# 資料挖掘在入侵偵測上的應用

研究生：張兆祥　　指導教授：蔡介元教授

元智大學 工業工程與管理研究所

## 摘要

資訊科技的迅速發展及網際網路與電子商務的盛行，無疑為人與人之間的溝通帶來極大的方便。正當大眾對這些先進的資訊技術愈加依賴時，網際網路的安全問題亦隨之產生，此種現象特別在商業社會受到重視，倘若忽視則可能造成企業無法估計的損失與公眾形象的破壞。

入侵偵測系統是近年來相當風行的資訊安全保護機制，具有即時性的系統安全偵測與回報功能，用來偵查異常的入侵行為與監控網路環境安全，回報內部與外部的滲透者所產生非經允許的使用、誤用與濫用等可能傷害電腦系統的行為。以目前IDS的監測技術，做為預防駭客入侵及病毒的預警，是一個相當不錯的選擇，但IDS所產生的記錄巨細靡遺，一般人員很難能順利閱讀與瞭解，就連有專業背景的網路系統專家，對於大量的記錄亦無法即時判別。

一般而言，駭客對於選中的目標都預先備有數個攻擊範本，憑這些攻擊範本來嘗試不同的勘察及攻擊，直到攻擊成功或範本用盡為止；由於駭客攻擊時會觸發一到多個不同網路服務型式中的各種警示，而這些攻擊模式的組合在一般正常的網路通訊行為中卻是相當少見的。因此本研究利用入侵偵測系統能有效產生記錄的功能，依據目前已知的入侵手法及病毒特徵，將攻擊的來源、種類、時間、次數等加以歸納分析，並利用資料挖掘的技術，發展出一個自動警示機制，將可疑的攻擊事件從IDS警示事件中過濾出來，讓真正有問題的警示事件及其攻擊模式，能明顯地被發現，發揮入侵偵測系統的最大效能。

關鍵詞：入侵偵測　資料挖掘　駭客　網路攻擊