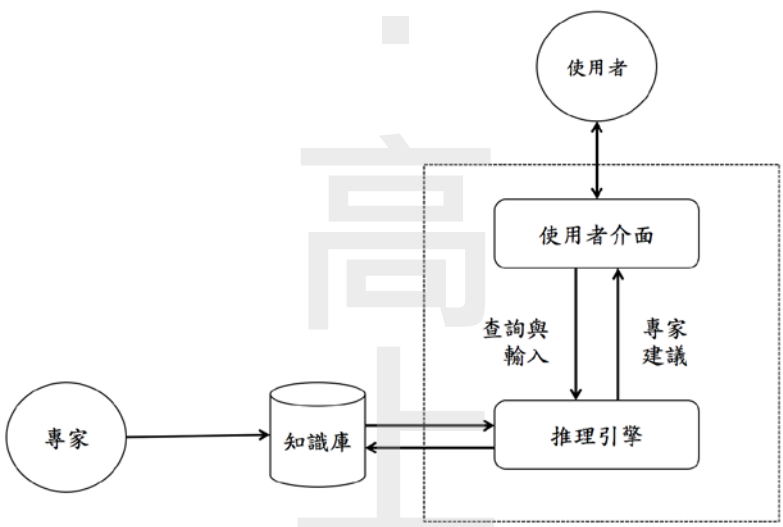
《資訊管理概要》

一、請詳述專家系統（Expert System）的核心模組架構，並舉例說明專家系統的實務應用。（25分）

試題評析	專家系統一直是企業到政府常用的基本資訊系統，用以幫助一般使用者做最佳的決策。而專家系統最重要的不是要取代專家，而是為了要將專家的知識與經驗可以更快速的傳遞與推廣，大部分的企業或是政府機關在實務上也希望透過此技術來找出對於組織有幫助的決策模式。 此題考的是非常基礎的專家系統基本架構，除了需要熟悉基本架構外，也需要知道其與實務上的應用方式。透過先考學生基本概念—專家系統之基本架構，再要求學生分析實際使用之情境。 核心模組架構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。 實際應用上只要熟悉上課所舉的例子，基本上也是可以遊刃有餘的作答，唯須注意在答題上若可以將應用分類，則可以獲得較好的分數。
考點命中	《高點‧高上資訊管理與資通安全講義》第二回，蕭老師編撰，頁104-106。

答：

(一)專家系統的基本功能為將特定領域內的專業知識儲存在電腦資料庫中，再透過系統的推理引擎來提供專家的意見或協助組織解決問題。



1.知識庫

將特定領域的專家之內隱知識和經驗法則以規則的方式儲存在資料庫中。

2.推理引擎

為系統內的一部分，將使用者所輸入的事實，根據邏輯判斷與分析並模擬專家的建議與分類依據，獲得最終結果的軟體。

3.使用者介面

提供一般使用者較友善的輸入方式，並在查詢分析後提供視覺化的解釋與說明，且可以提供諮詢功能之介面。

通常在使用者介面與推理引擎中會有一個合適的「解釋機制」，此機制幫助使用者理解推理引擎的推理邏輯與方法，透過友善的視覺化呈現，使用者可以快速理解推理過程。

(二)推理的過程可以分為以下兩種：

1.正向推理

根據使用者所輸入的資訊來推論出可能的結果。

目前有許多醫院可以透過分析病患的病徵來分析可能的疾病，並及早幫助病患預防與治療，在遠距醫療上此系統也可以提供醫生更快速更準確的判斷依據。

2.逆向推理

根據結論來問使用者是否有這種前提存在，以判斷帶解決問題的狀況。例如：企業是否可以在今年提升50%以上的市佔率。

二、若無部署適當的資通安全機制，使用網路系統將可能面臨那些安全威脅與攻擊？（25分）

試題評析	資訊安全為常見的題型，此題算是中規中矩，在考試時看到此題頭腦一定會冒出許許多多的攻擊名詞與手法，如果只是單就攻擊方式條列式答題，則會較無章法與邏輯，反而得不到高分。 越簡單的題目在下筆之前越要小心，此題除了要記住與理解上課所說明的攻擊方式外，更要針對各種攻擊方式進行分類，如此在答題上才可以獲得較高的分數，也可以展現邏輯分析能力。 此外在答題上，也要盡可能的針對某種攻擊的方式提供實例。
考點命中	《高點‧高上資訊管理與資通安全講義》第三回，蕭老師編撰，頁69-72。

答：

資訊安全的威脅與攻擊可以分為兩大類，分別是「主動式攻擊」與「被動式攻擊」。

(一)主動式攻擊：指入侵者針對檔案或通訊內容進行偽造或修改。

1.偽裝

攻擊者透過技術或是社交工程的方式欺騙認證系統，非法取得資源的獲取權限。最常見的例子如：利用社交工程騙取一般大眾的信任，或者利用網路竊聽的方式取得密碼後登入系統，之後再對有用的資料進行竄改或是竊取。

2.重播

攻擊者截取網路上的通訊內容或是認證資訊，並且重新發送給認證系統，以騙取認證系統的信任。

攻擊者將從網路上截取的某些通訊內容(如認證資訊)重新發送，以欺騙伺服器認證機制。又可以依據重放的方式分為三種：

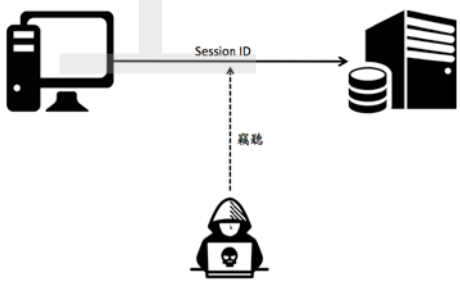
(1)直接重播：系統直接在未授權的情況或是時間下，重新發送原來的驗證檔給驗證系統，在此關係中發送方和驗證方均不變。

(2)反向重播：將原本發給驗證方的消息反向發給發送方。

(3)第三方重播：將驗證資訊發送給網域內其他的驗證方。

3.訊息竄改

攻擊者針對網路通訊的內容進行刪增或者更動。例如：利用竊取通訊資訊(Session Hijacking)，攻擊者可以利用多種方式竊取Cookie中的通訊資訊或驗證資訊，實作方法如下圖：



4.服務阻絕

又稱洪水攻擊，一種透過網際網路的攻擊手法，目的在讓目標伺服器或網路的資源耗盡，造成目標所提供的服務中斷，讓一般使用者無法存取。

(二)被動式攻擊：未經授權的攻擊者取得資料的相關內容或存取權限，但是並未對內容進行竄改，只是加以分析並等待時機。

1.竊聽

攻擊者會針對檔案或通訊內容進行監控。最常見的例子是於影片中時常出現的電話監聽與網路監聽等等。

2.通訊分析

又可以再細分為流量分析與通訊內容分析，流量分析是針對網路通訊的流量、行為...等進行分析，用以獲取組織的通訊模式與習慣等資訊。

而通訊內容分析則是會試圖分解與破解所傳遞的內容，但是都不會對於內容進行修改，可以獲得可觀且寶貴的資料，例如：伺服器位址...等。

三、請詳述機器學習（Machine Learning）的定義及其應用。（25分）

試題評析	近年來由於人工智慧的崛起，與人工智慧有關的名詞和領域越來越常出現在考題中，此題的機器學習便是。故近幾年在準備考試時，需要多關注與此有關的議題與名詞，當有常出現名詞時，要能夠理解其基本意義並熟記，依照此種準備方式即可應付大部分相關的時事考題，並且在答題上要能夠掌握機器學習的基本理論與架構，和它相關的其他理論。 考試時，如果一時想不到課堂上的舉例，只需要想到生活中常見、通俗和好懂的應用並舉例即可。
考點命中	《高點‧高上資訊管理與資通安全講義》第二回，蕭老師編撰，頁18-20。

答：

機器學習為實現人工智慧的其中一種方式，此領域涉及機率論、統計學、計算複雜性理論等多門學科。機器學習理論主要是設計和分析一些讓電腦可以自動「學習」的演算法，透過演算法讓電腦從資料中自動分析出有用的規律與判斷準則，並對未知的資料進行預測。演算法設計上，機器學習理論關注可以實現的學習演算法，在目前很多推論問題都屬於無法用程式來推論之難度，所以部分的機器學習研究是開發容易處理的近似演算法。

而在機器學習上又可以分為以下幾類：

(一)監督式學習

在訓練的過程中會將正確的答案告訴電腦，也就是在資料打上標籤，以確保電腦朝向正確的方向學習，通常會有較高的準確率，常見的例子為目前有許多的軟體可以透過分析圖片的特徵來分析圖片中有沒有出現特定的人物，或是類似人臉辨識。

(二)非監督式學習

訓練資料沒有標準答案，也不會提供具有標籤的資料給電腦學習，在學習時並不知道其分類結果是否正確，電腦在訓練時會自動從這些範例資料中找出潛在的規則。

「群集式分類」：在實際的應用上只要是採用群集式分類的即可算是非監督式學習法，群集的基本概念為找出較為相似的資料並將其歸為一類，形成群集（Cluster），其中相似的依據是採用每個資料點之「距離」，相對距離愈近、相似程度越高，會被歸類至同一群集。

「關聯規則分析」：以資料一起出現的情況、時間、次數…等來考量資料間的相似性，例如：在分析超市中消費者的購物行為時，可能會發現「買紅茶又買鮮奶的人的比例非常大」，因此許多賣場在擺放商品時可以藉此提高商品的銷售。

(三)半監督式學習

介於監督式與非監督式之間的學習法。將資料分群的過程當中，會先使用一群具有標籤的資料將全部資料大致分成幾群，再利用剩下無標籤資料的整體分布，分析出其他資料屬於哪一個分類。此種學習方式不但具有非監督式學習高自動化的優點，又能降低標籤資料的成本。

(四)增強學習

電腦會透過環境的不同而有不同的行動，並隨時會根據新進來的資料給予正向或負向的回饋來逐步修正。

目前常見使用案例為機器人的行為，例如：我們想要讓機器人可以模擬特定的人類行為時，當機器人所做的動作越來越接近目標行為時，就會給予正向回饋，反之就給予負向的回饋，如此可以讓機器人快速做到學習動作的目的。

目前AI在生活上的應用非常廣泛，其中又以Google和Facebook的應用最廣為人知，例如：Facebook所提供的人臉辨識與標註功能，即是利用我們所上傳的照片所含有的相似人臉，來辨認是否為我們的朋友，並提供標註的建議。

四、數位證據（Digital Evidence）是取之於電腦系統、儲存媒體或行動裝置內，可作為犯罪偵防

及資安事件調查的數位資料。當數位證據保全人員處於開機狀態的標的設備中擷取揮發性與邏輯性資料完畢後應如何保全這些數位證據？（25分）

試題評析	數位鑑識領域在國家考試中也一直是重點複習項目，此題所問的資料保存方法乍看之下會感覺在課堂上沒有提過，但同學只需靜心設想，即可發現其實其處理方式和一般的數位資料保存類似，唯獨需要注意此類型的資料是需要當做往後的鑑識作用，故需要更嚴謹的過程與保證。 此題在政府機關資安事件數位證據保全標準作業程序中已經有明確的定義，同學如果照此回答，必可以得到高分，但是此條文難以記憶，可以用以下思考模式： 答題上可以分成兩個大方向來思考，第一級是一般數位資料該如何保存，並且不會遺失。二為此種資料必須當做日後審判的依據，所以在蒐集上需要更多證據來證明資料沒有被破壞或更動，結合以上兩點的回答即可在此題獲得高分。

答：

根據《政府機關（構）資安事件數位證據保全標準作業程序》中擷取揮發性與邏輯性資料之保存方法可以分為以下幾點：

(一)各機關得視其資訊人力資源進行不同程度之揮發性及邏輯性資料擷取。

(二)如相關標的設備處於開機狀態下，數位證據保全人員應考量資安事件類型及現場狀況後，擷取揮發性資料，以避免部分儲存於記憶體中之重要資料因系統關機而消逝。

數位證據保全人員應考量資安事件類型及現場狀況後，擷取邏輯性資料，如作業系統資訊、網路狀態、執行程序資訊、系統稽核日誌記錄及使用者上網行為記錄等。

針對防火牆設備、入侵偵測或防禦設備、紀錄保存與資安事件分析設備、防毒設備、流量控管或網路監控設備、應用系統及資料庫等設備，若各機關有資訊人力，得在數位證據保全人員檢視下，由應用系統或網路管理人員將稽核日誌檔案匯出至特定目錄內，由數位證據保全人員對其進行邏輯性資料擷取。

數位證據保全人員於擷取揮發性與邏輯性資料完畢後，應產生相對應之雜湊運算值，並記錄擷取之資訊或以自動化工具所產生之報表為之，如擷取日期與時間、電腦名稱、所蒐集之揮發性與邏輯性資料項目、雜湊運算值等，經執行人員與資安事件發生單位主管簽章確認。

(六)記錄人員應以全程錄影或拍照方式記錄揮發性與邏輯性資料擷取之步驟

1.針對工具連結至標的設備時進行拍照

2.針對工具執行時之螢幕畫面進行拍照

3.針對工具之重要操作步驟之螢幕畫面進行拍照

4.針對工具執行完成時之螢幕畫面進行拍照

(七)數位證據保全人員應將揮發性與邏輯性資料進行封緘，並視需要運送至上級機關或鑑識單位。

【參考來源】

行政院公布之「政府機關（構）資安事件數位證據保全標準作業程序」