111 年公務人員普通考試試題

類　科：資訊處理
科　目：資訊管理與資通安全概要

甲、申論題部分：

一、請闡述資訊管理職場生涯的職種，包括資訊長（Chief Information Officer,CIO）、知識長（Chief Knowledge Officer, CKO）以及資訊安全長（Chief Security InformationOfficer, CSIO）的工作性質與所需具備的能力或經驗。（20 分）

【解題關鍵】
《考題難易》：★★★
《破題關鍵》資訊管理組織題，了解資訊長、知識長、資安長意義即可解答。
《命中特區》：H1K03 資訊管理講義 P683 命中資訊長、知識長，資安長為近年新興議題，資安長為資通安全管理法相關新議題。

【擬答】

㈠資訊長通常是負責對企業內部資訊系統和資訊資源規劃和整合的高級行政管理人員，扮演下列角色：

1. IT 策略執行者：以資訊技術（IT）配合企業策略的執行。
2. 科技掃描者：掃描評估並引進適合的新 IT 架構。
3. 創業家：尋找新的業務技術找尋顧客、用戶、合作夥伴。
4. 仲介談判者：成功達成策略夥伴的合作關係。
5. 資源規劃者：把 IT 資源整合並且配置在企業重要的地方。
6. 變革管理者：透過策略管理變革，順利推動組織資訊化。
7. 功能管理者：有效領導、組織、規劃、考核、指導管理資訊系統（MIS）部門。

㈡知識長負責公司的知識管理計劃。CKO 幫助設計發現新知識源的程序和系統，或者幫助在組織和管理過程中對現有的知識進行更好的應用。知識長必須具備以下能力或經驗：

1. 獨立思考能力，具未來觀與國際觀，能抓住流行趨勢，觀察要敏銳，判斷要準確，能快速處理危機。可以快速整合、創新、管理、運用知識，把知識化為寶貴資產甚至申請專利權，避免遭到對手控告侵權，外購及技術移轉要注意技術本身及過程作業是否合法。
2. 了解企業核心競爭力，配合企業實力推行，計劃未來知識發展目標。規劃知識管理架構，推行實務作業及整合運用。不斷溝通與學習，能全心全力投入。
3. 有創新能力，把想像的東西化為實際的商品。且可將知識管理具體化，用數據及文字、圖形表現出來，定期盤點知識損益狀況、淘汰挖掘知識。並參與企業營運、策略規劃、經營管理、電子商務發展。
4. 發揮資訊科技能力，利用網絡整合企業資源、知識庫、經驗庫及人才庫，快速反應問題處理。具有研發基礎與經驗，能領導研發團隊及頂尖技術專家。

㈢資安長負責企業組織資訊與資料的安全。要成為一位稱職的資安長，首先要能夠定義資安角色與職掌功能，也要能夠了解企業集團風險並連結績效指標，更要配合業務發展策略，投入相對應的資源。

二、請闡述下列名詞的意涵：工作分解結構（Work Breakdown Structure）、組織分解結構（Organization Breakdown Structure）、工作包（Workpackage）以及工作項目（Activity），並且說明它們的關係。（20 分）

【解題關鍵】
《考題難易》：★★★
《破題關鍵》專案管理範疇規劃題，了解專案管理範疇規劃過程即可作答。
《命中特區》：AF26-1 系統專案管理講義 P2-67~69 完全命中

【擬答】

㈠工作分解結構（WBS）是一個以交付標的（Deliverable）為導向，目標是建立一個有效的工作架構，以定義全部專案之範疇。專案之各項活動在經過 WBS 分解後能充分的顯示與展開，並表達出專案各活動間與交付產品之關聯性。是專案「科層化」（Hierarchical）的結構圖形，用以區分專案不同層次的工作。

㈡組織分解結構（Organization Breakdown Structure，簡稱 OBS）。OBS 是由 WBS 演化而來的一種方法，它在組織範圍內分解各層次人員。OBS 最終能顯示出負責每個項目活動的具體組織單元，它是將相關部門或單位與工作包分層次、有條理地聯繫起來的組織安排。

㈢工作包（Work Package）指專案中近程且可明確定義的工作，屬可以獨立指派、管理及監控的工作單元。

㈣活動 （Activity） 是由工作包 （Work package） 分解而來，是實現工作包所需的具體工作。工作包是 WBS 底層的可交付成果，是 WBS 的一部分，活動不是 WBS 的一部分。工作包不表示時間、也不表示順序，只表示專案範圍；活動可表示時間、順序、是資源估算、歷史估算、費用估算的重要依據。

三、有一網路設備的網路設定如下：IP 位址為 167.11.12.88、網路遮罩為 255.255.255.0。針對此網路設備的子網路，請回答下列問題：（每小題 5 分，共 10 分）

㈠子網路 ID（Subnet ID）為何？

㈡常用的預設閘道器的 IP 位址為何？

【解題關鍵】
《考題難易》：★
《破題關鍵》資通網路 IP 位址基本計算題，掌握 IP 位址基本概念即可作答。
《命中特區》：F1A22 資通網路講義 P371 完全命中。

【擬答】

㈠子網路 ID 為 167.11.12.88 &（逐位元 and 運算）255.255.255.0=167.11.12。

㈡常用的預設閘道器的 IP 位址通常為可用 IP 範圍（167.11.12.1~167.11.12.254）的最後一個 IP，故為 167.11.12.254。

四、密碼學是資通安全管理者必須知曉的基本知識，請回答下列問題：

㈠傳統加密方法可分為取代法（Substitution）以及換位法（Transposition），請問著名的凱薩（Caesar）加密法是屬於那一種？回答時須附上正確的理由才予以計分。（5 分）

㈡請比較對稱式密鑰方法和非對稱式密鑰方法的特性與優缺點。（10 分）

㈢ SSL（Secure Sockets Layer）安全協定是只利用對稱式密鑰方法，還是只利用非對稱式密鑰方法或是兩種方法都使用？回答時須附上正確的理由才予以計分。（10 分）

【解題關鍵】
《考題難易》：★★
《破題關鍵》網路安全機密性防護基本題，掌握加密相關觀念即可作答。
《命中特區》：H1K21 資通安全講義 P208 命中㈠、P212（命中㈡）、P229（命中㈢）

【擬答】

㈠凱撒密碼（Caesar cipher）是一種最簡單且最廣為人知的加密技術。凱撒密碼是一種替換加密技術，明文中的所有字母都在字母表上向後（或向前）按照一個固定數目進行偏移後被替換成密文。例如，當偏移量是 3 的時候，所有的字母 A 將被替換成 D，B 變成 E，以此類推。故為取代法進行加密。

㈡比較如下表：

特性	對稱式密鑰	非對稱式密鑰
密鑰數目	單一密鑰	成對之密鑰
密鑰種類	私密密鑰	私密密鑰與公開密鑰
密鑰管理	不易管理、密鑰之傳遞難題	易於管理（但需要 CA 之配合）、無密鑰之傳遞難題
運算速度	快	慢
用途	用來做大量資料的加密	只能做小規模資料之加密

㈢ SSL 主要利用對稱密鑰演算法在網際網路上提供傳接雙方身份認證與通訊保密，但密鑰的傳送是利用非對稱密鑰方法以數位信封的方式完成，因此會同時使用對稱密鑰與非對稱密鑰兩種方法。

五、防火牆（Firewall）是現代企業重要的安全防護工具，請回答下列問題：

㈠防火牆的工作原理包括封包過濾式（packet filtering）以及應用程式代理（application proxy）兩種方法，請說明這兩種方法的特性與優缺點。（10 分）

㈡一般公司通常將 web 伺服器放在防火牆的 DMZ（Demilitarized Zone）區，其理由為何？請詳細說明之。（10 分）

㈢近年來一種稱為 WAF（Web Application Firewall）的新型態防火牆受到重視，請說明 WAF 的功能及特性。（5 分）

【解題關鍵】
《考題難易》：★★
《破題關鍵》網路安全可用性防護基本題，掌握防火牆相關觀念即可作答。
《命中特區》：H1K21 資通安全講義 P223~225（命中㈠），㈡在 102 調查局特考、與㈢在 105 外交四等特考有類似題。

㈠

1. IP 封包檢查路由器

這是由過濾封包來進行事前預防的工作。IP 封包檢查路由器的做法是經由預先決定好之過濾法則來過濾通過防火牆的資訊封包。可以根據網路協定、目的位址、來源之 IP 位址進行檢查，同時也可以對出去的封包進行過濾。此種裝置最大的優點在於價格便宜，但其缺點則有缺乏彈性與容錯性。

2. 代理伺服器（proxy server）

這是指一個位於使用者與 Internet 之間的閘道，對此使用者提供中間人服務或代理服務，譬如一個公司網路上的使用者想要和另一個機構的使用者透過代理伺服器進行交談的話，第一位使用者事實上是先與此代理伺服器交談，這個代理伺服器再與對方的電腦交談，因此對方所看到的 IP 事實上是由代理伺服器所發出。最常見的應用是快取文件（caching document），就是將文件儲存在近端的伺服器上，當使用者重覆存取此文件時，不必再到遠端去存取，直接從近端的伺服器就可取得，如此可以不必浪費網路頻寬又可以增快存取速度。代理伺服器的優點包括資訊隱藏、對危險網路及應用程式加以限制、利用代

理伺服器的快取功能來提昇網路之應用效能、身份驗證及登錄。代理伺服務之缺點是對於 HTTP 這種主從式的協定，進來與出去的連接都必須要兩個步驟，所花費的時間太多。代理防火牆對病毒來說，是個弱勢的保護方法。目前幾種二進位的編碼方式來做的網路傳送及不同的檔案格式均無法做足夠的監視。

㈡ DMZ（Demilitarized Zone），是一種網路架構的布置方案，在不信任的外部網路和可信任的內部網路外在另外建立一個面向外部網路的實體或邏輯子網，該子網能設置用於對外部網路的伺服器主機。可以使用在防火牆、路由器等區隔內外網的網路設備，以方便管理。利用此種方式，可以用設置良好的防火牆把大部分的“幼稚腳本”阻止在防火牆外，同時由於 DMZ 泛指內部網路和外部網路之間的緩衝地帶，因此即使此處被入侵也不會造成太大損失，可使組織有較充裕時間因應。

㈢網頁應用程式防火牆（Web Application Firewall， WAF）的設計宗旨是防禦針對 web 應用程式的常見攻擊，諸如跨網站攻擊（cross-site scripting）以及 SQL injection 攻擊，位於網頁瀏覽者與網頁伺服器間，專責分析「應用層」的網路流量內容，並依據事先設計好的安全政策，發掘違反安全政策的封包。