《資訊管理與資通安全概要》

一、請說明資料（Data）及資訊（Information）的定義，並說明如何評估資料品質（Data Quality）？（25分）

試題評析	此題分成兩部分，前半部資料與資訊的差異為資訊管理的基本題型，同學只要有基本認知即可完整作答。第二部分為資訊品質的評估，這部分學者有各自的看法，同學在答題上要盡可能統整出一個完整的答案，如範例答題所示，除此之外，各指標的大分類一定要清楚明確地寫出，例如：「資料正確性」、「即時性」……等，透過大項再去細分明確的指標，才可以獲得較高的分數。
考點命中	《高點‧高上資訊管理與資通安全講義》第一回，蕭老師編撰，頁3-4。

答：

(一)1.資料（Data）：未經處理的原始記錄，缺乏相關性的事實，無本質上的意義。

2.資訊（Information）：經過有系統性的整理、分析……等，變成具有相關性且可從中獲得可以作為判斷或行動的依據。

Michael H. Zack (1999) 認為，「資料」是從相關情境（Context）中獲得的事實和觀察，本身並無直接意義，將資料放在某個有意義的情境之中所獲得結果就是「資訊」。

(二)根據學者馮容莊整理之資料品質可以透過以下的指標來判定：

資料正確性	涵蓋性指標	對所提供的資料能針對參照母群體有明確的說明，確認且紀錄資料來源不足或在事前定義的範圍中超過比例（超出可接受範圍），以及資料的架構可與外在及獨立資料庫比對。
	獲取與收集指標	所謂「獲取」是指資料輸入乃依據有用性資料架構，且符合資料供給者的角度。所謂「收集」是指不同的資料提供者將資料輸入雷同資料庫中。
	單位無反應	當某單位的資料在資料庫內完全不存在或遺失。
	部分無反應	當匯入的資料中有部分資料項目缺少則稱為部分無反應。
	測量錯誤	所得資料的數值與其真正價值的附合性，亦即資料效度（validity）的檢視。
	校正與責咎指標	所謂「校正」是指將空白資料確認其是屬錯誤（incorrect）或遺失（missing）的一種過程。所謂「責咎」則是指對一些不正確或遺失的資料，以特定數值替代的過程，以使在編輯過程中不會被以空白或"零"資料認定。
	處理與概估指標	所謂「處理」是指對某一資料庫的資料為任何一個特定目的所執行的檢視程式或流程之過程。所謂「概估」是指資料集合所呈現的價值能表示參照群體的特性與情況。
即時性	資料釋出即時性	其測量方式是計算資料釋出時間與最後一次的時間點差距，其差距越短表示所釋出的資料呈現越接近目標。
	資料紀錄即時性	維持高品質的資料紀錄最重要的一點是，當使用者取用或彙集資料其資料是具有效用的。
比較性	連結指標	當在使用資料連結時應有隱私與保密指引，其內容包括應用地理分類標準、資料收集使用一致性的標準，以及資料編碼具一致性。
	均等指標	指資料可從一種表格對應到任何一種格式。
有用性	可近性指標	當資料用於分析或製作報告時應儲存於安全的檔案中，且作為未來參照之用。根據資料使用者的目的與需求，資料可以不同的格式與版本建置出來。

	紀錄指標	資料紀錄主要是提供使用者充分的資訊，同時亦可了解資料的品質狀況是否符合其使用的需求。
	解釋力指標	資料的結構設計與潛在性限制是影響資料解釋力（詮釋）的因子。
相關性	適應力指標	指它是否能根據使用者的需要，對現存的或未來資訊的位置設定有足夠的彈性或明確的界定。
	價值性指標	所謂資料庫的「價值性」意指其對系統的知識或應用的貢獻度。

二、請分別說明自由軟體（Free Software）與開源軟體（Open Source Software）的定義及特性，並比較它們之間的差異性。（25分）

試題評析	此兩個概念是一般人容易搞混的，只要針對基本概念闡述，即可輕鬆應對此題，若同學在考場中一時分不出來，只要思考相對應的範例即可闡述出兩者的差異性。

答：

(一)自由軟體（Free Software）：根據自由軟體基金會的定義，是一類可以不受限制地自由使用、複製、研究、修改和分發的，尊重用戶自由的軟體，這方面的不受限制正是自由軟體最重要的本質。自由軟體受到選定的「自由軟體許可協議協議」保護而發布（或是放置在公有領域），其發布以原始碼為主，二進位文件可有可無。

(二)開源軟體（Open Source Software）：又稱開放原始碼軟體，是一種原始碼可以任意取用的電腦軟體，這種軟體的著作權持有人在軟體協定的規定之下保留一部分權利並允許用戶學習、修改以及以任何目的向任何人分發該軟體。

(三)開源軟體與自由軟體是兩個不同的概念，只要符合開源軟體定義的軟體就能被稱為開源軟體。而自由軟體有比開源軟體更嚴格的概念，因此所有自由軟體都是開放原始碼的，但不是所有的開源軟體都能被稱為「自由」。但一般絕大多數開源軟體也都符合自由軟體的定義。開放原始碼的規定較寬鬆，而自由軟體的規定較嚴苛。

三、假設你是某機關的網管監控人員，當你發現系統網站突然流量激增，系統服務受到重大影響，初步判斷可能遭受分散式阻斷服務攻擊（Distributed Denial of Service，簡稱DDoS），請問你該如何處置？（25分）

試題評析	此題為情境題，預防DDoS的方法非常多，如果此題只針對預防方法闡述，則分數不高。重點為需要站在題目所描述的「網管人員」立場來答題，除了一般的預防方式外，也要思考網管人員一般情況下要如何查看可疑流量與時常的預防方法。
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73。

答：

(一)網管人員可以透過以下方法來查看與避免：

定期查看 Log 檔案，看有無可疑 IP 流量。

1.避免下載網路上未經授權的軟體與檔案。

2.時常更新電腦與防毒軟體版本。

3.個人電腦也需要安裝相關防毒軟體。

(二)網管人員可以用以下設置方法來阻擋：

1.防火牆：可以透過規則的設定，允許或拒絕特定通訊協定或是 IP 位址，當發現攻擊是從少數不正常的 IP 位址發出時，可以有效阻止該 IP 所發出之攻擊。

2.複雜攻擊難以用簡單規則來阻止，此外，防火牆可能處於網路架構中過後的位置，路由器可能在惡意流量達到防火牆前即被攻擊影響。然而，防火牆能有效地防止用戶從啟動防火牆後的電腦發起攻擊。

3.雲端流量防護：將流量先送到 DDoS 防護中心中的軟體處理，將正常與惡意流量分離，即可讓真實的用戶存取服務，系統也可以避免惡意之攻擊。

4.路由器：啟動入口過濾（Ingress filtering）防止路由器傳送來源地址跟收到介面不符的封包。但無法阻止在相同網路上的機器發起欺騙攻擊，可防止機器對外部網路發起欺騙攻擊。

5.入侵防禦系統：入侵防禦系統（Intrusion-prevention systems，IPS）對於特徵明顯攻擊是可以有效防禦的。但是攻擊趨勢已轉向為以合法流量掩飾非法行為的攻擊方式，對於此類的攻擊 IPS 的防禦顯得不足。

四、何謂電子簽章（Electronic Signature）？經由密碼學演算法（Cryptographic Algorithm）產生的電子簽章將具備那些特性？（25分）

試題評析	此題為基本的資訊安全類考題，同學只要特別注意電子簽章與數位簽章之差異即可。第二小題的特性直接以數位簽章特性回答即可獲得高分。
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62-63。

答：

(一)電子簽章（electronic signature）是指以電子形式存在，依附在電子文件並與其邏輯相關，可用以辨識電子文件簽署者身分及表示簽署者同意電子文件內容。

(二)具有以下特性：

1.完整性（Integrity）

資料內容僅能被合法授權者所更改，不能被未經授權者篡改或偽造。資料完整性必須要確保資料傳輸時，不會遭受篡改，以保證資料傳輸內容的完整性，可用來確保資料傳輸過程中，不會被駭客篡改及偽造，以確保資料之完整性。

2.不可否認性（Non-repudiation）

確保網路交易的雙方無法否認曾進行過的交易、或通訊參與的雙方皆無法否認曾進行資料傳輸或接收訊息。公開金鑰基礎架構（Public Key Infrastructure, PKI）對使用者身分及訊息來源做分別的鑑別方法，以達權責歸屬及不可否認性。

3.鑑別性（Authentication）

(1)訊息來源的鑑別

能確認資料訊息的傳輸來源，以避免有惡意的傳送者假冒原始傳送者傳送不安全的訊息內容，一般利用電子簽章或資料加密等方式來解決訊息的來源鑑別問題。

(2)身分鑑別

系統要能快速且正確地驗證使用者身分，為了預防暴力攻擊者的惡意侵犯，對於使用者身分鑑別的時效性比起訊息驗證要來得嚴謹。