《資訊安全實務》

答題關鍵	本份試題著重於法規與制度面，諸如資通安全管理法、政府機關（構）資安事件數位證據保全標準作業程序。是以，學員在準備上，除資安實務面如數位證據、數位鑑識外，新興資安法規、政府資安政策以及資安作業程序亦需多所涉獵。

一、請說明政府主管機關在金融、電信等關鍵基礎設施建置資安資訊分享與分析中心（Information Sharing and Analysis Center, ISAC）的主要目的，並具體說明在不同特定領域的ISAC之間的協同運作關係。（20分）

【擬答】

依據資通安全管理法第 8 條：主管機關應建立資通安全情資分享機制。前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之。

因此，行政院國家資通安全會報技術服務中心 (https://www.nccst.nat.gov.tw/NISAC)說明：鑒於國內外資安情資來源漸趨多元，且資安情資數量日益增加，為有效管理與傳遞跨領域資安情資，並達成橫向之資安聯防目標，「國家資安資訊分享與分析中心」(National Information Sharing and Analysis Center, N-ISAC)於民國 107 年 1 月正式運作。透過情資格式標準化與系統自動化之分享機制，提升情資分享之即時性、正確性及完整性，建立縱向與橫向跨領域之資安威脅與訊息交流，達到情資迅速整合、即時分享及有效應用之目的，提升國家資訊安全整體應變與防護能力。

此外，依據資通安全情資分享辦法第 9 條：各機關進行情資分享，應分別依主管機關或中央目的事業主管機關指定之方式為之。各機關因故無法依前項規定方式進行情資分享者，分別經主管機關或中央目的事業主管機關同意後，得以下列方式之一為之：

一、書面。
二、傳真。
三、電子郵件。
四、資訊系統。
五、其他適當方式。

二、依據我國資通安全管理法的規定，當政府公務機關發生資通安全事件時，針對該事件的調查、處理及改善報告中，應包括那些重要事項？（20分）

【擬答】

資通安全管理法第 14 條：公務機關為因應資通安全事件，應訂定通報及應變機制。

公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。

公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；無上級機關者，應送交主管機關。

前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，由主管機關定之。

針對該事件的調查、處理及改善報告中，應包含以下內容：

(1)事件發生或知悉其發生、完成損害控制或復原作業之時間。
(2)事件影響之範圍及損害評估。
(3)損害控制及復原作業之歷程。
(4)事件調查及處理作業之歷程。
(5)事件根因分析。
(6)為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。
(7)預定完成時程及成效追蹤機制。

三、請詳述單向雜湊函數（One-Way Hash Function）的學理特性，並具體舉出三種採用單向雜湊函數的實務應用及可滿足的安全需求。（20分）

【擬答】

單向雜湊函數是將不定長度的位元資料輸入雜湊函數(Hash Function)後，以函數運算轉換為固定長度的雜湊值(Hash Value)輸出。由於雜湊值是獨一無二的，因此可做為該位元資料的獨特標記。可防止資料被竄改，驗證其資料完整性。其具有以下特色：

(1)單向映射

位元資料可由雜湊函數計算而得雜湊值，而難以從雜湊值回推原始位元資料。

(2)不易碰撞

產生的雜湊值不易與其他位元資料所產生的雜湊值相同。

採用單向雜湊函數的實務應用有：

(1)完整性(Integrity) 。

(2)檔案正確性。

(3)病毒特徵識別。

四、為確保數位鑑識程序符合法規，當進行揮發性（Volatile）資料的證據擷取時，請詳述數位鑑識人員證據保全的做法。（20分）

【擬答】

依據政府機關（構）資安事件數位證據保全標準作業程序，當進行揮發性資料的證據擷取時數位鑑識人員證據保全的做法如下：

(1)各機關得視其資訊人力資源進行不同程度之揮發性及邏輯性資料擷取。

(2)如相關標的設備處於開機狀態下，數位證據保全人員應考量資安事件類型及現場狀況後，擷取揮發性資料，以避免部分儲存於記憶體中之重要資料因系統關機而消逝。

(3)數位證據保全人員應考量資安事件類型及現場狀況後，擷取邏輯性資料，如作業系統資訊、網路狀態、執行程序資訊、系統稽核日誌紀錄及使用者上網行為紀錄等。

(4)針對防火牆設備、入侵偵測或防禦設備、紀錄保存與資安事件分析設備、防毒設備、流量控管或網路監控設備、應用系統及資料庫等設備，若各機關有資訊人力，得在數位證據保全人員檢視下，由應用系統或網路管理人員將稽核日誌檔案匯出至特定目錄內，由數位證據保全人員對其進行邏輯性資料擷取。

(5)數位證據保全人員於擷取揮發性與邏輯性資料完畢後，應產生相對應之雜湊運算值，並記錄擷取之資訊或以自動化工具所產生之報表為之，如擷取日期與時間、電腦名稱、所蒐集之揮發性與邏輯性資料項目、雜湊運算值等，經執行人員與資安事件發生單位主管簽章確認。

五、網站日誌檔（Web Log Files）是系統人員監測及分析網站使用狀況的重要資訊來源。請說明網站日誌檔的主要紀錄內容及其實務用途。（20分）

【擬答】

網站日誌檔為網站伺服器(Web Server)的紀錄檔，其中包含：

(1)客戶端 IP 位址。

(2)請求日期/時間。

(3)請求的網頁。

(4)HTTP/HTTPS 編碼。

(5)執行的動作。

(6)代理伺服器。

(7)參照位址。

上述資料可能寫入同一檔案，也可能分隔成不同的紀錄檔，諸如存取紀錄檔、錯誤紀錄檔。一般而言，僅有網站管理員或其他管理人員有權存取。

網站日誌檔實務用途有：

(1)錯誤管理。

(2)入侵偵測。

(3)網路行銷。