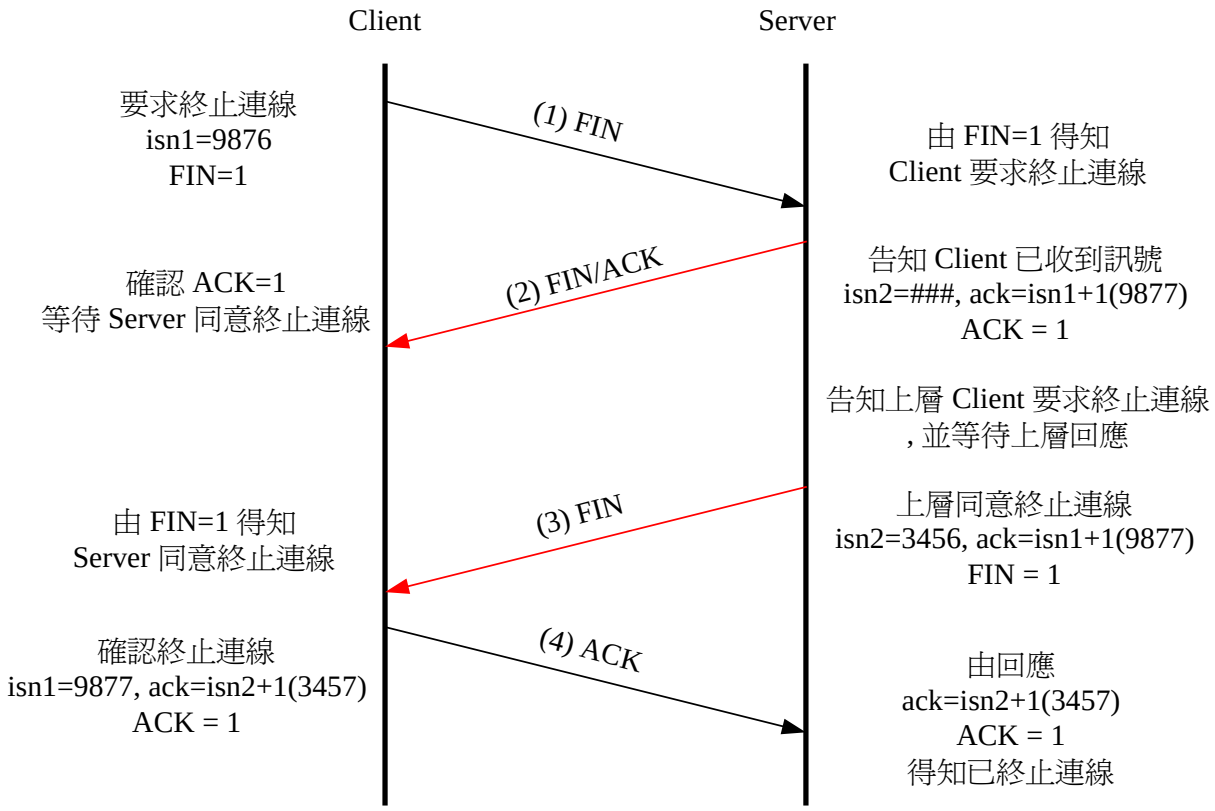

圖 2-2　TCP 終止連線之程序

2.5 國際資通安全管理標準

所謂標準就是經由大多數國家或團體認定，以爲各項活動有關的規則、指導綱要或特性所建立之文件，國際標準組織（International Organization for Standardization，ISO）爲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爲「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 BS 7799、EA7/03，COBIT 等。

ISO/IEC 17799：2000（BS 7799 Part I）的全名是「Code of practice for information security management」，是一個由英國 BSI（British Standards Online）在 1995 年 2 月所提

出、1995 年 5 月修訂，爲目前國際上最知名的安全規範[13]。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，此部份於 2000 年 12 月被 ISO 接納成爲標準。我國工業局標準檢驗局依據此標準轉定爲國家標準 CNS 17799，建議組織作爲建立資訊安全管理制度之指導文件。

而 Part II「Specification for Information Security Management Systems，ISMS」，內含資訊安全管理系統的詳細說明書、詳述 IT（Information Technologic）安全應用與稽核所應遵循的架構，作爲資訊安全管理系統（ISMS）評估的基準，是一個正式驗證的標準，於 2002 年 9 月 5 日重新修訂公佈 BS 7799-2：2002。我國工業局標準檢驗局依據此標準轉定爲國家標準 CNS 17800，爲我國受理資訊安全管理制度之驗證標準。表 2-1 所示爲資訊安全管理標準 BS 7799-1 與 BS 7799-2 之比較。

表 2-1　資訊安全管理標準比較表

安全標準	BS 7799-1	BS 7799-2
英文全名	Code of practice for information security management	Specification for Information Security Management Systems
用途	資訊安全管理系統實務準則	資訊安全管理系統驗證規範
目的	提供管理要領、控制目標及方法，確保資訊之機密性、完整性及可用性	確認資訊安全管理系統符合標準之要求，並尋找出提供改善資訊安全之方向
含括項目	10 大管理要項、36 個執行目標、127 項控制項目	PDCA（Plan-Do-Check-Act）管理循環
經 ISO 認證	ISO/IEC 17799：2000	
經 CNS 認證	CNS 17799	CNS 17800

2.5.1 ISO/IEC 17799：2000（BS 7799-1）

ISO 17799：2000 內容計分爲十大管理要項，卅六個執行目標及一二七項控制項目，僅就十大管理要項摘述如下：

1. 安全政策（Security policy）

「安全政策」的目標：提供管理階層對資訊安全的指導與輔助。管理階層應該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。

2. 安全組織（Security organization）

「安全組織」的目標包括：

(1) 管理組織內部的資訊安全。

(2) 維護組織的資訊處理設施和資訊資產被第三方存取時的安全。

(3) 在委外作業時，應該維護資訊之安全。

3. 資產分類及控制（Asset classification and control）

「資產分類及控制」的目標包括：

(1) 維持對於組織資產的適切保護。對組織資產做適當的保護。

(2) 確保資訊資產受到適當程度的保護。

4. 人員安全（Personnel security）

「人員安全」的目標包括：

(1) 降低因人員錯誤、偷竊、詐騙或不當使用設施所造成的風險。

(2) 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織資訊安全政策的能力。

(3) 可經由適當的管道回報安全事件、安全缺失及安全弱點。

5. 實體及環境安全（Physical and environmental security）

「實體及環境安全」的目標包括：

(1) 防止對企業營運所在地及資訊未授權的進入與存取、破壞及干擾。

(2) 預防資產遺失、破壞或損失，和防止企業營業活動遭受干擾。

(3) 防止資訊或資訊處理設備損毀或遭竊。

6. 通訊與操作管理（Communications and operations management）

「通訊與操作管理」的目標包括：

(1) 確保正確與安全地操作資訊處理設備。

(2) 將系統失效的風險降至最低。

(3) 保護軟體和資訊的完整性。

(4) 維護資訊處理和通訊服務的完整性及可用性。

(5) 確保網路中資訊之安全性，以及保護支援之基礎設施。

(6) 防止資產遭受損害以及企業營運活動遭受干擾。應控制媒體並對其進行實體保護。

(7) 防止組織間交換資訊時資訊遭受遺失、修改或不當使用。應控制組織間的資訊和軟體的交換，並且交換應符合有關立法。

7. 存取控制（Access control）

「存取控制」的目標包括：

(1) 控制對資訊的存取。應該根據業務要求和安全要求對資訊存取與業務流程加以控制。

(2) 防止對資訊系統的未經授權存取。

(3) 防止未經授權的使用者存取。授權使用者的合作態度對有效地保障安全至關重要。

(1) 保護網路化服務。應該控制對內外網路服務的存取。

(2) 防止未經授權的電腦存取。

(3) 防止對資訊系統中資訊的未經授權存取。

(4) 偵測未經授權活動。應該對系統進行監控，檢測與存取控制政策不符的情況，將可以監控的事件記錄下來，在出現安全事故時作爲證據使用。

(5) 保證在使用可移動式電腦運算及電腦通訊遠距工作設施時資訊的安全性。

8. 系統開發及維護（Systems development and maintenance）

「系統開發及維護」的目標包括：

(1) 保證安全機制內建於資訊系統中。

(2) 防止應用系統中使用者資料遭受遺失、修改或不當使用。

(3) 保護資訊的安全性、真實性或完整性。

(4) 確保資訊科技的專案及支援性活動以安全的方式來進行。

(5) 維護應用系統軟體和資訊的安全性。

9. 業務持續運作管理（Business continuity management）

「業務持續運作管理」的目標爲防止業務活動中斷，確保重要業務流程不受重大故障和災難的影響。

10. 符合性（Compliance）

「符合性」的目標包括：

(1) 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。

(2) 保證系統符合組織的安全政策和標準。

(3) 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擾和對系統稽核過程的干預。

ISO/IEC 17799 包含了所有面向的最先進企業安全政策，從安全政策的擬定、安全責任的歸屬、風險的評估、到定義與強化安全參數及存取控制，甚至是防毒的策略。ISO/IEC 17799 風險評估技術適用於整個組織、或者組織的某一部份以及獨立的資訊系統、特定系統元件或服務等，進行風險評估需要系統化考量以下問題：

1. 安全故障可能造成的業務損失，包括由於資訊和其他資產的機密性、完整性或可用性損失可能造成的後果。

2. 當前主要的威脅和漏洞帶來的現實安全問題，以及目前實施的控制機制。

評估結果有助於指導用戶確定事宜的管理手段，以及管理資訊安全的優先順序，並實施所選的控制措施來防範這些風險。必須經過多次重複執行評估風險和選擇控制措施的過程，以涵蓋組織的不同部分或各自獨立的資訊系統。

依據 ISO/IEC 17799 風險評估方法論[14]風險存在於企業所有處理程序中，與競爭環境、法令符合性、保護 IT 系統的使用及其相關的企業活動、確保企業重要資訊的可靠性與有效性、及詐欺有關，所以風險與組織政策及策略直接相關，如擴充、企業再造、緊急投資、開發新產品及服務、經營加值服務或改變供應鏈管理等。

資訊安全目標是確保資訊的機密性（Confidentiality）、完整性（Integrity）與可用性（Availability），「機密性」指確保只有經過授權的人才能存取資訊；「完整性」指保證資訊及其處理方法的準確性和真實性；「可用性」指確保經過授權的用戶在需要時可以存取資訊並使用相關資訊資產，如避免資訊系統及網路服務遭到阻絕服務攻擊 DoS。ISO/IEC 17799 風險評估方法論是一個企業處理方法，其目的是爲了建立 ISMS（Information Security Management System）之範圍、差異分析風險評估項目及程序；評估風險步驟含：識別 ISMS 資產、資產的價值、弱點及威脅，評估資產、弱點與威脅時可能產生的衝擊及風險分析，如圖 2-3 所示[14]。

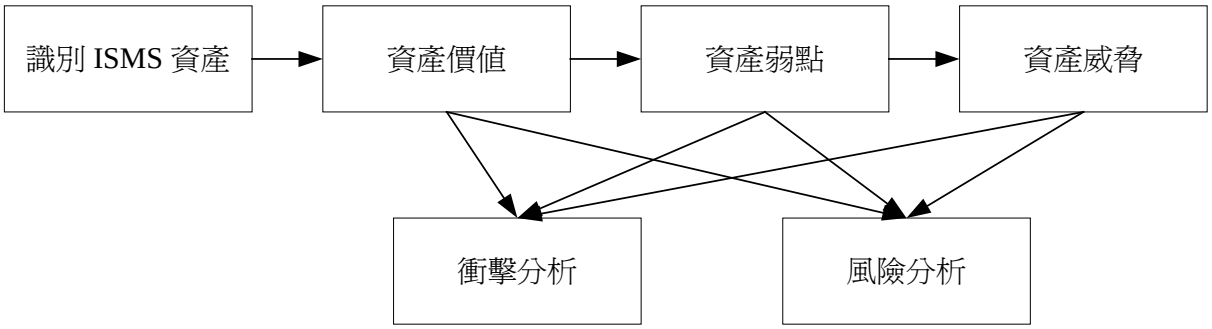

圖 2-3　ISO/IEC 17799 評估風險步驟

第3章 網路安全威脅

一個組織在網路建構完成後，爲了確保網路通訊的安全性，往往會隨著資訊科技的進步，調整其網路系統功能，通常會包括：對網路設備的安全規範及管理、網路各節點間（組織內部與外部）的通訊控制及安全審核機制等。

由於網際網路的普及，網路上可以找到許多簡單易用的入侵攻擊程式與指令集，使用者也很容易便能下載取得，因此，不是電腦玩家也能成爲駭客，以致於各種入侵與破壞事件層出不窮。要防禦這些不當的網路行爲，通常是在閘道、伺服器及網路的適當位置，設定嚴密的存取監控機制。然而，入侵攻擊手法不斷翻新且形態繁多，許多安全機制往往祇能從事局部的安全防制，因此，在面對網路各種的安全威脅，必須採取有力的保護措施來保護系統資源的安全。網路要做到比較安全的防禦，必須有全面性的考量，俾阻擋較多的入侵攻擊。然而知己知彼，必須要瞭解自己，也要瞭解對方，從而活用自己的長處，建置有效的安全措施／策略，才能防制來自網路的安全威脅，以下將分別探討在 TCP/IP 架構下網路硬體設施的缺陷、通訊協定上的疏漏、作業系統的缺失、網路系統的入侵技術等問題[15, 16]。

3.1 硬體設施的缺陷

在網路上，祇要網路設施設計不良或設定不當，都有可能成爲入侵者進入系統竊取資訊的門道。在本節中，我們將探討網路裝置，包含(1)路由器及(2)網路防火牆兩設施在存取控制上的瑕疵與常被駭客利用的溝通媒體。

1. 路由器是在網路層連接不同結構的網路，例如，Ethernet 與 Token Ring 等，並轉送不同的通訊協定（例如，IP、ICMP、IGMP 等）的封包，使其得以順利地到達目的地，圖 3-1 爲其示意圖。當路由器接收到網路封包時，會解析其標頭，分析其協定，俾交予專職處理之模組，例如，ICMP、RIP（Routing Information Protocol）、OSPF（Open Shortest-Path First Interior Gateway Protocol）處理之，以回應訊息。圖 3-2 爲 ICMP Redirect 轉向訊息的示意圖[12]

(1) 當主機 A 傳送 IP 資料報 P 至其預設的路由器 R1。

(2) 在 R1 收到 P 時，會在路由表中尋找路由路徑，發現 P 的下一行程（Next-hop）路由器應是 R2，此時 R1 會傳送 P 至 R2，在傳送同時偵測到 R1 與 R2 是在同一（區域）網路內，則 R1 就可以發送 ICMP Redirect 轉向訊息給 A，告知 A 更新路由表（Routing Table），以後 IP 資料報應該傳送到 R2。

(3) R2 再依 P 標頭所指定的目標位址、大小和優先順序，爲 P 選擇最佳傳輸路徑，使其得以順利迅速地傳送到指定地點。

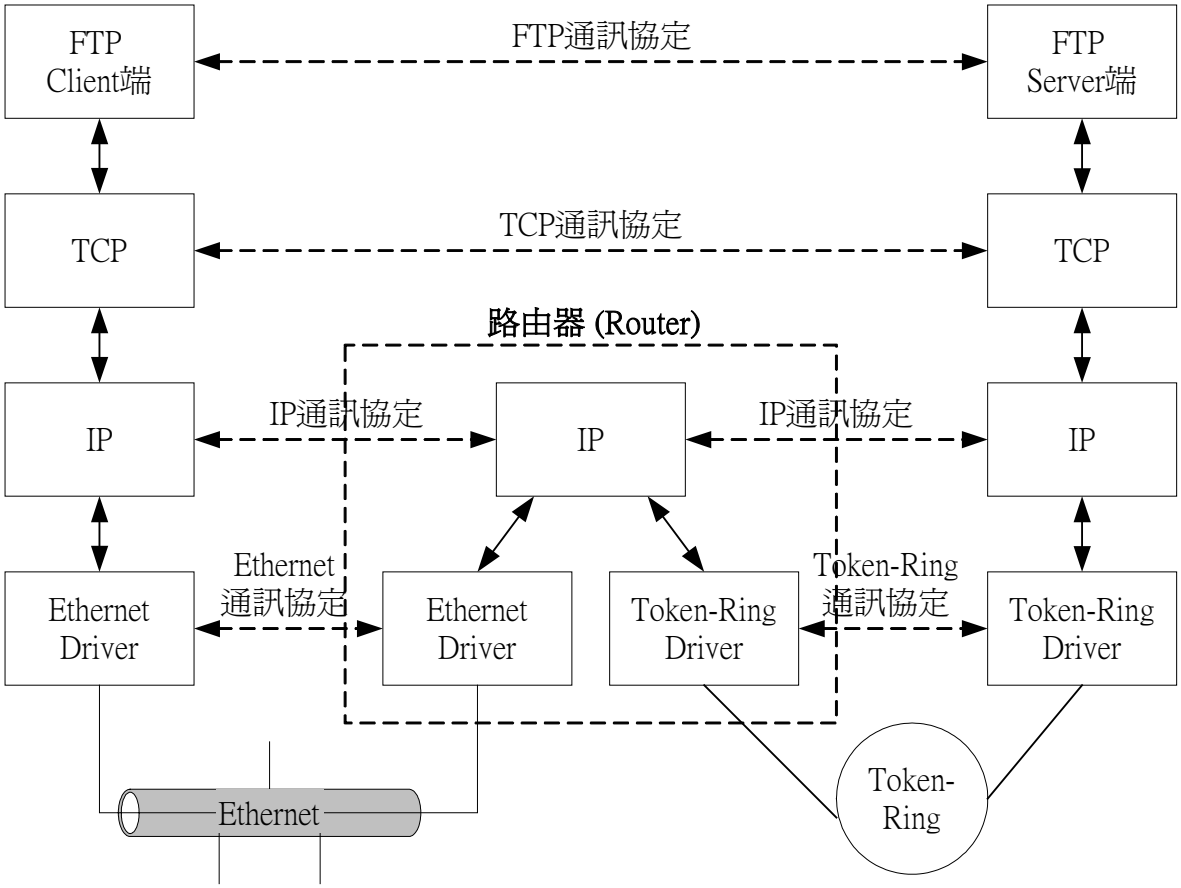

圖 3-1　在 TCP/IP 架構下，路由器連結不同結構的網路

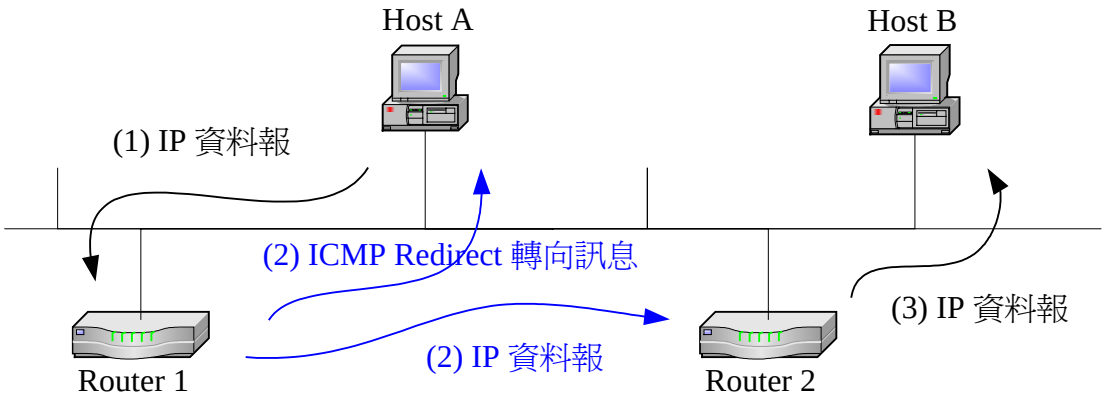

圖 3-2　ICMP Redirect 轉向訊息

2.　網路防火牆架設於網際網路與組織內部網路之間，是內部受信任網路與外部不受信任網路之間的通道，它提供各個網路間的控管功能及雙向的安全管理機制，管制所有進出組織的網路連線與封包，並留下詳細記錄，以供後續稽核與追查，不僅防止外界的入侵，也限制內部主機對外傳送不合法的資訊流。

3.1.1　溝通媒體

乙太網路（Ethernet）及環狀網路（Token Ring）爲兩個常見的共享式網路媒體（shared media）。乙太網路是利用載波感測多重存取／衝突偵測（Carrier Sense Multiple Access/Collision Detection，CSMA/CD）資料傳輸技術，將目的封包傳送到同一個區段（Segment）上的所有節點，當然也同時將資料送至此區段上的各聆聽裝置。駭客常利用封包擷取及密碼竊聽工具，例如，用 dsniff[17]竊聽以明文（Clear Text）方式傳送或使用安全性不佳的演算法加密的密文，並判斷網路媒體型態，再探索路由器 R1（如圖 3-3）的廠牌與作業系統版本，一旦 R1 被駭客確認出來，並入侵路由器後，就可以用 SRIP（Simple Routing Information Protocol） Message 更改 R1 的靜態路由（Static routes）使封包轉向，或假造一個 RIP v1（RFC 1058）／v2（RFC 1723）封包欺騙 R1，告知 R1 將封包轉送到一個未經確認的駭客主機 H 上，使所有要傳送到伺服主機 S 的封包，都會先送到 H，以擷取或竊聽通過 R1 上機密性的封包，然後予以丟棄或再轉送至目的地 S。

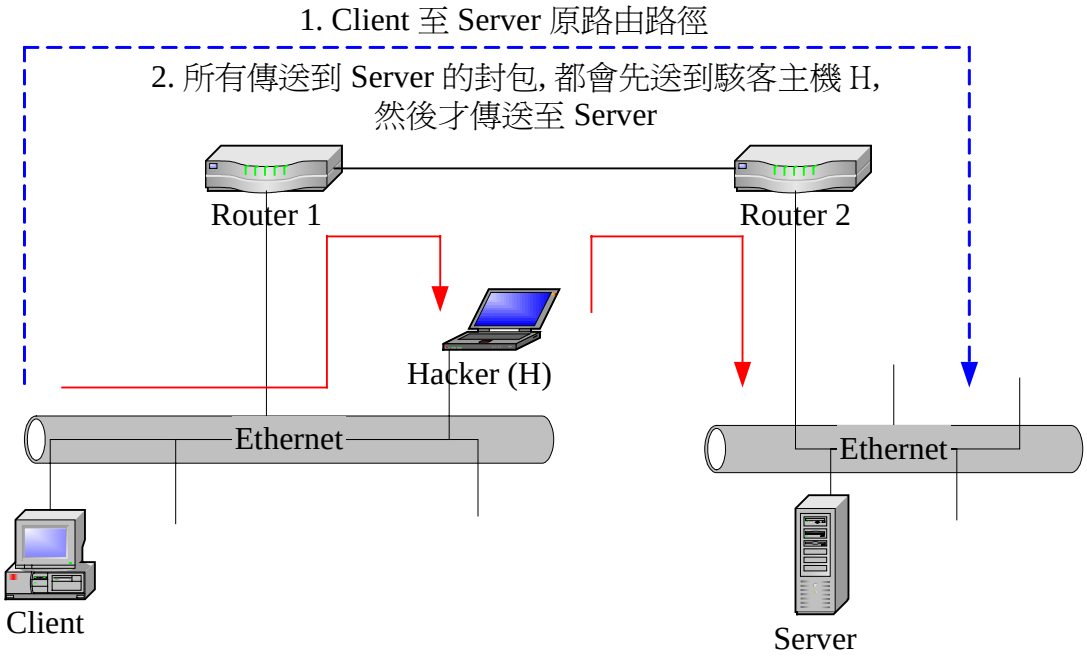

圖 3-3　RIP 假造更改路由路徑

3.1.2　存取控制

以下將介紹入侵者如何利用網路硬體設施在存取控制上的缺陷，從事系統入侵及非法竊取資料等活動，所利用的對象包含預設後門（Back door）與封包存取控制等。

1.　預設後門：

網路設備廠商爲了方便網路管理者管理網路設備，在出廠時會預先設定一個帳號與密碼（與一般管理帳號不同），表 3-1 所示爲 Cisco 和 3Com 常見之預設帳號與密碼，供後續更改設定或維護使用，即一般俗稱之「後門」，後門是入侵者常用來入侵系統的漏洞之一。例如，利用 traceroute（UNIX）或 tracert（Windows）工具，可以找出來源主機與目標主機之間所經過的主要路由器；再利用通訊埠掃瞄工具，找出目標路由器所有正在運作通訊埠的特徵，例如，對 Cisco 11.2 路由器預設開啓的 Port 23／2001 探詢時，會回覆要求輸入“User Access Verification：”與“Password：”的識別標誌訊息，或以 nmap[18]工具掃瞄 Port 13 偵測該裝置的作業系統時，會回覆”Remote operating system guess：Cisco Router / Switch with IOS 11.2”，即可得知廠牌及型號。亦可透過網管協定封包判斷，例如，利用 nmap 工具對 Cisco 11.2 路由器的 Port 1999 發送 TCP/SYN 封包，會發現其回應 RST/ASK 封包資料部份的來源埠爲“1999（Cisco-id）”標籤得知

Cisco-id，確實爲 Cisco 產品。表 3-2 所示爲網路設施預設通訊埠。

表 3-1　網路設施常見的預設帳號與密碼

裝置	帳號	密碼	權限
Cisco router	enable	cisco	administrative
	(telnet)	cisco routers	administrative
3Com router	admin	synnet	administrator
	debug	synnet	administrator
	manager	manager	administrator

表 3-2　網路設施的預設通訊埠

網路設施	**TCP 服務之連接埠號**	**UDP 服務之連接埠號**
CISCO ROUTERS	21(ftp)	49(domain)
	23(telnet)	67(bootps)
	79(finger)	69(tftp)
	80(http)	161(snmp)
	513(login)	
	514(shell)	
	1993(Cisco SNMP)	
	1999(Cisco ident)	
	23(telnet)	0(tcpmux)

Cisco switches	23(telnet)	0(tcpmux)
	7161	123(snmp)
	21(ftp)	7(echo)
	23(telnet)	67(bootps)
		69(tftp)
		161(snmp)

2. ICMP 與 UDP 封包的存取控制：

許多網路設施，例如，路由器、防火牆等，都允許 ICMP Echo、ICMP Echo Reply 及 UDP 封包進出，若其存取控制表 ACL（Access Control List）未給予嚴謹設定，例如，規則允許“所有來源 IP 位址”可以連線至“所有目的地 IP 位址”，對系統提供的“所有服務”存取動作“完全接受”，任意讓封包自由進出，ISP（Internet Services Provider）在替該組織做 DNS 區域移轉時，即某一 DNS 伺服器向另一台 DNS 伺服器傳遞更新資料，會有機會讓入侵者從組織外部掃瞄（例如，Nettlesting[19]提供的 axfr）整個內部網路，辨識所執行的作業系統與提供的服務，例如，FTP、SMTP、Telnet 等，洩漏系統資訊，而可能給系統帶來難以估計的損失，遭受惡意的攻擊或系統入侵的危險。

3.2 通訊協定的問題

網路攻擊的方法相當多，但仔細歸納後發現，有一大部份幾乎都是借助網路上的各種弱點與缺陷[5, 6, 15]，包括不被監控的封包、不易檢測之通道、及各項通訊協定的疏漏等。

3.2.1 通訊協定

網際網路是透過 TCP/IP 協定連接各網路節點，讓不同國家或不同網路的使用者可以彼此交換資訊、共用資源。網路協定通常都以層（Layers）發展，每一層都有各自的職責與功能。例如，鏈結層提供與實體網路間可靠之資料傳送與接收資料框的建立及錯誤偵測；網路層處理整個網路封包（例如，IP、ICMP、IGMP 封包）的繞送（Routing）；

傳輸層爲其上的應用層，提供兩主機間的資料流（例如，TCP 與 UDP）；應用層處理應用軟體的各協定（例如，Telnet、FTP、SMTP 等）[12]。

較有經驗的駭客，會利用不易檢測或監控的網路活動進行非法行爲，通常他們／她們會在網路傳輸封包上做一些手腳，攜帶惡意攻擊指令或病毒，進行各項入侵活動，下面將分別敍述通常不被監控的網路封包與不易檢測的隱藏通道。

3.2.2 通常不被監控的網路封包

ICMP 通常是做爲機器與機器間交談、相互傳遞錯誤訊息與其他需要特別注意之狀況之通訊協定，例如，當封包的傳遞發生錯誤時，路由器會發出 ICMP 的錯誤訊息，傳回給送出封包的主機。就因爲不是讓使用者直接用來傳遞訊息，一般而言，很少受到網路管理人員的監控。目前 ICMP 計有 18 種訊息，在一般的網路管理上，並不允許所有的 ICMP 訊息都能直接與網際網路各伺服器溝通，否則，攻擊者就可以發動 ICMP 阻斷服務攻擊（Denial of Service，DoS）。另外，網路管理者除了特殊原因外，並不對電子郵件 SMTP 與 POP（Post Office Protocol）等通訊協定，做全面性的監控，以免影響網路服務績效。因此，入侵者可以藉由電子郵件附加檔案的方式夾帶木馬，借由木馬程式竊取使用者帳號及密碼建立後門，以利於爾後入侵之用，這個通道隱然形成一個入侵系統的最佳路徑。

3.2.3 不易檢測的隱藏通道

一個有經驗的入侵者會透過加密通道，讓網路監視系統無法發揮作用。他們通常會以隱藏通道（Tunneling）的技術[5]，在一個已經被破解的系統上建立後門，再利用一般網路防火牆並沒有過濾 ICMP Echo、ICMP Echo Reply 與 UDP 流量的特性，將攻擊指令封裝（Encapsulate）在 ICMP 或 UDP 的標頭內，送到已被植入木馬（Trojans）的伺服器中，伺服器內的木馬就會執行此指令，而將執行結果封裝在 ICMP Reply 內，回傳給控制端（駭客）。例如，Loki 與 Lokid[20]（分別是用戶端與伺服端程式）即利用此觀念運作。其中，Loki 便是將攻擊指令封裝在 ICMP Echo 的程式裡，Lokid 即安裝在伺服端聽令行事之木馬，它會將執行結果（例如，取得 Email 帳號及密碼）裝在 ICMP Echo Reply 內，回傳給攻擊者。

3.2.4 通訊協定的疏漏

一般對 TCP/IP 的攻擊方法計有不實的 IP 位址、TCP 序號預測與連線劫持（connection hijack）等。

1. 不實的 IP 位址

不實的 IP 位址主要是僞造來源主機 S 之 IP 位址，以攻擊某一個目標主機 T ，使得 T 無法追溯 S，DoS 與 DDoS 攻擊爲其典型例子，而 Smurf 攻擊爲 DoS 攻擊方法之一，係利用導向廣播造成擴大效應方式進行，程序如下（請參考圖 3-4）：

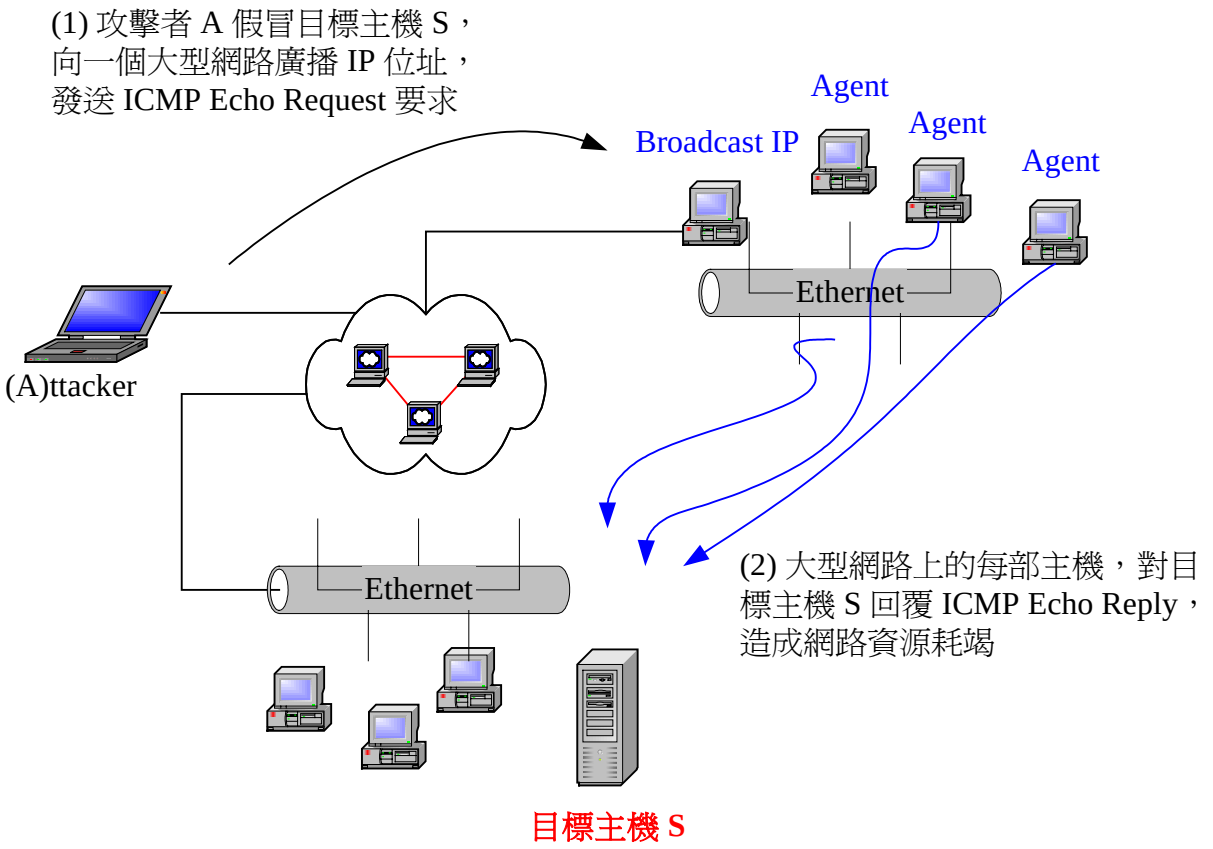

圖 3-4 Smurf DoS 攻擊

(1) 攻擊者 A 假冒目標主機 S 的 IP 位址，向一個大型網路 N 的廣播位址（Broadcast IP）發送 ICMP Echo Request 封包。

(2) N 中除了不在該網段及關閉 echo 服務功能的主機之外，其他大多數主機都會收

到這個封包，並且對 S 回覆 ICMP Echo Reply 封包訊息，造成 S 的網路頻寬耗竭。

另一個不實 IP 的例子是 DDoS 攻擊，方法是透過控制許多被入侵的主機，分散地對目標主機 S 發動攻擊，程序如下（請參考圖 3-5）：

(1) 攻擊者 A 控制許多已被入侵操控的某一台主機 H，並在 H 的主機上安裝具有僞造封包或自動掃瞄網路弱點的軟體。

(2) 利用 H 再入侵多台主機 G，稱爲代理主機（Agent），而以 G 爲入侵攻擊跳板。

(3) 當 A 發動攻擊時（或自動執行），經由 H 向代理主機 G，要求對 S 發出大量封包，以癱瘓 S 的網路頻寬或造成 S 當機，而使一般使用者無法得到正常的服務。

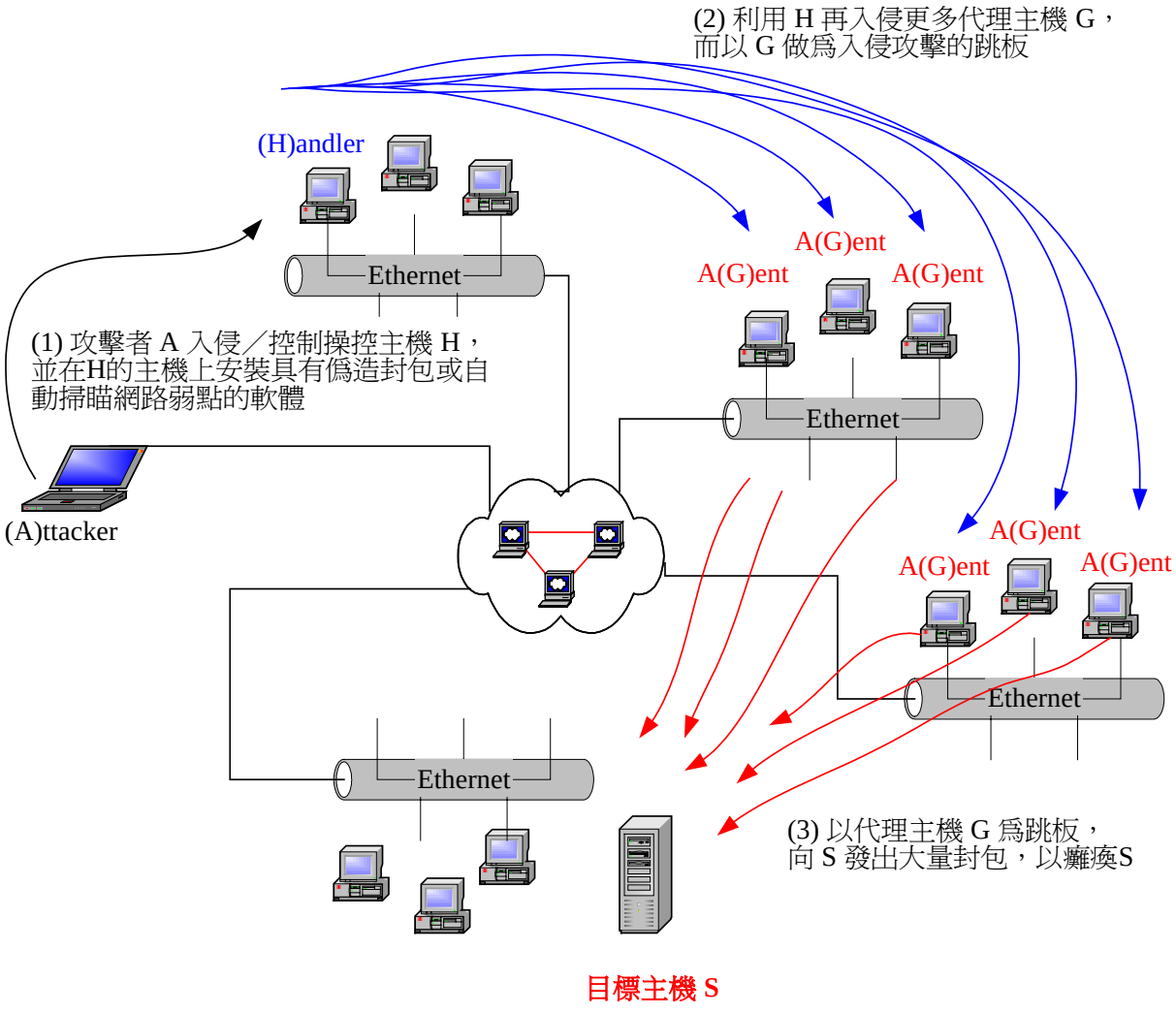

圖 3-5　DDoS 攻擊

2. TCP 序號預測

所謂 TCP 序號預測，是駭客 A 首先監視目標主機 S 與 S 之信任主機 C 之間的資料傳輸，並嘗試計算 S 下一個將傳送之 TCP 封包的序號，進而取得與 S 的連線，程序如下（請參考圖 3-6）：

(1) A 在監聽 C 與 S 之間的傳輸資料後，對 C 發動 TCP SYN 氾濫攻擊，造成 C 暫時無法回應其原先已連線之目標主機 S。

(2) A 僞造 C 的位址，傳送一個正常封包給 S，觀察其回應的 TCP 封包序號，預測 C 將對 S 送出的下一個 TCP 封包的序號。

(3) A 向 S 發送來源 IP（僞造）爲 C 且序號已經過計算的 TCP 封包，使 S 誤以爲是來自真正 C 的訊息，而繼續與 C 保持信任關係，獲取與 S 的連線，原先 C 與 S 的連線傳輸，由於封包序號已不連續，則會被 S 認爲是非法連線而中斷。接著 A 可以將木馬程式或偵測工具安全裝在 S，從而取得管理者帳號與密碼，再以管理者身份竊取資料或破壞系統。

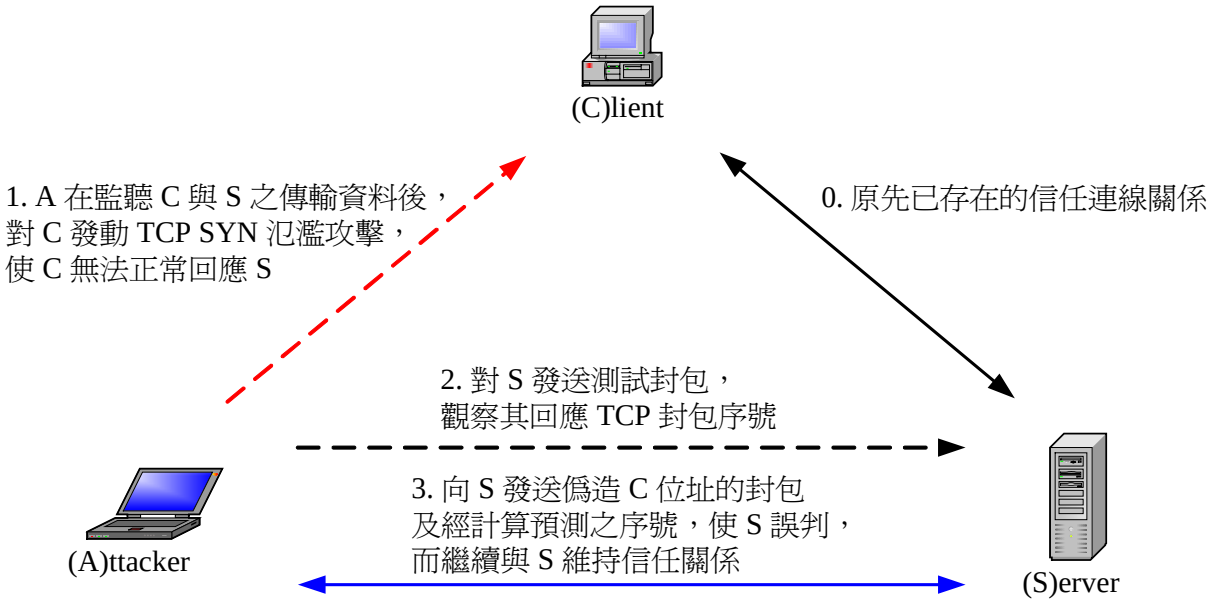

圖 3-6 TCP 序號預測

3. TCP 連線劫持

TCP 連線劫持是利用 TCP/IP 協定的疏忽，在共享式媒體上進行，係利用 CSMA/CD

資料傳輸技術特性及缺陷。如前述，駭客可以利用密碼竊聽工具 dsniff[17]及連線劫持工具 Hunt[21]等的輔助，監聽 TCP 的連線及來往封包，並取得連線上以明文（Clear Text）方式傳送或經不嚴謹演算法加密的使用者名稱、密碼等資訊（常見的以明文傳送資訊的應用程式有 FTP、telnet、POP、SNMP、HTTP 與 Oracle SQL*Net 等等），再以下述之程序劫持連線（請參考圖 3-7）：

(1) 追蹤連線取得目前封包的 SEQ 與 ACK 序號。

(2) 辨識目前連線的狀態，包括：已連線、穩定（stable）沒有資料正在傳輸、目標主機 S 的 SEQ 序號不等於信任主機 C 的 ACK 序號（即 S 正傳送資料至 C，若 C 尚未回應確認訊息 ACK 至 S 時，則 S 的 SEQ 序號會等於 C 的 ACK 序號）、C 的 SEQ 序號不等於 S 的 ACK 序號（即 C 正傳送資料至 S）等。

(3) 插入經過 TCP 預測序號之攻擊封包，取得與目標主機的連線[22]與信任關係，此時 C 再傳送至 S 的封包序號已不正確，則 S 會認爲 C 在對 S 傳輸不合法的資料，而中斷 S 與 C 的連線。

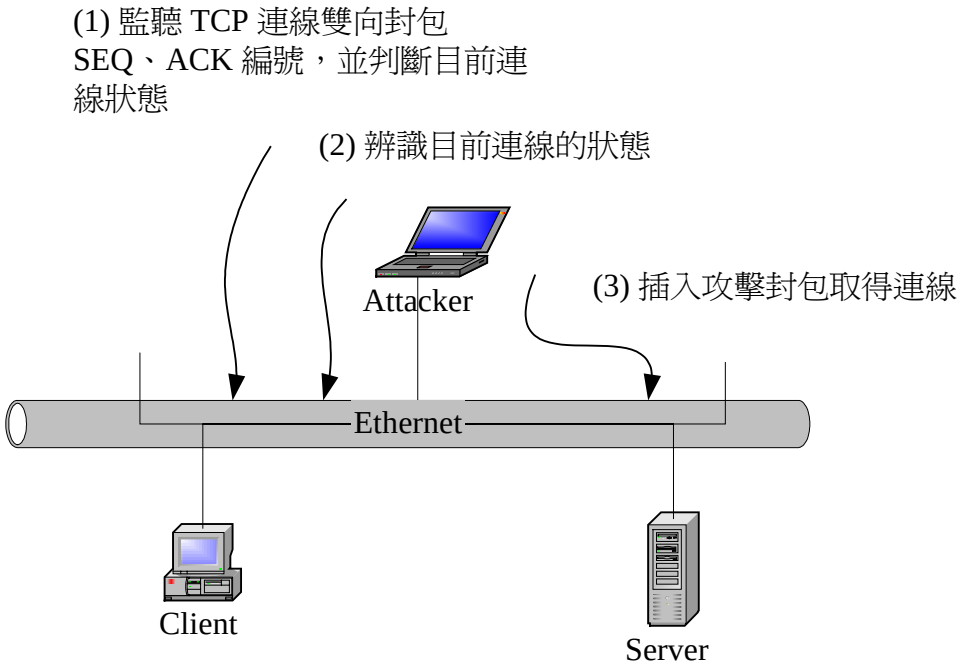

圖 3-7　TCP 連線劫持

3.3 作業系統／應用系統的缺失

以下歸納出幾個在作業系統上的安全漏洞[5, 23, 24]，包括有一般型漏洞、Windows 漏洞與 Unix 漏洞，以下分述之。

3.3.1 一般型漏洞

一般型漏洞之特質是在人爲管理與系統設定層面，未加以有效控管所致，而有下列數種情形。

1. 使用者若完全使用預設組態安裝應用軟體或作業系統，或未能適時的修正、或更新這些軟體的缺失版本，資訊系統就有可能會存在某些潛在的漏洞或弱點，入侵者便可以經由這些漏洞或弱點行入侵之實。

2. 使用簡單、容易記憶的使用者名稱與密碼，例如，以自己的姓名或公司廠牌做爲登入系統的帳號／密碼等，或使用權限管理不當，例如，不設定密碼等，便容易讓入侵者輕易猜測帳號／密碼，甚至不費吹灰之力，便可取得系統使用權限。

3. 網頁伺服器 CGI（Common Gateway Interface）或 ASP（Active Server Pages）的腳本（Script）設定不當，程式無法接受所輸入的資料或辨認語法錯誤，使得系統內部必須變更權限，並回應某些訊息，如此，易造成資訊洩漏，或讓使用者獲得不應獲得的權限，例如，駭客利用 Microsoft IIS（Internet Information Server）4.0/5.0 網頁瀏覽器“Malformed Hit-Highlighting Argument”漏洞缺失[2, 25]，輸入 URL：http://target/null.htw?CiWebHitsFile=/the.asp%20&CiRestriction=none&CiHiliteType=Full，就可以得到 IIS 根目錄下“the.asp”檔案的所有內容。原因是：webhits.dll 前面的 URL 是處理副檔名爲.htw 的 ISAPI（Internet Server Application Programming Interface）應用程式；但是，使用 null.htw 則不論該檔案是否存在，都可以透過 null.htw 執行 webhits.dll 提供的 Hit-Highlighting 查詢功能，使系統資訊外洩。

4. 開放不必要的連接埠（Port）或執行不必要的服務程式（例如，FTP、SMTP、Telnet），因爲入侵者常可透過這些開放的大門，擷取此聆聽埠的特徵，判斷出作業系統種類與應用程式版本，如果駭客事先已知道這些系統或程式已發現的缺失或漏洞，加上

管理人員未加以補強或管制，則系統是將暴露在遭到入侵的危險之中。

5. 缺乏網路層級、主機層級及遠端存取之監控與偵測機制，亦或日誌記錄不完整，均無法即時地獲悉系統狀況，而給予適時適切的修正或管理。

3.3.2 Windows 漏洞

Windows 漏洞的形成是在作業系統的預設機制與服務程式，未詳盡考量安全特性所造成，計有下列幾種。

1. 安裝 IIS 時，也會自動安裝索引服務（Indexing Services）ISAPI，並以 DLL（Dynamic Link Library）爲其副檔名。入侵者曾利用有些 DLL 檔（例如，idq.dll）接受過長的字串，內部無法處理，而發生所謂「緩衝區溢位（Buffer Overflow）」，造成系統的執行堆疊被覆蓋，此時因 IIS 之設計不當，使用者可以接著執行非法的指令或程式碼（例如，獲取系統（SYSTEM）管理權限），卻不受管制。在獲取管理權限後，進而接管 IIS，而以 SYSTEM 帳號執行任何指令。

2. 網路管理者（LAN Manager）密碼的簡易加密（Encryption）機制，因限制密碼長度祇有 14 個字元，並且會被轉換成大寫字母，再分割爲兩個 7 個字元的字串，因而非常容易被破解，保護效果不佳。

3. SMB（Server Message Block）協定用以分享檔案、印表機、序列埠，並使用 named pipes 與 mail slots 在電腦間通訊。在網路環境中，設置伺服器（Server）的目的是提供可利用的檔案系統和資源給客戶端（Client），當客戶端向伺服器發出 SMB Requests 時，伺服器會回應 SMB Responses。攻擊者可以利用使用者帳號或以預設匿名方式傳送假造的 SMB Requests 封包，對目標伺服主機 S 發動 DoS 攻擊，使 S 忙於回應，負荷過重而癱瘓，無法提供服務[26, 27]。

4. 預設的網管協定 SNMP v1（RFC 1157）／v2（RFC 1446）（Simple Network Management Protocol）[28, 29]代理程式（Agent）的社區名稱（Community name）（即密碼）是一組未經過加密的字串，表 3-3 所示爲各廠牌路由器常見的社區名稱／預設密碼[5]。入侵者可以此預設值在遠端進行設定及接管各式網路設備，以控管網路。例如，SNMP 在可讀／可寫（Read/Write）模式下，攻擊者 A 就可以使用 Network Associates

提供的密碼竊取工具 SniffPro[30]擷取 SNMP 社區名稱，插入或修改路由器的靜態路由（Static Routes）資訊，將路由轉向至 A 所指定的網址（例如，網頁伺服器），造成使用者的連線都會指向此網頁，而不是使用者所希望連線的網址。

表 3-3　路由器常見的社區名稱／預設密碼

廠牌	可讀社區名稱 （Read Community）	可讀／可寫社區名稱 （Read/Write Community）
Ascend	public	write
Bay	public	private
Cisco	public	private
3Com	public, monitor	manager, security

3.3.3 Unix 漏洞

Unix 系統漏洞的形成是因爲未詳盡考量預設遠端存取服務程式的安全設計，而皆以管理者 root（Supervisor）權限執行，入侵者在成功登入系統後，資源容易被竊取或破壞，一般在下面兩類較易遭到入侵者之窺覬。

1. UNIX 的許多版本皆有預設的遠端程序呼叫（Remote Procedure Call，RPC）服務，因而某些程式碼是在遠端的某些電腦上執行，這個設計當初是爲了讓 Sun 的網路資訊系統（Network Information System）與網路檔案系統（Network File System）搭配運作，而且以最高權限管理者 root（Supervisor）權限執行，攻擊者卻可以利用緩衝區溢位方式攻擊（如前述），取得 root 權限，而對目標系統爲所欲爲。

2. 在 DNS（Domain Name Service）區域轉移（Zone Transfers）時，如前述，BIND（Berkeley Internet Name Domain）服務程式因有緩衝區溢位的漏洞，攻擊者利用緩衝區溢位方式攻擊，取得 root 權限，在 DNS 執行任何不合法指令或程式，或取得該組織內部網路所有 IP 位址與主機名稱的對應資訊，進而對各主機 IP 位址進行入侵／攻擊。

3.4 網路入侵

一個有計劃的入侵作業，通常會從通訊埠的掃瞄開始，而展開一系列的系統探勘動作，包含擷取網路設施的資訊、辨識作業系統／應用程式、獲取存取權限、竊取機密資料、消除入侵蹤跡等等。本節將分別從入侵者常利用的掃瞄技術、入侵流程與入侵趨勢等一一敍述之。

3.4.1 掃瞄技術

當一個駭客或潛在的入侵者，想知道其所在的內部網路區段 S，是否存在可以入侵或攻擊的對象時，通常會先掃瞄 S 所有主機的連接埠，找出哪些系統是在運作中，且具有未修補（Patch）的弱點或漏洞，這就是所謂 Port Scanning。

一旦選定一台目標主機 T 之後，再

(1) 嘗試連接 T 上的各 TCP 與 UDP 連接埠，確定有那些正在執行的服務（Service）。

(2) 聆聽（Listen）連接埠狀態，以判斷 T 的作業系統種類及應用程式版本等資訊。

(3) 如果該系統並沒有做好安全設定，或其原本便存在安全漏洞，駭客可以經由此連接埠進入 T，以遂行破壞或盜取資訊。

至於要清查某一內部網路各主機的狀態，最簡單的方法就是利用 Ping 去試探。Ping 是對目標主機 T 發送 ICMP Echo（Type 8）的封包，如果 T 正在運作中，便會回送 ICMP Echo Reply（Type 0）封包。但是，由於 Ping 的效率限制，每次僅能掃瞄一台主機，若對 IPv4 Class A 網路（xxx.0.0.0），計有 16777214 個主機位址（2 的 24 次方減 2，即扣掉 xxx.0.0.0 網域位址與 xxx.255.255.255 廣播位址）進行全面性掃瞄，則得花上數小時或數天的時間，因此，比較適用在規模不大的網路。

較大型的網路通常以下列幾種型態的方式掃瞄[5, 31, 32]：

1. TCP 連接埠掃瞄

TCP 連線掃瞄係嘗試與目標主機 T 的連接埠 P 做一個完整的三階段確認（Three-Way

Handshake），即 SYN、SYN/ACK、ACK 等，若成功連線，表示 P 正在聆聽中；如果無法建立連線，就表示 P 並沒有開啓或不是在聆聽狀態。但是，這個連線掃瞄探測方法不論是否完成，皆會在 T 留下連線記錄（Log File），因此，很容易被管理人員或被入侵偵測系統（Intrusion Detection System，IDS）偵測出來。

2. UDP 掃瞄

UDP 掃瞄會對目標主機連接埠 P 送出 UDP 封包，如果從 P 收到回覆訊息“ICMP Port Unreachable”，表示 P 是關閉的；否則，表示 P 是開啓的。不過 UDP 協定是非連接導向的，許多因素都會影響其準確性，例如，網路資源與系統資源的使用負載過大，處理速度緩慢，都有可能對此掃瞄的準確性及可靠性造成影響。

3. 秘密掃瞄

秘密掃瞄就是對目標主機 T，施以非完整 TCP 連線掃瞄技術，且 T 不會留下任何連線記錄，可分成下列數種：

(1) TCP SYN 掃瞄：它對目標主機 T 的某連接埠 P 發送 SYN 封包，如果從 P 收到 SYN/ACK 的回應，就可以確定 P 正在聆聽狀態；如果收到的回應是 RST/ACK（RST 是重置（reset）連線旗標）或逾時 Time Out 訊息，就表示 P 不在聆聽狀態或 T 未開機。這技術又被稱爲“半開式掃瞄”（Half-Open Scanning），因爲它並沒有完成一個完整的 TCP 連線動作（缺少對 T 做 ACK 回應），如圖 3-8 所示。此掃瞄技術，一般 T 皆不會留下記錄，因此，又稱爲秘密掃瞄，僅有少數網管較爲嚴謹的 T，例如，設置入侵偵測系統的主機，會記錄之。

圖 3-8 避免留下痕跡的秘密掃瞄

(2) TCP FIN 掃瞄：會對目標主機 T 的某連接埠 P 送出 FIN 封包（FIN 爲一旗標，用以告知發送端完成資料傳送），如果 P 不在聆聽狀態，則 T 會回覆 RST 訊息

（約在 30～120 秒之間）；否則，T 會丟棄此封包，而不回應任何訊息。駭客可以由此知悉 T 是否存在入侵途徑 P 可以進行入侵行爲。

(3) TCP Xmas Tree 掃瞄：是對目標主機 T 的某連接埠 P 送出 FIN、URG 與 PSH 封包（URG 爲一旗標，用以啓動封包中的緊急指標（urgent pointer）欄位，目的是告知連線的另一端有緊急資料（urgent data）置於資料流裡，請其接收處理。PSH 旗標，則用以設定接收端必須儘快將此資料傳給應用程式，免於 TCP 緩衝（buffering）），如果 P 不在聆聽狀態，則 T 會回覆 RST 訊息；否則，T 會丟棄此封包，而不回應任何訊息。

(4) TCP Null 掃瞄：對目標主機 T 的某連接埠 P 發送將所有旗標都關閉的封包，如果 P 並不在聆聽狀態，則會回覆 RST 訊息；否則，T 會丟棄此封包，而不回應任何訊息。

(5) TCP RST 掃瞄：對目標主機 T 的某連接埠 P 傳送 RST 封包，如果 P 正在聆聽狀態，則不會有任何回應；若 P 是一個不存在的位址，則 P 所在網域上的路由器，收到這一組無法傳送或轉送的資料報，就會回覆錯誤訊息“ICMP Host Unreachable”（也大約在 30～120 秒之間）。

事實證明，利用各式掃瞄工具與技術偵測目標系統，確實可以找出所有正在運作中的系統，並可以清楚地知道潛在的攻擊目標與路徑。

3.4.2 入侵流程

一個入侵者爲執行一次實質的攻擊，通常會盡可能有系統地蒐集目標物的所有網路架構及各種主機／設備資訊，進而盜取系統資源或竊取機密資料，且不留下任何蛛絲馬跡。所謂『知己知彼，百戰百勝』，在談論安全防制前，我們必須先瞭解這些入侵者常利用的技術及手法，才可以制定有效的入侵防制方法。圖 3-9 爲網路入侵行爲模式、圖 3-10 爲駭客基本入侵流程[5]，以下分述之：

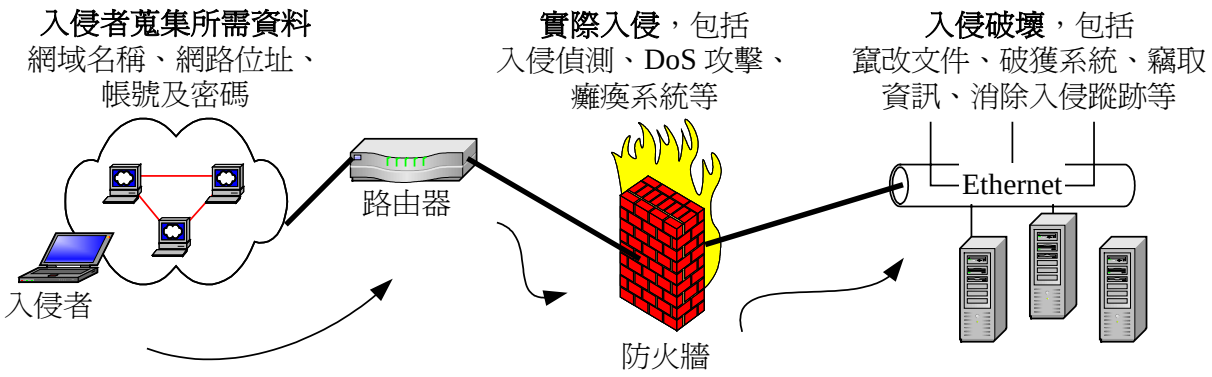

圖 3-9　網路入侵行爲模式

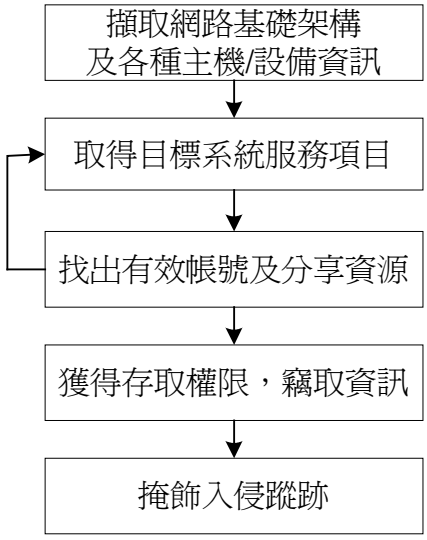

圖 3-10　網路入侵流程

1.　擷取網路基礎架構及各種主機／設備資訊

駭客在發動實質攻擊前，常會蒐集、匯整目標系統各種有用資訊，包含網域名稱（Domain Name）、網路區塊（Network blocks）、遠端存取機制（Remote access mechanism）及內部網路（Intranet）的主機位址與服務等相關資訊。而取得這些資訊或部份資訊的方法或時機如下：

(1) 如前述，利用區域移轉時，取得組織內部 DNS（Domain Name Server）所有主機（例如，名稱伺服器、電子郵件伺服器等）名稱與 IP 位址對映資訊。Nettlesting[19]提供的 axfr，便是一典型的竊取工具。

(2) 以上述的一些方法，取得潛在的存取路徑及網路拓樸（Network topology）。UNIX 及 Windows 提供的 traceroute、tracert 指令，便是典型的例子。

2. 取得目標系統服務項目

即掃瞄各 IP 的通訊埠，判斷哪些主機是在正常運作狀態，及所提供之服務，再擷取對方各服務程式之特徵，判別其所用的軟體系統之種類，過程是：

(1) 對目標系統發出 ICMP Echo 封包，清查暴露 IP 位址於網路上的各主機，並確定那些主機現在是在正常運作狀態。Rhino9[33]提供的 Pinger 即屬於這一類的工具。

(2) 再以前述的方法，掃瞄目標系統的 TCP 及 UDP 通訊埠，以瞭解其所提供的服務及現在運作之狀態，探索出所使用的作業系統及特定應用程式與版本等。Hobbit[34]提供的 netcat 工具爲其一例。

3. 找出有效帳號及分享資源

利用系統弱點或以破解密碼的方式，找出有效的使用者帳號或其所釋放出來的分享資源。以下兩項爲典型的案例：

(1) 在 Windows NT 作業系統上，以 NetBIOS 檢視網路上所顯露出來的分享項目，再利用 Somarsoft[35]所提供的免費資源列舉（enumeration）工具 DumpACL，透過空連線（Null Connection）以匿名連線方式登入，取得一個開放通道，找出該系統的登錄資訊（Registry keys）、分享資源、群組、使用者帳號等。

註：目前微軟在 Service Pack 3 的 Restrict Anonymous（限制匿名）改善了此一缺失，防止大部份資訊透過此空連線流出，但是，仍允許匿名連線，因此，駭客仍可利用列舉更詳細的工具 sid2user[36, 37]，列舉出使用者名稱與群組。

(2) 系統執行 SNMP 代理程式，入侵者可以透過預設的社區名稱（即密碼），例如，public、private、community、admin 等簽入後，存取系統資源。

4. 獲得存取權限，竊取資訊

以自動化工具竊聽使用者登入時之溝通內容，例如，L0pht Heavy[38]提供的

L0phtcrack 工具可以猜測 Windows NT 密碼，以獲取系統管理者的存取權限，進而接管系統，而以管理者的權限執行任何指令，竊取未經授權的資料，甚至建立後門，以便於爾後登入。

5. 掩飾入侵蹤跡

掩飾入侵蹤跡，清除事件記錄，避免被偵測出來。Jesper Lauritsen[39]提供的 elsave 爲一典型工具，它可以使用管理者的權限查詢此系統的安全稽核規則，若是在開啓狀態，則將之關閉，待於離開系統前再予以開啓，最後再清除日誌記錄，整個過程讓網管人員完全不知。

3.4.3 入侵趨勢

前面已敍述過若干入侵／攻擊手法及防禦方式，然而各網路的弱點及缺失不斷呈現，駭客手法亦不斷翻新，網路安全／管理人員必須熟悉其趨勢，方得以提出因應之道，下面將分別闡述各種入侵的威脅的趨勢[5, 15, 16, 40]。

1. 滲透防火牆系統能力的增加

對入侵攻擊的防禦措施，目前的網路系統大部份都是透過防火牆的機制，但是，一般的防火牆對於系統漏洞、缺陷、後門、內部攻擊與病毒等問題，仍無法有效地防制，僅能防範已知的安全威脅，而無法預測新的攻擊方式，例如，前面說明「不易檢測的隱藏通道」及「ICMP 與 UDP 封包的存取控制不當」皆是入侵者常利用的漏洞，較有經驗的入侵者，除了會利用這些缺失，還會運用各式的入侵偵測工具，使入侵破壞行爲更容易得逞。

而網路防火牆，是以防禦外來的威脅爲目標，對下述的入侵／攻擊項目，卻不易防範：

(1) 難以防範來自內部人員對內部網路的攻擊或竊取機密資料，原因是一般防火牆的存取規則設定是針對網路外部在向內部系統存取的控制，且內部所有系統主機皆暴露於內部網路上，若重要主機沒有另外增加安全機制，則無法防範來自內部的攻擊與竊取行爲。

(2) 面對透過系統的漏洞、缺陷或電子郵件的附加檔案所夾帶的後門病毒入侵亦束手無策，例如，透過電子郵件夾帶可對內部發動 DDoS 攻擊的木馬程式時，防火牆是無法阻絕這類對內部的攻擊模式，原因是防火牆僅過濾使用者的合法性，因此，對於防火牆原本系統的漏洞與缺陷，及合法使用者經由電子郵件所夾帶的的檔案，並沒有過濾阻擋，讓病毒入侵。

(3) 內部人員亦可透過私接數據機撥接連線，這種人爲所造成的後門，會吸引有心人士的窺視及竊取撥接連線的資訊（撥接門號、使用者名稱與密碼等），卻無法有效加以防範，原因是這私自架設的撥接連線並沒有經過防火牆安全機制的過濾，使得外部入侵者可以直接入侵／攻擊內部網路系統，造成難以估計的損失。

2. 對網路設施的威脅增加

在複雜的網路社會中，駭客的攻擊行爲、動機與目的，與現實的社會是一樣的，他／她不一定是要去獲取某系統的存取權限或竊取機密資料，他／她可能只是去癱瘓一個網路系統或一部主機的運作，祇要能造成某組織或某網路無法運作，即達到其目的。

由於網路的資源是有限的，駭客可以利用消耗網路頻寬資源與系統資源耗竭（例如，CPU、Memory、Process 等）兩種方式攻擊：

(1) 攻擊者可以從遠端透過多台代理主機，向目標主機 T 送出大量的服務請求封包，使 T 窮於應付，造成網路連線飽和／癱瘓，而無法服務真正的需求者，一如前面所提 DoS、DDoS 攻擊。

(2) 利用作業系統或應用程式的瑕疵（Bug）或無法處理例外狀況，造成系統當機（Crash），而無法提供正常服務，例如，前面所提的「緩衝區溢位（Buffer Overflow）」攻擊即爲一例。

3. 網路入侵工具的自動化

由於入侵工具不斷的修正與改良，從掃瞄／偵測目標主機的通訊埠、作業系統、應用程式，至漏洞的探勘與攻擊行爲的發動，已可以完全自動化一氣呵成，而且可跨作業平台，不但可以隨機地選擇攻擊步驟，或利用事先設計的不同攻擊方法發動攻擊，使得攻擊行爲分析與偵測，越來越不容易。例如，僞造 IP 位址或透過代理主機發動 DDoS

攻擊，即跳板攻擊，使網路蒐證不易，無法追蹤實際的攻擊源頭。

這些攻擊技術與方法已愈來愈成熟且多樣化，使得網路安全管理的挑戰，愈來愈嚴苛。事實上，爲了保障網路上各伺服主機、網路設備與所傳遞訊息的安全，網路安全管理機制與策略，不能不隨著網路結構與應用的改變而調整，如此，方能效防範不當的使用。此外，管理人員亦應不斷的繼續充實安全知識，若是得過且過有問題再處理的心態，或對駭客行爲／工具不清楚，都是網路危機之一。

第4章 網路存取監控

由於網路隨時會遭到不當的存取或惡意的攻擊，爲便於網路監控與封包分析，網管人員必須事先熟悉

1. 網路運作的各項標準。
2. 合法網路存取行爲。
3. 特定服務及功能的網路流量及行爲。
4. 各種封包標頭及封包內容的特徵。

俾在建構及管理網路時，能夠確保資料的安全性，及防制惡意或無意的入侵破壞。下面將分別在防制策略、監控項目與地點、網路防火牆、入侵偵測及存取控制等層面上，一一說明如何適當地利用資訊安全防制、網路封包特徵、身份鑑識技術與行政控管等方式，建構安全的資料存取與傳輸機制，防止未經授權的使用、誤用或濫用等。

4.1 防制策略

爲防範可能的網路安全威脅，我們必須有適當的網路安全防制策略與機制爲組織做最全面的保護，依安全政策的規範與程序推行到整個組織。下面將對防制策略的思考形成邏輯與安全政策的安全機制分別陳述之。

4.1.1 策略邏輯

本論文之網路安全防制策略定義爲：組織爲達到網路安全目標，經由威脅分析與風險評估之區隔與定位，訂定之防制策略，包含技術與管理兩層面，如圖 4-1 爲其示意圖。我們建議防制策略思考應該

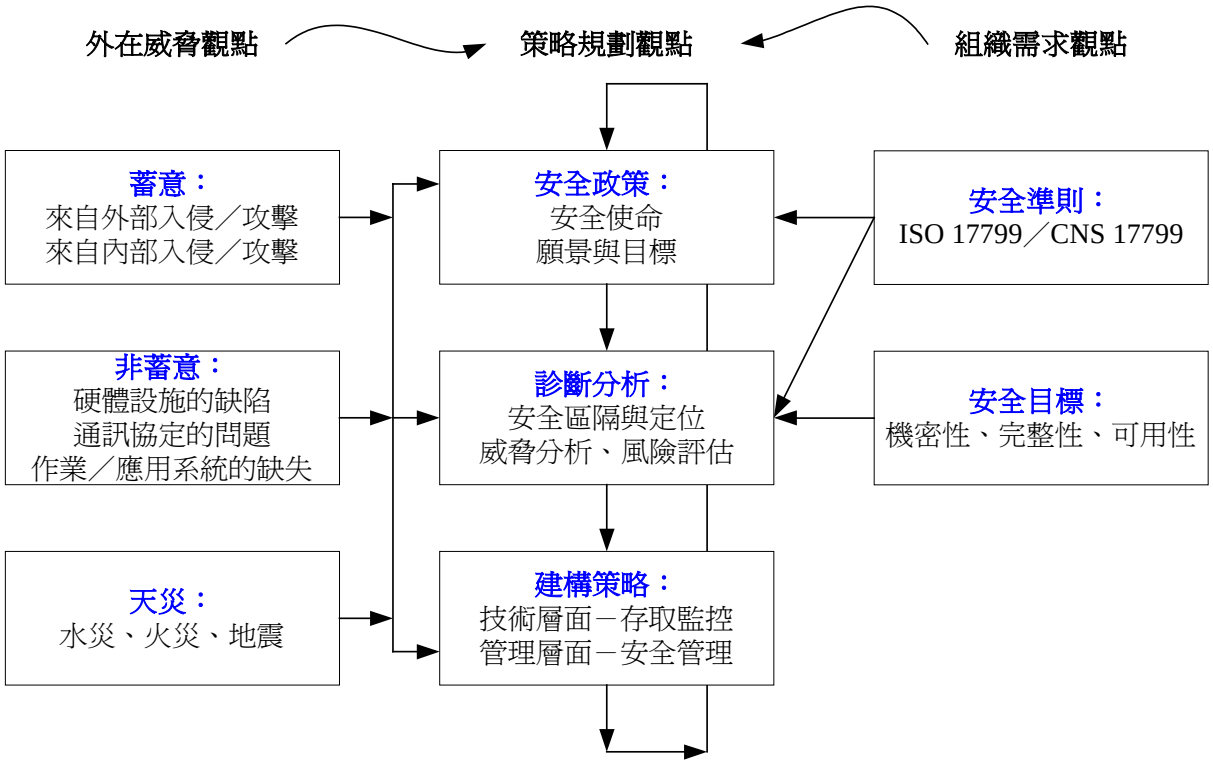

圖 4-1　防制策略分析之架構

1.　組織需求觀點

從組織對網路安全的需求思索，包含有

(1) 安全準則

依據 ISO 17799 資訊安全管理系統實務準則所提供管理要項、控制目標及方法，建構一套符合組織資訊安全的政策，確保資訊安全，亦可做爲 IT 人員的遵循標準。

(2) 安全目標

必須達到組織對資訊安全要求的三大目標，即機密性、完整性、可用性，以確保組織資訊之機密、完整及可用。

2.　外在威脅觀點

在面對目前與未來可能的外在安全威脅，應該思考資訊資源遭受入侵／破壞的可能性，及發生時會遭受到什麼樣的衝擊，如

(1) 蓄意入侵／破壞行爲

面對來自網路外部與內部的人爲蓄意之入侵／攻擊行爲，例如，DoS、DDoS 攻擊等，必須建立一套資訊安全防範政策落實執行，避免組織資訊資源的損失。

(2) 非蓄意破壞行爲

面對非蓄意的網路安全問題，例如，硬體設施的缺陷、通訊協定的問題、作業／應用系統的缺失等，必須建立系統維護與弱點通報程序，以適時修正，減少系統安全威脅衝擊。

(3) 天災所引發的損失

面對不可預測的天災，例如，火災、火災、地震等，我們必須建立一套備份機制與危機處理程序，以降低災害損失。

3. 策略規劃觀點

依據組織的資訊資源、技術資源、財務資源等能力，建立最佳的安全防制策略。我們必須評估

(1) 安全政策

組織對於網路安全的願景與目標，必須明確訂定規範，包含指導方針、運作程序、管理規範及人員聘雇合約等，以提供安全管理遵循參考。

(2) 診斷分析

對組織資訊資源做一安全威脅分析，評估所面對的資訊安全漏洞、威脅與影響，以做有效監控與防制。並做風險評估與管理，列舉各資產價值、威脅與弱點，以建立監督與控制之機制。

(3) 建構策略

在技術層面與管理層面，分別建立存取監控策略與安全管理策略，以防範資訊資源遭受各種安全威脅，確保組織持續運作、減少損失。

4.1.2 防制機制

經由前述充份瞭解網路所面對安全威脅後，對於這些威脅的可能來源，擬定一套適當的防制機制，如圖 4-2 所示，做爲施行到整個組織的程序與規範，以下分述之。

<table>
<tr><td colspan="9">資訊安全標準 ISO/IEC 17799
安全稽核與管理</td><td>Strategy</td><td>決策層</td></tr>
<tr><td colspan="4">技術角度</td><td colspan="5">管理角度</td><td rowspan="2">Managerment</td><td rowspan="2">管理層</td></tr>
<tr><td>身份鑑識</td><td>RBAC</td><td>傳輸控制</td><td>多層防禦</td><td>風險評估</td><td>人員管理</td><td>系統維護</td><td>實體安全</td><td>危機管理</td></tr>
<tr><td colspan="9">Authentication / PKI
Application Layer Firewall / Host-Based IDS</td><td>7 Application</td><td rowspan="6">技術層</td></tr>
<tr><td colspan="9" rowspan="2"></td><td>6 Presentation</td></tr>
<tr><td>5 Session</td></tr>
<tr><td colspan="9">SSL / SET
Packet Filtering Firewall / Network-Based IDS</td><td>4 Transport</td></tr>
<tr><td colspan="9">VPN / Anti-Virus
Packet Filtering Firewall / Network-Based IDS</td><td>3 Network</td></tr>
<tr><td colspan="9">Lock IP_MAC Address</td><td>2 Data Link</td></tr>
<tr><td colspan="9"></td><td>1 Physical</td></tr>
</table>

圖 4-2　網路安全防制機制

1. 決策層

資訊安全的管理，是需要組織高階管理階層的支持與認知，經由各層級人員的充份溝通與參與，建立符合組織資訊安全的政策。我們可以參照 ISO 17799 的資訊安全標準制定符合組織之安全政策與程序，建構資訊安全防護機制，減少組織網路與系統安全的弱點與缺失，並提昇組織的風險控管能力。

2. 管理層

資訊安全的管理，可分別從技術與管理兩方面著手，以達成組織資訊安全目標與政策，分述如下：

(1) 技術角度

資訊安全在技術層面，爲確保網路存取的安全性，可以經由網路的安全威脅分析，瞭解資訊系統與網路所存在的弱點及潛在威脅，對系統與網路施以技術層面的存取監控，例如，嚴謹的身份鑑識、採用 RBAC 的存取控制機制、網路傳輸的控制、多層防火牆的防禦、非軍事區系統的設置等，以阻絕不合法的網路傳輸與存取，避免機密資料的竊取與破壞，保障組織資訊資源的安全。

(2) 管理角度

資訊安全在管理層面，要適當的保護組織資訊資產的安全，可以經由風險評估及管理，瞭解資訊資產的類型及其個別價值，評估資訊安全漏洞對資訊設備的威脅與影響，以可接受的成本，實施保護與控制措施，例如，人員安全管理控制、系統維護控制、建立實體環境的安全防護、資料輸出與輸入控制、應變及緊急處理計畫之規劃等，防制可能影響資訊安全的風險，將危害減至最小。

3. 技術層

在網路的存取控制上，我們可以利用網路協定中各階層封包的特性，設定網路存取規則，有效監控網路封包傳輸行爲，分述如下：

(1) 在 OSI 應用層

我們可以利用應用層防火牆與主機型入侵偵測系統，在應用層透過應用代理程式處理客戶端的連線要求，與檢查對主機作業系統或應用程式的攻擊行爲，例如，FTP 服務程式，有自己對應的 FTP Proxy 代理程式處理連線要求，與執行檔的稽核值試算等，避免入侵者的直接連線攻擊，與應用程式的緩衝區溢位攻擊等。

並利用 RBAC 的存取控制機制，管理每位使用者對組織資源的使用權限，例如，對於不同職責的使用者給予不同的存取權限，讓每位合法的使用者，僅能存取所賦予的資訊資源，避免逾越權限的存取。

(2) 在 OSI 網路層與傳輸層

我們可以利用封包過濾式防火牆與網路型入侵偵測系統，在網路層監控 IP 標頭內容，例如，來源與目的 IP 位址、TCP/UDP 來源埠與目的埠等，阻止不符合網路存取規則的網路封包；在傳輸層監控 TCP 連線狀態，例如，失敗連線與阻斷連線，避免非法的入侵掃瞄探測行爲。

(3) 在 OSI 資料鏈結層

在乙太網路環境下，我們可以利用網路介面卡的乙太網路位址（MAC）唯一識別的特性，在資料鏈結層監控封包所傳送 MAC 內容，再與該主機所對應之合法 IP 位址做爲網路存取控制之識別，此 IP_MAC 可以加強網路身份的鑑識， 並可以防止不合法位址的存取。

4.2 監控項目與地點

爲了保護網路與系統的安全，管理人員必須實施網路監控，並蒐集與分析網路封包。至於該在何處實施監控？異常的連線活動又該如何辨識？方得以蒐集完整證據與資訊，以確認或制止可疑的入侵／攻擊行爲[6, 31, 41]？以下分述之。

4.2.1 異常連線

異常連線是指伺服主機、網路線路或網路設備發生 TCP 不正常的連線，如前述，它是駭客用以掃瞄網路主機狀態的方式之一，唯此時網路其他部份的運作仍是正常的。

導入 ISO 17799 9.5.7 與 9.5.8 控制方法，監控 TCP 的連線狀況，分析兩主機之間連線異常／失敗的原因，可以辨識是否有潛在的入侵或非法的網路通訊，方法則是檢查重要主機（例如，檔案伺服器、網頁伺服器）或路由器所發出的 ICMP 控制訊息，例如，ICMP Echo Request、ICMP Echo Reply、ICMP Destination Unreachable。下面將分別闡述經常發生的異常連線：

1. 連線失敗：對於在短時間內，多次嘗試對目標主機進行連線，但是並沒有具體的實際連線。必須從 IP、TCP、UDP 等封包的標頭資訊分析封包來源，辨識是否爲授權

的連線，否則應該拒絕此來源封包，避免可能的連線掃瞄偵測行爲。

2. 阻斷的連線（Blocked Connection）：在攻擊主機 A 與目標主機 T 之間尚未建立正式連線前，攻擊者可以對 T 進行“半開式掃瞄”，藉此判斷 T 的作業系統與開放的連接埠，這種不完整的連線，例如，TCP SYN、TCP Xmas Tree、TCP RST 等，很可能是入侵攻擊的前置動作，通常要升高系統危險等級。

4.2.2 監控節點

由於網路的資源有限，若全面地實施監控與檢測，將對網路績效造成重大影響。因此，最佳的做法便是在網路傳輸特別敏感的區段或節點（例如，網路交通閘道、曾經被入侵之主機），做全面性的監測，其他重要性比較其次的區段，例如，一般工作站主機，則祇做局部性的抽樣。以下將介紹網路上經常遭到入侵攻擊的節點／區段，包括：重要主機、外部與內部網路的交接邊界、曾經遭受入侵的系統或子網域等，這些節點／區段自然也是監控的重點所在（如圖 4-3）。

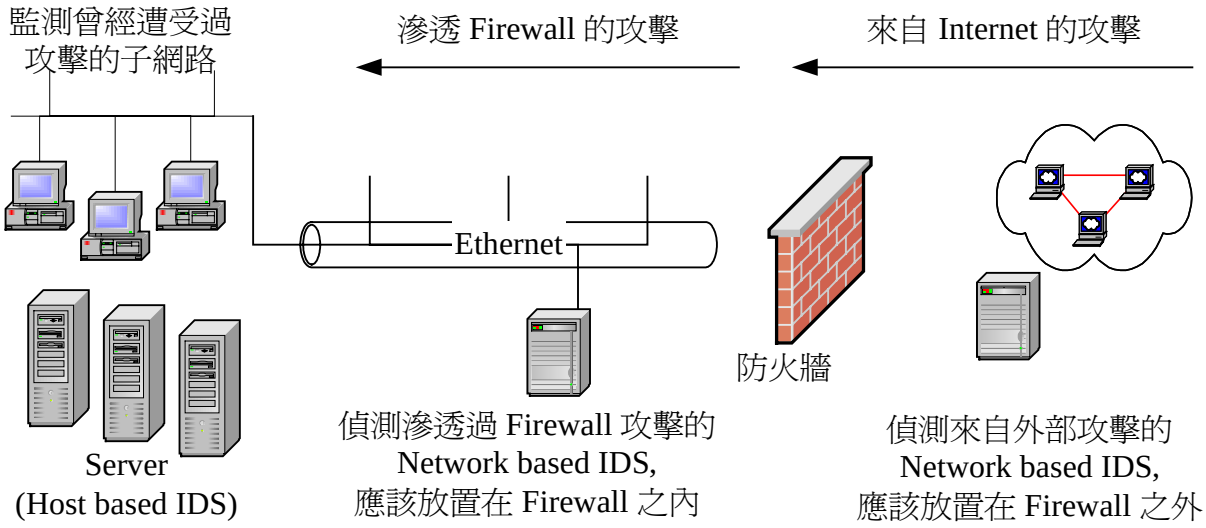

圖 4-3 選擇監控的節點／區段

1. 重要主機，是提供組織重要服務與資訊的機制，爲防止未經授權的使用、資訊竊取及破壞，應該予以監測。

2. 外部與內部網路的交接邊界，這個區域可以監控所有來自網路外部或內部對外的異常網路行爲，而給予網管人員即時的告警或直接制止，故應加以偵測。

3. 對於曾經遭受過攻擊或入侵的系統或子網域，爲防止攻擊者在其中某些主機上建立後門或木馬，而以這些主機爲跳板，對該網路發動攻擊或啓動對外的連線，因此，其網路流量不論是輸入或輸出，皆應做全面性的檢測。

4.3 網路防火牆

網路防火牆（Firewall）是一個用以區隔組織內部網路（Intranet）與網際網路（Internet）間存取資料的雙向安全控管機制。除了防止外界對內部資訊的不當存取，當然也限制了內部主機對外部的不當通訊。方法是藉由網路存取規則（ACL），管制所有進出內部網路的連線，及檢查所有通過防火牆的網路封包，並且留下詳細紀錄（Log），以爲日後稽核與追查的依據。下面將分別介紹網路防火牆技術、限制與建置方法[6, 31, 42, 43]。

4.3.1 種類

防火牆對封包的處理方法計可分成兩大類：封包過濾式防火牆（Packet Filtering Firewall）與應用層防火牆（Application Layer Firewall）。

1. 封包過濾式防火牆

過濾封包是最早被運用於防火牆的技術，屬於 OSI 七層架構中的第三層（網路層）運作，安裝在網路閘道（Gateway）出入口處，監控每個來往的 IP 封包標頭（IP Header），檢視其內容是否符合事前設定的網路存取規則。優點是速度快、建置容易且成本較低。然而，依據過濾規則這種防火牆又可細分爲靜態封包過濾式（Static Packet Filtering）與動態封包過濾式（Dynamic Packet Filtering）兩種，下面分別敍述之：

(1) 靜態封包過濾式

靜態式的是根據事先定義的過濾規則，對封包的來源 IP 位址、TCP/UDP 來源埠、目的 IP 位址及 TCP/UDP 目的埠進行篩選，如果這些資料內容符合事先設定的規則，就讓該封包通過，反之則予以拒絕或丟棄，圖 4-4 爲其示意圖。

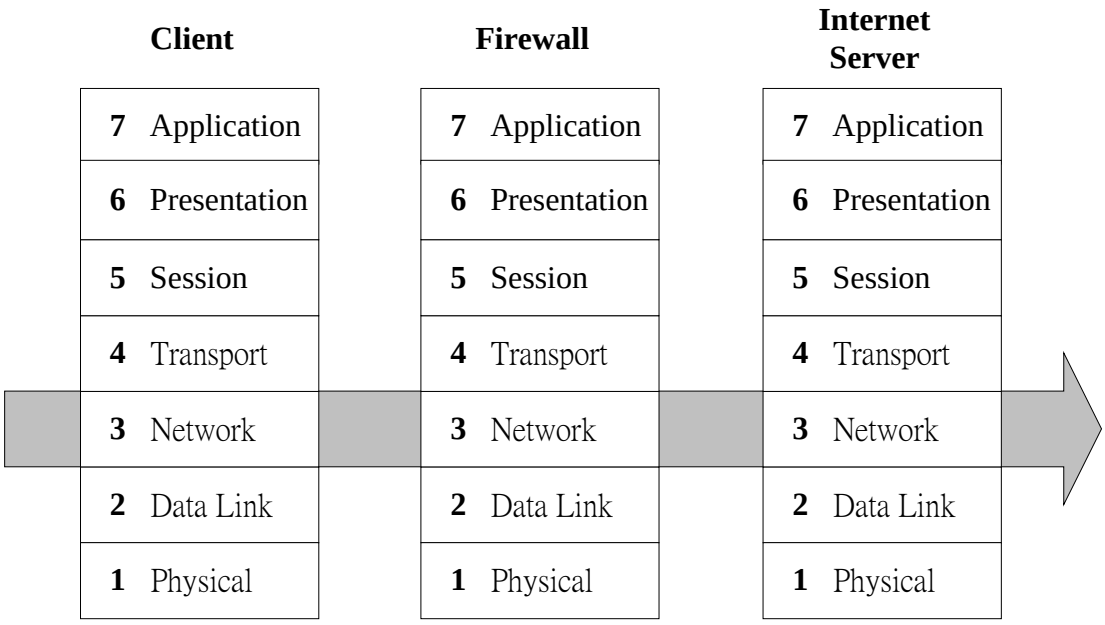

圖 4-4　靜態封包過濾式防火牆

(2) 動態封包過濾式

動態式者除了使用靜態封包過濾的方法來監控網路傳輸以外，對封包內容與連線行爲，也會做動態的檢查，例如，對通過防火牆的每個連線（包含有來源 IP 位址、TCP/UDP 來源埠、目的 IP 位址、TCP/UDP 目的埠、時間及所要求服務等）都進行追蹤，並在記憶體中建立每一個資料流各封包的前後關聯，然後根據此關聯檢查每一個新收到的封包，判斷是新連線或是現有連線的延續，並且可以依需要動態地增加或更新過濾規則，亦稱爲狀態檢視（Stateful Inspection）防火牆，圖 4-5 爲其示意圖。其中 Stateful Packet Inspector 即爲對網路封包內容與連線檢查之功能模組。

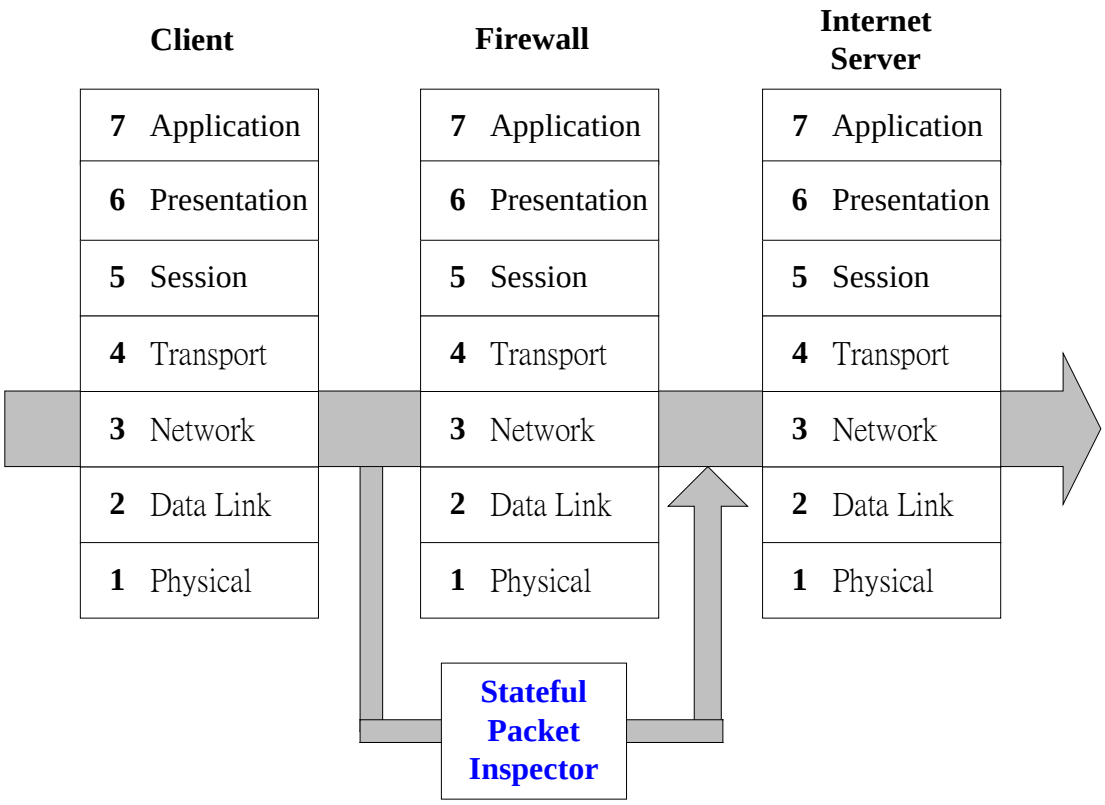

圖 4-5　動態封包過濾式防火牆之狀態檢示

封包過濾式防火牆的優點有：

(1) 建置容易，成本較低。

(2) 僅單純封包過濾，處理速度較快。

缺點是：

(1) 無法過濾加密過的資料。

(2) 封包過濾規則定義複雜，容易出現配置不當不一致的問題，例如，封包過濾規則一允許所有外部使用者，可以任意存取所有內部伺服主機所提供的所有服務，而規則二不允許外部使用者存取內部 FTP 伺服主機所提供的服務，而系統對存取規則的判讀是依照規則順序，因此，祇要符合規則一的使用者，皆可以存取內部 FTP 的資料，造成資訊外洩。

2. 應用層防火牆

應用層防火牆是在 OSI 七層架構中第七層（應用層）運作（圖 4-6 爲其示意圖），它利用代理程式（Proxy）所設定的安全存取規則，儲存並轉發（Store and Forward）客戶端（Client）對伺服端（Server）提出的連線要求；組織內部欲對外界提出連線要求時，其運作原理亦同，只是方向是由內向外。此方式客戶端與伺服端雙方無法直接連線，必須透過此特別設計的安全代理程式代爲處理，避免入侵者直接連線攻擊，其優點除了提供代理服務外，在應用層也提供較好的用戶認證（除一般授權檢查外，也可以限制使用者登入／拜訪主機、登入時間等）、日誌訊息（Audit log）及過濾規則，依開發技術可以再分爲代理型（Proxy）與調適代理型（Adaptive Proxy）兩種，下面分述之：

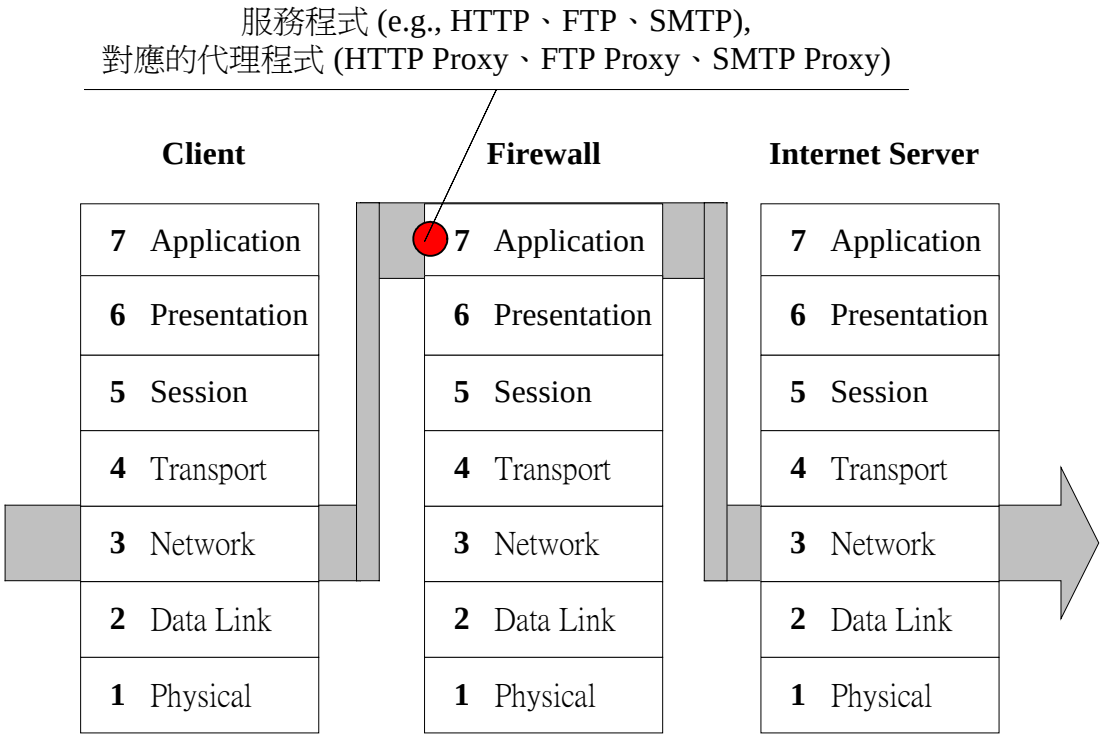

圖 4-6　代理型防火牆

(1) 代理型

防火牆的安全政策／規則是在代理程式上設計，每一種被允許的服務程式都有其特定代理程式，例如，HTTP、FTP、SMTP 等服務程式，各有對應之 HTTP Proxy、FTP Proxy、SMTP Proxy 代理程式來處理，其在外部網路向內部網路申請服務時發揮了中間轉接的作用，當客戶端將連線要求傳送到防火牆時，防火牆會分析其封包的內容及協定，如果政策／規則允許，則防火牆就會代表客戶

端與伺服端建立一條新的連線，圖 4-6 爲其示意圖。

(2) 調適代理型

它結合代理伺服器與動態封包過濾的功能，在防火牆中設定所需要的服務類型所對應的代理程式即可，防火牆中的代理程式就會接受客戶端之連線要求與要求服務之封包，並檢查封包標頭或資料，再爲該代理程式與伺服器建立新連線，而未設定代理程式之封包，則在網路層直接過濾與轉發，換言之，它結合了代理型防火牆的安全性和封包過濾式防火牆的高速度等優點，圖 4-7 爲其示意圖。

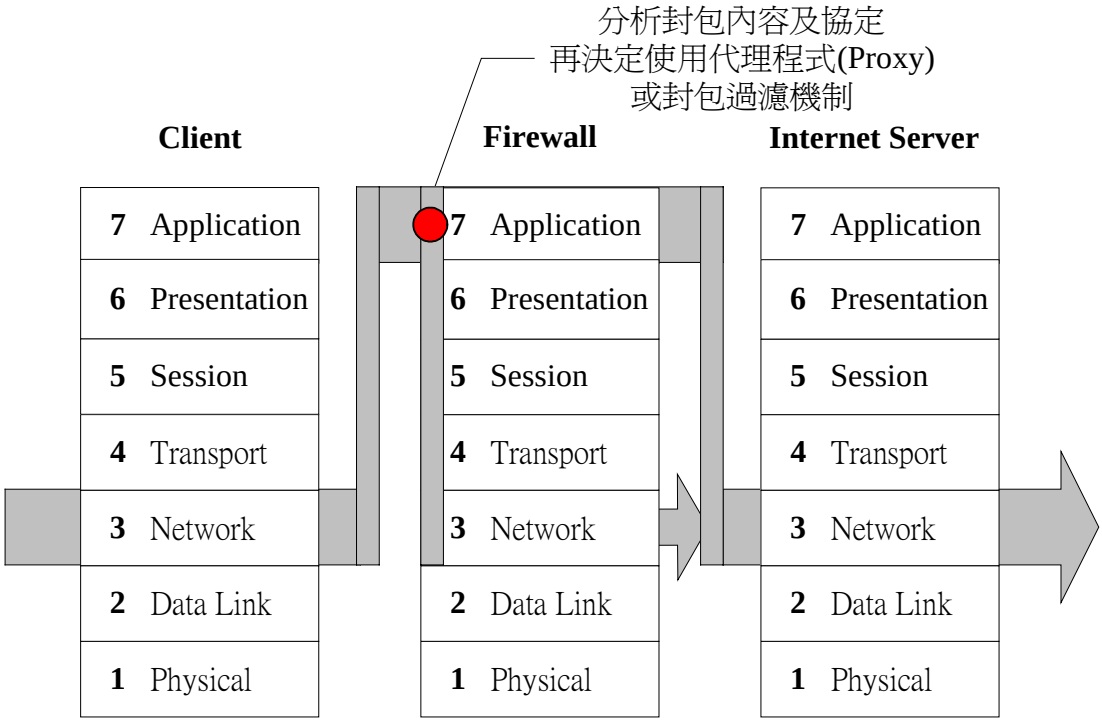

圖 4-7　調適代理型防火牆

應用層防火牆的優點有：

如前述，在 OSI 第七層應用層代理程式的儲存並轉發客戶端對伺服端提出的連線要求，能防止直接的連線攻擊。

缺點是：

和封包過濾式防火牆相比較，則因是在應用層處理之故，速度比較慢，不適用於高速網路，例如，非同步傳輸（Asynchronous Transfer Mode，ATM）高速網路等。

4.3.2 限制

防火牆的安全設計，並無法完全防範所有的攻擊，例如，在後門問題、內部攻擊及病毒威脅上仍有不足之處，下面將分別說明。

1. 後門問題

後門程式有兩種，一種是由系統入侵者在已被破解的系統 T 上所建立的，方便入侵者藉此路徑下載T的機密資料或監控T的活動等,此種後門程式可藉由病毒程式傳遞(例如，含病毒的電子郵件）或入侵系統後植入。另一種是由系統管理者，爲了方便遠端管理而建立的，若未善加管理，例如，使用預設帳號與密碼，則很容易成爲入侵者進入組織內部網路的另一個管道。

2. 內部攻擊

大部份的網路安全規則，都是用以防止來自外界的網路攻擊，但是，根據 CSI/FBI 統計[44]企業組織的網路攻擊行爲約 71%來自內部，內部攻擊往往會對網路造成難以彌補的傷害。依 CSI/FBI 所公佈之數字顯示，每年內部網路未經授權的存取，造成 U.S. $4503000 損失，從 Intranet 內部中竊取機密資料爲一典型例子，其重要原因之一是網路防火牆常不能對於內部攻擊提供有效的保護功能。

要解決內部攻擊的問題，僅有另外建立入侵偵測機制予以防範，或是將存放敏感重要資料的伺服器，加一道防火牆區隔，借以防範來自內部攻擊及減少因內部不當行爲所造成的損害。

3. 未經防火牆的連線

防火牆無法防制未經防火牆的連線攻擊，例如，網管人員爲能從網路外部透過撥接連線至 Intranet 內部主機維護系統，而在 Intranet 內部設置數據機，這種沒有經過防火牆的管制與防護的撥接連線，容易被入侵者／駭客偵測獲取，而直接入侵攻擊重要伺服主機，造成不可預知的損失。

4. 病毒威脅

一般的防火牆所採取的安全政策是拒絕它不信任的服務及來源 IP 位址，但是一個合法的使用者從 Internet 下載的檔案或是電子郵件的附加檔案所夾帶的病毒，則不做掃瞄與過濾，這些惡意的病毒，例如，Melissa、CIH 等，一旦進入系統會造成資料被竊取／損毀、主機網路癱瘓等後果。

4.3.3 防火牆建置

在瞭解整體網路架構的潛在威脅與缺失後，我們該如何設置防火牆？以下分述之。

1. 咽喉點

若能在內部網路 I 與網際網路之間維持一個唯一的通道 C，又稱爲咽喉點（Choke Point），所有進出 I 的封包，都必須經由 C，則管理人員比較容易對 I 進行監視與控制，其代價則是 C 可能會是整個系統的瓶頸，否則便須在 C 設置比較大型、比較高速的網路設備，價格自然也比較昂貴，當然 C 的當機，整個對外的交通也將陷於癱瘓。在近代的網路安全設計上，大多數的防火牆 F 都是被設置在 C 處從事網路系統的監控，管理人員事先在 F 上製定安全政策，祇讓事先定義的服務通過，俾使系統運作符合安全政策的要求。當然，不經過咽喉點的傳輸，便無法進行安全的監控。

2. 非軍事區

非軍事區（De-Militarized Zone，DMZ）是一個受到「部份保護」而不能完全信任的網路區域，它的網路存取通常是受防火牆或路由器控制，一般而言，管理者會把所有對外服務的主機（例如，Email、Web、FTP 等）置放於非軍事區內，以便將 Internet 與 Intranet 的服務區隔開來，原因如下：

(1) 非軍事區的意義

尚若不設置非軍事區，而直接將對外服務主機置放於防火牆後方時，當對外服務主機 S 被入侵破壞，則 S 的控管權可能會落入駭客手中，駭客便可以使用各種技巧或工具擷取後端資料庫的資料，或藉由 S 攻擊網路上其他主機（包括網內主機及其他網域主機），即將 S 當作攻擊跳板。

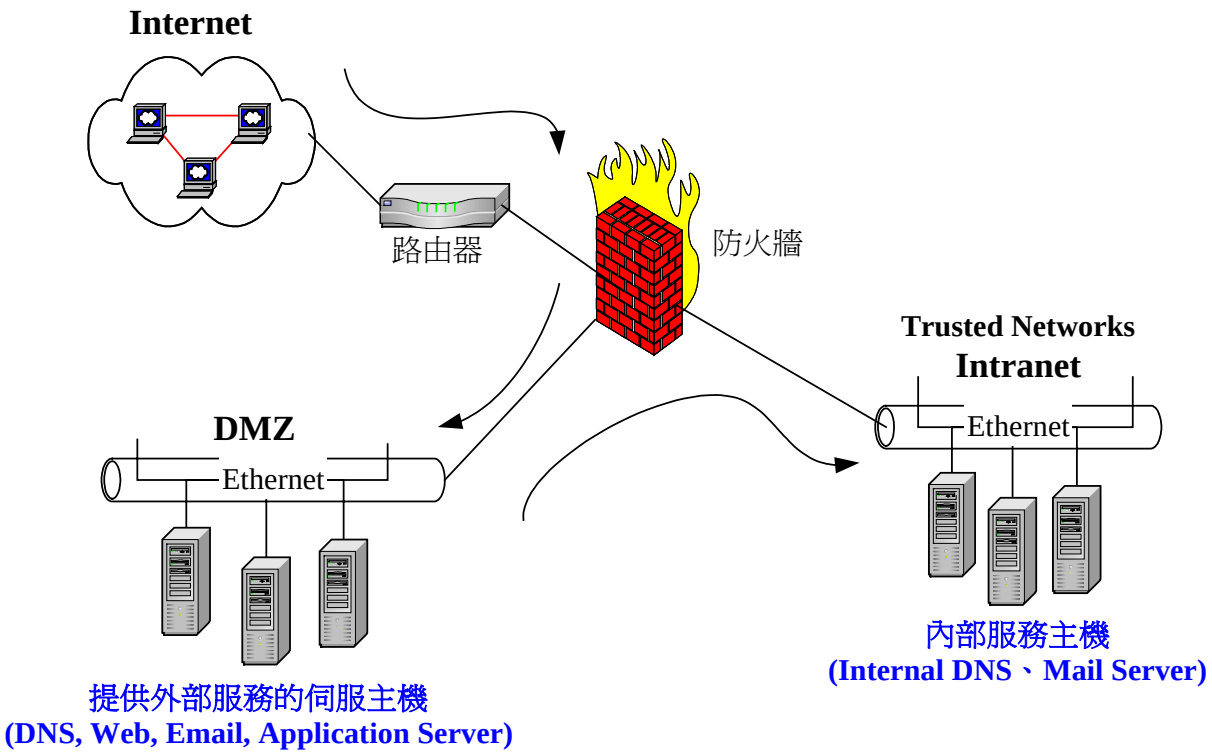

圖 4-8　非軍事區與防火牆

設立非軍事區後，見圖 4-8[31]，並能搭配，防火牆還有網路位址轉換（Network Address Translation，NAT）機制，會隱藏內部網路 IP 位址，此時，若防火牆被駭客滲透，入侵伺服主機，其僅能在該 DMZ 區域內滲透破壞，所損失的祇有這些對外服務主機上的資料，駭客不易入侵到防火牆後方的 Intranet 網路，使組織內部的重要資料及資源得以受到相當程度的保護。

(2) 非軍事區之系統

所有提供 Internet 存取服務的伺服主機，例如，Mail Server、Web Server、FTP Server 等，都應該放置在非軍事區，但是，如果其中有一部伺服主機允許交談式連線，例如，Telnet，當對外服務主機 T 被入侵，則入侵者就可以藉由 T 攻擊非軍事區中的其它主機。因此，站在系統安全的角度上來看，並不建議提供交談式連線的服務。

4.4 入侵偵測

防火牆是網路邊界安全的第一道防線，由於是曝露在外，很容易遭受攻擊，部份的入侵者甚至可以透過防火牆的不當設定，避開防火牆封包過濾機制的防護，發動 DoS 攻擊。由於係其功能上的限制，無法檢查通過的封包內容。如果要檢查這些封包內容，必須建置入侵偵測系統（Intrusion Detection System，IDS），而在不影響網路效能的情況下，於網路系統重要節點蒐集各種封包，並分析之，做法則是透過封包的監視、安全審計與攻擊辨識等，判斷是否有違反安全策略或攻擊行爲，即時地向管理人員反應與警示，以提昇系統安全。下面將分別介紹入侵偵測系統的類型、偵測模式及建置位置[45]。

4.4.1 類型

入侵偵測系統依部署環境的不同，可以區分爲網路型入侵偵測系統（Network-based Intrusion Detection System，N-IDS）、主機型入侵偵測系統（Host-based Intrusion Detection System，H-IDS）、混合型入侵偵測系統（Hybrid Intrusion Detection System）與誘捕系統（Deception system）四類：

1. N-IDS

N-IDS 一般會配置兩張網路卡（Network Interface Card，NIC），一張以不配置 IP 的方式監控網路封包，因此，不會回應任何探測訊息，而隱形於網路上；另一張卡則配置 IP 位址，用來直接與內部網路的 N-IDS 管理系統進行溝通及傳遞入侵警示訊息。

N-IDS 以軟體程序（Process）形式存在於特定的硬體系統上，例如，某一台電腦或專屬之硬體系統，並將第一張網路卡設定爲雜亂模式（Promiscuous Mode），該網路卡會蒐集流經網路層（Network Layer）的所有封包的傳輸資料與連線狀態，例如，IP 標頭中的來源位址、目的位址、服務類型等。N-IDS 再以事先定義的規則或攻擊行爲特徵比對分析，例如，網路封包的 IP 來源位址是否屬於拒絕往來之黑名單或網路流量與網路流向是否異常等，判斷可能的入侵威脅。一般而言，N-IDS 可以偵測到的攻擊行爲，包括 TCP SYN flood 不正常連線的 DoS 攻擊、Port mapping 蒐集網路上的資訊等，若發現攻擊行爲，N-IDS 會發出訊息給管理者，切斷可疑的連線，並記錄於日誌記錄檔案中，以

供後續的攻擊分析與研究。

佈署 N-IDS 的優點有：

(1) 設置成本較低。祇需設置一部 N-IDS 即可偵測同一區域網路中的所有可能入侵行爲，且不需更改現有的網路架構與作業系統。

(2) 隱形在網路上偵測。入侵者無法得知偵測系統的存在，其入侵／攻擊行爲記錄無法掩滅。

(3) 可以同時偵測多個重要主機傳輸資訊。一部 N-IDS 可以偵測同一網路內的所有主機的網路傳輸資訊。

(4) 可偵測來自網路封包的攻擊模式。N-IDS 是偵測 OSI 第三層網路層所有的封包傳輸情形，因此可以偵測網路封包型態的攻擊模式，例如，DoS、DDoS 等。

缺點包括：

(1) 僅偵測事先定義之規則與封包特徵，無法偵測新型的攻擊行爲。

(2) 網路流量過大或超出所能處理範圍時，N-IDS 則無法完全偵測所有網路封包的傳輸狀況。

(3) 無法偵測經過加密的傳輸資訊內容。

(4) 無法判斷入侵／攻擊行爲是否成功。

2. H-IDS

架構於伺服器主機 S 上，也是以軟體程序的形式存在，而與 S 的作業系統及應用程式密切結合，主要是偵測來對 S 之 OSI 應用層（Application Layer）的入侵行爲，例如，對 S 的作業系統或應用程式進行緩衝區溢位（Buffer overflow）攻擊、檔案存取與系統操作等，並使用稽核記錄與事先定義的規則做比對分析，判斷可疑的攻擊行爲或模式，例如，依 Time trap 或 Event trap 比對稽核記錄與系統設定檔比對是否一致、試算執行檔的稽核值（Checksum hash、MD5 或 Digital signature）是否正確。當發現攻擊行爲時，可以結束使用者連線或停止其使用權限等，並通知管理人員做適當的處置，例如，鎖定此攻擊來源或停止服務等。由於 H-IDS 所有的稽核與監控行爲都在此 S 主機上進行，故

得其名。

佈署 H-IDS 的優點有：

(1) H-IDS 可以依據日誌記錄，判斷入侵／攻擊行爲是否成功。

(2) H-IDS 主要是偵測 OSI 第七層應用層，適用於有加密或交換式（Switch）網路環境。交換式網路的技術是對該網域內的所有主機，建立一個媒體存取控制（Media Access Control，MAC）表，亦即網路卡位址對應表，交換器上的高速晶片會依封包所指定之 MAC 位址轉送，而不會傳送到其他主機。

缺點包括：

(1) H-IDS 會暴露在網路上，行蹤可能會被發現，而被攻擊損毀。

(2) 僅偵測事先定義之規則與特徵行爲，對新型的攻擊型態無法偵測。

(3) 可能無法完全相容於所有不同主機的作業平台，使得佈署與維護工作比較複雜，且無法防護作業系統本身的安全漏洞，若駭客入侵／攻擊這些作業系統安全漏洞，將導致 H-IDS 失去效用。

(4) 無法偵測主機所在網域的所有電腦主機，H-IDS 僅偵測其所在之主機所接收的封包資訊。

3. Hybrid IDS

結合 H-IDS 與 N-IDS 技術的入侵偵測系統，Hybrid IDS 係以主機系統爲基礎，會辨識網路封包流向或來自某主機的封包攻擊，並監測系統的日誌記錄、目錄及登錄檔中的攻擊行爲，較 N-IDS 不易發生誤報的狀況；另外它並不會檢查所有的網路封包，因此，其流量效能會比 N-IDS 佳。但是，由於它較 H-IDS 與 N-IDS 耗費主機系統的 CPU 運算資源，且有作業平台的限制與部署位置的爭議等缺點，一般不被採用[46, 47]。

4. Deception system

誘捕系統又稱爲"Honeypot"，它的功能如同其字義解釋”裝滿蜜糖的罐子”，不同於傳統的入侵偵測系統，它沒有偵測入侵／攻擊行爲[48, 49]的能力，也無法獨自從所蒐集到的日誌記錄中追蹤到真正的入侵者／駭客，其主要功能是借由模擬（Simulate）一

主機系統易遭受攻擊的漏洞或缺失，目的是要引起入侵者的偵測、入侵或攻擊等行爲，再經由詳細的日誌記錄分析及安全警示機制，獲得入侵者的行爲模式與動機，提供建構安全網路的修正建議。而 Honeypot 應該如何部署才能吸引入侵者的目光，也是一大問題，因此，一般企業組織幾乎不採用。

4.4.2 偵測模式

入侵偵測系統會使用不同的分析比對技術來偵測惡意的活動，區分爲異常偵測（Anomaly Detection）、誤用偵測（Misuse Detection）與混合偵測（Hybrid Detection）三種，分別敍述如下：

1. 異常偵測

是利用統計的理論，歸納將使用者的使用習慣與資料存取的規則，以建立一個記錄檔（Profile），做爲偵測電腦系統是否遭受入侵／破壞的依據；其次，採用正面表列方式，爲 IDS 建立正常的行爲規則集。然後，將目前系統的行爲稽核記錄與 IDS 的正常規則集做行爲差異之判斷與比較，差異若過大即可能爲不當的異常行爲，亦即符合過去行爲規則的行爲才算是正常的，否則，視同入侵／攻擊，例如，過度或非正常時間使用系統、使用者的系統呼叫程序改變等。特性是偵測率高、誤判率亦高。

2. 誤用偵測

是以規則爲基礎（Rule-Based）的技術，採用負面表列方式，替 IDS 建立各種已知的入侵攻擊樣式（Patterns）或特徵（Signature），然後藉由樣式比對（Pattern match）的方式，偵測出已確定的入侵或攻擊行爲；但是尚未定義的攻擊樣式，則無法偵測，亦即符合攻擊樣式或特徵之存取行爲，方視爲入侵／攻擊，其他者視同正常行爲。特性是偵測率低、誤判率亦低。

3. 混合偵測

結合異常偵測與誤用偵測兩者特性，採用正面表列定義安全規則集，以負面表列敍述攻擊樣式等兩種方式，目的爲互補二者的缺點。首先利用偵測率高的正面表列規則集比對，若發現異常狀況時，再交給誤判率低的負面表列攻擊樣式比對偵測，以提昇偵測

率、降低誤判率。偵測率與誤判率介於二者之間，表 4-1 爲三者之比較。

表 4-1　入侵偵測技術比較

類型	偵測率	誤判率	行爲規則
異常偵測	高	高	正面表列 建立正常行爲規則
誤用偵測	低	低	負面表列 建立異常行爲規則
混合偵測	中	中	混合

4.4.3　入侵偵測建置之建議

入侵偵測系統的設置位置一般而言有下列幾處，如圖 4-9 所示：

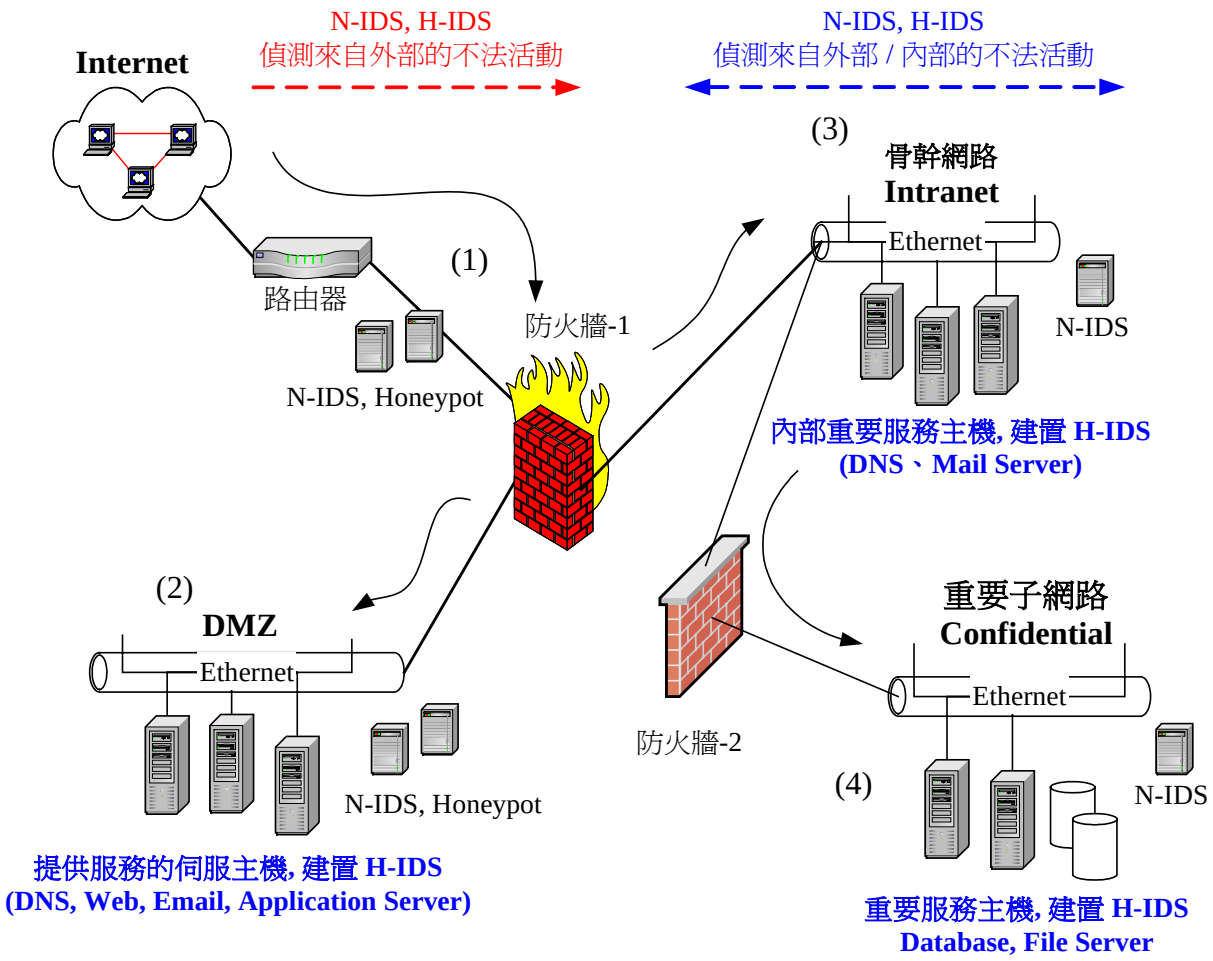

圖 4-9　IDS 建置位置

1. Internet 與防火牆之間

導入 ISO 17799 12.3.1 與 12.3.2 控制方法，在 Internet 與防火牆之間設置 N-IDS 與 Honeypot，這種設置方式的目的在保護防火牆本身與分析入侵／攻擊行爲，其意義是在防火牆實際遭受攻擊之前預先偵測出來，類似守門員在 Internet 與內部網路的必經節點上，即時蒐集經過此通道的網路封包，並分析比對 Honeypot 所蒐集的偵測、入侵與攻擊的日誌記錄，亦可利用 UDIDT（Union Defense of Intrusion Detection and Trace-back system）[50]偵測入侵攻擊來源，提早偵測不被允許的傳輸／網路存取行爲，並立即反應。例如，來自 Internet 惡意的 TCP SYN flood DoS 攻擊，N-IDS 可立即回應 TCP RST 封包中斷連線，避免攻擊封包進入內部網路，並即刻通知管理人員做適當處理。

2. DMZ 區域

導入 ISO 17799 9.1.1、9.4.1、9.4.6、10.1.1、10.2.1~4 與 12.3.1~2 控制方法，在非軍事區內建置 N-IDS、H-IDS 與 Honeypot，此種混合建置方式的目的分別是：

(1) 運用 N-IDS 偵測出已穿透（Penetrate）防火牆-1（見圖 4-9）的攻擊行爲，包括封包及連線，找出防火牆設定與存取規則不足之處，以修正改善之；同時可以監控 DMZ 內的封包行爲，阻止不合法的連線行爲與網路封包，一般而言，包括：

(i) 不允許由 DMZ 內的主機，向 Intranet 內部伺服主機要求連線。

(ii) 亦不允許 DMZ 主機上種植木馬。（註：目前僅 H-IDS 可防制種植木馬）

(iii)向 Intranet 內部伺服主機發動 DDoS 攻擊。

(iv)有異常或變形的 ICMP 封包進出。

(2) 在 DMZ 中的各重要主機上，例如，對外服務的 DNS、Mail、FTP 等伺服主機架設 H-IDS，目的是彌補 N-IDS 的不足，方法則是蒐集主機的系統記錄，以比對 N-IDS 未偵測出來的可疑的攻擊模式或特徵。

(3) 在 DMZ 設置 Honeypot 模擬一重要主機，蒐集並分析穿透防火牆入侵／攻擊的資訊與行爲，瞭解系統的漏洞或缺失，以修正系統安全措施。

3. 網路骨幹與重要子網路

導入 ISO 17799 9.4.7 與 9.4.8 控制方法，在網路骨幹（Backbone）與重要子網路上建置 N-IDS，並隱形於網路上以偵測所有主機[6]，並可同時監測網路流量與重要的網路資源，增加偵測機率，例如，低負載形式網路異常偵測器[51]爲一可行的實例。並建議網管人員設置一獨立子網路，將內部網路中關鍵的重要主機伺服器，例如，後端資料庫等，置於此區域，再架設偵測及防護系統防護之，例如，在網路骨幹上設置 N-IDS 分析進出該網路的封包，尋找違反事先定義存取規則的網路連線與存取，若有發現可疑事件，例如，未經授權的使用者，想透過網路連線竊取資料庫資料，N-IDS 會立即送出警示訊息給管理者或中斷此連線。

4. 重要主機

導入 ISO 17799 10.2.1 控制方法，在重要主機上設置 H-IDS，目的是偵測特定主機的入侵與攻擊，將所蒐集到的系統記錄與 H-IDS 的攻擊特徵分析模組相比對，例如，特殊字串比對或封包特徵是否遵循 RFC 標準等，若發現有符合攻擊特徵者，立即中斷此連線，並通知管理人員做適當的處理及反制。例如，偵測出駭客對 Windows IIS 網頁伺服器的 ISAPI 程式漏洞，施以緩衝區溢位攻擊，則管理人員應立即停用此服務程式，並對 IIS 做適當的修補（Patch）。此外，H-IDS 也能偵測個別使用者的上線使用記錄，例如，使用者的連線、對重要檔案修改或刪除、用哪些程式開啓哪些檔案、系統對外開啓連接埠的記錄等，及監測兩主機之間點對點的加密連線，提供管理者詳盡的記錄與點對點連線的防護。

綜合上述的敍述，入侵偵測系統係以監測網路封包的方式，偵測違反使用者訂定的安全規則或未經授權的使用、誤用或濫用等攻擊行爲，且能即時偵測出來自內部或外部的威脅[45]，例如，DoS、DDoS。也可以辨識封包所挾帶惡意指令或程式碼。其實，IDS 並不取代原有的網路安全機制（例如，加密演算、身份驗證等），而是互補網路防火牆僅信任特定服務與來源 IP 位址連線的存取規則等，在安全防護與控管上的不足之處，以增強開放式網路系統的安全。

4.5 存取控制與管理

在充分瞭解網路面臨的入侵攻擊及威脅後，我們將提出利用網路封包的特徵、身份鑑識與多層防禦等機制，來建構一個比較安全的防護系統，以有效保護內部重要主機及其中的資料。下面將分別就網路管理層面及技術方面的防護等，陳述基本的安全原則與機制。

4.5.1 技術層面之控制

意即由電腦系統在技術層面執行安全控制，因此，而對系統的弱點、缺失、不完善及漏洞，必須適當地利用身份鑑識、存取控制、傳輸控制等不同安全等級的工具或技術彌補之，以建構安全偵測防護體系。我們認爲在技術層面上應有以下之控制方法：

1. 嚴謹的身份鑑識

設立強韌的使用者身份驗證密碼，使其不易遭破解，可以防止未經授權的使用者擷取系統資訊，也可以防止合法使用者存取授權以外的資訊。我們認爲：

(1) 導入 ISO 17799 9.4.6 控制方法，在必要時利用網址轉換（NAT）機制轉換內部網址，不讓外部使用者知道內部的 IP 位址，因而，亦無從直接加以攻擊。

(2) 導入 ISO 17799 9.5.1~4 控制方法，在使用者帳號與密碼控管存取權限外，可以訂定較爲嚴謹的鑑識存取機制，例如，指紋、聲紋比對、智慧卡等，增加破解的困難度。

(3) 導入 ISO 17799 9.4.4 控制方法，建議利用 MAC 的唯一識別特性，因爲在網際網路上的每個網路介面，都有一個特定的網際網路位址（Internet Address，即 IP Address），這些位址是由 32 位元的數字所組成，當兩部主機欲在網際網路上溝通時，會藉由網域名稱系統（Domain Name System，DNS）所提供 IP 位址與主機名稱（Host Name）的動態對映，辨識出該主機所在網域，再將此封包訊息傳送至該網域。而在區域網路（LAN）中，當一個乙太（Ethernet）網路封包由一部主機傳送至另一部主機時，是由一組 48 位元的乙太網路位址（MAC）決定此封包傳送到那個介面。利用合法的 IP 與該主機唯一的 MAC（IP_MAC）配對使用，正面表列合法的 IP_MAC，訂定對伺服主機安全存取的過濾機制，例如，僅允許特定且合法的 IP_MAC 存取／維護檔案伺服器，以過濾不合法的封包，多一層身份存取鑑識。缺點則是網管人員亦難以從外部網路遠端存取該內部網路。

2. 採用 RBAC 的存取控制機制

導入 ISO 17799 9.1.1 與 9.6.1 控制方法，對於內部網路資料的存取，建議採用 RBAC 的概念[52]，及 Sandhu 等學者提出的存取控制模型理論[53, 54]，依使用者（User）、角色（Role）、授權（Authorization）、角色的執行時間（Session）等四個元素設計存取機制，將角色事先授予使用者，並授予符合該角色的存取權限，使用者依據所授予的權責來進行系統的存取。此種方式，不但簡化系統授權與維護的管理程序，並且可以有效地控管資料的存取，也提昇了資料的安全性。

3. 網路傳輸的控制

在網路傳輸控制方面，有下列的建議：

(1) 導入 ISO 17799 9.4.7、9.8.1 與 9.8.2 控制方法，在網路連線後，不論是以撥號連線或直接連上公眾網路，對資訊流向應做適當的監控管理，而僅允許合法的帳號及網路位址對特定資料的存取。例如，從外部網路傳送進來的封包來源 IP 卻是屬於本內部網路的位址；相對的從內部網路傳送出去的封包來源 IP 卻不屬於本內部網路的位址，前者表示有人冒用本內部主機之 IP 傳送封包，後者則表示有某一網路主機 T 已遭到入侵，而入侵者以 T 爲跳板且以假 IP 去攻擊其他主機。這類不合法的封包傳輸，必須予以阻斷及禁止存取。

(2) 導入 ISO 17799 9.4.8 控制方法，建議設定內部重要主機 S 傳送資料的路由繞送規則 R，讓合法使用者向 S 要求資料時，S 會依循我們所設定的路由路徑 R 傳送給使用者；對於不合法的使用者，則不提供路由服務，使之無法向 S 提出服務要求，防止不合法的存取服務。

(3) 導入 ISO 17799 9.4.8 控制方法，在封包的流向與流量控管上，可以對 TCP/IP 協定的 TCP、UDP 及 ICMP 封包，在不同的環境上，做不同層次的控管，例如，一般傳統的 DoS 攻擊或掃瞄偵測，都是送出大量 OSI 第三層封包進行攻擊，或利用 TCP／UDP 封包探測目標系統，甚至運用很少被監控或過濾的 ICMP 封包（例如，ICMP Echo、ICMP Echo Reply 等建立後門），以竊取資訊，或將攻擊指令封裝於封包內進行系統攻擊等。因此，必須有效控管封包的流向與流量，才可以有效地發覺可能的入侵管道。

(4) 導入 ISO 17799 9.7.1 與 9.7.2 控制方法，在重要節點上，例如，路由器、防火牆、伺服主機，記錄網路使用狀況、日誌記錄（Audit log）及建立系統存取稽核機制，以便後續之追蹤或監控，以提供路由／存取控制的修正資訊。

(5) 導入 ISO 17799 9.4.1、9.4.5、9.4.9 與 10.3.1 控制方法，對於以明文方式傳送的網路服務，例如，FTP、Telnet，易被駭客擷取／竊聽，必須做網路連線的控管，並關閉不必要的通訊埠，避免駭客／入侵者直接對系統在該種服務上之弱點進行入侵及建立後門。

4. 多層防火牆的防禦

爲使網路防火牆更加堅固、安全，可以

(1) 導入 ISO 17799 9.5.5 控制方法，增加網路防火牆的設置，並利用不同廠商、不同系統種類的特性，提高防禦力。因爲使用相同的系統，入侵者祇要能夠破解或入侵其中一個，就可以入侵其他的防火牆；而不同品牌防火牆設定相同錯誤的機會就減少了，系統缺失亦不儘相同，可增加入侵的困難度，系統的安全性自然提高。

(2) 導入 ISO 17799 9.4.6 控制方法，依實際之環境需求，採用不同型式的防火牆運用。一般而言，在相同的平台上，封包過濾式防火牆的效能會比應用層防火牆好，因爲前者並不需要處理額外的連線動作，也不需要經過代理程式的介入與轉換處理，可獲得速度快的好處；相對地，後者沒有給予內部或外部網路任何直接連線的機會，且可以在封包到達真正的目的地之前，先檢視其命令，降低應用層的入侵攻勢，安全性較高。爲兼顧封包過濾的速度與安全性，應依實際環境上的需要，採用不同的型式的防火牆運用。

我們的建議則是：

(i) 導入 ISO 17799 9.4.6 與 9.4.7 控制方法，利用兩個防火牆一內一外，分別阻隔內部網路與外部網路，見圖 4-10，其中，非軍事區則設置在兩個防火牆之間。在接連外部網路的地方，必須承擔非軍事區的大量網路流量，建議採用效能較高的封包過濾式防火牆擔負對外的第一線防禦；第二層防火牆，僅負責內部網路的傳輸，流量小，安全性要求高，建議使用應用層防火牆。

(ii) 導入 ISO 17799 9.4.6、9.4.7、9.6.2 及 10.4.3 控制方法，在內部網路中另外設置一內部防火牆（防火牆-3）。存放敏感資料的伺服器若曝露在內部網路的共用網路區域，內部的使用者可以直接對它進行攻擊。因此，在內部網路中，建議另外建置一個內部防火牆，分隔一般使用者使用網段與存放極重要資料的服務網段（例如，資料庫、檔案伺服器），並嚴格限制內部使用者存取權限，僅允有權限的使用者，透過特定的應用程式（例如，透過 SQL *Net）存取資料庫，不允許其他非法軟體／程式直接存取之，以增加資料存取的安全性[31]。由於此網段的重要資料，僅提供特定的對象、特定的服務，例如，資料庫的維護、檔案的存取等，網路傳輸效能不需太高，因此建議使用安全性較高的應用層防火牆

建置。

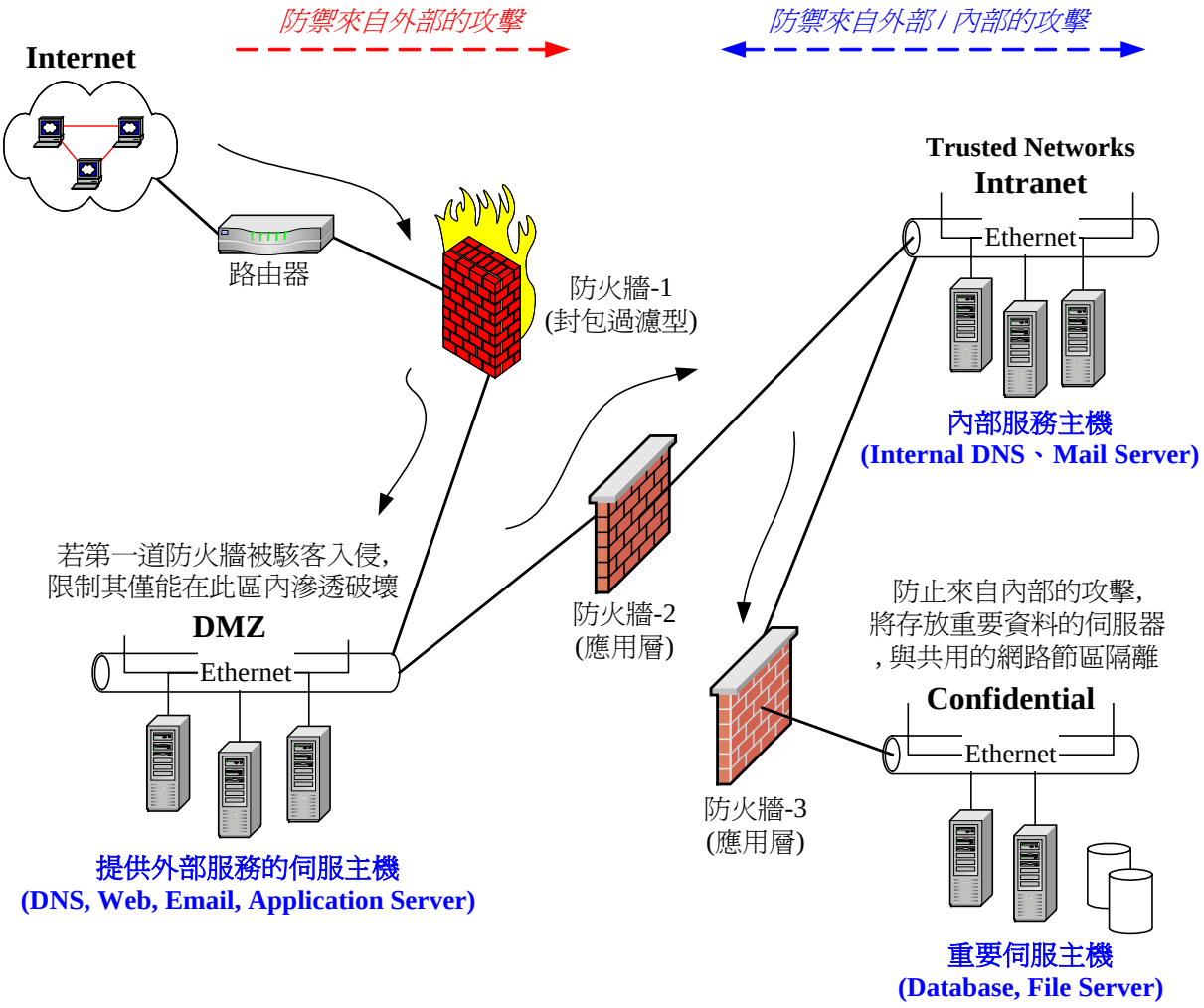

圖 4-10　多層防火牆架構

5.　非軍事區系統的設置

對非軍事區系統內的建議是：

(1) 導入 ISO 17799 9.4.6 控制方法，建議對交談式連線服務，另外建立一個非軍事區來放置這些交談式連線的伺服主機[31]。

(2) 導入 ISO 17799 8.7.3、8.7.4、8.7.6、9.4.2 及 9.4.3 控制方法，依伺服主機所提供服務的特性，例如，DNS、Mail 伺服主機，分別在非軍事區及防火牆後端建置對外與對內的伺服主機，以降低系統遭受入侵的損害，及節省系統的回復時間。又若網頁伺服器會存取內部資料庫，建議透過第三部系統 M（應用程式伺服器）與內部

資料庫 D 溝通，意即，使用者透過 M 間接地存取 D，以降低直接連線危及 D 的風險。（如圖 4-11）

(3) 導入 ISO 17799 9.1.1 與 9.4.8 控制方法，在設定 Intranet 內部網路與非軍事區間的連線規則時，應該儘量是由 Intranet 內部系統對非軍事區發起連線要求，避免非軍事區的系統遭到入侵植入惡意的木馬程式，對內部網路發動攻擊；至於 Intranet 內部系統是否可以直接存取非軍事區，則可以視組織政策決定，但是，絕對不允許外部使用者直接存取 Intranet 內部系統。

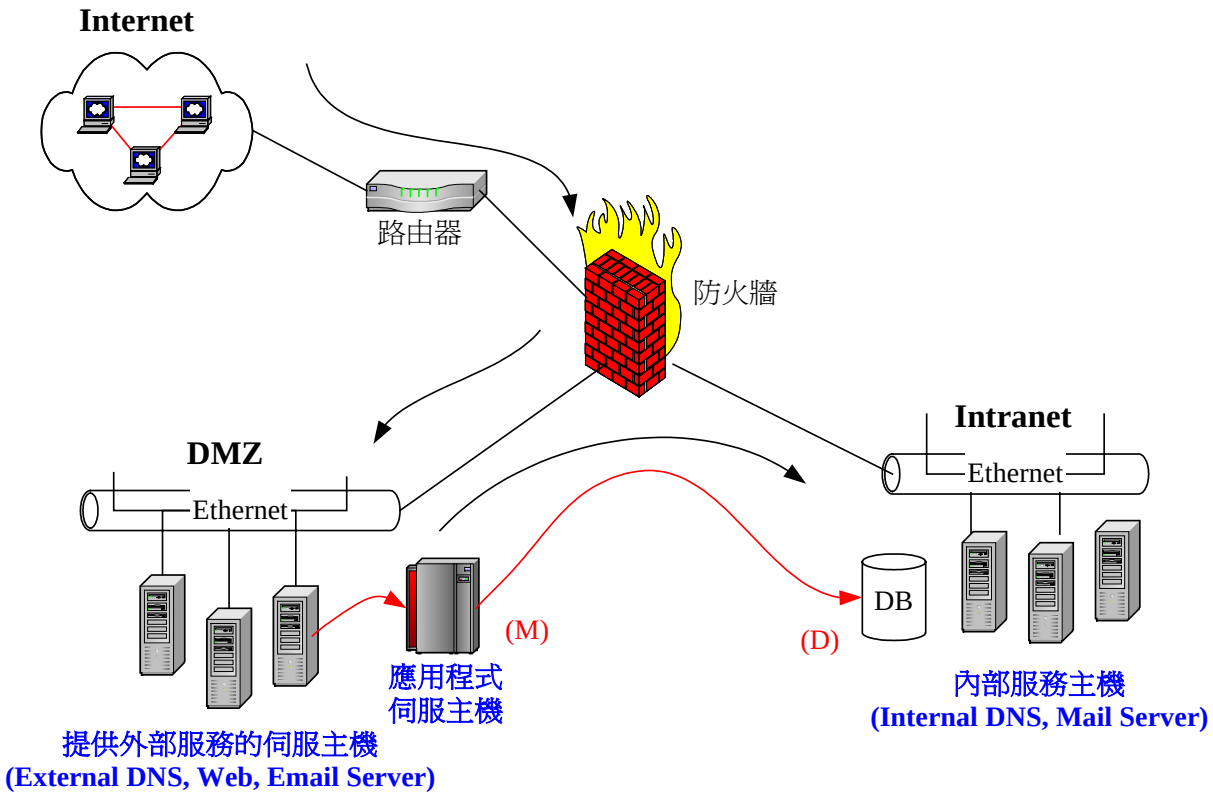

圖 4-11　置於非軍事區的系統

隨著入侵／攻擊技術的成長，與網路結構與應用的變化，適時地調整網路安全的管理方式及安全策略，並加強網路內部未經授權的服務與安全較薄弱節點的監控，必要時檢查與分析網路封包，找出異常的網路行爲或攻擊，予以拒絕，才可以保護內部主機與資源的安全。

4.5.2 管理層面之管控

對於網路設施及系統安全的設定，皆應由系統管理人員依需要而爲之，規範各級管理人員作業範圍，並明訂資訊設備安全政策[13, 55, 56, 57, 58]，包括：

1. 風險評估及管理

針對系統可能面臨的挑戰與潛在威脅，對系統、網路及組織層級，做系統滲透測試評估，以爲建立安全計畫的基礎，分述如下：

(1) 資產分類，產生清冊[56, 59]

導入 ISO 17799 5.1.1~3、7.2.1、7.2.4~5 與 8.6.1~2 控制方法，對資產分類，指明其需要、優先順序和保護級別，再根據資產分類之結果，彙整資產清冊。目的是在保證資產，使其得到適當的保護，幫助企業／機關確保對資產實施有效的保護。

(2) 風險評估

爲減少系統安全威脅，應

(i) 導入 ISO 17799 5.2.3 控制方法，對組織各項資產，面對可能因爲人、事、時、地、物等因素所產生之危害，進行風險評估，訂定危機等級與類別[59]，以針對各安全重點所在施以安全管理。

(ii) 導入 ISO 17799 5.1.1 控制方法，當一個系統、設施或資料引起窺覬或挑戰時，就會產生安全威脅，入侵者（含內部員工）就會有計劃的蒐集目標主機的資訊，包含：網路 IP 位址、使用者帳號／密碼、系統安全的弱點等，再透過網路（含 Internet）或直接實際的存取。因此，應借由安全威脅分析，列出易被入侵攻擊的目標，及可能造成的損失，賦予各項安全威脅加權值，做爲安全改善評估依據。

(iii) 導入 ISO 17799 10.4.1 與 10.5.1~3 控制方法，網管人員應該定期依系統公告之新版本之修補（Patch）程式更新系統，改善系統的安全漏洞。

(3) 滲透測試

在系統建置完成後，應

(i) 導入 ISO 17799 10.4.2 控制方法，由系統安全人員模擬入侵者所有可能的入侵／攻擊模式，並利用駭客常用的入侵攻擊工具，嘗試入侵系統竊取資料，再依成功入侵系統的審計資料分析，與評估各項安全方案的應變能力不健全之處，改善目前的安全機制。

(ii) 導入 ISO 17799 11.1.5 控制方法，依據安全標準，例如，ISO/IEC 17799[13]，執行系統規劃設計，定期測試、評估資訊安全技術與措施，例如，漏洞掃瞄、入侵偵測等，找出系統缺失或漏洞，給予適當修正或採行合宜的安全技術。

2. 人員安全管理控制

針對使用者的安全管理與考核，應

(1) 人員安全評估

導入 ISO 17799 6.1.1~4 及 6.2.1 控制方法，聘雇人員之工作職責會觸及機密性資料與設施者，應該經過安全調查。人員聘用之安全評估參考項目包括個人性格、申請者之經歷、學術及專業能力及資格、人員身分之確認、財物及信用狀況等[60]。在聘僱階段，應該說明使用者之安全責任，並列入聘雇合約內，且在聘雇期間進行監督[59]。

(2) 系統使用規定

導入 ISO 17799 9.2.1~4 及 9.3.1 控制方法，訂定系統存取政策及授權範圍規定，依不同等級使用者，給予不同的存取權限，例如，限制使用者不允許存取機密資料檔案、或僅給予讀取權限等控制，並定期更改登錄密碼；另外，必須隨使用者職務的異動，依規定調整其使用權限，例如，對離職／休職人員，應立即取消其使用權限，以避免惡意的破壞。

(3) 安全稽核

導入 ISO 17799 8.4.2、8.4.3 與 12.1.5 控制方法，記錄每位使用者使用系統的記

錄與行爲，一旦發現有違法或未經授權的網路行爲，例如，異於往常的網路存取、或存取不被允許的資料等，必須立即回應，並通知管理人員實際瞭解與處理。

(4) 資訊安全教育

導入 ISO 17799 6.2.1 控制方法，爲提昇組織內部所有人員對資訊安全的認識，我們必須

(i) 針對工作職責與角色，所負責處理資訊的機密性及敏感性，應經過安全程序評估，並對不同層級的人員，進行資訊安全教育及訓練，包括資訊安全政策、資訊安全法令規定、資訊安全作業程序，以及如何正確使用資訊科技設施之訓練等[59, 61]，將可能的安全風險降到最低。

(ii) 定期對使用者實施資訊安全教育及訓練，讓使用者瞭解資訊安全的重要性及與各種可能的安全風險，以提昇使用者的安全意識[61]。

(iii) 導入 ISO 17799 4.3.1 控制方法，除組織內部使用者外，還對對外包協力廠商進行資訊安全教育及訓練。

(iv) 導入 ISO 17799 6.3.1、6.3.3 及 6.3.5 控制方法，訂定組織資訊安全事件之通報及處理程序、責任歸屬及獎懲規定等[56]，讓使用者在遭受安全威脅時，能依循安全政策與處理程序處理安全事件。

3. 系統維護控制

對支援重要業務運作的資料中心或機房，應建立良好的安全措施，及適切的人員出入管制制度，防止非管理人員卻能直接接觸不應觸及之系統或資料，以下分述之：

(1) 使用者認證辨識

導入 ISO 17799 7.1.2、7.1.3 及 9.4.4 控制方法，除了傳統的門禁管理與使用密碼登錄系統外，還必須增加認證辨識技術（例如，視網膜辨識、聲紋辨識等）加強對使用者的辨認；另外，爲確實管理各使用者在網路存取的辨識，建議應該給予個人固定的 IP 位址，並與網路卡 MAC 位址的唯一性組合運用，以提昇

網路的存取辨識。

(2) 作業安全管制

導入 ISO 17799 4.3.1、8.3.1 及 10.5.5 控制方法，系統在（外包）建置、維護、更新等各階段，即應實施安全管制，避免系統被種植木馬、建置後門或病毒等安全漏洞，例如，維護人員擅自建立帳號、或遠端遙控軟體，將危害系統安全，並規範限制建置／維護人員，不允許接觸不該接觸之重要系統或機密資料，以確保資訊資源之安全。

(3) 系統使用權限管理

導入 ISO 17799 8.1.4、8.1.6 及 9.3.2 控制方法，必須建立網路設施的使用與管理制度，例如，防火牆、路由器，由專職管理人員負責管理，並明確規範使用者對系統資源的使用權限與合理授權範圍，例如，在某主機上的使用者（透過 IP_MAC 鑑識），僅能讀取檔案伺服器的公用資料庫，且不允許發送電子郵件等，俾易於系統安全監測管理，增加識別不合法的網路存取行爲。

4. 建立實體環境的安全防護

爲防止對工作場所資訊的非法存取、破壞和干擾，必須建立物理安全環境，以保障資通訊設施硬體的安全，以下分述之：

(1) 隔離區

導入 ISO 17799 7.1.1 控制方法，依據風險評估對資訊設施與辦公地點劃分安全區域，並爲每個安全區域建立物理保護設施，例如，電磁防護及電源接地，提高整體的保護效果[56]。

(2) 出入管制

導入 ISO 17799 7.1.2 與 7.1.4 控制方法，系統存放的安全區域必須對人員的進出做適當的管制，若未經允許與批准，任何人員皆不得進出此安全區域，對於進入管制區的人員身份與目的必須事先查明，並告知安全要求與緊急狀況處理步驟，嚴格限制對資訊系統的存取，並定期審查安全措施與規定[56]。

(3) 委外開發規定

導入 ISO 17799 4.2.1~2、4.3.1、7.1.1 與 8.1.5 控制方法，系統委外（Outsourcing）開發設計、測試環境，應該另外建置系統開發／測試環境，實體區隔正式環境與測試環境，避免承包商觸及組織內部資訊／資源，例如，另外設置一子網路供承包商進行系統的開發與測試，防止組織資訊暴露或被有心人士竊取，並與承包商簽訂保密條款，及控管考核所有參與該建置專案的人員，防止非法使用系統資源[62]。

5. 資料輸出、輸入控制

對各項資料輸出或輸入，均應建立識別通行碼管理制度，對重要性、敏感性資料在建檔時，應加密或加設資料存取控制，以防止外洩，以下分述之：

(1) 傳輸連線加密

導入 ISO 17799 10.3.2~4 控制方法，透過 Internet 傳送機密資料，必須採用加密認證或數位簽章等安全技術，例如，SET（Secure Electronic Transaction）、SSL（Secure Socket Layer）等，也不允許以電子郵件夾檔方式傳輸，避免在網路傳輸資料時被截取及監聽。

(2) 機密資料加密

導入 ISO 17799 10.3.2 與 12.1.6 控制方法，對機密資料在建檔時，施以加密（Encryption）措施，增加一層資料存取的安全防護，例如，未經授權的使用者，即使拿到此文件資料，沒有解密程式／密碼，仍無法看到本文內容，亦可避免遭受篡改及不當使用。

(3) 網路監控

導入 ISO 17799 8.5.1、9.5.5、10.5.4、11.1.2 及 12.3.1 控制方法，設置網路防火牆與入侵偵測系統，偵測／監控網路封包與連線行為，當發現可疑或不符合安全規則／策政的事件，例如，入侵者植入後門程式危害系統、或網路流量異常增加等，則及時警示告知或自動阻止反制，例如，中斷連線、管制使用者存取，並通知管理者做適當處置，例如，調查使用者目的、或適時修正系統安全漏洞

等。

(4) 安裝防毒軟體

導入 ISO 17799 8.3.1 與 8.7.4 控制方法，防火牆與入侵偵測系統，對合法使用者在網路上的存取，並無法過濾含有危害系統的病毒郵件。因此，爲了防範病毒的威脅，應該在組織內部採用強韌的防毒軟體，分別安裝於重要的檔案伺服器、郵件伺服器及個人電腦上，且定期更新病毒碼程式，以防範新型病毒的威脅。

(5) 資訊交換管理

導入 ISO 17799 8.7.1~2、8.7.5 與 8.7.7 控制方法，在組織與組織之間的資訊傳輸與交易，必須遵循統一的傳輸協定標準與資料格式標準，且傳輸連線施以加密措施或數位簽章，利用防火牆、入侵偵測與追蹤系統，分隔 Internet、Intranet 與保護組織內部重要資訊，確保組織間資訊傳輸的安全性。

6. 應變及緊急處理計畫之規劃

導入 ISO 17799 8.1.3 控制方法，擬定危機管理及復原計劃[56]，制定備份政策，建立資訊安全事件的緊急處理機制，降低入侵事件的損害，並節省系統回復時間，以下分述之：

(1) 備份機制

設置備份機制，讓系統在災害發生時，能利用此備份資料／系統復原。可以

(i) 導入 ISO 17799 6.3.2 與 6.3.4 控制方法，依網路安全弱點與威脅分析，訂定安全處理機制，做爲備份與災害應變參考，例如，DNS 伺服主機應該配置第二套備用服務主機，在第一套 DNS 無法正常提供服務時，可以立即取代之，以使網路作業環境維持正常。

(ii) 導入 ISO 17799 8.4.1 與 11.1.1 控制方法，定期／不定期的備份系統資訊與資料，並制定資料／文件保存方案（例如，備份資料必須存放一份於網路資料中心及異地備援），及建立異地備援系統，以提供災害應變回復之用。

(iii) 導入 ISO 17799 11.1.3 控制方法，定期檢討備份計劃與測試復原程序的可靠性，確保備份機制的有效性，以符合系統環境的變更。

(2) 緊急處理程序

緊急處理程序必須從零思考，當災害發生時，可以從網路架構的建置至完成爲止，所有的軟硬體設施皆能回復至災害發生前的正常狀態。我們必須

(i) 導入 ISO 17799 11.1.2 控制方法，爲每個層級（例如，網路設施、作業系統、應用程式、伺服主機等），制定明確修復程序與方法，例如，伺服主機資料損毀時，首先應從建置系統環境開始，其次加入安全機制，再做資料回復作業、測試，最後才開放使用，並在各階段明確指定負責單位與配合人員（含供應商）等，以加速系統重建。

(ii) 導入 ISO 17799 11.1.5 控制方法，定期測試或更新災害復原計劃，以驗證系統重建能力、或改進備份作業、與安全措施之不足。

(iii) 導入 ISO 17799 11.1.3 控制方法，研擬一替代方案，在系統無法由備份機制復原時，使組織運作不致停滯。

本論文導入 95 項 ISO 17799 之資訊安全管理控制方法，尚有 32 項方法未納入，如表 4-2 所示。

表 4-2　未納入控制項目

編號	控制項目	控制方法
3.1.1	資訊安全政策	資訊安全政策文件
3.1.2	資訊安全政策	審查及評估
4.1.1	安全組織	管理資訊安全委員會
4.1.2	安全組織	資訊安全協調

4.1.3	安全組織	資訊安全責任分派
4.1.4	安全組織	資訊處理設備的授權程序
4.1.5	安全組織	資訊安全專家的建議
4.1.6	安全組織	組織間的合作
4.1.7	安全組織	獨立的資訊安全審查
7.1.5	安全區域	輸運和裝載區域的區隔
7.2.2	設備安全	電源供應
7.2.3	設備安全	纜線傳輸安全
7.2.6	設備安全	設備報廢或再利用的安全防護
7.3.1	一般控制	辦公桌面淨空及電腦螢幕淨空政策
7.3.2	一般控制	資產的移出
8.1.1	作業程序與權責	文件化的操作程序
8.1.2	作業程序與權責	操作變更控制
8.2.1	系統規劃與認可	容量規劃
8.2.2	系統規劃與認可	系統驗收
8.6.3	媒體控管	資訊的處理程序

8.6.4	媒體控管	系統文件的安全
9.5.6	作業系統存取控管	提供受脅迫警報以保護使用者
9.7.3	監控系統之存取與使用	計時器同步
10.3.5	加密措施控管	金鑰管理
11.1.4	企業永續經營	業務持續運作規劃之架構
12.1.1	遵循法令之要求	鑑別適用的法律規定
12.1.2	遵循法令之要求	智慧財產權
12.1.3	遵循法令之要求	組織記錄的保護
12.1.4	遵循法令之要求	個人資訊的隱私及資料保護
12.1.7	遵循法令之要求	證據蒐集
12.2.1	安全政策之檢視與技術之遵循	安全政策的符合性
12.2.2	安全政策之檢視與技術之遵循	技術符合性的檢查

第5章 結論

網路系統的安全性，往往取決於網路系統中最脆弱的環節，也必須即時發現入侵或攻擊，並予以有效修補與防制，才能有效保障網路系統的安全。

本論文從資訊科技的角度，探索架構及管理一個網路時，應該考量那些因素以確保網路的安全性，這些因素包括：曝露在外界的網路設施的缺失及漏洞、潛藏的外在威脅與破壞、網路內部不易偵測的漏洞，及一般駭客的入侵技術、方法與管道等，俾在建置監測機制時，對各項不足之處或有安全疑慮之處，做適當的修補與改進，防制惡意或無意的入侵破壞。我們係從網路安全威脅、入侵者常利用的技術及手法、網路安全設計及網路存取監控角度來探討，首先分析網路安全的各項威脅，並探討各項入侵系統的技術與知識，包括：1、從入侵者的角度思考在網路架構上，那些資訊是入侵前必需要獲得的？哪些網路設施有哪些潛在的入侵管道？並歸納出網路系統可能面臨的安全威脅。2、網路設施的設計瑕疵及存取控制等，讓網路管理者瞭解系統先天的缺失及缺陷。3、駭客如何借助於網路的各種弱點、缺陷與攻擊手法入侵一個系統。俾期望有助於建立全面性的網路安全架構。

其次探討入侵者常利用的技術及手法，及駭客入侵的各項偵測技術，包括：1、站在入侵者的角度思考，駭客的基本入侵流程，及其盜取系統資源或竊取機密資料，而不留下任何蛛絲馬跡的手法。2、從入侵的趨勢與入侵封包的特徵，分析目前入侵者的行爲趨勢與手法，及 TCP/IP 網路入侵封包標頭的特徵與特性，認知目前網路內部未來將面臨的安全威脅。3、從駭客用以偵測系統弱點，確認及聆聽各個連接埠的開啓／關閉及服務狀態等相關掃瞄技術。期望管理人員／技術人員能依之在網路重要節點，擷取適當的網路封包，分析其標頭資訊，過濾特定種類或不合法的網路封包，而偵測出駭客的入侵或破壞行爲。

研究在網路安全設計上，如何應用不同的技術監控網路，以保護整個內部網路系統，包括：1、在內部網路各重要地點設置網路防火牆，以建立一道有效的雙向安全控管機制，防止外界對內部資訊的不當存取，及限制內部主機對內及對外部的通訊。2、應用入侵偵測技術強化封包過濾機制，補足網路防火牆的不足，在網路重要節點蒐集各

種封包訊息，透過封包監視、安全審計與攻擊辨識等，判斷是否有違反安全策略或攻擊行爲，提早警示反應，提昇系統安全性。

最後，探究在網路存取監控上，網管人員在充分瞭解網路面臨的入侵攻擊及威脅後，如何利用網路封包特徵、身份鑑識機制與多層防禦機制等，並導入 ISO 17799 國際資通安全管理標準，建構安全的傳輸機制，包括：1、在監控地點蒐集與分析網路封包，而從封包特徵的辨識及異常的連線確認等，制止可疑的入侵與攻擊行爲。2、根據網路存取的基本原則、管理控制到技術控制上防止系統入侵及未經授權之資料存取。3、依據網路封包存取的特性，制定封包傳遞的規則，及利用 IP_MAC 位址的唯一性，嚴格的封包過濾與進階的身份鑑識機制，並利用多層防火牆的防禦機制，區隔存放敏感資料的地點，以保障內部網路安全與重要伺服器資訊的安全。表 5-1 爲網路存取監控之建議彙整表。

表 5-1　網路存取監控之建議

項次	存取監控項目	控管措施
1	4.2.1 異常連線	1. 連線失敗 2. 阻斷的連線。
2	4.2.2 監控節點	1. 重要主機 2. 外部與內部網路的交接邊界 3. 對於曾經遭受過攻擊或入侵的系統或子網域。
3	4.4.3 入侵偵測建置建議	1. 在 Internet 與防火牆之間設置 N-IDS 與 Honeypot 2. 在非軍事區內建置 N-IDS、H-IDS 與 Honeypot 3. 在網路骨幹與重要子網路上建置 N-IDS

4	4.5.1 技術層面控制	1. 嚴謹的身份鑑識 2. 採用 RBAC 的存取控制機制 3. 網路傳輸的控制 4. 多層防火牆的防禦
5	4.5.2 管理層面之管控	1. 風險評估及管理 2. 人員安全管理控制 3. 系統維護控制 4. 建立實體環境的安全防護 5. 資料輸出、輸入控制 6. 應變及緊急處理計畫之規劃

參考文獻

[1] Taiwan Computer Emergency Response Team / Coordination Center, http://www.cert.org.tw, July 2003.

[2] 呂芳懌、楊子逸，“IIS 伺服器漏洞剖析與防備，”第四屆 2002 年「網際空間：資訊、法律與社會」學術研究暨實務研討會，2002 年 11 月。

[3] 蘇澈　譯，駭客的秘密：網際網路篇，碁峰資訊，1998 年 6 月。

[4] K. Lars, J. Edward and Jr. Renehan, Hacker Proof: The Ultimate Guide to Network Security, Delmar Learning, January 1997.

[5] J. Scambray, S. Mcclure and G. Kurtz, Hacking Exposed: Network Security Secrets & Solutions, 2nd ed. McGraw-Hill, 2001.

[6] K. Mandia and C. Prosise, Incident Response's: Investigating Computer Crime, McGraw-Hill, 2001.

[7] Distributed Denial of Service (DDoS) Attacks/tools, http://staff.washington.edu/dittrich/misc/ddos/, July 2003.

[8] L.T. Heberlein, G.V. Dias, K.N. Levitt, B. Mukherjee, J. Wood and D. Wolber, "A Network Security Monitor," Research in Security and Privacy, Proceeding of IEEE Computer Society Symposium, pp. 296-304, May 1990.

[9] S. Snapp and J. Brentano and G. Dias, "DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and an Early Prototype," Proceeding of the 14th National Computer Security Conference, pp. 167-176, October 1991.

[10] National Computer Security Center, Glossary of Computer Security Terms, Ver. 1, Rainbow Series, October 1988.

[11] Lunt, Tamaru, Gilham, Jagannathan, Neumann and Jalali, "IDES: A Progress Report," Proceedings of the 6th Annual Computer Security Applications Conference. December 1990. (Available: http://www.sdl.sri.com/papers/870/, July 2003.)

[12] W. R. Stevens, TCP/IP Illustrated, vol. 1, The Protocols, Addison-Wesley, 2000.

[13] ISO/IEC 17799：2000（E），資訊技術－資訊安全管理的作業要點，經濟部標準檢驗局，2002 年。

[14] T. Humphreys and A. Plate, "Risk Assessment, Risk Management, Policies and Procedures," BS7799 Training Course, 2001.

[15] 呂芳懌、蘇俊維，“網路入侵與防禦策略探討，”第三屆網際網路應用與發展研討會，2002 年 5 月。

[16] 呂芳懌、蘇俊維、許惟翔，“內部網路安全威脅分析與防制，”2003 電子商務與數位生活研討會，2003 年 4 月。

[17] D. Song, http://monkey.org/~dugsong/dsniff, January 2002.

[18] Insecure Organization, http://www.insecure.org/nmap/, July 2003.

[19] Nettlesting software, http://www.nettlesting.com/nettoolbox/documentation/dns.htm, July 2003.

[20] Project Loki, http://phrack.org/phrack/49/P49-06, Phrack Magazine, Volume 7 Issue Forty-Nine, August, 1996. January 2002.

[21] P. Krauz, http://lin.fsid.cvut.cz/~kra/index.html, January 2002.

[22] How-too hijack a TCP connection, http://www.dsinet.org/textfiles/faqs/alt-hacking-FAQ/howto5.html, July 2003.

[23] C.E. Landwehr and D.M. Goldschlag, "Security Issues in Networks with Internet Access," Proceedings of The IEEE, Vol. 85, No. 12, December 1997.

[24] SANS/FBI Institute, "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus," http://www.sans.org/top20/, July 2003.

[25] 呂芳懌、楊子逸，“IIS 網頁伺服器 Unicode 漏洞探討，”2001 年第五屆資訊管理學術暨警政資訊實務研討會，2001 年 6 月。

[26] Microsoft Security Bulletin MS02-045: Unchecked Buffer in Network Share Provider Can Lead to Denial of Service (Q326830),

http://www.gsn-cert.nat.gov.tw/news86.html, July 2003.

[27] Network Share Provider 未核取的緩衝區會導致阻絕服務 (Q326830)，http://www.microsoft.com/taiwan/security/bulletins/MS02-045.asp，2003 年 7 月。

[28] Request for Comments: 1157, A Simple Network Management Protocol (SNMP), http://www.faqs.org/rfcs/rfc1157.html, July 2003.

[29] Request for Comments: 1446, Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2), http://www.faqs.org/rfcs/rfc1446.html, July 2003.

[30] Sniffer Pro - Investigater, http://www.snifferpro.co.uk/, July 2003.

[31] E. Maiwald, Network Security: A Beginner's Guide, McGraw-Hill, 2001.

[32] G. Xiaobing, Q. Depei, L. Min, Z. Ran; X. Bin, "Detection and protection against network scanning: IEDP", Proceedings of Computer Networks and Mobile Computing, pp. 487-493, October 2001.

[33] Pelt Tech - Computer Security, http://www.pelttech.com/tools/pinger.zip, July 2003.

[34] The SANS Institute, http://rr.sans.org/audit/netcat.php, July 2003.

[35] SomarSoft Utilities, http://www.somarsoft.com, July 2003.

[36] user2sid and sid2user, http://www.chem.msu.su/~rudnyi/NT/, July 2003.

[37] From: Evgenii Borisovich Rudnyi, name of built-in administrator, http://www.chem.msu.su:8080/~rudnyi/NT/sid.txt, July 2003.

[38] Stake, Inc. http://www.l0pht.com, July 2003.

[39] IBT - Center for Anvendt Datalogi, Jespers NT tools, http://www.ibt.ku.dk/jesper/Nttools, July 2003.

[40] A. Householder, K. Houle, and C. Dougberty, CERT Coordination Center, "Computer Attack Trends Challenge Internet Security", Computer, Volume: 35 Issue: 4 , pp. 5-7, Aprial 2002.

[41] 陳昱仁、謝文川，“具即時組態與主動回應之網路式入侵偵測系統設計，”第十二屆全國資訊安全會議，2002 年 5 月。

[42] M. Goncalves, Firewalls A Complete Guide, McGraw-Hill, 2000.

[43] 江玉婷，淺談網路防火牆之技術與應用，http://lips.lis.ntu.edu.tw/ytchiang/study/study_big.htm，2003 年 7 月。

[44] R. Power, "2002 CSI/FBI Computer Crime and Security Survey," Computer Security Institute, 2002. (Available: http://www.gocsi.com/, July 2003.)

[45] B. Mukherjee, L. T. Hoberlein and K. N. Levitt, "Network Intrusion Detection," IEEE Network, Volume: 8, Issue: 3, pp. 26-41, May 1994.

[46] 賽門鐵克公司，入侵偵測系統－降低網路安全風險，http://www.symantec.com/region/tw/enterprise/article/intrusion_detection.html，2003 年 7 月。

[47] 強化企業資安利器：入侵偵測，http://taiwan.cnet.com/enterprise/people/story/0,2000040558,20063241-2,00.htm，2003 年 7 月。

[48] Intrusion Detection Systems, Honeypots and Incident Handling, http://www.honeypots.net/, July 2003.

[49] KeyFocus Ltd., http://www.keyfocus.net/kfsensor/, July 2003.

[50] 呂芳懌、鄭真真、洪嘉鴻，“UDAIDT：以 Hash 爲基礎的主動式區域聯防入侵偵測與追蹤系統，”第十四屆國際資訊管理學術研討會，2003 年 7 月。

[51] 呂芳懌、黃品璁、楊子逸、胡凱崴，“低負載形式網路異常偵測器，”2003 電子商務與數位生活研討會，2003 年 4 月。

[52] D. Ferraiolo and R. Kuhn, "Role-Based Access Control," Proceedings of 15th NIST-NCSC National Computer Security Conference, October 1992.

[53] R.S. Sandhu, E.J. Coyne, H.L. Feinstein and C.E. Youman, "Role-Based Access Control Models," IEEE Computer, Vol. 29, Issue: 2, pp. 38-47, February 1996.

[54] Z. Tari and Shun-Wu Chan, "A Role-Based Access Control for Intranet Security," Internet Computing, IEEE, Vol. 1, Issue: 5, pp. 24-34, September 1997.

[55] ISO/IEC TR 13335，資訊技術－資訊安全管理的指導，經濟部標準檢驗局，2002年。

[56] 王俊雄、林宜隆，“警政資通安全管理政策之研究，”第六屆資訊管理學術?警政資訊實務研討會，2002 年 5 月。

[57] 東海大學網路安全白皮書，http://dado.thu.edu.tw/research/p2/2/whitepaper.htm，2003 年 7 月。

[58] 行政院及所屬各機關資訊安全管理要點，http://www.dgbas.gov.tw/eyimc/switch6/law/af08.htm，2003 年 7 月。

[59] 王俊雄、林宜隆，“警政資通安全現況分析及管理政策之研究，”2002 年台灣網際網路研討會，2002 年 10 月。

[60] 行政院主計處電子處理資料中心資訊法令輯要，http://61.60.106.101/eval/law.htm，2003 年 7 月。

[61] 公務員之資訊法規須知，http://www.cga.gov.tw/行政組織/通電資訊處/資訊法規/law00.htm，2003 年 7 月。

[62] 賴淑賢，”警政資訊安全風險評估與管理－以車輛車牌失竊處理系統爲例，”中央警察大學資訊管理研究所，碩士論文，2003 年 6 月。