《資訊安全實務》

一、請條列並說明「數位證據保全標準作業程序」中，進行「電腦設備或儲存媒體蒐集」之作法。（25分）

命題意旨	此題屬於數位證據保全標準的作業程序。
答題關鍵	此題可以電腦是否可關機、可關機狀態是否有外接儲存媒體、無法中斷服務關機狀態與外表廠牌、型號等客觀事實進行描述，以這四個要點為答題關鍵。

【擬答】

根據政府機關資安事件數位證據保全標準作業程序之電腦設備或儲存媒體蒐集：

(一)如系統於得關機情況下，各機關原則上應封緘完整電腦設備，以待上級機關或鑑識單位進行後續協助。但如確有拆卸之必要者，記錄人員須針對儲存媒體拆卸及取出過程進行全程錄影，並應將儲存媒體進行封緘，並視需要運送至上級機關或鑑識單位。所稱上級機關，指該機關直屬之上一級機關；其無上級機關者，由該機關執行本作業程序所規定上級機關之職權。

舉例：查扣詐騙機房個人電腦，但是電腦設備被使用密碼鎖不利搬運，因此需要將個人電腦拆卸。

(二)如系統於得關機情況下，且有其他外接式儲存媒體存在時，數位證據保全人員應將儲存媒體進行封緘，並視需要運送至上級機關或鑑識單位。記錄人員須針對儲存媒體拆卸及取出過程進行全程錄影。如以拍照方式進行，其步驟如下：

1.針對儲存媒體拆卸前進行拍照（包含線材連結畫面）。

2.針對儲存媒體拆卸後進行拍照（包含線材無連結畫面）。

3.針對儲存媒體取出時進行拍照。

舉例：查扣詐騙機房個人筆電，有外接式硬碟。

(三)如伺服主機系統無法中斷服務，應在上級機關或鑑識單位之監督下，以嚴謹之方式進行資料轉錄。

舉例：詐騙機房中的伺服器目前與遠在異地的同夥進行連線，若是關機，則連線 IP、port 等揮發性資料即不復有，因此不能中斷服務，在鑑識單位監督下，按照 SOP 進行錄製備份。

(四)針對儲存媒體之廠牌、型號、序號及儲存容量等相關資訊進行拍照。數位證據保全人員應將其數位證據蒐集結果填寫於數位證據蒐集工作表（電腦設備）或數位證據蒐集工作表（儲存媒體）。

舉例：針對儲存媒體的品牌、容量、序號等描述加以記錄，未來可以核對相關的採購或是消費紀錄，蒐集更多犯罪訊息。

二、請條列說明三項 IDPS（Intrusion Detection and Prevention System）偵測技術，並就精準度、已知攻擊、未知攻擊、計算能力與策略調整方式等五個面向做比較。（25 分）

命題意旨	入侵防禦偵測技術與適用範圍。
答題關鍵	IDPS 的三種類型偵測技術與其特色，實務適用狀況的二維度比較。

【擬答】

在美國 NIST 的 Guide to Intrusion Detection and Prevention Systems 文件中，IDPS 有三種偵測技術：

(一)狀態的協定分析 Stateful protocol analysis：使用主機或是網路特徵資料檔進行可疑活動判讀，簡單來說，若是使用者經過授權，便會依照該授權給予相對應的特定權限，進行該身分能允許操作，例如：某使用者經過授權，只有 read 功能。IDPS 便會追蹤這些對話後續的操作。

(二)異常行為偵測 Anomaly-based detection：IDPS 透過既有正常的網路、主機、使用者等正常行為的「設定檔」，去判讀目前活動是否有異常，因此異常偵測主要是比較正常使用活動與觀察可疑活動是否有特別差異。

(三)特徵偵測 Signature-based detection：大部分的網路攻擊或是惡意程式都有特定的攻擊特徵，因此若是具有惡意攻擊特徵，如 telnet，帳戶名稱為 root，有很高機率是攻擊，特色是會有已知發生的特徵模式。

	狀態的協定分析	異常行為偵測	特徵偵測
精準度	佳，狀態協定有能力追蹤和理解傳輸、網路與有狀態概念的應用協定；但是對於未違反使用角色功能的攻擊類型，如 DDos 是合法存取的殭屍電腦，偵測效果大大減弱。	差，因為隨著時間跟技術改變，行為變化誤判性高。	有收錄的特徵偵測佳；若未收錄模式庫的未能偵測。
已知攻擊	佳，若是符合狀態則即時阻斷。	普通	最佳，已知道發生攻擊之特徵模式。
未知攻擊	佳，記錄該用戶 session 和封包前後關係。	普通	最差，攻擊之特徵模式尚未收錄。
計算能力	需要的計算能力最多，因為要記錄每個網路狀態。	計算統計值是否超過門檻或是預設值。	與資料庫進行特徵比對。
策略調整	更新協定追蹤狀態。	更新統計值記錄檔。	更新特徵模式庫。

三、請條列說明零信任（Zero Trust）的核心機制與六項組織應考量的零信任原則。（30 分）

命題意旨	主要考零信任的核心機制與網路落實原則。
答題關鍵	除了說明零信任外，應要提到零信任與傳統 VPN 有何不同，與組織應考量零信任於網路管理。
考點命中	《112 高點司法三等・調查局考場特刊》，資通安全第二題，頁 4-1。

【擬答】

零信任是因應政府與企業的雲端導入各種 X 即服務型態，邊界定義逐漸模糊，是以個別的資源、使用者和資產本身為主體，而每位使用者在存取企業的每項資源之前，都必須個別通過認證，個別皆通過驗證後，才可以獲取一次性的存取權限。

三大核心機制：(參考資料：行政院資通會)

(一)身分鑑別：多因子身分鑑別與身分鑑別聲明，例如：開通帳號與密碼，需使用憑證登入或是手機驗證，機敏機關須使用指紋或是人臉辨識登入。

(二)設備鑑別：設備鑑別與設備健康管理。

1.基於公開金鑰加密系統的信任平台模組(TPM)之設備鑑別。

2.設備健康管理：持續更新設備狀態，並依設備健康狀態與壽命，換算健康等級。

(三)信任推斷：隨時依使用者行為與設備狀態，偵測異常存取，有一套基於分數與情境之信任推斷機制，例如：錯誤次數過多，IP 位址來自境外，登入時間非上班時間或於敏感國際情勢時，可以導入「人工智慧」動態計算信任等級。

組織應考量的 6+1 項原則：(參考資料來源：NIST SP 800-207)

1.所有資料和計算服務皆需視為資源，因此只要是資源就要保護與可能非受信賴。

2.不管是在內部網路或是外部，皆需確保通訊安全，假設內部網路可能已有潛伏攻擊者。

3.對於存取企業資源，應以該次為單位去連線與授權。

4.存取資源的許可與否應視動態政策，包含員工外、合約商、約聘雇，BYOD 的員工皆須考量。

5.企業監控與衡量所有擁有與相關資產的完整性與安全性狀態。

6.在允許存取前，所有資源驗證與授權是動態且嚴格執行的。

7.企業應盡可能收集自身資產、網路基礎建設和通訊相關的更多資訊，使用這些資訊並確保這些資源處於安全狀態。

四、以下是張三和李四以 Diffie-Hellman key exchange 之技術為基礎欲產生共同密鑰，但未做取模運算（Modulus），所以也沒有選定 Diffie-Hellmankey exchange 模數運算的質數，他們所選用的公開基礎參數（底數）g 為 3。請從他們交換的參數破解出張三的秘密參數 X_A、李四的秘密參數 X_B 以及他們產生的共同密鑰 Key。（需有推演計算的過程才給分）（20 分）

張三：選定秘密參數 X_A，後計算出公開參數 Y_A=27 傳給李四。
李四：選定秘密參數 X_B，後計算出公開參數 Y_B=243 傳給張三。
張三、李四：各自計算出二人的共同密鑰 Key。

命題意旨	Diffie-Hellman 協議法。
答題關鍵	交談金鑰於 Diffie-Hellman 計算。

【擬答】

張三		李四
X_A	秘密金鑰	X_B
YA=g^X_A	公開金鑰	Y_B=g^X_B
SK=Y_B^X_A	交談金鑰	SK=Y_A^X_B

此題的題示有說明未做取模運算，mod 運算省略：
(一)27=3^X_A，可以推得 X_A=3
(二)243=3^X_B，可以推得 X_B=5
(三)SK=243^3=27^5=14348907