105年公務人員特種考試司法人員、法務部調查局調查人員、國家安全局國家安全情報人員、海岸巡防人員及移民行政人員考試試題　代號：10760　全一頁

考 試 別：司法人員
等　　別：三等考試
類 科 組：檢察事務官電子資訊組
科　　目：資通安全
考試時間：2 小時　座號：_____

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

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證（multi-factor authentication, MFA）。
㈠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）
㈡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㈠小題中三項資料性質的那一種？（4 分）
㈢承㈡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）

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。
㈠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）
㈡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）

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。
㈠請列出系統會被植入此惡意程式的至少三種手法。（15 分）
㈡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）

四、資訊安全管理制度（Information Security Management System, ISMS）。
㈠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）
㈡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）