中央警察大學 115 學年度碩士班入學考試試題

所　別：資訊管理研究所
科　目：電腦犯罪與資訊安全

作答注意事項：

1.本試題共 4 題，每題各占 25 分；共 2 頁。
2.不用抄題，可不按題目次序作答，但應書寫題號。
3.禁用鉛筆作答，違者不予計分。

一、執法機關引入大型語言模型（LLM）輔助刑事偵查與數位鑑識（如自動摘要扣案手機對話、OSINT 情蒐整合、社群媒體犯罪偵測），然而 LLM 的黑盒子特性使其推論過程不透明，導致 AI 輸出結果於法庭上的證據採信度受到質疑。請說明可採用哪些可解釋人工智慧（Explainable AI, XAI）技術，以提升 AI 分析結果的司法透明度與可信度？

二、你因公需稽核一台對外服務的 Tomcat 應用伺服器日誌，懷疑近期有內部帳號遭竊並被用於資料滲漏（Data Exfiltration）。由於你對 Tomcat 日誌格式不熟悉，且每日日誌量高達百萬筆，直接將原始日誌輸入 LLM 將立即超出 Token 上限且成本極高。請自行規劃一套 AI 輔助分析工作流（Workflow），並直接寫出各階段所使用的具體 Prompt，最終輸出須為包含「來源 IP、異常行為說明、風險等級」的結構化可疑帳號清單。

三、請回答下列問題：

（一）依據《資通安全管理法》第 3 條第 1 款定義說明並舉例「資通系統」。（5 分）

（二）除了法律上的定義，從實務角度來看，資通系統的組成可以更細分為哪五個關鍵要素？（10 分）

（三）《資通安全管理法施行細則》第 8 條說明資通安全事件調查、處理及改善報告應包含哪些內容？（10 分）

四、依 Google Cloud Security 所做的 2026 年 Security 網路安全預測，網路犯罪分子於 2026 年將鎖定代管檔案傳輸（Managed File Transfer, MFT）軟體進行攻擊。

（一）請說明 MFT 的功能與優勢。（10 分）

（二）這類的犯罪常見的攻擊手法及調查方式為何？（15 分）