ITE 資訊專業人員鑑定

資訊安全類-資訊與網路安全管理概論試題

試卷編號：ISN107

學科 100% （為單複選題，每題 2.5 分，共 100 分）

1.	以下針對光碟的長期保存方式描述，哪一個是對的？ （A）光碟只要置於承裝盒內後即可隨意置放，不需要特別的保存環境 （B）光碟雷射讀取面上的指印或灰塵不會干擾光碟的讀取 （C）為了區別方便，長期儲存用的光碟在標籤面可以黏貼標籤 （D）光碟必須保存在溫度較低且較乾燥的環境，並避免極端的環境波動
Ans：D	
2.	GPU 由 NVIDIA 公司在 1999 年 8 月首先提出的概念，可以提供強大的運算能力，讓複雜計算耗費較少時間即可完成。請問 GPU 的全名是？ （A）Gigabyte Processing Unit （B）General Processing Unit （C）Graphics Processing Unit （D）Geographic Processing Unit
Ans：C	
3.	現在電腦儲存容量愈來愈大，有些雲端網路甚致提供以 EB 為單位的儲存空間。請問 EB 的全名是？ （A）Extra Byte （B）Extend Byte （C）Excellent Byte （D）Exa Byte
Ans：D	

4.	企業允許員工攜帶自己的行動設備上班，這種作業方式稱之為？ （A）Electronic Business （B）Office Automation （C）Bring Your Own Device （D）Enterprise Resource Planning
Ans：C	
5.	以下哪些方法是屬於強調快速開發的軟體開發方法？**【複選】** （A）Agile Software Development （B）Extreme Programming （C）Scrum （D）System Development Life Cycle
Ans：ABC	
6.	下列有關系統管理行為的描述，哪一項是不適當的？ （A）使用者離職時，必須在規定時間內註銷使用者帳號 （B）隨時監視控制台，檢視是否有不明身分使用者企圖登入系統 （C）系統稽核檔（Log File）很多，有空再檢查是否有異常狀況即可 （D）定期備份資料，並確認備份資料是否放置於安全地方，以及是否加以管制
Ans：C	
7.	為避免資料隱碼（SQL injection）攻擊，開發人員於開發程式時應注意哪些事項？**【複選】** （A）對字串輸入加以過濾 （B）對字串輸入限制長度 （C）加強身分認證時之密碼長度 （D）避免使用 cookie
Ans：AB	

8. 在 ISO 27001:2013 資訊安全管理系統標準中，下列何者屬於系統獲取、開發及維護（System acquisition, development and maintenance）的控制項目？

（A）對程式源碼之存取控制（Access control to program source code）
（B）變更管理（Change management）
（C）系統變更控制程序（System change control procedures）
（D）技術脆弱性管理（Management of technical vulnerabilities）職務區隔（Segregation of duties）

Ans：C

9. 以下哪些是安全電子郵件系統？**【複選】**

（A）Pretty Good Privacy
（B）Privacy Enhanced E-Mail
（C）Secure Multipurpose Internet Mail Extensions
（D）Secure Socket Layer

Ans：ABC

10. 物聯網的架構有三層，不包含下最哪一項？

（A）Perception Layer
（B）Network Layer
（C）Application Layer
（D）Presentation Layer

Ans：D

11. 藍牙裝置使用者可以透過哪些措施來保護自己的隱私？**【複選】**

（A）將裝置設為隱藏模式
（B）不要和不認得的裝置配對，但是可以接收其傳送的內容
（C）使用八個字元以上且字母和數字混合的 PIN 碼
（D）利用軟體修補程式來防止安全問題

Ans：ACD

12. 使用網路瀏覽器上網時，如果在網址欄處出現如附圖 ，請問這表示以下哪一項？（請參閱附圖作答）

（A）這個網站不能使用 SSL 機制連線
（B）這個網站的網頁內含惡意程式
（C）https 連線毀損
（D）這個網站的 SLL 憑證未取得網路認證發放機構的認證

Ans：D

13. 以下針對零時差攻擊（Zero Day Attack）的描述哪些正確？
（A）當系統被發現具有風險性弱點後，立即進行的惡意攻擊行為
（B）當系統被惡意攻擊後，系統立即失效無法使用
（C）惡意攻擊系統的時間不超過 1 天
（D）當系統被發現具有風險性弱點後，在修正程式發佈之前或是使用者更新前，所進行的惡意攻擊行為

Ans：D

14. 某甲登入網路銀行時，依序輸入身分證字號、網路銀行帳號、網路銀行帳號密碼、以及由一次性密碼產製器產生的密碼。請問此種身分認證方式，稱之為？
（A）單因素認證
（B）雙因素認證
（C）三因素認證
（D）四因素認證

Ans：B

15. 下列哪兩項是 Bell & Lapadula 安全模式的重要法則？**【複選】**
（A）Simple Security Property
（B）*-Property
（C）Least Privilege
（D）Separation of Duties

Ans：AB

16. 電腦設備的環境安全管理包含多項因素，但是不包含以下哪一項？
（A）溫濕度
（B）防塵
（C）電壓
（D）場地租金

Ans：D

17. 企業資料備分的策略分為三種，下列何項不包含在內？
（A）Completely Backup
（B）Selective Backup
（C）Incremental Backup
（D）NoSQL Backup

Ans：D

18. 下列對 Single Sign-on 的解釋，何者正確？
（A）使用者在所有系統都設定同樣的一組帳號密碼以方便登入
（B）只需要單一的登入動作，就可以取得對於多個系統的存取權限
（C）使用者只需要在一台系統中設定帳號密碼，其他台系統都不需要設定帳號密碼
（D）使用者對任一個系統只需要成功登入一次，以後就不需要再登入即可使用此系統

Ans：B

19. 下列何者與會議連線劫持（session hijacking）無關？
（A）登入 Cookie 必須是唯一的，每個用戶均不相同
（B）跨站腳本攻擊（Cross-site Scripting）可造成連線劫持
（C）連線劫持跟偽冒的回應封包及檔頭有關
（D）入侵受害主機並提權後竄改所有連線封包

Ans：D

20. 下列關於跨站腳本攻擊(Cross-site Scripting)的描述，哪些正確？**【複選】**
（A）惡意腳本可能來自於使用者端的網址列 URL
（B）惡意腳本可能來自於伺服器端的資料庫
（C）惡意腳本可能來自於使用者端瀏覽器的 DOM（Document Object Model）
（D）惡意腳本可能來自於檔案輸入，即使是純文字檔（.txt）

Ans：ABCD

21. 某位伺服器管理者在檢視系統紀錄時，發現大量出現如附圖，類似訊息已連續出現幾日且仍在持續出現，來源位址都相同。請問下列發生何種事件的可能性最大？（請參閱附圖作答）

```
Mar 17 11:36:31 www sshd[13259]: Failed password
for root from 113.196.50.133 port 39136 ssh2
```

（A）該主機可能遭到暴力攻擊法（Brute-Force Attack）來猜測 ssh 服務的管理者密碼
（B）該主機可能遭到分散式阻斷攻擊法（DDoS Attack）來癱瘓網頁服務
（C）該主機已被入侵，正在對其他電腦進行暴力攻擊法（Brute-Force Attack）來猜測 ssh 服務的管理者密碼
（D）該主機已成為殭屍電腦的成員，正在對 113.196.50.133 的電腦進行 ssh 連線

Ans：A

22. 附圖為某組織連外線路的流量紀錄，經由數據分析，組織內部的機器發生何種事件的可能性最大？（請參閱附圖作答）

序號	內部電腦	埠號	外部電腦	埠號	協定	流入Bytes	流出 Bytes
…	…	…	…	…	…	…	…
3351	172.17.123.111	39133	168.95.1.1	3030	TCP	0	82
3352	172.17.123.111	39134	168.95.1.1	3031	TCP	0	82
3353	172.17.123.111	39135	168.95.1.1	3032	TCP	0	82
3354	172.17.123.111	39136	168.95.1.1	3033	TCP	0	82
3355	172.17.123.111	39137	168.95.1.1	3034	TCP	0	82
3356	172.17.123.111	39138	168.95.1.1	3035	TCP	0	82
3357	172.17.123.111	39139	168.95.1.1	3036	TCP	0	82
3358	172.17.123.111	39140	168.95.1.1	3037	TCP	0	82
3359	172.17.123.111	39141	168.95.1.1	3038	TCP	0	82
3360	172.17.123.111	39142	168.95.1.1	3039	TCP	0	82
3361	172.17.123.111	39143	168.95.1.1	3040	TCP	0	82
…	…	…	…	…	…	…	…

（A）組織內部機器對外進行位址掃瞄（IP Scan）
（B）組織內部機器對外進行通訊埠掃瞄（Port Scan）
（C）組織內部機器對外進行阻斷攻擊（DoS Attack）
（D）組織內部機器對外進行分散式阻斷攻擊（DDoS Attack）

Ans：B

23.	某甲存放在電腦系統裏的公務資料無任何資訊安全保護，被某乙利用隨身碟複製竊取，請問某乙的行為違反下列哪一項資訊安全基本需求？ （A）Confidentiality （B）Integrity （C）Non-Repudiation （D）Accountability
Ans：A	
24.	稽核是用來幫助系統管理者追查可疑的行為，但是不包括下列哪一項目標？ （A）確保所有的運作均能按照既定的安全政策執行 （B）確保所有資料的存取都要經過授權 （C）確保所有資料的正確性 （D）確保爭取到足夠的資訊安全經費
Ans：D	
25.	資通安全辦公室於民國 104 年修正之「資訊系統分級與資安防護基準作業規定」中明定，「全球資訊網」必須符合智慧財產權相關法令尊重他人智慧財產，以及遵守哪一項法律進行資訊內容管理，否則將涉及違反法律之遵循性？ （A）政府採購法 （B）國家機密保護法 （C）醫療機構電子病歷製作及管理辦法 （D）兒童及少年福利與權益保障法
Ans：D	
26.	資訊倫理是在討論人們對資訊的態度以及行為，應用於電腦的使用、資訊科技、資訊系統、資訊網路的倫理規範。下列哪一項不包含在資訊倫理的四大議題（PAPA）之中？ （A）Privacy （B）Availability （C）Property （D）Accessibility
Ans：B	

27.	資訊倫理是在討論人們對資訊的態度以及行為，應用於電腦的使用、資訊科技、資訊系統、資訊網路的倫理規範。下列哪些議題是在資訊倫理討論的範圍之內？**【複選】** （A）網路禮節 （B）網路安全 （C）網路侵權行為 （D）網路色情氾濫
Ans：ABCD	
28.	下列哪些措施不能預防勒索病毒侵入公司電腦系統？ （A）啟用郵件內容過濾代理伺服器 （B）增加資料備分的次數 （C）以密碼上鎖電腦系統裏的特定功能 （D）加強員工警覺性訓練
Ans：B	
29.	下列哪些是屬於國內危機處理暨協調中心（Computer Emergency Response Team）組織？**【複選】** （A）TWNCERT （B）EC-CERT （C）NCC-CERT （D）TWCSIRT
Ans：ABCD	
30.	在網路新聞或消息未有完整說明前，任意和他人一起在網路上出言不遜謾罵當事人，此舉可能構成何項網路犯罪行為？ （A）網路誹謗與公然侮辱 （B）網路煽惑他人犯罪 （C）網路詐欺 （D）網路恐嚇
Ans：A	

31. 某甲工作表現優異，依據個資法第 20 條利用規定，基於人事管理之特定目的，公司是否可以在公佈欄上替某甲張貼榮譽榜，何者正確？
（A）公司可以張貼榮譽榜，且不需要事先取得某甲的同意
（B）公司可以張貼榮譽榜，但是需要事先取得某甲的同意
（C）公司不可以張貼榮譽榜，以避免洩漏某甲的個資
（D）這是某甲的私事，公司不需要張貼榮譽榜

Ans：A

32. 工商憑證是公司、分公司、有限合夥或商業用來作為網路上身分驗證用，並提供相關安全認證服務，以保障使用者權益。請問工商憑證管理中心（MOEACA）是隸屬於哪一個單位？
（A）行政院
（B）內政部
（C）經濟部
（D）國土安全辦公室

Ans：C

33. 憑證機構針對金鑰生成參數與參數品質的安全控管，依法應於何種文件中載明？
（A）風險評鑑報告（risk assessment report）
（B）資產清單（inventory of assets）
（C）憑證實務作業基準（certification practice statement）
（D）適用性聲明書（statement of applicability）

Ans：C

34. 在 ISO 27001:2013 的規範中，對許多控制項目進行了大幅調整與修改。下列何者被仍列入網路安全管理（Network security management）的控制項目？
（A）網路區隔（Segregation in networks）
（B）網路設備識別（Equipment identification in networks）
（C）網路連線控制（Network connection control）
（D）網路選路控制（Network routing control）

Ans：A

35. 在資訊安全管理系統中，風險評鑑（Risk Assessment）是個重要的環節。下列哪些項目屬於風險評鑑？**【複選】**

（A）風險識別（Risk Identifiy）
（B）風險分析（Risk Analysis）
（C）風險評估（Risk Evaluation）
（D）風險處理（Risk Treatment）

Ans：ABC

36. 下列何種方法是預防社交工程攻擊的最好方法？

（A）教育訓練及宣導
（B）安裝入侵偵測與防禦系統（IDPS）
（C）安裝網站過濾伺服器
（D）安裝端末管理機制

Ans：A

37. 為貫徹「資安即國安」戰略—提高資安主導層級之重要策略，105 年 8 月 1 日成立資安專責單位—資通安全處，擔任資安會報的幕僚單位。請問資通安全處是隸屬於哪一個單位？

（A）行政院
（B）內政部
（C）法務部
（D）國土安全辦公室

Ans：A

38. ISO27001 透過 PDCA 四個程序來建立、實施、監控、審查、維護、及改進組織的資訊管理系統。請問以下何者不在 PDCA 程序之中？

（A）Plan
（B）Do
（C）Check
（D）Audit

Ans：D

39.	Using Components with Known Vulnerabilities 是列於 OWASP 在 2017 年提出的十大網站安全風險之中，以下哪一項措施無法避免此項威脅？ （A）移除系統不需要的元件（component） （B）隨時檢核元件（component）是否具有新的弱點 （C）為了方便，可以從任意網站下載系統開發所需要的程式庫（library） （D）避免使用缺乏安全更新的程式庫（library）
Ans：C	
40.	何者不是區塊鏈的特徵？ （A）去中心化 （B）開放性 （C）安全性 （D）無匿名性
Ans：D	