資訊安全工程師

初級能力鑑定學習指引

科目二：資訊安全技術概論

序

為提供授課教師及考生掌握評鑑方向，準備有所依循，本計畫委託委員會題庫組及規劃組領域專家，以科目評鑑內容為分項，展開重點說明及考題解析。

本手冊為學習指引，並非教材也非題庫，僅做為引導學習的考前準備工具手冊，並不保證考試通過之責，建議依循考試簡章所公告之評鑑主題內容準備考試。

目錄

職能基準

經濟部為有效提升產業人才素質，近年來持續致力於專業人才培訓發展。為了更明確產業對各類專業人才的能力需求，特別針對亟需人才的多項重點產業，邀集產官學專家，發展產業職能基準，提供各界依其內涵辦理培訓課程及規劃能力鑑定機制。

一、何謂職能?

為完成特定職業(或職類)工作任務，所需具備的能力組合(知識、技能、態度)

二、資訊安全工程師職能基準

職類名稱	資訊安全工程師
工作描述	具備相關資訊安全知識，藉由組織內部能力或尋求外部廠商、專家協助，建立符合法規與組織安全需求之系統、網路與安全防護架構，並執行相關維運作業與協助其他單位執行資訊安全相關活動。
入門水準	1.大學或專科以上學歷，或具有資訊安全相關背景，資訊或電機相關科系尤佳。 2.具備英文閱讀能力，具跨領域學習特質者尤佳。
基準級別	4

完整的資訊安全工程師職能基準，可從 iPAS 網址下載：

https://www.ipas.org.tw/AbilityStandardDownload.aspx

第一章. 考科與評鑑內容

科目	評鑑主題	評鑑內容	百分比
考科二：資訊安全技術概論	網路與通訊安全	1-1.網路安全	15%
		1-2.通訊安全	10%
	作業系統與應用程式安全	2-1.作業系統安全	10%
		2-2.作業系統與應用程式 (含資料庫與網頁)攻擊手法	10%
		2-3.程式與開發安全	10%
	資安維運技術	3-1.惡意程式防護與弱點管理	10%
		3-2.資料安全及備份管理	10%
		3-3.日誌管理	10%
	新興科技安全	4-1.雲端安全概論	5%
		4-2.行動裝置安全概論	5%
		4-3.物聯網安全概論	5%

第二章. 參考書目

參考書	作者	出版社
資訊安全概論（第三版）	林祝興、張明信	旗標
資訊與網路安全：基礎系統資訊安全技術與實務（修訂版）	賈蓉生、許世豪、林金池、賈敏原	博碩
資訊安全概論與實務（第三版）	潘天佑	碁峰

第三章. 考科內容

本指引將說明「資訊安全工程師」之考科二「資訊安全技術概論」考試內容，包含評鑑主題「網路與通訊安全」、「作業系統與應用程式安全」、「資安維運技術」與「新興科技安全」，並在章節後面添加練習評量供讀者練習。

第四章. 網路與通訊安全

第一節　網路安全

隨著經濟全球化的發展，網路的使用日益廣泛與多元，搭配多樣終端設備的應用，除了豐富一般使用者的生活經驗外，也大幅提升企業的競爭力。

網路安全的目標，為確保資訊在網路以及其支援的資訊處理設施上可得到保護。然而網路上的威脅無所不在，這些現象除了造成管理使用網路的困擾外，也對個人或是企業的資訊安全產生更大的風險與挑戰。

一、網路攻擊的類型

（一）攔截/中斷（interruption）：資料在網路傳輸過程中，被未授權的人中途擷取，無法傳送到目的地，影響資料的可用性。

（二）竊取/介入（interception）：資料在網路傳輸過程中，在未經授權的情況下，取得傳送的資料內容，影響資料的機密性。

（三）篡改（modification）：當系統資源被未經授權的人取得後，所儲存或傳輸的資料內容遭到修改，影響資料的完整性。

（四）假冒/偽造（fabrication）：未經授權的人假冒他人傳送資料，影響資料的確實性或驗證性。

二、網路攻擊的手法

（一）實體層：是 OSI 模型的最底層，規範纜線的規格、傳輸速度、電壓值等。

- 線路搭接：搭接網路線路進行封包或資訊的竊聽。

（二）資料連結層：在網路之間建立邏輯連結，並且在傳輸過程中處理流量控制及錯誤偵測。可以採用加密的技術，但須確認所使用的加密演算法要夠強，難以破解。例如：使用較理想的無線網路加密通信協定（如：以 WPA 或 WPA2 取代 WEP）以預防網路竊聽 。

- 封包監聽（Packet sniffing）

  如果網路傳輸時採用明文方式，攻擊者可以藉由網路監聽工具（如：Sniffer）來竊取機密資料。

（三）網路層：定義網路路由及定址功能，讓資料能夠在網路間傳遞。

- Source Route

  IP 封包的路由主要由路由器（Router）來決定，藉由 Source Route 可以讓傳送者指定 IP 封包的傳送路徑，此項攻擊是運用 Source Route 的功能進行來源 IP 的偽冒（IP Spoofing）。

（四）傳輸層：主要負責電腦整體的資料傳輸及控制。

- 分散式阻斷服務（Distributed Denial of Service, DDoS）攻擊

  ✧ DDoS 攻擊區分為基礎設施層（Layer 3 網路層和 4 傳輸

層）和應用程式層（Layer 6 展示層和 7 應用層）。

- ✧ 阻斷服務攻擊是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常用戶無法存取。
- ✧ 阻斷服務攻擊可能會癱瘓網路，讓使用者無法使用服務，或將服務等級調降，產生可用性的問題。可藉由防火牆來限制同一來源 IP 的連線數量。

（五）應用層：處理應用程式，提供使用者網路應用服務。

- Brute force Login

  駭客藉由猜測密碼來入侵應用系統。解決方案為設定有數次機會可輸入正確的密碼，超過後密碼被鎖定。

- SQL injection（SQL 資料隱碼攻擊）：
  - ✧ 通常影響非常嚴重，整個資料庫可能被讀取或修改，資料的機密性或完整性會被破壞。
  - ✧ 在輸入的字串之中夾帶 SQL 指令，在設計不良的程式當中，忽略了字元檢查。這些夾帶進去的惡意指令，就會被資料庫伺服器誤認為是正常的 SQL 指令而執行，因此遭到破壞或是入侵。

三、網路安全的防禦措施

（一）防火牆

- 防火牆是針對兩個或多個網路間，執行網路間存取或控制的一套硬體或軟體，主要功能可以管理與過濾通過網路的封包，保護企業內部網路，提升系統的安全性。
- 防火牆是首要的防衛機制，應該放置在所有網路的邊界位置，通常位於網際網路和企業網路之間。防火牆的類型主要有兩種：
  - ✧ 過濾型（Filtering）防火牆：可區分成網路層（Network Layer）防火牆和應用層（Application Layer）防火牆兩種。
  - ✧ 2.代理型（Proxy）防火牆。
- 網路層防火牆的一項主要技術是封包過濾（Packet Filtering），管理者依據組織的策略與需求設定好封包通過的規則（包含來源端和目的端），只允許符合規則的封包通過設備。
- 應用層防火牆可以檢查與攔截進出某應用程式的所有封包。較新的應用層防火牆可以針對應用程式（如 Web 應用程式）做深層的分析與保護，預防身分與資料的盜竊、應用程式的中斷與詐騙等針對性的攻擊。
- 代理（Proxy）伺服器可以代理 client 端執行網路資源的存

取（例：內部電腦存取外部網頁資源時），協助回應其所收到的封包來實現防火牆的功能，包含封鎖或拋棄其他的封包。代理的機制可以增加駭客從外部網路竄改內部系統的困難度。

- 在防火牆上制定的規則應受到嚴格的限制，並且設定所需主機（host-by-host）與服務（service-by-service）的規則，只允許必需的網路通信（Default Deny）。定期測試防火牆，以確保防火牆對來自外部與內部的資訊流量能夠發揮預期的作用。

（二）入侵偵測與防禦系統

- 入侵檢測系統（Intrusion Detection System, IDS）是一種積極主動式的網路安全防護裝置或應用軟體，可以監控網路傳輸或者系統，檢查是否有可疑活動或者違反企業的政策。偵測到時會發出警報或者採取主動反應措施。
- 入侵預防系統（Intrusion Prevention System, IPS）是一部電腦網路安全裝置，可以監視網路或裝置的資料傳輸行為，能夠即時的中斷、調整或隔離一些不正常或是具有傷害性的網路傳輸。

（三）防毒系統

- 所有連上公司的電腦必須安裝、使用標準及有支援的防毒

軟體；任何受病毒影響的電腦將從公司網路移開，直到驗證確認完成。

（四）垃圾郵件過濾系統

垃圾郵件（Spam email）為未經使用者同意，強行塞入信箱的電子郵件，使用垃圾郵件過濾器或反垃圾郵件的軟體可以減輕一些問題與負擔。

（五）電子郵件社交工程攻擊與防護

社交工程（Social engineering）是藉由與他人的合法交流，使其做出某些動作或者是透露一些機密資訊的方式，通常被認為是一種欺詐他人以收集個人資料，並進而做出其他惡意或非法的行為。

（六）釣魚式攻擊（Phishing）

是一種利用社交工程技術來欺騙使用者，或是進行未經授權的交易；一種企圖從電子通訊中，透過偽裝成信譽卓著的法人媒體以獲得如用戶名、密碼和信用卡明細等個人敏感資訊的犯罪詐騙過程。

模擬考題

（一）關於安全管控，下列何者較「不」安全？

(A) 定期檢視網路架構

(B) 定期針對重要設備進行設定檔備份

(C) 針對網路設備之存取不限制存取來源 IP

(D) 建立防火牆連線規則管理政策

- 答案：(C)
- 解析：針對網路設備之存取「宜」限制存取來源 IP。

（二）關於網路型入侵偵測系統（Network-based IDS），下列敘述何者正確？

(A) 安裝後對於網路流量的影響很大

(B) 只要安裝網路型入侵偵測系統即可以保護所有電腦不被入侵

(C) 資料來源是作業系統、應用程式或網路登入/登出紀錄（Log）

(D) 如果流量（Traffic）太高，可能會影響偵測攻擊準確度

- 答案：(D)
- 解析：如果流量（Traffic）太高，可能會影響偵測攻擊準確度。

（三）請問下列何者攻擊手法比較容易被採用來執行分散式服務阻斷（DDoS）攻擊？

(A) UDP 封包攻擊

(B) TCP 封包攻擊

(C) HTTP 封包攻擊

(D) SQL 封包攻擊

- 答案：(A)
- 解析：UDP（使用者資料報協定）是一種無連接協定，當封包通過 UDP 傳送時，所有的封包在傳送和接收時不需要進行握手驗證。當大量 UDP 封包傳送給受害系統時，可能會導致頻寬飽和從而使得合法服務無法請求存取受害系統。

（四）在網頁登入時，常常在帳號密碼輸入的欄位之下，還要求如下圖所示輸入其他驗證資訊，其請問此機制為下列何者？

(A) 詢問握手認證協議（Challenge-Handshake Authentication Protocol, CHAP）

(B) 晶片卡驗證（Smart Card Authentication）

(C) 全自動區分電腦和人類的公開圖靈測試（Completely Automated Public Turing test to tell Computers and Humans Apart, CAPTCHA）

(D) 簡訊服務驗證（SMS Authentication）

- 答案：(C)
- 解析：在 CAPTCHA 測試中，作為伺服器的電腦會自動生成一個問題由使用者來解答。這個問題可以由電腦生成並評判，但是必須只有人類才能解答。由於機器無法解答 CAPTCHA 的問題，回答出問題的使用者即可視為人類。

（五）關於網路位址轉換（Network address translation , NAT），下列敘述何者「不」正確？

(A) 可減少公有 IP（Public IP）位址使用數量

(B) 可隱藏內部 IP 位址

(C) 可防止暴力攻擊（Brute-Force Attack）

(D) 內部網路中, 使用私有 IP 位址（Private IP）

- 答案：(C)
- 解析：網路位址轉換不可防止暴力攻擊。

（六）下列 IP 地址何者是私有網路位址（Private IP）？

(A) 1.1.1.1

(B) 8.8.8.8

(C) 9.9.9.9

(D) 10.10.10.10

- 答案：(D)

- 解析：10.10.10.10 是私有網路位址。

（七）關於防火牆規則管理，下列敘述何者「不」正確？

(A) 安全性規則的數量會影響防火牆的效能

(B) 防火牆管理員應制定一套開放標準讓大家遵從，以避免每個人的管理模式不同，導致防火牆規則難管理

(C) 防火牆設定無需訂定管理辦法，只要管理員熟悉設備即可

(D) 防火牆開放方式最好使用白名單開放，較黑名單安全

- 答案：(C)
- 解析：防火牆設定需訂定管理辦法。

（八）關於狀態檢視防火牆，下列敘述何者「不」正確？

(A) 狀態檢視防火牆所看的內容較封包過濾防火牆少

(B) 狀態檢視防火牆可以根據目的埠號做阻擋

(C) 狀態檢視防火牆可以根據目的位址做阻擋

(D) 狀態檢視防火牆會紀錄連線狀態

- 答案：(A)
- 解析：狀態檢視防火牆所看的內容較封包過濾防火牆多。

（九）關於代理防火牆，下列敘述何者「不」正確？

(A) 使用者透過代理防火牆進入時，代理防火牆會開啟新連線，再將回覆回給使用者

(B) 駭客可能透過多層代理防火牆來隱匿其真實來源位址

(C) 代理防火牆設定上較複雜，需依照各種協定客製代理程式

(D) 代理防火牆運作於第四層網路層

- 答案：(D)
- 解析：應用層防火牆也稱為代理防火牆，這種防火牆在應用層運作，會檢查內部網路和流量來源之間的流量。

（十）請問下列何種攻擊方式的主要目的是為了讓使用者無法進行資料的存取？

(A) 中間人攻擊（Man-in-the-Middle Attack）

(B) SQL 資料隱碼攻擊（SQL Injection）

(C) 社交工程攻擊（Social Engineering）

(D) 阻斷服務攻擊（Denial-of-Service Attack）

- 答案：(D)
- 解析：阻斷服務攻擊的目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常使用者無法存取。

第二節　通訊安全

通訊安全的目標為保持資訊在組織內部，或是與任何外部組織在資訊通訊上的安全性。

一、管理和控制

組織對於網路應進行管理和控制，以保護系統和應用程式上的資訊：

（一）建立網路設備的管理責任及程序：藉由程序以管理所有的網路設備，例如，路由器、防火牆、VPN switches、無線設備等。

（二）定期執行弱點評估，確保符合網路的安全性原則。

（三）對連接至網路的系統宜設限：設備必須要經過驗證與授權，才能存取網路上的服務或資料。

（四）網路存取保護：用戶端電腦必須以所設定的安全狀態，才能連上企業網路。

二、網路管理系統

（一）網路管理系統 (Network Management System)是實施各項網路管理功能的軟體或硬體系統。依據管理的對象可區分為兩種類型：

- 通用型網路管理系統，可管理整個網路。

- 網路設備型管理系統，只管理單獨的設備，如交換機、路由器、伺服器等。

（二）網路管理系統中一個很重要的項目就是網路管理協議（Network Management Protocol），網路管理協議定義網路管理器（Network Manager）與被管代理（Managed Agents）間的通信方法，以及相對的儲存結構、處理方法等。

（三）目前應用最廣的網路管理協議是簡單網路管理協定（Simple Network Management Protocol, SNMP），能夠監測連接到網路上的裝置，是否有任何可能產生管理上關注的情況。

三、通訊安全的控制措施與技術

（一）妥善保護所傳送的資訊，防範被截取、複製、修改、破壞，不論使用何種類型的通信設施或管道，都能保護資訊的傳遞。

（二）藉由加密技術的使用來保護資訊安全，特別針對機密資訊或敏感性個人資料等透過 internet 傳輸時，必須使用安全的機制。

（三）藉由資訊轉移的政策、程序和控制措施，不論使用何種類型的通信設施，都能保護資訊的傳遞。

（四）虛擬私人網路（Virtual Private Network, VPN）

- VPN 用戶端使用通道通訊協定（Tunneling Protocol）的特殊 TCP/IP 通訊協定，在兩部電腦之間建立用來傳送資料

的安全通道，沒有加密的 VPN 訊息依然有被竊取的危險。

- 常用的 VPN 協定有：資料連結層的加密通訊協定（Layer-2 Forwarding, L2F）、資料鏈結層（Layer 2 Tunneling Protocol, L2TP）、點對點通道通訊協定（Point to Point Tunneling Protocol, PPTP）、網際網路安全協定（Internet Protocol Security, IPsec）、傳輸層安全性協定（Transport Layer Security, TLS）、安全通訊端層（Secure Sockets Layer, SSL）。

（五）電子簽章與數位簽章

- 數位簽章

  指將電子文件以數學演算法或其他方式，運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證。數位簽章可提供不可否認性及訊息完整性。

- 電子簽章

  指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。電子簽章所涵蓋的範圍較廣，除了數位簽章之外，其他如指紋、人臉、視網膜、聲紋、簽名筆跡等，能夠辨識使用者的資料都可包含在內。

- 憑證

  指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。

模擬考題

（一）請問 TCP/IP 通訊協定中之應用層是合併 OSI 參考模型的哪幾層？

(A) 應用層、傳輸層、網路層

(B) 應用層、表達層、會議層

(C) 應用層、傳輸層、會議層

(D) 應用層、表達層、網路層

- 答案：(B)
- 解析：TCP/IP 通訊協定中之應用層是合併 OSI 應用層、表達層、會議層。

（二）下列何種應用服務會使用到 TCP 和 UDP 二種傳輸層協定？

(A) FTP

(B) SMTP

(C) Telnet

(D) DNS

- 答案：(D)
- 解析：DNS 使用到 TCP 和 UDP 二種傳輸層協定。

（三）交換器在何種情況下會將一個訊框（Frame）溢送（Flood）到所有交換器的端口？

(A) 當來源的 MAC 位址並未在交換器的 MAC 位址表格內

(B) 當目的的 MAC 位址並未在交換器的 MAC 位址表格內

(C) 當目的的 MAC 位址是多點傳送（Multicast）位址

(D) 當目的的 MAC 位址是 00-00-00-00-00-00

- 答案：(B)
- 解析：當目的的 MAC 位址並未在交換器的 MAC 位址表格內。

(四)「虛擬私有網路(VPN)」是利用什麼技術來建立安全通訊連線？

(A) 通道（Tunnel）技術

(B) 資料壓縮技術

(C) 調變與解調變技術

(D) 無線通訊技術

- 答案：(A)
- 解析：VPN 用戶端使用通道通訊協定(Tunneling Protocol)的特殊 TCP/IP 通訊協定，在兩部電腦之間建立用來傳送資料的安全通道。

(五) 下列哪一層的協定，負責在 TCP/IP 通訊協定中，提供定址與路由之任務？

(A) 應用層

(B) 表達層

(C) 傳輸層

(D) 網路層

- 答案：(D)
- 解析：網路層負責在 TCP/IP 通訊協定中，提供定址與路

由之任務。

（六）TCP/IP 通訊協定中稱為網路介面層，負責與硬體溝通的是下列何者？

(A) 應用層（Application Layer）

(B) 傳輸層（Transport Layer）

(C) 連結層（Link Layer）

(D) 網路層（Network Layer）

- 答案：(C)
- 解析：連結層負責與硬體溝通。

（七）關於 TCP 三項交握流程，下列敘述何者「不」正確？

(A) 第一步驟 Client 先發 SYN 給 Server

(B) 第二步驟 Server 回給 Client SYN+ACK

(C) 第三步驟 Client 再回 SYN 給 Server，之後連線建立

(D) TCP 三項交握僅有 TCP 會使用，UDP 並無交握流程

- 答案：(C)
- 解析：第三步驟 Client 再回 ACK 給 Server，之後連線建立。

（八）關於 TCP 連接狀態，下列敘述何者「不」正確？

(A) SYN-SENT：Client 送往 Server 的第一個要求連線封包(已送出 SYN，在等待對方回覆的期間）

(B) SYN-RECEIVED：Server 收到 Client 的連線後，回覆給

Client SYN+ACK，並且等待 Client 回覆 ACK

(C) ESTABLISHED：Client 回覆 ACK 後，Client 及 Server 均進入 Established 狀態，雙方可以正常傳輸，TCP 三項交握已完成

(D) CLOSE-WAIT：被動關閉方收到 FIN 後發出 SYN+ACK 時，會進入這個狀態，此時可以傳輸資料，也可以接收資料

- 答案：(D)
- 解析：等待從本地使用者發來的連線中斷請求，被動關閉端 TCP 接到 FIN 後，就發出 ACK 以迴應 FIN 請求（它的接收也作為檔案結束符傳遞給上層應用程式），並進入 CLOSE_WAIT。

（九）關於 SSL 與 TLS，下列敘述何者較「不」正確？

(A) TLS 是 SSL 的後續版本

(B) 兩者都是加密協議，用於從客戶端到伺服器、電腦或應用程式數據傳輸的加密和驗證

(C) HTTPS 結合了處理資料傳輸的 HTTP 和處理資料加密的 SSL/TLS

(D) TLS 3.0 是目前資料進行傳輸過程中，大多數設備和瀏覽器所支援的

- 答案：(D)
- 解析：目前最新版本為 TSL 1.3，而 TLS 1.2 是目前資料進行傳輸過程中，大多數設備和瀏覽器所支援的。

（十）關於 IPSec，下列敘述何者較「不」正確？

(A) IPSec 是 IP Security 的縮寫，是運用在網路層的保護機制

(B) IPSec 提供資料加密（Data Confidentiality）、資料完整性（Data Integrity）、以及身份認證（Authentication）

(C) IPSec 將整個封包（IP 標頭和資料本身）進行加密保護

(D) IPSec 重新封裝後的封包可以正確的在既有網路上傳送，不會因為標頭被更改而受到影響

- 答案：(C)
- 解析：IPSec 只對資料本身（Payload）進行加密保護

第五章. 作業系統與應用程式安全

第一節　作業系統安全

一、主機作業系統的資訊安全

（一）主機包含資料中心的伺服器、與使用者所使用的電腦設備等。主要功用是啟動最少的功能來配置作業系統，移除所有不必要的服務、功能及介面。

（二）針對所有主機實施相關保護措施，例如：防毒軟體、作業系統修正程式（Patch）的管理等，宜使用集中配置與變更管理的方式來發佈所有的保護軟體。

- 修正程式（Patch）的管理
  - ✧ 及時或定期地套用所有相關的資訊安全修正程式及重大的更新，包含 clients 與 servers。
  - ✧ 使用集中式管理方式進行修正程式的部署。
  - ✧ 對於已經不再提供資訊安全修正程式支援的舊系統或應用程式的電腦，考量從網路隔離的可行性。

（三）使用者的管理：建立正式的使用者註冊與取消註冊程序，做為存取權限的分配。為需要存取 IT 資源的所有人員建立個人使用者帳戶，方法如下：

- 使用獨立唯一的帳號，將使用者對網路存取的活動連結起

來。

- 建議部署使用者帳號與密碼的集中式管理機制。
- 集中式使用者的管理機制中，輕量型目錄存取協定（Lightweight Directory Access Protocol, LDAP）是一項很重要的技術，提供集中式使用者管理的產品包含有：
  - ✧ Windows Server Active Directory
  - ✧ Network Information Service, NIS
  - ✧ OpenLDAP
  - ✧ Amazon Cloud Directory
- 在預設情況下，為建立的帳戶啟用所需的最低權限，使用者應負責維護他們的認證資訊。

（四）對運作中系統軟體的更新或安裝，應訂定適當的流程予以控制。運作中軟體、應用程式及程式館有可能需要更新或變更，以修正軟體的安全性問題、改正程式的錯誤或新增軟體的功能。更新工作宜由受過訓練的管理者，於獲得管理階層的授權後，才能執行。

（五）實施變更前，應準備好還原（rollback）策略，宜保留應用軟體的先前版本，以作為應變措施。

二、電腦中儲存媒體與檔案的保護

（一）對於可移除設備的使用宜予以管理、限制或監控，例如：

- 對可移除設備內檔案的加密
- 限制可移除設備的使用，例如：USB 隨身碟等
  - ✧ 如果組織要大量部署，統一設定所有的電腦，可以使用 Windows AD 的群組原則進行控管，或使用能夠控管周邊裝置存取的專用軟體。
  - ✧ 如果是個別電腦的控管，則可使用 Windows 作業系統中的本機群組原則。
  - ✧ 如對象是訪客，則可以在 USB 埠貼上警語貼紙暫時停用。
- 週邊設備網路 ports 的封鎖，包含 Bluetooth、i1394、IrDA（紅外線傳輸）等。
- 燒錄 CDs/DVDs 使用的控管與限制。
- Disable 電腦媒體的 autorun，如：CDs、DVDs 及 flash。

（二）建立資料外洩的管理計畫，並有效實施下列事項：

- 制訂事故處理程序，確保有正確與即時的處理。
- 依據法規要求或內部程序，對資料外洩事件作通報。萬一發生資訊安全事件時，應採取正確的行動，例如：立即記錄所有重要的細節、不自己執行任何行動，但立即通報聯絡點。

- 進行外洩狀況與營運衝擊的評估，視需要採取措施避免資料繼續外洩，並針對問題追蹤、分析及解決。
  - ✧ 觀察問題的症狀：問題重現。
  - ✧ 執行根本原因的分析：視需要收集並保全稽核存底及類似的證據，以備分析或提供為法律證據等。
  - ✧ 進行假設並進行驗證或測試。
  - ✧ 解決問題。
  - ✧ 預測未來的問題。
- 界定職責：成立事故回應小組。
- 資料外洩的通知。
- 識別事故的嚴重性，並確定所需採取的措施與程序。
- 定期的測試或演練（至少每年一次）。

模擬考題

（一）下列何者「不」屬於作業系統主要的功能？

(A) 做為使用者之介面

(B) 分配與管理系統資源

(C) 提供系統服務與保護

(D) 提供影像處理服務

- 答案：(D)
- 解析：影像處理服務不屬於一般作業系統應具之主要功能。

（二）關於 EternalBlue 弱點，請問是基於下列何者機制所產生的？

(A) Windows SMB

(B) Widdows Kerberos

(C) Windows RDP

(D) Windows UAC

- 答案：(A)
- 解析：EternalBlue 弱點利用 Windows SMB 所產生。

（三）下列何者「不」是 UTM（Unified Threat Management）整合式威脅管理設備的常見功能？

(A) 啟用 IPS(Intrusion Prevention System)入侵偵測防禦功能，防禦異常的網路攻擊封包

(B) 管理外網與內網的各子網段交換路由

(C) 以 IPSec 通訊協定建立加密傳輸路由

(D) 使用 Honeypot 誘捕系統功能來蒐集與分析入侵威脅

- 答案：(D)
- 解析：UTM（Unified Threat Management）整合式威脅管理不包含設立 Honeypot。

（四）下列何項新廠區的網路規劃「不」屬於資安考量？

(A) 安裝 3 台接取網路交換器並設定 3 個 VLANs 且分為 3 個子網段（subnet）供不同部門使用

(B) 使用 VPN 閘道器建立總廠與新廠的安全傳輸網路

(C) 在新生產線佈署工規交換器，並且設定獨立的 VLAN 與子網段連接 SCADA（Supervisory Control and Data Acquisition）自動化生產與控制系統設備

(D) 建置網路路由器提供網路流量交換

- 答案：(D)
- 解析：建置網路路由器提供網路流量交換不屬於資安考量。

（五）下列敘述何者「不」正確？

(A) 木馬後門程式常偽裝成提供便利或實用的免費軟體,吸引使用者下載使用

(B) 電腦病毒具有散播、隱藏、感染、潛伏及破壞等特性

(C) 阻絕服務攻擊（DoS）通常指攻擊者攔截通訊的資料，並讓資料最後傳送到錯誤的接收者

(D) 蠕蟲（Worm）會不斷複製，並利用網路感染其他主機

- 答案：(C)
- 解析：阻斷服務攻擊是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常用戶無法存取。

（六）請問 cat ~/.bash_history 指令，是要執行下列何種功能？

(A) 列出系統使用者

(B) 列出使用者曾經下過的指令

(C) 列出系統目錄

(D) 列出系統內的檔案

- 答案：(B)
- 解析：cat ~/.bash_history 指令執行下列列出使用者曾經下過的指令。

（七）請問下列何者「不」屬於預防（Preventive）性機制的安全管控機制？

(A) 實施強制性密碼原則管理

(B) 安裝防毒軟體並啟動即時偵測

(C) 定期檢視安全記錄檔（Log）

(D) 定期套用安全性更新（Patch）

- 答案：(C)
- 解析：定期檢視安全記錄檔不屬於預防（Preventive）性機制的安全管控機制。

（八）若要安全傳送資料，達到只有接收方能開啟並確認內容未遭篡改，下列敘述何者正確？

(A) 資料以雜湊（Hash）演算後，以接收方的公開金鑰（Public Key）加密後傳送

(B) 資料以雜湊（Hash）演算後，以傳送者的公開金鑰（Public Key）加密後傳送

(C) 資料以雜湊（Hash）演算後，以接收方的私密金鑰（Private Key）加密後傳送

(D) 資料以雜湊（Hash）演算後，以傳送者的私密金鑰（Private Key）加密後傳送

- 答案：(A)
- 解析：資料以雜湊（Hash）演算後，以接收方的公開金鑰（Public Key）加密後傳送。

（九）應用程式執行特定作業結束後，並沒有通知作業系統，故無法向作業系統要求釋放記憶體空間，此狀況稱為下列何者？

(A) 記憶體暫存（Memory Register）

(B) 記憶體注入（Memory Injection）

(C) 記憶體映像（Memory Mapping）

(D) 記憶體洩漏（Memory Leaks）

- 答案：(D)
- 解析：記憶體洩漏將應用程式執行特定作業結束後，並沒有通知作業系統，故無法向作業系統要求釋放記憶體空間。

（十）關於 UAC（User Account Control），下列敘述何者「不」正確？

(A) 保護或提醒管理員用戶免受軟體組件執行的惡意提權行為

(B) 系統管理員通常會以最大的使用者權限執行

(C) 通過限制應用軟體對系統層級的存取，從而改進 Windows 作業系統的安全性

(D) 設計概念為消除不必要的提高許可權

- 答案：(B)
- 解析：系統管理員通常會以最小的使用者權限執行。

第二節　作業系統與應用程式(含資料庫與網頁)攻擊手法

一、作業系統與應用程式的攻擊手法

（一）緩衝區溢位（Buffer overflow）

- 是針對程式設計缺陷，大量寫入程式輸入緩衝區導致溢位的內容(通常是超過緩衝區能儲存的資料量)，從而破壞程式執行、趁著中斷之際取得程式乃至系統的控制權。

（二）後門程式

- 後門程式會繞過電腦系統的正常安全控管方法，以比較隱秘的管道取得對程式或系統存取權。管理維護用的後門程式是在軟體開發時，設定後門可以方便日後軟體的管理、維護、修改，以及測試程式中的缺陷。
- 另有被惡意植入的後門程式，這些後門程式大多數是藉由類似病毒感染的方式傳遞,像是夾帶在電子郵件或軟體中，當你存取所接收或分享的電子郵件或軟體時，後門程式就被觸發而啟動。這種惡意的後門程式可能會竊取使用者的密碼或個人資料、控制主機的開/關機、刪除檔案、或從遠端遙控或監視使用者的螢幕或鍵盤等。

（三）勒索軟體（Ransomware）

- 勒索軟體是一種惡意軟體,近年來對全球產生重大的影響，有可能以病毒、蠕蟲或木馬等形式來啟動攻擊。攻擊方式

可能會將受害者的電腦鎖起來，或是將受害者硬碟上的檔案加密。勒索軟體通常會要求受害者繳納贖金以取回對電腦的控制權，或是取回受害者根本無從自行取得的解密金鑰以便解密檔案。

（四）邏輯炸彈（Logic bomb）

- 是一些嵌入在正常軟體中並在特定情況下執行的惡意程式碼，會在特定時間或狀況爆發。這些特定情況可能是更改檔案、 特別的程式輸入序列、或是特定的時間或日期。惡意程式碼可能會將檔案刪除、使電腦主機當機、或是造成其他的損害。

（五）殭屍網路（Botnet）

- 駭客利用分散式阻斷服務攻擊程式，將數萬個淪陷的機器組織成一個個的命令與控制節點，用來傳送偽造或垃圾封包，使預定的攻擊目標癱瘓，形成「阻斷服務」。

（六）Rootkit

- Rootkit 一詞最早出現在 Unix 系統上，系統入侵者為了取得系統管理員級的 root 權限，或者為了清除被系統記錄的入侵痕跡，會重新組譯一些軟體工具（術語稱為 kit），如 ps、netstat、w、passwd 等。其後類似的入侵技術或概念在其他的作業系統上也被發展出來，主要是檔案、處理程序、

系統記錄的隱藏技術，以及網路封包、鍵盤輸入的攔截竊聽技術等，許多木馬程式都使用了這些技術，因此木馬程式也可視為 Rootkit 的一種。

二、OWASP 2021 十大 Web 應用程式安全性風險

（一）權限控制失效（Broken Access Control）

- 未對通過身分驗證的使用者，實施適當的存取控制，攻擊者可以利用這些缺陷，存取未經授權的功能或資料，例如：存取其他使用者的帳戶、查閱敏感性的資料檔案、修改其他使用者的資料、變更存取權限等。
- 預防：為了保護應用程式免受駭客攻擊訪問，企業應預設拒絕訪問功能並設定身份驗證。

（二）加密機制失效（Cryptographic Failures）

- 主要跟加密的錯誤或是缺少加密，導致機敏資料外洩，包含寫死密碼，損壞或有風險的加密算法及熵不足。
- 預防：因手動加密在現在複雜的解密工具面前往往很弱，所以防止加密機制失效的最佳方法是使用受信任的加密解決方案。

（三）注入式攻擊（Injection）

- 將不受信任的資料作為命令或查詢的一部分發送到解析器

（interpreter）時，會產生如 SQL Injection、OS Injection 或 LDAP Injection 等缺陷。攻擊者的惡意資料，可以誘使解析器在沒有適當授權的情況下，執行非預期命令或存取資料。

- 預防：為防止注入式攻擊，軟體開發人員應取消用戶提供的密碼輸入，並用行動 OTP（政府系統，銀行皆已廣泛使用）、生物識別身份驗證、下拉式選項和使用第三方支付平台來取代。

（四）不安全設計（Insecure Design）

- 不安全設計定義了與應用程式設計缺陷相關的風險，不一定是設計錯誤，而只是有心人士可利用了能造成損害的漏洞。如：網站允許前 100 名獨立訪問者獲得折扣，但有心人士卻使用不同的 IP 位置購買多種打折產品並轉售以獲取收益。
- 預防：建議軟體開發人員使用安全的設計模組和參考架構來構建應用程式。

（五）安全設定缺陷（Security Misconfiguration）

- 安全設定缺陷最常見原因是系統管理員沒有更改預設配置，或者他們在打開系統進行測試後忘記重新關閉系統。
- 預防：為了防止安全設定缺陷，企業應禁用所有預設的不必要功能、特權和權限，並僅開放給特定對象使用。

（六）危險或過舊的元件（Vulnerable and Outdated Components）

- 危險或過舊的元件是指網路中的元件包含了未修補已知漏洞的情況，通常是過時且不受支援的操作系統、應用程式、Web 應用程式伺服器、API 和數據庫管理系統（DBMS）。
- 預防：消除危險或過舊元件的最佳方法是定期掃描漏洞並保持更新和修補所有軟體元件。

（七）認證及驗證機制失效（Identification and Authentication Failures）

- 目前越來越多企業組織採用多因素身份驗證（MFA）以及行動 OTP 和生物識別等高級身份驗證技術，這些技術都有助防禦社交攻擊、憑證填充和蠻力攻擊，因此目前此現象因此獲得改善。
- 預防：在無法補救前，建議企業組織採用多因素身份驗證 MFA，謝絕非法使用者進入大門。

（八）軟體及資料完整性失效（Software and Data Integrity Failures）

- 軟體及資料完整性失效是由於缺乏資料完整性驗證過程而使用篡改或損壞的資料做出某些決定的狀況。例如，駭客使用惡意軟體去破壞軟體更新文件，而應用程式會自動安裝更新，而無需驗證文件是否為原始文件。
- 預防：為了防止資料損壞，建議使用 PKI 憑證的驗證機制來確定資料的真實性和完整性。

（九）資安記錄及監控失效（Security Logging and Monitoring Failures）

- 資安記錄及監控失效描述了入侵監控和 report 系統未能捕獲和寫入駭客入侵的跡象，可能是因為某些資安事件未記錄或日誌僅存儲在本地，或者警報值不足。
- 預防：為了防止資安記錄及監控不充分，資安管理員必須確認所有失敗的登錄嘗試和伺服器端輸入驗證都被立即記錄和警示。

（十）伺服端請求偽造（Server-Side Request Forgery, SSRF）

- 當網頁應用程式正在取得遠端資源，卻未驗證由使用者提供的網址，此時就會發生偽造伺服端請求。即便有防火牆、VPN 或其他網路 ACL 保護的情況下，攻擊者仍得以強迫網頁應用程式發送一個經過捏造的請求給一個非預期的目的端。這些損壞的請求可能會導致數據洩露。隨著雲端服務和雲端結構的複雜性，SSRF 攻擊的嚴重性將會愈來愈嚴峻。
- 預防：防止 SSRF 的最佳方法是配置網路訪問控制策略，實施預設「阻止所有外部流量」，在應用上建議為用戶端提供的資料設置白名單允許列表。

模擬考題

（一）黑帽駭客（Black Hats）是指惡意攻擊電腦系統及網路的人，下列何者「不」是其行為？

(A) 誘騙使用者上當並植入木馬程式

(B) 利用電腦裝置的漏洞進行入侵

(C) 通知網站客戶該網站有漏洞

(D) 釣魚式攻擊

- 答案：(C)
- 解析：通知網站客戶該網站有漏洞，不屬於惡意攻擊電腦系統及網路。

（二）規劃縱深防禦（Defense in Depth）時，我們常會採用多種不同面向的管控措施（Controls），下列何者屬於偵測手段（Deter）？

(A) 防火牆（Firewall）

(B) 入侵偵測防禦系統（IDS/IPS）

(C) 病毒與垃圾郵件過濾閘道系統

(D) 虛擬私有網路（VPN）

- 答案：(B)
- 解析：入侵檢測系統（Intrusion Detection System, IDS）是一種積極主動式的網路安全防護裝置或應用軟體，可以監控網路傳輸或者系統，檢查是否有可疑活動或者違反企業的政策。

（三）根據 Open Web Applications Security Project（OWASP）研究報告所指出網頁十大安全性弱點利用與攻擊中，為了防範常見的跨網站指令碼（Cross-Site Scripting, XSS）攻擊、注入式缺陷（Injection Flaw）攻擊和跨網站請求偽造（Cross-Site Request Forgery, CSRF）等攻擊，您應採用下列何種策略？

(A) 整個網站均採用 TLS 傳輸

(B) 採用嚴謹的驗證方式

(C) 網頁程式中需做好輸入檢查工作

(D) 實施端點安全性檢查

- 答案：(C)
- 解析：網頁程式中需做好輸入檢查工作可防止跨網站指令碼（Cross-Site Scripting, XSS）攻擊、注入式缺陷（Injection Flaw）攻擊和跨網站請求偽造（Cross-Site Request Forgery, CSRF）等攻擊。

（四）使用者瀏覽網頁時，執行攻擊者插入到網頁中 HTML 或 Script 的指令，此為遭受到什麼攻擊？

(A) 資料隱碼攻擊（SQL injection）

(B) 跨網站腳本攻擊（Cross-Site Scripting, XSS）

(C) 跨站請求偽照（Cross-Site Request Forgery, CSRF）

(D) 搜尋引擎攻擊（Google Hacking）

- 答案：(B)
- 解析：跨網站指令碼（英語：Cross-site scripting，通常簡稱為：XSS）是一種網站應用程式的安全漏洞攻擊，是代

碼注入的一種。它允許惡意使用者將程式碼注入到網頁上，其他使用者在觀看網頁時就會受到影響。

（五）對於防禦資料隱碼攻擊（SQL Injection），下列何著較「無」效果？

(A) 使用參數化語句

(B) 強化對輸入值的驗證

(C) 使用單一登入（Single sign-on），避免帳戶太多難以管理

(D) 區分資料庫使用者的用戶權限

- 答案：(C)
- 解析：使用單一登入對於防禦資料隱碼攻擊（SQL Injection）較無效果。

（六）請問，入侵步驟中的「提權（Privilege Escalation）」是指下列何者？

(A) 提升使用者權限至系統管理權限

(B) 刪除入侵軌跡

(C) 刪除使用者帳號

(D) 找出具有最高權限的帳號

- 答案：(A)
- 解析：提權（Privilege Escalation）指提升使用者權限至系統管理權限。

（七）請問下列何者是密碼潑灑（Password Spraying）攻擊？

(A) 蒐集常用的密碼，放入字典，嘗試登入系統

(B) 用單一弱密碼，嘗試登入系統

(C) 使用已外洩的帳號與密碼的各種組合，嘗試登入系統

(D) 使用可能各種密碼組合，嘗試登入系統

- 答案：(B)
- 解析：密碼潑灑（Password Spraying）攻擊指用單一弱密碼，嘗試登入系統

（八）關於 IP Spoofing，下列敘述何者最為正確？

(A) 利用資料庫弱點冒用他人 IP

(B) 透過變造封包等手法，以偽冒他人的 IP

(C) 因為 IP 重複，導致系統錯誤

(D) 利用 IP 清單避免使用者遭受攻擊

- 答案：(B)
- 解析：在電腦網路裡面，IP 位址欺騙或 IP 欺騙是指帶有假的源 IP 位址的 IP 協議分組（數據報），目的是冒充另一個計算系統身份。

（九）關於 SYN Flood，下列敘述何者最為正確？

(A) 大量送出 SYN 封包至目標

(B) 收到 SYN 封包後不回應

(C) 由於目標持續等待 SYN 封包導致資源耗盡

(D) 在 SYN 封包中帶入惡意指令進行攻擊

- 答案：(A)
- 解析：SYN flood 或稱 SYN 洪水、SYN 洪泛是一種阻斷

服務攻擊，起因於攻擊者傳送大量的 SYN 請求到目標系統。

（十）下列何者是被 SQL 資料隱碼攻擊（SQL Injection）成功的原因？

(A) 作業系統漏洞未即時更新修補程式（Patch）

(B) 未對使用者的輸入資料進行過濾與檢查

(C) 資料庫存取權限設定錯誤

(D) 遭受大量網路流量攻擊

- 答案：(B)
- 解析：未對使用者的輸入資料進行過濾與檢查易造成 SQL 資料隱碼攻擊（SQL Injection）。

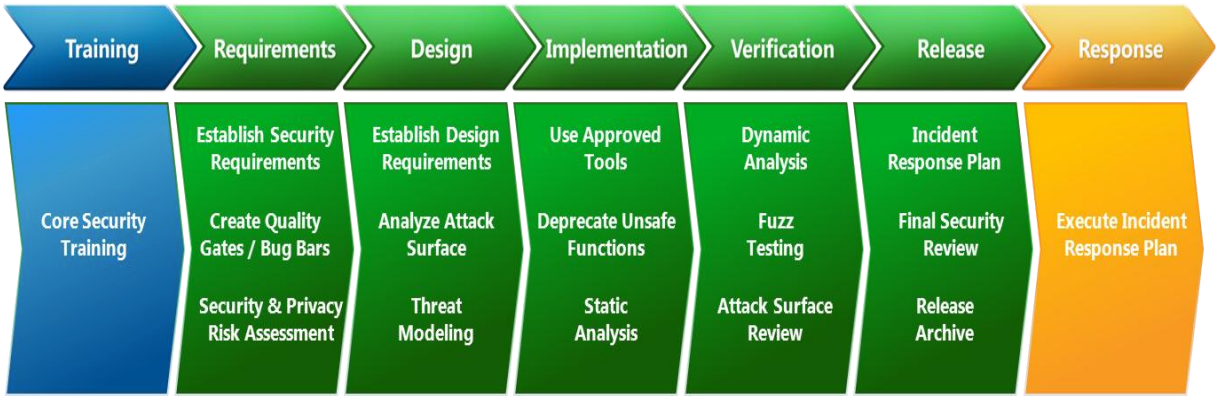
第三節　程式與開發安全

一、安全軟體開發生命週期簡介

軟體開發的生命週期中，參考所使用軟體開發方法論的安全指引，以及程式語言中有關安全性的指導綱要，以確保資訊系統的資訊安全，在開發的生命週期內被設計與實現；安全軟體開發相關的國際標準和方法論如下：

（一）ISO/IEC 27034-是專門針對開發軟體安全性所需流程與框架的國際標準。

（二）安全開發生命週期（Microsoft Security Development Lifecycle）



(圖片來源：Microsoft)

- 訓練階段
  - ✧ 基本軟體安全訓練應涵蓋的基礎概念包括：安全設計、威脅模型、安全測試和隱私權等。
- 要求階段
  - ✧ 針對計畫在運行環境中執行的應用程式，確定其安全和隱私的最低可接受級別。

- ✧ 安全風險評估和隱私風險評估。

- 設計階段
  - ✧ 設計要求：在設計階段應仔細考慮安全和隱私問題。
  - ✧ 減小攻擊面：減小攻擊面包括關閉或限制對系統服務的存取、應用最小許可權原則以及盡可能進行分層防禦。
- 實施階段
  - ✧ 使用核准評估過的開發工具。
  - ✧ 禁止使用不安全的函數和 API。
- 驗證階段
  - ✧ 為確保程式功能按照設計方式工作，有必要對軟體程式進行運行時驗證。
  - ✧ 模糊測試（Fuzz Testing）：故意向應用程式輸入錯誤格式或混亂的資料，檢驗是否會引起程式的故障。
  - ✧ 威脅模型和攻擊面評析：在給定應用程式完成編碼後重新評析其威脅模型和攻擊面。
- 發行階段
  - ✧ 每個軟體發行都必須包含事件回應計畫，即使在發行時不包含任何已知漏洞的程式也可能面臨日後新出現的威脅。
  - ✧ 最終安全評析：在發行之前仔細檢查對軟體應用程式執行的所有安全活動。

二、應用程式的安全控制

組織應建立並維護安全的開發環境（Secure development environment），包括與系統開發與整合相關聯之人員、流程與技術。

（一）建立安全的開發環境可考量下列事項：

- 不同開發環境間隔離的需要。
- 對開發環境之進出及存取的控制措施。
- 環境內工作人員之可信賴性。
- 適用之外部及內部要求事項，例如：法規或政策。

（二）應用程式的品質與安全檢測

- 安全的應用程式開發與規劃能大幅減少駭客的攻擊。
- 在資訊系統的開發或實作前，也就是在專案的需求階段，宜識別並議定所有的安全要求。
- 對每個系統的取得或開發專案，可以指派一位資訊安全的專家或代表參與專案。

（三）適用之外部（如法規）及內部（如政策）之要求事項

- 應用程式對個資的儲存應符合個人資料保護法的要求屬之。
- 個資的儲存以達到企業目的所需最短的時間為準
- 如果個資以隱藏的方式儲存（如 Cookie），使用者對資料的儲存或分享，有適當的控制權，同時需讓使用者瞭解 Cookie。
- 典型應用：是當登入一個網站時，如果使用者勾選「下次

自動登入」，代表使用者名稱和密碼會儲存在用戶端上的Cookie（檔案型式）中。若以 Persistent Cookie 型式儲存個資時，應將個資予以加密（使用者關閉瀏覽器不會被清除掉，會繼續留在使用者的電腦裡）。

（四）安全功能的測試，應該在取得或開發過程中進行。驗證資訊安全的保護措施與機制，可以依照預期運行，可以協助組織與使用者控制資料的外洩。

（五）對於組織內部的開發，這些測試一開始由開發小組負責，後續則進行獨立的驗收測試，以確保系統如預期的運作。

（六）「變更控制」應採用正式的變更控制程序，來控制開發生命週期內之系統的變更，可以確保系統、應用程式及產品的完整性，包含從初期的設計階段到後續的維護工作。而新系統的引進或對既有系統的重大變更，宜遵循相關程序，確保不會危及既有之安全控制措施與程序。

（七）當作業平台改變，關鍵業務應用程式宜進行審查和測試，以確保沒有對組織的運作和安全產生負面的影響。作業平台包含作業系統平台、資料庫平台、以及中介軟體平台等。如果要將既有應用程式的作業平台改變，應對應用程式控制與完整性程序做審查，確保其未被作業平台變更所破壞。

（八）一般不鼓勵修改軟體套件，對軟體套件的修改應限於必要的變

更，所有的變更都應嚴格控制。在 Service Pack 或新版本的發行中，可能會將安全性的修復與許多與安全性無關的其他軟體更新混淆在一起，這個目的是為了使逆向工程（Reverse Engineering）變得更加困難，讓駭客更難破解應用程式。

- 逆向工程：又稱反向工程，是一種技術流程，即對一產品進行逆向分析及研究，從而演繹並得出該產品的處理流程、組織結構、功能及效能規格等設計要素。逆向工程可能會被誤認為是對智慧財產權的嚴重侵害，但是在實際應用上，反而可能會保護智慧財產權所有者。

三、委外作業的資訊安全要求

資訊系統不論是自行開發或是委外取得，資訊安全的要求或標準應該要一致。組織應監督與監察委外的系統開發活動，將資訊安全的要求與控制，加入委外專案的需求中。

（一）系統開發委外時，宜考量下列事項：

- 與委外相關之使用授權的安排、程式碼所有權、智慧財產權等。
- 對交付產品之品質及準確性進行驗收測試。
- 組織仍然應遵守適用之法律的責任，並有效控制與查證。

模擬考題

（一）下列何者「不」是 Source Code Review 軟體？

(A) FortifySCA

(B) Checkmarx

(C) BurpSuite

(D) SonarQube

- 答案：(C)
- 解析：Burp 或 Burp Suite 是一個用於測試網絡應用程式安全性的圖形化工具。

（二）在軟體安全測試方法中，關於黑箱測試，下列敘述何者正確？

(A) 更容易鑑別出軟體問題的根因。

(B) 更容易發現邏輯性缺失。

(C) 更容易鑑別出軟體部署後的問題。

(D) 可測試程式碼涵蓋範圍更大。

- 答案：(C)
- 解析：黑箱測試更容易鑑別出軟體部署後的問題。

（三）某網站在設計時進行過安全分析，也在開發時要求程序員編寫安全的代碼，但佈署時由於管理員將備份存放在 WEB 目錄下導致了攻擊者可直接下載備份，為了發現系統中是否存在其他類似問題，下列何種測試方式是最佳的測試方法？

(A) 模糊測試

(B) 源碼測試

(C) 整合測試

(D) 滲透測試

- 答案：(D)
- 解析：滲透測試，是為了證明網路防禦按照預期計劃正常執行而提供的一種機制。

（四）全自動區分電腦和人類的公開圖靈測試（CAPTCHA），較能防護下列何種攻擊？

(A) 資料隱碼攻擊（SQL Injection）

(B) 跨網站偽造請求（Cross-Site Request Forgery, CSRF）

(C) 跨站腳本攻擊（Cross-Site Scripting, XSS）

(D) 緩衝區溢位（Buffer Overflow）

- 答案：(B)
- 解析：全自動區分電腦和人類的公開圖靈測試（CAPTCHA）可防禦跨網站偽造請求（Cross-Site Request Forgery, CSRF）。

（五）若程式在源碼檢測時，發現存在可能遭受到有心人士的中間人攻擊（Man-in-the-Middle, MiTM）的漏洞，下列何者是此程式最可能的主要問題？

(A) 無稽核（Lack of Auditing）

(B) 無憑證檢查（Lack of Certificate Verification）

(C) 無邊界檢查（Lack of Boundary Check)

(D) 無輸入驗證（Lack of Input Validation）

- 答案：(B)
- 解析：無憑證檢查可能遭受到有心人士的中間人攻擊（Man-in-the-Middle, MiTM）的漏洞。

（六）請問針對跨站請求偽造（Cross-Site Request Forgery, CSRF）攻擊，下列何種防禦方式最有效？

(A) 輸入參數黑名單過濾（Black List）

(B) 輸入參數白名單過濾（White List）

(C) 輸入參數長度過濾（Length Filter）

(D) 使用全自動區分電腦和人類的公開圖靈測試（CAPTCHA）

- 答案：(D)
- 解析：全自動區分電腦和人類的公開圖靈測試（CAPTCHA）可防禦跨網站偽造請求（Cross-Site Request Forgery, CSRF）。

（七）下列何者「不」是因為開發過程中，未留意程式安全造成的問題？

(A) 魚叉式網路釣魚（Spear Phishing）

(B) SQL 資料隱碼攻擊（SQL Injection）

(C) 跨站指令碼攻擊（Cross-Site Scripting, XSS）

(D) 跨站請求偽造（Cross-Site Request Forgery, CSRF）

- 答案：(A)
- 解析：魚叉式網路釣魚係指針對特定目標進行攻擊的網

路釣魚攻擊。

（八）在軟體開發生命週期（SDLC）中，修正軟體中同一個安全性問題，於下列何者階段的成本最高？

(A) 設計階段

(B) 需求階段

(C) 產品階段

(D) 測試階段

- 答案：(C)
- 解析：在軟體開發生命週期（SDLC）中，修正軟體中同一個安全性問題，於產品階段的成本最高。

（九）關於系統開發測試中白箱測試與黑箱測試，下列敘述何者較「不」正確？

(A) 白箱測試主要測試內部邏輯架構的正確性

(B) 黑箱測試主要運用機器掃描原始程式碼

(C) 滲透測試屬於黑箱測試

(D) 原碼掃描屬於白箱測試

- 答案：(B)
- 解析：機器掃描原始程式碼屬於白箱測試。

（十）關於應用系統安全部署，下列敘述何者較為正確？

(A) 建立維護用後門

(B) 以最高權限執行軟體

(C) 移除除錯用的原始程式碼

(D) 開啟所有的底層服務

- 答案：(C)
- 解析：移除除錯用的原始程式碼屬於應用系統安全部署。

第六章. 資安維運技術

第一節　惡意程式防護與弱點管理

一、何謂惡意軟體

惡意軟體（Malware）指的是不需要或不受歡迎的軟體，如電腦病毒、電腦蠕蟲、特洛伊木馬、勒索軟體、間諜軟體、恐嚇軟體，或利用漏洞執行的軟體等；惡意軟體一般會藉由網路、可攜式儲存裝置等途徑來散播，對個人電腦、伺服器、行動裝置、網路等造成影響，包含：資料外洩、系統損害或預期的故障等資安問題。常見的惡意軟體類型有：

（一）病毒（viruses）

- 病毒是一段電腦程式碼，會將自身附加到程式或檔案中，並在電腦之間傳佈，其特徵有傳播性、隱蔽性、感染性、潛伏性、可激發性、表現性或破壞性。為了傳播病毒需依賴包含可執行碼的載體（carriers），載體可能是程式，也有可能是文件。病毒在傳播期間一般會隱蔽自己，由特定的條件觸發，產生軟體、硬體或檔案的破壞。

（二）蠕蟲（worms）

- 電腦蠕蟲未必會直接破壞被感染的系統，但可能會執行垃圾程式碼以發動拒絕服務攻擊，使電腦的執行效率大幅度

降低，進而影響電腦的正常使用；也可能會損毀或修改目標電腦的檔案；亦可能只是浪費頻寬。

- 與電腦病毒不同的是，蠕蟲不需要附在別的程式內，可能不用使用者介入操作也能自我複製或執行。

（三）木馬（Trojan）or 特洛伊木馬

- 特洛伊木馬是一種後門程式，駭客用來盜取其他使用者的個人資訊，甚至是遠端控制對方的電腦，然後藉由各種手段傳播或者騙取目標使用者執行該程式，以達到盜取密碼等各種資料之目的。
- 其特徵是可以不經過電腦使用者的准許，就可以獲得電腦的使用權。木馬的植入通常是利用作業系統的漏洞，繞過對方的防禦措施（如防火牆）。
- 特洛伊木馬不會自動操作或自動執行，它可能會暗藏在某些文件中，當使用者下載開啟時，特洛伊木馬才會運行，資訊或文件才會被破壞和遺失，且有可能因為資源被大量佔用，速度會減慢或莫名當機。

（四）間諜軟體（spyware）

- 間諜軟體是指在使用者不知情或未經同意下，搜集其個人資訊的電腦程式，有些間諜程式專門監控使用者在 internet 的存取活動與行為。

- 間諜軟體或程式被安裝後，常有下列現象：
  - ✧ 電腦比平常慢。
  - ✧ 電腦運行的程式是未曾執行或從未見過的。
  - ✧ 開啟網頁時出現各種類型的彈出視窗。

（五）其他相關的攻擊與威脅，如釣魚式攻擊（Phishing）、垃圾郵件（Spam email）等。

二、惡意軟體的防範與控制

（一）組織應實施針對惡意軟體的檢測、預防和復原的控制措施，並結合適當的使用者認知活動。另外應制定政策，禁止使用未經授權的軟體，以及存取惡意網站。

- 實施控制措施來預防或偵測未經授權軟體的使用，如：應用程式白名單。
- 實施控制措施來預防或偵測已知或有嫌疑之惡意網站的使用，如：黑名單。

（二）防毒軟體通常含有即時程式監控辨識、惡意程式掃描、清除和自動更新病毒資料庫等功能，而有的防毒軟體附加損害恢復等功能，可降低可能被惡意軟體利用的弱點，以對抗惡意軟體。

- 偵測惡意軟體的方式
  - ✧ 特徵碼（signatures）的掃描，適用已知的惡意軟體。

- ✧ 檔案完整性掃描：對檔案進行掃描後，將正常檔案的內容，計算其校驗和（Checksum）後予以儲存或記錄；之後定期地或每次使用檔案前，檢查檔案現在內容算出的校驗和，並與原來儲存的校驗和檢查是否一致，以發現檔案是否感染病毒。
- ✧ 對於新的惡意軟體，可以藉由探索的方法來檢查或搜尋程式中可疑的邏輯，另外，也可以在獨立或隔離的沙箱（沙盒）或虛擬機器中執行程式，進行驗證。目前有些防毒軟體內建沙箱的功能，可以將懷疑或可疑的程式放在裡面，實際運行看是否會產生問題。

- 安裝並定期更新惡意軟體偵測與修復軟體，定期掃描電腦及儲存媒體，執行的掃描宜包括：
  - ✧ 經由網路或任何儲存媒體接收到的所有檔案，於使用前，先掃描有無惡意軟體。
  - ✧ 電子郵件附件及下載的檔案，於使用前，宜於他處先行掃描。
  - ✧ 掃描網頁有無惡意軟體。
- 針對新惡意軟體資訊的取得，可訂閱相關資訊，或查證有提供相關資訊的網站，但須確保使用合格來源的資訊，以區別惡作劇程式及真正的惡意軟體。

三、弱點或漏洞的管理與控制

弱點可能發生在組織、流程、程序、營運、人員、實體環境、硬

體、軟體、網路通訊與資訊系統組態等。

（一）組織需識別可被威脅利用而對組織或資產產生損害的弱點，可利用技術弱點的評估方法有：

- 自動化弱點掃描工具：掃描網路或主機是否包含已知的弱點。弱點掃描程式可以實施例行的試探攻擊，然而需謹慎安排，以免觸發入侵偵測系統（IDS）警報。
- 安全性測試與評估：目的在測試所實施的資訊安全控制措施的有效性，包含網路通訊、主機、存取控制、應用程式等各項技術措施。
- 滲透測試：模擬駭客的手法，對網路或主機進行攻擊測試，目的是為了發現相關弱點或漏洞、並提出改善方法。

（二）程式碼審查：關於正在使用的資訊系統技術中漏洞的資訊應及時獲得，針對該組織所承受的這些漏洞進行評估，並採取適當的措施來解決相關的風險。

（三）建立現行且完整的資產清冊，是有效管理技術弱點的基本原則。一旦識別出潛在技術的弱點，組織宜識別相關聯的風險，以及待採取的作為，包含：弱點系統的修補，或採取其他控制措施。

（四）安裝修補程式前，應測試並評估之，以確保有效性，而且不會導致無法容忍的副作用。對於那些還沒有修補程式的安全性弱點或漏洞，惡意人士可能會加以利用，進行所謂的零日攻擊或

零時差攻擊（Zero-day attack），因此，組織宜考量下列措施：

- 關閉與弱點相關之服務。
- 調整或新增其他控制措施。
- 增強監控以偵測真實的攻擊。
- 提升員工對弱點的認知。

模擬考題

（一）在網站弱點檢測報告中，發現系統本身有存在 XSS 及 Open Redirect 問題，可以採取下列何者方案進行修補？

(A) XSS 可以透過過濾此符號”<”，即可根治

(B) Open Redirect 可以採用圖像式驗證即可根治

(C) HTML.Encode 是可以解決 XSS 的一種方法

(D) 採用 Prepared Statement 可以解決 XSS

- 答案：(C)
- 解析：避免 XSS 的方法之一主要是將使用者所提供的內容進行過濾，許多語言都有提供對 HTML 的過濾。

（二）下列何者「不」是在軟體逆向工程動態分析時，所會使用到的技巧？

(A) 設定中斷點

(B) 顯示堆疊（stack）內容

(C) 單步執行

(D) 程式碼重構

- 答案：(D)
- 解析：程式碼重構不是在軟體逆向工程動態分析所使用到的技巧。

（三）關於防毒軟體（Antivirus），下列敘述何者較「不」正確？

(A) 無法偵測所有攻擊

(B) 非 Windows 系統無需安裝防毒軟體

(C) 常使用特徵（Signature）比對來偵測惡意程式

(D) 可監視作業系統的可疑活動與應用程式的行為

- 答案：(B)
- 解析：非 Windows 系統也需安裝防毒軟體。

（四）系統人員通常無法立刻針對漏洞本身進行修補（Patch）的是屬於下列何種類型的漏洞？

(A) 區域漏洞（Local Vulnerabilities）

(B) 稀疏漏洞（Sparse Vulnerabilities）

(C) 沙盒漏洞（Sandbox Vulnerabilities）

(D) 零時差漏洞（Zero-Day Vulnerabilities）

- 答案：(D)
- 解析：零時差漏洞通常是指還沒有修補程式的安全漏洞，而零時差攻擊則是指利用這種漏洞進行的攻擊。

（五）下列何者「不」是 SYN Flood 的防禦方式？

(A) 利用防火牆阻擋所有 TCP 連線

(B) 增加 Backlog Queue 的數量

(C) 重置最舊的 Half-Open TCP 連線

(D) 使用 SYN Cookie

- 答案：(A)
- 解析：利用防火牆阻擋所有 TCP 連線不為 SYN Flood 的防禦方式。

（六）關於評估弱點，下列敘述何者正確？

(A) 不同的弱點管理方式都可使用相同的風險評級對弱點進行評分

(B) 對弱點評分可協助組織提升在業界中的口碑

(C) 弱掃報告中的弱點評分可依據組織產業類型或性質重新給予評分

(D) 弱掃工具提供的報告結果準確性高，無需再對弱點進行評估

- 答案：(C)
- 解析：弱掃報告中的弱點評分可依據組織產業類型或性質重新給予評分。

（七）關於 Session Hijacking 的偵測與防禦，下列敘述何者「不」正確？

(A) 實踐自動登出的功能也是 Session Hijacking 的其中一種防禦方式

(B) 防毒軟體對 Session Hijacking 也有部分功效

(C) 加密的連線可預防 Session Hijacking

(D) IPS 只能偵測 Session Hijacking；IDS 則可偵測與防禦

- 答案：(D)
- 解析：IDS 只能偵測 Session Hijacking；IPS 則可偵測與防禦。

（八）下列何者「不」是進行中間人攻擊所採用的技巧？

(A) Clickjacking

(B) Sniffing

(C) Packet Injecting

(D) Session Hijacking

- 答案：(A)
- 解析：Clickjacking 點擊劫持是一種在網頁中將惡意代碼隱藏在看似無害的內容之下，並誘使使用者點擊的手段。

（九）請問 CVE（Common Vulnerabilities and Exposures）是指？

(A) 常見漏洞和風險編號

(B) 弱點種類

(C) Exploit Code

(D) 漏洞修補建議

- 答案：(A)
- 解析：CVE 是指常見漏洞和風險編號。

（十）下列何種病毒會使用「不」同金鑰加密來改變自身外形？

(A) Polymorphism

(B) Scripting viruses

(C) Macro Viruses

(D) Visual Basic Script

- 答案：(A)
- 解析：Polymorphism 每次繁殖會以不同的病毒碼呈現。

第二節　資料安全及備份管理

在業務的持續性規劃或災難復原計畫中，資料可否復原是極為關鍵重要的。組織平常對資料所做的備份（Backup），其目標就在防止資料的遺失。組織應依據所同意的備份政策，備份相關的資訊、軟體以及系統映像檔（Image），並做定期的測試。

一、備份類型

（一）完整備份（Full Backup）

- 將硬碟或資料庫內的所有檔案、資料夾或資料，做一次性完整的複製。
- 優點是容易讓人理解，當需要復原資料時，只須執行一次的還原，即可復原毀損或丟失的資料。
- 缺點是每天所執行的完整備份，除所需時間較長外，也需較大量的備份媒體，成本增加。

（二）增量備份（Incremental Backup）

- 指對上一次完整備份或增量備份後更新的資料進行備份。
- 優點在於備份速度比完整備份快很多，所需的備份媒體也比較少。
- 缺點是資料還原的次數比較多，所需時間可能較長，效率相對較低。

（三）差異備份（Differential Backup）

- 針對前次執行完整備份後所變更的檔案進行備份。
- 在進行資料的還原時，只需對最後一次完整備份和最後一次的差異備份進行還原即可。
- 差異備份可避免上述兩種備份策略的缺陷，又具備各自的優點。

二、備份與還原

（一）備份（Backup），的主要目的是防止資料的遺失，且應定期執行完全備份。提供足夠的備份設施，以確保所有相關的資訊及軟體於災難後，或儲存媒體失效後可以復原。

（二）備份策略必須能處理系統和應用程式至完全還原的情況。根據業務需要確定所有重要資產，並依最佳經驗為每項重要資產實施備份機制。對於重要服務與系統，還原流程應當在最短時間內使其完全恢復使用。

（三）備份和還原的管理，應定期測試備份和還原的流程，以找出有故障的媒體，並提高中斷時成功還原的機會。並應妥善記錄還原不同系統與應用程式的詳細流程，同時審查所有備份和還原檔案，確保這些檔案包括保持業務連續性所需的所有重要系統。

三、儲存媒體的管理

（一）若可再利用媒體的內容不再需要，則組織宜予以移除，並無法復原。儲存媒體如有包含機密資訊或法規規範的個人資料，應依組織規定進行分類資訊的標示。此標示是資訊安全處置與資訊分享的關鍵要求，每個人可以藉由分類的標示瞭解到資訊內容的敏感程度。

（二）所有媒體宜依製造商規格儲存於安全且保全之環境，當不再需要媒體時，宜使用正式程序加以安全汰除，含有機密資訊之媒體宜安全地儲存及汰除，例如：經由燒毀或粉碎，或抹除資料後，再使用在組織其他的應用。另外要限制可移除設備的使用，如隨身碟等。

模擬考題

（一）只有在第一次備份時做完整備份，而之後每次備份時，只從上次備份至目前有改變的檔案進行備份。請問上述為何種備份方式？

(A) 完整備份（Full Backup）

(B) 差異備份（Different Backup）

(C) 增量備份（Incremental Backup）

(D) 選擇式備份（Selective Backup）

- 答案：(C)
- 解析：增量備份（Incremental Backup）為只有在第一次備份時做完整備份，而之後每次備份時，只從上次備份至目前有改變的檔案進行備份。

（二）關於資料備份之原則，下列敘述何者「不」正確？

(A) 完整及正確之備份資料

(B) 備份資料時須注意實體安全

(C) 資料備份時應挑選未加密之資料進行備份

(D) 資料備份維持三代以上

- 答案：(C)
- 解析：完整及正確之備份資料。

（三）關於資料備份，下列敘述何者正確？

(A) 為避免備份資料佔用儲存空間，僅需留存最新副本即可

(B) 資料庫叢集之抄寫功能（Replication），即為資料備份機制

(C) 備份資料還原測試應定期執行，確保副本資料正常留存

(D) 資料中心（IDC）進出管制嚴密，因此備份資料與來源資料存放於同地機房即可避免損毀

- 答案：(C)
- 解析：備份資料還原測試應定期執行，確保副本資料正常留存。

（四）下列何種議題「不」屬保護資料機密性的範圍？

(A) 網站因 SQL Injection 弱點導致遭駭客取得員工資料

(B) 購物系統被駭客入侵，客戶資料外洩

(C) 訂票系統因大量會員同時登入，系統當機，無法提供服務

(D) 學校教學系統，遭人入侵，竄改學生分數

- 答案：(C)
- 解析：訂票系統因大量會員同時登入，系統當機，無法提供服務屬於可用性之範圍。

（五）為確保公司備份資料之完整性，下列何種處理方式最佳？

(A) 加解密

(B) 身分驗證

(C) 雜湊計算

(D) 資訊隱藏

- 答案：(C)
- 解析：雜湊計算可確保公司備份資料之完整性。

（六）下列關於強化異地存放的備份資料的「可用性」的作法，何者較正確？

(A) 將備份資料進行加密（Encrypt）

(B) 將備份資料進行雜湊（Hash）函數計算

(C) 將備份資料將備份資料進行定期回復（Restore）測試

(D) 將備份資料進行壓縮（Compress）

- 答案：(C)
- 解析：將備份資料將備份資料進行定期回復（Restore）測試可強化異地存放的備份資料的「可用性」。

（七）某組織規劃了資料備份策略為週日進行完全備份，週一至週六進行「X」備份。若某日該組織週四因系統問題導致資料毀損，此時資料備份管理員之處理程序為先還原週日完全備份資料後，再依序將週一至週三所備份之資料還原，請問此「X」備份係指下列何者？

(A) 完整備份

(B) 增量備份

(C) 巨量備份

(D) 差異備份

- 答案：(B)
- 解析：增量備份指對上一次完整備份或增量備份後更新的資料進行備份。

（八）若資料持續不斷增加，則差異備份、增量備份、完整備份三種備份方式的備份速度，由慢到快依次為下列何者？

(A) 完整備份、差異備份、增量備份

(B) 差異備份、增量備份、完整備份

(C) 增量備份、差異備份、完整備份

(D) 完整備份、增量備份、差異備份

- 答案：(A)
- 解析：備份方式的備份速度，由慢到快依次為完整備份、差異備份、增量備份。

（九）在雜湊（Hash）之前將雜湊內容的任意固定位置插入特定的字串，此方式被稱為什麼？

(A) 數位簽章（Digital Signature）

(B) 加鹽（Salt）

(C) 編碼（Encoding）

(D) 替換（Substitution）

- 答案：(B)
- 解析：加鹽係在雜湊（Hash）之前將雜湊內容的任意固定位置插入特定的字串。

（十）某公司的網站伺服器內，將五顆硬碟作 RAID 5，並且備份機制中規劃每週日 23:30 進行完整備份（Full Backup），其餘每天 23:30 進行差異備份（Differential Backup），若於某週三 23:00 時，伺服器其中一顆硬碟發生故障，請問應採取下列何種處理

方式？

(A) 上週五的 Full Backup 磁帶回存，再依序將週日、一、二的增量備份磁帶回存

(B) 將上週五的 Full Backup 磁帶回存，再將週二的備份磁帶回存

(C) 將上週三的磁帶回存

(D) 只需更換有問題的硬碟，重作 Rebuild

- 答案：(D)
- 解析：當 RAID 5 的一個磁碟資料發生損壞後，可以利用剩下的資料和相應的奇偶校驗資訊去恢復被損壞的資料。

第三節　日誌管理

日誌中記錄了使用者的活動、異常狀況、錯誤與資訊安全事件的資訊，應該產生與保留相關的系統、服務或事件日誌，並定期檢討與檢視。

一、事件記錄（Event logging）

（一）事件日誌中記錄了使用者的活動、異常狀況、錯誤與資訊安全事件的資訊，應該產生與保留事件日誌，並定期檢討與檢視，宜包括下列項目：

- 使用者識別碼（ID）。
- 系統活動。
- 關鍵事件（如：登入及登出）的日期，時間及細節。
- 存取系統、資料或其他資源成功及被拒絕情形的紀錄。
- 系統組態的變更。
- 特別權限的使用。
- 所存取的檔案及存取的種類。
- 網路位址及協定。
- 使用者於應用系統中所執行的紀錄。

二、日誌的管理措施

（一）日誌的記錄工具與日誌資訊應加以保護，防止篡改和非授權的存取。日誌的控制措施著重於防範日誌資訊遭未經授權的變更，並防範存錄設施之操作問題，內容包括下列各項：

- 所記錄訊息形式之更改。
- 被編輯或刪除的日誌檔。
- 日誌檔媒體儲存超過容量，導致無法記錄事件或覆蓋以前所記錄事件。

（二）日誌包含多種系統或服務的事件或記錄，例如：網路、目錄服務、檔案伺服器、資料庫、網站、以及各項應用程式等，可能包含不同的儲存格式、欄位。組織可以嘗試建立日誌集中儲存、管理的機制，將日誌的種類減少。另外，為在資料量龐大的各項日誌中，篩選出特定條件的事件或記錄，組織可以使用日誌的分析與彙整，方便產生所需的報告。

（三）系統日誌通常包含大量資訊，其中大多與資訊安全監控無關。為協助識別資訊安全監控用途之重要事件，考量自動將適切的訊息複製到另個安全性日誌中，或使用適當之系統公用程式或稽核工具，執行相關檔案的訊問或衡量合理性。

（四）稽核日誌可能被要求封存或留存，以作為紀錄保存政策的一環，或是因應收集及保存證據的要求。保留的期限應符合法規或政

策的要求，未來如有司法訴訟或相關仲裁時，可以滿足調查所需，蓄意違反法律或規定的人員也難以否認以前的惡意行為。

三、管理者與操作員的日誌

系統管理者和系統操作員的活動應被記錄，紀錄的日誌要予以保護並定期檢視。可使用不受系統或網路管理者控制管理的入侵偵測系統、監視系統及網路的管理活動，確保遵循性。

模擬考題

（一）若某公司以 UDP port 514 的方式，遠端蒐集 Syslog 進行日誌留存，請問下列敘述何者最正確？

(A) 遠端蒐集之日誌，無法作為有效證據

(B) 網路流量大時，有可能遺失封包（資料）

(C) Syslog 無需考量加密即可保護資料傳輸之安全

(D) 遠端蒐集之日誌，存放時不應加密，以免破壞資料的正確性

- 答案：(B)
- 解析：在 TCP/IP 模型中，UDP 為網路層以上和應用層以下提供了一個簡單的介面。UDP 只提供資料的不可靠傳遞，它一旦把應用程式發給網路層的資料傳送出去，就不保留資料備份。

（二）關於 Syslog 日誌傳輸協議，下列敘述何者正確？

(A) 為確保資料傳輸效率，僅能透過 UDP 協議使用

(B) 為確保資料正確性，僅能透過 TCP 協議使用

(C) 為確保資料機密性，可透過 TLS 協議進行加密傳輸

(D) 為確保資料機密性，日誌需先自行加密後再進行傳輸

- 答案：(C)
- 解析：業界大量使用之 Syslog 日誌傳輸協議為確保資料機密性，可透過 TLS 協議進行加密傳輸。

（三）在進行日誌分析前，通常會先將已收集的資料中，格式不正確或完整度不足的資料進行刪除或修正，這個動作我們一般稱之為？

(A) Data Collection

(B) Data Profiling

(C) Data Normalization

(D) Data Cleaning

- 答案：(D)
- 解析：Data Cleaning 係指在進行日誌分析前，通常會先將已收集的資料中，格式不正確或完整度不足的資料進行刪除或修正。

（四）要求相關的資訊系統、網路設備須有一致性的同步時脈（鐘訊同步），其主要的目的為何？

(A) 確保作業系統的機密性

(B) 防範資料的漏失

(C) 避免被分散式阻斷服務攻擊（DDoS）

(D) 確保稽核日誌的準確性，以便紀錄事件與生成證

- 答案：(D)
- 解析：鐘訊同步確保稽核日誌的準確性，以便紀錄事件與生成證。

（五）為了分析集中收容的不同設備之日誌，常會發生不同設備之日誌格式、命名方式不同之分析難題，此時需要進行下列何種處

理？

(A) 去識別化（De-identification）

(B) 初始化（Initialization）

(C) 正規化（Normalization）

(D) 最佳化（Optimization）

- 答案：(C)
- 解析：正規化係為分析集中收容的不同設備之日誌，常會發生不同設備之日誌格式、命名方式不同之分析。

（六）請問「留存系統、網路日誌」是為了保護資訊安全的何種特性？

(A) 機密性（Confidentiality）

(B) 可用性（Availability）

(C) 可靠性（Reliability）

(D) 不可否認性（Non-Repudiation）

- 答案：(D)
- 解析：留存系統、網路日誌是為了保護資訊安全的不可否認性。

（七）關於事件紀錄檔，下列敘述何者較「不」正確？

(A) 事件記錄包含伺服器登入資訊

(B) 事件記錄可以作為調查佐證

(C) 事件記錄包含工單資料

(D) 事件記錄需要至少保存足夠期間可供查詢

- 答案：(C)

- 解析：事件記錄不包含工單資料。

（八）關於日誌的管理，下列敘述何者較「不」正確？

(A) 選擇適當的整合式 Log 管理工具，並且測試確認是否能快速查詢分析

(B) 可以考慮將有機敏資料的日誌加密儲存，以避免資料遭到竄改

(C) 為了資料完整，應將系統的所有稽核日誌全部啟動與儲存

(D) 應定義事件分類，以有效分析

- 答案：(C)
- 解析：為了資料完整，應將系統的重要稽核日誌全部啟動與儲存。

（九）請問若日誌與系統管理人員，想把不同系統、程式之日誌檔進行管理、分析，則該先將這些日誌檔如何處理最為合適？

(A) 去識別化

(B) 文件化

(C) 無需處理

(D) 正規化

- 答案：(D)
- 解析：正規化係為分析集中收容的不同設備之日誌，常會發生不同設備之日誌格式、命名方式不同之分析。

（十）關於日誌與監控作業，下列敘述何者較「不」正確？

(A) 日誌應記錄使用者活動、異常，並且依法定要求的時間保存

(B) 系統日誌為避免外洩，應在出資安事件時才查詢，平日不應存取

(C) 日誌應避免可被該系統管理人員修改

(D) 資訊處理系統、網路設備的鐘訊，應與議定的準確時間來源同步

- 答案：(B)
- 解析：系統日誌中記錄了使用者的活動、異常狀況、錯誤與資訊安全事件的資訊，應該產生與保留事件日誌，並定期檢討與檢視。

第七章. 新興科技安全

第一節　雲端安全概論

一、何謂雲端運算

依據美國國家標準與技術研究院（NIST）的定義，雲端運算是一種依照需求，可以方便地存取一組共用及分享電腦資源的模式。所配置的資源包括網路、伺服器、儲存空間、應用程式及服務等，可以在最少的管理工作及服務提供者的介入下，快速地提供與交付。主要特性如下：

（一）依客戶需求的自我服務（On-demand self-service）

- Consumer 可以單方向在有需要的時候，在沒有人為介入的狀況下，要求電腦的處理能力。

（二）廣泛的網路存取（Broad network access）

- 藉由網路的標準機制存取。

（三）共用的資源：

- 雲服務提供者的電腦資源藉由租賃的方式，依照需求提供給多個使用者。
- 電腦資源包括儲存空間、處理器、記憶體、網路、與虛擬機器等。

（四）迅速與彈性：

- 電腦能力可以迅速與彈性地提供，可以快速地 scale out 與 scale in。

（五）可供量測的服務（Measured Service）

- 藉由所提供的量測能力，雲端系統可以自動地控制資源，並最佳化。資源的使用可以被監控與報告，並正確地提供給服務提供者與使用者。

二、雲端運算的服務模式

（一）基礎架構即服務（Infrastructure as a Service, IaaS）

- 提供電腦相關硬體資源，包含伺服器、網路（防火牆、路由器、負載平衡等）、Storage、以及資料中心的空間等。

（二）平台即服務（Platform as a Service, PaaS）：

- 架構在 infrastructure 上的平台，提供所需的開發環境與運行環境，客戶或使用者可以在該平台上開發或部署所需的應用程式。

（三）軟體即服務（Software as a Service, SaaS）

- 透過網路來使用雲服務提供者的應用程式。

三、雲端運算的部署模式

（一）公有雲（Public Cloud）

- 為公眾所使用且規模龐大的雲端運算環境與資源。
- 存在於雲服務提供者的處所。

（二）私有雲（Private Cloud）

- 雲端運算環境由特定一個組織建立與營運管理。
- 地點可能在企業擁有的處所或外部所租借的環境。

（三）社群雲（Community Cloud）

- 為特定社群的組織或消費者所共享的雲端運算環境與資源。

（四）混和雲（Hybrid Cloud）

- 由兩種或以上的雲所組成，藉由一些標準或專有技術來整合，維持資料與應用程式的可移植性。

四、雲端運算的資訊安全（Cloud Computing Security）

雲端運算資訊安全是典型資訊安全的一個子領域，藉由一套政策、技術、與佈署的控制措施，來保護雲端運算上的資料、應用程式、與基礎架構等。

（一）與雲端運算資訊安全有關的議題有很多，一般將其分為兩大類角色：

- 雲服務提供者：必須確認其雲端的基礎架構與設施是安全的，客戶的資料與應用程式能夠被妥善地保護。
- 雲服務的使用者：必須確認服務提供者已經採取適當的措

施，以保護他們的資訊安全。基於雲端運算特性的資訊安全實施措施屬之，如虛擬化、聯邦式身分認證、加密等。

五、雲端運算風險的因應措施

（一）雲端運算資訊安全的控制措施，其主要部分與其它 IT 環境中的安全控制措施，在項目上並沒有太大的差異。然而，基於所使用的服務模式、部署模式以及相關的技術，與傳統 IT 解決方案有所差異，因此面臨不同的風險可能就需要不同的控制措施。

（二）一個組織的資訊安全狀態，取決於其資訊安全管理的成熟度、有效性，以及基於風險管理所實施措施的完整性。雲服務提供者以及使用者，都需承擔資料安全性的責任。

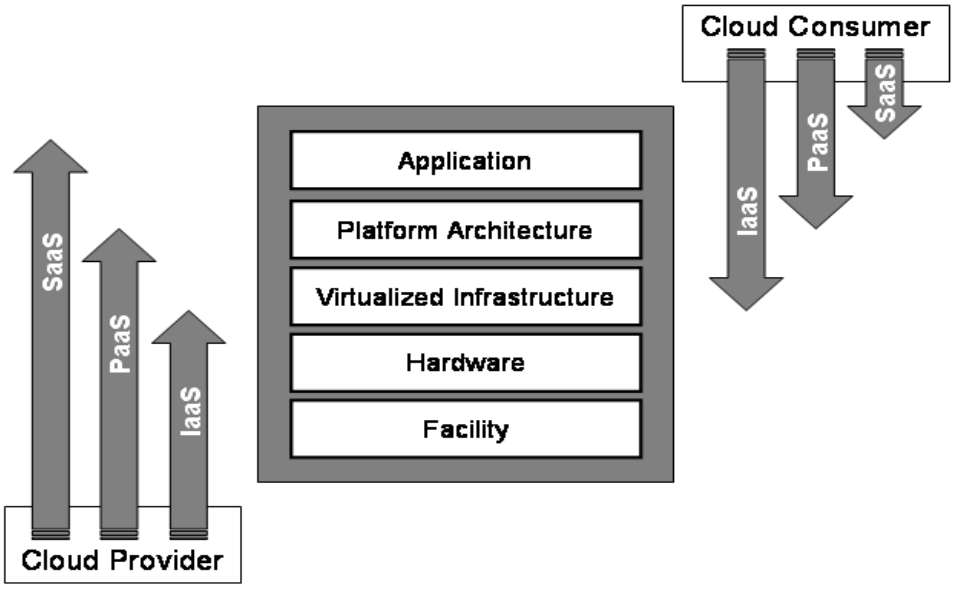
（三）使用者對服務提供者應做適當的監督，確認相關的要求與實施都在掌握中。

（四）當雲端運算服務委由第三方廠商來管理，或是部署在企業外部時，如果企業沒有或缺乏供應商管理的經驗，可能有牴觸法規的可能性，因此在規劃雲服務時也須妥善因應。

（五）不同的服務模式，影響企業對運算資源的控制。在不同雲服務模式中，雲服務提供者和使用者在資訊安全上的職責有很大的差異，如：

- SaaS：對資訊安全規範與要求的遵循，服務提供者扮演重要的角色。法規的要求，很多需要雲使用者透過合約來確認達成。
- PaaS：雲使用者與服務提供者共同合作來達成規範的要求。
- IaaS：雲使用者負責較多的控制以達成規範要求，因此應要瞭解雲服務提供者所提供的存取控制流程與措施。除了與服務提供者應有合約的要求外，雲使用者對於資訊安全保護機制，以及控制措施也必須有效地評估與實施。

（六）雲端運算上資料的保護，雲服務提供者與使用者雙方都有相關的責任。對於資料外洩事件，雲服務提供者和使用者應在合約上註明各自的承諾與處理方式。



資料來源：NIST

（七）依據雲端安全聯盟（Cloud Security Alliance, CSA）的調查，雲端運算服務的威脅主要包含有：

- 資料洩露（Data Breaches）
- 弱的身分認證、密碼與存取管理（Weak Identity, Credential and Access Management）
- 不安全的應用程式開發介面（Insecure APIs）
- 系統和應用程式漏洞（System and Application Vulnerabilities）
- 帳戶的劫持（Account Hijacking）
- 惡意的內部人士（Malicious Insiders）
- 進階持續性的威脅（Advanced Persistent Threats, APTs）
- 資料遺失（Data Loss）
- 盡職調查不足（Insufficient Due Diligence）
- 濫用與惡意的使用雲端運算服務（Abuse and Nefarious Use of Cloud Services）
- 阻斷服務攻擊（Denial of Service）
- 共享技術的問題（Shared Technology Issues）

六、法規的遵循與稽核

（一）使用者在使用雲端服務前，必須與提供者確認雙方在法規遵循上與稽核上的責任。對於遵循與稽核上的責任與要求，透過合

約清楚規範：

- 使用者是否有稽核的權力應註明於合約。
- 為滿足法規所要求的查核，使用者應該指明所需記錄與收集的資訊給提供者，如：存取記錄、系統或應用程式日誌、稽核事件報告等。

（二）不同的雲端服務模式，對於法規遵循所需的控制項目與能力會有所不同。使用者衡量雲服務提供者對法規遵循、稽核的能力與承諾，以決定是否適合採用該雲端運算服務。

七、虛擬化（Virtualization）

虛擬化是將電腦資源以邏輯的方式予以呈現，不受現有資源的架設方式、地域或物理組態所限制，將電腦資源妥善予以切割與分配，如 CPU、Memory、Storage 等，產生與實際硬體所對應出的虛擬化系統。

（一）虛擬化包含下列三種特性

- 切割（Partitioning）：將實體系統的可用資源切割以支援作業系統與應用程式。
- 隔離（Isolation）：每個虛擬機器與其實體主機或是其他虛擬機器都是被隔離的。一部虛擬機器 crash，不會影響其他的虛擬機器，同時其中的資料也不會和其他虛擬機器分享。

- 封裝（Encapsulation）：一部虛擬機器可以用一個單一的檔案來代表，可以藉由所提供的服務容易地予以識別。

模擬考題

（一）下列何種雲端型態的安全性最佳？

(A) 公有雲

(B) 社區雲

(C) 混合雲

(D) 私有雲

- 答案：(D)
- 解析：私有雲較其他雲端型態的安全性最佳。

（二）下列何者「不」是雲端運算服務形式？

(A) 軟體即服務（SaaS）

(B) 平台即服務（PaaS）

(C) 知識即服務（KaaS）

(D) 基礎架構即服務（IaaS）

- 答案：(C)
- 解析：雲端運算服務形式包含 SaaS、Paas、Iaas。

（三）下列何者「不」是和雲端安全有關的國際標準？

(A) ISO/IEC 27011

(B) ISO/IEC 27017

(C) ISO/IEC 27018

(D) CSA STAR

- 答案：(A)

- 解析：ISO/IEC 27011-對於電信組織根據 ISO/IEC 27002 標準的資訊安全管理指導。

（四）下列何者「不」是由美國國家標準技術研究院（NIST）所定義的雲端運算的五項關鍵特徵之一？

(A) 可量測的服務

(B) 快速且彈性的架構

(C) 廣泛的網路存取方式

(D) 資源調配皆由供應商的人員協助

- 答案：(D)
- 解析：資源調配皆由供應商的人員協助不屬於美國國家標準技術研究院（NIST）所定義的雲端運算的五項關鍵特徵之一。

（五）使用者租用了雲端服務提供商所提供的虛擬伺務器（VM），可自行管理並且在上面安裝軟體，雲端服務供應商只提供必要的基礎設施，像是網路、儲存空間、處理器等資源。以上描述屬於何種雲端服務型式？

(A) 軟體即服務（SaaS）

(B) 平台即服務（PaaS）

(C) 知識即服務（KaaS）

(D) 基礎架構即服務（IaaS）

- 答案：(D)
- 解析： IaaS 使用者負責較多的控制以達成規範要求，因

此應要瞭解雲服務提供者所提供的存取控制流程與措施。

（六）在雲端平台建置過程中常會使用磁碟陣列（Redundant Array of Independent Disks, RAID）當作儲存空間，請問下列何種模式容錯率最高？

(A) RAID 0

(B) RAID 1

(C) RAID 2

(D) RAID 5

- 答案：(B)
- 解析：RAID 1 為兩組以上的 N 個磁碟相互作鏡像，在一些多執行緒作業系統中能有很好的讀取速度，理論上讀取速度等於硬碟數量的倍數，與 RAID 0 相同。另外寫入速度有微小的降低。只要一個磁碟正常即可維持運作，可靠性最高。

（七）關於雲端蜜罐（Honeypot），下列敘述何者「不」正確？

(A) 通常設置在正式的產品運作環境之中

(B) 任何連線蜜罐的行為都是可疑的

(C) 偽裝成有價值的網路或電腦系統，並設置漏洞，誘使駭客攻擊

(D) 可用來取得電腦病毒樣本

- 答案：(B)
- 解析：任何連線蜜罐的行為並不一定都是可疑的。

（八）當連線到使用雲端架設的 Http 服務時，回傳 404 的 HTTP 狀態碼，請問這個狀態碼代表下列何者？

(A) Gateway Timeout，伺服器嘗試執行請求時，未能及時從其他伺服器取得回應

(B) OK，請求已成功，所請求的回應標頭或資料本體將被送回

(C) Not Found，請求失敗，請求所希望得到的資源未在伺服器上被發現

(D) Request Timeoutt，請求逾時，客戶端沒有在伺服器預備等待的時間內完成一個請求的傳送

- 答案：(C)
- 解析：404 的 HTTP 狀態碼 Not Found，請求失敗，請求所希望得到的資源未在伺服器上被發現。

（九）駭客入侵雲端服務供應商，再以此為跳板入侵使用者竊取資料稱之為？

(A) 封包監聽

(B) 雲端跳躍

(C) 阻斷服務攻擊

(D) 社交工程

- 答案：(B)
- 解析：此即為著名駭客 APT10 所使用之攻擊手法。

（十）下列何者「不」是常見的雲端運算的部署模式？

(A) 公有雲（Public）

(B) 私有雲（Private）

(C) 自由雲（Free）

(D) 混合雲（Hybrid）

- 答案：(C)
- 解析：自由雲（Free）不是常見的雲端運算的部署模式。

第二節　行動裝置安全概論

隨著科技的進步與發展，行動裝置（如智慧型手機）的運算能力越來越強、記憶體也越來越多，行動式設備在工作或生活中角色越來越重要。

一、行動式運算與特性

（一）藉由一部可以在行動中使用的裝置，來存取網路上的資源與服務，我們稱為行動式運算（Mobile Computing），包含以下三個主要項目：

- 行動通信（Mobile Communication）：處理基礎架構網路的通信問題，如：通信的性能、協定、資料格式與相關的技術。
- 行動硬體（Mobile Hardware）：行動的裝置、設備或輔助硬體元件，如：智慧型手機、平板電腦、穿戴式裝置等。
- 行動軟體（Mobile Software）：處理行動應用程式的功能。

（二）行動式設備的特性在於使用者比較不受地域位置的限制，可以方便地使用服務。不論是企業組織或個人使用者，行動裝置的使用可以提升工作的生產力、資訊的利用與分享等好處。然而若在移動狀態時使用行動裝置，必須要特別注意其安全性。例如，在開車時使用 LINE 或簡訊等相關服務是非常危險的，使

用者會分心，當遇危急狀況時無法及時地採取適當的措施。一些國家的法律基於安全（safety）考量，規定禁止在駕車時使用手機。

（三）傳統行動運算環境中，行動應用程式在行動設備中執行，而其使用的資料也是儲存在設備中。主要的優勢是沒有延遲或網路頻寬的問題，然而，這類型的應用程式一般都有功能上的限制，以及較難提供企業級的應用。

（四）將行動裝置與雲端運算結合的模式，稱為行動雲端運算（Mobile Cloud Computing）。雲端運算的運作模式很多是將使用者的工作與資料保存在 internet，有需要時即可存取，而不是放在個別的設備中。因為資料在雲端運算與行動式設備之間移轉，因此資料傳輸的延遲與網路的頻寬，可能會對運用造成影響。另外，在行動雲端運算模式中，使用者可以從遠端伺服器來執行應用程式，然後將結果傳送回使用者。既然所有的計算與資料都在雲上處理，行動式設備就不需要功能很強的配置，如 CPU 或 memory，可以節省成本。

（五）行動式存取在資訊安全方面，有以下的限制：

- 使用行動設備時，應特別注意確保企業資訊或機密隱私資料不會外洩。
- 當企業使用行動設備執行商業或協同作業時，設備中所存

放之資料，應妥善予以分類儲存，並實施適當之保護與管理控制措施，如：將單一行動設備中所儲存之公司與個人資料予以隔離等。

（六）在公共場所與其他未受保護區域，應謹慎地使用行動設備。另外如使用公眾網路等通訊方式，應注意傳輸之機密性與安全性。其它如行動設備遺失或失竊的因應，也應特別考量。

（七）在行動設備的遠端管理方面，企業應可否套用既有的資訊安全政策、以及管理措施（如：防毒、防駭、Patch 管理、身分識別的管理機制等）及相關的安全措施。

（八）在應用程式的要求方面，多樣且功能強大的移動式設備紛紛推出，而支援行動式平台的應用程式也越來越多。目前市場上有多個行動式平台（指在行動式設備上所運作的作業系統），但是其異質性造成互通性與轉移上的困難，並非所有的應用程式皆可用於所有的移動平台上，因此應用程式的標準化是非常重要的。

（九）在網路的可用性方面，雲應用程式對網路頻寬與傳輸效率，要求一個穩定的連線。HTML 5 支援 data caching，即使暫時失去連線，行動雲端運算的應用程式，仍可繼續工作。

二、行動裝置安全的控制措施

（一）應制定政策和配套的安全措施，以管理因使用行動設備而帶來的風險。一個行動設備的政策應考慮到下列項目：

- 行動設備的註冊：經過註冊程序才能存取企業的資源或應用程式。
- 實體保護的要求：行動裝置如果要報廢、販賣或捐贈時，應先完整清除裝置上的所有資料，並且將行動裝置恢復成出廠的狀態。當行動裝置透過 USB 傳輸線充電時，也應確認所連接到電腦或是傳輸線是可信任的，否則容易遭到入侵攻擊。
- 軟體安裝的限制：僅安裝可信任來源的軟體，如官方的軟體商店。在軟體安裝時，應了解該軟體所要求開放存取權限的項目是否是合理的，經過評估後再行安裝。
- 行動設備的軟體版本和修正程式更新的要求：行動裝置上的作業系統或軟體，應定期自動或手動安裝更新修正程式。
- Web 服務和 Web 應用程式的使用：設定白名單或黑名單應用程式。
- 存取控制：如果不影響使用的便利性，最好將行動裝置設置密碼，如手機開機或閒置一段時間沒有使用，螢幕自動進入鎖定模式。如果行動使用者違反規定、裝置不符合規

範、或使用者離職，應取消其對公司資源或服務的存取權。

- 連線的功能：首先應小心使用公開未知的無線 Wi-Fi 網路，特別應避免用來傳輸隱私性或機密的資料。一些不常使用的連線功能也予以關閉，如：藍牙、近場通訊（Near Field Communication, NFC）、GPS 等，以避免有心人士利用這些介面進行干擾，或藉由這些技術的漏洞入侵行動裝置。
- 加密技術：依業界標準對裝置、記憶卡及傳輸中的資料加密。
- 惡意軟體的保護：安裝防護軟體或防毒軟體，以偵測已知的惡意軟體或網站。
- 遠端禁用、刪除或鎖定行動裝置：行動裝置不幸遭竊或遺失時，藉由內建或安裝的遠端定位與資料刪除功能，來找出遺失裝置的位置、鎖定裝置及刪除資料。
- 備份：定期將行動裝置內的資料進行備份，當不幸行動裝置的資料毀損或遺失時，可以進行還原。

（二）如允許使用私有的行動設備（Bring Your Own Device, BYOD），應對政策及相關的安全措施加以考慮，如下：

- 企業資訊與私人資訊的隔離。
- 提供存取企業資訊前，使用者應已簽署協議確認自己相關的職責，並考量隱私性法規的規範。

模擬考題

（一）有些 App 都會要求授權讀取行動裝置上的個人資訊，如聯絡人資料、照片、撥打電話、簡訊等。下列敘述何者「不」正確？

(A) 授權 App 直接用行動裝置撥打電話或簡訊給特定對象可能會需要額外費用

(B) 行動裝置上的聯絡人資料、照片屬於個人資料，要小心保護，以免觸犯「個人資料保護法」

(C) 絕不散佈未經求證之訊息、及違反社會善良風俗之照片或影片，以免觸法

(D) 為了 App 對個人資訊的蒐集，App 要求行動裝置上聯絡人的讀取權限，可以直接同意授權

- 答案：(D)
- 解析：應謹慎了解要求，進行評估後再進行授權。

（二）關於強化行動裝置安全的方法，下列何者較「不」安全？

(A) 設定螢幕鎖定需輸入密碼或指紋後方能使用

(B) 當收到系統安全性更新的提醒即進行更新

(C) 啟動無線區域網路自動連線機制以避免連接不受信任的 App

(D) 避免使用不信任的第三方 App

- 答案：(C)
- 解析：應關閉無線區域網路自動連線機制以避免連接不受信任的 App。

（三）下列何者較「不」能避免使用者，在使用行動裝置時，遭受網路釣魚攻擊（Phishing）？

(A) 用無痕跡的瀏覽器開啟網頁

(B) 留意點選的網址是否異常

(C) 不隨意開啟來路不明的信件連結

(D) 不隨意連接不信賴的 Wi-Fi 熱點

- 答案：(A)
- 解析：無痕跡的瀏覽器開啟網頁若隨意開啟來路不明資料仍可能發生釣魚事件。

（四）關於運用 HCE（Host Card Emulation）於行動裝置上進行行動支付，下列敘述哪些是正確的？

(1) 從雲端支付平台取得的金鑰是有時效性的

(2) 無需挑選通過服務平台安全認證的手機

(3) 手機無需具備安全元件來儲存支付資訊

(4) 需更換具備安全防護特殊的 SIM 卡才能支援

(A) (1)(2)(3)

(B) (1)(2)(4)

(C) (1)(3)(4)

(D) (2)(3)(4)

- 答案：(A)
- 解析：HCE（Host Card Emulation）是僅使用軟體對智慧卡進行的虛擬而精確的呈現。在 HCE 架構之前，NFC 交

易只通過安全元件（Secure Element）進行。

（五）下列何者較可以避免行動裝置連接 Wi-Fi 時，遭受到中間人攻擊（Man-in-the-Middle, MiTM）？

(A) 設定開機密碼鎖

(B) 連線使用加密 VPN 連線服務

(C) 限制連線 Wifi 之速率

(D) 只連線具身分認證機制的 Wifi 熱點或服務

- 答案：(B)
- 解析：連線使用加密 VPN 連線服務建立通道，防止中間人攻擊。

（六）使用行動裝置的 NFC 功能進行行動支付或資料交換時，較「無」需防範下列何種攻擊？

(A) 中間人攻擊（Man-in-the-Middle Attack）

(B) 竊聽（Sniffing）

(C) 重送攻擊（Replaying Attack）

(D) 通行碼暴力破解（Password Brute Force Attack）

- 答案：(D)
- 解析：行動裝置的近場通訊（Near Field Communication, NFC）功能進行行動支付或資料交換時與通行碼暴力破解較無關係。

（七）關於行動裝置上運用代碼技術（Tokenization）行動支付方式的安全，下列敘述何者正確？

(A) 無法由代碼去推算使用者原本的卡號

(B) 以手機本身的 Secure Elemen 儲存 Tokenization 是不安全的

(C) 手機遺失時，儲存在手機的信用卡卡號仍會被取得

(D) 應越獄（Tethered Jailbreak）取得手機權限來管理較安全

- 答案：(A)
- 解析：行動裝置上運用代碼技術（Tokenization）無法由代碼去推算使用者原本的卡號。

（八）關於行動裝置通訊軟體，下列敘述何者較「不」正確？

(A) 開啟「阻擋訊息」，阻擋非來自好友之訊息

(B) 只在信譽良好網站或官方 APP 市集中下載使用

(C) 對於聳動的訊息，可直接分享給相關好友

(D) 不在公用電腦登入，並定期更改密碼

- 答案：(C)
- 解析：資訊需謹慎評估，不可直接分享。

（九）BYOD（Bring Your Own Device）是指帶行動裝置至辦公環境中辦公事，在資安標準作業規範 ISO/EC 27002:2013 中，關於 BYOD 的指導綱要與安排項目，「不」包含下列何者？

(A) 合理性查核，已測試輸出資料是否合理

(B) 提供適當的通信設備，包括保護遠端存取的方法

(C) 提供軟硬體支援與維護

(D) 稽核與安全監視

- 答案：(A)
- 解析：自攜電子設備亦稱自攜技術、自攜電話或自攜電腦是一種允許員工使用個人行動裝置進入他們工作區域並用以處理公司資訊與應用程式的作業方式。

（十）關於行動裝置可能遭受的安全威脅，下列敘述何者「不」在其中？

(A) 行動裝置遺失資料外洩

(B) 行動裝置感染病毒

(C) 行動裝置因欠費，無法連上網路

(D) 行動裝置因安裝不明軟體，有遭植入後門之風險

- 答案：(C)
- 解析：行動裝置因欠費不屬於行動裝置可能遭受的安全威脅。

第三節　物聯網安全概論

伴隨著資訊科技的發展與演進，物聯網概念的應用在這幾年也快速的成長，應用範圍越來越廣，包含了穿戴裝置、車載應用、零售庫存、醫療照護、工業與能源應用、以及智慧家庭與智慧城市等。

網際網路或是企業網路的使用，可以方便讓一般使用者與企業組織與外界溝通，資訊的交流與交換也日益增多，但這些都對個人或是企業的資訊安全，產生更大的風險與挑戰。

若物聯網的應用發生資訊安全的攻擊與事件，所產生的影響不再只是網路、服務的中斷，或是電腦、行動裝置中的資料外洩，而是可能對人身安全、生產製造、商務營運、以及家庭或是社會的運作產生更嚴重的影響。因此在物聯網服務或系統的設計之前，應將重點放在威脅分析和風險評估上，以衡量發生資訊安全事件或違規的行為時，所產生的影響與衝擊。

一、物聯網安全性的威脅與弱點

(一)物聯網設備或系統在安全性的挑戰或威脅，分為以下六點說明：

- 設備的安全性
  - ✧ 物聯網設備常常是小型、廉價的設備，因此幾乎沒有導入實體的安全性，且可移動式的設備可能被盜，固定式的設備可能被移動，因此應實施實體的保護。
- 系統的安全性

- ✧ 當晶片大量嵌入到物聯網的平臺或系統時，使用者個人甚至可能不知道他們的活動或狀態正在被記錄。

- 網路的安全性
  - ✧ 架構上缺乏連線的備援機制，當主要連線中斷時，服務即終止。
- 管理的安全性
  - ✧ 在設備上線期間和之後，不容易執行安全性的遠端管理。
- 存取控制的安全性
  - ✧ 駭客可能藉由未經授權的方式來存取感測器、驅動器等，以操縱控制物聯網的裝置或系統，產生傷害。
- 隱私權
  - ✧ 藉由位置資訊的搜集與分析，可能對人的行為和活動進行未經授權的跟蹤。

（二）OWASP IOT TOP 10 2018 專案中，針對最常見物聯網弱點或漏洞進行研究，提出了十大風險的建議：

- 弱密碼（Weak, guessable or hard coded passwords）
- 不安全的網路服務（Insecure network services）
- 不安全的生態界面（Insecure ecosystem interfaces）
- 不安全的更新機制（Lack of secure update mechanisms）
- 使用不安全的元件（Use of insecure or outdated components）
- 隱私防護不足（Insufficient privacy protection）

- 不安全的資料移轉和儲存（Insecure data transfer and storage）
- 缺乏裝置設定（Lack of device management）
- 不安全的預設（Insecure default settings）
- 缺少物理加固措施（Lack of physical hardening）

二、物聯網資訊安全的目標與要求

（一）參考正在發展中的物聯網國際標準 ISO/IEC CD 30141 Internet of Things Reference Architecture，下列為與安全性有關的特性：

- 穩健性（Robustness）
  - ✧ 包含準確性（Accuracy）、可靠性（Reliability）及彈性（Resilience）。
- 安全性（Security）
  - ✧ 包含可用性（Availability）、機密性（Confidentiality）、完整性（Integrity）及安全（Safety）。
- 保護個人資料（Protection of personally identifiable information）

（二）企業應採取積極措施來解決資訊安全的問題，除了藉由不同管道提升專業能力外，也應該將上述資訊安全的目標與要求加進物聯網專案的規劃與設計。另外，分享資訊安全的各種資訊可以促進合作學習，並有助於避免產業之相關組織遇到同樣的網路威脅或風險。

三、物聯網安全的策略與原則

（一）參考美國國土安全部（Department of Homeland Security）針對物聯網資訊安全的挑戰提出下列的策略原則：

- 在規劃設計階段納入安全。
- 促進資訊安全更新與漏洞的管理。
- 運用公認的資訊安全作法。
- 依據潛在影響來安排安全措施的優先順序。
- 在物聯網促進其透明度。
- 深思熟慮且謹慎的連接。

（二）由於物聯網應用與服務的多樣性，其系統架構或使用的技術會有所差異，實務上很難有通用的解決方案來降低所有物聯網的安全性風險。

（三）物聯網的開發商或製造商需要知道他們整體的供應鏈中，是否有任何所提供的軟體或硬體元件，包含有相關的弱點或漏洞。

四、物聯網資訊安全的規劃設計要點

（一）將安全納入物聯網系統的架構與規劃

- 物聯網的應用非常多元，不同的應用會有不同的系統架構，而且使用的一些技術也比較新且多元化，資訊安全的風險與需求可能會有所差異。企業必須先規劃設計所需物聯網

產品或服務的系統架構,以及各組成項目在安全性的要求,才能妥善因應相關威脅與風險。

（二）實施分層式的縱深防禦安全防護以保護物聯網資產

- 多層次縱深防禦是一種防禦機制，主要是利用多層次的防禦技術來阻絕網路上的攻擊，縱使其中一層無法有效預防或偵測攻擊，但後續仍有其他機制來攔阻該項攻擊。物聯網的分層式縱深防禦包含有：
  - ✧ 實體層
  - ✧ 設備層
  - ✧ 網路層
  - ✧ 應用層

（三）藉由加密技術來保護敏感資訊

- 物聯網系統對於加密技術的使用，因物聯網設備與環境的特性，除了考量加密強度外，也應注意性能（效能）方面的影響，如：部分嵌入式的物聯網設備因為資源有限，有可能需選擇較小的密鑰。

模擬考題

（一）當兩個物聯網裝置在通訊過程中，攻擊者分別對個別裝置進行獨立連線，並擷取與轉送雙方間傳遞資料，使原通訊雙方以為處於一個安全的資料傳輸環境。請問以上描述屬於下列哪種攻擊手法？

(A) 重送攻擊

(B) 分割攻擊

(C) 中間人攻擊

(D) 路由迴圈攻擊

- 答案：(C)
- 解析：題目敘述為中間人攻擊。

（二）在物聯網裡，連網的智慧家電多數是採用安全性不高的通訊協定，駭客可藉此進行攻擊，下列何者不是這種利用通訊協定漏洞進行的攻擊手法？

(A) 中間人攻擊（Man-in-the-Middle）

(B) 劫持（TCP/IP Hijacking）

(C) 重播攻擊（Replay）

(D) 垃圾搜尋攻擊（Dumpster Diving）

- 答案：(D)
- 解析：題目敘述為垃圾搜尋攻擊。

（三）物聯網裝置採用低功耗藍牙通訊技術建立連線時，選用頻外配

對（Out-of-Band, OOB）是為了可以避免下列何種惡意攻擊？

(A) 緩衝區溢位（Buffer Overflow）

(B) 中間人攻擊（Man-in-the-Middle Attack）

(C) 重送攻擊（Replay Attack）

(D) 蟲洞攻擊（Wormhole Attack）

- 答案：(B)
- 解析：在電腦領域，頻外管理（Out-of-band management）是指使用獨立管理通道進行裝置維護。其允許系統管理員遠端監視和管理伺服器、路由器、網路交換機和其他網路裝置。獨立通道係為防範中間人攻擊。

（四）惡意駭客可以架設高功率的無線基地台，冒用相同的 SSID 名稱，來誘導使用者連線至偽冒的基地台，偷取使用者的登入帳號及密碼。下列何者為上述的攻擊方式？

(A) Rouge AP and Evil twin

(B) Sniffing

(C) MAC Address Spoofing

(D) Man in the Middle Attack

- 答案：(A)
- 解析：題目敘述為 Rouge AP and Evil twin。

（五）網路犯罪分子可能經由猜測密碼，而入侵網路或連到特定網路的設備，此為下列何種攻擊手法？

(A) 監聽攻擊（Sniffing Attack）

(B) 密碼攻擊（Password-Based Attack）

(C) 金鑰淪陷攻擊（Compromised-Key Attack）

(D) 阻斷服務攻擊（Denial-of-Service Attack）

- 答案：(B)
- 解析：題目敘述為密碼攻擊。

（六）網路犯罪分子可能竊取用來加密通訊的金鑰，並將之用於解譯加密過的資料，屬於下列何種攻擊手法？

(A) 監聽攻擊（Sniffing Attack）

(B) 密碼攻擊（Password-Based Attack）

(C) 金鑰淪陷攻擊（Compromised-Key Attack）

(D) 阻斷服務攻擊（Denial-of-Service Attack）

- 答案：(C)
- 解析：題目敘述為密碼攻擊金鑰淪陷攻擊。

（七）物聯網時代的來臨，有人提出「預防無用論（Perfect Prevention is Impossible）」，此一論點的主要見解為下列何者？

(1) 企業應永遠假設自身正在遭受攻擊

(2) 企業應儘可能地降低攻擊所帶來的衝擊與影響

(3) 企業絕對可以成功阻止針對性攻擊的入侵

(4) 企業應建立整體性的持續防禦流程

(A) (1), (2), (3)

(B) (1), (2), (4)

(C) (1), (3), (4)

(D) (2), (3), (4)

- 答案：(B)
- 解析：沒有任何資安防禦絕對可以成功阻止針對性攻擊的入侵。

（八）關於物聯網安全，下列敘述何者「不」正確？

(A) 政府與 IoT 開發商應協力降低 IoT 的安全風險問題

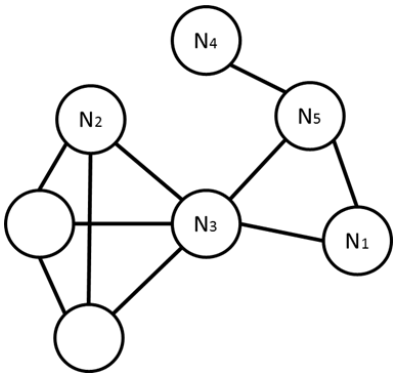
(B) 建立與利益相關人的風險意識

(C) 規劃出提升 IoT 安全的獎勵措施

(D) 不用建立損害侵權、保險補償、安全認證等措施

- 答案：(D)
- 解析：需要建立損害侵權、保險補償、安全認證等措施。

（九）在下圖中，只有節點 N5 具備有向外連網能力，其他節點皆必須透過節點 N5 才能與外界進行網際網路連結，請問當節點 N5 為絕對安全的情況下，哪個節點消失時對整體網路的影響最大？



(A) N1

(B) N2

(C) N3

(D) N4

- 答案：(C)
- 解析：N3 節點消失後，造成 3 個節點失效。

（十）攻擊者控制了物聯網其中一個節點，並丟棄（Drop）所有傳送至此節點的封包，此為下列何種攻擊手法？

(A) 黑函攻擊

(B) 分割攻擊

(C) 蟲洞攻擊

(D) 黑洞攻擊

- 答案：(D)
- 解析：題目敘述為黑洞攻擊。