《資通安全》

一、身分認證（authentication）在資安防禦裡是一項基本重要的防禦機制。傳統利用使用者名稱（Identifier, ID）及密碼（password）的方式，很容易被竊取而造成資安的一大漏洞，且在犯罪偵查過失責任上很難釐清是否為本人或是竊取者所為。一種比較嚴謹的身分認證方式稱為多重因子身分認識（multi-factor authentication, MFA）。

（一）請說明多重因子身分認證的設計主要是考量那三項資料性質，其綜合資訊比較能夠充足地認證使用者的真實身分？每一項資料性質請舉出至少兩個實例。（21 分）

（二）目前電子商務在實務操作對使用者身分認證，廣為採用在該認證事件發生的當下用動態產生一辨識碼（access code），送到宣稱的使用者手機或是電子郵件信箱，使用者必須輸入該辨識碼以確認身分。請問這種做法是屬於(一)小題中三項資料性質的那一種？（4 分）

（三）承(二)所提的做法通常會限制例如：使用者必須在三分鐘內回應輸入送至手機或是電子郵件的辨識碼。請問這樣的做法的目的為何？（5 分）

命題意旨	本題在測驗考生是否了解身分認證的三個重要的因子，對因子的實務應用加以舉例，並能正確區分動態密碼使用的因子及運作原理。
答題關鍵	第一小題考生需先指出三個因子，並依序對因子內容加以說明，再依照題意舉出兩個以上的實例。 第二小題指出動態密碼使用的因子，並說明原因。 第三小題說明動態密碼的時間限制之原因，關鍵在安全性。
考點命中	《高點資通安全講義》第二回，金乃傑編撰，頁 1-4。

【擬答】

(一)身分認證是透過一定的手段，完成對使用者身分的確認，其目的是確認當前所聲稱為某種身分的使用者確實是該身分。用以判別身分的因子可分為三種：所知之事（something you know）、所持之物（something you have）及所具之形（something you are），而多因子身分認證即使用兩個以上的因子進行驗證，因要同時具有多個因子難度較高，因此能提高身分認證之安全性。以下說明各因子之內容並舉例相關的驗證方法。

1.所知之事：利用正確的使用者才知道的事情進行認證，實例：

(1)靜態通行密碼（Password）：只有特定的使用者知道正確的帳號密碼配對組合。

(2)暗號（通關密語）：只有內部特定人員才會知道的一句用語，通常用在取得特定資源前由人工進行驗證。

2.所持之物：利用正確的使用者才會持有的東西進行認證，實例：

(1)RFID 卡：只有特定人員才會配備的 RFID 卡片，透過 RFID 閱讀器可檢測卡片中晶片的特定資訊，以確認卡片有效性。

(2)鑰匙（Key）：只有特定人員才會配發的工具，依照鑰匙設計的紋路吻合裝置鎖孔中預先定義的規則以開啟裝置。

3.所具之形：利用正確使用者本身的生物特徵進行認證，實例：

(1)指紋（Fingerprint）辨識：透過比較手指末端指腹上由凹凸的皮膚所形成的紋路的細節特徵的區別來進行鑒別。

(2)臉部辨識：可分為兩種方法，整體特徵法與局部特徵方法。整體特徵法直接將整張人臉當作單一特徵來做辨識；局部特徵法先找出臉上的局部特徵，通常是眼睛、鼻子和嘴巴，然後分別辨識局部特徵，最後結果統合計算。

(二)使用者驗證時，透過簡訊或電子信箱進行身分認證即為動態密碼，其因子為「所持之物」。因為只有特定使用者才會持有所聲稱之手機（或電子信箱帳號）。值得一提的是，此種身分驗證前通常需先進行一般的帳號密碼登入，因此具備雙重驗證（two factor authentication）的特性，即帳號密碼的「所知之事」加上額外驗證的「所持之物」。

(三)在特定時間內必須輸入所收到的驗證碼是避免遭受暴力破解法攻擊。因為暴力法破解密碼通常會需要一段時間，因此若此密碼不限使用時間，則仍可能被破解。此外，動態密碼機制也常搭配輸入次數的限制，若一組動態密碼已經成功驗證過，其他人則無法再使用該組動態密碼登入系統，如此可以有效避免重送攻擊。

二、現今很多企業網路在與網際網路連結的閘道路由器(gateway router)使用網路位址轉換(Network Address Translation, NAT)技術，使得企業網路內部之聯網裝置的 IP 位址是私有的(private)，只有閘道路由器或特殊用途的伺服器才使用合法（legitimate）IP 位址。

(一)使用網路位址轉換技術對企業而言，除了節省使用合法 IP 位址的成本費用外，請列出至少三項在資安管理上的好處。(10 分)

(二)網際網路資安犯罪偵查與鑑識之溯源追蹤（IP Traceback）是指例如有疑似來自企業內部設備攻擊外部網路某一伺服器的事件。在偵查鑑識上，假如擬從受害機器端根據攻擊封包的來源 IP 位址（source address）一路追蹤回溯，但是因為 NAT 功能，追蹤到企業的閘道路由器線索可能被迫中斷。請說明應該在 NAT 設備上採取何種措施，以利溯源追蹤可以一直延伸到企業內網偵查，找到真正的攻擊來源。(15 分)

命題意旨	本題在測驗考生對 NAT 功能的了解、對組織的安全價值；並進一步指出在 NAT 環境下進行 IP 追蹤的方法。
答題關鍵	第一小題可從 NAT 間隔公有與私有 IP 著手，並指出 NAT 可搭配 DHCP 進行 IP 設定相關的配置。第二小題需指出 IP 追蹤的方法如何應用在 NAT 環境下，關鍵在於 NAT 因連結異質網路，故其本質亦為路由器。
考點命中	《高點資通安全講義》第二回，金乃傑編撰，頁 22-23。

【擬答】

(一)網路位址轉換技術透過重寫 IP 來源位址、目的位址，使外部連線必須透過 NAT 才能轉址到對應的內部 IP，讓內部網路的多台電腦透過相同的對外 IP 連上網際網路。其帶來的資安管理好處說明如下：

1.完全隱匿內部電腦：透過 NAT 轉址會配給內部電腦私有 IP，因私有 IP 之特性無法在網際網路上傳送，因此就算攻擊者知道內部電腦的 IP，亦無法直接連線攻擊，所有流量都必須要透過 NAT 轉址，因此只要在 NAT 進行阻擋即可有效保護內部避免駭客攻擊。

2.自動配置安全性：由於 NAT 將公有 IP 與內部私有 IP 互相轉換，因此通常要搭配 DHCP 服務對內部電腦配置私有 IP。在 DHCP 服務配置時，可以同時指定 DNS 伺服器、代理伺服器（應用層閘道器）等資訊，直接設定內部網路電腦安全性，並快速大規模佈署。

3.提供伺服器負載均衡：若伺服器架設在 NAT 內部，可透過伺服器反應速度偵測的技術動態的將流量平均分配到多台伺服器上，進行簡易的負載平衡，提高服務之可用性。

(二)由於 NAT 將 IP 在公有與私有間轉換，因此若攻擊者來自於 NAT 內部，則較難追朔到攻擊主機。此時可透過 Logging 或 ICMP Traceback（iTrace）進行追蹤，說明如下：

1.Logging：在 NAT 伺服器上使用 Log 紀錄所有的封包轉換紀錄，紀錄包括來源位址、目的位址及封包數量等資訊。當追查到該 NAT 伺服器時，則根據對外連線的目的位址反推來源位址，並配合 DHCP 中的 Log，以追蹤到當時擁有該私有 IP 的主機網路卡號碼，確認實體位址。Logging 雖為最直覺的作法，但由於 NAT 伺服器紀錄 Log 空間有限，因此實作成本高，且很容易因新紀錄覆蓋而使先前紀錄遺失。

2.ICMP Traceback：由 ICMP 協定推展小組所提出，透過路由器中的 ICMP 封包夾帶資訊以追蹤來源位址，支援的路由器稱為 iTrace 路由器。該路由器會發出特殊形式的 ICMP 封包，將該路由器的位址以一定的機率紀錄在 IP 表頭的識別欄上。由於攻擊路線上會經過多台路由器，因此表頭識別欄中會依序紀錄經過的路由器 IP。以一定機率紀錄的原因是避免增加過多的網路流量，也避免讓 ICMP 封包過大。當受攻擊目標追蹤封包時，就可以根據 ICMP 封包追查到最初來源。若網路中所有邊界路由器都支援 iTrace，則中繼的路由器不支援也能找到確切攻擊位址。此外，也可以透過「當主機感受到攻擊時」再要求來源端路由器紀錄 IP，亦能有效減少網路流量。由於 NAT 伺服器亦屬於路由器，因此若 NAT 支援 iTrace，便可透過擴展 iTrace 的 ICMP 封包，紀錄內部來源端的主機 IP 位址，以達成在 NAT 轉址下的來源追蹤。

補充資料	關於 IP 追蹤技術的延伸閱讀：1，2。

三、最近眾所矚目的勒索軟體（Ransomware），其目的是鎖住系統、螢幕或加密檔案，直到受害者依照指示支付勒索贖金。事實上，勒索軟體的散播機制並沒有創新性。

（一）請列出系統會被植入此惡意程式的至少三種手法。（15 分）

（二）請說明為何這些手法可以繞過傳統的安全解決方案例如：防火牆及防毒軟體？（5 分）

命題意旨	本題在測驗考生是否掌握如何防止惡意程式的方法；並了解防火牆與防毒軟體的限制。
答題關鍵	第一小題需指出三種惡意軟體可能的感染途徑，根據途徑說明感染過程、解決方法為佳。 第二小題關鍵在防火牆無法阻擋未經防火牆的攻擊，及對於加密的病毒攔截成效較差。
考點命中	《高點資通安全講義》第一回，金乃傑編撰，頁 49-51；第二回，頁 21。

【擬答】

(一)以下討論在受害主機上安裝惡意程式之作法：

1.直接誘使使用者安裝：透過社交工程的電子郵件附件，或誘使下載網路上的程式執行檔（例如：某程式之破解版），讓使用者在沒有防備的狀態下將惡意程式在電腦中執行。此法為最簡單的手法，對於無資訊相關背景的人有效，但若電腦中有安裝並定期更新防毒軟體，或透過資訊安全宣導即可避免受害。

2.檔案病毒：透過被感染的檔案在電腦間散播。攻擊者將病毒植入檔案中，常見如在 Office 文件中透過內建的巨集（Marco）修改系統設定，甚至自動下載並執行惡意程式，再將此檔案透過電子郵件、USB 隨身碟或網路儲存媒體進行散播，讓開啟檔案的同時安裝惡意程式。此種攻擊通常可以透過防毒軟體有效避免。

3.網頁病毒：在網頁中使用 JavaScript 等腳本語言進行 XSS 攻擊，讓使用者在瀏覽到特定網頁時自動下載惡意程式，再透過瀏覽器或瀏覽器外掛元件（如 Flash）的緩衝區溢位問題將惡意程式的執行檔在本機執行。此法為最常見的攻擊方式，也較難防禦。除了必須要定期更新瀏覽器、瀏覽器外掛與防毒軟體外，也要避免連上安全性差或來路不明的網站。

(二)繞過安全解決方案可能有以下原因：

1.BYOD 盛行，許多人會使用自己的裝置執行公務，因此若在家或用自己的 4G 連線上網，即不會透過公司的防火牆，因此防火牆無法保障。

2.此類惡意軟體可以透過加密傳送資訊，因此防火牆、防毒軟體未必能有效攔截其所執行的惡意指令碼。

四、資訊安全管理制度（Information Security Management System, ISMS）。

（一）在計算資訊資產的風險值時，通常會對盤點出的資訊資產清單上依據資訊資產性質之不同作分類。請說明分類須考量那三個安全面向及區分成幾級？（15 分）

（二）資訊資產分類後，通常會建立資產風險評鑑的標準以計算資訊資產的風險值。請說明風險值計算除可考量資訊資產價值外，尚可考慮那些重要因素？試說明之。（10 分）

命題意旨	本題在測驗考生關於資訊安全風險管理中的風險公式之內容，並能說明每一項風險參數之計算方法。
答題關鍵	第一小題之三面向為 CIA 三要素。 第二小題則需說明威脅等級、脆弱性等風險因子的內容及其分數計算方法。
考點命中	《高點資通安全講義》第二回，金乃傑編撰，頁 61-62。

【擬答】

(一)資訊資產的風險（Risk）指的是對於目標會產生影響的事件發生的機會，是未來的不確定事件，該事件會影響組織目標的達成。計算資訊資產之風險時，根據資訊安全面向分為機密性（Confidentiality）、完整性（Integrity）與可用性（Availability）三種。其中機密性指資訊資產的內容必須僅限授權者存取；完整性是維持資訊資產內容的正確與完整，不遭受竄改或遺失；可用性只確保資訊資產能隨時提供使用。每個面向根據其破壞後果的影響力區分為三個等級，3 是最高，2 居中，1 代表普通。將此三個分數相加即可獲得該資訊資產的「價值」分數。

(二)進行資訊資產之風險評鑑會計算該資訊資產之風險等級，通常風險等級在 20 分以下為可接受的風險，其公式為：威脅等級 * 脆弱性 * 價值。以下針對威脅等級及脆弱性說明：

1.威脅（Threat）：可能對資產或組織造成損害事故的潛在原因（必須利用脆弱性才能對資產造成傷害）。常見的威脅如：未經授權的存取、惡意軟體、軟體失效、火災、竊盜與人為的錯誤等。評估時必須確認威脅引起的原因、目標及發生的機率，參考分數 7 代表經常；5 代表每月至少一次；3 代表每季最多二次；1

則為每年最多四次。

2.脆弱性（Vulnerability）：資產或資產組中能被威脅利用的弱點，涵蓋於實體環境、人事及管理程序、軟硬體軟體或通訊設施中。常見的弱點如：缺乏適當的實體保護、錯誤的密碼選擇或使用、對外連接的網路未受保護、文件的儲存未有適當的保護、缺乏適當的資訊安全教育等。評估脆弱性時著重被威脅利用的機率，參考為數 7 代表 90%；5 代表 75%；3 代表 50%；1 代表 25%。