代號：37320
頁次：2－1

115年公務人員高等考試三級考試試題

類　　科：資訊處理
科　　目：資通網路與安全
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。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、一網管工程師在為一棟新大樓建置網路架構，大樓內部有一個對外提供服務的學術網站伺服器機房。請回答以下問題：（每小題 10 分，共 30 分）

㈠新大樓的路由器與學校機房之間接了兩條實體線路（一條主線、一條備援線）。若網管工程師放棄手動寫靜態路由，改為啟用 OSPF 動態路由協定。當某天主線路不小心被挖斷時，大樓的網路流量會發生什麼變化？請從動態路由協定的特點與選路依據來合理解釋。

㈡學校將大樓的「學術網頁伺服器」放在防火牆的 DMZ（Demilitarized Zone），而不是直接接在外網或安全的內網。當外網的使用者想要連進來瀏覽網頁時，防火牆的安全策略（Security Policy）應該要如何放行？請寫出必須設定的三個關鍵要素。

㈢為了防止學生在教學實驗室連上惡意詐騙網站，網管工程師架設了一台 Proxy 伺服器，「代表學生（客戶端）」向外網發送請求並進行安全檢查。請問這台架設在學生前端、幫忙過濾外網網頁的設備，屬於「正向代理（Forward Proxy）」還是「反向代理（Reverse Proxy）」？請詳述兩者的本質區別。

二、在數位經濟與雲端運算高度發展的時代，個人資料（Personal Data）已成為組織核心的資訊資產，同時也是資安防範與法律合規的重中之重。依據我國個人資料保護法與歐盟一般資料保護規則（GDPR）之法理精神，企業在處理個人隱私時，必須將安全防護思維融入資料的完整生命週期中。為了在「數據分析利用」與「隱私保護」之間取得平衡，企業常採用「去識別化」（De-identification）技術。去識別化技術又包含「匿名化」（Anonymization）及「擬匿名化」（Pseudonymization）技術。請回答以下問題：（每小題 10 分，共 30 分）

㈠請解釋何謂「匿名化」（Anonymization）。

㈡請解釋何謂「擬匿名化」（Pseudonymization）。

㈢請舉一個例子說明「匿名化」及「擬匿名化」兩者之差異。

三、當代組織面臨的營運威脅日益複雜，從勒索軟體癱瘓機房到新興供應鏈中斷風險，皆可能對組織造成無法估計的損失。營運持續管理（Business Continuity Management, BCM）已成為企業與政府機構建構「數位韌性」的核心管理機制，旨在確保關鍵商務功能在遭受重大衝擊時仍能維持底線運作。組織在建構完整的 BCM 計畫前，必須透過「風險評估（Risk Assessment, RA）」來掌握潛在威脅。請詳細列舉出風險評估流程中的五個核心執行步驟，並逐一扼要闡述各步驟的主要工作目標為何？（10 分）

四、某公司使用一套由外部廠商提供的遠端管理工具，該工具平時用於協助資訊人員更新軟體、派送設定檔與維護內部主機。某次例行更新後，多台內部主機開始出現異常連線行為，但使用者並未點擊可疑郵件，也未下載未知檔案。初步調查發現，異常程式是透過該遠端管理工具的正常更新流程被派送到主機上，因此在部分紀錄中顯示為「合法更新」。請回答下列問題：（每小題 15 分，共 30 分）

㈠此事件中，攻擊者為何不一定需要直接攻擊公司內部系統，也能使內部主機執行惡意程式？請分析其可能涉及的攻擊方法，並說明此類攻擊與一般使用者自行下載惡意程式有何不同。

㈡若公司只檢查「員工是否點擊可疑郵件」或「主機是否存在未修補弱點」，為何可能無法發現此類攻擊的真正原因？請說明應如何從第三方風險管理、更新驗證與內部監控三個面向降低風險。