國營臺灣鐵路股份有限公司
115年從業人員甄試試題

應試類科：第9階-事務員-資訊
測驗節次：第二節
測驗科目：網路通訊與資通安全概要

—作答注意事項—

①應考人須按編定座位入座，作答前應先檢查答案卡，入場證號碼、桌角號碼、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，不予計分。

②測驗期間，嚴禁隨身攜帶及使用行動電話或其他具可傳輸、掃描、交換或儲存資料功能之電子通訊器材或穿戴式裝置(包括但不限於：微型耳機、智慧型手錶、智慧型手環、智慧型眼鏡、電子字典、個人數位助理機、呼叫器等)，並不得置於座位四周或放置於作答區，違者該節以零分計。

③答案卡須保持清潔完整，請勿折疊、破壞或塗改入場證號碼及條碼，亦不得書寫與答案無關之任何文字或符號。

④本試題本為雙面，總分共100分，答案卡每人一張，不得要求增補。未依規定劃記答案卡，致讀卡機器無法正確判讀時，由應考人自行負責，不得提出異議。

⑤試題若有選擇題，限用2B鉛筆作答。請按試題之題號，依序在答案卡上同題號之劃記答案處作答，單選題在ABCD四個選項中選擇一個正確的答案，若有複選題在ABCDE五個選項中選擇所有正確的答案。未劃記者，不予計分。欲更改答案時，請用橡皮擦擦拭乾淨，再行作答，切不可留有黑色殘跡，或將答案卡汙損，也切勿使用修正帶或其他修正液。

⑥試題若有手寫題及作文，限用筆尖較粗之黑色或深藍色原子筆或墨水筆，不得使用鉛筆。在答案卡上規定的區域紅色框線內書寫，不得超出框線。修正時只可使用修正帶，不可使用修正液。若因字跡潦草、超出框線、寫到別的題號位置、或修正不清等原因，致評閱人員無法清楚辨識者，應考人責任自負。

⑦測驗結束前不得離場，擅自離場者以零分計。考試結束，試題本及答案卡務必繳回，未繳回者以零分計。

禁止翻面

讀完本頁說明，**鐘響時**才可以開始作答；翻面以違規記。

00000072

單選題【四選一，共50題，每題2分，共100分】

1 開放系統互連七層模型中，最上層是哪一層？
(A) 實體層
(B) 應用層
(C) 資料連結層
(D) 網路層

2 開放系統互連七層模型中，最下層是哪一層？
(A) 會議層
(B) 傳輸層
(C) 實體層
(D) 表示層

3 用來把網路位址對應到硬體位址的協定是？
(A) 位址解析協定
(B) 網域名稱系統
(C) 動態主機設定服務
(D) 檔案傳輸協定

4 家用網路中，常用來分享網路給多台設備的設備是？
(A) 滑鼠
(B) 鍵盤
(C) 路由器
(D) 喇叭

5 常見的網路位址格式由幾組數字組成，中間用點分隔？
(A) 兩組
(B) 三組
(C) 五組
(D) 四組

6 自動分配網路位址與相關設定的服務是？
(A) 動態主機設定服務
(B) 網域名稱系統
(C) 檔案壓縮服務
(D) 防毒服務

7 把網站名稱解析成網路位址的服務是？
(A) 網域名稱系統
(B) 印表服務
(C) 時間同步服務
(D) 備份服務

8 在電腦中，用來測試能不能連到對方並收到回應的工具是？
(A) 文字輸入工具
(B) 回音測試工具
(C) 圖片剪裁工具
(D) 磁碟清理工具

9 把一個網段分成更小的多個網段，這個動作叫什麼？
(A) 檔案合併
(B) 子網切割
(C) 螢幕截圖
(D) 音量調整

10 一般未加密的網頁瀏覽服務，常用的通訊埠號是？
(A) 二十一
(B) 五十三
(C) 四四三
(D) 八十

11 加密的網頁瀏覽服務，常用的通訊埠號是？
(A) 四四三
(B) 二十五
(C) 八十
(D) 一一零

12 負責把電子郵件送出去的協定名稱是？
(A) 檔案傳輸協定
(B) 時間同步服務
(C) 網域名稱系統
(D) 簡單郵件傳輸協定

13 服務品質在網路中，最主要想改善的是？
(A) 鍵盤手感
(B) 電池容量
(C) 螢幕亮度
(D) 延遲與抖動

14 資訊安全三要素最常指哪三項？
(A) 速度，容量，價格
(B) 重量，高度，寬度
(C) 機密性，完整性，可用性
(D) 畫質，音質，亮度

15 木馬程式最常見的特徵是？
(A) 只能在印表機使用
(B) 一定是硬體故障
(C) 假裝正常程式誘人安裝
(D) 只會讓螢幕變亮

16 把資料變成看不懂的內容，讓只有持有金鑰的人才能讀懂，叫什麼？
(A) 備份
(B) 壓縮
(C) 加密
(D) 排序

17 對稱式加密最符合的描述是？
(A) 加密與解密用同一把金鑰
(B) 一定不需要金鑰
(C) 只能保護圖片
(D) 只能在離線使用

18 非對稱式加密最符合的描述是？
(A) 使用一把公鑰與一把私鑰
(B) 只有一把共同金鑰
(C) 完全不需要驗證
(D) 只能在同一台電腦

19 網站使用憑證最主要是為了什麼？
(A) 讓字體變大
(B) 讓電腦降溫
(C) 讓鍵盤更滑
(D) 確認身分並建立加密連線

20 最小權限原則的意思是？
(A) 每個人都有最高權限
(B) 所有人都不能登入
(C) 只給完成工作需要的最少權限
(D) 所有人都用同一個帳號

21 依角色分配權限的存取控制方式是？
(A) 隨機分配權限
(B) 角色為基礎存取控制
(C) 依顏色分配權限
(D) 依身高分配權限

22 防火牆最主要的功能是？
(A) 依規則允許或阻擋網路連線
(B) 修理硬碟壞軌
(C) 提高螢幕解析度
(D) 增加鍵盤按鍵

23 集中收集日誌並做關聯分析與告警的系統是？
(A) 安全資訊與事件管理系統
(B) 檔案瀏覽系統
(C) 影像剪輯系統
(D) 音樂播放系統

24 三二一備份原則最正確的描述是？
(A) 三台電腦，兩個螢幕，一個鍵盤
(B) 三次登入，兩次錯誤，一次關機
(C) 三個帳號，兩個密碼，一個滑鼠
(D) 三份資料，兩種媒體，一份異地或離線

25 資安事件發生時，為了避免影響擴大，常先做哪一件事？
(A) 圍堵並限制擴散
(B) 把檔案全部刪除
(C) 立刻買新電腦
(D) 立刻把螢幕關掉

26 用於識別網路卡的唯一位址為？
(A) IP 位址
(B) MAC 位址
(C) Port 號碼
(D) URL 位址

27 TCP 與 UDP 最大差異在於？
(A) 是否建立連線
(B) 是否使用加密
(C) 是否支援廣播
(D) 是否具備位址

28 DNS 服務的主要功能為？
(A) 網域名稱解析
(B) 電子郵件傳送
(C) 檔案資料傳輸
(D) 遠端主機控制

29 下列何者屬於短距離無線通訊技術？
(A) Bluetooth
(B) SMTP
(C) FTP
(D) HTTP

30 下列何者為對稱式加密演算法？
(A) 進階加密標準（AES）
(B) 數位簽署演算法（DSA）
(C) 橢圓曲線加密（ECC）
(D) 公鑰加密演算法（RSA）

31 下列何者為防火牆（Firewall）最主要的核心功能？
(A) 過濾網路封包
(B) 偵測電腦病毒
(C) 加密通訊內容
(D) 管理帳號權限

32 下列何項通訊協定的主要功能為在網路中自動分配 IP 位址給客戶端電腦？
(A) 動態主機配置協定（DHCP）
(B) 網域名稱系統協定（DNS）
(C) 超文字傳輸協定（HTTP）
(D) 檔案傳輸協定（FTP）

33 根據 IEEE 標準組織的定義，下列何者為有線乙太網路（Ethernet）的通訊協定標準？
(A) IEEE 802.3 標準
(B) IEEE 802.11 標準
(C) IEEE 802.15 標準
(D) IEEE 802.16 標準

34 UDP 協定最適用於哪種應用？
(A) 即時影音串流
(B) 電子郵件
(C) FTP 傳輸
(D) 網頁下載

35 HTTPS 相較 HTTP 的額外安全機制為？
(A) SSL/TLS 加密
(B) 封包路由
(C) 流量控制
(D) IP 封包標記

36 Wi-Fi 安全機制中 WPA2 的主要功能為？
(A) 加密無線通訊
(B) 增加傳輸速率
(C) 限制網路範圍
(D) 管理 IP 分配

37 在資訊安全管理中，實施「多因素驗證」（MFA）最主要的目的為何？
(A) 強化身分識別安全
(B) 提升網路傳輸速率
(C) 確保實體硬體安全
(D) 集中儲存加密金鑰

38 電子郵件傳輸使用的主要協定為？
(A) SMTP
(B) HTTP
(C) FTP
(D) DNS

39 在網路通訊安全中，建置「虛擬私人網路」（VPN）最主要的功能為何？
(A) 建立加密安全傳輸通道
(B) 提升骨幹網路傳輸速率
(C) 提供大規模資料備援儲存
(D) 進行實體網路之網段分割

40 在資訊安全威脅中，下列何者最能精確描述「阻斷服務攻擊」（DoS）的主要目的？
(A) 耗盡資源使目標系統癱瘓
(B) 誘騙使用者洩漏帳號密碼
(C) 秘密竊取資料庫中敏感資料
(D) 長期監控使用者網路行為

41 在 OSI 七層模型中，傳輸控制協定（TCP）最主要的功能為何？
(A) 資料加密與壓縮
(B) 媒體存取控制
(C) 網際網路路徑選擇
(D) 確保資料可靠傳輸

42 在無線區域網路（WLAN）的實體層架構中，其傳輸資料的主要媒介為何？
(A) 玻璃纖維（Optical Fiber）
(B) 無線電波（Radio Waves）
(C) 屏蔽雙絞線（STP）
(D) 同軸電纜（Coaxial Cable）

43 在資訊安全管理領域中，關於「資安三要素」所追求的目標，下列哪一組對應最為精確？
(A) 保護資訊機密、防止資料篡改、確保服務可用性
(B) 加速資料傳輸、加密網路封包、提升硬體效能
(C) 建立防火牆、部署 IDS、架設 VPN
(D) 管理域名解析、監控 HTTP 流量、傳輸檔案資料

44 在資訊安全技術中，「雜湊函數」（Hash Function）與「資料加密」（Encryption）技術差異為何？
(A) 雜湊函數具備「不可逆性」，無法由運算結果反推回原始資料
(B) 資料加密運算速度慢，雜湊函數則專用於網路路由路徑選擇
(C) 雜湊函數必須搭配非對稱式金鑰，資料加密則完全不需金鑰
(D) 雜湊函數主要用於壓縮大型檔案，資料加密則用於加速網路

45 在資訊安全威脅中，關於「阻斷服務攻擊」（DoS）與「分散式阻斷服務攻擊」（DDoS）的主要差異，下列描述何者最正確？
(A) 攻擊封包是否經過 AES 加密
(B) 是否利用殭屍網路（Botnet）達成多點同步攻擊
(C) 攻擊時所使用的網路通訊協定（TCP 或 UDP）
(D) 攻擊目標是位於區域網路（LAN）還是廣域網路（WAN）

46 在規劃企業資訊安全策略時，若要建立一個「多層次防護」的體系，以確保在單一防禦點失效時仍能維持安全性，應優先採用下列哪一種架構？
(A) 縱深防禦架構（Defense in Depth）
(B) 單點安全設備（Single Point of Protection）
(C) 單一認證機制（Single Authentication）
(D) 集中儲存系統（Centralized Storage）

47 在企業資訊安全管理體系（ISMS）中，「資訊安全政策」的主要功能與重要性為何？
(A) 降低資訊系統之硬體建置與維護成本
(B) 改善底層網路通訊之傳輸品質與延遲
(C) 建立組織安全管理之最高指導準則與規範
(D) 提升自動化設備之運算速率與執行效率

48 在 TCP/IP 四層參考模型中，負責處理使用者介面、資料格式化及應用程式溝通的「HTTP 協定」，應歸類於哪一層？
(A) 網際網路層（Internet Layer）
(B) 傳輸層（Transport Layer）
(C) 應用層（Application Layer）
(D) 網路存取層（Network Access Layer）

49 在網路防禦設備中，入侵偵測系統（IDS）與入侵防禦系統（IPS）最關鍵的功能差異為何？
(A) 是否具備針對惡意流量的即時阻斷能力
(B) 是否能夠產生系統運作日誌（Log）
(C) 是否提供網路層（L3）的路由封包路徑選擇
(D) 是否能針對應用層傳輸進行 SSL/TLS 加密

50 在現代網路安全通訊（如 TLS/SSL）中，所謂的「混合式加密系統」其運作機制為何？
(A) 單獨採用 RSA 等演算法進行大規模資料封裝
(B) 結合對稱式加密的高效率與非對稱式加密的金鑰交換優勢
(C) 捨棄金鑰管理機制以換取更快的封包傳輸速率
(D) 僅使用 AES 演算法並搭配硬體防火牆進行資料保護

國營臺灣鐵路股份有限公司115年從業人員甄試 筆試試題標準答案

代號:1150406-TT1-072-1

應試類科:第9階-事務員-資訊

測驗科目:網路通訊與資通安全概要

題號	第1題	第2題	第3題	第4題	第5題	第6題	第7題	第8題	第9題	第10題
答案	B	C	A	C	D	A	A	B	B	D

題號	第11題	第12題	第13題	第14題	第15題	第16題	第17題	第18題	第19題	第20題
答案	A	D	D	C	C	C	A	A	D	C

題號	第21題	第22題	第23題	第24題	第25題	第26題	第27題	第28題	第29題	第30題
答案	B	A	A	D	A	B	A	A	A	A

題號	第31題	第32題	第33題	第34題	第35題	第36題	第37題	第38題	第39題	第40題
答案	A	A	A	A	A	A	A	A	A	A

題號	第41題	第42題	第43題	第44題	第45題	第46題	第47題	第48題	第49題	第50題
答案	D	B	A	A	B	A	C	C	A	B