計算機概論【資訊管理與資通安全】試題解答

王道　老師提供

一、答：

（一）訊息公私混雜，拖慢工作效率

公務／私用訊息平台，必須分開！利用社交通訊軟體作為公務通訊軟體所碰到的第一個問題即是員工易被私人訊息干擾、或是被廣告訊息吸引，員工被迫處於無法專心的工作環境。其次，當員工需要傳遞公務資料時，可能會不小心傳到私人群組中，導致不慎機密外洩的狀況。若能由管理者發起，員工群起響應，鼓勵分流「公務」及「私用」通訊軟體，打造能專心處理公務的通訊環境，更可有效加速企業營運效能。

（二）任務交辦不明確，易有漏辦事項

由於缺乏適合的訊息回溯功能，使用社交型即時通訊，常需要花很多工作時間翻找舊訊息，才能從每日密密麻麻的對話中找到新增的工作任務，很容易造成零碎事項的疏漏，甚至無人負責的情況。而公務即時通訊可以幫助您在閱讀訊息的同時，就幫訊息「折角」，之後只要搜尋有被「折角」的訊息就可快速掌握任務數量。

（三）對話訊息（及檔案）的保存期限不夠長

工作溝通常需一併傳輸文件、照片、或圖片檔案，且檔案總是會有更新版。一般的通訊軟體常有檔案過期無法下載、或是找到的版本不正確的情況發生，造成事後追查的溝通誤會，無形間導致整體效率降低。而工作上專用的即時通訊，需可更長期的保存舊訊資料，包含文檔、圖片、或影片，所以員工可放心傳送重要公務檔案，不用擔心檔案保存期限過短，臨時要用才發現檔案過期無法下載。

（四）缺乏「聊天室管理者」，成員易被偽冒、訊息易被竊聽

工作專用的即時通訊平台，在預防詐騙訊息、病毒檔案、或釣魚連結等資安議題上有更多保障。除了可避免員工不小心把公務資料傳到私人聊天室，造成機密外洩之外，每一個使用單位都有「聊天室管理者」，可以妥善的進行帳號管理。近期詐騙及駭客事件頻傳，社交通訊軟體的聊天群組（例如：一個 10 多人的群組），往往有回音的只有寥寥幾人，容易潛伏不知名的人士、或是早已被棄置多時的帳號，群組的聊天內容可能不知不覺被圈外人讀取。

公務專用即時通訊，可降低訊息無意曝光的風險。訊息溝通時會使用加密傳輸，再透過「聊天室管理者」的權限，可以有效確認組員帳號是否正確。想導入至辦公室，還可與常見的公務帳號/群組系統整合、綁定 AD／LDAP、更可與公務信箱帳號整合，專人專號。

帳號管理更安全、公務隱私更有保障；在對於隱私高度要求的情況下，管理者可限制登入者的 IP 來源，防護使用者帳號被盜、或被駭客登入竊聽，冒名參與重要公務討論的風險。

工作專用的即時通訊，不一定會額外花錢，同樣屬於企業溝通工具，Email 電子信箱常會附帶即時通訊功能，只要您的企業/機關有使用公務信箱，通常就會有工作專用的即時通訊軟體，建議可優先詢問您的郵件服務廠商。提高辦公室資安意識，拒用免費即時通訊，

導入工作專用即時通訊，不一定會花費額外成本。提早完成工作、準時下班享受生活，「工作」與「私用」即時通訊明確分渠，工作、生活雙雙更有效率！

二、答：

（一）勒索軟體，又稱勒索病毒，是一種特殊的惡意軟體，又被人歸類為「阻斷存取式攻擊」（denial-of-access attack），其與其他病毒最大的不同在於手法以及中毒方式。其中一種勒索軟體僅是單純地將受害者的電腦鎖起來，而另一種則系統性地加密受害者硬碟上的檔案。所有的勒索軟體都會要求受害者繳納贖金以取回對電腦的控制權，或是取回受害者根本無從自行取得的解密金鑰以便解密檔案。勒索軟體通常透過木馬病毒的形式傳播，將自身為掩蓋為看似無害的檔案，通常會通過假冒成普通的電子郵件等社會工程學方法欺騙受害者點擊連結下載，但也有可能與許多其他蠕蟲病毒一樣利用軟體的漏洞在聯網的電腦間.....傳播。

原先勒索病毒只在俄羅斯境內盛行，但隨著時間推進，受害者開始廣布全球。2013 年 6 月，網路安全公司 McAfee 釋出了一份數據，顯示該公司光在該年度（2013）第一季就取得了超過 250,000 種不同的勒索病毒樣本，並表示該數字是去年（2012）同季的超過兩倍。隨著 CryptoLocker 的流行，加密形式的勒索軟體開始進行大規模的攻擊，在遭當局瓦解以前取得了估計三百萬美元的贖金。另一個勒索軟體 CryptoWall，被美國聯邦調查局估計在 2015 年 6 月以前獲得了超過一百八十萬美元的贖金

（二）

1.立即切斷網路，避免將網路磁碟機或共享目錄上的檔案加密。
2.立即關閉電腦電源：關閉電腦電源的目的是不讓勒索病毒繼續加密電腦中的檔案，關機時間愈快被加密的檔案愈少，建議強制關閉電腦電源。
3.保留電腦，通報專業資安人員。
4.不要付錢。

（三）

1.三不
(1)不上鉤：收到標題吸引人的郵件，務必停看聽。
(2)不打開：不隨便打開 Email 附件檔案。
(3)不點擊：不隨意點擊 Email 中的網址。
2.三要
(1)要備份：依據 3-2-1 原則妥善備份重要資料—在兩種不同媒介上建立三個備份，其中一個備份要放在不同地方。
(2)要確認：打開 Email 前要確認寄件者身份。
(3)要更新：作業程式、軟體、病毒碼要隨時保持更新狀態，當軟體廠商(例如 Flash/SilverLight/IE)公布修補程式請盡快更新。

三、答：

（一）優點如下：

1.完成 App 實名認證後，可簡化報關的委任程序，不需再提供身分證正反面影本給報關業者，保護個資更周全。

2.此 App 僅限本國國民適用，1 支手機門號僅能綁定 1 組身分證字號，註冊程序相當簡捷，只需填上個人資料並經過身分驗證，即可完成實名認證程序。3、EZ WAY App 也提供線上報關委任服務，主動推播網購貨物通關訊息至已實名認證手機，使用者於手機確認相關報關資料無誤後，只按「申報相符」，即可完成委任報關手續，且可直接查詢貨物通關進度，無須再以紙本申請。

（二）缺點如下：

1.實名認證的推廣便是希望能夠解決個資外洩，但也難以杜絕冒名案件的發生，提醒消費者在收到海外包裹的報關通知，要仔細檢查金額和品項是否與自己購買的內容相符，因為關稅的關係些微的金額差距是合理的，但若對價格差距仍有疑慮的消費者，可以直接撥打電話尋求協助，以免遭人冒名白白誤領將錢送給別人。

2.EZ Way 自從上路以來，有許多民眾抱怨明明沒有訂購卻收到 EZ Way 的通知，或是註冊完成卻遭系統說尚未完成實名認證等等 App 出包的問題，想說好的軟體開發是需要一點時間進程的，所以建議消費者在收到有疑慮的通知時，一定要向受理單位確認，也給相關業者一點時間，改善冒名現況。

四、答：

（一）資訊的正確性(Information Accuracy)的定義

資訊的正確性(Accuracy)：由於資料的品質差、資料錯誤等常常會造成個人與組織很大的傷害，因此在精確性方面，Mason(1986)認為主要的倫理議題在於討論資訊的精確性應該由誰來負責，有哪些人可能造成資訊的不精確性，對於資訊的不精確性、錯誤所造成的後果，應該由誰來負責，如何追究責任？如何可以避免錯誤的發生？

（二）資訊正確性產生問題的主要原因包括：(1)輸入資料的錯誤；(2)軟體開發的錯誤；(3)硬體設備的故障。

（三）系統管理者應有三個重要的防護措施

1.系統開發的品質規範：為了防止軟體的錯誤，系統的開發應制定品質認證標準，目前一般企業所推行的 CMMI 認證制度即為最佳典範。

2.硬體安全與防範計畫：例如符合 ISO27001 的安全認證機制，亦是一個很好的典範。

3.重視專業倫理守則。

五、答：

（一）變臉詐騙往往從攻擊者入侵企業高階主管郵件帳號或任何公開郵件帳號開始。通常經由鍵盤側錄惡意軟體或網路釣魚（Phishing）手法達成，攻擊者會建立類似目標公司的網域或偽造的電子郵件來誘騙目標提供帳號資料。在監控受駭電子郵件帳號時，詐騙者會試著找出進行轉帳及要求轉帳的對象。詐騙者通常會進行相當的研究，尋找財務高階主管變動的公司，高階主管正在旅行的公司或是進行投資人電話會議來製造機會以進行騙局。

1.變臉詐騙有三種手法：
(1)第一個手法：透過偽造的郵件、電話或傳真要求匯款給另一個詐騙用帳戶。
(2)第二個手法：詐騙者自稱為高階主管（CFO、CEO、CTO 等）、律師或其他類型的法定代表。
(3)第三個手法：駭客入侵員工的電子郵件帳號。

2.六個防止成為變臉詐騙受害者防禦之道
(1)仔細檢查所有的電子郵件。小心來自高階主管送來的不尋常郵件，因為它們是用來誘騙員工去緊急動作，檢視要求資金轉移的電子郵件以確認該請求是否正常。
(2)教育和訓練員工。雖然員工是公司最大的資產，當提到資訊安全，他們往往也是最脆弱的一環。依照公司的最佳實作來培訓員工。提醒他們遵守公司政策是一回事，但養成良好的安全習慣是另一回事。
(3)供應商付款位置改變要由公司人員進行第二層簽核來加以確認。 了解你客戶的習性，包括細節和付款背後的原因。
(4)使用手機驗證來確認資金轉移請求以作為雙因子認證，使用已知的熟悉號碼而非來自電子郵件中所提供的內容。
(5)如果你懷疑自己成為變臉詐騙郵件的目標，立即向執法部門回報。

（二）同第二題。

六、答：

（一）OWASP Top10 主要目的，是將最常見的網路應用系統安全弱點，教育開發者（Developers）、設計者（Designers）、架構師（Architects）和組織（Organizations），提供基本的方法保護防止這些弱點，是軟體開發安全計劃最好的開始。

1. Cross Site Scripting（XSS）：當應用程式未將使用者提供的資料先審核或進行內容編碼，就直接將資料傳輸到網路瀏覽器，即可能發生 XSS 問題。XSS 能讓攻擊者直接在受害者的網路瀏覽器上執行 Script，攻擊者便可以 hijack user sessions、或竄改網站內容等。
2. Injection Flaws ：在網路應用程式，SQL Injection 裡很常見。Injection 之所以會發生，是因為使用者提供的資料傳輸到一個 interpreter，此被當成指令（Command）或是查詢（Query）。攻擊者就能用惡意的資料欺騙 interpreter，而達到執行指令或是竄改資料的目的。
3. Insecure Remote File Include：有弱點的程式碼讓攻擊者可附加惡意程式及資料，甚至導致毀滅性的攻擊，例如整個伺服器被入侵。

4. Insecure Direct Object Reference：Direct object reference 發生的原因是因為開發者暴露了 reference to an internal implementation object，像是檔案、檔案夾、或資料庫的 record，或是 key，來作為 URL 或是 Form 的參數。攻擊者可藉由操作這些 references 擅自進入其他 objects 中。
5. Cross Site Request Forgery（CSRF）：CSRF 攻擊強迫受害者登入的瀏覽器傳輸 pre-authenticated request 給有弱點的網路應用程式，接著強迫受害者瀏覽器執行對攻擊者有好處的的行為。
6. Information Leakage and Improper Error Handling：應用程式可能洩漏關於程式的 configuration 訊息，程式內部的運轉模式，或者透過多種應用問題違犯隱私。攻擊者利用這個程式弱點侵犯隱私，或者更進一步的攻擊。
7. Broken Authentication and Session Management：Account credentials 和 session tokens 因經常沒有受到正確及嚴密的保護。而被攻擊者使用密碼、或 keys，或是 authenticationtokens 來冒用其他使用者的身份。
8. Insecure Cryptographic Storage：網路應用程式很少正常使用 cryptographic functions 來保護資料，使得攻擊者有機可乘並冒用其他使用者身份，進行其他犯罪行為，如盜刷信用卡等。
9. Insecure Communications：保護敏感的通訊資料是必要的，但應用程式卻經常忽略以「加密」方式來保護網路通訊。
10. Failure to Restrict URL Access：應用程式敏感地區是被保護的 Links 或是 URLs，而這些是不會提供給未被授權的使用者。這也容易讓攻擊者利用這項弱點進入，並進行未被授權的行為。

（二）Injection（注入攻擊）是一種古老的漏洞，從 Web 發展開始，此漏洞即如影隨形，不但每年榜上有名，而且都名列前茅，數一數二。

此安全漏洞肇因於程式設計師出於疏失或經驗不足而未對於使用者輸入的參數值進行驗證（包含驗證資料型態及驗證內容），以致於惡意使用者可利用惡意的輸入值（如惡意 SQL 指令串或惡意的 Script 碼），即可能讓系統自動執行惡意的指令而對系統造成危害。此類攻擊以 SQL Injection、Command Injection 為代表，其中以 SQL Injection 最具代表也最具危害性。

七、答：

本題極度困難需要看過行政院國家資通安全會報技術服務中心資通系統委外開發 RFP 範本 (v2.0) 裡面的系統與服務獲得欄位，才能夠解答。

範本裡面有歸納三項如下：

3.2.1.4.1 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	系統應設計錯誤處理機制，當系統發生錯誤時，儘可能採取錯誤代碼或簡短訊息呈現，避免將詳細或除錯用訊息直接顯示於使用者頁面，以防被攻擊者用來刺探系統內 部資訊，或根據錯誤訊息推測出系統可能之弱點。確保系統所有功能的程式碼，在程式的進入點之後，盡可能採用程式語言的 try-catch 陳述，捕捉可能發生的錯誤與例外狀況。另外，採用程式語言的 finally 陳述，確保將該段功能程式碼所使用的資源正確釋放。
3.2.1.4.2 具備系統嚴重錯誤之通知機制。	系統應區分錯誤等級，若發生嚴重等級錯誤時，採用電子郵件或簡訊等通知機制，使系統管理員或相關人員可及時掌握狀況，以利進行後續處理。
3.2.1.4.3 資通系統相關軟體，不使用預設密碼。	系統相關軟體元件或組態設定若有使用預設密碼，應於系統正式上線前變更完畢。

八、答：

（一）Atomicity (原子性）- 在資料庫的每一筆交易中只有兩種可能發生，第一種是全部完全(commit)，第二種是全部不完成(rollback)，不會因為某個環節出錯，而終止在那個環節，在出錯之後會恢復至交易之前的狀態，如同還沒執行此筆交易。

（二）Consistency (一致性）- 在交易中會產生資料或者驗證狀態，然而當錯誤發生，所有已更改的資料或狀態將會恢復至交易之前。

（三）Isolation (隔離性）- 資料庫允許多筆交易同時進行，交易進行時未完成的交易資料並不會被其他交易使用，直到此筆交易完成。

（四）Durability (持續性）- 交易完成後對資料的修改是永久性的，資料不會因為系統重啟或錯誤而改變。

九、答：

資安健診的目的是透過整合各項資訊安全項目的檢視服務作業，提供資安改善建議，藉以實施技術面控制措施，以提升網路、資訊系統及個人電腦安全防護能力，檢測項目主要有 7 大項：

（一）網路架構檢視

1.針對架構、設備佈署、備援方式、防火牆規則與主機佈署進行討論
2.產出架構脆弱點、防火牆規則與主機佈署不當之處，提供強化建議

（二）有線網路惡意活動檢視-封包監聽與分析

1.由 Switch 複製流量到封包側錄系統
2.取回封包側錄紀錄進行連線分析
3.產出網路設備異常事件(如中繼站等異常連線)

（三）有線網路惡意活動檢視-網路設備紀錄檔分析

1.使用工具收集網路設備 Log，針對發現之可疑程式與相關紀錄進行分析
2.分析過濾內部電腦或設備是否有對外之異常連線紀錄
3.發現異常連線之電腦或設備需確認使用狀況與用途

（四）使用者端電腦檢視

1.檢查使用者電腦惡意程式和更新檢視
2.由 AD 派送工具到檢測主機上進行檢查，並回收 Log
3.若無 AD 派送則逐一使用工具檢測 • 產出結果，列出高風險電腦清單，並提供改善建議
4.可疑程式協助送防毒廠商製作解毒劑

（五）伺服器主機檢視

1.檢查伺服器主機惡意程式和更新檢視
2.由 AD 派送工具到檢測主機上進行檢查，並回收 Log
3.若無 AD 派送則逐一使用工具檢測
4.產出結果，列出高風險主機清單，並提供改善建議
5.可疑程式協助送防毒廠商製作解毒劑

（六）安全設定檢視-AD 伺服器群組原則設定

檢視目錄伺服器中群組的密碼設定與帳號鎖定原則，例如 AD(Active Directory)伺服器有關群組原則(Group Policy)中之「密碼設定原則」與「帳號鎖定原則」設定

（七）安全設定檢視-防火牆連線設定

檢視防火牆的連線設定規則(如外網對內網、內網對外網、內網對內網)是否有安全性弱點，確認來源與目的 IP 與通訊埠連通的適當性

十、答：

（一）主機型防火牆

此防火牆需有兩張網路卡，一張與網際網路連接，另一張與內部網路連接，如此網際網路與內部網路的通道無法直接接通，所有封包都需要透過主機傳送。

（二）雙閘型防火牆

此防火牆除了主機型防火牆的兩張網路卡外，另安裝應用服務轉送器的軟體，所有網路封包都須經過此軟體檢查，此軟體將過濾掉不被系統所允許的封包。

（三）屏障單機型防火牆

此防火牆的硬體裝置除需要主機外，還需要一個路由器，路由器需具有封包過濾的功能，主機則負責過濾及處理網路服務要求的封包，當網際網路的封包進入屏障單機型防火牆時，路由器會先檢查此封包是否滿足過濾規則，再將過濾成功的封包，轉送到主機進行網路服務層的檢查與傳送。

（四）屏障雙閘型防火牆

將屏障單機型防火牆的主機換成雙閘型防火牆。

（五）屏障子網域型防火牆

此防火牆藉由多台主機與兩個路由器組成，電腦分成兩個區塊，屏障子網域與內部網路，封包經由以下路徑，第一個路由器->屏障子網域->第二路由器->內部網路，此設計因有階段式的過濾功能，因此兩個路由器可以有不同的過濾規則，讓網路封包更有效率。若一封包通過第一過濾器封包，會先在屏障子網域進行服務處理，若要進行更深入內部網路的服務，則要通過第二路由器過濾。

十一、答：

（一）封鎖階段

當進展到封鎖階段時，我們的目的是希望能夠止血，避免災情擴散。我們該如何找到攻擊者，並阻止造成更多損害，就是此階段的目標。

因此，在此部分我們將討論短期封鎖、以及長期封鎖的策略，當然包含了對於系統之備份，以及鑑識映像檔製做的相關議題。

封鎖階段包含了三個小階段，三個階段是有順序性的。

1.短期封鎖策略
2.系統備份
3.長期封鎖策略

（二）根除階段

當進展到根除階段時，則是表示災情停止擴大，我們要開始清理攻擊者留下來的現場。

此階段最主要是需要判斷資安事件的原因與徵狀：

1.用先前偵測分析階段與封鎖階段得到的資訊
2.嘗試將攻擊隔離開來，並判斷這些攻擊是如何被執行

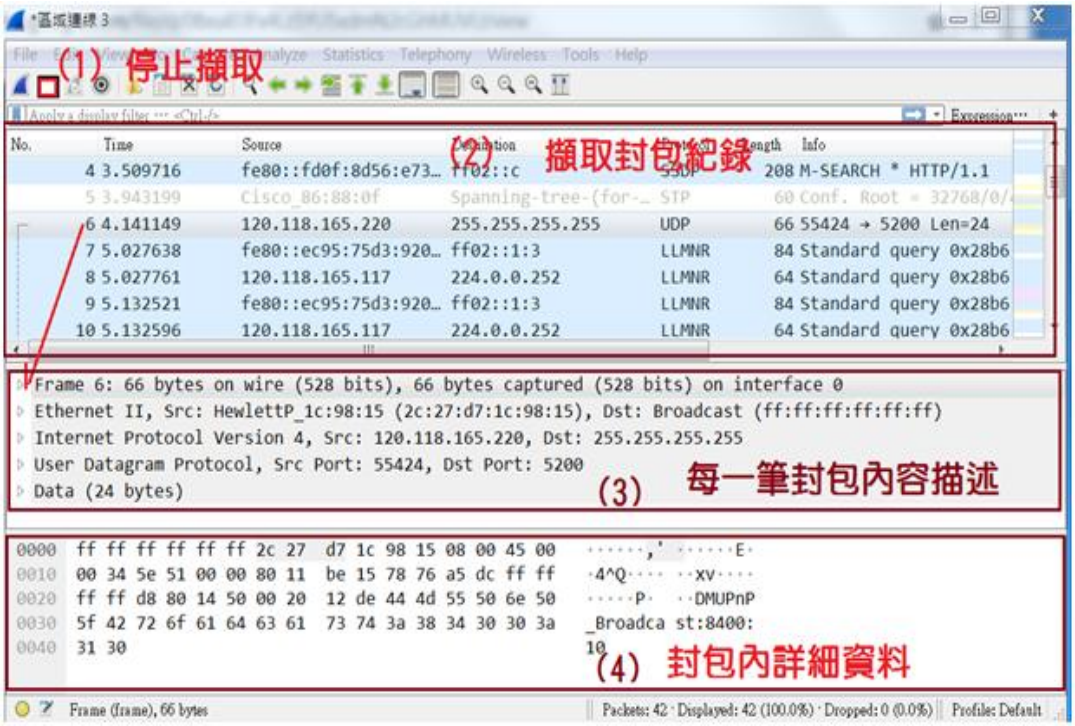
（三）復原(回復)階段

資安事件復原階段的目的，是要讓受影響的系統，能安全地回復正常運作，因此我們需透過完整的測試計畫，檢驗與判斷系統是否恢復正常。

回復作業的時間選擇是很重要的，應該選在對業務衝擊最少的時段進行。而對於回復計畫執行項目與時間的最後決定，可由系統擁有者進行決策。

十二、答：

本題的重點是要知道可以使用 Wireshark 軟體來協助封包側錄並且判讀正常與異常流量，然而 Wireshark 是一個免費開源的網路封包分析軟體。網路封包分析軟體的功能是截取網路封包，並盡可能顯示出最為詳細的網路封包資料，可以透過此軟體來選擇網路介面卡，並且點選介面卡之後立即開始擷取封包，(1)須按暫停才會暫停擷取。於擷取視窗 (2)是擷取到的每一個 IP 封包，可點選某一個封包，則在視窗 (3)出現該封包的分析資料，而封包內的詳細資料如視窗 (4) 所示，畫面如下：



十三、答：

（一）1.網路層。

2.Open Shortest Path First。

說明：

(1)開放式最短路徑優先 Open Shortest Path First(OSPF)

(2)基於 IP 協定的路由協定，屬於網路層

(3)為內部閘道協定

(4)計算最短路徑

（二）1.應用層。

2.HyperText Transfer Protocol Secure。

說明：
(1)由 HTTP 進行通訊，利用 SSL/TLS 來加密封包
(2)屬於應用層

（三）1.傳輸層。

2.Secure Sockets Layer。
說明：
(1)網頁伺服器和瀏覽器之間以加解密方式溝通的安全技術標準
(2)屬於傳輸層

（四）1.com 是網際網路的通用頂級域之一，「com」是「company (公司)」的縮寫。

2.org 是網際網路的通用頂級域之一，「org」是英文「organization (組織)」的縮寫。

（五）非對稱數位使用者線路（英語：Asymmetric Digital Subscriber Line）又稱非對稱數位用戶回路（Asymmetric Digital Subscriber Loop），簡稱 ADSL。

十四、答：

（一）

1.防火牆的定義：
防火牆是能夠監控傳入和傳出網路流量的網路資安裝置，並依據一組已定義的資安規則來決定允許或封鎖特定流量。多年來，防火牆一直是網路資安的第一道防線。它們在安全受控制的信任內部網路和不信任的外部網路（例如網際網路）之間建立一道屏障。 防火牆可以是硬體、軟體或兩者皆是。

2.防火牆的主要功能：
(1)封包過濾路由器:
①由預先決定好之過濾法則來過濾通過防火牆的資訊封包。
②通常只檢查 IP、TCP、UDP、ICMP 封包的標頭(Header)，並不會檢查資料段內容。
③優點:價格便宜
④缺點:缺乏彈性
(2)狀態檢視防火牆:
是一種動態封包過濾的防火牆技術，能夠更細部的檢視封包及連線工作階段　的防火牆。可以透過連線狀態來判斷是否為合法授權的封包。
(3)代理伺服器:
進入或外出的封包並不直接通過防火牆，而是由某一個代理伺服器（Proxy Server）來完成客戶端的要求，再轉傳給客戶端。
(4)應用層閘道器:
需要在防火牆主機執行特定應用程式，負責應用層級的訊息過濾與轉送處理。

（二）先了解那些存在於應用層的服務可以幫助管理防火牆，舉例來說如果需要阻擋過濾沒有安全加密的 http 的封包類型，就要知道 http 該類型的通訊協定之應用埠為 80 或者是 8080，

然後了解通訊協定之應用埠（Port）也可以幫助管理者設計防火牆的安全對策來幫助過濾跟阻擋存在風險性的封包。

十五、答：

本題需要了解風險值定義，並且知道其風險值評估的公式如下

風險值=弱點等級 x 威脅等級 x 資訊資產價值

因此系統的風險跟弱點等級、弱點等級與資訊資產價值這三個主要情境改變而有所變化。

十六、答：

（一）5V 定義如下：

容量（Volume）：數據的大小決定所考慮的數據的價值和潛在的信息。
速度（Velocity）：指獲得數據的速度。
種類（Variety）：數據類型的多樣性。
價值（value）：合理運用大數據，以低成本創造高價值。
真實性（Veracity）：數據的質量。

（二）由於上述 5V 的特性，也可以看成大數據本身在應用時的需求條件，為此而發展的實體技術就是雲端儲存與運算。

現在最熱門的雲端儲存與運算技術是由兩個關鍵服務組成：
1.數據儲存：利用 Hadoop 分散式檔案系統（HDFS，Hadoop Distributed File System）
2.數據處理：利用「Hadoop MapReduce」。

雲端數據儲存的主要原理就是:在網路上架構數千數萬個節點伺服器共同儲存、偕同運作，數據被切成 Block(數據塊;資料塊)分散儲存,利用多重複製與大量伺服器的方式儲存 Block，避免單一節點伺服器掛點後資料的遺失。(類似 Raid-5 的概念)

運算的部分則是運用 Hadoop MapReduce 的方式在各節點各自運算後再回傳主伺服器進行彙整，因此，小塊數據的運算就發生在各節點上而非主伺服器，達到分散運算的效果

十七、答：

（一）本題也是需要了解法規才有辦法寫出答案，因此請同學除了專業內容閱讀之外，請定期查閱政府資通安全事件通報及應變辦法文件，才能應付此種題目。

根據資通安全事件通報及應變辦法第三條資通安全事件之通報內容，應包括下列項目：
1.發生機關。
2.發生或知悉時間。
3.狀況之描述。

4.等級之評估。
5.因應事件所採取之措施。
6.外部支援需求評估。
7.其他相關事項。

（二）本題也是需要了解法規才有辦法寫出答案，因此請同學除了專業內容閱讀之外，請定期查閱政府資通安全事件通報及應變辦法文件，才能應付此種題目。

1.根據資通安全事件通報及應變辦法第四條公務機關資通安全事件之通報及應變：
2.公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。
3.前項資通安全事件等級變更時，公務機關應依前項規定，續行通報。
4.公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。
5.公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。

根據資通安全事件通報及應變辦法第五條公務機關資通安全事件之通報及應變：
1.公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜：
(1)第一級或第二級資通安全事件，於知悉該事件後七十二小時內。
(2)第三級或第四級資通安全事件，於知悉該事件後三十六小時內。
2.公務機關依前項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改善報告。
3.前項調查、處理及改善報告送交之時限，得經上級或監督機關及主管機關同意後延長之。
4.上級、監督機關或主管機關就第一項之損害控制或復原作業及第二項送交之報告，認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求公務機關提出說明及調整。

十八、答：

（一）雜湊函數:亦稱訊息摘要或雜湊值，可將一個可變長度的訊息產生固定長度的雜湊碼。設計妥當的雜湊函數在輸入不同訊息時，幾乎不可能產生相同的雜湊值，而且也很難從雜湊值推論函數的輸入。
常見的演算法有產生 128 位元的 MD5(message digest 5)與產生 160 位元的 SHA-1(Secure Hash Algorithm 1)

（二）因爲取雜湊的過程，實際上是將輸入鍵（定義域）對映到一個非常小的空間中，所以衝突是無法避免的，能做的只是減少 Hash 碰撞發生的概率。影響雜湊碰撞（衝突）發生的除了雜湊函數本身意外，底層陣列容量也是一個重要原因。

很明顯，極端情況下如果陣列容量爲 1，哪必然發生碰撞，如果陣列容量無限大，哪碰撞的概率非常之低。

所以，雜湊碰撞還取決於負載因子。

負載因子是儲存的鍵值對數目與陣列容量的比值，比如陣列容量 100，當前存貯了 90 個鍵值對，負載因子爲 0.9。

負載因子決定了雜湊表什麼時候擴容，如果負載因子的值太大，說明儲存的鍵值對接近容量，增加碰撞的風險，如果值太小，則浪費空間。

十九、答：

（一）微型服務的特性

1.自發
微型服務架構中的每項元件服務都可以自由開發、部署、運作和擴展，並不會影響其他服務的功能。這些服務不需要與其他服務分享任何程式碼或實作。獨立元件之間會經由定義良好的 API 進行所有通訊。

2.專門
每項服務專為一組功能設計，並著重於解決特定問題。如果開發人員不斷提供更多程式碼，導致服務變得更加複雜，可以將服務分解成較小型的服務。

（二）微型服務的優勢

1.敏捷性
微型服務促進組織組成小型獨立團隊，並具備其處理之服務的擁有權。團隊可在小型簡易的環境中行動，並能夠更獨立且快速地工作。這有助於縮短開發週期時間。彙總的組織輸送量能為您帶來莫大好處。

2.可彈性擴展
微型服務可讓每項服務獨立擴展，以滿足其支援的應用程式功能的需求。這可讓團隊依架構需求調整合適的大小、準確地衡量功能的成本，以及在服務出現需求激增時維持可用性。

3.輕鬆部署
微型服務可持續整合和持續交付，方便您嘗試新點子，並在發生問題時進行復原。失敗的成本較低，可讓您進行實驗，以便更新程式碼，並縮短新功能的上市時間。

4.技術的自由
微型服務架構不適用於「一體適用」的方法。團隊可自行選擇可解決其特定問題的最佳工具。因此，建立微型服務的團隊可為每項工作選擇最佳工具。

5.可重複使用的程式碼
將軟體劃分為定義良好的小型單元，可讓團隊將功能用於多種用途。專為特定功能撰寫的服務可充當其他功能的建構模塊。這可讓應用程式自行引導操作，以便開發人員建立新功能，而無需從頭開始撰寫程式碼。

6.恢復能力
服務的獨立性可提升應用程式的受挫能力。在巨型架構中，如果單一元件故障，可能會造成整個應用程式故障。在微型服務中，應用程式可將功能降級，以處理整個服務故障問題，避免造成整個應用程式當機。

二十、答：

（一）風險識別主要是盡可能地發現會導致資訊系統發生風險的原因，讓組織有系統地了解風險的組成來源跟可能帶來傷害衝擊的等級，來達到風險管理的目的。
我們可以透過篩選、監測與診斷這三個步驟來協助組織是別其風險。

（二）風險估計主要是用來評估風險發生的可能性與會影響組織的項目，我們應該採取定量分析與定性描述此兩種方法來協助組織來進行風險評估。
我們可以透過估計風險發生率、估計損失與估計衝擊來協助組織進行風險評估。

（三）風險評估是每個組織進行風險管理時候一個重要的程序，然而國際標準組織 ISO 也有提出完整的成險評估的內容需要包含風險識別、風險分析與風險評價這些過程才健全。