代號：41460
頁次：1－1

109年公務人員特種考試司法人員、法務部調查局調查人員、國家安全局國家安全情報人員、海岸巡防人員及移民行政人員考試試題

考 試 別：調查人員
等　　別：三等考試
類 科 組：資訊科學組
科　　目：資訊安全實務
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、請說明政府主管機關在金融、電信等關鍵基礎設施建置資安資訊分享與分析中心（Information Sharing and Analysis Center, ISAC）的主要目的，並具體說明在不同特定領域的 ISAC 之間的協同運作關係。（20分）

二、依據我國資通安全管理法的規定，當政府公務機關發生資通安全事件時，針對該事件的調查、處理及改善報告中，應包括那些重要事項？（20分）

三、請詳述單向雜湊函數（One-Way Hash Function）的學理特性，並具體舉出三種採用單向雜湊函數的實務應用及可滿足的安全需求。（20分）

四、為確保數位鑑識程序符合法規，當進行揮發性（Volatile）資料的證據擷取時，請詳述數位鑑識人員證據保全的做法。（20分）

五、網站日誌檔（Web Log Files）是系統人員監測及分析網站使用狀況的重要資訊來源。請說明網站日誌檔的主要紀錄內容及其實務用途。（20分）