111 年度初級資訊安全工程師能力鑑定試題

科目 1：資訊安全管理概論
考試日期：111 年 05 月 28 日　　第 1 頁，共 8 頁

單選題 50 題（佔 100%）

A	1.「有人假冒大學電算中心人員，打電話向你詢問，並騙取你的帳號密碼。」請問上述屬於下列何種攻擊法？ (A) 社交工程（Social Engineering） (B) 垃圾桶攻擊法（Dumpster Diving） (C) 中間人攻擊法（Man-in-the-middle Attack） (D) 後門攻擊法（Backdoor Attack）
B	2. 組織已開始著手進行資訊資產之盤點、建立清冊，並實施風險評鑑作業，請問此作業屬於 PDCA 循環之何者階段？ (A) P（Plan） (B) D（Do） (C) C（Check） (D) A（Act）
C	3. 下列何者為國際上受到業界認可，並可驗證的資訊安全管理系統（Information Security Management System, ISMS）標準？ (A) ISO 9001 (B) ISO 27000 (C) ISO 27001 (D) ISO 27002
C	4. 下列何者「不」是風險評鑑過程中主要的活動？ (A) 風險鑑別 (B) 風險分析 (C) 風險處理 (D) 風險評估
D	5. 下列何者「不」屬於威脅來源之一？ (A) 天然災害 (B) 憤怒的員工 (C) 未經授權存取機密資料 (D) 程式的瑕疵
A	6. 使用 Wireshark 工具，主要可能影響資訊安全中的何種特性？ (A) 機密性（Confidentiality） (B) 可用性（Availability） (C) 完整性（Integrity） (D) 真確性（Authenticity）
A	7. 下列何種資訊設備較「無法」從網路層進行存取控制以限制合法的來源？

	(A) DLP（Data Loss Prevention） (B) DNS（Domain Name Service） (C) Firewall (D) Switch
D	8. 在 Linux 作業系統中，下列何者「不」為檔案存取權限的分類？ (A) 可寫（Write） (B) 可讀（Read） (C) 可執行（Execute） (D) 測試（Test）
C	9. 下列何者「不」是建立高安全強度密碼的原則？ (A) 密碼需定期變更 (B) 設定複雜度高的密碼，如包含英文字母大小寫、數字及特殊符號 (C) 密碼應可立即變更 (D) 密碼長度越長越好
D	10. 最近無線網路的安全備受重視，請問在無線網路相關協定中，下列何項協定的規範內容與身份認證與安全機制有關？ (A) 802.11n (B) 802.11a (C) 802.11ac (D) 802.11i
C	11. 使用指紋或是掌紋來辨識身份，屬於下列何種身份認證方式？ (A) 所知之事 (B) 所持之物 (C) 所具之形－靜態特徵 (D) 所具之形－動態特徵
A	12. 依據「資通安全事件通報及應變辦法」，主管機關於接獲通報後，若判定為 3 級或 4 級事件，應於幾小時內完成審核？ (A) 2 小時 (B) 4 小時 (C) 8 小時 (D) 12 小時
C	13. 下列敘述何者較「不」正確？ (A) RTO 時間越長，代表可容忍系統無法使用時間越長 (B) RPO 的時間點要求越遠，代表可允許之資料備份週期越長 (C) RPO 的時間點要求越遠，代表可允許之資料備份週期越短 (D) MTPD 時間越長，代表可容忍系統無法使用時間越長

A	14. 常見的磁碟陣列（Redundant Array of Independent Disks, RAID）中，RAID5 可以容忍同時幾顆硬碟損毀？ (A) 1 (B) 2 (C) 3 (D) 4
B	15. 關於個人資料保護，下列何者為「不」可直接識別個人資料？ (A) 身分證統一編號 (B) 出生年月日 (C) 護照號碼 (D) 指紋
B	16. 下列何者「不」是保護智慧財產權的適當做法？ (A) 向知名且信譽良好的店家購買電腦軟體 (B) 從網路下載破解版的軟體 (C) 制訂保護智慧財產權的政策 (D) 定期審查是否僅安裝經授權的軟體
C	17. 下列何者「不」在著作權的保護範圍內？ (A) 自創音樂 (B) 小說創作 (C) 公文內容 (D) 攝影作品
B	18. 下列何種為個人資料保護法中所定義的特種個人資料？ (A) 離婚身份 (B) 犯罪前科 (C) 住家電話 (D) 銀行負債情形
C	19. 關於營運持續計畫（Business. Continuity Planning, BCP），下列敘述何者較「不」正確？ (A) 詳細規劃啟動條件 (B) 應讓營運計畫小組人員接受教育訓練，確保計畫過程無慮 (C) 無需太多人知曉計畫內容，避免備援地點外洩 (D) 需有明確的復原程序及復原時間
B	20. 下列何者為資訊安全資產清冊製作及維持的主要目的？ (A) 方便帳務管理 (B) 適切的保護資產 (C) 對於財產價值的管理

	(D) 便於資訊備份
B	21. 關於自然人憑證，下列敘述何者「不」正確？ (A) 使用非對稱式演算法產生金鑰對 (B) 簽驗章和加解密是使用同一組金鑰對 (C) 目前自然人憑證設有有效期，但可以展延 (D) 透過自然人憑證進行簽章時，被簽章之資料無長度限制
A	22. 一般而言，公開公鑰會透過憑證管理中心發行公開憑證來傳遞，對於仍在有效期內，卻因為某些因素造成憑證廢止的情形，可以透過下列何項協定來查詢？ (A) Online Certificate Status Protocol（OCSP） (B) Online Certificate Register Protocol（OCRP） (C) Online Certificate Revoke Protocol（OCRP） (D) Certificate Transmit Protocol（CTP）
D	23. 在資訊安全管理系統（Information Security Management System, ISMS）中定義並進行資訊資產分級，下列何者最適合納入評估面向？ (A) 資訊資產的變現金額 (B) 資訊資產的折舊 (C) 資訊資產的流動性 (D) 資訊資產的機敏性
C	24. 關於資訊資產的分級，下列敘述何者較「不」正確？ (A) 透過資訊資產分級，可讓資產受到適當程度的保護，也可以兼顧資安執行成本 (B) 依照各類資產所具有之機密性、完整性、可用性對該資產之價值進行評估 (C) 公司公開教育訓練手冊和主管的電腦檔案，兩者的價值不同，應投入相同保護資源 (D) 為確保資產被系統性管理，可透過資產編號、條碼等方式來進行分類標示
D	25. 通用漏洞評分系統（Common Vulnerability Scoring System, CVSS）是一個可衡量漏洞嚴重程度的公開標準。CVSSv3 以基本指標群（Base metric group）、暫時指標群（Temporal metric group）及環境指標群（Environmental metric group）等 3 個群組來進行判斷。關於基本指標群，下列何者「不」是其考量因素？ (A) 機密性衝擊（Confidentiality Impact） (B) 攻擊途徑（Attack Vector） (C) 攻擊複雜度（Attack Complexity）

	(D) 可靠性衝擊（Reliability Impact）
B	26. 關於日誌與監控作業，下列敘述何者較「不」正確？ (A) 日誌應記錄使用者活動、異常，並且依法定要求的時間保存 (B) 系統日誌為避免外洩，應在發生資安事件時才查詢，平日不應存取 (C) 日誌應避免可被該系統管理人員修改 (D) 資訊處理系統、網路設備的鐘訊，應與議定的準確時間來源同步
A	27. 下列何者「無法」加強使用者權限管理？ (A) 強制要求密碼的複雜度（數字、大小寫文字與符號雜湊）與長度 (B) 審查權限變更紀錄 (C) 審查存取權限 (D) 特權帳號審查
B	28. 關於系統安全性中，IETF（Internet Engineering Task Force）制定的 AAA 協定，下列何者定義主要說明認證機制？ (A) Applicability (B) Authentication (C) Authorization (D) Accounting
B	29. 公司將資訊系統的資料進行備份，最主要是為了保護資訊安全中的何種特性？ (A) 機密性（Confidentiality） (B) 可用性（Availability） (C) 完整性（Integrity） (D) 真確性（Authenticity）
D	30. 為了確保資訊依其對組織之重要性，受到適切等級的保護，下列何者「不」為其控制要求？ (A) 資訊之分級 (B) 資訊之標示 (C) 資訊之處置 (D) 資訊之統計
B	31. 為強化身份認證機制，我們常會使用雙因素認證機制，下列何種組合並「不」屬於雙因素認證的定義？ (A) 密碼（Password）+RFID 感應卡（如悠遊卡） (B) RFID 感應卡+自然人憑證 IC 卡 (C) 自然人憑證 IC 卡+指紋 (D) 指紋+密碼

A	32. 智慧財產權（Intellectual Property Rights）是指由人類思想、智慧、創作而產生具有財產價值的產物。下列何者「不」屬於智慧財產權？ (A) 肖像權 (B) 專利權 (C) 著作權 (D) 軟體版權
C	33. 下列何者「不」是組織在實作資訊安全營運持續時的必要做法？ (A) 任命有經驗及能力可處理事故的人員 (B) 制定營運持續計畫和災害復原的程序 (C) 確保不利於組織情況的災害不會發生 (D) 以文件化記錄營運持續的過程和結果
B	34. 下列何種人員負責風險評鑑後風險處理與殘餘風險結果的核可？ (A) 資產擁有者（Asset Owner） (B) 風險擁有者（Risk Owner） (C) 設備擁有者（Device Owner） (D) 資料擁有者（Data Owner）
B	35. 下列何種技術最常被拿來作為檔案完整性（Integrity）的檢查使用？ (A) ECC (B) SHA2 (C) RSA (D) AES
B	36. 依據資通安全事件通報及應變辦法所訂定的資安事件影響等級，共分為幾種等級？ (A) 3 級 (B) 4 級 (C) 5 級 (D) 6 級
D	37. 請問資通安全管理法的何項子法，有定義資通系統防護基準要求？ (A) 資通安全事件通報及應變辦法 (B) 資通安全情資分享辦法 (C) 公務機關所屬人員資通安全事項獎懲辦法 (D) 資通安全責任等級分級辦法
B	38. 資訊安全管理系統（Information Security Management System, ISMS）採用 PDCA 循環的概念，下列何者「不」包含在此流程中？ (A) 高階管理審查會議 (B) 業務達成率審查

	(C) 內部稽核執行 (D) 災難復原計畫演練
B	39. 關於歐盟一般資料保護規範（General Data Protection Regulation, GDPR），下列敘述何者正確？ (A) GDPR 規範僅限歐盟當地企業及組織 (B) GDPR 主要目標為取回個人對個資的控制權 (C) 若違反 GDPR 規定的義務內容，僅會受到名譽上的損害，並無任何罰款 (D) 保護的個資範圍不包含線上定位資料
D	40. 關於資產分類分級，下列敘述何者較「不」正確？ (A) 可以依照資訊安全三大指標 CIA 進行分類 (B) 大致上可以分為一般、限閱、敏感、機密四種 (C) 分類可以根據各企業組織自行制定自己的分類方式 (D) 資產分類的目的僅是方便識別
D	41. 下列何者「不」屬於風險評鑑之範圍及執行步驟？ (A) 風險分析 (B) 防護措施的選擇 (C) 風險接受 (D) 營運持續計畫
D	42. 下列何者「不」是風險評鑑後，對於風險事項的處理方式？ (A) 風險規避 (B) 風險移轉 (C) 風險控制 (D) 風險再評鑑
D	43. 關於 IPSec 金鑰管理機制，下列敘述何者正確？ (A) IPSec 使用 SKIP 作為金鑰管理協議 (B) IPSec 將 IKE 作為候選協議且從未實作 (C) SKIP 協議分為兩版本：SKIPv1 和 SKIPv2 (D) SKIP 為 IKE 金鑰管理協議的前身
D	44. 下列何者較「不」需要資料加密？ (A) 登入網銀輸入帳密 (B) 線上刷卡購物輸入卡號 (C) 報稅插入自然人憑證 (D) 瀏覽維基百科
B	45. 關於 S/MIME 電子郵件加密協定進行跨組織的資訊往來，下列敘述何者「不」正確？

	(A) 使用者應通過權威憑證機構（CA）來簽署憑證（公鑰） (B) 只針對電子郵件訊息加密，不包含附件 (C) S/MIME 是由美國 RSA 公司所提出之規範標準 (D) S/MIME 使用之憑證應通過權威第三方簽署
C	46. 關於事件應變，下列敘述何者較正確？ (A) 為求時效，一旦找到受感染主機應立即進行證據採樣 (B) 資料收集時，應著重在相關人員的口述資料 (C) 主機與網路證據為常見搜集標的 (D) 鑑識分析之最終目的為反擊攻擊來源
B	47. 事件過後的檢視改善中，「不」包含下列何者？ (A) 組織政策調整 (B) 滿意度調查 (C) 安全設定強化 (D) 教育訓練
A	48. 關於差異備份，下列敘述何者較為正確？ (A) 只備儲存媒體內自上次完全備份後曾更改或新增的檔案 (B) 只備儲存媒體內自上次備份後曾更改或新增的檔案 (C) 只備儲存媒體內第三次備份後曾更改或新增的檔案 (D) 只備儲存媒體內自上次完全備份後曾新增的檔案
C	49. 下列何者「不」屬於營運持續計畫之演練方式？ (A) 模擬測試 (B) 檢查表測試 (C) 黑箱測試 (D) 完全中斷測試
D	50. 企業網路電路的使用較符合資訊安全管理系統（Information Security Management System, ISMS）的何種資產類型？ (A) 軟體資產 (B) 資訊資產 (C) 韌體資產 (D) 服務資產