

《資訊管理概要》

試題評析

相對於以往的題目，今年普考的MIS算是比較標準的題型。一樣配了20%的資訊安全，及20%基本的名詞解釋。唯獨第二題「分散式資料庫」與第五題的「檢測方法」是以往考試中沒有出現過的新考點，若沒有相關的實務經驗會較難拿到高分。但分散式資料庫的部分，若能掌握分散式運算的優缺點，便能觸類旁通。此外，第三題算是比較活用的題目，必須了解資訊爆炸所面臨的問題、Data Mining中不同方法的特性以及現有的推薦機制，才能掌握該題並寫出足以說服考官的答案。總體而言，今年的題目難度中等，程度較好的考生應可有70-80分，而程度中等的考生也能拿到50分以上。

一、請解釋以下名詞：（每小題5分，共20分）

- (一)地理位置服務 (Location-based Service, LBS)
- (二)資料庫管理系統 (Database Management System, DBMS)
- (三)主管資訊系統 (Executive Information System, EIS)
- (四)使用者自建系統 (End User Computing, EUC)

答：

(一)地理位置服務：

又稱為地理位置服務，透過行動電話網路或外部定位的方式（如：GPS）獲取行動裝置使用者的位置資訊。並藉由 GIS 的支援，為使用者提供相應服務的一種增值服務。一般而言，可以結合其他的系統應用於生活中：

- 1.全球定位系統：提供使用者所在地的座標資訊，可以對使用者的位置進行追蹤，進而提供與使用者所在地相關的支援。例如：找到與使用者最接近的朋友位置。
- 2.地理資訊系統：提供地理空間與屬性資料，可以讓使用者知道自己所在地的相關資訊，進而產生消費行為或取得服務。例如：可以知道所在地附近的優惠商家；另外或是進行路線規劃與導航。

(二)資料庫管理系統：

資料庫管理系統是用來建立和維護資料庫的軟體。有以下功能：

- 1.定義資料：接受原始形式的資料定義，並將其轉變成適當的目的形式。
- 2.處理資料：處理使用者的要求，提供併行性管理，並產生對應的結果。
- 3.確保資料安全性與完整性：監督使用者的需求，並拒絕任何侵犯資料庫管理員所訂定之安全性及完整性規則的意圖。

一般而言，以架構而言，可分為關聯式資料庫管理系統、物件導向資料庫管理系統、階層式資料庫管理系統與網路式資料庫管理系統四類。

(三)主管資訊系統：

企業利用快速、及時、整合的資訊科技，篩選、彙整與追蹤外在事件與內部關鍵資料，即時產出最重要的多維度資訊，提供決策者、高階主管判斷，提升企業競爭力。其主要架構如下：

高點·高上高普特考 goldensun.get.com.tw 台北市開封街一段2號8樓 02-23318268

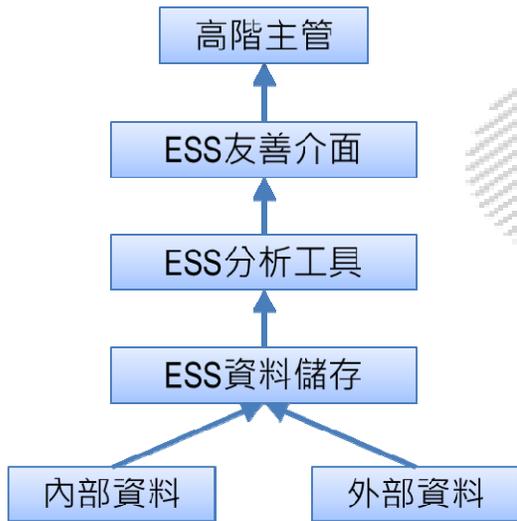
【中壢】中壢市中山路100號14樓·03-4256899

【台中】台中市東區復興路四段231-3號1樓·04-22298699

【台南】台南市中西區中山路147號3樓之1·06-2235868

【高雄】高雄市新興區中山一路308號8樓·07-2358996

【另有板橋·淡水·三峽·林口·羅東·逢甲·東海·中技·雲林·彰化·嘉義】



說明：

- 1.資料儲存：資料庫 (Database)、資料超市 (Data Mart)、資料倉儲 (Data Warehouse)
- 2.分析工具：OLAP、Web-OLAP、資料採礦 (Data Mining) 工具、DSS 模式庫 (Model Base)

(四)使用者自建系統：

使用者自行利用易學、容易上手的軟體 (例如：4GL)，由資訊人員扮演支援協助的角色，進行開發、維護自己所需要的應用程式。有以下特色：

- 1.個人化功能：反應需求且接受度高、富創意，但卻未必符合組織需求，功能受 4GL 或技術限制。
- 2.分散成本：節省資訊部門人力，但卻花費使用者上班時間、失去規模經濟優勢、重複購買設備。
- 3.速度快：4GL 開發速度快，使用者不需等待、降低轉換時間。
- 4.不符標準：不易整合、維護、缺乏文件、詳細測試。

【高分命中】

- 1.金乃傑《資訊管理與資通安全》講義，第一回，頁52。
- 2.金乃傑《資訊管理與資通安全》講義，第一回，頁25, 26。
- 3.金乃傑《資訊管理與資通安全》講義，第一回，頁53-54。
- 4.金乃傑《資訊管理與資通安全》講義，第二回，頁42。

二、何謂分散式資料庫？(6分) 並請分析分散式資料庫的優缺點？(14分)

答：

(一)分散式資料庫是用電腦網路將物理上分散的多個資料庫單元，連接起來組成的一個邏輯上統一的資料庫。每個被連接起來的資料庫單元稱為節點。從使用者角度而言，分散式資料庫是一個很大的單一資料庫，但實際上資料卻是分散在網路的多個地方，透過分散式資料庫管理系統來從事資料的管理與控制。有以下特色：

- 1.物理分散性：資料庫的實體分散於不同的地區，節點間的記憶體與硬體資源各自獨立。
- 2.邏輯整體性：從使用者角度而言仍是使用單一資料庫，使用者也不需要知道資料庫實際存放的細節，即可進行操作 (通透性, Transparency)。
- 3.節點自治性：具備資料冗餘，避免單點失敗；並配合組織地方分權的架構，在管理上也有較高的彈性。

高點·高上高普特考 goldensun.get.com.tw 台北市開封街一段2號8樓 02-23318268

【中壢】中壢市中山路100號14樓·03-4256899

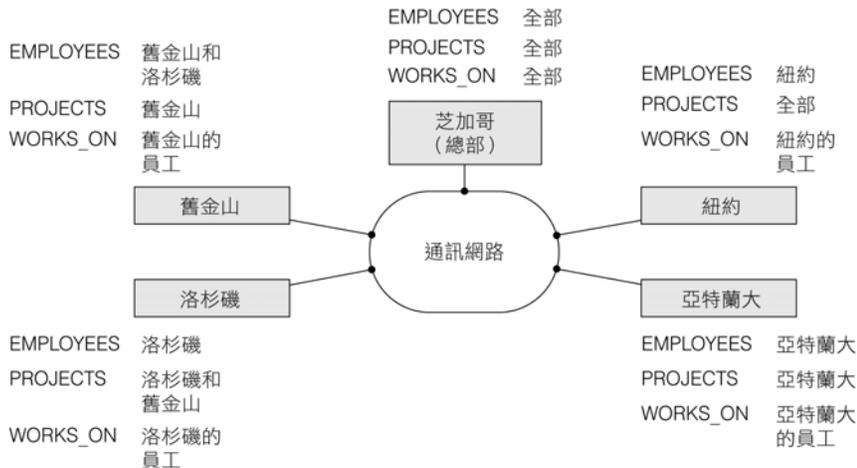
【台中】台中市東區復興路四段231-3號1樓·04-22298699

【台南】台南市中西區中山路147號3樓之1·06-2235868

【高雄】高雄市新興區中山一路308號8樓·07-2358996

【另有板橋·淡水·三峽·林口·羅東·逢甲·東海·中技·雲林·彰化·嘉義】

下圖為大型組織分散式資料庫的參考架構：



(圖：引用自《資料庫系統管理》，台灣培生，2008)

(二)由於分散式資料庫資料分佈在不同節點且從使用者角度視為單一資料庫，茲將優缺點分析比較如下：

優點：

- 1.反映組織架構、允許區域自治性：可在不同的分公司設立部分資料庫，充分實行地方分權，並能隨時針對各區域的使用者做調整。
- 2.降低網路的流量，增加處理速度：根據統計，分公司有 80%的資料存取都是要查詢自己的營業資料，因分公司的節點正存著這些資料的副本，因此可以比較快速的取得資料。
- 3.擴充性高：隨著企業的成長而做漸進式的擴充，另外也可透過網路連接已存在的資料庫系統，與既有系統進行整合。
- 4.可作平行處理，增進可靠度以及妥善率：若查詢的資料來自不同節點，則節點可同時處理資料，不但運算較快，也可以使負載平衡。
- 5.邏輯上一個大型資料庫，並非各分公司的獨立資料庫：技術上改善集中式資料庫系統無法應付使用者需要跨越多個資料站做整體運算的缺點。

缺點：

- 1.處理與管理複雜度高：由於資料分佈在不同節點中，在設計時必須要考量同步的問題，並確保資料的一致性，管理上也比一般單一資料庫來的複雜。
- 2.儲存較花時間、空間：一份資料卻必須同步儲存到不同的節點中，會花比儲存單一資料較久的時間，且也會占用較多的硬體空間，花費額外的成本。
- 3.資料的機密性與安全性受到威脅：不同節點的資料透過網路整合，因此傳輸過程中如何確保資訊的機密性、完整性，以防止未授權的資料存取，也是分散式資料庫的一大挑戰。

【高分命中】

- 1.金乃傑《資訊管理與資通安全》講義，第一回，頁25-56及上課補充。

三、過去中間商因靠著資訊不對稱，可在其中獲得利潤，稱為中間化 (intermediation) 的特性，隨著資訊科技的發展，交易雙方獲得資訊的成本降低，因此產生了中間化 (disintermediation)。然而資訊不對稱的情況雖然得到解決，卻也造成資訊爆炸的狀況，請回答以下問題：

(一)請問要採用何種方式解決上述資訊爆炸的問題？並舉例說明之。(5分)

(二)在社群網路上也存在資訊爆炸的問題，請問如何採用資料探勘 (Data Mining) 的那些功能可對此情況進行改善？(15分)

【台北】台北市中山路147號3樓之1·06-2235868 【台中】台中市東區復興路四段231-3號1樓·04-22298699
 【台南】台南市中西區中山路147號3樓之1·06-2235868 【高雄】高雄市新興區中山一路308號8樓·07-2358996
 【另有板橋·淡水·三峽·林口·羅東·逢甲·東海·中技·雲林·彰化·嘉義】

答：

(一)解決資訊爆炸問題可以從兩個方面著手：1.提供更方便的資訊檢索系統；2.只顯示使用者有興趣或重要的資訊。以下分項描述之：

- 1.提供更方便的資訊檢索系統：不管是透過分類機制，像奇摩的網站分類檢索，或建立強力有效的搜尋引擎，如：Google 或 Bing，都是有效讓使用者找到自己有興趣的資訊的方法。另外，也可以透過 Web 3.0 的技術，讓電腦能「看的懂」這些龐大的資訊，以便使用者能更有彈性且更容易找到所需的資訊，而不需要接觸到大量且不相關的資料。
- 2.只顯示使用者有興趣或重要的資料：透過協同過濾機制或社群網路朋友推薦，可以讓出現在使用者眼前的資訊都是使用者較感興趣的。例如：在 Amazon 上可以看到「看這本書的人也會看...」，這樣就比呈現成千上萬本書還對使用者來的有價值。另一方面 Facebook 也會推薦使用者朋友都按讚的粉絲專頁，一樣能降低使用者暴露於過多的資料之下而無法找到真正要的資訊。

(二)社群網路因為每個使用者都可以很容易的在上面分享資訊，因此很可能產生許多不相關或使用者不感興趣的資訊，因而造成資訊爆炸。

在資料探勘的技術中，有兩種方法可以解決此一資訊爆炸的問題：分群與關聯分析。以下分述如下：

- 1.分群分析 (Clustering)：透過資料探勘的分群技術對使用者進行分群，可以使群組內的差異最小化，群組間的差異最大化，如此可以找到使用者所在的群組，從群組中其他活躍使用者的好惡來對使用者進行推薦。舉例來說，假設根據分析發現某一群的使用者對偶像歌手較有興趣，則可以推薦他們一些偶像歌手相關的轉貼連結、影音或粉絲專頁，這些資訊對這群的使用者而言可能就會比國家考試來的有吸引力，讓使用者吸收自己有興趣的資訊。
- 2.關聯分析 (Association)：關聯分析的目的是找出「喜歡 A 也會喜歡 B」或「不喜歡 A 也不喜歡 B」的模式 (Pattern)，以往最常見於購物來分析，用來了解哪些產品會一起被買等消費資訊。在社群網路中，我們也可以透過關聯分析找到使用者感興趣的主題。例如：在 Facebook 中，當使用者對某些貼文「按讚」之後，可以找出「按 A 貼文讚也會按 B 貼文讚」的模式，進而在訊息串上顯示 B 貼文，讓使用者覺得看到的資訊都是自己較有興趣的，而避免資訊爆炸的問題。

實際上，分群與關聯分析也可以整合在一起運作，例如：先找出關聯，再從關聯中建立特定的群組模式，避免分群常遇到群組過大而失去推薦價值的問題。另外社群網站在設計時，也不能完全只顯示他們認為使用者感興趣的資訊，必須偶爾穿插一些其他資訊，觀察使用者對這類資訊的反應，如此才能更加了解使用者，進而提升社群網站的資訊品質。

【高分命中】

- 1.金乃傑《資訊管理與資通安全》講義，第一回，頁32-34。

四、試說明與比較電子安全交易機制常用之 SSL (Secure Socket Layer) 與 SET (Secure Electronic Transaction)。(20分)

答：

SSL與SET的內容：

- 1.SSL (Secure Sockets Layer)：使用數位信封技術 (Digital Envelope)，以對稱金鑰加密傳送的文件，再用 PKI 將對稱金鑰加密，為目前最廣泛應用的網頁傳輸安全性協定，即 HTTP 加 SSL 等於 HTTPS。
- 2.安全電子交易協定 (Secure Electronic Transaction Protocol, SET)：在 Internet 上以信用卡付款方式的安全交易協定，是一個整合利用 PKI 與數位簽章機制，保護買賣雙方資料傳遞的隱密性、安全性與確認性。

茲將 SSL 與 SET 以表格比較如下：

	SSL	SET
目的	確保資料在網路上傳輸時不會被竊聽，進而避免資料遭到竄改。例如：在網路上輸入密碼時。	確保網路上的信用卡交易安全，並避免賣方不肖利用使用者信用卡資料。
主要使用者	任何在網路上需要加密連線，避免監聽的個別使用者或公司組織	網路上進行信用卡交易的個別使用者；網路賣家的網站 (做資料轉送)

	SSL	SET
使用時機	建立加密連線時。	使用者信用卡發卡銀行、賣家合作信用卡銀行。 網路購物確定貨品後，選擇線上信用卡付款時。
使用設備	使用者端：能SSL加密的應用程式，例如：瀏覽器、FTP用戶端、SMTP用戶端。 伺服器端：具有SSL憑證的伺服器（此憑證未必要透過第三方有效簽發，網站工程師可自行簽發）。	使用者端：能SSL加密的瀏覽器。 賣家伺服器：具有有效簽發SSL憑證的伺服器 銀行端：能進行SET交易流程的銀行伺服器。
提供的安全特性	1.機密性：使用IDEA、3DES、RC4 對稱性加密技術。 2.身分認證：使用RSA、DSA和數位簽章等公開金鑰加密技術。 3.完整性：使用MD5、SHA等雜湊為基礎的訊息確認碼。	1.資料完整性、機密性：使用DES作為付款資訊的加密處理方法，並且使用RSA作金鑰交換和數位簽章，SHA-1提供完整性服務。 2.身分認證、不可否認性：使用持卡者、商店的憑證及數位簽章進行不可否認的驗證，確認消費者、商家之身分的正確性。 3.機密性：採雙重簽署機制以便讓商家無法得知消費者卡片帳號資料，收單行無法取得消費者訂單資料。
處理流程	1.伺服器傳送自己的電子憑證。 2.使用者透過瀏覽器內建的CA公鑰驗證電子憑證中的數位簽章（身分認證性、伺服器不可否認性），並取出其中的伺服器公鑰（資料完整性）。 3.使用者瀏覽器產生隨機的對稱金鑰。 4.使用者使用該金鑰對傳送的文件加密（隱密性），並用對方的公鑰對該金鑰加密，再將兩者一併傳送給對方伺服器。 5.伺服器使用自己的私鑰解開使用者的對稱金鑰，再用該金鑰解開使用者傳送的文件。	1.商品結帳，選擇線上刷卡。 2.賣家伺服器將交易導向到合作的銀行的交易網站，買方在該網站上輸入卡號等資料。 3.合作銀行向買方發卡銀行確認信用卡資料。 4.買方發卡銀行回應信用卡有效性，並核准交易。 5.合作銀行發送訊息告訴賣家伺服器已核准交易。 6.賣家出貨，並印製發票給買方。 7.賣家定期向合作的銀行要求付款。 8.買家銀行寄出信用卡帳單要求買家繳交卡費。

實際上，SET必須要建構在SSL之上。因為使用者在賣家合作的銀行網站上輸入卡號時，其瀏覽器就會使用SSL連線，以確保卡號的傳輸不會被不肖人士從中攔截盜取。因此，SSL算是一種傳輸的技術，而SET則是搭配其他協定，變成一個完整的信用卡安全交易的解決方案。

【高分命中】

- 1.金乃傑《資訊管理與資通安全》講義，第三回，頁41-42。

五、網頁應用程式的檢查方式可以分為「源碼檢測」、「弱點掃描」與「滲透測試」等三種方式。試說明與比較此三者的區分。（20分）

答：

源碼檢測、弱點掃描、滲透測試可以為網頁程式找出不同層面的問題，以下分別描述再以表格比較三者差異：

- 1.源碼檢測：透過對原始碼的檢查，挖掘已知或未知的網頁問題。在開發流程中每一階段都需要源碼檢測完成，才能移至下一階段。近年來，採用流程相依檢視法（flow-sensitive），依程式控制流程與資料控制流程來發覺異常問題的進入點，針對這些進入點檢測程式是否已經處理。此類驗測是由使用者角度出發，所以驗收或稽核單位通常會採用人工與自動工具並行制。稽核員將程式碼送入自動工具中，針對產出報告中的弱點人工逐一驗證確認，然後再交由承包商修復復檢，以快速達到驗測目的。

【另有板橋、淡水、三峽、林口、羅東、逢甲、東海、中技、雲林、彰化、嘉義】

- 2.弱點掃描：著眼在環境與系統上的錯誤，除了網頁程式碼本身的問題之外，使用者設定疏漏與安裝環境的強固性也是最常被入侵的環節，因此需要弱點掃描。弱點掃描除了檢查已知的網站伺服器漏洞外，也會模擬惡意使用者的瀏覽行為，檢查受測程式的所有連結後，對所有可輸入的連結送出惡意數值，觀察記錄回應狀態。另外也會猜測所有隱藏目錄、管理後臺、程式備份檔或資料庫檔案位置。對於可登入的頁面，則進行密碼猜測的工作，以便檢測管理者的安全警覺性。弱點掃描由上層角度來找出整套系統的安全性，測試的出發點較為接近真實世界。
- 3.滲透測試：滲透測試所針對的目標是受測系統與所有大環境的運作，像是程式中的邏輯問題（而非程式問題）、系統運作流程瑕疵、社交工程漏洞等，都包含在滲透測試範疇內。也因此，滲透測試難以被工具取代，必須使用人力協助進行。滲透測試人員檢視整個系統的運作邏輯，來思索可能侵入的點。滲透測試人員將自己視為駭客，用異於常人的觀點來試探系統可靠度，從而找出所有潛在的威脅。

茲將源碼檢測、弱點掃描、滲透測試以表格比較如下：

	源碼檢測	弱點掃描	滲透測試
目的	檢測程式碼的安全性	檢測系統與執行環境上的錯誤	驗證所知弱點被駭的可行性
執行者	自動化測試系統或測試人員	弱點掃描工具	滲透測試人員
執行時機	開發流程中的每一階段	系統完成後	系統完成後
分類	白箱測試	黑箱測試	黑箱測試
測試範圍	程式原始碼	程式輸入輸出、伺服器配置	受測系統與所有大環境的運作，像是程式中的邏輯、系統運作流程瑕疵、社交工程漏洞等
成本	若為人工檢測成本高，自動檢測成本極低	極低	極高，需要專業駭客知識

【高分命中】

- 1.金乃傑《資訊管理與資通安全》講義，第二回，頁71、72及上課補充。

高點·高上高普特考 goldensun.get.com.tw 台北市開封街一段2號8樓 02-23318268

【中壢】中壢市中山路100號14樓·03-4256899

【台中】台中市東區復興路四段231-3號1樓·04-22298699

【台南】台南市中西區中山路147號3樓之1·06-2235868

【高雄】高雄市新興區中山一路308號8樓·07-2358996

【另有板橋·淡水·三峽·林口·羅東·逢甲·東海·中技·雲林·彰化·嘉義】