

# 大數據與AI

銘傳大學人工智慧應用學系

鍾健雄 博士

# 個人資訊



## 學歷

- 美國維吉尼亞大學系統暨資訊工程博士



## 研究與教學

- 機器學習、資料探勘、模式與模擬、資訊安全
- 程式開發、遊戲程式、資料工程、企業架構分析



## 聯絡

- Email: [jc7qxccit@gmail.com](mailto:jc7qxccit@gmail.com)
- Cell: 0919341293
- LineID: jc7qx

# 參與專案

- 縱火犯罪調查與防制資料庫建置計畫，中央警察大學，2010-2011
- 關鍵基礎設施安全防護資訊共享平台系統架構分析與建構之研究，科技部，2016-2018
- 以巨量資料分析觀點探討毒品施用者及暴力犯罪再犯因子及預測之應用，法務部，2017
- 強化核能電廠資通安全與管制研究，原能會，2016-2021
- 智慧交通與運輸資訊安全技術與防範策略研究，財團法人國家實驗研究院，2022
- 開發建置受保護管束人再犯風險評估智慧輔助系統-以巨量資料分析觀點探勘犯罪風險因子與保護管束再犯之關聯性，法務部，2021-2023
- 有無繼續施用毒品傾向評估標準信度及效度評估與實證計畫，衛福部，2024



# 簡報大綱



人工智慧簡介 Artificial Intelligence

機器學習 Machine Learning

人工智慧生成內容 AIGC

預測模型 Predictive Modeling

演算法治理趨勢 Algorithmic governmentality

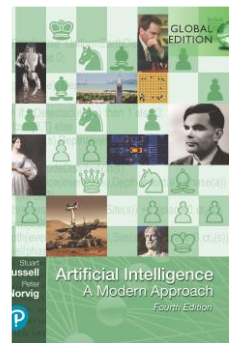
# 人工智能(AI)簡介

# 何謂人工智慧?



艾倫、圖靈，約翰、麥卡錫

- 機器能展現類似人類的智慧行為的能力



司徒爾特、羅素，彼得、若維格

- 創建智慧型機器（智慧電腦程式）的科學與工程



馬文、明斯基

- 使機器做「人類需要智慧才能完成的事情」的科學



吳恩達

- 創建能夠推理、學習、和自主行動智慧代理的電腦科學和工程

# 人工智慧技術分類—能力



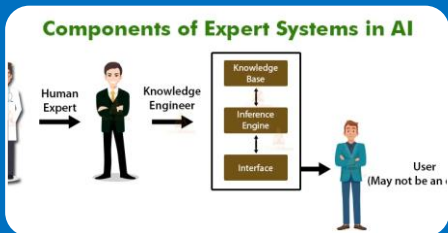
## 弱人工智慧

- 特定型人工智慧，專注於解決某特定問題，現今所看到的人工智慧系統都屬於若人工智慧



## 強人工智慧

- 通用型人工智慧，可以解決任何問題，具有人類同等的學習能力和思考能力，真正擁有人類智慧，目前沒有任何一個人工智慧系統達到強人工智慧境界



## 專家系統

- 透過蒐集專家知識，儲存於電腦中，使電腦能夠模擬專家的決策過程，如醫療診斷、金融決策

# 人工智慧技術分類—應用

- 預測式人工智慧

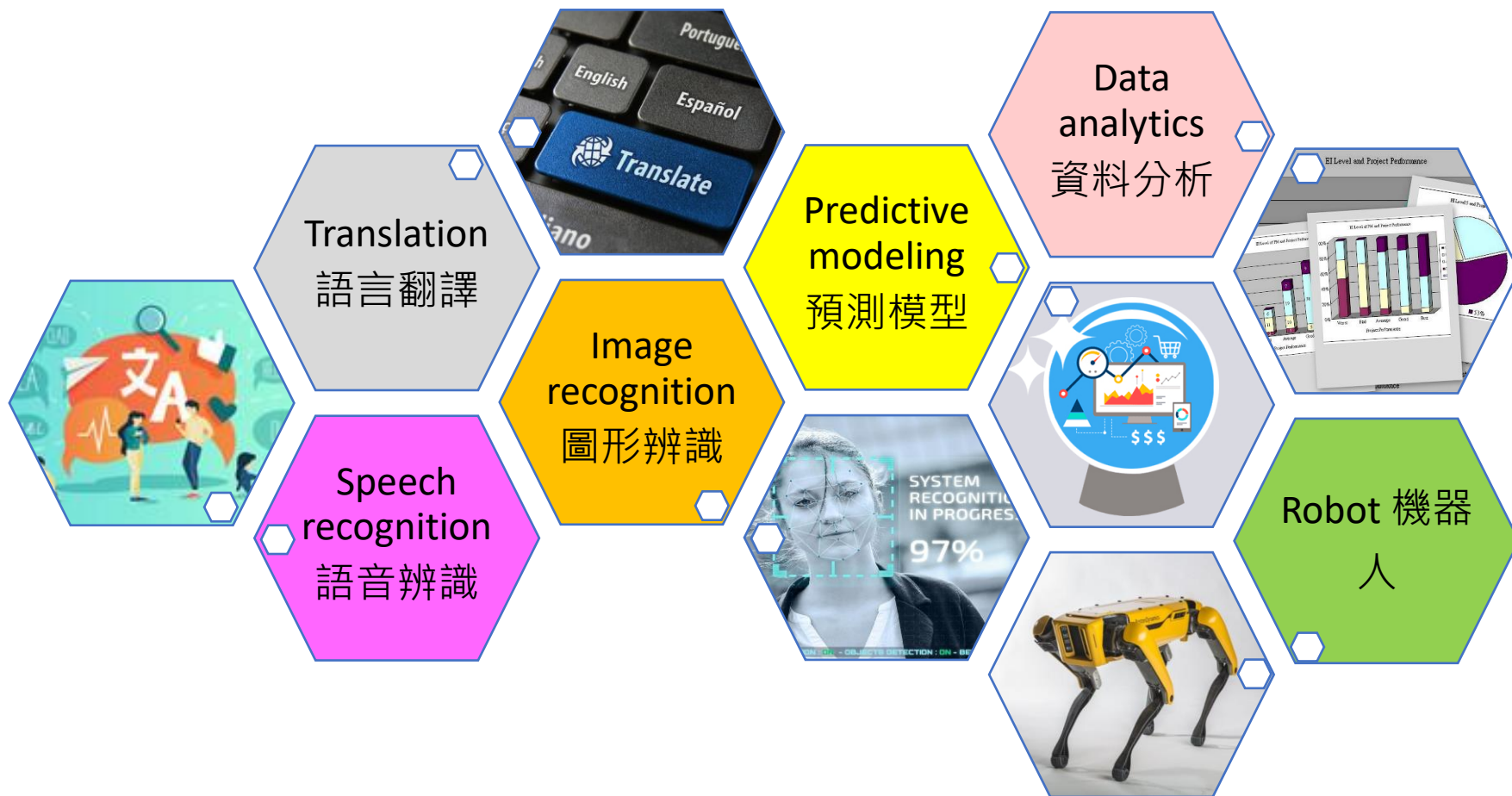
- 機器根據一組數據，找出模式，用於輔助決策，例如根據犯罪者歷史紀錄預測是否再犯。機器在這些任務中變得越來越聰明，技術已大量進入商用領域。

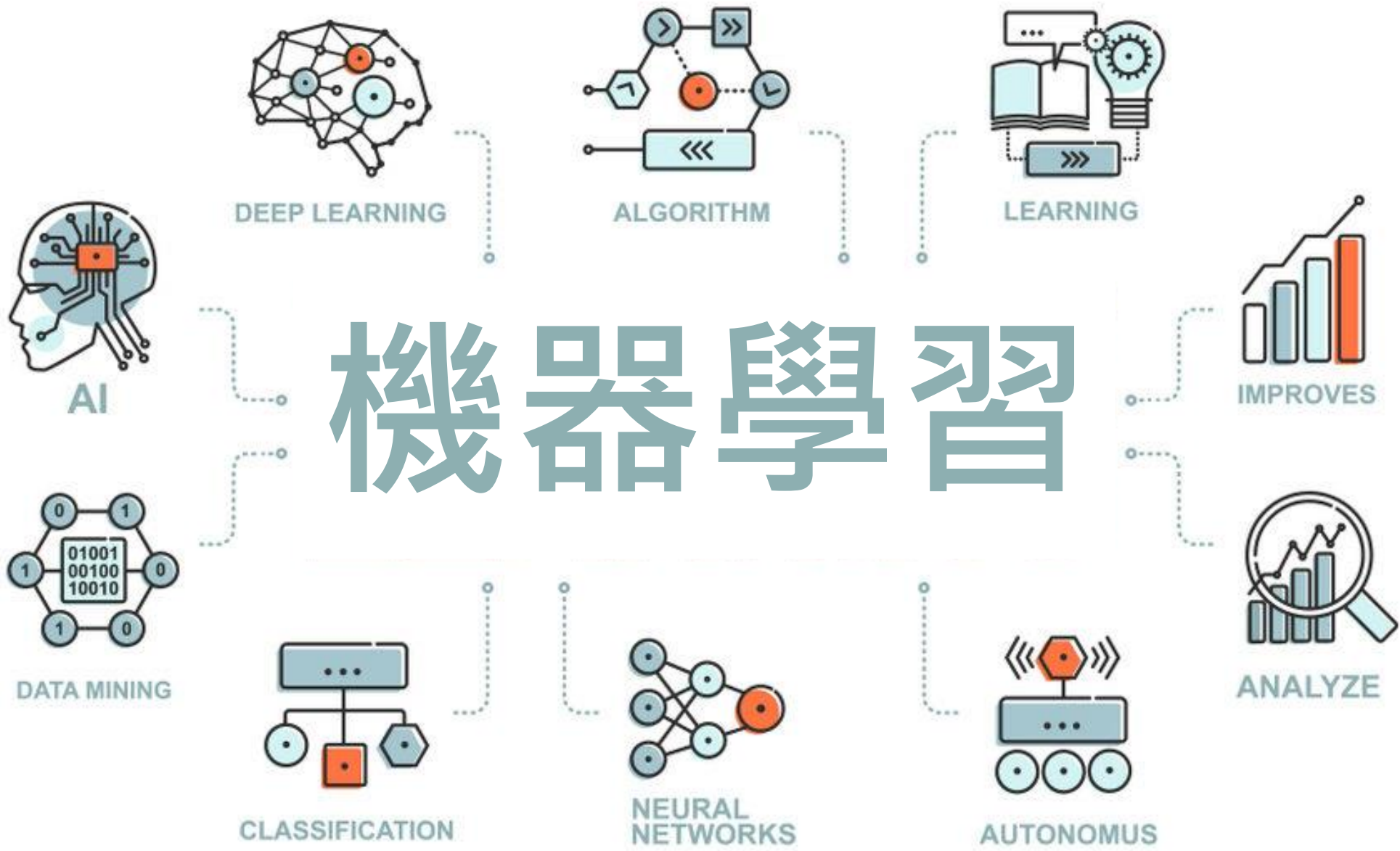
- 生成式人工智慧

- 機器已經可以根據已有的資料產生出新的結果，例如產出文件及產生新的藝術畫作，新的影片，此種技術稱為「生成式AI」



# 人工智慧的應用領域

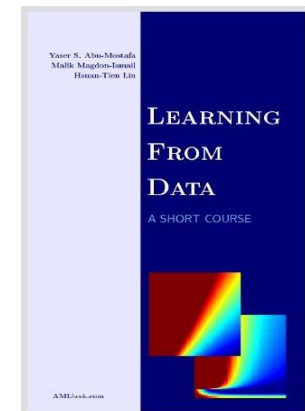


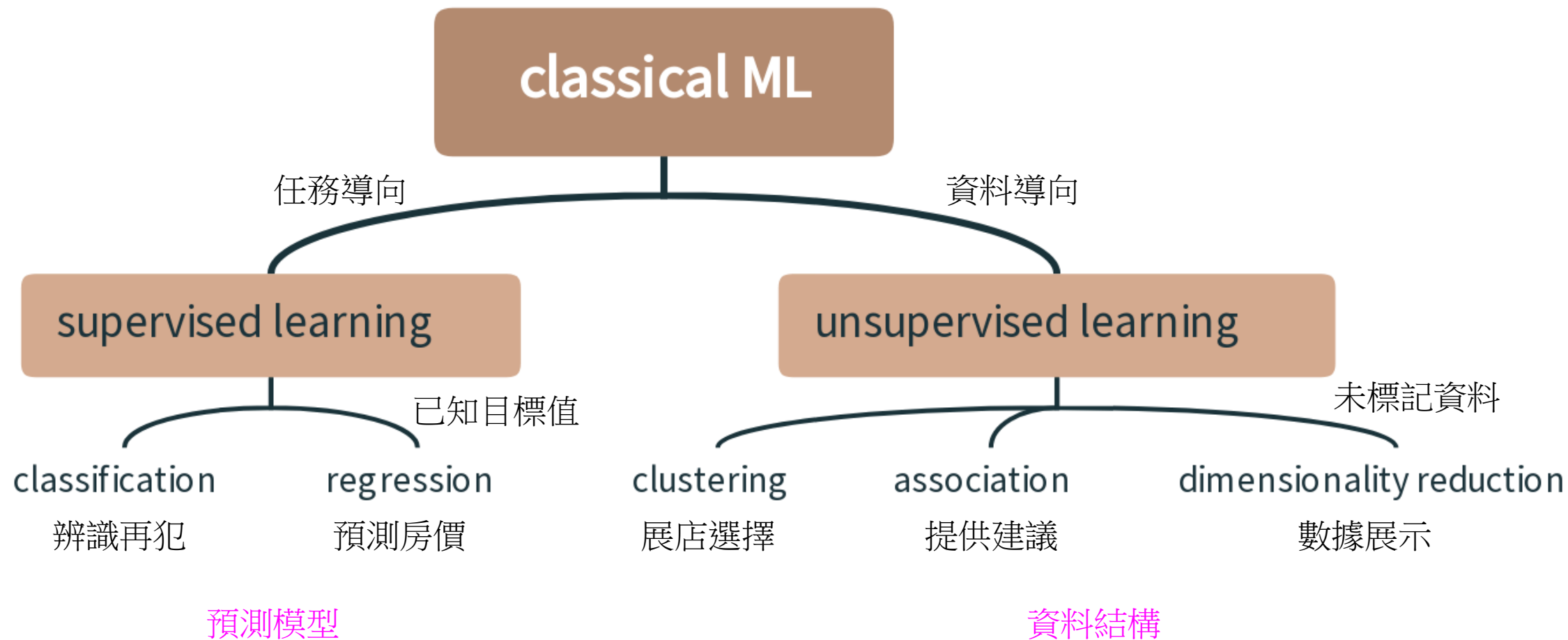


# 機器學習(ML)

- 用於電腦運作解釋及表示人類知識(Knowledge)
- 從案例或觀察資料中自動地學習有意義的關係與模式
- 創建分析模型產生預測、規則、答案、及建議...以實現AI應用
- 重覆地經由問題相關的訓練資料學習，找出隱藏的複雜規則，適用於解決如分類、回歸、或分群...等應用問題
- 成功地應用於詐欺偵測、信用卡額度、語音及影像辨識、或自然語言處理(NLP)等領域

Machine learning allows computational systems to adaptively improve their performance with experience accumulated from the observed data.

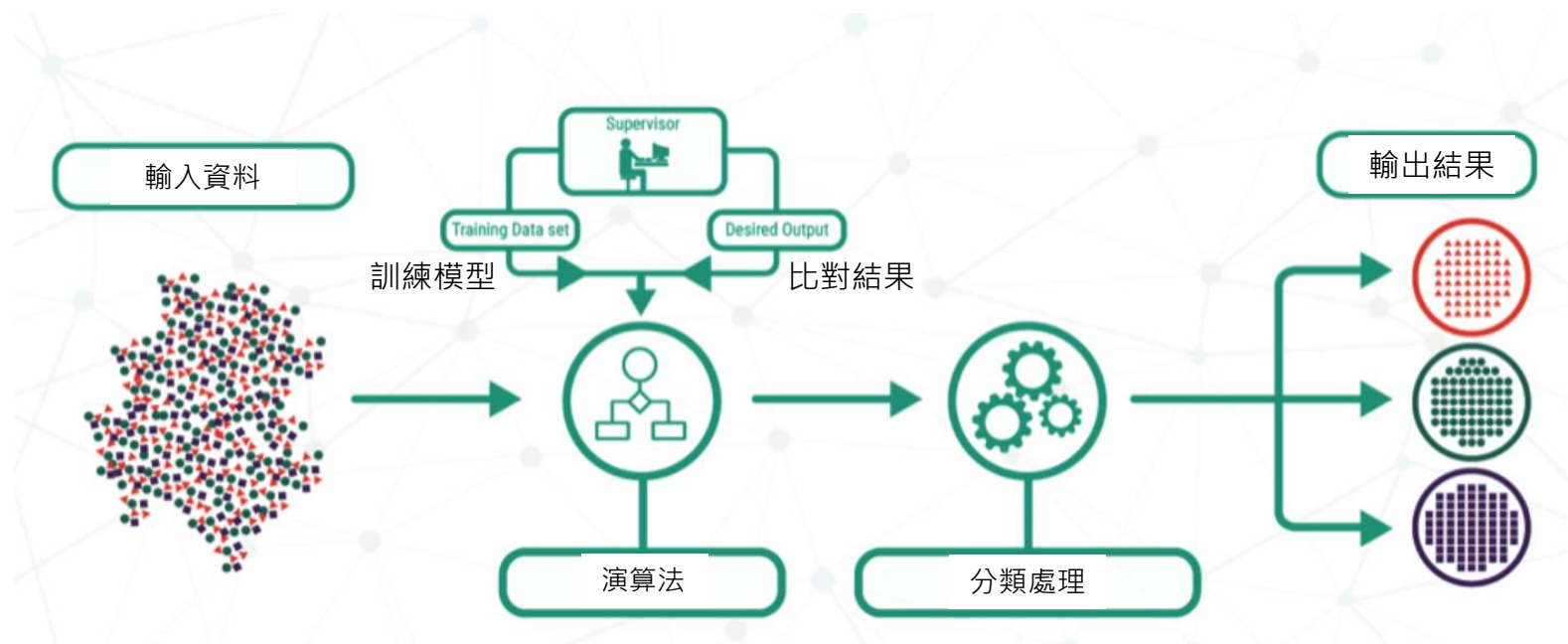






- 監督式學習 (Supervised Learning)

- 監督式學習需要輸入資料及確定的輸出資料，找出輸入/輸出轉換函數(演算法)
- 資料必須提供輸出目標值，可能是數值或是分類類別，如根據犯罪人的特性、監所表現、刑案紀錄，預測是否再犯？



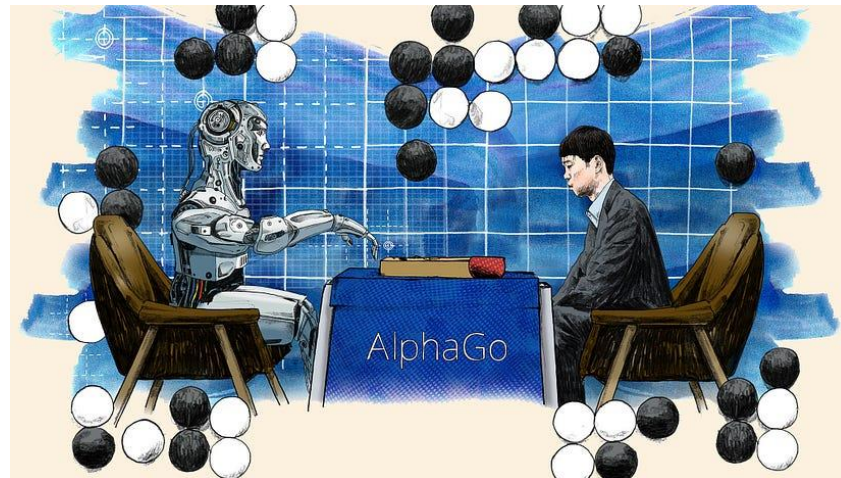
- 非監督式學習 (Unsupervised Learning)

- 非監督式學習根據輸入資料觀察個案的特徵向量值，不需要輸出結果，找出特定的資訊結構，如針對個案資料是否可以產生分群現象(clustering)
- 分群演算法根據每一個資料個案特徵的相似性 (Similarity)，找出資料的結構特性。
- 在犯罪學領域，可以根據犯罪者的犯罪地點建立犯罪製圖，找出犯罪熱區，即為非監督式學習的應用之一



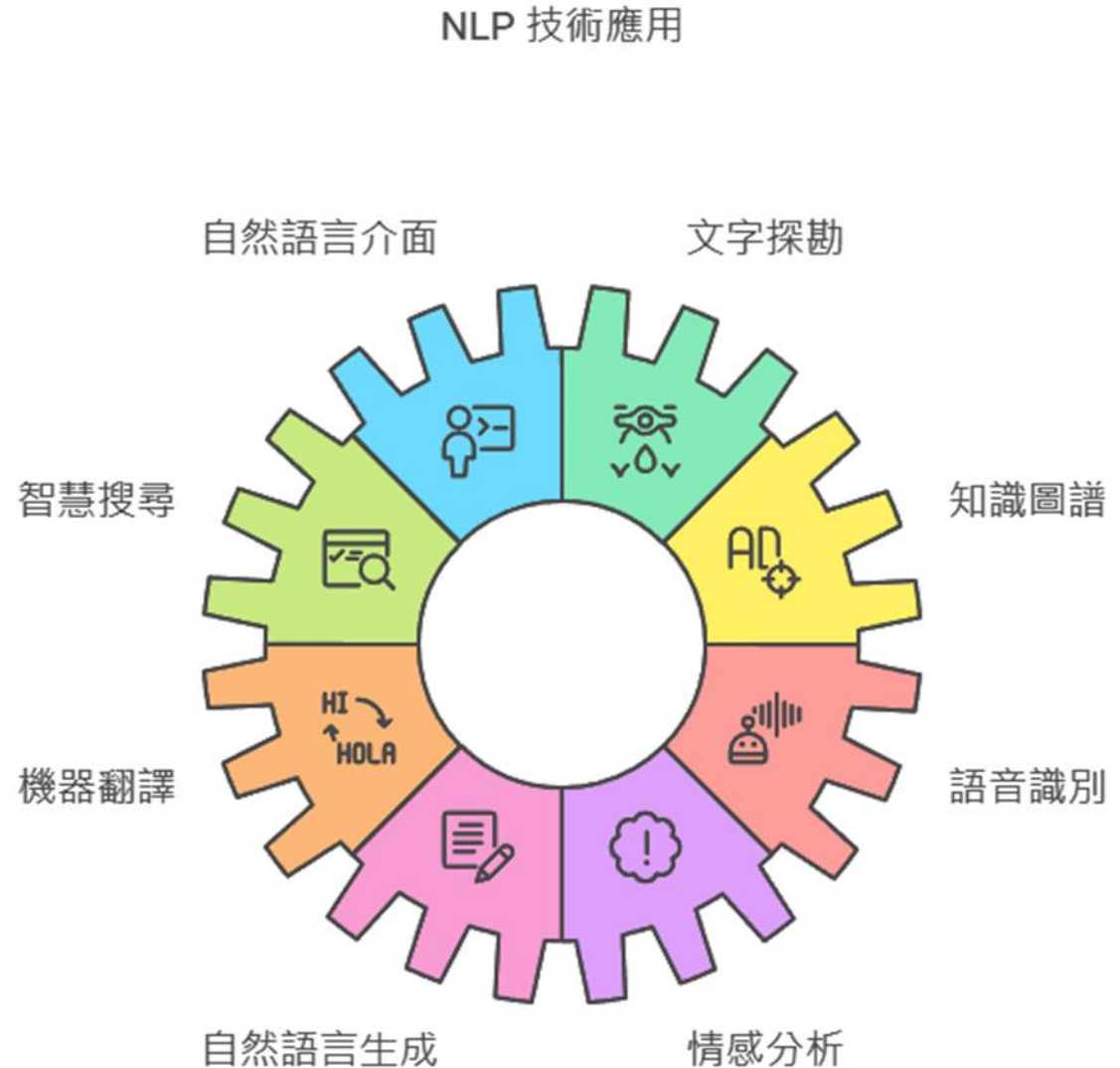
- 增強式學習 (Reinforcement Learning)

- 增強學習的目標是讓機器自己學習。人類學習的過程中正確的學習步驟產生好的結果(reward)，否則將受到懲罰(punishment)，因此RL利用嘗試錯誤(trial and error)的方式來學習建立一個策略在每一步行動過程根據策略，避開不好的方向，趨向更好的方向。
- 增強學習(RL)不僅能夠學習輸入與輸出關聯性，可依據環境中的狀態和給定狀態下採取可能的行動
- AlphaGo一種人工智慧的下棋系統，利用增強學習支持棋弈決策，是目前RL是成功的應用之一



# 人工智慧技術—自然語言處理(NLP)

- 自然語言理解
  - 透過分析語法、語意、情感和其他資訊來讓電腦能夠理解人類自然語言的意義
- 自然語言生成
  - 透過分析數據、撰寫報告、或生成回應的方式，讓電腦能夠使用人類自然語言生成文本





# ChatGPT: Optimizing Language Models for Dialogue

We've trained a model called ChatGPT which interacts in a conversational way. The dialogue format makes it possible for ChatGPT to answer followup questions, admit its mistakes, challenge incorrect premises, and reject inappropriate requests. ChatGPT is a sibling model to [InstructGPT](#), which is trained to follow an instruction in a prompt and provide a detailed response.

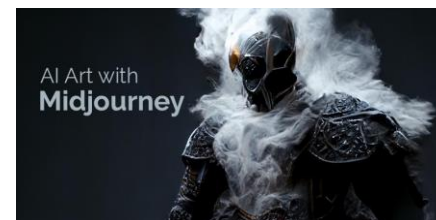
[TRY CHATGPT ↗](#)

讓機器學習模型研究歷史資料，運用深度學習技術，創造出一個全新生成的成品(文字、圖像、音訊、音樂、影片、程式碼、各種設計、行銷素材、3D模型等)

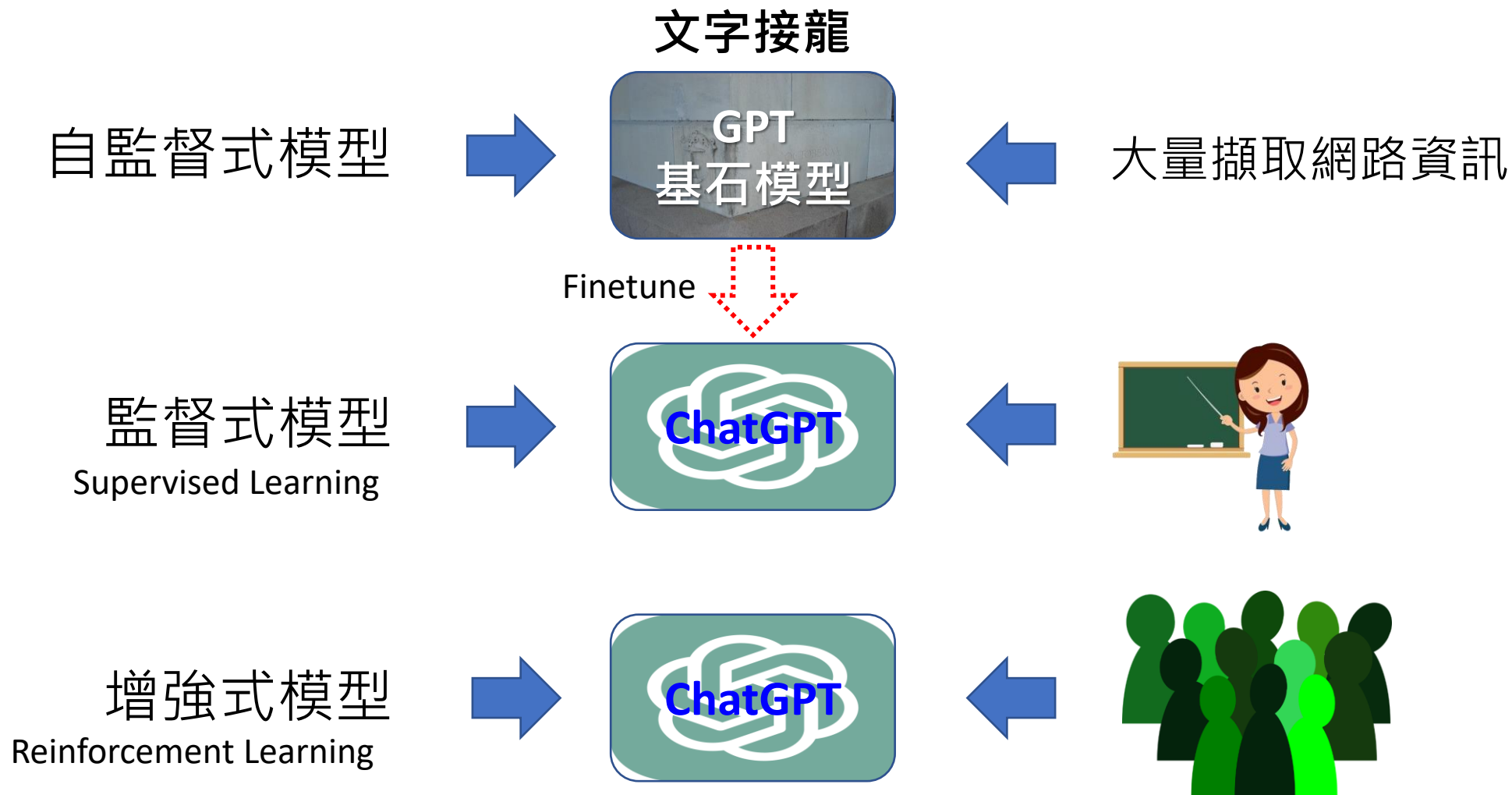
## 人工智慧生成內容 Artificial Intelligence Generated Content

# 生成式AI ( Generative Artificial Intelligence )

- 生成式AI是一種**機器學習模型**，其目標是**創造新的數據**，而不僅是基於現有數據做出預測。
- 生成式AI系統對**大量的訓練資料**學習，利用這些資料生成與訓練資料類似的新的內容。因此可以創造出新的圖像、文本、音頻等內容。
- 生成式AI系統的核心為**深度神經網路模型**，在自然語言處理、圖像生成、音訊合成、文字摘要等領域有重要的進展
- 生成式AI模型如 OpenAI 的 ChatGPT 是一種生成式AI產品，GPT 代表 **Generative Pre-trained Transformer** 模型



# ChatGPT誕生





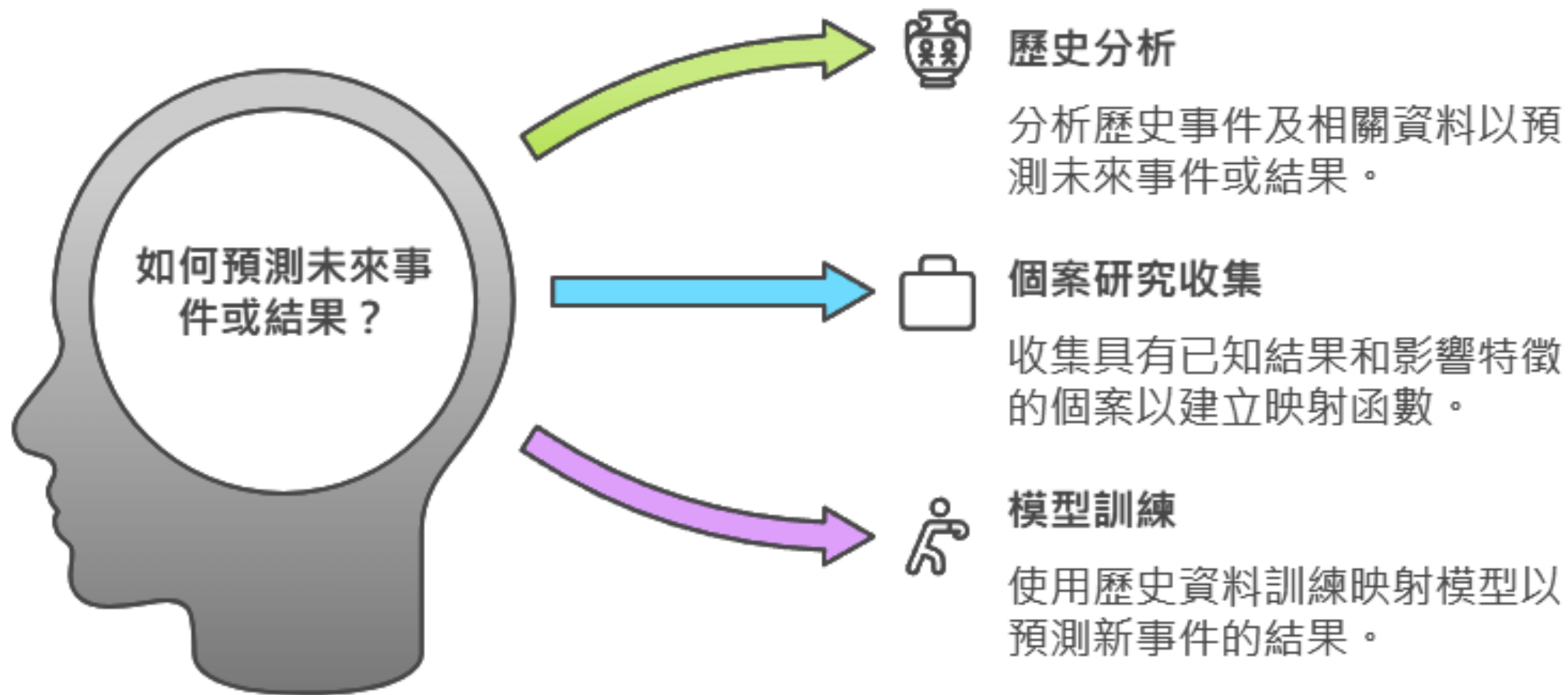
# 預測模型

Predictive modeling





# 預測建模 (predictive modeling)



# 預測問題分類

## 分類 Classification

- 根據歷史資料執行歸類分析(categorical analysis)

## 分群 Clustering

- 基於蒐集資料，依據資料特性進行分群

## 異常偵測 Outliers detection

- 基於蒐集資料，辨識異常資料

## 預測 Forecast

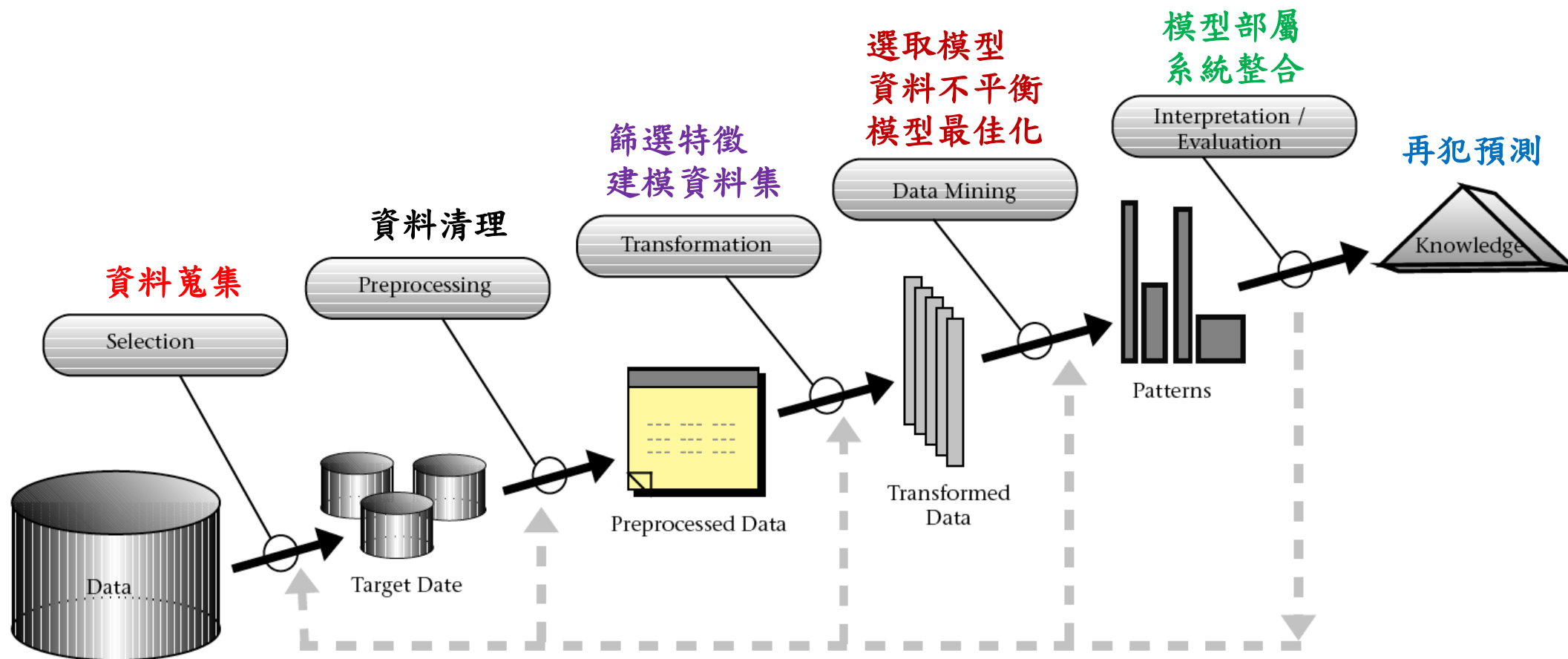
- 根據歷史資料執行結果預測

## 時間序列 Time Series

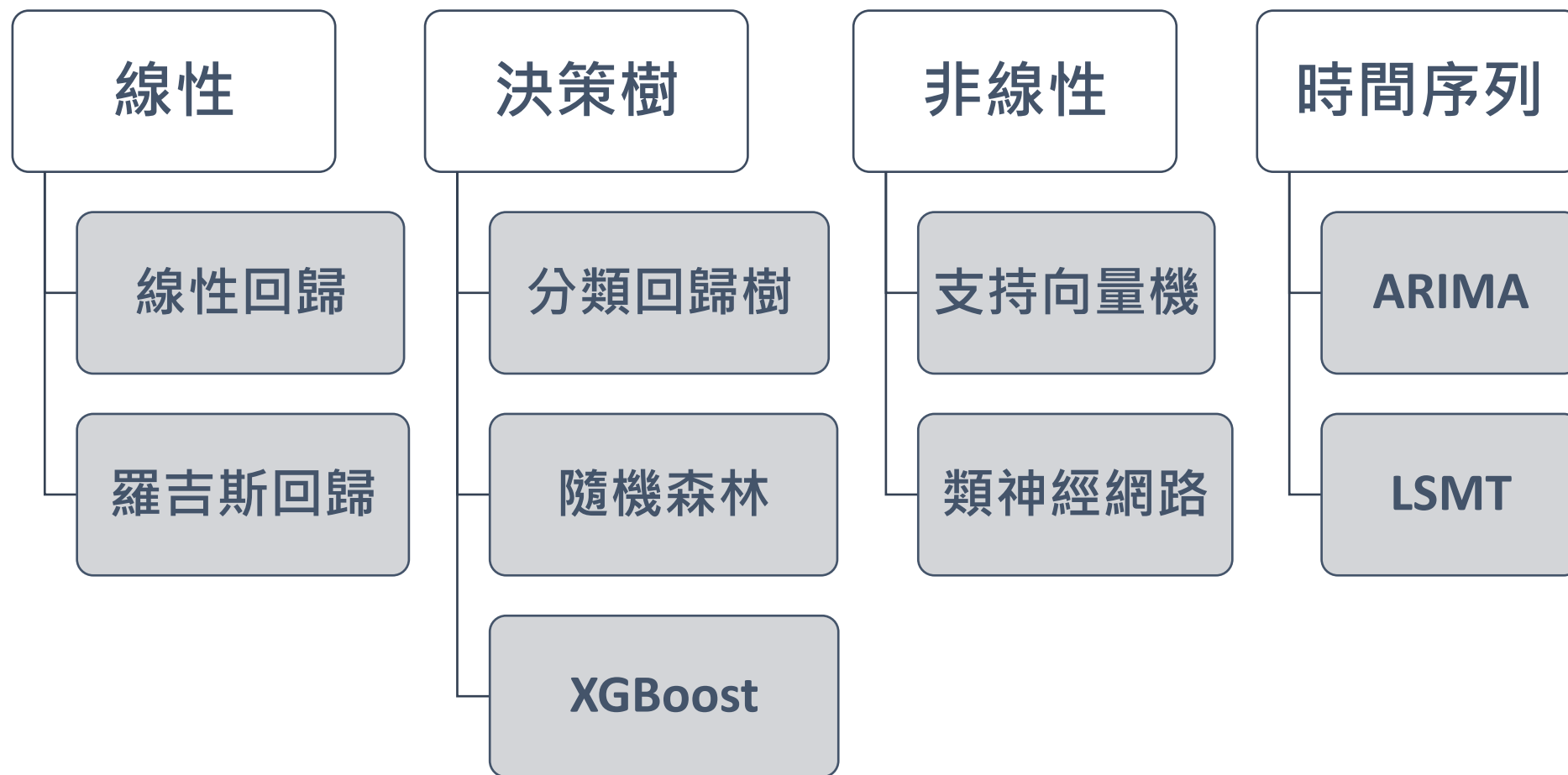
- 資料具時間標籤可以用來預測趨勢或熱時分析

# 預測建模流程

- 從巨量資料中萃取出知識



# 預測模型技術





# 資料蒐集與分析

- 資料蒐集

- 資料蒐集必須深入問題領域、瞭解決策過程、觀察作業流程
- 探尋可靠資料源及分析資料庫結構

- 資料分析

- 針對蒐集的原始資料必須執行**資料清理**，包括遺失值、不同檔案格式、離群值、錯誤值等處理
- **資料探索**是對資料瞭解的重要步驟，可利用統計參數及圖表展現來剖析資料
- 應用蒐集資料於預測模型必須經過**資料轉換**以符合模型運作使用，如資訊編碼、資料正規化...

# 建模與評估

## 特徵因子選取

- 根據問題專業知識選取影響因子組成特徵向量作為預測模型輸入，適當特徵因子提昇模型預測準確度，選取最小特徵因子空間可降低模型維度改進模型執行效率

## 決定適當模型

- 依據問題分類與特性決定適當模型，模型技術分為線性、非線性、決策樹、與集成式模型

## 訓練模型

- 蒐集原始資料分為訓練與驗證資料集，訓練資料集，包括特徵輸入向量與結果，供模型訓練以獲得模型結構參數，驗證資料集供評估模型效能

## 模型驗證評估

- 驗證資料集提供特徵輸入向量使預測模型產生預測結果，再經由比對預測結果與實際結果，調校模型，產生模型效能評量指標

# 模型評估指標

## 混淆矩陣 Confusion Matrix

		Real Situation	
		Positive	Negative
prediction	Positive	<b>TP</b>	<b>FN</b>
	Negative	<b>FP</b>	<b>TN</b>

TP：預測為陽性(p)，預測正確(T)。

TN：預測為陰性(n)，預測正確(T)。

FP：預測為陽性(p)，預測錯誤(F)。

FN：預測為陰性(n)，預測錯誤(F)。

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Accuracy: 準確率

$$Precision = \frac{TP}{TP + FP}$$

Precision: 精確率

$$Recall = \frac{TP}{TP + FN}$$

Recall: 召回率

$$F1 = \frac{2TP}{2TP + FP + FN}$$

**ROC-AUC** 在ROC曲線下的面積

X軸為False Positive Rate (FPR)，

Y軸為True Positive Rate (TPR)

# 模型參數最佳化

- 超參數調校(Hyperparameter tuning)設定模型參數使其獲得最佳效能
- 超參數調校必須於模型訓練前設定完成
- 模型參數最佳設定是針對不同的參數組合建立模型並評估效能
- 僅針對訓練資料評估模型將造成過度擬合(overfitting)問題，超參數調校採用交叉驗證(cross validation)方法解決
- 隨機搜尋(random search)與網格搜尋(grid search)技術配合交叉驗證(CV)找出最佳參數組合

## 隨機森林模型超參數組合

```
{'bootstrap': True,  
 'criterion': 'mse',  
 'max_depth': None,  
 'max_features': 'auto',  
 'max_leaf_nodes': None,  
 'min_impurity_decrease': 0.0,  
 'min_impurity_split': None,  
 'min_samples_leaf': 1,  
 'min_samples_split': 2,  
 'min_weight_fraction_leaf': 0.0,  
 'n_estimators': 10,  
 'n_jobs': 1,  
 'oob_score': False,  
 'random_state': 42,  
 'verbose': 0,  
 'warm_start': False}
```



# 演算法治理 Algorithmic governmentality





# 演算法治理應用

- 結合大數據、演算法、機器學習技術已成為國防、安全、反恐、打擊犯罪、及情蒐等領域的重點主題
- 情治單位於網際網路、社群媒體、通訊信息...蒐集、過濾、分析情資
- 警政執法機構建立犯罪預測工具，如PredPol(加州)、HunchLab(費城)、Precobs(慕尼黑)、Maprevelation(法國)
- 法院預審預測系統(Public Safety Assessment, PSA)及緩刑假釋評估系統(費城假釋犯二年再犯評估工具)

# 預測再犯風險-費城隨機森林工具

- 美國賓州大學犯罪學系與費城「成人假釋與緩刑」部門（**APPD**）合作籌建電腦化預測程式評估假釋犯回到社會後2年內再犯的可能性
- 成功地運用於評估假釋犯再犯的可能性，已有4年實際運作經驗
- 美國費城當新的假釋個案成立時利用該工具區分假釋犯高、中、低風險類別
- 該研究中所使用的預測技術為「隨機森林」

*Predicting Recidivism Risk: New Tool in Philadelphia Shows Great Promise*



中華民國

法務部

Ministry Of Justice



中華民國

中央警察大學

Central Police University

# 以巨量資料分析觀點探勘犯罪風險因子與保護管束再犯之關聯性

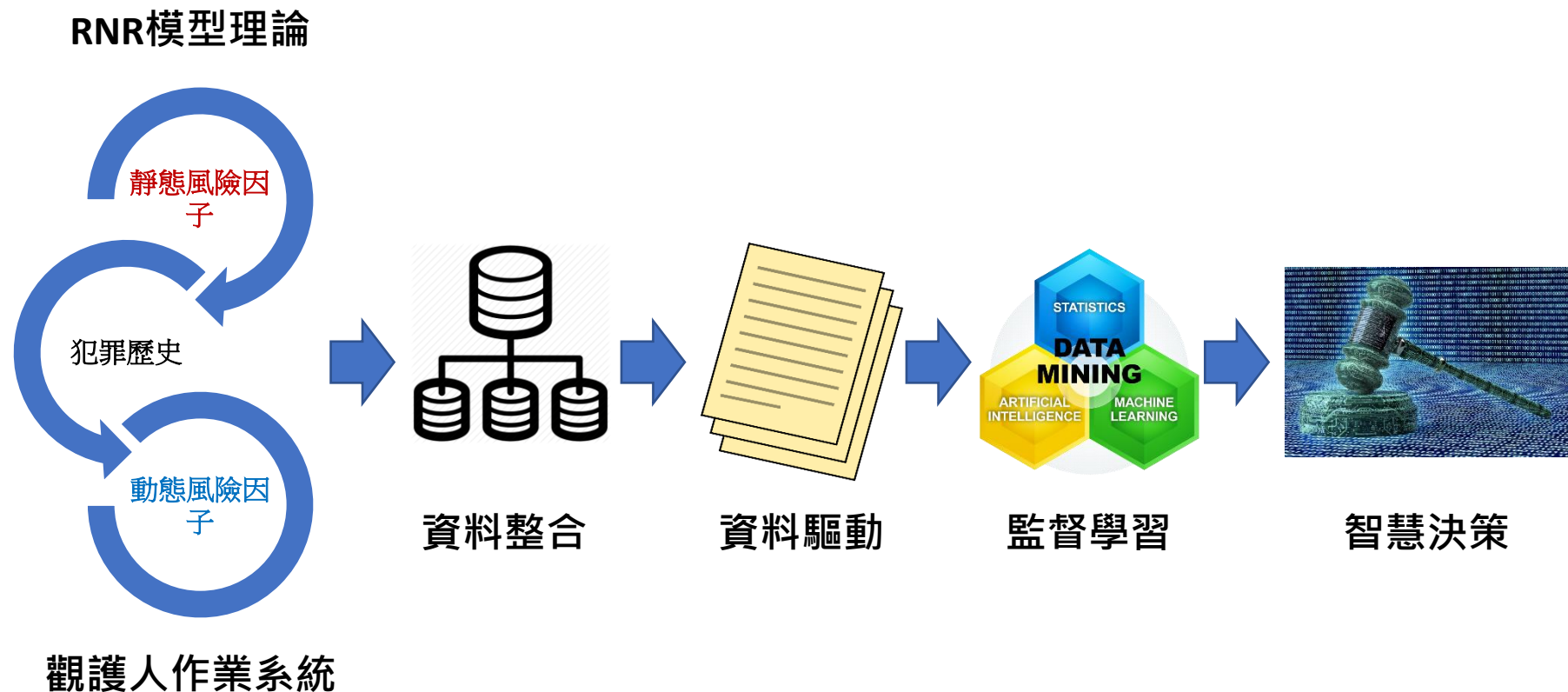
## 委託研究案

# 機器學習應用於再犯預測

- 犯罪再犯(criminal recidivism)之預測與探討的歷史可以追溯到90年前。再犯風險評估工具(risk-assessment tools)在最近二十年來，也已廣泛的使用於刑事司法系統。
- 由於電腦運算力及連結力提升，機器學習(Machine Learning)與大數據分析(Big Data Analytics)方法得以精進實現，成功地應用於各種領域，其中包括犯罪再犯之預測。
- 利用機器學習方法進行犯罪再犯預測的研究受到重視，本研究蒐集整理國內外相關論文，並作為建立再犯風險預測模型參考。



# 機器學習與再犯風險評估

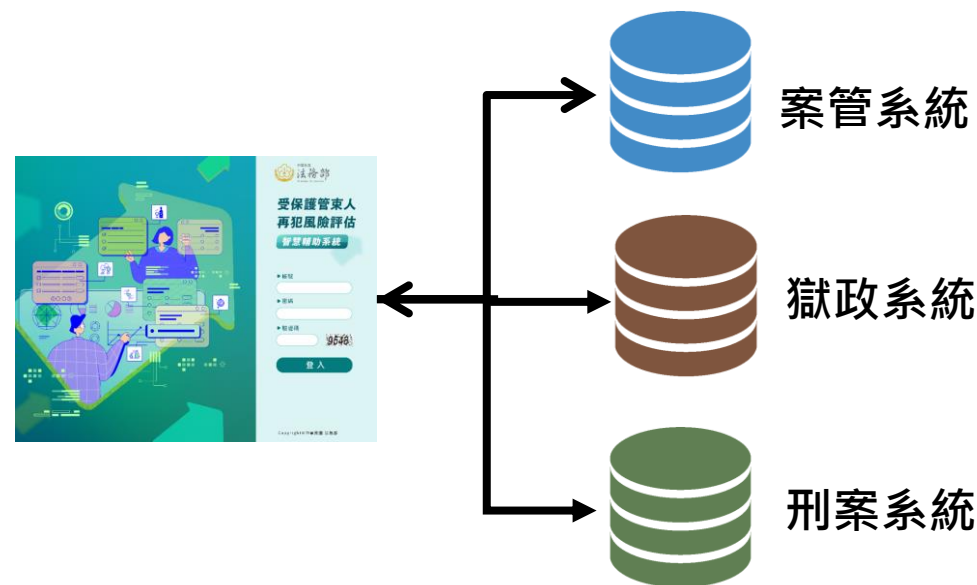


# 作業情境



# 資料蒐集

- 蒐集與分析觀護人案管作業子系統、獄政管理資訊系統、刑案資訊整合系統等電子資料
- 蒐集全省22地檢署保護管束個案資料，包括性暴力犯罪、毒品犯罪、暴力犯罪、財產犯罪、詐欺犯罪、酒駕犯罪、公共危險罪等七類
- 依與觀護人訪談結果及參考國外文獻考量之特徵因子擬定資料蒐集項目共計78項



# 決策樹模型

Decision tree trained on all the iris features

- 將特徵空間(即所有預測因子變數值所組成的向量空間)進行分割，以便將具有相似性的結果分為一類，分割完成後，在每個區域內產生較為一致的預測分類結果



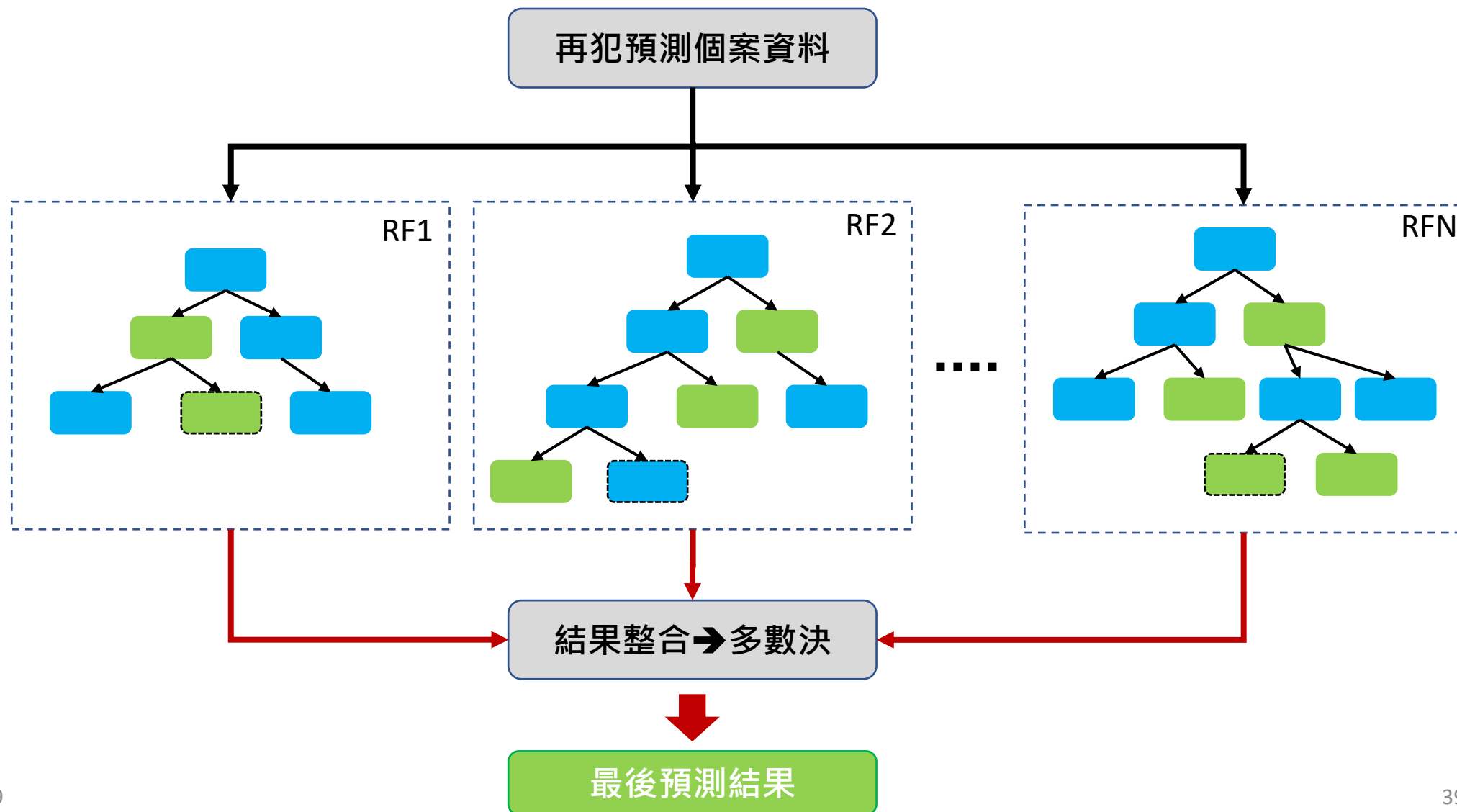
# 隨機森林模型

- 隨機森林(Random Forest)以決策樹(Decision Tree)為基礎的**集成式機器學習**演算法，可用於迴歸分析應用及分類應用
- 隨機森林演算法利用隨機抽樣技術使單一決策樹產生結果的變異性降低，是Bagging技術的改良
- 隨機森林在高維度問題中達成高準確度預測，提供因子重要性量度反應每一個因子在個別及互動下的重要性
- 隨機森林可以自動地由重複隨機抽樣學習資料以產生預測準確率的實際估測
- 美國司法研究所(NJI)與賓州費城成人假釋與緩刑部門研究受保護管束人回到社會後兩年之內再犯風險預測，並已開發一套現役預測工具

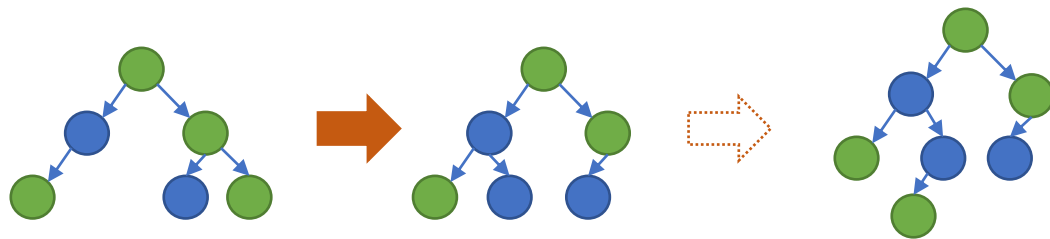


# 隨機森林

集成式機器學習演算法



# 極限梯度提升 XGBoost



$$F(t) = F(t - 1) * \eta * \left(-\frac{Loss}{F(t - 1)}\right)$$

$\eta$  = 學習率

Loss =  $f(p, \hat{p})$ ,  $p$ : label,  $\hat{p}$ : prediction

$F(t)$  = model output at  $t$

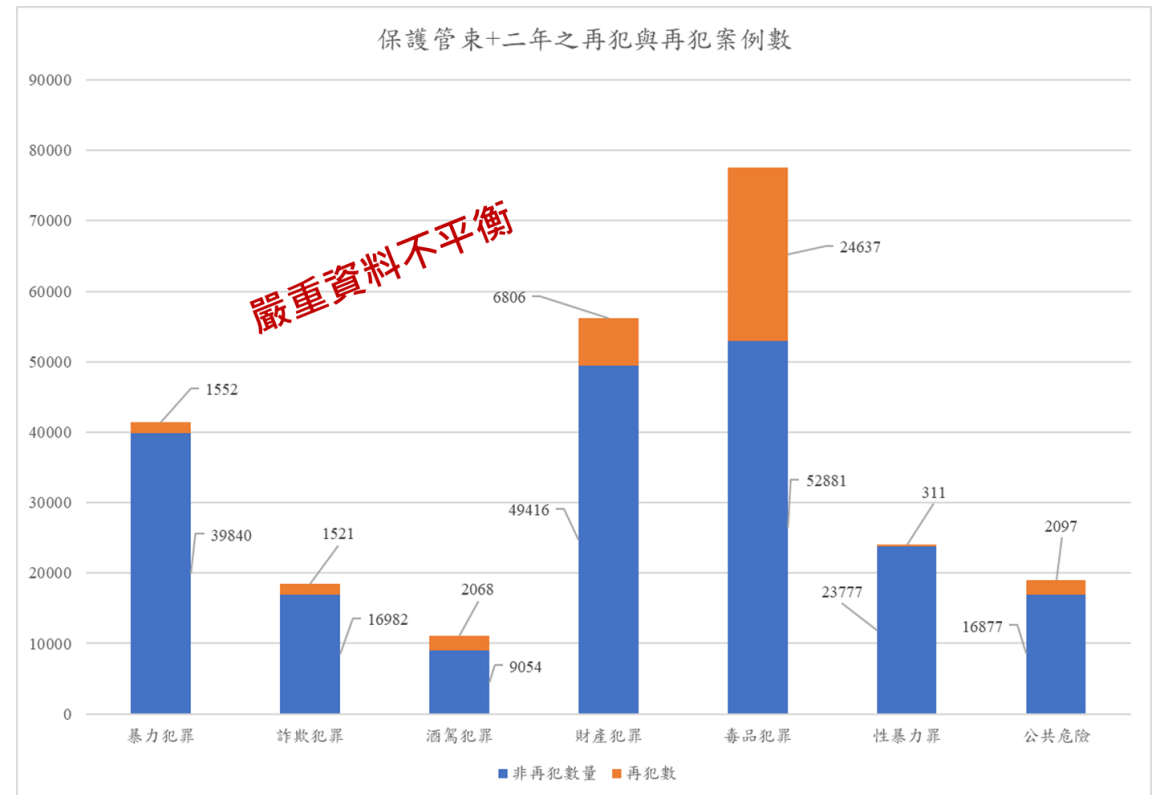
- 建立分類樹過程中後生成的分類樹修正前分類樹錯誤，新的分類樹針對舊的分類樹預測不好的部分做補強，再將所有簡單的樹結合在一起成為最後的預測輸出
- 高效、靈活且易於使用的機器學習算法，能夠處理各種結構化和非結構化數據
- 支持並行處理，具高度可解釋性，協助分析特徵重要性，評估對模型的貢獻最大因子

# 類別資料分佈不平衡

機器學習分類模型對於類別資料分佈不平衡的效能不佳，因為模型分類結果傾向至資料多數的類別。

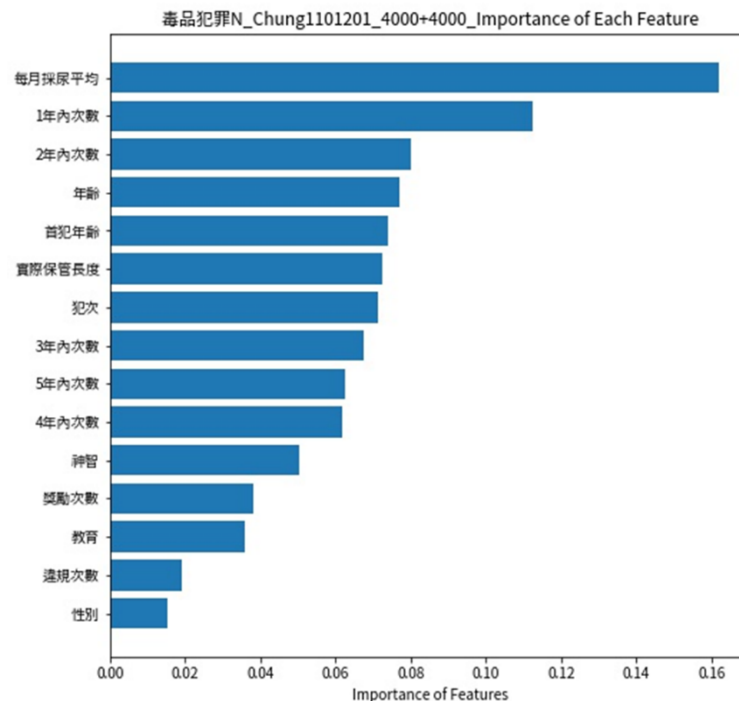
## • 解決方法

- **權重法**:依成本敏感概念，少數分類案例分類錯誤比對於多數類別案例的分類錯誤更嚴重。藉由多數類和少數類的資料數量分佈反比來校正模型的預測
- **上採樣 (Oversampling)**:由少數資料類別抽樣新資料樣本擴充少數資料類別樣本量
- **下採樣 (Undersampling)**:由多數資料類別中隨機採樣選取與少數資料類別相同數量的資料



# 重要因子評估

- 隨機森林給予每一個預測因子在不同環境下相同機會建立模型，以探討對於結果較複雜的反應
- 預測變數重要性評估計算每一個預測因子在所有建立的分類樹中的影響



# 再犯風險評估智慧輔助系統開發



受保護管束人  
再犯風險評估

智慧輔助系統

密碼

驗證碼

 9548

登入

Copyright © 中華民國 法務部



# 再犯風險預測

## AI預測模型屬性

評分日期: 113/03/27

[首頁](#) > [個案資料管理](#) > [個案管理](#) > [再犯預測評估](#) > AI預測模型屬性

■ 黃O賢 觀護案號: 苗栗地檢111毒執護000052號

返回

是否犯罪：再犯性低

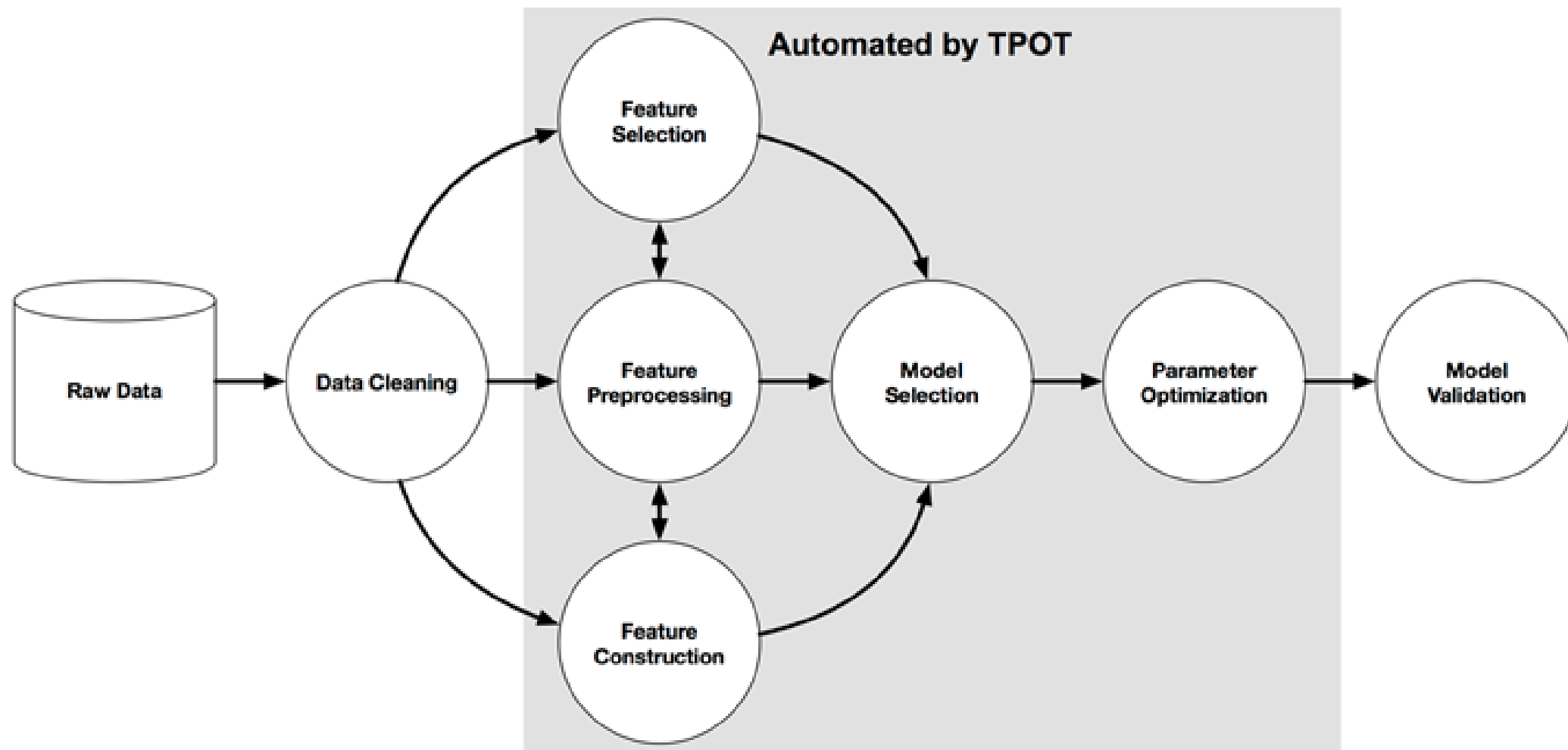
(此機率由AI人工智慧模組運算)

案類

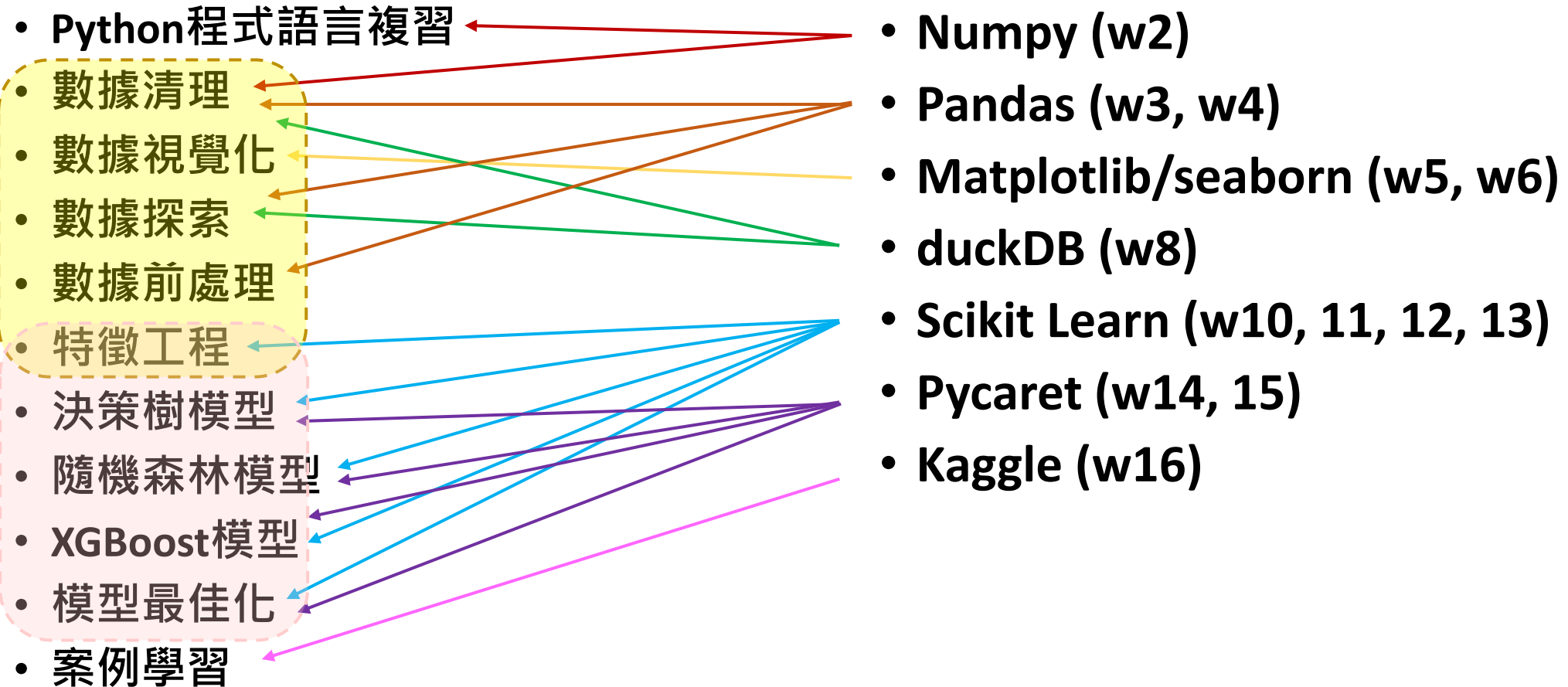
毒品

題項	題目	選項
1	性別	<input type="radio"/> 女 <input checked="" type="radio"/> 男
2	教育	<input type="radio"/> 博士、碩士、研究所 <input type="radio"/> 專科、大學 <input checked="" type="radio"/> 高中、高職 <input type="radio"/> 國中、國小 <input type="radio"/> 其他
3	神智	<input checked="" type="radio"/> 良好、健康 <input type="radio"/> 欠佳、不健康 <input type="radio"/> 罹病 <input type="radio"/> 其他
4	年齡(歲)	<input type="radio"/> 19-30 <input checked="" type="radio"/> 31-40 <input type="radio"/> 41-50 <input type="radio"/> 51-60 <input type="radio"/> 61-70 <input type="radio"/> 71以上
5	保護管束時間長度(月)	<input type="radio"/> 0 <input checked="" type="radio"/> 1-10 <input type="radio"/> 11-20 <input type="radio"/> 21-30 <input type="radio"/> 31-40 <input type="radio"/> 41-50 <input type="radio"/> 50以上
6	違規次數(次)	<input type="radio"/> 0 <input checked="" type="radio"/> 1-10 <input type="radio"/> 11-20 <input type="radio"/> 21-30 <input type="radio"/> 31以上
7	獎勵次數	<input type="radio"/> 0 <input checked="" type="radio"/> 1-10 <input type="radio"/> 11-20 <input type="radio"/> 21-30 <input type="radio"/> 31以上
8	犯次	<input type="radio"/> 【初犯】 <input type="radio"/> 【初再犯同罪】與【初再犯異罪】 <input checked="" type="radio"/> 【再犯】、【再犯同罪】與【再犯異罪】 <input type="radio"/> 【初累犯同罪】與【初累犯異罪】 <input type="radio"/> 【累犯】、【累犯同罪】與【累犯異罪】 <input type="radio"/> 【未註記】與其他
9	每月採尿平均次數	<input type="text" value="2"/>
10	接受保護管束前一年內犯罪次數	<input type="text" value="2"/>
11	接受保護管束前兩年內犯罪次數	<input type="text" value="2"/>
12	接受保護管束前三年內犯罪次數	<input type="text" value="2"/>
13	接受保護管束前四年內犯罪次數	<input type="text" value="2"/>
14	接受保護管束前五年內犯罪次數	<input type="text" value="2"/>
15	首犯年齡(歲)	<input type="radio"/> 11-20 <input checked="" type="radio"/> 21-30 <input type="radio"/> 31-40 <input type="radio"/> 41-50 <input type="radio"/> 51-60 <input type="radio"/> 61-70 <input type="radio"/> 71以上

# 課程範圍



# 課程內容



# 課程進度

- Python程式語言複習 (w2)
- 數據清理 (w3, 4)
- 數據視覺化 (w5)
- 數據探索 (w6, w8)
- 數據前處理 (w10)
- 特徵工程 (w11)
- 決策樹模型 (w12)
- 隨機森林模型 (w13)
- XGBoost模型 (w14)
- 模型最佳化 (w15)
- 案例學習 (w16)
- 期中報告 w9
- 期末專題報告 w17, 18

# 成績計算 85~95

- 平時成績 **50**
  - 平時作業 **40** (四個作業)
  - 出席成績 **10**
- 期中報告 **20**
  - 結合論文與本課程相關議題提報
  - 3年內本課程相關論文提報
- 期末專題 **30**
  - 挑選kaggle中任何一個與本課程議題相關專案執行(含書面及口頭簡報)



# 課程使用工具

請同學上課時自行攜帶筆電同步學習

## 課程工具

- **Github**
  - 檔案儲存與分享
- **Anaconda**
  - 虛擬執行環境
- **Jupyter notebook**
  - 程式開發與執行
- **Google colab**
  - 雲端程式開發與執行
- **Kaggle**
  - 資料集與專案
- **Notion.so**
  - 資訊分享

## 程式套件

- Excel
- Numpy
- Pandas
- duckDB
- Scikit Learn
- Pycaret

# Anaconda3

- Anaconda是 Python 及 R 語言的一個免費開源發行版本，主要用於資料科學(Data Science)、機器學習(Machine Learning)、巨量資料處理(Large-Scale Data Processing)及預測分析(Predictive Analytics)，可對許多套件(Packages)進行管理，是目前全世界最受歡迎的 Python 資料科學(Data Science)平台，全球擁有超過2000萬用戶。區分為「個人版」、「團隊版」、「企業版」
- [Anaconda 下載頁面](#)

# Google Colab

- 方便寫程式的平台，用網頁瀏覽器就能寫 Python 程式、並且執行的平台，雲端的 Jupyter Notebook！
- Colab 免費提供你雲端的運算資源。提供免費的 GPU 讓你高效運算機器學習與深度學習演算法
- Colab 支援 Notebook 強大的互動式計算環境特色，將文字（Markdown）、Python 程式碼、還有程式輸出與圖表放在同一個頁面裡面，呈現出的頁面同時是程式也是文件
- [colab使用教學](#)

# Jupyter Notebook

- Jupyter Notebook 可以想像成是 IPython + Notebook 整合架構，是一個介於編輯器(例如 Atom )及 IDE (Spider、PyCharm、Vim) 之間的應用環境，可讓您編寫程式時利用其直譯式的特性，達到高互動執行結果，並且很容易呈現資料視覺化的執行
- Notebook 是一個可互動式計算，提供網頁 (Web-based) 方式來處理整個計算過程，包括開發、編輯、文件化及執行程式，並可立即傳遞結果
- 本課程將 numpy、matplotlib、seaborn、pandas、scikit-learn 等 python 套件整合於 jupyter notebook，提供學習數據清理、轉換、統計、探索、可視化、AI建模...等應用。
- 官方建議使用 Anaconda Distribution 來進行安裝 notebook，因為 Jupyter Notebook 常用的科學計算 (Scientific Computing)及資料科學 (Data Science) 所需 packages 都已經包含在裡面

# Python 虛擬環境

- Python 虛擬環境是一個獨立的 Python 環境，與系統中其他 Python 環境隔離，可以管理不同專案所需的套件版本，避免衝突和相依性問題
- 每一個 Python 專案都可以有自己的獨立虛擬執行環境，每個專案可以使用不同的 Python 版本和套件，而不會影響其他專案。
- 無論是在本地開發、部署到雲端伺服器，還是與其他同事合作，虛擬環境都能提供一致的執行環境，有助於減少因為環境改變（而不是程式本身）產生的錯誤、提高開發效率
- [Venv](#) 是最推薦的入門款，Python 3.3 版本開始，venv 已被加入 Python 標準函式庫之中，不用另外用 pip 安裝，從 Python 3.5 版本開始，Python 官方建議使用 venv 來建立虛擬環境
- Conda 虛擬環境管理工具用於管理在安裝不同 package，使用 conda 時，你可以建立(create)、輸出(export)、列表(list)、移除(remove)和更新(update)環境於不同 Python 版本及 Packages，同時也可以分享你的虛擬環境。安裝conda最簡單的方式就是安裝 [anaconda](#)。