Chapter 1

資訊安全簡介

1-1 前 言

- 資訊科技不但為人類帶來便利生活，也顛覆企業的傳統思維，更帶動數位服務的蓬勃發展。我們在享受這些科技帶來的便利之餘，卻常常忽略了這些科技背後所潛在的安全問題。
- 要如何保護在網路中傳遞及儲存於電腦系統或雲端伺服器 (Cloud Server) 之機密資料，免於遭受未經授權人員之竊取、篡改、偽造及破壞等不法行為之威脅，則是雲端服務時代當務之急。

1-1 前 言

- 資訊安全通常注重三類資料：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。
  - ✓機密資料，是指軍事、情報及有關國家安全之資料統稱。
  - ✓而敏感資料是指政府、機構及企業等具敏感性之資料。
  - ✓正確資料則是保護該資料之正確性及有效性，禁止該資料被破壞、偽造及篡改。

1.2 資訊安全的威脅

- 資訊安全的目的即在保護各企業及機關單位所有資訊系統之資源：
  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與資料。
  3.避免電腦資源（ 例如，中央處理機、 記憶體、 磁碟機及印表機等 ）被盜用。
  4.避免電腦設備受到災害的侵襲。

1.2 資訊安全的威脅

- 威脅資訊安全分類如下：

1.天然或人為

天然的安全威脅起因於天然災害。

人為的安全威脅則是起因於人為的因素，管理人員的疏失或是系統人員的蓄意破壞。

2.蓄意或無意

蓄意的安全威脅是指駭客企圖破解資訊系統之安全。

無意的安全威脅則是導因於系統管理不良或系統管理員的疏忽。

1.2 資訊安全的威脅

3.主動或被動

被動的安全威脅行為並不會更改資訊系統的資料，主動的安全威脅行為則會破壞或篡改資訊系統之資料。

4.實體或邏輯

實體的安全威脅，對象為實際存在之硬體設備；邏輯的安全威脅，對象則為資訊系統上之資料。

1.3 資訊安全的基本需求

- 根據 ISO 27001 資訊安全管理系統 (Information Security Management System, ISMS) 的規範，系統必須對其機密性、完整性及可用性作適當的風險管理。

1.機密性

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。存取，包括讀取、瀏覽及列印。另外「資料是否存在於系統」也是一項很重要的資訊。

可透過資料加密的程序達到此目標。

1.3 資訊安全的基本需求

2.完整性

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。

資料完整性必須確保資料傳輸時不會遭受篡改。

3.可用性

確保資訊系統運作過程的有效性，以防止惡意行為導致資訊系統被毀壞(Destroy) 或延遲使用 (Prolong)。

1.3 資訊安全的基本需求

- 系統視其應用的範疇可能還需要以下特性來滿足其對資訊安全的要求。

1.鑑別性 (Authentication)

鑑別性包括身分鑑別 (Entity Authentication) 及資料 (或訊息) 來源鑑別 (Data or Message Authentication) 。

訊息來源鑑別是要能確認資料訊息之傳輸來源，以避免惡意的傳送者假冒原始傳送者傳送不安全的訊息內容。一般均利用**數位簽章**或**資料加密**等方式，來解決訊息的來源鑑別問題。

使用者身分的識別，系統必須快速且正確地驗證身分。通常使用者身分鑑別的時效性比起訊息來源鑑別要來得重要。

1.3 資訊安全的基本需求

2.不可否認性 (Non-Repudiation)

在資訊安全需求中，對於傳送方或接收方，皆不能否認曾進行資料傳輸、接收及交易等行為，意即傳送方不得否認曾傳送某筆資料，而接收方亦無法辯稱未曾接收到某訊息資料。

數位簽章 (Digital Signature) 及**公開金鑰**基礎架構 (Public Key Infrastructure, PKI) 對使用者身分及訊息來源做身分鑑別及資料來源鑑別，並可再與使用者在系統上的活動進行連結，以達權責歸屬及不可否認性。

1.3 資訊安全的基本需求

3.存取控制 (Access Control)

資訊系統內每位使用者依其服務等級，而有不同之使用權限。服務等級愈高者，其權限愈大；相反地，服務等級愈小者，其權限愈小。

存取控制主要是根據系統之授權策略，對使用者做授權驗證，以確認是否為合法授權者，防止未經授權者存取電腦系統及網路資源。

1.3 資訊安全的基本需求

4.稽核 (Accountability)

資訊系統不可能達到絕對安全，也就是不可能百分之百的安全。

必須藉由稽核紀錄 (Audit Log) 來追蹤非法使用者，一旦發生入侵攻擊事件，除了可以回復系統 (Recovery) 外，也可以盡快找到發生事件之原因，進而提出偵測此類入侵的方法，以防止系統再一次被入侵。

1.4 資訊安全的範疇

- 資訊安全的領域相當廣泛，確保資訊系統正常運作及確保機密資料之機密性與完整性的機制都是資訊安全的範疇。

圖 1.1　管理資訊系統的一般架構

1.4 資訊安全的範疇

- 整體架構之操作環境的安全問題。

1.使用者

系統的使用者可能是組織中的員工或顧客。

2.操作介面

對於不同等級的使用者，必須提供不同的頁面。

3.後端處理程式

負責處理回應使用者所要求的服務，若使用者要取得資料庫中的資料，也必須透過此系統元件存取。後端處理程式可說是系統中之靈魂。

4.資料庫

負責保存重要資料與一般資料。依據不同需求，有不同的資料格式與儲存方式。

1.5 資訊系統的安全分析

1.弱點分析 (Vulnerability Analysis)

對整個系統架構進行了解及測試，包括系統架設哪些硬體、使用哪些通訊協定、安裝哪些應用軟體、哪些人會使用本系統、授權哪些權限給使用者等。管理者了解這些資訊後，進而分析系統的弱點在哪裡、哪些人可能會進行攻擊、目的為何、以及要攻擊哪些地方。

1.5 資訊系統的安全分析

2.威脅分析 (Threat Analysis)

了解系統的弱點之後，進而要分析系統可能遭受的安全威脅及攻擊。常見入侵並危及系統安全的方式，包含利用電子郵件、遠端登入、施放電腦病毒、試圖得到具有高存取權限的帳號、刪除或移動檔案等。

有關電腦網路安全相關威脅及事件，美國電腦網路危機處理暨協調中心 (Computer Emergency Response Team/Coordination Center ，網址 https://www.cert.org/ 及臺灣電腦網路危機處理暨協調中心 (TWCERT/CC) ，網址 https://www.twcert.org.tw/) 。

1.5 資訊系統的安全分析

3.對策分析 (Countermeasure Analysis)

針對上述弱點及所面臨的安全威脅，研擬安全策略及所需的安全機制。例如，存取控制、使用者認證、加密及數位簽章等。

1.5 資訊系統的安全分析

4.風險分析 (Risk Analysis)

評估及分析系統的風險，對於部分重要資料必須採取進一步的防護。

例如，定期做備份及回復處理等，在系統發生安全問題時可確保重要資料的正確性，降低問題發生時所帶來的風險及損失。

因安全漏洞所造成的損失分為有形損失及無形損失。

1. 有形損失包括硬體與軟體設備、人力成本、雜支成本及其他因工作延宕所造成之損失；
2. 無形損失則是指公司形象受到影響，其損失費用無從計算。
3. 通常投資在資訊安全之費用，應小於系統發生安全漏洞後所造成之損失，但要大於其損失的十分之一。例如，若預估之系統發生安全事件，所造成之損失為 1,000 萬元，那麼所投資之成本就應在 100 萬與 1,000 萬元之間。

1.5 資訊系統的安全分析

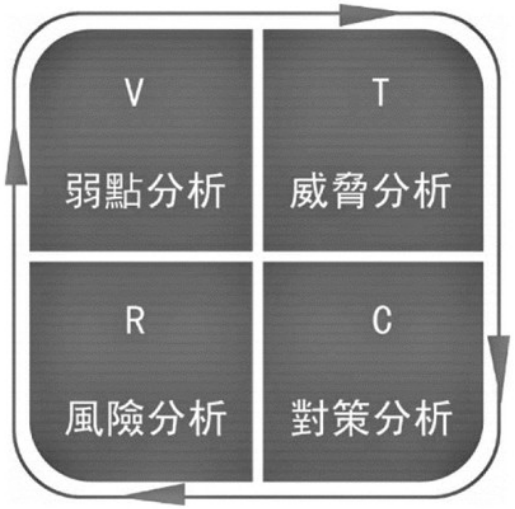

圖 1.2　資訊系統的四種安全分析

1.6 安全的資訊系統架構

圖 1.3　電腦系統的架構之六個安全性層次

1.6 安全的資訊系統架構

- 外圍層牽涉到有關電腦系統外圍的周邊環境因素。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。
- 中心層是內部層與外部層的溝通橋樑，內部層牽涉到資料實際儲存及管理的方式。分析層牽涉到系統之管理與安全威脅的分析。法律層則是牽涉到資訊安全相關的法律條文。

1.6 安全的資訊系統架構

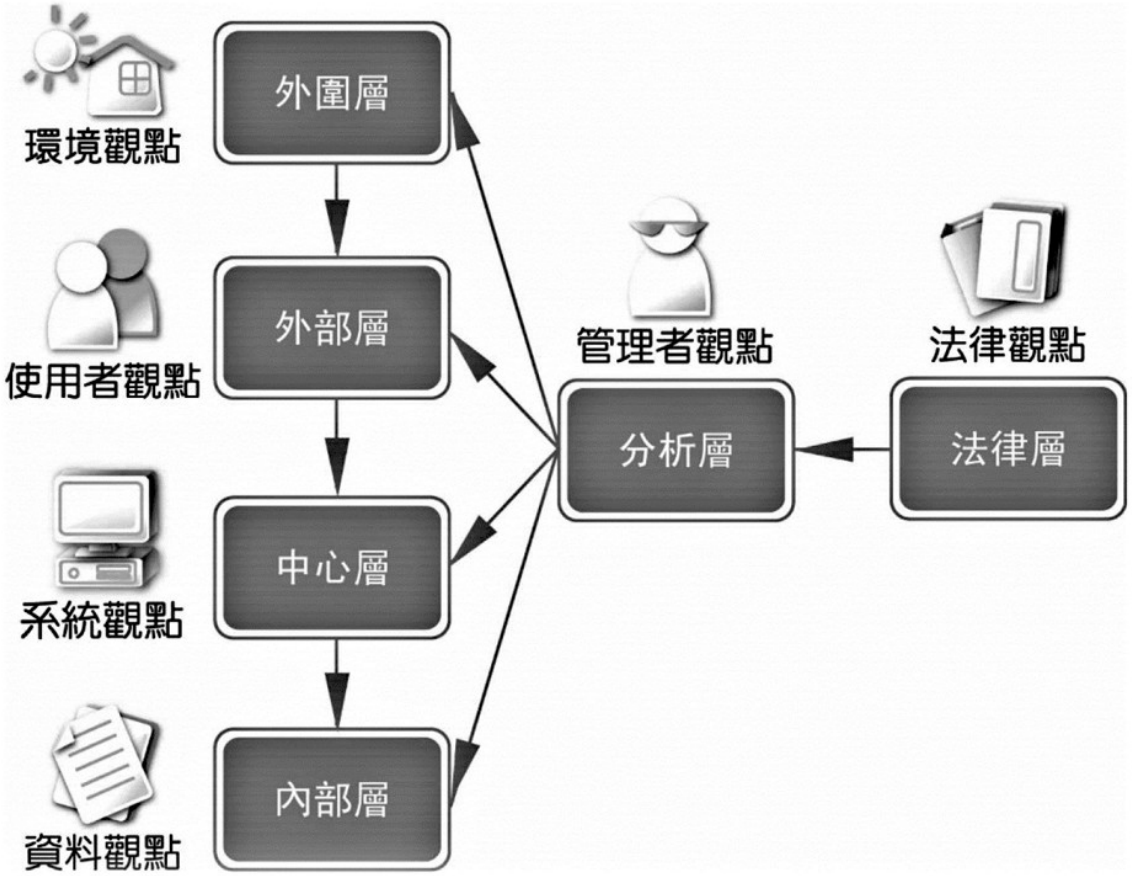

圖 1.4　以不同的觀點來看電腦系統之六個安全性層次

1.6 安全的資訊系統架構

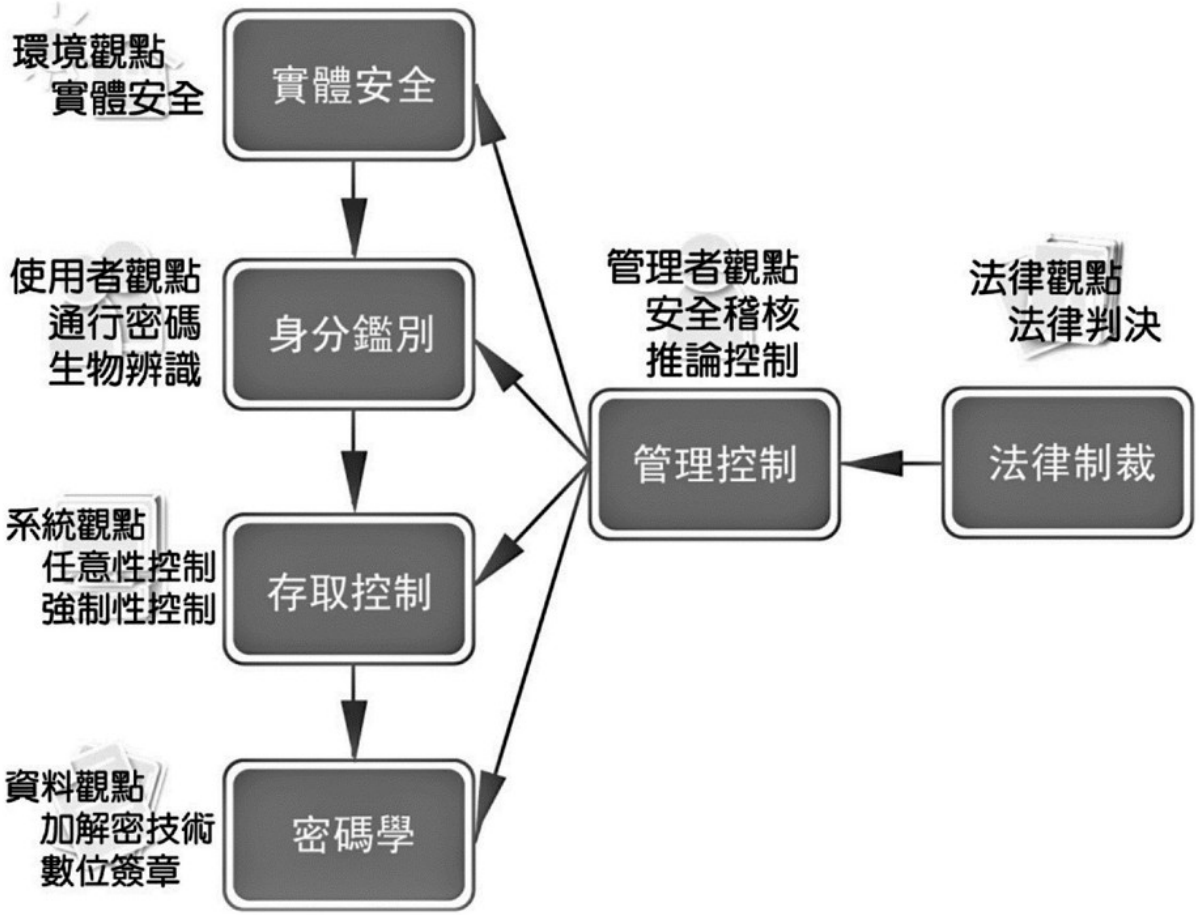

圖 1.5　六個安全性層次之資訊安全技術

1.6 安全的資訊系統架構

- 資訊流向一旦某資訊擁有者將部分或全部權力授予他（她）人後，就很難再控制此資訊，因為此資訊之權力很可能再轉遞予第三者。至於顆粒性方面，任意性存取控制方法是將一檔案當作存取控制基本單位。
- 系統應該允許使用者存取到資料內某一基元（Atomic）資料，此類控制方式稱為強制性存取控制或多層性存取控制。

1.7 法律觀點

- 電腦系統的安全架構除了要有外圍層、外部層、中心層、內部層及分析層外，還需要相關的法律來約束使用者在電腦網路這個虛擬世界上的行為。

1.隱私權法（ 或《個人資料保護法》）

「資訊隱私權」(Information Privacy)，其中包含了使用不同媒介與他人溝通且不受他人監聽的通訊隱私權 (Communications Privacy)，以及個人資料不應被他人以自動化方式蒐集或處理的資料隱私權 (Data Privacy)。

台灣於 2015 年 12 月 30 日公布實施《個人資料保護法》，規範個人資料之蒐集、處理及利用，以避免人格權受到侵害，並促進個人資料之合理利用。

1.7 法律觀點

2.資訊空間安全法

確保由電腦及網路所形成空間內的資料、人身及財產安全。

3.智慧財產權法

數位產品在網路環境中更容易被複製並散播。

數位產品的智慧財產權保護目前都是世界各國非常關注的議題。

1.7 法律觀點

4.電子商務法

網路上的電子交易涵蓋了買賣契約的訂立、電子付款及金融交易等，而這些網路上所訂立的契約及交易行為是否具法律效力，就需有相關的法律規範。

台灣於 2001 年 11 月 14 日公布實施《電子簽章法》，作為推動普及運用電子交易，以確保電子交易之安全，並促進電子化政府及電子商務之發展。

1.8 資訊安全標準

- 國內對資訊安全管理系統的相關認證及專業證照愈來愈重視，其中又以 ISO/IEC 27001 資訊安全管理系統的相關認證最受各界接受。
  - ✓ ISO/IEC 27001 提供了建立資訊安全管理系統 (Information Security Management Systems, ISMS) 所需的要求事項 (Requirements) ，組織可依據其個別的需求，導入 ISO/IEC 27001 ，並適當的運用安全控制措施，以保護資訊資產，達到資訊安全與風險控管的要求。

1.8 資訊安全標準

- ✓ ISO/IEC 27002 經過 2013 年及 2022 年二次修訂。 ISO/IEC 27001 國際標準的附錄 A 中有關資訊安全、網路安全、和隱私保護之控制措施提供了詳細資訊說明。ISO/IEC 27002 提供機構組織的需要和環境，在資訊安全管理系統 (ISMS) 範圍內選擇、實施、和管理控制措施的作業規範 (Code of Practice for Information Security Management) 。
- ✓ ISO/IEC 27003 提供了資訊安全管理系統實作指引 (Information Security Management System Implementation Guidance) 。提供 ISO 27001 實施 ISMS 的明確指導，以滿足 ISO 27001 的詳細標準。

1.8 資訊安全標準

- ✓ ISO/IEC 27004 提供資訊安全管理系統監測、測量、分析、和評測 (Information Security Management - Monitoring, Measurement, Analysis And Evaluation) 指南。
- ✓ ISO/IEC 27005 提供資訊安全、網路安全、和隱私保護 (Information Security, Cybersecurity and Privacy Protection) ，作為資訊安全風險管理指南 (Guidance on Managing Information Security Risks) 。
- ✓ ISO/IEC 27006 提供資訊安全管理系統稽核與驗證機構之要求 (Requirements for Bodies Providing Audit and Certification of ISMS) 。

1.8 資訊安全標準

- ISO/IEC 27701 為 ISO 於 2019 年發布的隱私資訊管理國際標準 (Privacy Information Management Standard, PIMS) 。 ISO/IEC 27701 是 ISO/IEC 27001 和 ISO/IEC 27002 的延伸。 ISO/IEC 27701 提供個人隱私資訊保護指南，通過補充額外的控制要求來建立、實施、維護、和持續改進 ISMS 範圍內的隱私資訊管理，以降低個人隱私資訊面臨的風險。