# 兆豐國際商業銀行 106 年新進行員甄選試題

**甄試類別【代碼】：系統、網路管理人員【K0305】**
**科目二：資訊安全**

**＊請填寫入場通知書編號：＿＿＿＿＿＿＿＿**

注意：①作答前須檢查答案卡（卷）、入場通知書編號、座位標籤號碼、甄試類別是否相符，如有不同應立即請監試人員處理，否則不予計分。
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，合計 60 分】與【非選擇題 2 題，每題 20 分，合計 40 分】，共 100 分。
③選擇題限以 2B 鉛筆於答案卡上作答，請選出最適當答案，答錯不倒扣；未作答者，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、入場通知書號碼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、工程函數功能、儲存程式功能)，但不得發出聲響；若應考人於測驗時將不符規定之電子計算器放置於桌面或使用，經勸阻無效，仍執意使用者，該節扣 10 分；該電子計算器並由監試人員保管至該節測驗結束後歸還。
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 40 題（每題 1.5 分）

【3】1.在公開金鑰基礎建設（PKI）環境中，有關加解密的敘述，下列何者正確？
①用小金的私鑰加密的訊息，只有小金的私鑰可以解密
②用小金的公鑰加密的訊息，只有小金的公鑰才能解密
③用小金的公鑰加密的訊息，只有小金的私鑰可以解密
④用小金的私鑰加密的訊息，只有小金的公鑰可以解密

【1】2.關於職務變更安全控管的敘述，下列哪些正確？ A.員工職務變更或離職前，應將其所有屬組織的資產歸還給組織、B.員工一離職，應立即取消或刪除該人員之存取權限、C.應定期檢視使用者帳號，以清查是否有已調職或離職之使用者帳號仍存在於系統中、D.員工離職後，如自動排程程式仍須以離職人員的帳號執行，則可保留該帳號持續使用
①僅 ABC ②僅 BCD ③僅 ACD ④僅 ABD

【2】3.系統管理員可能常須將伺服器的映像檔轉換為一個虛擬實例(Virtual Instance)，下列何者最能適切說明虛擬化伺服器的資訊安全要求，以確保較佳的安全性？
①虛擬化伺服器要求作業系統強化，但不用更新防毒檔
②虛擬化伺服器的資訊安全要求必須和實體伺服器一樣
③虛擬化伺服器需要資安控制措施，但是不需要版權
④虛擬化伺服器從系統管理程序繼承資訊安全需求

【3】4.某公司允許部分員工可使用遠端登入方式進入公司電腦來工作，以提供靈活的工作條件，請問哪些技術可以用來提供較佳安全性的遠端登入環境？ A.子網路切割、B.網路存取控制、C.防火牆、D.虛擬私有網路
①僅 AB ②僅 BC ③僅 CD ④僅 AD

【1】5.採取下列哪項安全措施，較能有效防止網路遭受 ARP 欺騙攻擊？
①虛擬區域網路隔離 ② IP 過濾器 ③網際網路安全協定 ④日誌分析

【4】6.如果行動設備受到惡意攻擊破壞，為了減輕其內部所儲存的數據資料內容遭竊取的風險，採取下列何種措施是較好的防範措施？
①通用管制卡 ②強密碼的複雜性 ③生物驗證 ④全磁碟加密

【4】7.安全管理人員在檢查網站伺服器的連線記錄時，發現該伺服器在執行過一個特定的搜索字串後，該公司的網路商店便立即崩潰當機。請問該伺服器最可能遭受到何種類型的攻擊？
①欺騙攻擊 ②垃圾信息 ③重送攻擊(Replay Attack)④阻斷服務(DoS)攻擊

【1】8.使用者向安全管理人員反應無法下載某些網站的任何資料檔案，安全管理人員亦收到有關在網路出現可疑流量的警告訊息。請問下列何者是最可能發生此種狀況的原因？
①網路式入侵防禦系統(IPS)正在阻止從特定網站來的流量
②防火牆(Firewall)正在阻止網站活動
③路由器(Router)正在阻止所有從特定網站來的流量
④網路式入侵偵測系統(IDS)正在阻止從特定網站來的流量

【3】9.小金在瀏覽網際網路時，發現瀏覽器出現正在下載檔案的訊息，隨後系統便發生崩潰當機狀況。在重新啟動電腦後，系統性能卻變得異常緩慢，並出現數百個對外連線分別連接到不同的網站。請問小金的個人電腦最可能發生何種狀況？
①該部電腦已被間諜軟體感染 ②該部電腦已被廣告軟體感染
③該部電腦已成為殭屍網路的一部分 ④該部電腦已變成垃圾郵件主機

【4】10.為了避免使用者收到不想要的電子郵件或廣告，安全管理人員可採用何種工具軟體以協助管理？
①反間諜軟體 ②主機式防火牆 ③防毒軟體 ④反垃圾郵件軟體

【4】11.為有效防制 Web 應用程式遭受 SQL 注入攻擊，下列哪項安全措施最為需要？
①安裝操作系統缺少的安全更新 ②更改伺服器的 SSL 私鑰，並把前一個私鑰提交至 CRL
③安裝主機型防火牆 ④添加表單輸入驗證功能

【2】12.使用者反應不能夠傳送文件到伺服器上，而安全管理人員確定網路防火牆的相關傳輸埠是開放的。請問安全管理人員接下來應該要繼續檢查下列哪一項？
①反垃圾郵件軟件 ②存取控制清單 ③防毒軟體 ④網路型入侵偵測系統

【2】13.安全管理人員若要限制使用者在 19:00 後不能連線銷售部門的伺服器，並在任何時候都不准連線會計部門的網路。請問安全管理人員應該實施哪二種項措施，即可達成上述目的？ A.職責分離、B.時間限制、C.存取控制清單、D.強制登入控制
① AB ② BC ③ CD ④ AD

【3】14.某公司頒布的密碼使用政策中，規定密碼有效期限為 90 天，且更換新密碼時不能是最近 5 次使用過的舊密碼。然而有些員工卻想利用連續更改密碼 5 次，然後再重新使用回原來舊密碼的方式來規避該密碼使用政策。請問在最少管理工作量的前提下，管理人員可以採取哪項作法來防止員工的上述不安全投機作法？
①監視員工帳戶，將更改密碼過度的員工鎖定其帳戶②限制密碼必須不小於 10 個字符
③限制密碼每天不能更改一次以上 ④監視員工帳戶和更改密碼行為，找出這樣做的員工

【4】15.透過避免使用 HTML 標籤的方式，可以減輕 Web 應用程式的何種安全弱點的攻擊？
①緩衝區溢(Buffer Overflow)攻擊 ② SQL 注入(SQL Injection)攻擊
③ LDAP 注入(LDAP Injection)攻擊 ④跨站腳本(Cross-Site Scripting, XSS)攻擊

【3】16.哪二項是使用數位簽章(Digital Signature)所要達到的主要安全目的？ A.完整性(Integrity)、B.機密性(Confidentiality)、C.不可否認性(Non-Repudiation)、D.可用性(Availability)
① AB ② CD ③ AC ④ BD

【2】17.安全管理人員完成一台電腦的記憶體鑑識圖像後，可再採取何種安全措施來確保該圖像的完整性(Integrity)？
①將圖像透過 AES128 加以運算 ②將圖像透過 SHA256 加以運算
③把圖像壓縮成密碼保護的檔案 ④將圖像透過一個對稱加密算法加以運算

【4】18.淘汰舊的硬碟前，首先應執行哪項措施後再行淘汰，較能避免資料外洩？
①格式化硬碟 ②刷新硬碟韌體 ③使用廢物處置設施 ④執行位元級別的擦除或覆寫

【3】19.企業執行滲透測試的最主要原因為何？
①確定企業內的所有漏洞和弱點 ②找出忠誠度不高的員工
③確定安全威脅對企業的影響 ④提供安全管理人員的培訓需求

【4】20.當公司使用雲端服務業者提供的雲端運算服務後，通常會喪失掉何種安全控制措施？
①接觸應用程式的管理設定 ②接觸數據資料的管理性存取
③數據資料的邏輯控制 ④數據資料的實體控制

【3】21.小金平時使用密鑰以對稱式密碼機制加密文件，當小金離職後，安全管理人員立即將其帳戶刪除，則日後最可能出現哪二項後果？ A.須重新創建小金的帳戶來查閱先前文件內容、B.使用恢復代理來解密先前被加密的文件、C.使用 root 帳號來查閱文件內容、D.文件內容是不可恢復的
① AB ② CD ③ BD ④ AC

【3】22.滲透測試須經由系統所有者的書面同意，並只在受控制條件下進行的主要原因為何？
①弱點掃描器在風險評估過程會造成大規模的網路流量
②滲透測試是針對安全控制措施執行被動測試的策略，並能識別出漏洞
③滲透測試主動測試各項安全控制措施，並可能導致系統不穩定
④白箱滲透測試無法識別零時差漏洞(Zero-day exploit)

【2】23.如果喪失解讀資料的能力是無法接受的，實施 PKI 的相關保護時，應該要求下列何種安全措施較妥當？
①憑證撤銷清單(CRL) ②金鑰託管(Key Escrow)）
③信任網站 ④不可否認性

【請接續背面】

【2】24.安全管理人員在查核伺服器、遠端登入及 IDS 系統的日誌時，發現有惡意的內部員工使用個人的筆記型電腦，透過 VPN 連接進入公司系統並竊取數據資料。事後，公司想要檢查該員工的筆記型電腦，以確定損失程度，但該員工聘請的律師堅持筆記型電腦是無法識別的。請問下列哪項資訊是最能用來識別該部特定的電腦？
①電腦主機名稱　② MAC 地址　③ IP 地址　④用戶配置文件

【1】25.小金身為公司的安全管理人員，其擁有完全的網路管理權限，而公司要求小金與其他管理人員均須每季相互更換管理員角色與工作。請問這種形式的控制措施稱為下列何者？
①職務輪調(Job rotation)　②強制性休假(Mandatory vacations)
③最小權限(Least privilege)　④權責區分(Separation of duties)

【3】26.遠端辦公室人員反映無法登入使用主要辦公室的任何網路資源，而安全管理人員在完成問題除錯改正後，嘗試 ping 遠端辦公室之路由器卻一直沒有收到回應，但是卻能夠遠端登入到該路由器。請問下列何者最可能是安全管理人員無法 ping 到該遠端路由器的原因？
①主要辦公室的路由器故障　②遠端路由器的 SNMP 被關閉
③遠端路由器的 ICMP 被關閉　④遠端路由器的 IPSec 被封鎖

【4】27.數據中心經常會在半夜執行數據資料的異地備份工作。請問哪項措施較能在發生災難時，盡快恢復或維持系統運作，以確保最少的停機時間？
①數據資料的異地備份位置，也有備用的伺服器　②數據資料的異地備份位置，也有冷備援(Cold site)
③數據資料的異地備份位置，也有暖備援(Warm site)　④數據資料的異地備份位置，也有熱備援(Hot site)

【3】28.替代(Substitution)是基本的加密技術之一，若明碼形式之本文為 MADAM，下列何者不是替代技術加密後所產生的密文？
① KOPOK　② NQVQN　③ ASADH　④ 1301040113

【2】29.社交工程會造成資訊安全極大威脅的最主要原因為何？
①隱匿性高，不易追查惡意者
②惡意人士不須具備頂尖電腦專業技術即可輕易避過企業的軟硬體安全防護
③利用通訊埠掃瞄(Port Scan)方式，無從防範
④破壞資訊服務可用性，使企業服務中斷

【2】30.小金為了安裝盜版軟體特地下載一個金鑰破解工具，當執行該破解工具後，系統性能變得非常緩慢，並出現許多病毒警訊。請問該破解工具最可能是含有何種類型的惡意軟體？
①蠕蟲　②特洛伊木馬　③廣告軟體　④邏輯炸彈

【2】31.下列敘述何者錯誤？
①防火牆主要建置於內部網路與外部網路之間
②電路層閘道器可應用於高階硬體設備上，可支援 URL 的過濾功能
③應用層代理伺服器主要用在防火牆執行之程式
④屏障式防火牆主要用來過濾封包，又稱為封包過濾式防火牆

【4】32.「駭客用來掩護非法入侵以取得使用者權限之工具，並傳送給網路其他駭客來取得 root 或特殊的權限」，係指下列何者？
① Clickjacking　② Spyware　③ Haox　④ Rootkit

【3】33.關於「Honey Pots」，下列敘述何者正確？ A.將系統最有價值的部分隱藏，降低入侵者的目光、B.預先偵測可能入侵者的 IP，以及時阻斷其攻擊、C.設計一假的系統引誘入侵者
①僅 AC　②僅 AB　③僅 C　④ABC

【1】34.「異地備援服務提供商只提供資料處理中心的作業環境，但不包括中心內部所需要之電腦軟硬體」，係指下列何者？
①冷備援　②熱備援　③暖備援　④溫備援

【2】35.若員工利用公司電腦來訂購網路商品，此行為係指係下列何者？
①資訊竊取　②未經授權存取、使用　③網路授權　④身分驗證

【3】36.下列何者不屬於資訊安全管理規範？
①BS 7799　②ISO 27002　③ISO 14001　④ISO 27001

【3】37.關於足跡追蹤(footprinting)，下列敘述何者正確？
①駭客擷取使用者使用系統的歷程
②管理者用來稽核系統弱點的行為
③駭客評估欲攻擊目標系統的行為
④管理者分析系統被開啟之通訊埠

【4】38.關於電腦資訊犯罪相關之法律制定與實施仍有困難的因素，下列何者正確？ A.全球化因素致使國際間法律界限與司法管轄權更加模糊、B.各國法律規範標準不一，執行的程度產生落差、C.資訊科技快速演進，新法的制定可能造成新的問題
①僅 BC　②僅 AB　③僅 AC　④ ABC

【1】39.許多網路購物平台會利用何種機制以記錄消費者的瀏覽紀錄？
①Cookies　②Content filtering　③Adware　④Spoofing

【2】40.評估發生資訊安全漏洞所造成的損失（如有形損失或無形損失），係指下列何者？
①弱點分析　②風險分析　③威脅分析　④對策分析

## 貳、非選擇題 2 題（每題 20 分）

**第一題：**

請就使用雲端服務時，造成資料外洩，衍生資訊安全疑慮的原因？若您是企業之資訊安全長，您會採取哪些管理措施？請詳細說明至少三個原因與相應措施。【20 分】

**第二題：**

資料須經嚴謹的密碼系統進行加解密處理，以提升資訊安全性，因此若要判斷一個密碼系統的優劣，可以經由哪些因素進行評估？請詳細說明之。【20 分】