**2019/11/18 上午主題： 智能理財應用**

**(主講者：金融研訓院特約講座 尹相志)**

1. 關於「智能」的議題，老師首先特別說明「機器思考」是不可能發生，其只能透過以大量數據、訓練、建模來產生，亦即機器是沒有教過的就不會，因此只能解決有明確答案之問題(明確的input、明確的output)，並且也不會瞭解問題之本質，故認為「人機合作」才是最重要的。
2. 再來針對「什麼才算是智能理財」來進行引言，即以「智能的方式來理解客戶需求、智能的方式來進行投資、智能的方式來回應客戶」，再提出以「推薦算法」之思路來解釋如何提供智能理財，並探討新科技如何進行智能投資數據分析，以作為金融機構抓住客戶的契機，顯示同行間之差異性。另因目前金融機構於智能的應用上均大同小異且市場也飽和，故提出「客戶長尾化(80-20法則)」來抓住長尾後端量不大，但累積起來也是具可觀之族群。
3. 提供推薦算法思路 (商品推薦→用戶推薦→表徵推薦)
   1. 過去都是基於「商品的推薦」(如關聯式規則：尿布啤酒案例)，但其存在缺點：
      1. 對客戶背景資訊不瞭解
      2. 對快銷品或剛上市商品無法套用(因缺乏歷史資料來推測)
      3. 每一規則就要建一個模型，不同規則間無法適用(每建模一次，即須重新準備資料、變數清理、變數選擇轉換，故耗費人力與成本)
   2. 若改以「用戶的推薦」(矩陣分解技術matrix factorization techniques)，即以分類分群找出相似客戶的行為模式，如從會欠款的人，來看「通話行為、網路流量、APP的使用量、使用的手機品牌等」，據以判斷是否存在相同模式，將可用來建立萬用模型，故每次只要改變y變項即可，不須重新蒐集資料、變數篩選清理與轉換。再加上藉由AI深度學習技術，可再演進為基於「表徵的推薦」，即由機器去找出特徵向量及規則(生成式對抗模型Generative adversarial network )。
4. 針對智能方式來回應客戶最為人瞭解的是國外很紅的「聊天機器人」，但其實此技術離成熟還有點距離，特別是針對中文來說卻是一項嚴苛的挑戰，理由在於：
   1. 漢字數太多：中日韓統一表意文字有20,928個。
   2. 需依賴上下文來判斷語義
   3. 排列組合產生無限意義，無法以窮舉來表示

因此對中文來說，需從自然語言處理(NLP)轉變為自然語言理解(Nature Language Understanding)，使機器轉為理解「意圖識別」，藉以學習「語意類比」的相關性，如提供同類別的參考詞彙(美金、英鎊)，機器可判斷與之相同的類別詞(包括：美元、歐元、日圓、人民幣等)。然而若只是單純的回覆標準Q&A並不算是智能，將可進一步地提供中文視覺閱讀智慧問答，如提供一篇新聞對組織的描述或股價圖，機器藉以圖形向量特徵來判斷其股價漲幅。

1. 最後老師說明外界將人工智慧解讀為將取代人類，但實則不全然，需以持平的角度來看待，因人工智慧(至少在目前的技術上)仍不能取代人類，其價值發揮在於如何將人類從繁瑣無聊的作業中釋放出來。

**2019/11/18 下午主題：資安危機處理與因應**

**(主講者：勤業眾信聯合會計師事務所企業風險管理部副理 陳威棋)**

此主題主要探討於數位環境與新興科技環繞下，資安的風險與所面臨的問題，包括：網路攻擊、資料竊盜、關鍵資訊基礎設施崩壞、物聯網資安事件等，並說明駭客組織已經形成更有組織、熟悉產業且專業分工的犯罪集團。因此，傳統資安在數位科技浪潮下面臨以下挑戰：

* 1. 安全問題**不可見**：企業往往是“被告知”而非主動發現資安弱點
  2. 安全問題**不可控**：傳統資安設備或產品面對駭客起不了作用
  3. 安全問題**不可管**：社交工程、網路釣魚等由使用者發起的行為越來越難控制

而面對以上挑戰，現今全球各地除相繼進行區域聯盟，透過情資分享合作來降低威脅程度外，並且藉由資安事件應變之演練，用以提升資安防禦與整體應變能力，最終強化資安韌性。