網路安全與資訊倫理講義

第　一　回

607630-1

社團法人 考友社 出版發行

網路安全與資訊倫理講義　第一回

目錄

第一回（1/2）
第一講　資訊與網路安全…… 1
命題大綱…… 1
重點整理…… 2
一、資訊安全…… 2
二、網路安全…… 12
三、資訊管理…… 32
四、網路管理…… 44
第一回（2/2）
第二講　網路資訊倫理…… 1
命題大綱…… 1
重點整理…… 2
一、資訊倫理與法律…… 2
二、資訊隱私…… 14
三、資訊智慧財產權…… 20

第一講　資訊與網路安全

命題大綱

一、資訊安全
- ㈠資訊安全與資訊系統
- ㈡資訊安全的威脅與風險
- ㈢資訊安全的基本需求
- ㈣資訊安全的範疇
- ㈤資訊系統的安全分析
- ㈥資訊安全的防範對策

二、網路安全
- ㈠網路安全的概念
- ㈡OSI 參考模式
- ㈢TCP/IP 通訊協定
- ㈣網路安全的威脅

三、資訊管理
- ㈠資訊安全管理規範
- ㈡資訊安全管理運作模式
- ㈢資訊安全管理系統
- ㈣風險管理
- ㈤內部稽核控制

四、網路管理
- ㈠網路管理系統
- ㈡簡易網路管理協定

重點整理

一、資訊安全

㈠資訊安全與資訊系統：

1.資訊安全的意義：

⑴資訊安全威脅是一個複雜的問題，並非靠購置單一的軟、硬體資安設施即可解決。資訊安全防護是全面性的工作，需要綜合管理、技術與實體層面，才可達到目標。

⑵目前資訊安全管理普遍採用 BS7799 爲標準規範，BS7799 是英國標準協會制定之資訊安全管理系統標準。實施 BS7799 的目的是遵照資訊安全管理標準，建立完整的資訊安全管理體系，以達到動態的、系統的、全員參與的、制度化的、以預防爲主的資訊安全管理方式，並用最低的成本獲得較高的資訊安全，從根本上保證業務的連續性。

2.資訊系統的架構：

⑴從資訊安全角度，電腦系統的架構可分成六大層：

①外圍層（Environment Layer）：

外圍層牽涉到有關電腦系統周邊外圍的環境因素。

②外部層（External Layer）：

外部層是使用者與系統間的介面層次，所牽涉到的是個別使用者所能操作的系統。每位使用者所關注或授予的權力不盡相同，因此外部層依使用者性質分成許多不同介面。

③中心層（Central Layer）：

中心層是內部層與外部層的溝通橋樑，代表整個系統的安全核心。

④內部層（Internal Layer）：

內部層牽涉到資料實際儲存及管理的方式。

⑤分析層（Analysis Layer）：

分析層牽涉到系統之管理與安全威脅的分析。

⑥法律層（Law Layer）：

法律層牽涉到有關資訊安全相關的法律條文。

⑵對應電腦系統架構的資訊安全領域及其技術：

①實體安全（Physical Security）：

外圍層以實體安全技術爲主軸，實體安全是電腦系統安全重要的一環，各機關的資訊中心安全防護措施不盡相同，平時電腦機房人員與主管應定期做各種狀況的處理演練及預防，並隨時檢討改進安全上的措施。

②身分鑑別（User Authentication）：

外部層以使用者身分鑑別技術爲主軸，以確實驗明合法使用者之身分，通常這類技術有通行密碼技術（Password）、IC 識別卡、指紋識別以及手寫簽名技術。

③存取控制（Access Control）：

中心層以任意性存取控制及多層性存取控制二類爲主軸。早期資訊安全大多著重在任意性存取控制，但由於此種控制方式並不能有效控制資訊流向（Information Flow）及顆粒性（Granularity）問題。基本上，系統應該允許使用者存取到資料內某一基元（Atomic）資料，此類控制方式稱爲強制性存取控制或多層性存取控制。

註：A.資訊流向問題：

系統很難掌握資訊流向，一旦某資訊擁有者將部分或全部權力授予他人後，就很難再控制此資訊，因爲此資訊之權力很可能被授予者再轉遞予第三者。

B.顆粒性問題：

資料安全性的強弱。

④密碼學（Cryptography）：

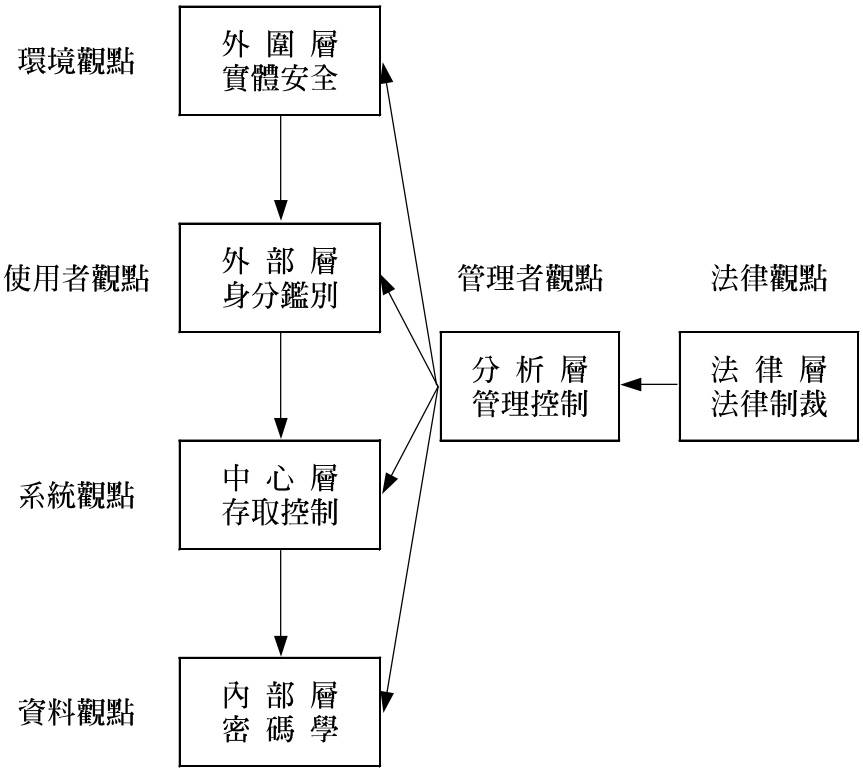
內部層是以密碼學技術爲主軸，相關的技術包括祕密金鑰加解密技術、公開金鑰加解密技術、數位簽章技術、金鑰管理、祕密安全會議、通訊安全、網路安全、電子商務交易安全、安全電子投票系統以及訊息確認技術等。

⑤管理控制（Management Control）：

分析層屬於預防型及補償型安全性技術。積極而言，是要找出可能影響安全威脅之要因，以預防系統之安全受到威脅。主要技術包括電腦病毒、祕密通道（Covert Channel）、推論（Inference）等。消極而言，當安全性受到威脅後做事後追蹤及補償，主要有安全稽核（Audit Control）技術。

⑥法律制裁：

在技術面及管理面都沒有辦法防範入侵事件下，只好使用最後的手段，以法律制裁，收嚇阻之效。



圖(一)　電腦資訊系統的架構

㈡資訊安全的威脅與風險：

1.威脅（Threat）：

⑴威脅的定義：

資訊會遭受到潛在的與可能的危害，這即是資訊安全的威脅。

⑵威脅的來源：

①環境因素：

包含地震、颱風、水災等天然災害。

②外部人員：

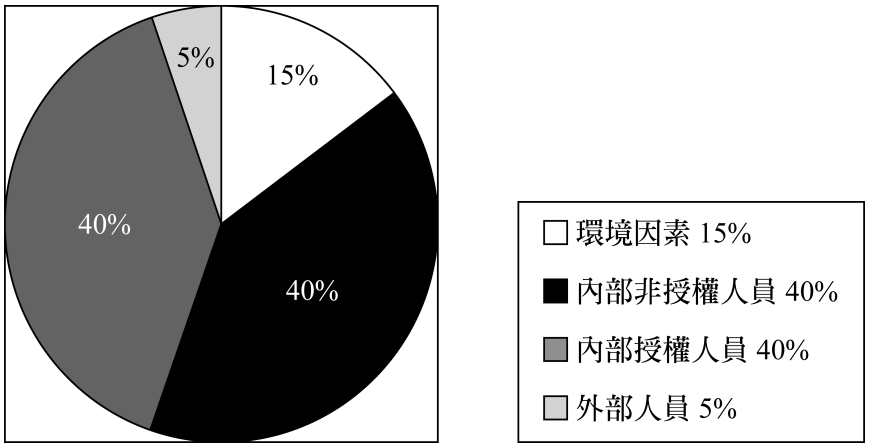
如駭客、病毒等，需要使用防火牆、入侵偵測系統（IDS）或防毒軟體加以防範。

③內部授權人員：

可能是由於作業疏忽或惡意竊取資源。

④內部非授權人員：

是指非授權人員企圖竊取公司的資源。



圖㈡　資訊安全的威脅來源

2.風險（risk）：

⑴由於有潛在的威脅，因此系統比較脆弱的部份會形成系統的弱點（Vulnerability）。弱點會導致風險提高，風險提高對於有形與無形資產將造成損害。

⑵將風險量化，對於因災害發生而直接受到影響的資產稱爲「風險暴露」，風險暴露之資產，需要實施相關的安全措施。

㈢資訊安全的基本需求：

資訊安全的目的，即在防止影響資訊安全的威脅。基本上，一套好的安全性資訊系統，需要具備下列七個特性：

1.保密性或機密性（Confidentiality）：

⑴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。存