《資訊管理與資通安全概要》

一、請回答下列有關資料探勘問題：

（一）資料探勘有那幾種模型？請說明每個模型。（15分）

（二）假設老闆要您分析顧客消費行為，您將會採取那種模型？說明其原因。（10分）

試題評析	資料探勘為近年來常考的題目，大部分的專家學者在實務上也希望透過此技術來找出對於組織有幫助的資料關連，所以對於資料探勘主題的掌握除了需要熟悉基本理論外，也需要知道其與實務上的應用方式。 本題是非常經典的題型，透過先考學生基本概念---資料探勘常見之模型，再要求學生分析哪種模型適合分析第二小題之情境。第一題只要有依照上課進度與書目的配合，對於考生都不會有問題，唯一要注意的是需要針對某些類型舉例，如此才可以正確的傳達你對於各種模型的掌握度。第二題主要是考學生對於此技術的反應力，如果對於理論都只是死記硬背，此題會無法有好看的分數，在平時練習時應該要多練習老師上課所提及的思考方式與實務舉例，才可以在第二題游刃有餘的回答。
考點命中	《高點‧高上資訊管理與資通安全》第二回，蕭老師編撰，頁18-20。

答：

(一)資料探勘為運用人工智慧、機器學習、統計學與資料庫的交叉比對方法對資料做分析，以找出有意義的關係或規則，挖掘出隱藏的資訊，常見的模型如下：

1.分類(Classification)：是根據一些變數的數值做計算，再依照結果作分類。通常會研究已經分類的資料其特徵，再根據這些特徵對其他未經分類的資料做預測。

2.回歸(Regression)：使用一系列的現有數值來預測一個連續數值的可能值，例如我們可以透過台灣每個縣市人民對於消費的習慣（消費時間、消費次數、每次消費金額、喜好商品種類…等），來分析即將推出的產品在每個縣市的銷售量。

3.時間序列(Time series)：分析的數值都與時間有關；其方法和回歸很像，只是它是用現有的數值去預測未來的數值。

4.群集(Clustering)：透過分組來分析各組間的差異與同組間的相似處。其方法和分類很像，差異在於分類在開始前有明確對應的類別／函數，也代表資料間已經有明顯的區隔，但群集在運算前與運算中無法得知資料之間的分類方式，也就是群集在事前不知道會以何種根據來分組。

5.關聯(Association)：找出在資料中會同時出現的資料。例如：顧客買了鮮奶與奶酪，那其會同時購買優格的機率是65%。

6.次序(Sequence)：與關連十分密切，不同的是此方法中相關的項目是以時間區分。例如：病患吃了某種藥品，隔天後出現腹瀉的機率是45%。

(二)最適合的資料探勘模型應為群集分析(Clustering)，利用統計方法將資料分為近似的幾組，其目的主要是將組與組之間的差異找出來，同時也要找出組中成員的相似性。此法與分類不同的是事先不知分組標準。例如可以利用此一方法由銷售資料中找出喜歡購買此商品的主要消費族群的特徵(可能是年齡、性別、收入等)，但在進行前並不知道分組標準，全由資料處理中浮現相關特徵。而其最適合用於分析消費行為的原因如下：

1.可以分群：群集分析的一大特點為會將資料結果進行分組。大多企業在推出商品時，無法利用完美差異定價的模式，故只能將商品分成一種甚至有限種的定價模式（例如在軟體業可以依照版本的不同），故可以依照分類出來的模式套用到企業的定價模式中，讓不同消費行為模式的消費者願意支付最大費用的消費模式。

2.事前不知道分組結果：消費者的消費模式在事前無法事先定義，此方法最符合現代多變的消費習慣，不會先入為主的將消費者歸納到特定的分組，而是透過分析資料的相關性產生多組，讓生產商可以依照各組之特性選擇符合消費行為的行銷模式。

3.可變動的分組函數：在實務上可以透過公式參數的變動與撰寫，分析出不同的結果，企業可以在有限的資源內，嘗試各種公式與參數的組合，找到最適合產品的消費模式分析方式，進而得到最適合的行銷與

產品策略。

二、請回答下列有關電子商務方面問題：

(一)請說明搜尋引擎行銷（Search Engine Marketing, SEM）。（10分）

(二)智慧型手機以及行動上網的普及，使得電子商務的經營模式除了傳統的B2B、B2C、C2B、C2C之外，更產生O2O的模式，請說明何謂O2O，並舉出兩個應用案例。（15分）

試題評析	電子商務的類型一直是這三至五年的常見題型，尤其近幾年題目會開始偏向與行銷有關，此題的SEM是較為新穎的題目，在上課時同學除了對於傳統的電子商務理論要有基本的理解外，對於搜尋引擎、Facebook…等新穎行銷手法也要有基本的認識與回答能力。 第一題回答上最好以條列式的分析其行銷方法，而最好拿分的部分莫過於SEO的探討，如果只是單單的回答什麼是搜尋引擎最佳化則會錯失得分的機會，需要具體的提出實例與想法。 第二題是佔分較重的題目，也是此大題的重點，答題上需要對於時事有充分的掌握才比較容易拿到高分，分析O2O的模式時如果只是舉了兩個一般的例子，分數也會非常一般，需要理解O2O的演進過程，然後分別舉例，才可以精準的傳達學生對於O2O的充分理解。
考點命中	《高點‧高上資訊管理與資通安全》第三回，蕭老師編撰，頁28-29、31-32。

答：

(一)搜尋引擎行銷常見的方法為以下兩類：

1.關鍵字行銷：可結合自身經驗，在利用搜尋引擎查找資訊時，是根據「何種目的」來輸入關鍵字或組合。而此方法需要圍繞在一個重要的主軸上，即是消費者需求。

2.搜尋引擎最佳化（Search Engine Optimization, SEO）：透過了解搜尋引擎的搜尋規則來調整網站內容與架構，以提高網站在搜尋引擎內的排名，其常用的實作方法有：

(1)優化文字：搜尋引擎會將網站中的所有文字透過爬蟲方式納入資料庫，並進行分析與分類。當用戶搜尋「健康飲食」時，搜尋引擎就可以把搜尋結果縮小到只與此主題有關的網頁。

(2)注重標題：標題與內容同樣都會被搜尋引擎納入資料庫中，依照其實作架構的不同，標題有可能有更高的權重，故在設定標題時要切中主題，並且盡可能的納入與主題相關的關鍵字詞，使用者在搜尋時才可以快速的連結到此網頁。

(3)重要連結（Links）：當一個網頁連結到另一個網頁時也算是一種推薦的模式，告訴讀者被連接的網頁有不錯的資訊。因此，搜尋引擎會提升獲得較多連結的網頁之搜尋排名。但是有些人會在網路上大量製造或購買造假的鏈結，連到自己的網站，企圖欺騙搜尋引擎。通常，當一個網站有很多這種鏈結的話，搜尋引擎反而是會將其排名調降。

(4)連結所用的文字：假如你的網頁提到「博客來有許多書籍」，而「書籍」是一個鏈結的話，那搜尋引擎就會確定博客來是與「書籍」相關的網站。這樣，當有人搜尋「書籍」等相關詞彙時，博客來就會有較高的排名。

(二)O2O（Online to Offline），將實體與電子商務結合的新型態銷售模式，透過網路無遠弗屆的力量聚集對產品有興趣的消費者，在透過行銷手法將消費者帶往實體通路進行消費。也就是所謂的「線上消費，線下服務」的模式。

較為早期O2O的作法是透過在網路上吸引消費者，當消費者對商品有興趣時，會創造出一個讓消費者必須到店內消費的理由，例如優惠、預約…等方式，在台灣較有名的案例為iPeen愛評網。

而近期的O2O則是注重在創造「內容」與「體驗」，讓消費者會想要嘗試該服務，而到實體的店面或是透過實體的方式去享受該服務，其中包含的範圍從餐飲、健身、住宿甚至是叫車服務皆在此範圍內。近期內最有名的便是很具爭議的Uber叫車服務，其擅長發掘網路上的使用者並會自己散布與創造有趣的內容與體驗。其最特殊的營運模式便是服務提供者及服務購買者都不屬於平台，Uber沒有一輛屬於自己的車，但他們卻顛覆以往對O2O的認知，早已擺脫早期傳送訊息的角色，發展出屬於自己的品牌故事與模式。

三、區塊鏈被視為被看好的金融科技技術，請說明區塊鏈是什麼？區塊鏈具有那些特色？（25分）

試題評析	區塊鏈與金融科技為這一兩年竄起的題目類型，在傳統的教科書中都沒有或只是擺在補充的區域，而老師認為這才是這一兩年最該出現的活題目，故皆要求同學要搞懂此部分的各種理論與實務上之應用。 此題在作答上不用太緊張，只需掌握基本概念即可，並且了解為什麼這一兩年此領域會突然竄紅，平實的作答與舉例即可得到不錯的分數。唯獨在區塊鏈中其特色與優點一定要具體的說明其優勢與相關技術，才可以傳達學生對於此理論的理解度。
考點命中	《高點‧高上資訊管理與資通安全》第二回，蕭老師編撰，頁52-57。

答：

區塊鏈是由區塊(Block)透過特定的技術手法組織起來的鏈條(Chain)，在此技術中，訊息與紀錄會被放在一個一個的區塊中，用密碼與簽名的方式連接到下一個區塊，換句話說，它就是一種改變「記帳」方式的新技術，它讓交易過程中每個節點的每一筆帳，都能透明又安全地被記錄下來。

可以把區塊鏈想像成是平等的各節點所連接，每個節點都有完整的數據資料，當其中一個節點上的紀錄有所變動時，系統上的其他節點都會跟著同步，區塊鏈技術由電腦系統按照寫好的規則自動化一切過程，因此交易或紀錄一旦發生就不可逆且具可溯性，不像是現在大部分的商業模式，由建立系統的公司或是各產業的中央機構居中，掌控大數據資料和所有的交易過程。

透過區塊鏈技術發送訊息時，系統上的每一個節點都會接收到訊息，但是只有擁有私鑰的人才可以解密看到訊息的內容，換句話說，每個訊息在傳送的時候都是有加密過的，因此可以達到非常安全的共享，也不會被竄改、遺失...等，但區塊鏈技術就像大數據一樣只是一種底層技術，需要應用在現實生活或是商業模式中才會產生價值，當運用區塊鏈技術產生新的商業模式時，對應的配套工具和服務是必要的，所以區塊鏈的相關開發上，除了其技術外，還要考慮整個生態系統的開發與應用才可以完整的產生有用的價值，譬如說做區塊鏈大數據分析的公司以及資訊安全技術公司等。

其技術之特點可以分為以下幾點：

(一)去中心化

不依賴第三方管理機構或硬體，完全去除中心化，除了自成一體的區塊鏈本身，通過分散式運算和儲存技術，各個節點會自己實現驗證、傳遞與管理的機制，去中心化是區塊鏈最重要也是最被推崇的特色。

(二)開放性

其技術基礎是開源的，除了交易的私有資訊會被加密外，區塊鏈的所有數據都是對外開放的，任何人都可以通過公開的介面查詢區塊鏈數據和開發相關應用，達到整體系統的高度透明。

(三)獨立性

基於一致的規範與交易協定，整個區塊鏈系統不會依賴其他第三方，其所有節點都能夠在系統內自動安全的驗證與交換數據，不需要任何人為的干涉。

(四)匿名性

從區塊鏈的技術上來講，各區塊節點的身分資訊不需要公開或驗證，資訊傳遞可以匿名進行。但是若有法律規範則不在此限內。

(五)安全性

只要沒有掌握到全部的51%的節點，就無法透過竄改節點資料來造假網路數據，而本身的節點數非常大，故此方法非常安全，幾乎不可能有人掌握到51%的節點。

四、請說明弱點掃描與滲透測試的差異，並試說明OWASP TOP 10 2013中的五項，再針對OWASP TOP 10 2013的第一名說明應用系統安全開發方式。（25分）

試題評析	此題的第一個問題為常見之題型，同學平時要對資訊安全相關的技術與攻擊手法有基本的了解，便可拿到此小題的分數。 而第二題則是讓大多數同學恐慌的題目，如果沒有聽過OWASP TOP 10又沒有背過其在2013年發表的文件，則會一時無法作答。此題在答題上需要掌握一個心法，即是每年攻擊的手法可能會不同，但是重點的攻擊方式皆是大同小異，所以沒有看過此報告的同學也只需要針對常見的攻擊手

	法回答即可，其中第一名的注入攻擊相信同學也可以大致猜到，此攻擊法一直在資訊安全議題的排行榜上高居不下。
考點命中	《高點・高上資訊管理與資通安全》第三回，蕭老師編撰，頁51-52。

答：

(一)弱點檢測與滲透測試

1.弱點檢測

根據過往漏洞歷史所產生的資料庫，透過掃描的方式，對遠端或本地的資訊系統之安全性進行檢測，並嘗試發現潛在弱點之方法。透過此種方法，網路管理員可以快速了解系統，並即時發現可能的威脅。又可以依照分類將其分成「對網路掃描」、「對主機掃描」與「對資料庫掃描」之類型。

其功能主要為以下四項：

(1)定期的網路自我檢測與評估

網路管理人員可以定期進行網路安全檢測，盡可能及早發現漏洞與修補。

(2)新軟體的安裝與軟體升級後的檢查

新軟體的安裝與新服務的啟動都有可能讓原本的漏洞暴露出來，故在進行這些操作後都要進行弱點檢測。

(3)網路建置後與改善後之評估與成效檢測

網路管理者需要維持與建立整體安全規則，對於網路有整體性的防護，故需要在改動後進行此項操作。

(4)網路事故後的分析調查

透過弱點檢測可以在事件發生後分析弱點位置與原因，並把資料存進資料庫，以便下一次進行分析。

2.滲透測試（Penetration Test）

為了證明網路防禦機制和預期的規劃一樣正常運行，測試人員在不同的網路位置與搭配各種手段，透過模擬惡意攻擊來評估組織網路安全的評估方法。

其特性有：

(1)逐步漸進式的分析與測試過程。

(2)盡量在不影響系統正常運行的方式進行模擬攻擊與測試。

	弱點掃描	滲透測試
執行者	自動化工具。	專業顧問。
執行思維	利用弱點資料庫來掃描現有系統的弱點。	具備高技術水準的資安人員模擬駭客思維，針對系統做攻擊。
規模	可以大規模檢視系統。	規模較小。
限制	許多漏洞無法找出，例如：商業邏輯漏洞、Dos攻擊漏洞…等。	耗時長、成本大且可能影響正常營運。
關係	1.滲透測試有可能包含弱點掃描。 2.滲透測試會依照弱點掃描的結果再嘗試深入攻擊系統以找出影響範圍。	

(二)OWASP（Open Web Application Security Project）為非營利性組織，其目標是要協助制定網路軟體安全之標準、工具與技術文件，並致力於協助組織瞭解與改善網頁應用程式與網頁服務的安全性，而TOP 10 2013中的前五名包含：

1.注入攻擊（Injection）

攻擊者在網頁可以輸入資料的地方嘗試填入不合法的語法，其目的為猜測網頁設計者背後撰寫語法的邏輯，利用該欄位搭配自己的語法組合成一個可以造成對網頁有害的攻擊指令，像是推測欄位數，table的名字，SQL的版本資訊，試著去拼湊輸入一條SQL指令，輕則刪掉資料庫，重則竊取全部的個資。

而針對第一名的注入攻擊，系統在開發時需要注意：

(1)不要將錯誤訊息給管理者以外的人看到，以避免攻擊者獲得更多的攻擊資訊。
(2)對於使用者的帳號權限需要有控管機制。
(3)需要對使用者所有輸入的字串進行合法性檢查。

2.失效的驗證與連線管理（Broken Authentication and Session Management）
網頁在建立Session時有可能會將Session ID直接擺在存取的URL中，而如果有人將URL直接傳給其他人，就可以能造成此Session的驗證是不合法的情況。
另外一種情況則是網頁端沒有針對每個Session設定timeout的機制，導致在公用電腦登入的合法使用者，在離開電腦後，被下一個使用電腦的人盜用其Session，直接登入。
除了以上兩點外，尚有未使用SSL加密連線資訊，或是密碼儲存時沒有加密…等情況。

3.跨站腳本攻擊（Cross-Site Scripting, XSS）
惡意使用者將程式碼注入到網頁中（常發生在有類似留言板功能的網頁），其他使用者在觀看此網頁時就會受到惡意程式碼的影響。這些惡意網頁程式碼通常是JavaScript，但實際上也可以包括Java，VBScript，ActiveX，Flash或者甚至是普通的HTML。攻擊成功後，攻擊者可以得到更高的權限、私密網頁內容、對談和cookie等各種內容。

4.不安全的直接物件參考（Insecure Direct Object Reference）
當網頁在設計時，如果沒有針對使用者所輸入的字串是否為合法字元時，可以造成攻擊者利用網站的檔案讀取功能，去任意的讀取敏感資料或重要檔案，進而分析這些檔案後，達到攻破網站的目的。

5.不當的安全設定（Security Misconfiguration）
常見之不適當的安全設定包含：
(1)未刪除或更改所使用套件的預設帳號密碼，攻擊者可以輕而易舉地透過嘗試法直接入侵。
(2)錯誤訊息直接回傳在使用者頁面上，此舉會透漏許多額外的訊息給予攻擊者。
(3)未刪除套件所附的範例應用程式，造成攻擊者利用範例的漏洞進行攻擊。