代號：11060
頁次：1－1

111年公務人員特種考試司法人員、法務部調查局調查人員、海岸巡防人員、移民行政人員考試及111年未具擬任職務任用資格者取得法官遴選資格考試試題

考 試 別：司法人員
等　　別：三等考試
類 科 組：檢察事務官電子資訊組
科　　目：資通安全
考試時間：2 小時　　座號：_____

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、資訊安全管理中緊急應變計畫是重要項目，緊急應變計畫中包含「訂定復原策略」，請說明「復原策略」的目的。復原策略內容包含資料備份與主機房異地備援，請說明「資料備份」的重要性。主機房異地備援分冷備援站（cold sites）、暖備援站（warm sites）、熱備援站（hot sites）、全備援站（mirrored sites），請條列逐一說明，內容需包含這四種備援站的成本與復原速度的比較。（24 分）

二、洛克希德馬丁公司發表網路攻擊鏈（Cyber Kill Chain）白皮書，透過軍事行動上常見的攻擊鏈來分析網路安全威脅，被視為解析駭客攻擊方法重要參考，其把駭客攻擊拆解成如後七個步驟：偵查（Reconnaissance）、武裝（Weaponization）、遞送（Delivery）、開採（Exploitation）、安裝（Installation）、發令&控制（Command & Control）和行動（Actions on Objectives）。請針對駭客此七個攻擊步驟逐一提出受害者可以降低攻擊風險或威脅的作為或行動。（28 分）

三、2021 年 OWASP 公布新版網站安全十大安全威脅（OWASP TOP 10 2021），其中前四名分別為：權限控制失效（Broken Access Control）、加密機制失效（Cryptographic Failures）、注入式攻擊（Injection）、不安全設計（Insecure Design）。請說明針對此四項威脅各自的預防措施。（24 分）

四、ISO27001 是廣為國內公務機關或私人企業所遵循資訊安全應用與稽核的國際標準。ISO27001 推行以 PDCA 循環持續地推動 ISMS 活動落實控制措施。請說明何謂 PDCA 循環並繪製一圖簡述此循環推動 ISMS。ISO27001 將組織文件分成四個階層，亦即所謂四階文件，請說明四階文件各階的特質。（24 分）