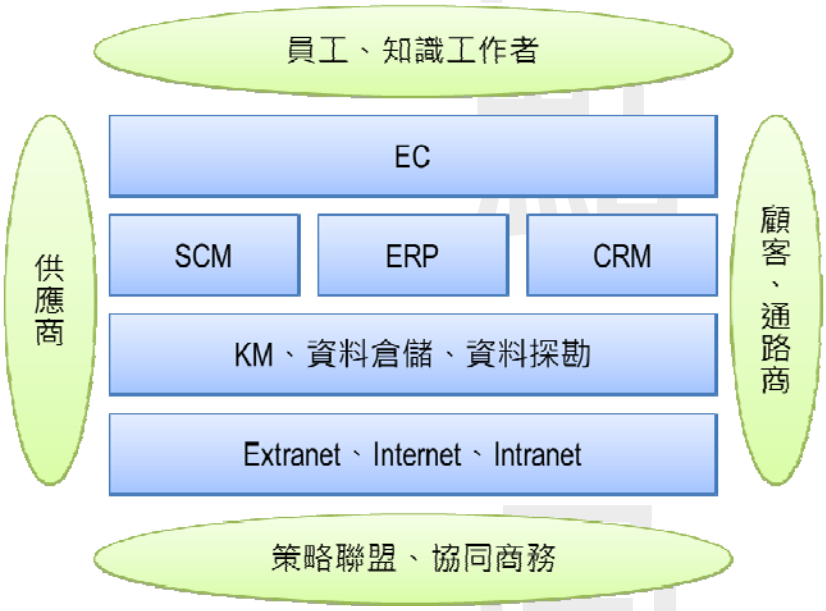
《資訊管理與資通安全》

一、數位化企業必備那四個資訊系統？（8分）請解釋此四個系統的功能。（12分）

試題評析	此題爲94地方特考相似題。雖題幹以較不常見的「數位化企業」稱之，但對有準備的考生而言實屬簡單，只要掌握各系統重要功能便能答得漂亮！
考點命中	1.《高點102年資訊管理與資通安全講義第三回》，金乃傑老師編撰，頁46。 2.《高點102年資訊管理與資通安全講義第二回》，金乃傑老師編撰，頁6、17、22、33、34。 3《高點102年資訊管理與資通安全總複習講義》，金乃傑老師編撰，考點6～9。

答：

(一)數位化企業是透過數位化的方式傳遞企業核心的商業關係。使用Internet、Intranet、Extranet及各種整合型的資訊系統，將企業內部的價值鏈與外部顧客、供應商、策略夥伴間的各種交易相關的活動。其核心架構如下圖所示：



在數位化企業中，透過SCM與供應商、CRM與顧客建立連結。內部使用ERP系統建立整合的運作環境，並透過KM輔助累積並分享企業知識，提升組織創新。

(二)以下說明SCM、CRM、ERP與KM四大系統之功能：

1.SCM：供應鏈管理（Supply Chain Management）系統，一個跨組織的模組化、整合性資訊系統，其主要功能在支援企業供應鏈相關主要活動的最佳化管理，並支援與上下游企業間相關供應鏈資訊的分享與協同作業。此系統依照功能可再細分爲供應鏈規劃與供應鏈執行兩部分：

(1)供應鏈規劃：提供供應鏈網路設計、生產規劃、倉儲規劃及配送規劃。

(2)供應鏈執行：支援供應鏈的交易執行，如追蹤實體貨物、倉儲、訂單履行、採購及運輸。

2.CRM：顧客關係管理（Customer Relationship Management）系統，企業從各種不同的角度來瞭解及區別顧客，以發展出適合顧客個別需要之產品或服務的一種企業程序與資訊科技的組合模式。顧客關係管理依其主要功能，可以分成行銷、銷售與客服三大模組：

(1)行銷：透過分析行銷與顧客資料，提供擷取潛在客戶與顧客資訊、提供產品與服務資訊、篩選潛在行銷對象，設計能滿足特定顧客需求及興趣的產品與服務。

(2)銷售：提供潛在銷售與聯絡資訊、產品資訊、產品結構功能與銷售報價功能，讓銷售人員將焦點放在最具獲利率、最佳產品銷售與服務對象的顧客身上。

(3)顧客服務及支援：透過分配與管理顧客服務請求的能力、網頁自助服務等功能與其他溝通工具，讓客

服中心、服務台與顧客支援服務人員更有效率。

3.ERP：企業資源規劃（Enterprise Resource Planning）系統，又稱企業系統（Enterprise System），電子化企業的後台骨幹。大型模組化、整合性的流程導向系統，整合企業內部資訊系統，快速提供決策資訊，提升企業的資源管理績效與快速反應能力。其六大功能模組包括：物料與庫存管理、生產與製造管理、銷售與訂單管理、財務會計管理、人力資源管理、企業行政管理等。

4.KM：知識管理（Knowledge Management）系統，組織實現知識管理的平台，其目標是透過將組織中的各種知識資源整合爲動態的知識體系，以促進知識創新，從而最終提高企業的核心競爭力。可依據知識的種類分爲三種系統：

(1)結構化知識系統：針對結構化知識，強調快速搜尋、正確性與易於了解。

(2)半結構化知識系統：針對數位化卻沒有標準格式的知識，加速應用的效率。

(3)知識網路系統：支援內隱知識，協助找尋專家或人與人的交流。

二、利用雲端運算（Cloud Computing）科技可以協助政府提升服務品質與效能。請列出SaaS、PaaS、及IaaS三種類型服務之中文或英文全名。（6分）並請分別舉例說明政府可以提供此三種類型之雲端服務。（14分）

試題評析	此題爲98年高考的相似題，相信考生對雲端的三層架構SaaS、PaaS、IaaS並不陌生。唯能掌握政府雲端建設分別設置在三層架構中的那些層次，並加以圖示補充，方能拿到高分。
考點命中	1.《高點102年資訊管理與資通安全講義第一回》，金乃傑老師編撰，頁29。 2.《高點102年資訊管理與資通安全講義第二回》，金乃傑老師編撰，頁52。 3.《高點102年資訊管理與資通安全總複習講義》，金乃傑老師編撰，考點2。

答：

(一)雲端運算是以網格運算技術，配合無所不在、隨選動態的網路，共享廣大的運算資源，可透過最少的管理工作及服務供應者互動，快速提供各項服務的一種服務模式。依照服務層次可分爲三層：

1.SaaS（Software as a Service）：軟體即服務，供應商將軟體放置於網路上，讓使用者透過瀏覽器直接使用。

2.PaaS（Platform as a Service）：平台即服務，供應商提供開發軟體與運作環境，讓使用者在其平台上開發服務。

3.IaaS（Infrastructure as a Service）：基礎建設即服務，供應商提供計算設備，讓使用者在其平台上部屬自己的環境。

(二)依照上文三層架構，政府可提供的雲端服務如下：

1.SaaS：

(1)政府施政計畫管理整合平臺建置計畫（GPMnet 2.0）：整合計畫管理服務，集中政府資訊以有效管理，全盤掌握中央對地方補助情形及地方執行成效，提供建置政府施政資訊管理儀表版（GPMnet Dashboard），使民眾更具系統的了解施政成果，並強化對各機關之施政的課責性。

(2)防救災雲端計畫：整合既有之防救災與消防資訊系統的潛勢資料、監測資料等，加上溪流坡地、重大建設、維生管線、房屋建物、戶籍人口等資料，搭配行動裝置、RSS、社交網路即時發布訊息，建立資訊共享服務。

(3)個人網路儲存空間服務：如雲端保管箱，提供民眾專屬個人網路空間以接收各機關遞送予民眾之政府行政文書（如：水電繳費通知單、罰單、稅費通知單等）。

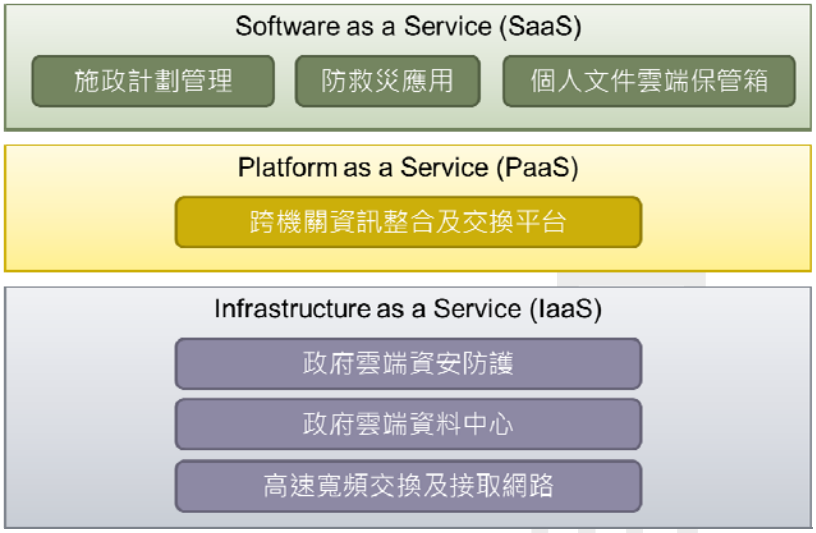
2.PaaS：跨機關資訊介接及交換，達成機關創新、資源減省、提升行政效能與厚植國內雲端產業發展之目的。以現有電子化政府服務平臺系統架構爲基礎，發展隨選即用及彈性擴充之能力，並因應未來跨機關業務主動通報服務、政府資料公開（open data）之需求，增建服務平臺服務元件。

3.IaaS：以政府機關基礎建設之經濟規模，提供網路、資訊安全防護、運算資源和儲存等的IaaS。

(1)雲端資安防護整合服務計畫：透過建立資安威脅情蒐雲端系統與服務、雲端協同防護資料交換標準及資訊事件處理與雲端鑒別技術服務，以完善資安情蒐與防護體系。

(2)政府雲端資料中心：提供機關用戶虛擬化的運算資源、儲存資源和網路資源，用戶無需採購、維護軟硬體，即可直接於基礎架構取得虛擬主機服務，建構各自平臺與應用。

電子化政府雲端服務平臺，架構如下圖所示：



三、國內剛施行的個人資料保護法（簡稱個資法）中規定，公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。可見公務機關人員必須對個資法及資訊安全管理有一定程度的了解。

（一）在個資法的規範裡，一般情況下有那五種特種個資不得蒐集、處理及利用？（10分）

（二）為防止個人資料被竊取、竄改、毀損、滅失或洩漏需採取技術及組織上的必要措施為何？（10分）

試題評析	此題爲個資法與資料安全的相關考題，其中第一子題需要對個資法有更深入的了解，能列出敏感性資料的內容，屬於記憶性題目；第二子題可使用資訊安全的角度切入，從「如何保護重要資料」去著手，並緊扣「個人資料」的主題，便能寫出不錯的答案。
考點命中	1.《高點102年資訊管理與資通安全講義第五回》，金乃傑老師編撰，頁68-69、82-83、99-102。 2.《高點102年資訊管理與資通安全總複習講義》，金乃傑老師編撰，考點26、28。

答：

(一)依《個資法》第6條指出，一般情況下不得蒐集之五種「敏感性資料」爲：醫療、基因、性生活、健康檢查及犯罪前科。

(二)依題意可將個人資料之竊取、竄改、損毀、滅失與洩漏分爲：機密性（竊取、洩漏）、完整性（竄改、滅失）與可用性（損毀）三類，其技術及管理措施整理如下：

1.通行密碼：保護「機密性」。使用者在存取個人資料時，系統必須提供通行密碼等驗證機制，以確保使用者有足夠的權限可以檢視這些個人資料，避免個人資料暴露於未授權的使用者前。另外透過密碼也可以達到「身分認證」與「不可否認」等資安的其他特性，確保個人資料的修改是在授權下進行，並透過稽核機制紀錄修正的過程以發揮「可責性」。

2.加密技術：保護「機密性」。對個人資料的儲存、傳送過程進行加密，例如：以SSL保護傳輸過程不受駭客監聽，並透過加密檔案系統儲存重要的個人資料，避免被機器上的其他使用者存取。另外，在存入資料庫前，也可以先行加密，避免資料庫帳號密碼遭到破解時的所有個人資料傾瀉而出。

3.數位簽章：保護「完整性」。透過數位簽章可以確保資料傳輸過程中沒有被竄改，因爲數位簽章中使用訊息摘要（Message digest）技術，透過雜湊演算法驗證訊息是否有被竄改過。另外，由於數位簽章使用PKI的架構，故如同個人密碼可以驗證身分，達到身分認證與不可否認性的保障。

4.資料備份：保護資料的「可用性」。避免因天然或人爲災害使系統故障而使得個人重要資料損毀。例如：採用異地備援，當機房燒毀時仍然可以從外地的儲存中心將資料救回，減少損失。

5.備援系統：保護資料的「可用性」。採用負載平衡或RAID等機制，確保不會因爲機器故障或流量高時阻斷或損毀了個人資料的存取。

6.執行資訊安全管理系統：資訊安全管理系統爲組織資訊安全管理的最高守則，其中包括11個安全控制領域、39個控制目及133個控制措施。執行時透過PDCA模式，用以建立、實施、操作、監督、維護並持續改進組織的資訊作業安全。

四、阻絕服務攻擊（Denial of Service, DOS）是目前最常見的網路攻擊行為之一，駭客透過各種方式把目標主機的網路資源及系統資源耗盡，使之無法提供正常的服務。

（一）請求氾濫攻擊（SYN Flooding Attack）是DOS常見的攻擊手法之一，請描述該攻擊的攻擊方式及過程。（8分）

（二）來源位址欺騙攻擊（Land Attack）是利用IP欺騙（IP Spoofing）的方式讓封包中的來源位址與目的地位址都是被攻擊目標主機的IP位址，使得目標主機收到封包後因無法回應訊息給自己而導致服務阻斷。請問何種安全通訊協定可用來鑑別IP來源位址的正確性？（4分）並簡述其運作過程。（8分）

試題評析	此題爲網路安全的題目，技術性質較高，若沒有相關經驗，很難回答。但相對而言較不需要作答技巧，只需要依照題意回答相關問題即可。
考點命中	1.《高點102年資訊管理與資通安全講義第四回》，金乃傑老師編撰，頁74及上課筆記。 2.102年高點‧高上《考前30分鐘好題神》，金乃傑老師編撰，考點27及上課筆記。

答：

(一)SYN Flooding是一種利用TCP三向交握（Three-way Handshake）協議缺陷，發送大量僞造的TCP連接請求，使被攻擊方的CPU或記憶體超過負荷的攻擊方式。三向交握流程爲：

1.用戶端發送一個SYN即同步（Synchronize）訊息，指明用戶端使用的連接埠以及TCP連接的初始序號。

2.伺服器在收到用戶端的SYN後，將回傳一個SYN+ACK的訊息，表示用戶端的請求被接受，同時TCP序號被加一，ACK即確認（Acknowledgement）。

3.用戶端也回傳一個確認訊息ACK給伺服器端，完成連線。

SYN Flooding的方法是發送大量的SYN訊息，此時伺服器會以SYN+ACK回應，但攻擊者就不再回覆確認的SYN訊息。一般而言伺服器會在30秒到2分鐘內重試回應訊息，這種等待與發送回應訊息就會佔用伺服器的系統資源，如果同時有數以萬計的要求時，伺服器便會無法負荷，造成無法回應正常連線的使用者而使得服務被阻斷。

(二)來源位址欺騙攻擊：

1.在IPv6協定中，使用IPSec的表頭確保來源位址的認證性。其中具有確認來源合法性的表頭有：IP Authentication Header（IP AH）及IP Encapsulating Secure Payload（IP ESP）。

2.AH標頭（RFC 2402）提供欄位的完整、認證及不可否認性。完整是指能夠判斷封包的資料是否有被更改，而認證及不可否認性則是能讓使用者可以認證對方的身份，同時也不能否認使用者曾經做過的行爲。此外，AH 的機制可以抵擋匿名的攻擊（spoofing attack）以及重播的攻擊（replay attack）。以下說明其運作流程：

(1)透過金鑰交換協議使傳送端與接收端擁有相同128位元的工作金鑰。

(2)傳送端利用金鑰計算整個封包的雜湊函數值（訊息摘要，Message Digest），然後將訊息摘要附在封包內的AH表頭中，一起送給接收端。

(3)接收端使用相同的金鑰計算封包資料的訊息摘要並與傳送端的訊息摘要比對，若兩者相同代表封包表頭沒有被修改過。

五、由於HTTP協定並未考慮到資料在傳遞時可能遭遇的安全問題，所以線上電子商務服務常用SSL（Secure Socket Layer）安全傳輸協定來確保瀏覽器與Web伺服器間資料傳遞的安全。

（一）SSL安全傳輸協定屬於TCP/IP通訊協定中那一層的服務？（4分）

（二）使用者如何辨識連結的網頁是否為SSL保護的網頁？（4分）

（三）請簡述SSL安全通訊協定能提供線上電子商務服務那些安全需求？（12分）

試題評析	此提議爲資訊安全的題目，專注於SSL的細部特性，屬於101年普考的相似題。其中第一子題屬於網路的部分，只要依照題意簡單回答即可得分；第二子題屬於SSL的使用細節，但若有上網經驗，應爲送分題；第三子題屬於考古題內容，考點是SSL所能提供的安全性。若要得到高分，除了要能指出所有的安全特性外，還必須要加以文字解釋。
考點命中	1.《高點102年資訊管理與資通安全講義第五回》，金乃傑老師編撰，頁83。 2.《高點102年資訊管理與資通安全總複習講義》，金乃傑老師編撰，考點28。

答：

(一)SSL（Secure Sockets Layer）：SSL採用PKI技術，確保應用程式間通訊的機密性和可靠性，讓用戶端與伺服器之間的通訊不被攻擊者竊聽，爲網際網路上保密通訊的工業標準。現行Web瀏覽器亦普遍將HTTP和SSL相結合，從而實現安全通信。其屬於TCP/IP協定中傳輸層（Transport layer，爲第三層）中的協定。

(二)使用者可以透過瀏覽器的網址列顯示的資訊來辨識。如果網址列中網址是以「https」開頭，則表示透過SSL加密的連線。另外常見的瀏覽器，如Google Chrome、IE…，也會在網址列用協定處以綠色顯示（相對爲白色），強調爲安全的連線。此外，使用者也可檢視網頁資訊，檢視伺服器所使用者憑證。

(三)電子商務的需要「機密性（Confidentiality）」、「完整性（Integrity）」、「身分認證性（Authentication）」與「不可否認性（Non-repudiation）」等四項安全機制，而SSL可以滿足的需求如下：

1.私密性：透過IDEA、3DES、RC4等對稱金鑰加密技術，可以確表資料在傳輸過程中不會被竊聽而洩漏，因此可以保護電子商務交易中的信用卡卡號、買賣物品內容、買家基本資料…等機密資料。此功能也是SSL最重要的功能。

2.完整性：在訊息傳遞時，SSL提供MD5、SHA等雜湊演算法爲基礎的訊息確認碼，確認訊息在傳輸過程中是否有被竄改。這些雜湊的訊息摘要演算法，只要資料中任一個bit被改變，都會產生出完全不同的訊息摘要（驗證碼），因此可以確保資料未受竄改的完整性。

3.身分認證：SSL雖然無法分辨用戶端電腦與使用者的身分，但由於伺服器要提供SSL連線時必須要跟CA申請數位憑證，架構建立在公開金鑰基礎建設（PKI）下。基於PKI，伺服器的身分都要經過CA驗證，因此可以讓使用者確保進行交易連線的伺服器就是真正的交易對象，他人無法冒名與使用者交易。