企業電子化人才能力鑑定

資安實務與技術

110/111 雲端指南

（內附試題彙編）

中華民國電腦技能基金會
Computer Skills Foundation

SPT 「資安實務與技術」學科試題及答案

第一類：資訊安全管理

BD 1-01. 下列哪些控制措施可增進資訊資產可用性之保護？**(複選)**

（Ａ）於其前方安裝防火牆

（Ｂ）增加網路頻寬

（Ｃ）將儲存資料加密

（Ｄ）安裝不斷電系統

B 1-02. 資訊安全的「完整性」目標是保護資訊的哪一項特質？

（Ａ）資訊之秘密性與隱私性

（Ｂ）資訊或系統之正確性

（Ｃ）資訊之便利性

（Ｄ）資訊與資訊處理的可獲得性

C 1-03. 下列何者為資訊安全的三個目標？

（Ａ）可取性、完整性、機密性

（Ｂ）可用性、機動性、完整性

（Ｃ）機密性、完整性、可用性

（Ｄ）機密性、方便性、完整性

B 1-04. 資訊或系統之正確性，應防制人為刻意竄改與自然雜訊干擾；防制假冒或未授權方式存取系統資源進行資料之處理或更改，意指資訊安全的哪一個目標？

（Ａ）機密性（Confidentiality）

（Ｂ）完整性（Integrity）

（Ｃ）可用性（Availability）

（Ｄ）不可否認性（Non-repudiation）

C 1-05. 資訊與資訊處理的可獲得性，應避免資訊因系統故障或人為惡意的阻斷服務屬，是屬於以下的哪一個資訊安全目標？

（Ａ）機密性

（Ｂ）完整性

（Ｃ）可用性

（Ｄ）不可否認性

A 1-06. 個人可識別資訊（personally identifiable information，PII）不可逆地變更之過程，稱為下列何者？

（Ａ）匿名化（anonymization）

（Ｂ）同意（consent）

（Ｃ）識別（identify）

（Ｄ）擬匿名化（pseudonymization）

D 1-07. 應用於個人可識別資訊（personally identifiable information， PII)，以別名替換個人識別資訊之過程，稱為下列何者？

（Ａ）匿名化（anonymization）

（Ｂ）同意（consent）

（Ｃ）識別（identify）

（Ｄ）擬匿名化（pseudonymization）

B 1-08. 分散式阻斷服務（DDOS）攻擊乃人為惡意的阻斷系統服務，違背資訊安全的何種特性？

（Ａ）機密性

（Ｂ）可用性

（Ｃ）完整性

（Ｄ）無違背

C 1-09. 組織內部某員工為了私利，將其所管理之薪資檔內容有關自己之薪資部分進行調整，試問此為下列哪一項資訊安全的目標遭受破壞？

（Ａ）資訊安全的機密性（Confidentiality）目標遭受破壞

（Ｂ）資訊安全的可歸責性（Accountability）目標遭受破壞

（Ｃ）資訊安全的完整性（Integrity）目標遭受破壞

（Ｄ）資訊安全的可用性（Availability）目標遭受破壞

ACD 1-10. 下列哪些技術適用於保護資訊的「可用性」？**(複選)**

（Ａ）存取控制技術

（Ｂ）數位簽章技術

（Ｃ）負載平衡技術

（Ｄ）容量規劃

D 1-11. 資料備份符合以下的哪一項資料保護選項？

（Ａ）機密性

（Ｂ）完整性

（Ｃ）不可否認性

（Ｄ）可用性

D 1-12. 試問下列選項何者係指資訊與資訊處理的可獲得性，應避免資訊因系統故障或人為惡意的阻斷服務？

（Ａ）機密性（Confidentiality）

（Ｂ）可歸責性（Accountability）

（Ｃ）完整性（Integrity）

（Ｄ）可用性（Availability）

D 1-13. 關於資訊安全威脅發展趨勢的描述，下列何者為非？

（Ａ）熱門社交網站成為個資外洩的新管道

（Ｂ）組織化網路犯罪與詐騙更形猖獗

（Ｃ）手機成新興資安威脅平台

（Ｄ）針對網頁攻擊將持續減少

D 1-14. 試問利用人性弱點，運用簡單的溝通和欺騙的技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料係下列哪一項攻擊手法之運用？

（Ａ）零時差攻擊

（Ｂ）分散式阻斷服務攻擊

（Ｃ）系統漏洞攻擊

（Ｄ）社交工程攻擊

C 1-15. 一個國家為了維持民生、經濟與政府等相關運作而提供之基本設施與服務，一般稱之為下列何者？

（Ａ）基礎資訊系統

（Ｂ）關鍵資訊系統

（Ｃ）關鍵基礎建設

（Ｄ）資訊基礎設施

A 1-16. 在全球所共同面臨的資訊安全威脅中，關鍵資訊基礎設施遭實體破壞的風險係因下列何種原因而導致風險倍增？

（Ａ）開放系統與網路

（Ｂ）新型控制設備

（Ｃ）新的防護措施使用

（Ｄ）封閉式系統與網路

ABD 1-17. 資訊安全是為了要確保資訊的哪些目標？**(複選)**

（Ａ）可用性

（Ｂ）機密性

（Ｃ）便利性

（Ｄ）完整性

AB 1-18. ISO/CNS 27014 提出的以 EDM 模式建立資訊安全治理架構， 而下列對 EDM 的描述哪些為正確的？**(複選)**

（Ａ）評估（Evaluate）

（Ｂ）指導(Direct)

（Ｃ）偵測(Detect)

（Ｄ）管理(Management)

A 1-19. ISO/CNS 27001 採用的 PDCA 流程導向方法， 下列何者描述有誤?

（Ａ）政策（Policy）

（Ｂ）執行(Do)

（Ｃ）檢查(Check)

（Ｄ）行動(Act)

ABC 1-20. 下列哪些項目屬於個人資料保護法所稱之個人資料？**(複選)**

（Ａ）護照號碼

（Ｂ）犯罪前科

（Ｃ）得以間接方式識別該個人之資料

（Ｄ）法人公司統一編號

B 1-21. 我國著作權法規定的著作權期限為下列何者？

（Ａ）著作人生存期間

（Ｂ）著作人生存期間及死亡之後 50 年

（Ｃ）著作人生存期間及死亡之後 20 年

（Ｄ）永久存在

SPT 「資安實務與技術」學科試題及答案

第二類：資訊安全風險管理

A 2-01. 在 CNS/ISO/IEC 27005 之資訊安全風險管理程流程中，建立風險接受準則，是屬於下列哪個階段應執行的事項？

（Ａ）建立全景階段

（Ｂ）風險評鑑階段

（Ｃ）風險處理階段

（Ｄ）風險接受階段

C 2-02. 組織準備導入一項新的技術，但使用該技術會違反現行資安規定。請問這樣的議題如何處理最佳？

（Ａ）強化現行資安規定

（Ｂ）修訂資安政策以允許使用該技術

（Ｃ）進行風險分析，鑑別風險，再決定處理方式

（Ｄ）進行研發，提供更好的技術

C 2-03. CNS/ISO/IEC 27005 風險管理流程中有以下的工作項目：(1) 建立全景、(2) 風險處理、(3) 風險監控與審查、(4) 風險評鑑、(5) 風險溝通、(6) 風險接受，上述何者為正確流程步驟？

（Ａ）1, 2, 3, 4, 5, 6

（Ｂ）1, 4, 5, 2, 6, 3

（Ｃ）1, 4, 2, 6, 5, 3

（Ｄ）1, 3, 2, 6, 4, 5

D 2-04. 下列何者為「風險評鑑技術」的國家標準？

（Ａ）CNS27001

（Ｂ）CNS27005

（Ｃ）CNS31000

（Ｄ）CNS31010

ABC 2-05. 下列哪些敘述是正確的？**(複選)**

（Ａ）風險管理係針對資訊系統所遭受的安全風險進行鑑別、評量、控制及最小化的流程

（Ｂ）威脅係指可能利用或引發脆弱性的潛在方法

（Ｃ）脆弱性係指資產已識別的易受攻擊之處

（Ｄ）風險係指當相對應脆弱性利用威脅，使其直接或間接造成組織資訊資產受到漏失或損害的可能性

A 2-06. 下列何者之主要目的在於決定風險處理之範圍？

（Ａ）風險接受準則

（Ｂ）衝擊準則

（Ｃ）風險評估準則

（Ｄ）風險處理準則

D 2-07. 風險評估準則（Risk Evaluation Criteria）主要目的為何？

（Ａ）設定風險評估量化值

（Ｂ）定義風險溝通共同語言

（Ｃ）設定風險監控的準則

（Ｄ）決定風險處理之先後次序

AB 2-08. 衝擊準則（Impact Criteria）主要為下列哪些因素結合，破壞資訊資產「機密性」、「完整性」及「可用性」？**(複選)**

（Ａ）威脅

（Ｂ）脆弱性

（Ｃ）衝擊程度

（Ｄ）事故發生時的處理應變人數

SPT 「資安實務與技術」學科試題及答案

第三類：資安事故處理與數位鑑識

AC 3-01. 某組織發現網站瀏覽速度很慢，經追查發現有駭客攻擊的行為發生，因此啟動緊急應變程序，下列哪些是可行的作為？**(複選)**

（Ａ）阻擋攻擊來源 IP 或網段

（Ｂ）執行反制程式反攻擊駭客

（Ｃ）將可疑的流量導到不存在的位址

（Ｄ）請駭客來喝咖啡並道德勸說

ABD 3-02. 在處理資安事件時，數位證據的取得方式必須嚴謹，下列哪些項目算是正確的處理方式？**(複選)**

（Ａ）相關證物在處時必須有完整明確的監管紀錄

（Ｂ）只能採用被接受的磁碟映像複製工具

（Ｃ）使用數位憑證以檢驗被複製出來的資料沒有被竄改

（Ｄ）數位證物最好要置於具有訊號阻隔功能的防靜電袋

B 3-03. 下列何者為正確的資安事件處理程序？

（Ａ）準備、識別、封鎖、回復、根除、經驗學習

（Ｂ）準備、識別、封鎖、根除、回復、經驗學習

（Ｃ）準備、回復、識別、封鎖、根除、經驗學習

（Ｄ）準備、封鎖、識別、根除、回復、經驗學習

AC 3-04. 在數位證據的取得過程中，針對硬碟上資料的取得應該有下列哪幾種作法？**(複選)**

（Ａ）映像複製

（Ｂ）備份開機磁區

（Ｃ）配合雜湊函數以檢驗被複製出來的資料沒有被竄改

（Ｄ）用作業系統內建指令，加上特殊參數，把資料複製到同樣規格的硬碟上

D 3-05. 資安事故的四個處理階段中，其中偵測與分析階段（Detection and Analysis）的主要目的為何？

（Ａ）記錄相關的處理過程，以便瞭解進行了哪些工作項目，並可進行改進

（Ｂ）讓受影響的系統，能安全地回復正常運作

（Ｃ）使團隊將事情準備妥當，以能進行事故處理

（Ｄ）蒐集並分析資安事件（Event），判斷是否為一個資安事故（Incident）

C 3-06. 下列何項為國際標準組織（International Organization for Standardization；ISO）針對數位證物的識別、收集、獲取以及保存所訂定的參考指南？

（Ａ）ISO/IEC 27011

（Ｂ）ISO/IEC 27018

（Ｃ）ISO/IEC 27037

（Ｄ）ISO/IEC 27040

D 3-07. 資安事故處理程序中， 封鎖階段的目的為何？

（Ａ）嘗試找出根因，移除與攻擊相關的因素

（Ｂ）讓被攻擊的系統恢復正常運作

（Ｃ）監視主機的行為，運用防毒軟體或是端點安全檢測軟體進行系統的防護偵測

（Ｄ）避免影響擴大，防止入侵的行為持續

A 3-08. 四個資安事故的處理階段中，其中事後處置階段（Post-Incident Activity）的主要目的為何？

（Ａ）記錄相關的處理過程，以便瞭解進行了哪些工作項目，並可進行改進

（Ｂ）讓受影響的系統，能安全地回復正常運作

（Ｃ）使團隊將事情準備妥當，以能進行事故處理

（Ｄ）蒐集並分析資安事件（Event），判斷是否為一個資安事故（Incident）

SPT 「資安實務與技術」學科試題及答案

第四類：實體與環境安全

AD 4-01. 門是當災害發生時很重要的逃生管道之一，下列哪些敘述是正確的？**(複選)**

（Ａ）門的設定 Fail Safe 是指當控制系統失效後，會自動打開

（Ｂ）門的設定 Fail Secure 是指當沒有電源時，會自動打開

（Ｃ）門應依疏散方向反向開啟（向內）

（Ｄ）門應依疏散方向順向開啟（向外）

B 4-02. 實體安全計畫中永遠的第一優先為？

（Ａ）控制的有效性

（Ｂ）生命安全

（Ｃ）資產價值的保護

（Ｄ）業務的持續不中斷

D 4-03. 何者為正確的「實體安全計畫規劃步驟」？（1）組織計畫擬定小組、(2）決定可接受風險程度、(3）實作與防護措施、(4）建立績效基準、(5）執行風險分析

（Ａ）1 → 2 → 4 → 3 → 5

（Ｂ）1 → 4 → 2 → 3 → 5

（Ｃ）1 → 2 → 4 → 5 → 3

（Ｄ）1 → 5 → 2 → 4 → 3

B 4-04. 煙霧偵測位置規劃，下列敘述何者正確？

（Ａ）應置於天花板上風處

（Ｂ）應置於天花板下風處

（Ｃ）應置於天花板通風處

（Ｄ）應置於天花板角落處

ABC 4-05. 關於實體安全計畫的描述哪些項目是正確的？**(複選)**

（Ａ）擬定實體安全防護措施計畫（包含：嚇阻、延遲、偵測、評估及處理等類別）

（Ｂ）設計量化指標以評估實體防護措施的有效性

（Ｃ）從可接受風險程度中確定績效基準，並建立防護措施績效衡量標準

（Ｄ）應採用安全失敗（Fail Safe）的原則，也就是如果門禁系統停電時，必須要維持關閉的狀態，以避免外部人員入侵

C 4-06. 在實體防護控制措施類型中有關「偵測」實體威脅，下列哪些項目不屬於相關的偵測工具？

（Ａ）門窗開啟偵測

（Ｂ）紅外線進出感應

（Ｃ）網路行為偵測

（Ｄ）動作感應器

B 4-07. 有關實體安全計畫規劃之步驟，下列何項有誤？

（Ａ）組織計畫擬定小組

（Ｂ）決定風險轉嫁措施

（Ｃ）建立績效基準

（Ｄ）實作與防護措施

B 4-08. 人員作業區域的門其開啟方向應為下列哪一項？

（Ａ）向內開啟

（Ｂ）依疏散方向順向開啟

（Ｃ）向右開啟

（Ｄ）向左開啟

AD 4-09. 下列何者為煙霧偵測器正確的擺放的位置？**(複選)**

（Ａ）天花板下風處

（Ｂ）天花板上風處

（Ｃ）空調系統出風口

（Ｄ）空調系統進氣口

SPT 「資安實務與技術」學科試題及答案

第五類：存取控制

C 5-01. 通行碼身分鑑別技術是運用哪一種身分鑑別機制的特質？

（Ａ）基於所有

（Ｂ）基於所生

（Ｃ）基於所知

（Ｄ）與生俱備

ABC 5-02. 下列關於存取控制中避免通行碼被破解的防護措施，哪些敘述是正確的？**(複選)**

（Ａ）定期更換密碼

（Ｂ）通行碼不以明碼方式在網路上傳送

（Ｃ）登入成功或失敗都應被記錄

（Ｄ）只要定期變更，通行碼重複也沒關係

A 5-03. 使用者持有已登錄的無線感應 RFID 門禁卡才能進出機房，在存取控管技術的實作上是屬於下列哪一項？

（Ａ）只有身份的識別

（Ｂ）只有身份的鑑別

（Ｃ）包含身份的識別與鑑別

（Ｄ）沒有包含身份的識別與鑑別

AD 5-04. 鑑別符可依其使用鑑別因素的數量與類型來區分，下列哪些敘述是正確的？**(複選)**

（Ａ）通行碼是屬於「Something you know」鑑別因素

（Ｂ）生物特徵是屬於「Something you have」鑑別因素

（Ｃ）智慧卡則是屬於「Something you are」鑑別因素

（Ｄ）鑑別符可大致區分為單因素鑑別與多因素鑑別

ABD 5-05. 讓所有存取行為都可歸責到使用者真實身分的機制，下列哪些相關的敘述是正確的？**(複選)**

（Ａ）必須要具備唯一識別符可代表使用者真實身分

（Ｂ）足夠強固的使用者鑑別技術，能防止身分鑑別機制被破解

（Ｃ）系統所有存取路徑被強制控管，所有失敗存取行為須被記錄，至於成功存取行為是否紀錄則視容量大小而定。

（Ｄ）稽核紀錄的時戳可代表存取的先後次序，且稽核紀錄應被妥善保護，任何人不得修改

B 5-06. 門禁屬於下列哪一種存取控制（access control）的方式？

（Ａ）特殊的（special）

（Ｂ）實體的（physical）

（Ｃ）管理上的（administrative）

（Ｄ）功能上的（functional）

B 5-07. 下列何者不是進行身份的識別與鑑別常會用到的三種條件之一？

（Ａ）使用者所知道的（something a person knows）

（Ｂ）使用者用的（something a person uses）

（Ｃ）使用者所擁有的（something a person has）

（Ｄ）使用者所具有的（something a person is）

C 5-08. 組織內部資安規定門禁卡於進用， 離職與職務異動時， 必須重新調整， 是屬於哪一類的存取控制類型？

（Ａ）技術性

（Ｂ）實體性

（Ｃ）管理性

（Ｄ）邏輯性

A 5-09. 在 Windows 作業系統中檔案擁有者可以自行指定其他使用者是否可以存取該檔案， 這種存取控制模型是哪一種？

（Ａ）Discretionary Security Mechanism

（Ｂ）Mandatory Security Mechanism

（Ｃ）Role-based Access Control

（Ｄ）Multi-Level Access Control

SPT 「資安實務與技術」學科試題及答案

第六類：網路安全

D 6-01. 系統管理員接到一通說是賣他防火牆那家公司新來的工程師的電話，由於產品有些弱點須立即補強，一個 patch 將會以電子郵件的附件寄出，請他收到後立即執行。系統管理員依指示做了，於是木馬程式卻悄悄的打開了電腦連接埠。請問這是哪一種攻擊？

（Ａ）密碼破解攻擊

（Ｂ）阻絕服務攻擊

（Ｃ）水坑攻擊

（Ｄ）社交工程攻擊

B 6-02. 攻擊者故意混淆與錯亂片段封包中的偏移序號（offset），讓接受端作業系統在重組片段封包時產生錯誤，進而導致系統當機。請問這是哪一種攻擊？

（Ａ）Ping of Death

（Ｂ）Teardrop

（Ｃ）Smurf Attack

（Ｄ）SYN Flood

ABCD 6-03. 欲防止駭客入侵，下列哪些方法是正確的？**(複選)**

（Ａ）可用防火牆（Firewall）區隔不同安全等級網段

（Ｂ）可用防火牆（Firewall）控管阻擋不被允許的通訊協定

（Ｃ）可用入侵偵測防禦系統（IDS/IPS）立即將攻擊事件或攻擊來源進行封鎖

（Ｄ）可用入侵偵測防禦系統（IDS/IPS）分析 HTTPS 中的內容

ABD 6-04. 有關分散式阻斷服務攻擊（DDoS）描述，下列哪些是正確的？**(複選)**

（Ａ）攻擊者控制多部主機，同時對受害者發動大規模攻擊

（Ｂ）其攻擊來源 IP 太多，通常很難透過防火牆封鎖來源 IP

（Ｃ）其攻擊方法是同時多處破壞系統軟體，以癱瘓服務

（Ｄ）網路流量清洗是防止 DDoS 攻擊的方法之一

D 6-05. 下列何者為最有效防禦 Web 應用程式遭受 CSRF（Cross-Site Request Forgery）攻擊的方法？

（Ａ）只接受 HTTP POST 方法

（Ｂ）採用 HTTPS 加密通訊

（Ｃ）資料輸出前過濾特殊字元

（Ｄ）採用伺服器隨機產生的短期符記（Tokens），並於每一個動作請求前檢驗符記有效性

A 6-06. 試問攻擊者使用 ARP Broadcast 封包持續不斷告訴其他電腦，192.168.1.2（Server）的 MAC 是攻擊者的 MAC。其他電腦要傳送給 192.168.1.2 的封包會被送到攻擊者的機器上。攻擊者將封包錄下後再轉送到真正的 192.168.1.2 機器的攻擊手法稱為？

（Ａ）ARP Spoofing 攻擊

（Ｂ）MAC Spoofing 攻擊

（Ｃ）DNS Spoofing 攻擊

（Ｄ）APP Spoofing 攻擊

BCD 6-07. 下列哪些方法可以防範密碼猜測攻擊？**(複選)**

（Ａ）詳細的登入紀錄

（Ｂ）密碼複雜度要求

（Ｃ）登入失敗鎖定機制

（Ｄ）多因子驗證技術

D 6-08. 下列哪一個通訊協定無法應用在虛擬私有網路（VPN）？

（Ａ）IPSec

（Ｂ）L2TP

（Ｃ）SSL

（Ｄ）HTTP

SPT 「資安實務與技術」學科試題及答案

第七類：密碼學與加密技術

C 7-01. 當有 10 個使用者使用對稱式加解密演算法時，需要管理幾把金鑰？

（A）10

（B）20

（C）45

（D）55

ABC 7-02. 對稱式加解密演算法的敘述，哪些為正確？**(複選)**

（A）相較於非對稱式加解密演算法，其加解密速度較快

（B）若金鑰長度夠長，將難以被破解

（C）將金鑰安全的交換至加密對象，需要額外的安全機制

（D）只提供機密性（Confidential）保護功能，也提供不可否認性功能

ABD 7-03. 關於對稱式加解密演算法的優缺點，下列哪些敘述是正確的？

(複選)

（A）將金鑰安全的交換至加密對象，需要額外的安全機制

（B）10 個使用者需要 45 把金鑰

（C）只提供不可否認性保護功能，無法提供機密性功能

（D）如果金鑰長度夠長，將難以被破解

A 7-04. 非對稱式加解密的演算法，配對的金鑰，由公開金鑰加密只能用私密金鑰解密，由私密金鑰加密只能用公開金鑰解密. 下列何者屬於非對稱式加解密的演算法？

（A）RSA

（B）DES

（C）AES

（D）RC5

A 7-05. 若 A 要傳輸一份文件 Doc_A 給 B，使用非對稱式加解密的演算法，下列何種方式可確保只有 B 能看的到 Doc_A 明文內容？

（Ａ）傳輸前，以 B 的公鑰對文件加密

（Ｂ）傳輸前，以 B 的公鑰對文件加簽

（Ｃ）傳輸前，以 A 的私鑰對文件加密

（Ｄ）傳輸前，以 A 的私鑰對文件加簽

ABC 7-06. 下列哪些項目有可能會影響加密技術的強度？**(複選)**

（Ａ）演算法強度

（Ｂ）金鑰保護機制

（Ｃ）亂數產生器的不可預測性

（Ｄ）演算法的保密

ABD 7-07. 加密與簽章技術係用來確保資訊的下列哪些目標？**(複選)**

（Ａ）機密性

（Ｂ）完整性

（Ｃ）可用性

（Ｄ）不可否認性

ABC 7-08. 下列關於「密碼」與「金鑰」的描述，哪些是正確的？**(複選)**

（Ａ）電腦系統的存取控制常使用帳號與密碼來限制

（Ｂ）密碼學裡頭常使用金鑰來對資料加密

（Ｃ）金鑰須搭配演算法來對資料進行加密（encryption）或是解密（decryption）

（Ｄ）「密碼」與「金鑰」兩者的概念是相同的

D 7-09. 下列何者非對稱式加密演算法？

（Ａ）3DES

（Ｂ）RC4

（Ｃ）AES

（Ｄ）RSA

SPT 「資安實務與技術」學科試題及答案

第八類：持續運作與災難復原

AD 8-01. 業務永續運作計畫（Business Continuity Plan， BCP）測試與演練的時機，哪些敘述正確？**(複選)**

（Ａ）定期

（Ｂ）發生事故前不須測試與演練，但發生事故後必須測試與演練

（Ｃ）上級長官視察之前

（Ｄ）SYN Flood

ACD 8-02. 關於業務永續運作計畫（Business Continuity Plan，簡稱 BCP）的敘述，下列哪些是正確的？**(複選)**

（Ａ）當組織面臨重大災難發生時如何持續業務營運

（Ｂ）屬操作性的文件、目的是要維護主要關鍵業務的運作

（Ｃ）必須獲得高階管理人員「認同與支持」

（Ｄ）主軸是「關鍵業務」，是從「業務流程」的思維來規劃，因此必須要關鍵業務所有相關部門的投入，才可能完整

D 8-03. 在業務永續運作計畫中「復原階段」與「重建階段」的目標差異為何？

（Ａ）「復原階段」是讓所有業務回復至暫時可運作的狀態，「重建階段」則是讓所有業務回復到一般正常作業

（Ｂ）「復原階段」是讓關鍵業務回復至暫時可運作的狀態，「重建階段」則是讓所有業務回復到一般正常作業

（Ｃ）「重建階段」是讓關鍵業務回復至暫時可運作的狀態，「復原階段」則是讓關鍵業務回復到一般正常作業

（Ｄ）「復原階段」是讓關鍵業務回復至暫時可運作的狀態，「重建階段」則是讓關鍵業務回復到一般正常作業

B 8-04. 當進行業務永續運作計畫時，其工作時程區分階段下列何者描述有誤？

（Ａ）啟動階段

（Ｂ）偵測階段

（Ｃ）復原階段

（Ｄ）重建階段

D 8-05. 試問業務永續運作管理之事項在組織內部是下列哪一個部門之責任？

（Ａ）資訊業務所有相關部門

（Ｂ）稽核業務所有相關部門

（Ｃ）組織內部所有相關部門

（Ｄ）關鍵業務所有相關部門

C 8-06. 「假如破壞與損失已經發生，組織要有復原的程序」，這種作業通常以下列哪一項目稱之？

（Ａ）業務持續運作（BCP，business continuity planning）

（Ｂ）病毒安全防護（VPP，virus protection planning）

（Ｃ）災難復原計畫（DRP，disaster recovery planning）

（Ｄ）緊急應變計畫（BCNP，business contingency planning）

B 8-07. 災難發生的時候可能平時營運作業的地點受到破壞，無法繼續正常運作，此時需要在另外的地點暫時先恢復作業，「備援地點有完整的運算設施以及網路連線，而且儲存的資料是由正常營運地點複製過來的」，以上描述的是一種什麼樣的替代性處理地點？

（Ａ）冷點（cold sites）

（Ｂ）熱點（hot sites）

（Ｃ）溫點（warm sites）

（Ｄ）行動點（mobile sites）

C 8-08. 下列何者為營運衝擊分析的正確說明？

（Ａ）政策宣示， 讓政策成為引導的標準， 並且開始分配負責的人力

（Ｂ）確認威脅以後， 找出方法， 以最經濟的方式來降低風險

（Ｃ）確認主要功能與系統， 同時讓企業決定其優先順序，找出弱點與威脅， 並且估計風險

（Ｄ）訂出災難發生時處理步驟與原則

SPT 「資安實務與技術」學科試題及答案

第九類：應用程式與軟體開發安全

D 9-01. 下列何者會幫助攻擊者了解系統並組織攻擊計畫？
（Ａ）反射注入
（Ｂ）明文密碼（Hard-coded Password）
（Ｃ）HTTP 應答分割（HTTP Response Splitting）
（Ｄ）資訊揭露

D 9-02. 在 Web 2.0 時期，有超過七成的攻擊來自網路 ISO/OSI 七層架構中哪一層？
（Ａ）實體層
（Ｂ）網路層
（Ｃ）傳輸層
（Ｄ）應用層

D 9-03. 何者為 OWASP 2017 十大資安風險之「首」？
（Ａ）入侵網頁伺服器進行網頁置換
（Ｂ）暴力破解帳號密碼
（Ｃ）分散式阻斷服務攻擊 （Distributed Denial-of-Service）
（Ｄ）注入攻擊（injection）

ACD 9-04. 下列哪些項目不算是 Web 應用程式常見的源碼弱點？**(複選)**
（Ａ）中間人攻擊（Man-in-The-Middle）
（Ｂ）明文密碼 （Hard-coded Password）
（Ｃ）偽裝 （Masquerade）
（Ｄ）連線劫持（Session Hijacking）

BCD 9-05. 下列哪些攻擊行為屬於應用層防火牆（WAF）的防護範圍？**(複選)**
（Ａ）避免檔案中存有明文密碼（Hard-coded Password）
（Ｂ）跨網站入侵字串（XSS）攻擊
（Ｃ）SQL 注入攻擊
（Ｄ）下載非一般常見的網頁檔案（如 bak、tmp 等副檔名）

BCD 9-06. 下列哪些項目屬於 Web 應用程式安全防護機制的範圍？**(複選)**

（Ａ）Web 應用程式源碼規模評估

（Ｂ）安全弱點評估

（Ｃ）滲透測試

（Ｄ）設定 Web 應用層防火牆規則

B 9-07. 當我們部署「網路防火牆」，於設定放置網頁伺服器的 DMZ 和個人使用區域的內網兩界面間的法則，下列何者較為適當？

（Ａ）DMZ 區自由進出內網以增加便利性

（Ｂ）適當限制 DMZ 流入內網區界面

（Ｃ）內網自由進出 DMZ 區以方便獲取檔案

（Ｄ）完全禁止內網進出 DMZ 區以增加安全性

D 9-08. 系統安全需求應在資訊系統規劃之何者階段，即將資訊安全需求納入，新開發的資訊系統，或是現有系統功能之強化，皆應明訂資訊安全需求，並將資訊安全需求納入系統功能？

（Ａ）程式實作階段

（Ｂ）測試與驗收階段

（Ｃ）架構設計階段

（Ｄ）需求分析階段

ABC 9-09. 關於應用程式的品質與安全檢測敘述，下列哪些項目是正確的？**(複選)**

（Ａ）任何應用程式都有可能有瑕疵或是弱點

（Ｂ）安全程式開發（secure programming）是直接嘗試消除程式瑕疵

（Ｃ）安全檢測是嘗試發現程式瑕疵

（Ｄ）源碼檢測（Static Code Analysis）是模擬攻擊者行為找出網站漏洞

BC 9-10. OWASP Top 10 中 XML External Entities 弱點可能會造成什麼樣的風險？**(複選)**

（Ａ）資料庫資料外洩

（Ｂ）內部檔案的洩露

（Ｃ）服務中斷

（Ｄ）遠端執行程式碼

D 9-11. 應用程式開發商為了方便系統維護， 在程式中置入可以任意存取後端資料庫的程式碼， 此項為哪一種應用程式威脅？

（Ａ）邏輯炸彈

（Ｂ）輸入攻擊

（Ｃ）緩衝區溢位

（Ｄ）後門程式

SPT 「資安實務與技術」學科試題及答案

第十類：安全作業

AB 10-01. 系統稽核紀錄應被妥善的保護，以維護紀錄的完整性與可追究責任性。關於稽核紀錄的保護下列哪些是正確的技術應用？**(複選)**

（Ａ）時間同步，以確保稽核紀錄能代表事實發生的時間序

（Ｂ）採用「唯讀儲存媒體」以避免非授權變動

（Ｃ）採用「雜湊」與「簽章技術」以避免非授權存取

（Ｄ）採用「存取控管」以檢查非授權變動

ACD 10-02. 當組織 RAID 5 的磁碟陣列壞了一顆之後並不影響其正常之運作，但在定期維護或異常偵測時發現了這種狀況，下列哪些做法不是正確的？**(複選)**

（Ａ）把所有硬碟全部更換

（Ｂ）儘快更換故障硬碟，以避免第二顆硬碟同時故障

（Ｃ）待第二顆硬碟故障時再予以更換

（Ｄ）將故障硬碟取下，避免感染第二顆硬碟

ABC 10-03. 減緩攻擊的封鎖行動，下列哪些算是合適的做法？**(複選)**

（Ａ）變更通行碼與權限，讓攻擊者無法再使用即用權限登入

（Ｂ）對於可疑的連線流量，可透過防火牆或路由器導到不存在的位址，讓可疑的連線可以被監控

（Ｃ）關閉不必要的服務，以避免不必要的服務被攻擊者所運用

（Ｄ）驚動入侵者以避免其後續攻擊

ABC 10-04. 下列關於作業安全中行政管理的描述，哪些是正確的？**(複選)**

（Ａ）責任分離算是預防性的方法，讓意圖不軌的人需要先找共犯，提高犯罪的難度

（Ｂ）在行政管理的控制上通常還會要求做到最少權限（least privilege）與僅知需知（need to know）

（Ｃ）假如有人想做壞事，透過工作輪替會比較容易發覺

（Ｄ）應讓企業成員能盡量存取需要用到的資源，擁有充裕的權限，這樣可以提升效率

C 10-05. 當電腦系統運作遇到異常狀況時，為避免情況惡化，下列哪一項非適當的處理方式？

（Ａ）暫時停止回應（freeze）

（Ｂ）關機（shut down）

（Ｃ）不予處理（ignore）

（Ｄ）重開機（reboot）

BC 10-06. 下列關於滲透測試進行實務的描述，哪些項目是錯誤的？**(複選)**

（Ａ）滲透測試可以針對限制的區域與時段

（Ｂ）滲透測試的對象應保持機密，不必事先取得同意

（Ｃ）滲透測試可存取機密資訊

（Ｄ）應透過滲透測試再度驗證修補是否有效

B 10-07. 「系統遇到無法控制的失敗狀況，一定要重新開機才能解決」，上述情況是系統作業失敗所採取的哪一類回應？

（Ａ）系統重開機（system reboot）

（Ｂ）系統緊急重開機（emergency system restart）

（Ｃ）系統冷開機（system cold start）

（Ｄ）系統安全關機（system shutdown）

B 10-08. 在組織中人員工作輪調機制， 在資訊安全的角度上除了訓練備援人手外， 還有何好處？

（Ａ）培養全能員工

（Ｂ）在工作輪調過程中比較容易發現工作弊端

（Ｃ）有利於組織創新發展

（Ｄ）藉此培訓主管人才

SPT 「資安實務與技術」學科試題及答案

第十一類：資訊安全管理實務

D 11-01. 電腦病毒的下列組成中的哪一項是用來「記錄進行破壞的方式或是保存破壞時所需要的資訊。」？

（Ａ）標記（Mark）

（Ｂ）感染機制（Infection mechanism）

（Ｃ）觸發條件（Trigger）

（Ｄ）破壞內涵（Payload）

B 11-02. 下列哪一種惡意程式會控制另一台網際網路上的電腦，然後利用該電腦來發動攻擊，讓原始來源難以追查？

（Ａ）蠕蟲（worms）

（Ｂ）僵屍（Zombie）

（Ｃ）廣告軟體（Adware）

（Ｄ）後門（backdoor）

A 11-03. 「假冒別人（例如銀行）送出電子郵件給受害者，裡面有連接假網站的超連結，通常網址跟真網站很接近，登入的畫面則一模一樣，一旦受害者登入之後，帳號密碼就會被記錄下來。」以上所描述的詐騙方式也稱為下列的哪一種惡意程式？

（Ａ）網路釣魚（phishing）

（Ｂ）特洛依木馬（Trojan Horse）

（Ｃ）後門（backdoor）

（Ｄ）蠕蟲（worm）

B 11-04. 「病毒會將自己複製到其他的程式中，或是儲存在磁碟上的系統區域。」以上所描述的是病毒發展的哪一個時期？

（Ａ）潛伏期（Dormant phase）

（Ｂ）傳播期（Propagation phase）

（Ｃ）觸發期（Triggering phase）

（Ｄ）執行期（Execution phase）

B 11-05. 個人電腦病毒風險評估法中沒有包括下列哪一種方法？

（Ａ）了解所使用的作業系統版本

（Ｂ）了解電腦所擺放的地點的溫度

（Ｃ）了解有多少人使用我們的電腦

（Ｄ）了解是否經常更新安全性的系統修補（security patches）

D 11-06. 小王是一位程式設計師，他在程式中隱藏了一段”當 4 月 1 日愚人節時將硬碟刪除”的程式碼，請問這是屬於哪一項的應用程式威脅？

（Ａ）緩衝區溢位（Buffer overflow）

（Ｂ）輸入攻擊

（Ｃ）隱藏通道（covert channel）

（Ｄ）邏輯炸彈

B 11-07. 下列哪一項是「木馬」程式的定義？

（Ａ）留在系統內不需經一般安全控管程序，就可以被植入者遙控的惡意程式

（Ｂ）是一種陷阱程式，等待使用者踩到陷阱程式後，再運用使用者權限執行不當的指令

（Ｃ）需被動依賴寄宿的應用程式重製自已或感染其他程式

（Ｄ）為存取控管機制的漏洞，原非預期用來傳送資料的管道被惡意運用後，可以跳脫存取控管機制存取到不應存取的資料

B 11-08. 電子資料處理的防護方法有很多類，就「存取權限管理」而言，在實作上應秉持下列哪一項原則？

（Ａ）防止資料殘存原則

（Ｂ）最小揭露原則

（Ｃ）可追溯原則

（Ｄ）適當稽核原則

C 11-09. 一份公文中有三份附件，其機密等級分別為：機密、密及一般。當三份附件分別保管時，則機密等級為下列何者？

（Ａ）密

（Ｂ）機密

（Ｃ）附件原有各該之機密等級

（Ｄ）一般

ABD 11-10. 企業在蒐集個人資料時，依現行個資法第 5 條規定，下列敘述哪些是正確的？**(複選)**

（Ａ）依誠實與信用方法為之

（Ｂ）不得逾越特定目的之必要範圍

（Ｃ）應與蒐集之組織具有正當合理之關聯

（Ｄ）尊重當事人之權益

BD 11-11. 下列有關於電子資料分級的描述，哪些項目是錯誤的？**(複選)**

（Ａ）電子資料在生成之初即應進行分級作業

（Ｂ）分級作業應由資料擁有者完成

（Ｃ）常見的缺失為分級作業未執行或人員為簡化程序將機密文件分級為一般文件

（Ｄ）分級作業與後續的保護措施無關

C 11-12. 下列有關於電子資料儲存的描述，哪一個項目是錯誤的？

（Ａ）為了防範毀損造成的危害，電子資料備份是不可或缺的

（Ｂ）從機密性的角度而言，備份資料的製作若未加密，也象徵著洩密管道的增加

（Ｃ）同時維護電子資料的可用性與機密性不會產生衝突

（Ｄ）採用加密的方式是最簡便的維護電子資料機密性的方式

A 11-13. 未經嚴謹銷毀程序之資料若遭駭客取得並回復，會破壞原本資料的哪一種安全特性？

（Ａ）機密性

（Ｂ）完整性

（Ｃ）可用性

（Ｄ）真實性

C 11-14. 在資料清除在下列哪種環境要確認難度最高？

（Ａ）個人電腦的硬碟

（Ｂ）機房內主機磁碟陣列

（Ｃ）公有雲服務

（Ｄ）唯讀光碟

C 11-15. 有關電子資料之蒐集，下列敘述何者不正確？

（Ａ）如為版權資料，應獲得授權後始得引用

（Ｂ）經其他單位傳送來之資料，應遵守原有資料之機密等級作業規定

（Ｃ）電子資料產生時，其所蒐集的參考資料可能本身具機敏性，但因僅作為過渡資料，故毋須分級

（Ｄ）網路蒐集而得之資料，應辨認或查驗其正確性，確保資料無誤

ABD 11-16. 有關電子資料處理之防護，下列哪些敘述是正確的？**(複選)**

（Ａ）於電腦中安裝暫存檔清除工具，可減少資訊殘存問題之發生

（Ｂ）確認雲端儲存的資料在合約終止後是否完全清除

（Ｃ）存取權限管理，透過相關工具軟體遵循「最大揭露原則」，供存取職務所需之資料

（Ｄ）記錄使用者的存取行為

A 11-17. 針對資料蒐集處理原則，當不同等級之國家機密合併使用或處理時，應以下列哪一項原則最佳？

（Ａ）以最高之等級為機密等級

（Ｂ）以最多之等級為機密等級

（Ｃ）以最低之等級為機密等級

（Ｄ）以個別原來之等級為機密等級

ABCD 11-18. 關於寄件人是有一致的分析，請問下列哪些正確？**(複選)**

（Ａ）比對 From: 標頭中的 domain 與 Received：

（Ｂ）比對 From: 標頭中的 domain 與 Message-ID

（Ｃ）比對 SMTP 的 MAIL FROM 與 From: 標頭

（Ｄ）比對 SMTP 的 RCPT TO 與 To: 標頭

C 11-19. 以下關於 SPF（Sender Policy Framework）中 DNS 紀錄，何者有誤？

（Ａ）A：名稱對應到 IP 位址

（Ｂ）MX：指出負責該網域的郵件伺服器

（Ｃ）PTR：名稱對應到 IP 位址

（Ｄ）TXT：任意文字字串，最長 255 字元

ABCD 11-20. 下列關於 DNS 反解之敘述哪些正確？**(複選)**

（Ａ）連線時檢查來源 IP 的 PTR 紀錄「是否存在」

（Ｂ）連線時檢查來源 IP 反解（IP 解析成名稱）所得的名稱再做正解（名稱解析成 IP）後是否一致

（Ｃ）若垃圾郵件發信人（Spammer）是使用自己的網域來發信，那麼 DNS 反解無法控管這類狀況

（Ｄ）來信端沒有設定好其自己的 DNS 反解時，有可能導致收不到正常的信件。

A 11-21. 下列何者無助於提高檢視電子郵件之安全性？

（Ａ）使用預覽視窗

（Ｂ）收信時以純文字方式閱讀

（Ｃ）盡量使用密件副本傳送多收件人

（Ｄ）關閉「傳送讀取回條」

A 11-22. 請問何者是提升人員對電子郵件使用安全的最適當方法？

（Ａ）定期舉辦「人員安全認知訓練」以及「社交工程演練」

（Ｂ）定期修補電子郵件伺服器的漏洞

（Ｃ）使用者電腦需要安裝防毒軟體

（Ｄ）過濾垃圾郵件

ABC 11-23. 請問下列哪些描述是郵件伺服器需要放在 DMZ 區的原因？**(複選)**

（Ａ）電子郵件伺服器需要對網際網路開放才能接收信件，因此放在 DMZ 比較合適

（Ｂ）透過防火牆設定，僅開放 25 port 對外公開服務，以降低攻擊表面

（Ｃ）避免電子郵件伺服器一但遭受入侵，就變成進入內網最佳跳板

（Ｄ）電子郵件伺服器需放在 DMZ 以便內部的使用者才可以連得到

B 11-24. 以下哪一種 Email 連線過濾機制的缺點是可能會造成延遲收到信？

（Ａ）將有效的網址列入白名單（Allowed List）

（Ｂ）灰名單（Graylist）過濾機制

（Ｃ）定期更新郵件黑名單（Realtime Blacklist）

（Ｄ）使用 DNS 反解

ABCD 11-25. 電子郵件安全威脅包括以下哪些？**(複選)**

（Ａ）注入式攻擊（Injection）

（Ｂ）進階型持續滲透攻擊（APT）

（Ｃ）社交工程攻擊

（Ｄ）勒索軟體（Ransomware）

D 11-26. 郵件伺服器管理者會都強烈要求不要使用 Email 預覽視窗，因預覽視窗容易發生以下哪一項威脅？

（Ａ）阻斷服務攻擊（DoS）

（Ｂ）密碼遭到破

（Ｃ）注入式攻擊（Injection）

（Ｄ）惡意病毒碼或後門程式

D 11-27. 下列有關電子郵件伺服器部署方式，可能形成防護架構上的漏洞或弱點之描述，下列何者為非？

（Ａ）開放 SMTP（TCP 25 port）內到外的連線，將無法控管使用者外寄信件，導致資料外洩或變成垃圾信件寄件者的跳板

（Ｂ）電子郵件伺服器置於內網，可能致使伺服器變成入侵跳板

（Ｃ）開放下載外部私人信件（POP3/IMAP4/Webmail），易形成電子郵件防毒、防垃圾與資料外洩的防護漏洞

（Ｄ）部署時應優先考量頻寬管理

ABD 11-28. 行動裝置具下列哪些與其他資訊設備不同的特性，而產生資安議題？**(複選)**

（Ａ）硬體可攜性

（Ｂ）可隨時上網

（Ｃ）資料可抹除性

（Ｄ）資料可攜性

A 11-29. 行動裝置的可信度，最容易因下列何者行為而遭破壞？

（Ａ）越獄（JailBreaking）

（Ｂ）啟用 QR 條碼

（Ｃ）接觸 NFC 晶片

（Ｄ）開啟無線熱點

B 11-30. 行動裝置資安議題中的行動通訊裝置管理（Mobile Device Management， MDM）解決方案應具備下列何項功能？

（Ａ）庫存管理與應用程式保護

（Ｂ）安全管理、監控與提報

（Ｃ）庫存管理與應用程式安全

（Ｄ）安全管理與應用程式使用紀錄

BCD 11-31. 下列有關於行動裝置管理 BYOD 模式的描述，哪些是正確的？**(複選)**

（Ａ）裝置所有權屬組織所有，資訊擁有權屬個人所有

（Ｂ）是指 Bring Your Own Device

（Ｃ）組織僅有權對於組織所擁有之資訊進行管理與處分

（Ｄ）應強化行動應用程式管理之需求

C 11-32. 下列有關於行動裝置可信度的描述，哪一項是錯誤的？

（Ａ）許多行動裝置，特別是個人行動裝置，未必值得信任

（Ｂ）行動裝置可能會發生越獄（Jailbreaking）

（Ｃ）行動裝置不會發生提權（Rooting）的狀況

（Ｄ）機構應假設所有的行動裝置都不可信任

A 11-33. 下列有關於行動裝置與其他系統互動的描述，哪一項是錯誤的？

（Ａ）機構配發的行動裝置應限於只能與個人所擁有的電腦進行同步動作

（Ｂ）對行動裝置可以同步的資料或設備應進行安全管控

（Ｃ）資料同步與儲存時，行動裝置可能需與其他系統互動

（Ｄ）有些與行動裝置互動的設備是屬外部的，無法予以管控

B 11-34. 下列有關於行動裝置使用定位服務的描述，哪一項是錯誤的？

（Ａ）內建 GPS 功能的智慧型行動裝置通常可以執行在地化服務（Location-based services）

（Ｂ）使用在地化服務功能的行動裝置可以降低目標性攻擊的風險

（Ｃ）使用者與行動裝置的所在位置的資訊，讓攻擊者易於利用這些資訊發動攻擊

（Ｄ）行動裝置使用定位服務時會比較耗電

C 11-35. 下列有關於機敏會議之行動裝置管理的描述，哪一項是錯誤的？

（Ａ）可運用行動裝置管理技術對於行動裝置的硬體進行控制

（Ｂ）重要會議應標示會議之機密等級，於會議開始之前將行動裝置集中保管

（Ｃ）出國參加重要機敏或是談判會議等，建議出國之人員應盡量使用自己的行動裝置

（Ｄ）SIM 卡可以出國前才新申請開通（使用舊門號換新 SIM 卡），以確保未遭受竊聽或是植入惡意程式竊取機敏資料

C 11-36. 下列有關於行動裝置的電磁波遮蔽與生物效應的描述，哪一項是錯誤的？

（Ａ）金屬或導電的材料對高頻的電磁波有比較好的遮蔽性

（Ｂ）針對機敏作業場所，建議可以採用電子圍籬（Electronic fences）安全管理機制

（Ｃ）手機的電磁波可以參考 SNR（訊號雜訊比）規範的說明

（Ｄ）離有害的電磁波越遠越安全

C 11-37. 下列有關於行動裝置上軟體下載與使用的描述，哪一項是錯誤的？

（Ａ）僅安裝來自可信任來源之軟體

（Ｂ）注意軟體權限

（Ｃ）軟體更新與修補程式應由原廠人工處理

（Ｄ）安裝資安防護軟體

B 11-38. 針對內容之「清除所有內容和設定」，這個動作通常是在行動裝置安全管控生命週期中的哪一個階段進行的？

（Ａ）發展

（Ｂ）汰舊

（Ｃ）維運

（Ｄ）建置

BCD 11-39. 下列有關於行動應用情境分析的描述，哪些是正確的？**(複選)**

（Ａ）是一種可以掌握組織現在以及過去行動需求分析之方法

（Ｂ）從資訊擁有者及裝置擁有者分析組織有哪些的業務活動，可以採用行動化之應用服務

（Ｃ）考量需要採取之管理模式

（Ｄ）幫助業務人員評估可導入的行動應用

D 11-40. 「利用竊取的憑證來欺騙原身份用戶的朋友或是同儕，達到惡意的目的」，以上的描述的是下列的哪一種社群網路的威脅？

（Ａ）點擊劫持（clickjacking）

（Ｂ）反匿名化（de-anonymization）

（Ｃ）假造身份（fake profiles）

（Ｄ）冒用身份（identity clone）

C 11-41. 下列有關於行動應用情境分析進行方式的描述，哪一項是錯誤的？

（Ａ）對外建立以使用者為中心的網路服務平臺，不要被網路實體隔離之觀念與機制所限制

（Ｂ）對內建置辦公室標準化公務作業環境，強化行動化工具支援

（Ｃ）應考慮現行之業務，尋找任何可以行動化應用之需求

（Ｄ）在安全與維運效率得以兼顧之前提之下，將實體隔離網路內部之部分資訊服務，適度延伸至行動裝置上

BC 11-42. 以下有關於委外人員安全管理的描述，哪些是正確的？**(複選)**

（Ａ）只要不是和業務直接相關的人員都算是委外人員，需要當成委外人員來進行安全管理

（Ｂ）在委外的過程中，應監督委外人員是否按照資安的要求執行委外的業務

（Ｃ）資訊安全作業應按照資訊管理的要求執行，例如機房進出的登記管制、重要系統的稽核紀錄

（Ｄ）委外人員透過遠端進行操作與存取時，因為不在機構現場，可不在資安管理的範圍內

B 11-43. 一般說來，以下所列的哪一項是資訊安全管理中最脆弱的一環？

（Ａ）防火牆

（Ｂ）機構內部的人員

（Ｃ）網站伺服器

（Ｄ）作業系統

C 11-44. 機關將關鍵資訊系統委託民間廠商開發及營運時，在委外作業各階段的安全控管措施，何者有誤？

（Ａ）在計畫階段進行風險分析並擬訂出安全需求

（Ｂ）在招標階段聘請具資安專長之委員協助評估廠商資安能力

（Ｃ）在履約階段由委外廠商稽核人員負責安全監督與稽核

（Ｄ）在履約階段相關作業應符合機關安全政策與程序之要求

A 11-45. 政府資訊作業委外作業流程，依據「政府採購法」可分為「計畫作業」、「招標」、「決標」、「履約管理」、「驗收」及「爭議處理」等各階段，請問「導入安全控制措施及確認委外資安需求」是在哪一階段進行？

（Ａ）計畫作業階段

（Ｂ）履約管理階段

（Ｃ）驗收階段

（Ｄ）爭議處理階段

C 11-46. 關於委外服務資安策略下列敘述何者為非？

（Ａ）政府資訊業務委外應建立事前規劃、事中招標及事後執行維運機制，並妥善規劃服務移轉事宜

（Ｂ）重要資訊專案委外案件於正式公告招標前，應透過公開徵求資訊或徵求修正意見等方式，廣納各界意見，據以訂定合宜之資安需求規格（Request For Proposal, RFP）

（Ｃ）為提升資訊安全服務品質，各組織應視個案機敏性質，將資訊安全投入成本另外評估，不計入計價亦不納入評選計分

（Ｄ）重要資訊專案採用規劃標、建置標及監督審驗標等程序辦理

C 11-47. 在資訊作業委外過程中在哪個階段應完成廠商的保密切結書？

（Ａ）計畫階段

（Ｂ）招標階段

（Ｃ）決標階段

（Ｄ）履約階段

A 11-48. 在委外案件的採構程序中，下列哪個階段在順序上通常相對在最後面？

（Ａ）爭議處理階段

（Ｂ）招標作業階段

（Ｃ）履約管理階段

（Ｄ）決標階段

C 11-49. 以下有關於社群軟體安全的描述，哪一項是錯誤的？

（Ａ）社群網路上的好友可能是假冒的，也有可能本來就不懷好意，應避免分享個資或機密

（Ｂ）花一點時間檢視自己在社群軟體裡頭的隱私設定，調整成比較安全的設定

（Ｃ）使用社群軟體時載具本身有一些固有的安全機制，比較不需

要再採取額外的安全措施

（Ｄ）惡意軟體在社群軟體上也會傳播的很快

A 11-50. 「駭客誘導使用者點按在不是原本想點按的位置上，引發惡意的效應如張貼垃圾訊息等」，以上的描述的是下列的哪一種社群網路的威脅？

（Ａ）點擊劫持（clickjacking）

（Ｂ）反匿名化（de-anonymization）

（Ｃ）假造身份（fake profiles）

（Ｄ）冒用身份（identity clone）

A 11-51. 為防止組織內之資訊因委外作業而遭未經授權的實體存取、損害及干擾，關鍵或敏感的資訊處理設施應置放於下列何處？

（Ａ）安全區域

（Ｂ）開放區域

（Ｃ）封閉區域

（Ｄ）公用區域

B 11-52. 「須避免當完成網路上的採購之後，確認的付款金額遭到更改，引起買賣雙方的糾紛」，以上所描述的屬於下列哪一種電子商務安全問題？

（Ａ）交易的私密性要求

（Ｂ）交易的完整性要求

（Ｃ）交易的真實性要求

（Ｄ）交易的身份識別要求

B 11-53. 「運用公開資訊與資料採礦的技巧，反解出用戶的識別，可針對社群網路發動攻擊」，以上的描述的是下列的哪一種社群網路的威脅？

（Ａ）點擊劫持（clickjacking）

（Ｂ）反匿名化（de-anonymization）

（Ｃ）假造身份（fake profiles）

（Ｄ）冒用身份（identity clone）

C 11-54. 下列關於在行動裝置上使用社群軟體的描述，哪一項是錯誤的？

（Ａ）社群軟體也會成為駭客攻擊的目標

（Ｂ）社群軟體的即時性使許多組織樂於導入使用於工作情境

（Ｃ）應強制在桌機上才能使用社群軟體來維繫資訊安全

（Ｄ）在公務上使用社群軟體應該取其利而避其害

B 11-55. 「商業機構透過電子商務平台將商品或服務銷售給顧客」，以上所描述的屬於下列哪一種電子商務型態？

（Ａ）B2B

（Ｂ）B2C

（Ｃ）C2C

（Ｄ）C2B

C 11-56. 「行動載具上定位資訊的洩漏等同於資訊洩漏，使用社群軟體有同樣的問題」，以上的描述的是下列的哪一種社群網路的威脅？

（Ａ）推演攻擊（inference attack）

（Ｂ）資訊洩漏（information leakage）

（Ｃ）位置洩漏（location leakage）

（Ｄ）網路騷擾（cyberstalking）

D 11-57. 「透過社群網路對特定的個人用戶或是社團進行不當的互動，進行的方式很多」，以上的描述的是下列的哪一種社群網路的威脅？

（Ａ）推演攻擊（inference attack）

（Ｂ）資訊洩漏（information leakage）

（Ｃ）位置洩漏（location leakage）

（Ｄ）網路騷擾（cyberstalking）

A 11-58. 「駭客可以結合公開資訊與社群網路上取得的資訊，利用演算法得到用戶的敏感個資」，以上的描述的是下列的哪一種社群網路的威脅？

（Ａ）推演攻擊（inference attack）

（Ｂ）資訊洩漏（information leakage）

（Ｃ）位置洩漏（location leakage）

（Ｄ）網路騷擾（cyberstalking）

C 11-59. 下列哪一項協定標準主要是用來確保商家和客戶的身份認證和交易行為的不可否認性？

（Ａ）SSL

（Ｂ）TLS

（Ｃ）SET

（Ｄ）PCI DSS

C 11-60. 惡意程式中蠕蟲與病毒的差異， 何者描述是正確的？

（Ａ）蠕蟲需要寄宿的程式， 而病毒不需要

（Ｂ）病毒會主動感染其他程式或電腦， 蠕蟲需藉由使用者執行時才進行感染

（Ｃ）蠕蟲可獨立存在， 並自動複製感染， 但病毒需要寄宿在其他檔案中

（Ｄ）蠕蟲通常不具備惡意行為， 但病毒會有惡意動作

A 11-61. 個人資料保護法實施後， 下列哪一種行為可能觸犯個人資料保護法？

（Ａ）老師將全班同學成績公告在網路上

（Ｂ）電子商務業者將買家姓名， 電話， 地址提供給合作的物流業者

（Ｃ）銀行在經過存戶同意後， 將聯絡資料轉給其他關係企業

（Ｄ）將自己的名片交給客戶

A 11-62. 以下關於電子商務優點的描述，哪一項是錯誤的？

（Ａ）交易時間延長

（Ｂ）省下實體經營的成本

（Ｃ）市場全球化

（Ｄ）營業時間拉長

A 11-63. 「當我們把信用卡號透過網路送出去的時候勢必不希望有其他人看到或讀取」，以上所描述的屬於下列哪一種電子商務安全問題？

（Ａ）交易的私密性要求

（Ｂ）交易的完整性要求

（Ｃ）交易的真實性要求

（Ｄ）交易的身份識別要求

ACD 11-64. 下列哪些是與個人資料保護有關的專法？**(複選)**

（Ａ）個人資料保護法

（Ｂ）資通安全管理法

（Ｃ）美國 HIPAA 法案

（Ｄ）歐盟 GDPR 法案

D 11-65. 下列對於勒索軟體的描述， 何者有誤？

（Ａ）採用加密技術

（Ｂ）要付贖金才能取得解密金鑰

（Ｃ）可能透過電子郵件進行感染

（Ｄ）不會自動感染其他電腦

C 11-66. 「假如交易完成後有任何一方否認，則要由權威機構來裁決，裁決的基礎來自於交易的資料」，以上所描述的屬於下列哪一種電子商務安全問題？

（Ａ）交易的私密性要求

（Ｂ）交易的完整性要求

（Ｃ）交易的真實性要求

（Ｄ）交易的身份識別要求

B 11-67. 在 B2B2C 的電子商務型態中，第二個 B 所指的是下列哪一項？

（Ａ）商品或服務的供應商

（Ｂ）從事電子商務的企業

（Ｃ）顧客

（Ｄ）商品或服務

B 11-68. 一般人在進行與交易相關的操作時，會發現常須輸入手機號碼，收到驗證碼之後，再輸入驗證，這種驗證機制也稱為？

（Ａ）多次驗證機制

（Ｂ）多元驗證機制

（Ｃ）多人驗證機制

（Ｄ）多層驗證機制

D 11-69. 下列哪一項標準是跟信用卡產業資訊安全相關的標準？

（Ａ）SSL

（Ｂ）TLS

（Ｃ）SET

（Ｄ）PCI DSS

D 11-70. 手機上接收電子郵件最合適的通訊協定為哪一個？

（Ａ）SMTP

（Ｂ）ESTMP

（Ｃ）POP

（Ｄ）IMAP

C 11-71. 下列何者不是 OWASP Mobile Top 10 2016 中提到的行動安全風險？

（Ａ）不安全的網路連線（Insecure Communication）

（Ｂ）不安全的加解密演算法（Insufficient Cryptography）

（Ｃ）啟用定位服務（Location Service Enabled）

（Ｄ）用戶端程式碼品質（Client Code Quality）

B 11-72. 當下載安裝一個遊戲 APP 時， 該 APP 要求開放存取手機的聯絡人， 相片， 定位資訊等資訊時， 該 APP 可能具備什麼樣的安全問題？

（Ａ）免越獄植入木馬

（Ｂ）惡意程式假冒正常程式

（Ｃ）勒索程式

（Ｄ）跨站程式存取漏洞

A 11-73. 人員工作或任務職務區隔之目的，何者正確？

（Ａ）避免需共謀而進行的惡意行為

（Ｂ）落實業務需知原則（Need to Know Principle）

（Ｃ）落實最低權限原則（Least Privilege）

（Ｄ）避免特殊權限誤用

A 11-74. 在委外案件的採構程序中，哪個階段應確認委外的資安需求？
（Ａ）計畫作業階段
（Ｂ）招標作業階段
（Ｃ）履約管理階段
（Ｄ）驗收階段

C 11-75. 人員安全管理作業下列何者描述是錯誤的？
（Ａ）人員授權應維持最低權限及業務需知原則
（Ｂ）在人員異動時， 必須重新評估人員之權限
（Ｃ）將重要任務儘量交付給單一人員負責， 避免太多人知悉
（Ｄ）定期對人員進行資安宣導課程

A 11-76. 委外人員之安全監督責任屬下列哪一個角色？
（Ａ）委託方
（Ｂ）受託方
（Ｃ）第三方
（Ｄ）外稽人員

D 11-77. 下列何者不是社群網路上常見的威脅？
（Ａ）社群網路平台或應用程式分析用戶的發言或行為， 造成隱私洩漏問題
（Ｂ）駭客可以結合公開資訊與社群網路取得的資訊推演出用戶敏感資訊
（Ｃ）利用竊取的憑證來冒用身份， 欺騙原身份用戶的朋友或同儕
（Ｄ）資料庫隱碼攻擊問題， 導致個人資料外洩

B 11-78. 使用社群軟體的警覺與資安認知， 下列何者有誤？
（Ａ）注意是否從同一人收到多次的交友邀請
（Ｂ）不要連線不可信賴的 WiFi 網路
（Ｃ）細讀業者的隱私聲明
（Ｄ）修改預設的隱私設定

C 11-79. 若接到電商客服人員來電要求操作 ATM 進行任何動作時， 應有什麼警覺？

（Ａ）是否分期付款方式按錯了

（Ｂ）應先確認是哪個訂單出問題

（Ｃ）應該是詐騙電話

（Ｄ）應先確認對方來電號碼是否正確

C 11-80. 由國際兩大信用卡公司 Visa 及 MasterCard 聯合制定的網路信用卡安全交易協定為何？

（Ａ）SSL

（Ｂ）TLS

（Ｃ）SET

（Ｄ）HTTPS

SPT 「資安實務與技術」學科試題及答案

第十二類：資安發展趨勢

A 12-01. 下列何者非雲端安全問題的源起？

（Ａ）企業對於雲端安全採用率仍低，使安全防護的能力較弱

（Ｂ）企業開始依賴虛擬化環境的應用

（Ｃ）傳統的防火牆難以監控虛擬機器（virtual machine）間的網路流量和安全

（Ｄ）這些網路流量未直接在實體網路留下足跡，實體網路的監控工具不易監控

ABD 12-02. 雲端服務的安全防護常用到加密技術，請問下列哪些選項描述是正確的？**(複選)**

（Ａ）應該要對靜態資料、傳送中的資料，或是使用的資料進行加密

（Ｂ）遠端用戶、企業客戶或是雲端業者都有加密的需求

（Ｃ）同態加密（homomorphic encryption）技術的運用，讓加密資料可快速解密後進行處理可降低資料暴露的風險

（Ｄ）雲端服務的安全防護對於加密有很大的倚重

A 12-03. 若從 IaaS 的角度來看雲端資安的問題，雲端業者不會面臨的問題為何？

（Ａ）應用程式執行的安全問題

（Ｂ）虛擬主機的入侵偵測與防護技術

（Ｃ）運作時的資料完整性

（Ｄ）安全遷移（migration）的技術

ABC 12-04. 下列哪些項目屬於雲端環境中虛擬化主機之安全威脅的問題？

(複選)

（Ａ）虛擬機器跳脫

（Ｂ）系統設定飄移

（Ｃ）內部威脅

（Ｄ）主機運算量不足

ACD 12-05. 隨著接受並採用雲端運算技術的企業越來越多，雲端系統的安全問題也面對許多挑戰，在下面安全問題的描述中，哪些是正確的？**(複選)**

（Ａ）虛擬化是雲端運算中最重要的一項技術，由於企業日益依賴虛擬化，傳統基於實體安全邊界的防護機制難以有效保護虛擬化環境下的應用

（Ｂ）傳統防火牆可以監控虛擬機器（Virtual Machine）間的網路流量和安全，但仍然會造成一些關鍵性資料的洩漏

（Ｃ）虛擬機器（Virtual Machine）間的網路流量未直接在實體網路留下足跡，實體網路的監控工具不易監控

（Ｄ）傳統系統採用的資料加密方式保護資料，在雲端運算環境下可能讓不同使用者資料被共同保存在同一實體機內，無法有效保證資料安全

BCD 12-06. 在不同雲端服務模型中，提供商和用戶的安全職責有些的不同，請問下列哪些選項描述是正確的？**(複選)**

（Ａ）IaaS 提供商不僅負責實體和環境安全，還必須解決基礎設施、應用相關的安全控制

（Ｂ）IaaS 使用者負責與 IT 系統（事件）相關的安全控制

（Ｃ）PaaS 提供商負責解決實體安全、環境安全、虛擬化安全和作業系統安全等安全問題

（Ｄ）PaaS 使用者負責應用和資料的安全

D 12-07. 在雲端環境裡頭，設施主要位於雲端服務提供者（CSP，Cloud Service Provider）的所在地，資安防護時，下列何者屬於用戶端的資安管理議題？

（Ａ）虛擬化環境的系統與網路安全

（Ｂ）僵屍網路

（Ｃ）惡意程式攻擊

（Ｄ）資料內容加密保護

ABC 12-08. 關於人工智慧對資訊安全的影響與關聯，下列哪些敘述是正確的？**(複選)**

（Ａ）資安系統透過人工智慧而自主與自動化

（Ｂ）透過人工智慧防治彈性的躲避與隱匿技術、或是仿正常的行為

（Ｃ）能運用大數據與機器學習的技術來找出資安威脅與攻擊的模式與特徵

（Ｄ）人工智慧可以快速填補資安專業人力的匱乏，百利而無一害

D 12-09. 大數據的資料類型（Big Data Types）可以區分為三種，試問下列哪一種描述有誤？

（Ａ）結構化的資料

（Ｂ）非結構化的資料

（Ｃ）半結構化的資料

（Ｄ）整合結構化的資料

ABD 12-10. 下列有關於雲端服務安全管理體系的描述，哪些項目是正確的？**(複選)**

（Ａ）雲端服務安全管理體系是在 ISMS 資訊安全管理體系的核心過程基礎上，增加雲端控制矩陣 CCM 的控制要求

（Ｂ）雲端服務提供者可以建立一套機制，降低管理程序被攻擊的風險

（Ｃ）已導入 ISMS 的用戶符合雲端服務安全的要求，不需另外再建立一個雲端服務安全管理體系

（Ｄ）雲端服務安全管理體系的範圍、邊界和範疇內所實施的控制措施是基於風險管理

B 12-11. 下列何者不屬行動裝置與物聯網安全防護建議？

（Ａ）對於具備藍牙、NFC 功能的行動裝置，應具備開啟、關閉藍牙、NFC 等連接介面之功能

（Ｂ）應用程式啟用無線介面連接功能，不須在用戶確認之情況下，無線介面連接功能就可以被啟用

（Ｃ）當行動裝置的無線介面藍牙或是 NFC 已啟動，行動裝置應在用戶主介面上，提供給用戶相對應之提示

（Ｄ）針對機敏作業場所，於人員進出或是舉行機敏會議時，可以採用電子圍籬（Electronic FEnces）安全管理機制

BCD 12-12. 下列關於雲端運算（cloud computing）的精簡客戶端（thin client）之描述，哪些項目是正確的？**(複選)**

（Ａ）使用者端的電腦效能必須很好才能支持雲端運算

（Ｂ）使用者端的設備僅限於輕薄短小的智慧手機或平板電腦

（Ｃ）使用者端的設備效能不必太好，主要的運算負荷在雲端

（Ｄ）使用者對於電腦化的需求比較薄弱

C 12-13. 下列有關於雲端環境中稽核與合規的描述，哪一項是錯誤的？

（Ａ）應從服務供應商和消費者角度來確認法規遵循要求

（Ｂ）受稽方或服務供應商要表現已符合特定法規的要求

（Ｃ）實施稽核的權利比較不適合納入合約

（Ｄ）用戶應要求有權獲得稽核所需的相關資訊

D 12-14. 下列有關於雲端環境中資料安全的描述，哪一項是錯誤的？

（Ａ）應基於資料生命週期來分析雲環境中資料的安全風險

（Ｂ）雲端環境中的資料比個人電腦或網路資料夾中的靜態資料具有更強的流動性

（Ｃ）對雲端服務的資料存取，可能在眾多節點和地理位置發生

（Ｄ）資料治理需求相關的風險評估應不定期執行

D 12-15. 下列有關於雲端環境中互操作性和可移植性的描述，哪一項是錯誤的？

（Ａ）在可移植與互通性方面，存在的阻礙包括一部分雲端服務提供者對於提供可攜性和互通性保障的積極性不大

（Ｂ）可能會造成用戶傾向於同時使用其他服務提供商所提供的產品或服務

（Ｃ）因為可攜性與互通性問題的存在，許多用戶擔心遷移到雲端服務環境後，提供服務的機器、應用和資料被鎖定在雲端平臺

（Ｄ）互通性問題的解決，雖可方便平臺和模型的交互共用與合作，但會阻礙整個雲端生態系統的繁榮發展

B 12-16. 下列有關於雲端環境中安全事故管理的描述，哪一項是錯誤的？
（Ａ）虛擬化技術和雲端服務平臺固有的彈性特質，會允許更有效率和效果的回應和恢復
（Ｂ）通常會比傳統資料中心技術需要更長的服務中斷時間
（Ｃ）在某些方面使得事件調查變得更容易
（Ｄ）對於雲的持續監控機制，可以減少承擔事故處理練習所需的時間或者事故回應

C 12-17. 下列有關於伺服器虛擬化的描述，哪一項是錯誤的？
（Ａ）雲端服務的伺服器在機房集中管理
（Ｂ）實體伺服器可經由虛擬化技術分成多台虛擬伺服器
（Ｃ）降低實體伺服器的使用率
（Ｄ）採用 Hypervisor 的技術

B 12-18. 下列何者不是一般用戶擔心的雲端資安問題？
（Ａ）雲端資料被竊取
（Ｂ）雲端機房的租金費用
（Ｃ）退租後資料是否移除
（Ｄ）資料是否會被其他租戶取用

A 12-19. 在 SaaS 的雲端服務中作業系統的安全應由誰負責？
（Ａ）雲端服務業者
（Ｂ）租用戶
（Ｃ）機房提供者
（Ｄ）線路提供者

B 12-20. 下列何者為人工智慧帶來的資安威脅？
（Ａ）以人工智慧方法分析資安攻擊行為
（Ｂ）攻擊者以人工智慧方法繞過資安防護的檢查
（Ｃ）人工智慧因誤判嚴重， 尚需耗費大量專家分析的問題
（Ｄ）機器學習採樣不完整導致無法判斷攻擊行為問題

D 12-21. 下列何者不是物聯網的安全威脅？
（Ａ）相連的物件在設計之初就沒有考量資安問題
（Ｂ）採用的作業系統老舊沒有更新
（Ｃ）具有漏洞的物件數量龐大， 可能受到資安攻擊目標愈多
（Ｄ）傳統攻擊手法雖不易移植到物聯網設備， 但不斷有新興攻擊手法出現