102年特種考試地方政府公務人員考試試題　　代號：34150　全一頁

等　　別：三等考試
類　　科：資訊處理
科　　目：資訊管理與資通安全
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。

一、公務和非公務機關平時應實施資通安全之管控與稽核工作，以減少電腦網路功能弱點（Vulnerability）的發生。這些功能弱點包括如下：
㈠身分驗證（Identification and Authentication）
㈡存取控制（Access Control）
㈢責任歸屬（Accountability）
㈣物件再用（Object Reuse）
㈤準確度（Accuracy）
㈥服務可靠性（Reliability of Service）
試從資通安全觀點，說明上述六項的功能弱點特性。（25分）

二、請試述下列名詞之意涵：（每小題5分，共25分）
㈠揮發性資料（Volatile Data for Digital Acquisition）
㈡App程式
㈢智慧型代理人（Intelligent Agent）
㈣零時差或零日攻擊（Zero-day Attack）
㈤數位鑑識（Digital Forensics）

三、資訊科技可用來支援組織（如民間和政府等）之各種資訊化活動，包括作業性、管理性和策略性等活動。請回答下列問題：
㈠何謂作業性、管理性和策略性等活動。（6分）
㈡指出並說明作業性活動之五種任務項目及其相對應軟體名稱與其功能的作業支援。（10分）
㈢近來國內發生一連串食品安全事件，引起各級政府對食品安全的重視。試從管理性活動觀點，提出政府如何善用資訊科技於國內食品安全管控與稽核的看法。（9分）

四、有關數位簽章（Digital Signature），請回答下列問題：（每小題5分，共25分）
㈠何謂雜湊值（Hash Value）？
㈡雜湊函數（Hash Function）的主要用途。
㈢若有文字型態之內容、編輯格式和字體大小等完全相同的兩個檔案，經由 MD5（Message-Digest Algorithm 5）所產生的雜湊值卻不相同，請說明其可能原因。
㈣在蜜罐誘捕系統（Honeypot）之惡意程式網路活動分析上，說明採用 MD5（或SHA-256）之目的。
㈤我國《個人資料保護法》（修正日期：民國99年5月26日）第22條第2項規定：「中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。」請說明如何進行證據之取證（Acquisition）及使用 MD5（或SHA-256）目的為何？