115 年灌溉管理組織新進農田水利事業人員甄試試題

甄試類別【代碼】：綜合行政人員資訊組【F501-F517】

專業科目二：資通網路與安全概要　　**＊入場通知書編號：＿＿＿＿＿＿＿＿**

注意：①作答前先檢查答案卡（卷），測驗入場通知書編號、座位標籤、應試科目是否相符，如有不同應立即請監試人員處理。使用非本人答案卡（卷）作答者，該節不予計分。
②本試卷為一張雙面，測驗題型分為【四選一單選選擇題 40 題，每題 1.5 分，共 60 分；非選擇題 2 題，每題 20 分，共 40 分】，總計 100 分。
③四選一單選選擇題限以 2B 鉛筆於答案卡上作答，請選出一個正確或最適當答案，答錯不倒扣；以複選作答或未作答者，該題不予計分。
④非選擇題限以藍、黑色鋼筆或原子筆於答案卷上採**橫式**作答，並請**依標題指示之題號於各題指定作答區內作答**。
⑤**請勿於答案卡（卷）上書寫應考人姓名、入場通知書編號或與答案無關之任何文字或符號。**
⑥本項測驗僅得使用簡易型電子計算器（不具任何財務函數、工程函數、儲存程式、文數字編輯、內建程式、外接插卡、攝（錄）影音、資料傳輸、通訊或類似功能），且不得發出聲響。應考人如有下列情事扣該節成績 10 分，如再犯者該節不予計分。1.電子計算器發出聲響，經制止仍執意續犯者。2.將不符規定之電子計算器置於桌面或使用，經制止仍執意續犯者。
⑦**答案卡（卷）務必繳回，未繳回者該節以零分計算。**

壹、四選一單選選擇題（每題 1.5 分，共 60 分）

【3】1.一個 Class C 網路被劃分為 8 個子網，其子網路遮罩應為何？
① 255.255.255.128　② 255.255.255.192　③ 255.255.255.224　④ 255.255.255.240

【2】2.下列何者不是 802.1X 認證架構中的主要組件？
①認證器（Authenticator）　②防火牆（Firewall）
③認證服務器（RADIUS）　④客戶端（Supplicant）

【2】3.下列「私有 IP 位址」（Private IP），何者不可直接在網際網路上路由？
① 7.7.7.7　② 172.16.128.2　③ 140.123.128.3　④ 168.95.123.4

【1】4.下列何種技術可以用來驗證資料的完整性？
①數位簽章　②加密　③防毒軟體　④防火牆

【3】5.下列何者無法提供私密性功能？
① AES 128　② RSA 2048　③ Sha 256　④ TDES

【4】6.下列何者做為通行碼（password）時，其安全性最高？
① 1QAZ2wsx　② Password　③ Qwerty12　④ GJO3xu4c

【2】7.在 WiFi 應用場域，下列何者提供行動裝置與 AP 間安全連線？
① WEP　② WPA 3　③ VLAN　④ TLS 1.3

【2】8.下列何者為「專門蒐集、分析及交叉關聯來自各種來源的資安資料如日誌，以便即時偵測、調查及回應潛在的威脅」？
① EDR　② SIEM　③ SSO　④ IPS

【1】9.下列何者可用來建立農田水利署與各地管理處間網路安全通道確保交換資料安全？
① IPSec　② SSH　③ SSO　④ VLAN

【3】10.在負載平衡（Load Balancing）技術中，"Sticky Session(Session Persistence)" 的主要目的為何？
①平均分配所有請求到不同伺服器
②防止 DDoS 攻擊
③確保同一使用者的請求總是分派到同一台後端伺服器
④加速 TLS 加解密過程

【4】11.在 IPsec 的運作模式，若要加密「整個原始 IP 封包」並加上新的 IP 表頭，應採何種模式？
① Bridge Mode　② GRE Mode　③ Transport Mode　④ Tunnel Mode

【1】12.有關 IPv6 的敘述，下列何者錯誤？
①增加了選項（Options）欄位到固定標頭中　②地址長度為 128 位元
③移除了標頭校驗和（Checksum）欄位　④不允許在中間路由器進行分段

【1】13.有關 HTTP 持久連接（Persistent Connections）的敘述，下列何者正確？
①伺服器在發送回應後會保持 TCP 連接開啟，允許後續請求重複使用
②僅在 HTTP 1.0 版本中提供 Persistent Connections
③每個請求/回應都需要建立新的 TCP 連接
④比非持久連接產生更多的 RTT 延遲

【4】14.網路管理中，SNMP（簡單網路管理協定）與 NETCONF 的主要區別為何？
① NETCONF 不支持 XML，而 SNMP 支持
② SNMP 運行在 TCP 上，而 NETCONF 運行在 UDP 上
③ SNMP 使用 YANG 語言模型，而 NETCONF 使用 SMI
④ SNMP 主要用於監控，而 NETCONF 更強調配置管理與事務處理

【3】15.虛擬可擴展局域網（VXLAN）技術的主要目的為何？
①取代所有的 IPv6 地址
②僅用於公共場域 Wi-Fi 加密
③透過 IP 隧道在三層網路上擴展二層網路，並支持超過 1600 萬個虛擬網路
④加快資料中心的實體線路連接

【3】16.社交工程（Social Engineering）攻擊主要是利用系統中的哪一個弱點來進行滲透？
①作業系統漏洞　②防火牆設定錯誤　③人性弱點　④網路協定設計缺陷

【2】17.為確保遠距辦公時，員工從外部網路連回公司內網的資料傳輸安全，應優先建置下列哪一項機制？
①入侵偵測系統（IDS）　②虛擬私人網路（VPN）
③防毒軟體（Antivirus）　④網站應用程式防火牆（WAF）

【2】18.下列哪一種協定用於加密網頁瀏覽的傳輸內容？
① HTTP　② HTTPS　③ FTP　④ Telnet

【4】19.「網路釣魚」（Phishing）攻擊的主要目的為何？
①增加網路流量　②破壞系統硬體　③佔用網路頻寬　④竊取帳號密碼或個人資料

【4】20.「阻斷服務攻擊」（DoS Attack）的主要目的為何？
①竊取系統資料　②植入後門程式　③竊取使用者身分　④讓使用者無法存取服務

【2】21.攻擊者將檔案加密並要求受害者支付虛擬貨幣以換取解密金鑰，此種惡意程式稱為下列何者？
①蠕蟲（Worm）　②勒索軟體（Ransomware）
③木馬程式（Trojan）　④鍵盤側錄器（Keylogger）

【2】22.任何 ISO 管理系統（包含 27001、27701、42001）皆遵循持續改善的核心框架，此框架簡稱為何？
① SDLC　② PDCA　③ ITIL　④ COBIT

【3】23.下列何者是用來測試遠端網路主機是否可正常連線的常用指令？
① tracert　② ipconfig　③ ping　④ nslookup

【1】24.下列何者是使用大型語言模型（LLM）作為工作助理時應注意的資安事項？
①避免在公開 LLM 服務中輸入機密資料、敏感個資或商業機密等
② LLM 的答案均來自官方資料庫
③使用 LLM 可取代防火牆（Firewall）資安工具
④ LLM 可自動偵測並修復系統漏洞

【請接續背面】

【4】25. ISO/IEC 27001:2022 中「內部稽核」（Internal Audit）的主要目的為何？
①取代外部認證稽核　②僅查核財務紀錄的正確性
③對外宣傳組織的資安成就　④驗證是否符合標準要求並有效運作

【4】26.「AI 幻覺」（AI Hallucination）在資訊安全情境中可能造成何種風險？
①提升系統執行效能　②導致網路頻寬不足
③加速資料加密速度　④產生看似合理但實際錯誤的資訊而誤導決策

【2】27.「深偽技術」（Deepfake）對資訊安全的主要威脅為何？
①加快網路傳輸速度　②偽造逼真的影音內容，用於詐騙或社交工程攻擊
③強化資料加密強度　④提升雲端服務可靠性

【2】28.利用大量的殭屍網路（Botnet）發送無用封包塞爆目標伺服器的頻寬或資源，導致正常用戶無法連線，這種攻擊稱為下列何者？
① SQL Injection　② DDoS　③ XSS　④ Phishing

【2】29.當軟體廠商尚未發現漏洞，或是發現漏洞但尚未發布修補程式前，駭客就利用該漏洞進行攻擊，屬於下列哪一種類型？
①阻斷服務攻擊　②零時差攻擊（Zero-Day Exploit）
③字典攻擊　④中間人攻擊

【2】30. VLAN（虛擬區域網路）的主要功能為何？
①增加實體網路線路數量　②將實體網路邏輯分割為多個廣播域
③提升無線訊號強度　④加密網路傳輸內容

【2】31.「滲透測試」（Penetration Testing）中的「黑箱測試」（Black Box）是指下列何者？
①測試人員擁有完整系統內部資訊　②測試人員在不具系統知識情況下模擬外部攻擊者
③測試人員僅針對原始碼進行審查　④測試人員擁有部分系統資訊

【4】32.「SQL 注入攻擊」（SQL Injection）主要利用哪一種弱點？
①網路頻寬不足　②使用者帳號密碼過於簡單
③伺服器的實體安全防護不足　④應用程式未對使用者輸入進行適當的驗證與過濾

【4】33.「跨網站指令碼攻擊」（XSS）的攻擊目標為何？
①防火牆設備　②網路路由器
③資料庫伺服器　④造訪惡意網頁的終端使用者瀏覽器

【4】34. ISO/IEC 42001:2023 中，對 AI 系統「透明度」（Transparency）的要求，主要指向何種義務？
①定期發布財務報告
②公開 AI 演算法的原始碼
③僅向政府機關說明 AI 系統功能
④讓相關利害關係人了解 AI 系統的目的、能力、限制及決策依據

【3】35.在開發新的人工智慧（AI）專案並遵循 ISO 42001 時，若該 AI 系統可能對個人權利或社會產生重大影響，組織應優先執行下列何項工作？
①申請著作權　②將研發部門外包　③ AI 系統的影響評鑑　④購買最高級伺服器硬體

【4】36.關於「進階持續性威脅」（APT）的特徵，下列敘述何者正確？
① APT 通常以大量掃描快速取得目標
② APT 攻擊通常在數小時內完成
③ APT 主要依賴勒索軟體進行攻擊
④ APT 具高度針對性、長期潛伏、多階段攻擊，且通常由國家級行為者或高技術組織發動

【3】37.下列何者是 AI 技術在網路安全中的常見應用？
①取代防火牆硬體設備　②自動修補網路實體線路故障
③利用異常行為偵測識別網路攻擊　④提升 Wi-Fi 無線訊號強度

【3】38.用來確認資料在傳輸過程中沒有被竄改，通常會使用下列何種技術？
①對稱式加密　② VPN
③雜湊演算法（Hash）　④憑證授權中心

【4】39. ISO/IEC 27701 中，「個人資料控管者」（PII Controller）與「個人資料處理者」（PII Processor）的主要區別為何？
①兩者職責相同，僅規模不同
②控管者在法律上不承擔責任
③控管者負責技術實作；處理者負責法規遵循
④控管者決定處理目的與方式；處理者依控管者指示處理個資

【1】40.使用者登入系統時，除了輸入密碼外，還必須輸入手機收到的簡訊驗證碼。這屬於下列何種安全機制？
①多重因素驗證（MFA）　②角色存取控制（RBAC）
③單點登入（SSO）　④生物辨識驗證

貳、非選擇題 2 大題（每題 20 分，共 40 分）

第一題：

因應生成式人工智慧（GenAI）的爆炸性發展，組織若欲依循 ISO/IEC 42001:2023 人工智慧管理系統（AIMS）標準，就必須執行「AI 系統風險評鑑（AI System Risk Assessment）」。

（一）請說明為何傳統的 IT 資安風險評估不足以涵蓋 AI 系統？【10 分】

（二）請舉出兩項 AI 系統特有的風險（如偏見、透明度等），說明它們對企業或社會可能造成的衝擊。【10 分】

第二題：

隨著雲端運算與遠距辦公的普及，企業逐漸導入「零信任架構（Zero Trust Architecture, ZTA）」。主要目的是解決信任邊界不明問題，確保資料於任何時間、地點存取時皆維持安全。

（一）請說明零信任架構的「核心概念」。【5 分】

（二）請說明與傳統企業網路「邊界防禦（Perimeter Defense）」模型在安全理念上的主要差異。【5 分】

（三）零信任架構的五大核心支柱，包含身分鑑別（Identity）、設備鑑別（Device）、應用程式（Application）、網路（Network）與資料（Data）。請簡述落實前述五大支柱的關鍵機制與技術。【10 分】