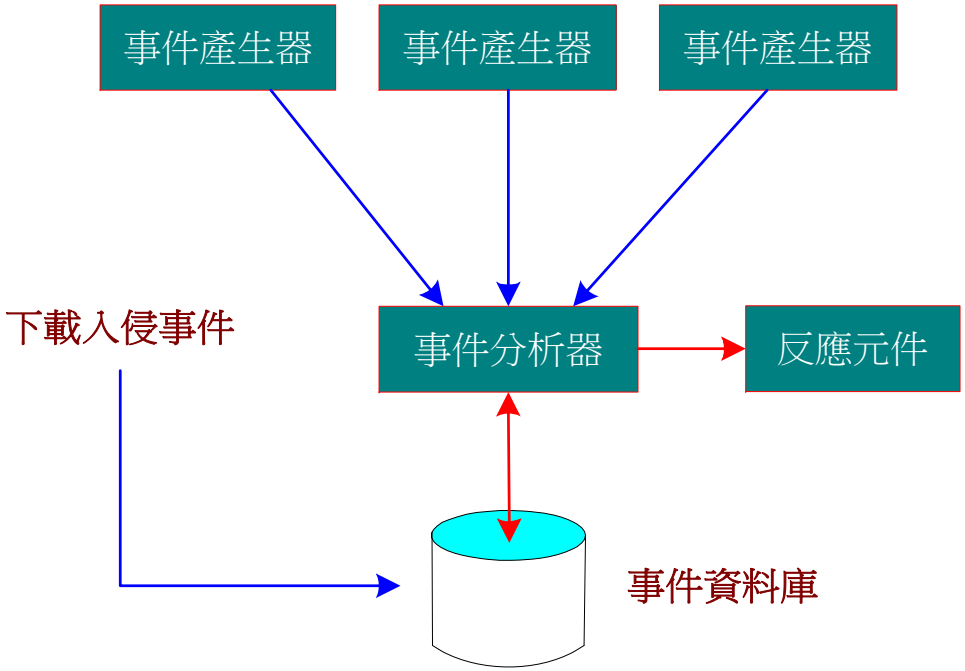
入侵偵測技術－資料引擎

- 資料引擎 (Data Engine) – 事件分析器
  - 專家系統 (Export System)
  - 有限狀態機 (Finite State Machine)
  - 統計分析 (Statistical Measure)
  - 類神經網路 (Neural Network)
  - 資料探勘 (Data Mining)



入侵偵測技術 –判斷依據

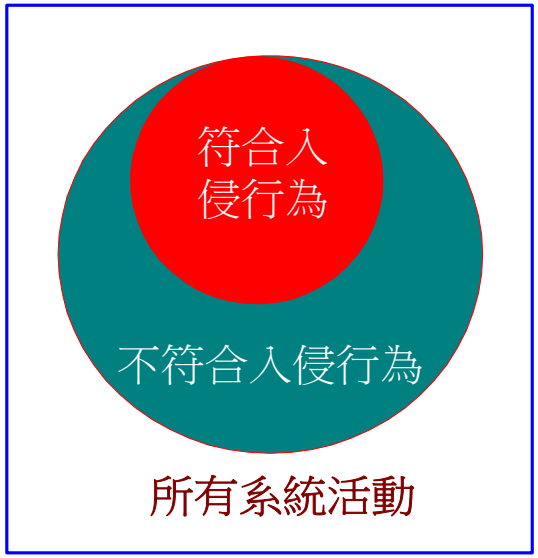
- **誤用偵測：(從寬 – allow)**

  假設所有都是不符合入侵行為，再找出符合入侵行為

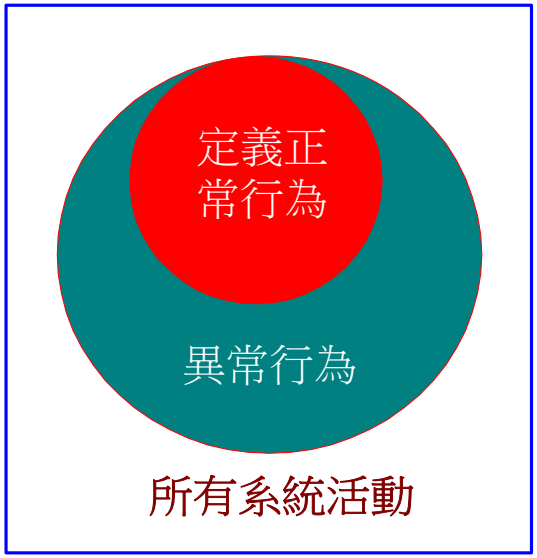
- **異常偵測：(從嚴 – deny)**

  假設所有都是異常行為，再找出正常行為

(a) 誤用偵測技術



(b) 異常偵測技術



入侵偵測技術 –判斷依據

- 正常與非正常活動