

109年公務人員特種考試警察人員、
一般警察人員考試及109年特種考試
交通事業鐵路人員考試試題

考試別：一般警察人員考試

等別：二等考試

類科別：刑事警察人員數位鑑識組

科目：網路與資訊安全（包括資訊安全技術與應用、資安事件處理）

考試時間：2 小時

座號：_____

※注意：(一)禁止使用電子計算器。

(二)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。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

- 一、當張三要傳送一訊息給李四，張三為確保此訊息的機密性、完整性及鑑別性，請問張三該使用那些資訊安全技術，並說明其處理步驟及程序為何？（30 分）
- 二、入侵防禦系統（Intrusion Prevention System, IPS）一般可分為主機端入侵防禦系統（Host Intrusion Prevention System, HIPS）、網路端入侵防禦系統（Network Intrusion Prevention System, NIPS）及應用端入侵防禦系統（Application Intrusion Prevention System, AIPS）三種類型，請說明這三種入侵防禦系統的主要功能為何？（20 分）
- 三、近場通訊（Near Field Communication, NFC）技術近年來被廣泛配置於行動通訊裝置中，也應用於許多行動付款機制中，請舉出四種 NFC 通訊機制可能發生的安全議題。（20 分）
- 四、請說明當資安事件發生時，在封鎖階段中應執行那些步驟及動作才能保持系統服務持續不中斷，並有效防止攻擊者進一步入侵系統造成災情擴散。（30 分）