

中央存款保險公司 109 年進用正式職員甄試試題

甄試類別【代碼】：電腦稽核人員(七職等)【Q5301】

專業科目 1：一、計算機概論；二、資訊安全概論

*入場通知書編號：_____

注意：①作答前先檢查答案卡，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。使用非本人答案卡作答者，該節不予計分。
②本試卷為一張雙面，四選一單選擇題共 80 題，每題 1.25 分，共 100 分，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。
③請勿於答案卡上書寫應考人姓名、入場通知書編號或與答案無關之任何文字或符號。
④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。
⑤答案卡務必繳回，未繳回者該節以零分計算。

- 【2】1.第一代電腦到第四代電腦的分野是根據下列何者？
①發展年份 ②硬體元件 ③功能與用途 ④執行速度
- 【1】2.請問下列何種手段會誘騙使用者透過電子郵件或網站提供其資訊？
①網路釣魚 ②阻斷服務 ③通行碼破解 ④特洛伊木馬程式
- 【3】3.微軟的 Windows Azure 屬於雲端運算架構中，何種層次的服務？
① DaaS ② IaaS ③ PaaS ④ SaaS
- 【1】4.請問 OSI 參考模型中，下列哪一層負責資料封包來源 IP、目的地 IP 位址？
①網路層(Network Layer) ②會議層(Session Layer)
③傳輸層(Transport Layer) ④應用層(Application Layer)
- 【4】5.下列何種伺服器可以提供網域名稱與對應的 IP 位址轉換服務？
① SMTP 伺服器 ② DHCP 伺服器 ③ FTP 伺服器 ④ DNS 伺服器
- 【2】6.請問在資料庫系統中，下列何者可以表示資料表中包含一組欄位，其儲存的資料無重複？
①資料列 ②主鍵 ③外來鍵 ④綱要
- 【4】7.電腦的主記憶體容量有限，作業系統必須協調主記憶體的分配與利用，讓程式執行完成後，由主記憶體中釋放，再讓其他程式使用，以上敘述說明作業系統的何項功能？
①提供使用者操作介面 ②提供網路服務與安全管理
③控制輸入／輸出程序 ④分配系統資源
- 【1】8.程式語言中有分為直譯式程式語言及編譯式程式語言，請問下列何組合為直譯式程式語言？
① PHP ② C ③ C++ ④ PASCAL
- 【1】9.在關聯式資料庫中有許多敘述，下列何者不屬於更修敘述？
① SELECT ② UPDATE ③ DELETE ④ INSERT
- 【1】10.在現今網際網路盛行的年代，網站的 URL 多數為 https://www.xxx.xxx.xxx，這代表該網站使用何種安全機制？
① SSL/TLS ② SAP ③ SAT ④ SET
- 【4】11.網際網路(Internet)使用下列何項資料交換技術運作？
①訊息交換(Message Switching) ②數位交換(Digital Switching)
③電路交換(Circuit Switching) ④分封交換(Packet Switching)
- 【3】12.一個資料庫交易(Database Transaction)在執行時，可將資料庫看成其專屬，而不用去考慮其他同時執行的交易，指的是：
①單元性(Atomicity) ②一致性(Consistency) ③隔離性(Isolation) ④永久性(Durability)
- 【1】13.下列何種網頁語言是由伺服器端執行後將結果傳給使用者端，而不是由瀏覽器下載到使用者端？
① ASP ② HTML ③ JavaScript ④ VBScript
- 【3】14.請問負責 CPU 與其他低速周邊裝置溝通的是下列何者？
① BIOS ② DRAM ③南橋晶片 ④北橋晶片
- 【2】15.請問如果 12.35.57.78、12.35.57.79、12.35.58.80 這三個 IP 位址是在同一個子網路，請問此時使用的子網路遮罩為下列何者？
① 255.0.0.0 ② 255.255.0.0 ③ 255.255.255.0 ④ 255.255.255.255
- 【3】16.資料庫系統中在關聯式資料表中，假設有設定外來鍵(Foreign Key)，請問外來鍵有何功能性？
①為資料加密 ②為資料作排序(sort)
③為資料建立鏈結(link) ④為資料掃毒
- 【3】17.在電腦 CPU 執行一個指令過程稱之為機器週期(Machine Cycle)，在一個機器中，其一個機器週期內，一個指令被分為 5 個步驟，來加以執行。分別為：(A)指令解碼(Instruction Decode) (B)指令執行(Instruction Execution) (C)指令擷取(Instruction Fetch) (D)記憶體存取(MEMmory Access) (E)結果回存(Result Write Back)，正確步驟應為下列何者？
① (A) (B) (C) (D) (E) ② (C) (B) (A) (D) (E) ③ (C) (A) (B) (D) (E) ④ (B) (C) (A) (D) (E)

- 【3】18.根據密碼系統中加密金鑰和解密金鑰之間關係，可將密碼系統分為對稱式密碼系統及非對稱式密碼系統，下列何種屬於非對稱式密碼系統？
① DES ② RC5 ③ RSA ④ AES
- 【2】19.對關聯式資料庫的關聯 R 與 S 做 R JOIN S 之合併，若結果保留 R 中的每個值組(Tuples)，則此合併稱為下列何者？
① INNER JOIN ② LEFT OUTER JOIN ③ RIGHT OUTER JOIN ④ FULL OUTER JOIN
- 【2】20.請問一具有 n 個位元的電腦系統採用 1 的補數法來表示負整數，則所能表示的最小整數為何？
① -2ⁿ⁻¹ ② -2ⁿ⁻¹ + 1 ③ -2ⁿ ④ -2ⁿ + 1
- 【1】21. SQL 隱碼(SQL Injection)是網路駭客最常使用的攻擊手法，下列敘述何者正確？
①透過更改語法邏輯或是加入特殊指令的方式，將攻擊指令放入資料庫命令中，藉以竊取或竄改資料
②利用仿冒的網站引誘使用者進入藉此騙取資料
③利用程式寄出大量廣告垃圾信件灌爆信箱使其無法正常運作
④藉由不斷猜測帳號與密碼入侵他人電腦
- 【3】22.某微處理器時脈頻率為 100 MHz，假設執行 1 個指令需要 4 個時脈，則執行該指令需要多少時間？
① 0.4 ns ② 4 ns ③ 40 ns ④ 400 ns
- 【1】23.下列何者非屬輔助記憶體？
① RAM ② SSD ③ HDD ④ SDHC
- 【3】24.作業系統管理的各種資源，不包括下列何者？
① CPU ②磁碟空間 ③外接投影機電源 ④記憶體
- 【2】25.下列何者非屬開放性原始碼作業系統？
① Android ② Windows ③ Linux ④ Free-BSD
- 【1】26.在 IP 位址中，.org 代表下列何種組織？
①財團法人或公益團體 ②教育、學術機構 ③網路服務組織 ④商業團體、公司行號
- 【4】27. IPv4 位址是由多少位元(bit)組成？
① 4 ② 8 ③ 16 ④ 32
- 【3】28. IPv6 位址是由多少位元(bit)組成？
① 32 ② 64 ③ 128 ④ 256
- 【3】29.有關物聯網的敘述，下列何者錯誤？
①可感知周遭環境如溫度等變化 ②英文縮寫為 IoT
③ RFID 不屬於物聯網的應用技術
④由實際物體經由嵌入式感測器和 API 等裝置，透過網際網路所形成的訊息連結與交換網路
- 【1】30.企業對消費者的線上交易行為之簡稱為下列何者？
① B2C ② B2B ③ C2C ④ O2O
- 【1】31.下列何種檔案類型帶有電腦病毒的機率最小？
① txt 檔 ② doc 檔 ③ JavaScript ④ ActiveX
- 【2】32.下列何者非屬物件導向程式語言？
① JAVA ② C ③ PHP ④ Python
- 【3】33.二進位表示法(11101.11)₂用十進位表示，為下列何種數目？
① (28.87)₁₀ ② (18.86)₁₀ ③ (29.75)₁₀ ④ (39.74)₁₀
- 【1】34.下列何項檔案格式的壓縮方式為破壞性壓縮(lossy compression)？
① JPEG ② BMP ③ PNG ④ TIFF
- 【2】35.下列何者非屬 TCP/IP 協定家族？
① SMTP ② WEP ③ POP3 ④ DNS
- 【2】36.有關 SSL 協定的敘述，下列何者正確？
①可以辨認消費者是否就是實際付款當事人 ②線上交易時，能確保線上資料傳輸時的隱密性
③需要向認證中心取得認證 ④使用 SSL 協定之購物網站無法取得消費者信用卡資料
- 【1】37.有關電腦病毒或惡意程式的敘述，下列何者錯誤？
①木馬程式屬於間諜程式的一種，會導致使用者電腦中的資料損毀或無法開機
②電腦病毒是指具有破壞性或是惡作劇性質的電腦程式
③開機型病毒會潛伏在磁碟啟動區，只要用感染病毒的磁碟開機，病毒可能會進入記憶體
④定期備份是一種預防勒索軟體病毒的方法
- 【4】38.下列何者非屬資料庫管理系統的優點？
①改進資料完整性 ②降低資料重複性
③縮短開發時間
④跟一般檔案處理系統相比，資料庫系統可以使用較少的記憶體
- 【3】39.乙太網路是最普遍的有線區域網路通訊協定，其制定的標準為下列何者？
① IEEE 802.11 ② IEEE 802.2 ③ IEEE 802.3 ④ IEEE 802.4

【請接續背面】

- 【2】40.防火牆的主要功能為下列何者？
①防止所有封包送出 ②防止未經認可的封包進入
③防止未經認可的封包送出 ④防止所有封包進入
- 【4】41.就目前科技而言，下列何種加密方法安全性最高？
① DES ② Triple DES ③ AES-128 ④ AES-256
- 【2】42.下列何項技術發送訊息者無須與接收訊息者先建立共同密鑰，即可加密訊息送給接收訊息者？
① Triple DES ② RSA ③ AES ④ Sha 256
- 【4】43. DDoS 攻擊為 DoS 攻擊之進階版，DDoS 之字首 D 代表的意義為何？
① Denial ② Dead ③ Distributor ④ Distributed
- 【2】44.下列何種攻擊為威脅資訊安全中的 integrity？
① snooping ② modification ③ replaying ④ denial of service
- 【1】45.電腦駭客在合法網站上插入惡意的 HTML 或 Script 程式，以散布惡意程式，可歸屬何種攻擊？
①跨站腳本攻擊 ②殭屍網路攻擊 ③進階持續攻擊 ④零時差攻擊
- 【1】46.若以發生外部入侵資訊系統事件，下列何者最能協助調查入侵情況？
① system log ② firewall ③ anti-virus software ④ router
- 【2】47.下列何種策略是適當防範 SQL Injection 攻擊的做法？
①增加 password 的長度 ②檢視或過濾輸入字元是否恰當
③不使用 SQL 資料庫 ④嚴格要求定期變更 password
- 【4】48.下列何種國際標準與 ISMS 關聯性最高？
① ISO 9001 ② ISO 20000 ③ ISO 20001 ④ ISO 27001
- 【1】49.下列何者與數位憑證的實施與運作關聯性最高且最直接？
① X.509 ② X.680 ③ X.800 ④ X.903
- 【3】50.以 ISO 之 OSI 網路模型為基礎，防火牆的運作通常不涉及哪一層？
① L3 ② L4 ③ L6 ④ L7
- 【3】51.以多層次防禦概念，下列何者為最內層的防禦？
①應用防禦 ②主機防禦 ③資料防禦 ④網路防禦
- 【1】52.下列哪一 ISO 標準和 Common Criteria 最為相關？
① ISO 15408 ② ISO 19001 ③ ISO 20001 ④ ISO 27001
- 【2】53.下列何者與「安全通道(tunneling)」技術關聯性最低？
① HTTPS ② PGP ③ SSH ④ VPN
- 【3】54.下列何者與無線網路安全的加密機制無關？
① WPA2 ② WEP ③ WAP ④ TKIP
- 【4】55.下列何者不包含在資訊倫理議題之 PAPA model 中？
① Property ② Accuracy ③ Access ④ Public
- 【3】56.下列何種攻擊為威脅資訊安全中的 availability？
① repudiation ② masquerading ③ denial of service ④ replaying
- 【4】57.下列何種協定可以讓多部組織內部電腦在 Internet 中以一共用 IP 與外網節點交換資料，進入內網才再區分至各自電腦 IP？
① DHCP ② DMZ ③ VLAN ④ NAT
- 【1】58.若明文大小為 1024 位元以 AES-256 技術進行加密時，運算過程明文將會被以何種區塊大小進行執行加密運算？
① 128 bits ② 192 bits ③ 256 bits ④ 1024bits
- 【3】59.下列何種攻擊是透過統計多筆智慧卡計算時間或消耗的電力，嘗試推算出晶片內密鑰的作法？
① lancet attacks ② manipulative attacks
③ side-channel attacks ④ physical invasive attacks
- 【1】60.電腦惡意程式會對電腦造成傷害，其中會主動透過網路及系統漏洞擴散的惡意程式稱為何？
①蠕蟲(Worm) ②病毒(Virus) ③後門(Back Door) ④殭屍(Bot)
- 【3】61.以叢集與負載平衡方式建立 HA 伺服器架構是要保證下列何項？
①機密性 ②完整性 ③可用性 ④適應性
- 【2】62. IPSec 技術是用來實作下列何種網路服務？
① OSPF ② VPN ③ SSL ④ WAF
- 【3】63.下列何者非屬資訊安全三要素 CIA 之一員？
①可用性 ②機密性 ③認證性 ④完整性
- 【1】64.下列何種習慣可以預防成為網路犯罪的受害者？
①定期更新防毒軟體與系統
②存有會議簡報之隨身碟只交給主辦方工作人員用其電腦讀取
③郵件寄件者只要是熟人，就放心的開啟該郵件的附件
④在臉書上只將旅遊打卡資料分享給好友

- 【2】65.臨時離開座位時，應該執行下列何項動作？
①趁這個時間自網路下載之後需要用到的檔案
②啟動需要密碼才能解鎖之螢幕保護程式
③關閉電腦螢幕電源，讓他人不能看到進行中的工作
④只是臨時離開，保持開機狀態，以節省重新開機時間
- 【4】66.資料備份是一項重要但繁瑣的工作，尤其是當需要備份的資料十分龐大時，更是需要耗費大量時間才能完成，請問資料備份是為了保護下列何者？
①資料的機密性 ②資料的鑑別性 ③資料的不可否認性 ④資料的可用性
- 【3】67.生物驗證中當不是合法使用者卻被驗證為合法使用者，這種結果被列入下列何種比率計算？
①正確接受率 ②正確拒絕率 ③錯誤接受率 ④錯誤拒絕率
- 【2】68.在嘗試破解登入系統或是文件加密的密碼，其中一項技術是嘗試用英文單字(Word)來破解，稱之為何？
①重送攻擊 ②字典攻擊 ③暴力破解 ④中間人攻擊
- 【1】69.下列何種伺服器的服務具備防火牆功能，可以保護內部用戶主機上網的安全？
① Proxy Server (代理伺服器) ② Sandbox Server (沙箱伺服器)
③ Web Server (網頁伺服器) ④ VPN Server (虛擬私有網路伺服器)
- 【2】70.電子郵件社交工程攻擊是網路入侵主要的管道之一，組織為避免成為受害者，主要需要採用下列何種應變機制？
①嚴格控管作業系統中的使用者帳號
②透過教育訓練等方式，提高使用者警覺性並加強其危機意識
③對於高階人員提高其使用者權限
④強制從組織寄出的郵件都要加上數位簽章
- 【3】71.管理者如果要使用命令列(Command Line)進行遠端系統管理，為避免傳輸的資料被擷取，要使用何種應用程式？
① ftp ② ping ③ ssh ④ telnet
- 【4】72.資訊安全管理的推動除考量安全性之外，也要採取可以運作的做法，因此下列何者為其重要觀念？
①追求絕對的安全性，避免危及資訊安全
②為降低資訊安全問題，減少使用資訊科技產品
③僅能使用直接相關的資訊技術，以避免資訊技術太新造成資訊安全威脅
④透過控制方法，把對資訊資產之風險降低到可接受的程度
- 【1】73.下列何種攻擊可以不需要利用軟體系統的漏洞？
①阻斷服務(Denial of Service) ②緩衝區溢位(Buffer Overrun)
③後門(Back Door) ④ SQL 隱碼(SQL Injection)
- 【1】74.運用各種控制措施與系統稽核工具對系統安全進行之測試審查，是屬於下列何種工作？
①技術審查 ②管理審查 ③風險審查 ④合規審查
- 【2】75. Radius 伺服器提供的是 AAA 服務，下列何者非屬 Radius 伺服器服務的內涵？
①審計或計帳(Accounting) ②稽核(Audit)
③認證(Authentication) ④授權(Authorization)
- 【4】76.電子郵件加入數位簽章，可以：
①對郵件內容加密 ②證明郵件不含病毒
③在收件者開啟郵件時發送回執信件 ④驗證寄件者身份
- 【3】77.下列何者與 SQL 隱碼(SQL Injection)的防護無關？
①網站伺服器不提供錯誤訊息給使用者
②網站伺服器之程式對於網頁資料輸入檢查是否符合規範與限制
③作業系統安裝防毒軟體並定期更新作業系統
④限制網頁應用程式存取資料庫的權限
- 【2】78.目前 Windows 預設開啟使用者帳戶控制(User Account Control; UAC)功能，請問這項功能的作用為何？
①設定用戶定期變更密碼的管理 ②限制應用軟體對系統層級的存取
③管制用戶可以使用電腦的時間 ④控制用戶使用網路的權限，避免用戶連線到不當內容網站
- 【1】79.網域名稱伺服器(DNS)主要提供網域名稱轉換成 IP 位址的服務，但在電子郵件服務方面，近年也發展出利用 DNS 服務來強化電子郵件服務的安全性，請問用 DNS 中 TXT 紀錄列出驗證郵件標頭與郵件內容二者之數位簽章所需的公開金鑰是何項技術？
① DKIM (DomainKeys Identified Mail)
② DMARC (Domain-based Message Authentication, Reporting and Conformance)
③ PSK (Pre-Shared Key)
④ SPF (Sender Policy Framework)
- 【4】80.安全政策是組織在施行資訊安全管理重要的依據，下列何種項目可以確保所有的運作均能按照既定的政策執行？
①持續營運計畫(Business continuity plan) ②群組權限管理(Group privilege management)
③技術審查(Technical Review) ④內部與外部稽核(Audit)