

108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：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：(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、請試述下列名詞之意涵：(每小題 5 分，共 25 分)

(一) Electromagnetic Recording

(二) Integrity

(三) Zero-Knowledge Penetration Test

(四) Hash Value

(五) Access Control List

二、有關入侵偵測與防禦系統 (IDS/IDPS)，請回答下列問題：

(一) IDS/IDPS 偵測資安事件有四種方法：Signature-based Detection、Anomaly-based Detection、Stateful Protocol Analysis Detection 及 Hybrid Detection。請說明這四種方法的運作方式。(15 分)

(二)以網路為基礎的 IDPS 會記錄它所偵測到的資安事件相關訊息，以提供驗證、告警、事件調查或其他相關資安紀錄的比對等用途，請寫出 IDPS 紀錄內容包括那些？(10 分)

三、美國國家標準暨技術局 (NIST) 的 SP800-30 文件「資訊技術體系風險管理指南」(Risk Management Guide for Information Technology Systems) 對風險 (Risk) 定義如下：

Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

(一)請針對上述風險 (Risk) 英文定義以中文表示。(5 分)

(二)定義「Vulnerability」和「Impact」。(10 分)

(三)請寫出我國《資通安全管理法》(公布日期：民國 107 年 06 月 06 日) 第 3 條第 3 款「資通安全」和第 7 款「關鍵基礎設施」之用詞定義。(10 分)

四、根據《中華民國刑法》第三十六章妨害電腦使用罪有關第 358 條至第 363 條之規定，以及資料（或資訊）隱藏，回答下列問題：

(一)何謂資料（或資訊）隱藏？（5 分）

(二)寫出三種資料（或資訊）隱藏技術。（6 分）

(三)寫出二種「反資料（或資訊）隱藏」的技巧或做法。（4 分）

(四)如果嫌疑犯利用資料（或資訊）隱藏技術致生被害人無法正常使用電磁紀錄時，則該嫌疑犯可能觸犯那條條文，請寫出適用條文內容，並加以說明。（10 分）