壹、前言

隨著網際網路的蓬勃發展，其應用層面日益擴大，使用網路的人口亦逐年增加，根據 Internet World Stats（2012）統計，全球上網人口從 2000 ～ 2012 年成長超過 500%，使用網路人數占全球總人口數約 32.7%。人們不僅在網路上進行資訊的傳輸，亦可透過網路遠距離互動，拉近了人與人之間的距離，以社群網站 Facebook 為例，人們可以透過 Facebook 認識不同國家的朋友，進行交談、分享照片及影音、遊戲互動等。根據 Internet World Stats 統計，2011 年 6 月底 Facebook 使用人數達到 7 億人次，相較於 2010 年 4 月底成長 37.2%。另一方面，網際網路亦使得電子商務成為傳統行銷以外的一個新興通路，民眾的消費型態從到有形的實體店面購買商品，轉變成為無形的遠距上網購物，以奇摩（Yahoo）網站為例，提供 24 小時的拍賣網，並且將商品加以分類，使消費者能清楚找到想要購買的商品，消費者不須出門便可購物，也可將欲出售的商品放置在網路平臺上，不須透過實體店面便可提供商品的詳細資訊，帶來另類創業的機會。再加上平板電腦及智慧型手機等行動上網設備，讓使用者可以隨時隨地上網，不侷限在固定的場所，根據財團法人資訊工業策進會（2011）（Institute for Information Industry，以下簡稱資策會）統計，2011 年第二季臺灣行動上網人數已達 2,000 萬人，相較於 2010 年第二季成長 10.3%，行動上網人數日益增加，帶動了另一波網路通訊產業的革命。近年發展的雲端技術更可將資料移轉到網路平臺上，透過雲端運算進行資料的存取、運算或線上作業的服務，使用者不須具備高效能的硬體設備，便可透過此項技術進行複雜的運算，將應用程式執行的結果透過網路交付給使用者，亦提供軟體程式開發及作業系統平臺，讓使用者只需透過網路就可進行程式撰寫執行和軟體上的應用。對企業而言，能大量降低電力、空間及資訊設備維修費用上的成本。總之，多元化的網路應用為社會大眾提供了快速且便利的服務，更為企業創造了無限商機。

雖然網路為企業與民眾提供便捷的服務及商機，但同時也引來有心人士利用網路通訊協定的漏洞進行非法行為，對網路的服務品質及安全性造成威脅。在網路安全性方面，常見的如駭客竊取商業機密、個人帳密及盜刷信用卡等，甚至植入木馬、蠕蟲等病毒影響網路安全。典型的攻擊方式有：監聽（monitoring）、密碼破解（password cracking）、漏洞（exploits）、掃描（scanning）、惡意程式碼（malicious code）及社交工程（social engineering）陷阱等，這些攻擊方式以類型區分可分為三類：偵查、入侵及破壞（張智晴、林盈達，2011）。賽門鐵克公司（Symantec, 2011）網路調查報告指出，過去 12 個月臺灣就有 67% 的公司遭

受網路攻擊，且有 96% 的公司因網路攻擊而受到損失。在網路服務品質方面，例如阻斷服務（Denial of Service, DoS）攻擊，長時間利用大量的封包來攻擊特定目標主機，使得目標主機耗盡頻寬資源以致於無法提供服務給使用者（張炫舜，2009；Lau, Rubin, Smith, & Trajkovic, 2000）。根據中華電信資安辦公室的統計，2009 年中華電信每天平均發生大約 3.7 次的分散式阻斷服務（Distributed Denial of Service, DDoS）攻擊，其中較大規模的攻擊是以每秒流量約 8 GB 進行攻擊，嚴重影響網路所提供的服務品質（引自黃彥棻，2009）。此外，突發重大的政治、社會事件或是在特定時點，例如，春節開放網路訂票、學校開放選課等，大量使用者同時間造訪網站請求服務，導致流量突然劇增，使得網路的服務品質降低；又例如麥可傑克森突然逝世，Google 搜尋服務流量突然增加，造成各地網路的延遲問題增加（ZDNET 新聞專區，2009），或賈伯斯逝世時，Twitter 推文量突然暴增，與賈伯斯相關的推文達到每秒 1 萬條（10,000 TPS），多次因流量過高導致網站停止服務（sugizo, 2011）。

為了維護網路安全與服務品質，目前已有許多機構基於不同原理開發出各種形式的安全防護機制，例如入侵偵測系統（Intrusion Detection System, IDS）（Anderson, Frivold, & Valdes, 1995; Ghosh & Sehwartzbard, 1999; Javitz & Valdes, 1994; Jonsson & Olovsson, 1997）、流量及日誌分析系統（李武耀、丁致中、廖百齡、江清泉，2003；林育生、陳宗煦、蔡輝榮、江清泉，2002；林佳毅、蕭漢威、林福仁，2000；林奕廷等，2001；Caberera, Ravichandran, & Mehra, 2000; Ledoux, 1997）、網路防火牆系統（Cisco System, Inc., 2000; Hari, Suri, & Parulkar, 2000; Hazelhurst, Attar, & Sinnappan, 2000）等，可用來監控網路流量與資訊安全，並可結合網路頻寬管理機制（Bjurling, Rasmusson, & Johansson, 2008; Suri et al., 2006），分配網路頻寬與排定各種服務的優先權。其中 IDS 具備較全面性的防護機制，能夠準確地偵測網路駭客攻擊事件，如偵測通訊埠掃瞄攻擊、緩衝區溢位攻擊、阻斷服務攻擊、蠕蟲攻擊、TCP 堆疊掃描、作業系統弱點攻擊等。就偵測模式而言，IDS 大致可區分成誤用偵測系統（Misuse Detection System）及異常偵測系統（Anomaly Detection System）兩大類型。

一、誤用偵測系統

誤用偵測系統類似於防毒軟體，主要是蒐集過去已知的入侵及攻擊行為，建立入侵特徵資料庫（Signature），再將蒐集的網路封包特徵值與入侵模式進行比對，若與入侵特徵相符即判定為攻擊行為，此種方式雖然能有效地偵測及防禦攻