《資訊管理與資通安全》

一、(一)請敘述美國國家標準與技術局（NIST）定義「雲端運算(Cloud Computing)」的「五大重要特徵（Five Essential Characteristics）」之意涵。（10分）
(二)分別由財務、技術與維運三個面向來剖析雲端運算如何影響成本以及對企業帶來的優勢。（15分）

試題評析	本題為雲端運算的基礎考題，不同於以往的是明確指出「五大特色」，且從指定的面向說明如何影響成本及優勢。由於第一小題為基本考點，只要有準備應不難應答；而第二小題必須從「成本面」指出其為企業帶來之效益，可從雲端運算的三層服務模式切入，針對各層次可以減少哪些成本敘寫，亦屬容易拿分的題目。若篇幅完整，敘寫具邏輯，程度中等的考生要拿到滿分並非難事。
考點命中	《高點資訊管理與資通安全講義》第一回，金乃傑編撰，頁20-22。

答：

(一)雲端運算指使用平行處理、網路運算、虛擬化等技術，將網路上眾多電腦連結而成超級電腦，在使用者有需要時能夠透過網路立即取得高彈性擴展性的網頁應用程式、網站平台、儲存空間或硬體資源的服務。根據美國NIST定義的五大重要特徵說明如下：

1.資源匯集（resource pooling）：服務者所提供的計算資源，例如：儲存空間、網路頻寬、計算能力、虛擬機器數量等，可類比為一個大水池，能隨時依需要分配給不同平台的多個使用者。使用者不需了解資源的實體位置（如資源是在哪個國家或什麼資料中心）或技術細節，只要知道網址來連線即可。

2.彈性、擴展性高（rapid elasticity）：能因應要求調整資源規模大小，對消費者而言，雲端似乎無窮無盡，且能依據需求增減運算能力採購額。

3.隨選自助（on-demand self-service）：消費者可以依其需求索取計算資源（如伺服器或儲存空間），且整個過程是單方面自動化的，無須與資源提供者互動。

4.隨處網路存取（broad network access）：網路使用無所不在，亦即雲端供應者服務可隨時在網路取用。

5.計算為服務（measured service）：各層次均由雲端供應者掌控與監管，以進行計費、存取控制、資源優化、處理能力規劃及其他工作。

(二)以下從財務、技術與維運三個面向說明雲端運算影響成本及對企業帶來的優勢：

1.財務面：相較於自行開發系統會因為人力、工作進度使成本難以估算，透過雲端運算的SaaS就如同購買套裝軟體，可以明確地掌握成本，值得一提的是雲端運算具有「根據使用量計費」的特性，根據使用期間、CPU使用率、儲存空間使用率等因子計費，並且提供短期租賃（最短的租約可以到1小時），比套裝軟體在成本控管上更有彈性。而雲端運算的PaaS及IaaS也可以免去建構機房、購買伺服器等級設備及設備安裝、維護、更新等資源獲取與管理成本，都能為企業降低初期營運投入的沉沒成本，讓企業專注在服務開發，強化核心能力。

2.技術面：不同於自行開發新系統必須讓員工（開發者）學習掌握新的技術，採用雲端運算如同「委外」，可以快速獲取國際上頂尖主流的技術，包括效能更好的演算法、安全性較高的軟體程式或更優秀的商業流程。因為雲端供應商有專業的開發團隊，並要接受國際市場的挑戰，在技術上常處於領先地位；且雲端運算因透過網路提供服務，會比委外開發的系統有更好的更新彈性，服務提供者只要在後台修改即可立刻完成更新。採用雲端運算除了可以降低學習新技術的成本，更能大大降低套用新技術失敗時的成本風險。企業快速獲取新技術，亦能提升企業之競爭優勢。

3.維運面：在企業的日常營運上，使用雲端運算可以有效管理分散在世界各地的資料，例如：一個組織有位於日本、台灣、美國的專家，可以透過雲端運算儲存各地專家的分析資料，並藉由雲端運算「資源為池」的特性，自動同步資料減少協同作業的溝通成本；另外，雲端運算的分散式運算優勢可以使企業獲取強大的運算能力，進而進行資料探勘或OLAP分析，找出潛在且有價值的知識，例如：擬定行銷策略、改善供應鏈規劃，甚至找到有價值客戶，以有效降低營運成本並提升獲利能力。

二、何謂「政府資料開放（Open Government Data）」？根據資料的「使用」、「散布」與「分享」說明其特性。政府資料開放有何重要性？請舉例說明之。（25分）

試題評析	本題詳細考「政府開放資料」的概念，乍看分為三個問題，但實際上定義與特性應配分10分，而對政府之重要性則佔另外15分。同學在答題時需要謹記開放資料的原因（提高政府及資料的透明性），使用上有何限制（似Open Source）以及能舉出實際的應用。由於題目靈活度高，較無所謂的標準答案，因此如同第一小題，若能敘寫豐富有條理，應都能夠拿到不錯的分數。
考點命中	《高點資訊管理與資通安全講義》第一回，金乃傑編撰，頁54。

答：

(一)將資料開放給任何人自由出版、使用，不該索取費用且不受著作權、專利權，以及其他管理機制所限制。而「政府資料開放」(Open Government Data)使用開放資料的精神，為滿足民眾資料使用需求，及促使跨機關資料流通增進施政效能，並強化民眾監督政府的力量。其內容為各機關職權範圍並依法做成的電子資料檔案，包括文字、數據、圖片、影像、聲音……，以開放格式於網路公開，提供個人或組織使用。政府資料開放可結合民間創意，活化政府資料應用，進一步提升政府資料品質及價值，進而創新政府服務。根據使用、散布與分享說明特性如下：

1.使用：各機關依作業原則規定，於政府資料開放平台集中公開列式之資料，以「無償」及「非專屬授權」方式提供使用者得不限時間、地域，並可對資料重製、改作、編輯、公開傳輸或開發各種產品或服務，無須取得資料提供機關之授權（不包含商標權及專利權）。但未經資料來源主管機關事前書面同意，不得將資料再開放授權或交付予第三人以任何方式使用。

2.發行：公開發行、公開展示或其他利用開放資料產生之加值衍生物，應以適當方式清楚註明資料來源主管機關，在開放第三人使用時則無須經主管機關同意，但不得違背現行法令、有違公序良俗、有誤導社會大眾或其他不當行為。資料來源主管機關如於資料集註明另訂使用規範或收費標準者，應依其規定辦理。

(二)開放資料之重要性舉例說明如下：

1.促使機關資料流通，提升施政效能：資料開放可以減少部門運作所需的經費，降低每日例行事務處理的成本。例如荷蘭教育部以往需要花費大量的人力時間在處理民眾的詢問，但在提供開放資料後，將所有相關的資料放在網路上，民眾就可以直接在網站找到答案，有效減少處理業務。另外某些國家也會使用類似維基百科的概念，透過開放資料將部份工作分配給人民團體或組織完成，如此亦能提高政府運作效率。

2.強化民眾監督政府的力量：透過開放資料，民眾能更有效監督政府運作，了解政府是否善盡管理責任，任制提昇人民參與公眾事務之意願。例如：英國開放資料網站「where does my money go（我的錢到哪）」，利用政府開放資料，將政府使用人民繳納稅金如何分配整理出來，甚至可以查出舞弊的情形；而丹麥的folketsting.dk網站提供追蹤國會動態，讓民眾清楚知道目前提出和審查的法案有哪些，以及民意代表們對這些法案的態度。

3.活化政府資料應用，創新政府服務：19世紀時已有使用政府資料改善生活的例子，倫敦的斯諾（Snow）博士將霍亂造成的死亡人口分布與飲用水的水井位置作結合與分析後，發現飲用水的污染與霍亂的關係，因此將現代化的地下污水處理系統引入倫敦，改善市民的整體健康狀況。現在，丹麥的husetsweb.dk網站利用政府的地籍資料、商業登記資料及政府補貼政策的相關資訊，協助民眾找到合適的房子，並檢視房屋的能源報告，以優化能源使用並尋找合適的資源提供者。

開放資料除了可以提升政府的內部運作，亦能增進人民參與，並藉由公眾的創意來改善全體社會的生活。

三、(一)在「網路鑑識（Network Forensics）」中，蒐集「網路數位證據（Network Digital Evidence）」是重要的一環。詳細分析存在於客戶端、伺服器端以及網路設備的網路數位證據，並舉例說明。（15分）

(二)分析「瀏覽器」與「網路數位證據」之關係。（10分）

試題評析	本題為數位鑑識，雖然數位鑑識不算新考點，但本題的細緻度較高，且如同第一題給定明確的答題方向。在答題前必須了解何謂數位證據，以及數位證據可以如何被儲存、鑑識。題目中要求考生詳加說明客戶端、伺服端與網路設備的數位證據，擬答時宜先列舉，再透過例子來使答案更具有內容。另外，也可搭配指出數位證據存在這些地方對鑑識時的優劣，提高答案價值性。第二小題則重點在瀏覽器會「儲存」哪些使用者資訊，其主要即是所謂的Cookie，可以從使用者瀏覽網頁會經過哪些操作來切入說明。若能掌握切入重點，則此題必定能拿到超過一半以上的分數。
考點命中	《高點資訊管理與資通安全講義》第四回，金乃傑編撰，頁117-118。

答：

(一)以下就存在於用戶端、伺服器端及網路設備的數位證據說明：

1.用戶端：用戶端是終端使用者使用之裝置，如智慧型手機、平板電腦、筆記型電腦或桌上型電腦等，而數位證據位於其中的儲存媒體（硬碟、記憶卡）或記憶體中。舉例而言，儲存在儲存媒體中的資料如瀏覽器的瀏覽紀錄、儲存的Cookie、通訊軟體的對話紀錄、圖片、照片或Word文件、Excel報表等；另外儲存在記憶體中的裝置執行狀態，如登入的使用者、執行中程式的資料。在用戶端的資料量最多、容易取得且相關性最高，但常可能受到使用者修改或清除，因此在資料的復原上挑戰最大。

2.伺服器端：伺服器為提供服務的電腦主機，讓使用者透過網路連線取得資源。數位證據儲存在伺服器的記錄檔（Log），根據提供的服務不同，可能留下的數位證據也不同。以網頁伺服器而言，會儲存使用者的點擊串流（clickstream）、瀏覽時間、IP位址、留言內容，若該伺服器為電子商務網站，也會保留使用者的個人基本資料、交易紀錄、瀏覽商品紀錄等。在伺服器的蒐證上，若伺服器由第三方架設，通常可以提供品質高的詳細紀錄，適合做為證據；但若為蒐證對象架設，則難度與用戶端相同。

3.網路設備：如路由器、交換器、防火牆等設備，通常記錄使用者的封包資訊，掌握使用者封包方向、內容。網路設備與前兩者的不同是將大部分的資料儲存在記憶體中，在斷電後即會失去，因此在數位鑑識時必須使用特殊儀器保留設備中的狀態資料。而在資料正確性上，由於這些設備並非終端節點，因此難以變造，真實性高且包含最多原始資料，若能有效利用整理，可以是最即時最詳細的資料來源。但由於網路設備的限制，若蒐集時間過短，可能難以掌握資料內容，且在資料關聯性上難以辨認，若使用者透過加密傳輸（如SSL），則擷取還原的機率極低。

(二)瀏覽器為使用者檢視網站資料時使用的應用程式，其功能是將原始的HTML、JavaScript、CSS等網頁程式碼轉換成圖像的畫面，並提供使用者直接以滑鼠、鍵盤操作網頁元件，並與後端伺服器互動。主流的瀏覽器如Google Chrome、Internet Explorer、Mozilla Firefox等。以下說明使用者使用瀏覽器連結社交網站時可能留下的數位證據：

1.在網址列輸入網址：留下「瀏覽紀錄」，包括瀏覽的時間、瀏覽頻率等紀錄。

2.登入輸入帳號密碼：有些網站會提供勾選「記住我」的功能，透過Cookie記憶使用者的登入帳號，讓使用者可以在下次時不要再輸入帳號密碼，而Cookie就是由瀏覽器管理紀錄，而成為數位證據。

3.記住密碼：登入完成後瀏覽器會跳出「記住密碼」選項，若勾選則網址、帳號與密碼就會被記錄在瀏覽器中，成為數位記錄。

4.瀏覽網頁：當使用者點選超連結時，瀏覽過的網頁一樣會出現在「瀏覽紀錄」中，並建立在網路設備及伺服器中的數位證據；若網頁中有廣告，則廣告會在瀏覽器中建立第三方的Cookie，追蹤記錄使用者的操作行為。

5.留言、打卡或按讚：使用者透過瀏覽器操作網頁，當發送這些網頁request時，則會透過瀏覽器將資料發送到伺服器上，而在伺服器上產生數位證據。

此外，除了瀏覽紀錄，瀏覽器的「快取」功能也會產生數位證據。快取功能會將看過的網頁、圖片等資料暫存，以加速網頁呈現或在斷線時提供瀏覽。若能取得快取資料，也可以更完整的還原使用者看過的畫面。

四、(一)何謂「數位憑證（Digital Certificate）」？數位憑證有那些種類？分別說明其用途。（15分）

(二)試說明數位憑證在設計「Diffie-Hellman金鑰交換協定（Diffie-Hellman Key Exchange Protocol）」的用處。（10分）

試題評析	第一小題要求考生指出數位憑證的種類，其種類為根據主要使用角色的不同來分類，因此僅需要對分類以例子舉出可能應用即可；第二小題則考SSL背後所使用的演算法，為具有標準答案的題目，因此必須平常有接觸或有專門學習過該領域，不然很難作答。本題實為新考點，故程度中等的同學若感覺難以做答不必太過焦慮。
考點命中	《高點資訊管理與資通安全講義》第四回，金乃傑編撰，頁26-27、33-37。

答：

(一)數位憑證：又稱為電子憑證，是一種用於電腦的身分識別機制。合法的憑證是由憑證機構（如政府、Verisign、Thawte Consulting…等）所頒發，代表確認申請者的身分，此申請者不是冒名的。根據X.509的規範，數位憑證中包括版本、序號、簽章演算法、憑證發行者、有效期限、憑證持有人、持有人公開金鑰、上述各資料之簽章。數位憑證根據用途主要可分為3種，說明如下：

1.個人數位憑證（Personal Certificate）：提供個人識別/證明身分之用，例如：在收發電子郵件時加上數位簽章確認發信者身分，或在進行線上交易時證明購買者身分，達到交易的不可否認性。常見的個人數位憑證如自然人憑證。

2.伺服器數位憑證（Server Certificate）：代表伺服器的身份，提供瀏覽器檢視驗證。另外若伺服器要建立SSL加密連線，瀏覽器就會從伺服器數位憑證中取得伺服器的公開金鑰，並用伺服器的公鑰對傳遞給伺服器的訊息加密。

3.物件數位憑證（Object Certificate）：代表程式碼的身分，以確保程式碼在傳遞或產生的過程中沒有被修改。主要應用於使用者在網路上下載程式檔案，在安裝前電腦便可以針對程式的簽署者及程式的內容是否遭竄改進行檢查，如果程式未受到合法單位簽屬，在安裝時便會跳出警告，以提醒使用者安裝此程式可能帶有風險。

(二)Diffie-Hellman金鑰交換協定：簡稱D-H，是SSL金鑰交換時重要的演算法基礎，為一種安全協定。其主要概念是訊息傳遞者取得訊息接收者的公開金鑰，並用公開金鑰加密傳送接下來真正要對其他資料加密的對稱金鑰（交談金鑰，Session Key）。此演算法之價值如下：

1.解決非對稱金鑰加解密效率差的問題：因對稱金鑰演算法複雜，在加解密時效能較差。但D-H最後使用對稱金鑰作加解密，效能較高。

2.解決非對稱金鑰加密後密文過長：非對稱金鑰加密後密文長度通常遠比原文長，增加網路傳輸流量。

3.解決對稱金鑰金鑰交換弱點：對稱金鑰因為必須要對方也能將密文解開，一定有交換金鑰的動作，而交換金鑰也是對稱金鑰最脆弱的地方，因為在交換過程中一但被截取，則其後所有的密文都會被破解。但使用D-H演算法，先以非對稱金鑰對要交換的對稱金鑰加密傳送，可以有效避免擷取的問題。