

資訊安全講義

第一回

60762A-1



社團 考友社 出版
法人 發行

資訊安全講義 第一回



第一講 字彙.....	1
命題大綱.....	1
重點整理.....	2
一、資訊與資通安全概論.....	2
二、資訊安全法律與倫理.....	20
精選試題.....	31

第一講 資訊安全與資通安全



- 一、資訊與資通安全概論
 - (一)資訊安全
 - (二)資通安全
- 二、資訊安全法律與倫理
 - (一)智慧財產權
 - (二)網際網路相關的法律
 - (三)電腦鑑識與數位證據
 - (四)資訊倫理



一、資訊與資通安全概論

(一)資訊安全：

1. 資訊安全注重的三類資料：

- (1)機密資料：指軍事、情報、以及有關國家安全之資料。
- (2)敏感資料：指政府、機構、企業等具敏感性之資料。
- (3)正確資料：保護該資料之正確性及有效性，禁止該資料被破壞、偽造以及篡改其中機密及敏感資料，只允許經授權的人存取，禁止非經授權者存取或閱讀。

2. 資訊安全的威脅：

(1)資訊安全的目的：

在於保護各企業及機關單位所有資訊系統資源，其應注意的事項如下：

- ①防止未經授權者得到有價值的資訊。
- ②防止未經授權者偷竊或拷貝軟體。
- ③避免電腦資源被盜用。
- ④避免電腦設備受到災害的侵襲。

(2)資訊安全重要事件：

- ①1994 年，一位俄國電腦專家利用網路進入美國花旗銀行自動轉帳電腦系統，竊取一千多萬美元的客戶存款，並轉存到國外帳戶。
- ②1996 年，某知名公司遭離職員工網路入侵篡改其積體電路佈局資料，導致生產出錯誤晶片，除了增加生產成本，也延誤交貨，影響企業商譽。
- ③1999 年 4 月，電腦駭客控制英國的一枚軍事通信衛星，並更改衛星路線。同年八月，國內監察院、營建署、勞委會及部分縣市政府等機構網站，陸續遭駭客入侵篡改網頁內容。
- ④2000 年 8 月，駭客陸續攻擊 Yahoo 及其他知名網站，導致網站無法提供正常服務，此攻擊稱為阻斷服務（Denial of Service；Dos），從此網路安全專家將開始關注 DoS 問題。

- ⑤2001年3月，亞馬遜網路書店的網站遭到入侵，被竊取近10萬筆顧客信用卡資料。同年9月，Nimda病毒肆虐全球電腦，癱瘓了220萬台電腦，估計全球損失的維修費高達五億美元，其他無形之損失則難以估算。

(3)資訊安全威脅的種類：

所有影響資訊安全而導致不能妥善保護資訊系統的資源，都將成為資訊安全的威脅，必須加以防範，資訊安全威脅的種類如下所示：

①天然或人為：

A.天然的安全威脅：

此種威脅是由於天然災害的發生，導致資訊本身或存取管道遭到破壞。

(A)常見的天然災害有：颱風、地震、水災、火災等，這些因素皆會對資訊系統造成直接性的破壞。

(B)在傳送資料的過程中，也可能因為打雷閃電，而造成傳輸時的干擾與資料改變等問題。

(C)不同災害對資料將造成不同程度的破壞。

B.人為的安全威脅：

此種威脅是由於人為的因素，導致系統的安全受到威脅及攻擊。

②蓄意或無意：

A.蓄意的安全威脅：

(A)是指駭客企圖破解資訊系統安全，其主要目的：

a.想從中獲取不當的利益，使用者利用專業知識或智慧，不斷地向電腦系統安全上的漏洞進行探測摸索。

b.為了測驗本身的能力，而後才轉為非法存取電腦資源，但是，這些行為已觸犯法律。

c.惡意地竊取電腦的服務，奪取重要機密或破壞資料。

(B)不易防範的原因：

在資訊安全威脅中，最不易防範的就屬蓄意的安全威脅。因為這關係到人的因素，變異最大，就算再精良的電腦設備，也無法預估攻擊者的思考模式與行為。所以，這方面的安全威脅最難克服。在此項破壞中，包含許多目前大多數人所熟知的破壞行為，如電腦病毒、駭客及其他電腦犯罪等。

B.無意的安全威脅：

由於系統管理不良或系統管理員的疏忽，導致系統出現安全上的漏洞，舉例說明如下：

- (A)架設電子商務網站時，爲了讓外界的使用者可以瀏覽網頁，而把網頁檔案權限開放爲唯讀，如果系統管理員不小心將目錄或檔案的權限開放成所有人都可以讀寫，那麼此網站將很容易被入侵。
- (B)架設 NT 伺服器或 MS SQL 伺服器時，系統管理員經常會忘記更改預設的超級使用者密碼，使得駭客輕易地就可以取得系統的控制權。許多安全問題是在正常的操作行爲下無意間發生的，這些可能危及系統安全的缺失，大部分是由於使用者的訓練不足及疏忽所引起的。

註：NT 與 MS SQL 的超級使用者 ID 及通行密碼均爲 Administrator。

③主動或被動：

駭客的攻擊可分爲主動攻擊與被動攻擊兩種。

A.主動攻擊：

- (A)主動攻擊是利用大量封包傳送，癱瘓受害者的電腦或伺服器、篡改傳送中的封包資料、傳送假的訊息給另一個具有利益關係的受害者，造成其財務上或精神上的損失。
- (B)主動的安全威脅行爲，會破壞或篡改資訊系統之資料，導致使用者無法正常取得資料或是得到的資料是經過篡改的。

B.被動攻擊：

- (A)被動攻擊是指在雙方傳輸的過程中，竊取資訊或是在他人的電腦中植入木馬程式，在不讓傳輸者發覺的情況下，直接取得電腦中的資源及機密文件。
- (B)被動的安全威脅行爲並不會更改資訊系統資料，駭客的主要目的是要窺探機密資料，以獲取不當利益或僅得知別人之隱私。

④實體或邏輯：

A.威脅對象的差異：

- (A)實體的安全威脅：對象爲實際存在之硬體設備。
- (B)邏輯的安全威脅：對象爲資訊系統上之資料。

B.典型的實體安全威脅是歹徒直接侵入電腦機房，以鐵鎚或其他方式破壞電腦設備，使其不能正常運轉。

- C. 電腦硬體經過長期使用，會造成硬體物理性的彈性疲乏及損壞。若無適當的保養，容易導致運算錯誤，造成決策失誤。
- D. 電腦軟體所產生的錯誤很容易從模擬結果得知，但硬體產生的問題則不易偵測出來。其他儲存硬體損毀，則會發生重要資料遺失等問題。

3. 基本的資訊安全需求：

資訊安全的目的，在於防止影響資訊安全的威脅。一套完善的安全性資訊系統，需具備的特性為：保密性、完整性、鑑別性、可用性、不可否認性、存取控制以及稽核，茲分述如下：

(1) 保密性或機密性：

機密性資料內容不能被未經授權者所竊知，僅能由被授權者存取，以確保資訊的機密，並防止機密資訊洩漏給未經授權的使用者。其中存取的種類包含：讀出、瀏覽、列印。

① 保密性存在的意義：

- A. 資料是否存在於系統是一項很重要的資訊，必須加以保密，不得直接或間接被不法人士獲得。
- B. 一旦資料經過轉遞的動作，就會存在著訊息內容被取得的風險，尤其是組織的決策文件、職員薪資或國家機密資料等，所以保密性很重要。
- C. 保密性的存在是爲了確保資料訊息不會遭受到第三者偷窺或竊取。

② 預防的方法：

可透過資料加密的程序，達到確保資料傳輸隱私的目標。

③ 忽略保密性的影響：

對於國防機要政策、企業的行銷策，若是忽略此需求將造成的後果如下：

- A. 國家安全遭受威脅，人民生活將陷入恐慌。
- B. 在企業行銷，將可能受到同業阻礙，或是對手利用竊取所得的資訊，率先搶得市場。

(2) 完整性：

- ① 資料內容僅能被合法授權者更改，不能被未經授權者篡改或偽造。其中更改的內容包括：新增、更正、更新、刪除等。
- ② 資料完整性必須確保資料傳輸時不會遭受篡改，以保證資料傳輸內容之完整性。



精選試題

一、一般資訊安全注重的資料有那些？

答：(一)機密資料：指軍事、情報、以及有關國家安全之資料。

(二)敏感資料：指政府、機構、企業等具敏感性之資料。

(三)正確資料：保護該資料之正確性及有效性，禁止該資料被破壞、偽造以及篡改其中機密及敏感資料只允許經授權的人存取，禁止非經授權者存取或閱讀。

二、哪些行為將造成蓄意的安全威脅？

答：(一)想從中獲取不當的利益，使用者利用專業知識或智慧，不斷地向電腦系統安全上的漏洞進行探測摸索。

(二)爲了測驗本身的能力，而後才轉爲非法存取電腦資源，但是這些行爲已觸犯法律。

(三)惡意地竊取電腦的服務，奪取重要機密或破壞資料。

三、如何區分實體與邏輯的安全威脅？

答：(一)實體的安全威脅：對象爲實際存在之硬體設備。

(二)邏輯的安全威脅：對象爲資訊系統上之資料。

四、試述管理資訊系統的基本架構及其演進過程。

答：(一)管理資訊系統的架構：

一般包含管理資訊系統、電腦作業系統以及資料庫管理系統。

(二)單機版資訊系統：

1. 大部分的管理資訊系統都會透過資料庫管理系統維護資料。
2. 早期的管理資訊系統與資料庫系統在同一台電腦。

(三)主從式或三層式架構：

1. 由於機關、企業之規模龐大且地點分散各地，資訊系統已由原先單機版系統擴展爲主從式或三層式架構。
2. 資料庫不需要與管理資訊系統位在同一台主機。反之，可以分散在不同主機系統上，可透過區域網路或網際網路存取分散在各地的資料。

五、資訊安全防範對策的實施應從哪此層面做起？

答：(一)管理層面：為確保資訊安全，訂立安全管理政策、規範與程序，以及人員進用管理，或機房管制等程序。

(二)技術層面：採用系統存取控制、防火牆、滲透測試系統、防毒軟體等。

(三)實體層面：整體環境控制、地震、火災、風災、水災及盜竊等人為破壞等控制機制。

六、解釋下列名詞：

(一)智慧財產權。

(二)著作權。

(三)專利權。

答：(一)智慧財產權：

包括商標權、專利權、著作權與營業秘密法等，是透過立法以保護這些人類精神智慧的產物，賦予創作人專屬享有之權利

(二)著作權：

主要是保護作者的權益，未經授權不得任意複製與使用。原則上，著作者完成著作時即取得著作權，不需要任何形式之申請與聲明。著作權是不分年齡的，任何年紀完成之作品均享有著作權。

(三)專利權：

是對發明授予的權利，對專利權人之發明予以保護，保護權利在一段期間內有效，一般期限為 20 年。

七、何謂競業禁止？

答：競業禁止是勞動者在勞動契約存續中，曾參與顧客、來源、製造、與銷售過程等機密，運用此機密對雇主可能會造成重大危險或損失。在勞動契約結束後，給予該勞動者禁止競業的義務。

八、試述資訊安全威脅的種類。

答：(一)天然或人為的安全威脅。

(二)蓄意或無意的安全威脅。

(三)主動或被動功擊。

(四)實體或邏輯的安全威脅。

九、試述資訊安全的範疇。

答：(一)資料庫安全。

(二)作業系統安全。