ISBN 978-986-457-047-8

CH14 資訊管理的安全與倫理議題

ISBN 978-986-457-047-8

本章大綱

- 組織的資訊安全議題
- 防火牆與網路安全
- 資訊的加密系統與數位簽章
- 組織整體的資訊安全管理策略與活動
- 組織的資訊倫理議題

ISBN 978-986-457-047-8

14.1 組織的資訊安全議題(1/2)

- 近年來發生了許多資安的大事件，包括：
  - 2018年4月臉書(facebook)表示估計有8,700萬個資遭「劍橋分析」(Cambridge Analytica)竊取。
  - 2017年10月3日遠東銀行SWIFT主機遭駭，駭客盜轉6,010.4萬美元（合計約新台幣18億元）至海外三國。
  - 2017年5月12日起，WannaCrypt勒索病毒橫掃全球，超過150國、逾20萬台出現紅色勒索畫面。
  - 2016年10月21日，美國Dyn公司提供的DNS服務遭到了數次透過殭屍網路Mirai所發起的大型DDoS攻擊。

ISBN 978-986-457-047-8

14.1 組織的資訊安全議題(2/2)

- 2016年，Yahoo再傳10億個用戶個資遭竊；Dropbox超過6800萬筆個資在網路流傳。
- 2016年10月，Uber有5700萬筆資料外洩，包括行程地點、信用卡帳號、銀行帳號、出生年月日。

❑ 因此，在e化以及M化的網路時代，組織的資訊安全便成為了一個非常重要的議題。

ISBN 978-986-457-047-8

14.1.1 組織資訊安全的主要議題

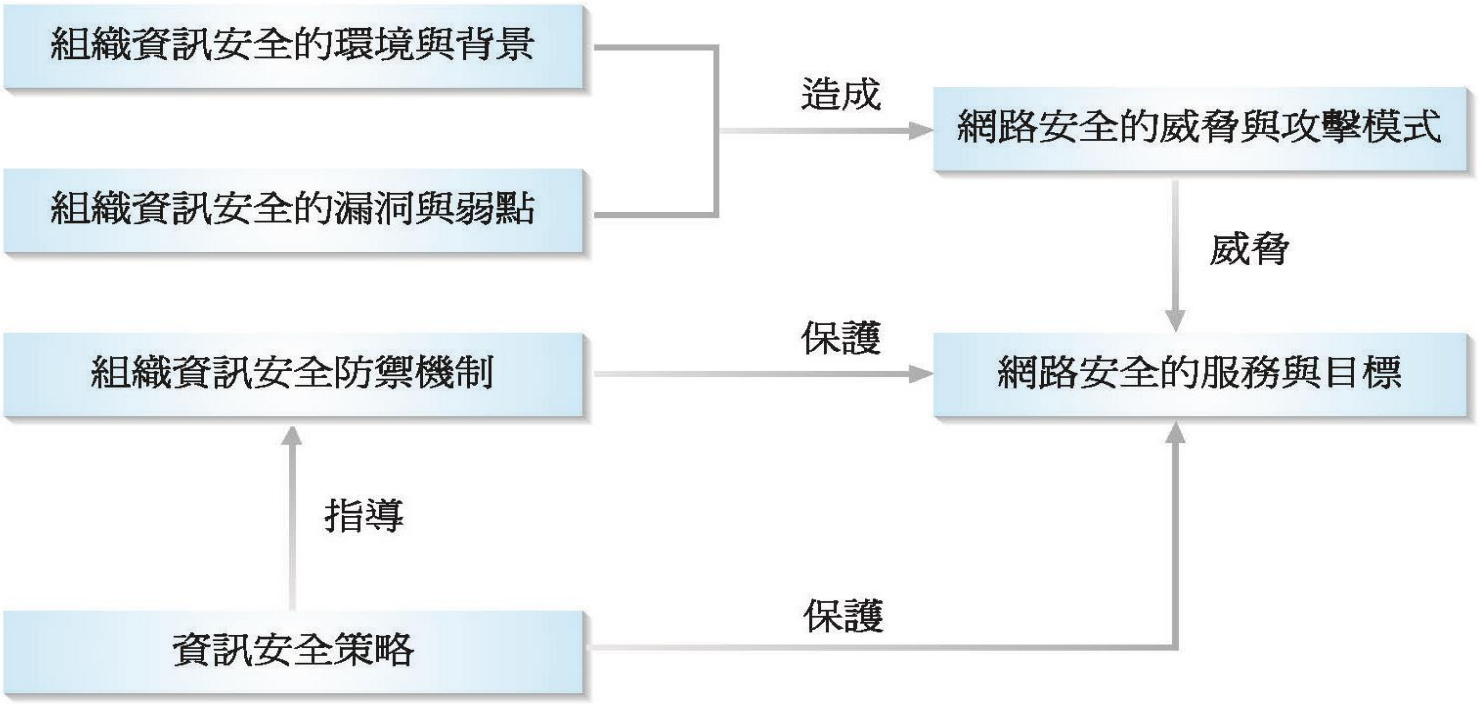


圖 14-1 資訊安全的主要議題與架構

ISBN 978-986-457-047-8

14.1.2 組織資訊安全的環境與背景

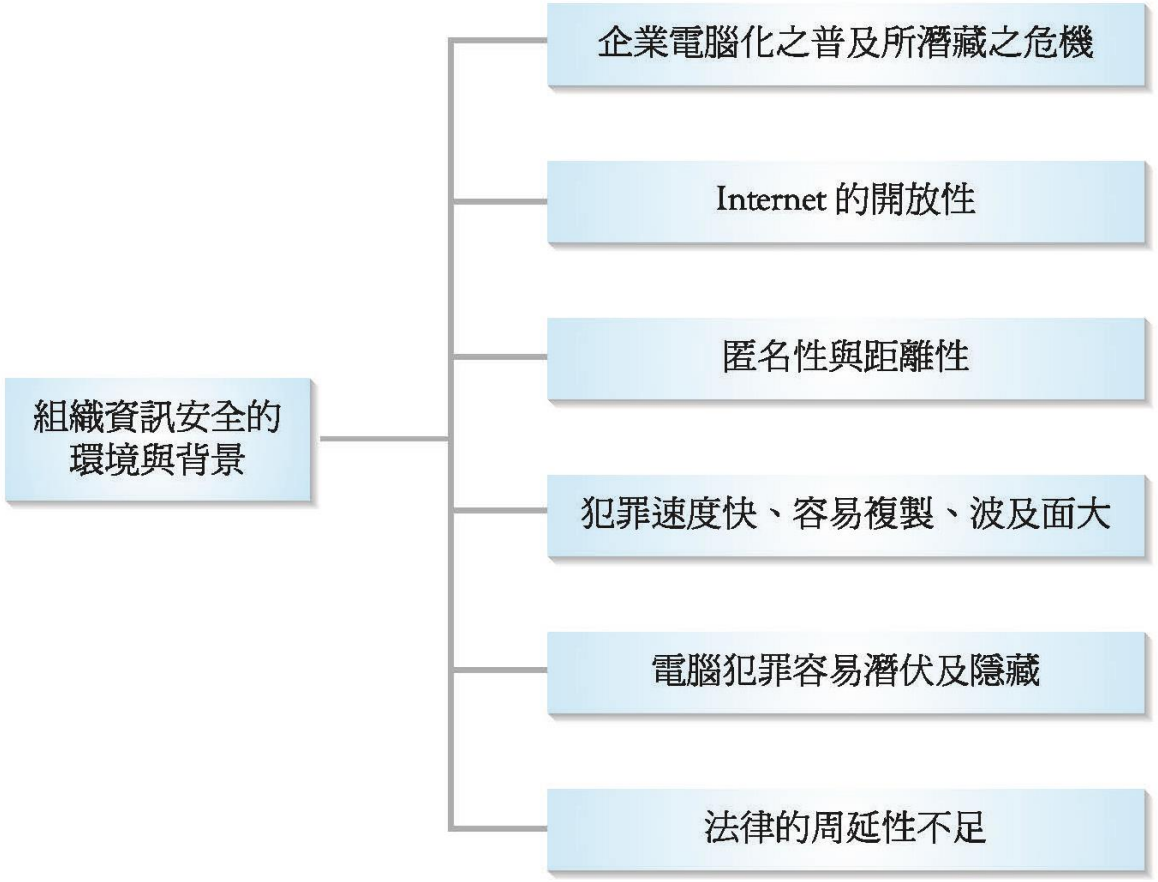


圖 14-2 組織資訊安全的環境與背景

ISBN 978-986-457-047-8

14.1.3 組織資訊安全的漏洞與弱點

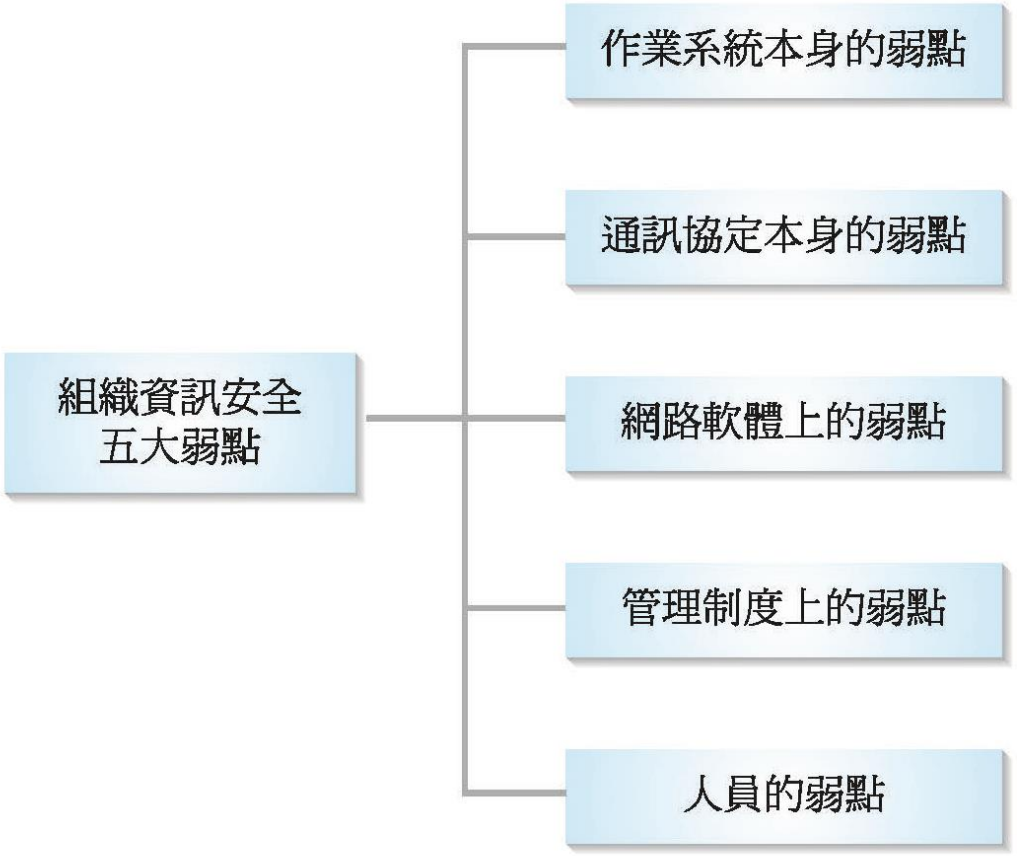


圖 14-3 組織資訊安全五大主要弱點

ISBN 978-986-457-047-8

14.1.4 網路安全的服務與目標

- 安全隱密性(Confidentiality)：指的是當資料傳遞時，除了被授權的人，不會受到外力的擷取。
- 身分認證性(Authentication)：指的是當傳送方送出資訊時，就必須能確認傳送者的身分是否為冒名。
- 資料的完整性(Integrity)：指的是當資料送達時必須保證資料沒有被篡改的疑慮。
- 授權性(Authorization)：使用者只能擷取被授權部分的資訊。
- 不可否認性(Non-Repudiation)：使用者已使用或接受某項服務（例如下訂單）時，不能否認其未使用過。

ISBN 978-986-457-047-8

14.1.5 網路安全的威脅與攻擊的模式(1/6)

- 電腦病毒(Virus)的散布：指的是會自行複製，能更改應用軟體或系統的可執行元件，或是刪除檔案、更改資料、拒絕提供服務，其常伴隨著電子郵件，藉由文件檔或執行檔的巨集指令來散布的惡意程式謂之。
- 阻絕服務(Denial of Service, DoS)：指的是：駭客利用極大量的流量來塞爆網站伺服器，使得該網站的系統或應用程式的存取被中斷或是阻止，讓使用者無法獲得服務。
- 後門或特洛伊木馬程式(Trapdoor/Trojan Horse)：指的是：未經授權的程式，可以透過合法程式的掩護，而偽裝成經過授權的流程來執行程式。如此會造成系統程式或應用程式被更換，而執行某些不被察覺的惡意程式，例如回傳重要個人或企業的機密給犯罪者。

ISBN 978-986-457-047-8

14.1.5 網路安全的威脅與攻擊的模式(2/6)

- 網路釣魚(Phising)：簡單的說，指的是：利用虛設或仿冒的網站以超低價或誘人的免費贈品來引誘消費者上網登錄個人私密資料或進行採購行為，利用此手法來「釣」到受害者的個人機密（如信用卡卡號）或金錢的一種電腦犯罪行為。有特定對象的網路釣魚稱之為「魚叉式釣魚」(Spear Phishing)，指的是駭客對於要釣魚的對象有特定的標的。
- 社交工程 (Social Engineering) ：指的是駭客利用人類的天性，包括同情心、好奇心、求知心、貪心、恐懼心，使用抽大獎、情色影片、恐嚇信、可憐求助、社會公益、環保救地球與老年人健康資訊等各種口號、動機等誘因來吸引使用者登入惡意網站。
- 勒索軟體(Ransomware) ：指的是2013年後流行的一種電腦病毒，當其入侵受害者的電腦後，會威脅或謊稱其電腦已中毒，必須馬上線上付「贖金」(Ransom)或購買解毒軟體，否則電腦硬碟內的資料會全部遭刪除，有的勒索軟體是將硬碟資料全部轉成亂碼，受害者必須馬上線上付款才能解碼。例如：上述的WannaCrypt。

ISBN 978-986-457-047-8

14.1.5 網路安全的威脅與攻擊的模式(3/6)

- 變臉攻擊(Business Email Compromise, BEC) ：又稱「商務電子郵件入侵」，指的是針對具有撥款權力的企業財務主管，透過入侵高階主管或外部供應商主管的電子郵件帳戶，通知要求其匯款轉帳到駭客帳戶的一種新型詐騙手法，這是目前投資報酬率最高、程序最簡單、金額獲利最大的一種詐欺方式。
- 進階持續滲透性攻擊(Advanced Persistent Threat, APT) ：所謂APT指的是基於經濟利益，針對某一特定組織所做的持續性、複雜且多元的網路攻擊，其可能持續幾天、幾週、幾個月，甚至更長時間，其利用多元的手段包括社交工程、惡意郵件、植入惡意程式，或弱點掃描、針對性入侵，再建立殭屍網路(Botnet)來竊取重要、有價值的情資。
- 水坑攻擊(Waterhole Attack) ：以前，駭客多半會寄送夾帶惡意程式或釣魚網站的電子郵件給攻擊目標，現今則是觀察攻擊目標習慣瀏覽哪些網站，再去入侵那些網站並植入惡意程式，等待攻擊目標造訪該網站時再趁機感染而竊取資料，這就是所謂的「水坑攻擊」。

ISBN 978-986-457-047-8

14.1.5 網路安全的威脅與攻擊的模式(4/6)

- 挖礦木馬程式(CryptoMiner) ：指的是在網站內嵌入挖礦程式，例如：Coinhive或CoinMiner，當不知情的使用者一旦進入這個網站後，挖礦程式的JavaScript自動執行，耗用使用者大量的CPU資源，來挖掘虛擬貨幣Monero或Electroneum。
- 間諜軟體與惡意程式：間諜軟體(Spyware)是一個廣泛的名詞，泛指所有快速繁殖，且能夠巧妙滲入PC的合法廣告軟體，以及具有明顯的惡意程式碼(Malicious Code)，例如鍵盤側錄器(Keystroke Loggers)，其又被稱之為可能不需要的程式(Potentially Unwanted Programs, PUPs)。
- 雲端運算架構上的攻擊(Cloud Computing Attach) ：攻擊者今後將會鑽研雲端服務計算提供商的API（應用程式介面）漏洞，以便更有效率地部署遠程攻擊，進而大幅拓展攻擊範圍。

ISBN 978-986-457-047-8

14.1.5 網路安全的威脅與攻擊的模式(5/6)

- 物聯網病毒（IOT病毒）：物聯網流行以後，當然也成為駭客的目標，許多物聯網裝置，尤其是攝影機，就成了病毒的攻擊重點。
- 社交網站攻擊(Social Network Attack) ：透過社交網站，許多認識或不認識的使用者集中在相同的平台上並作互動，一旦這些社交網站被挖掘出安全性弱點，攻擊者將可以快速地利用並影響到大量的使用者。YouTube、MySpace、Facebook、Twitter及Line等人氣網路社群、都是最容易成為網路威脅的目標。
- 行動病毒(Mobile Virus) ：指的是以行動手持設備為標的的病毒，其主要包括行動勒索(Mobile Ransomware)、行動木馬程式(Mobile Trojan)、行動釣魚(Mobile Phising)及行動挖礦(Mobile Cryptominer)。

ISBN 978-986-457-047-8

14.1.5 網路安全的威脅與攻擊的模式(6/6)

- 蠕蟲(Worm)與傀儡模式(Bot)的聯手攻擊：Botnet又稱傀儡程式(Bot)或「受控制的網路系統」或僵屍網路(Zombies)，指的是：一群已經被駭客入侵並控制的電腦所組成的攻擊網路（有些數目多達10萬台），這些僵屍已經在數位戰場上集結，等待駭客指揮官從遠端下達攻擊指令、進行攻擊，這種集結所形成的攻擊力量非常駭人，包括引發洪水般的分散式阻絕服務攻擊(Distributed DoS, DDoS)的大量寄發。
- 人工智慧資安的攻防戰：在防守方面，他將會學習過去數百數千種的攻防戰，而來尋求一個最有效的防守策略，相反的，在攻擊的駭客方也可以利用AI的深度學習來設計最難被預防、偵測、攻擊力最強的病毒，我們將拭目以待這個攻防大戰。

ISBN 978-986-457-047-8

14.1.6 網路安全的主要防護機制

表 14-1 網路的安全服務項目、威脅與防護法

安全服務項目	安全威脅	安全防護法
安全隱密性(Confidentiality)	竊聽、擷取、洩密	加密系統、數位信封
身分認證性(Authentication)	冒名交易及傳送	身分辨識碼、數位簽章
資料完整性(Integrity)	資訊的篡改、刪除與破壞	加密系統、數位簽章
存取控制(Access Control)	不合格的使用者	合格的系統軟體、通行密碼、防火牆、侵入偵測系統
不可否認性(Non-Repudiation)	否認收發資料	數位簽章

ISBN 978-986-457-047-8

14.2 防火牆與網路安全

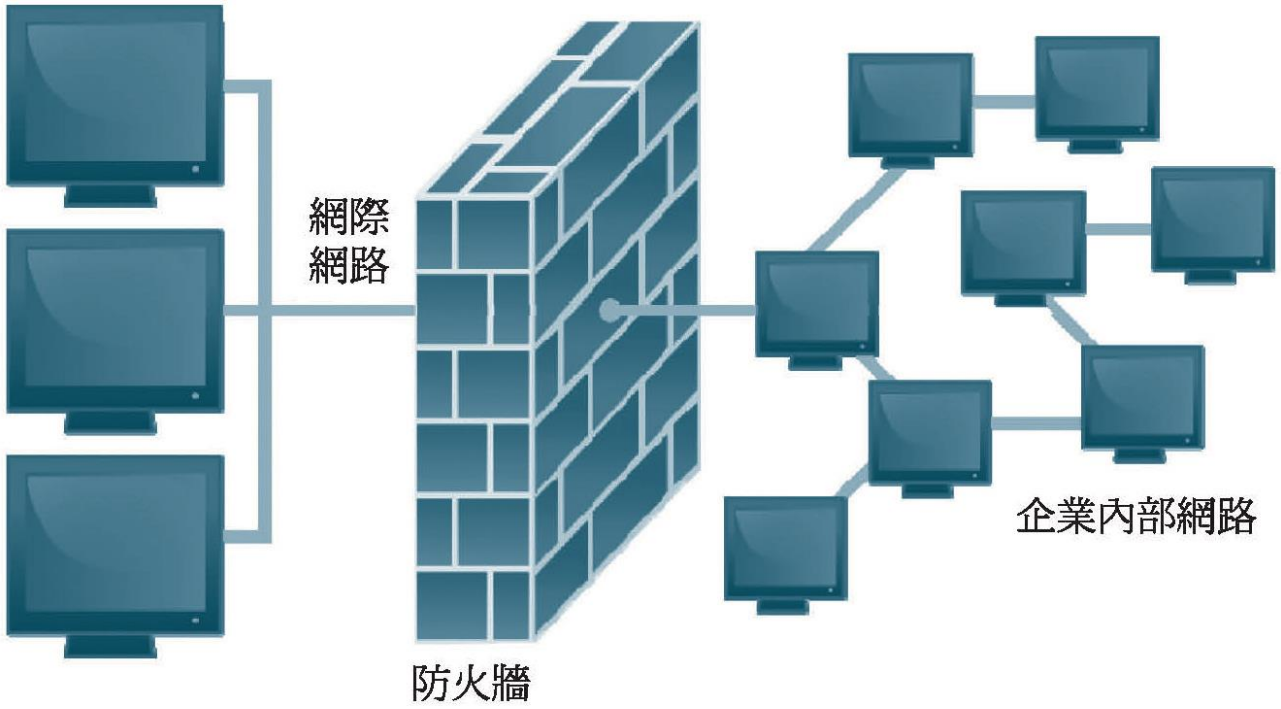


圖 14-5 防火牆示意圖

ISBN 978-986-457-047-8

14.2.1 防火牆的基本概念

- 防火牆(Firewall)顧名思義就是防止網際網路上的危險延伸到企業內部網路。介於網際網路和企業內部網路相連結之間。所以網際網路和企業內部網路兩者之間的傳輸，均需經過防火牆，如此防火牆可先檢查傳輸的合法性；若是合法，傳輸連結方能送達目的地。

ISBN 978-986-457-047-8

14.2.2 防火牆的技術與架構

- 基本上防火牆可分兩種型態：
  - 封包過濾型
  - 代理者型

ISBN 978-986-457-047-8

14.2.3 防火牆的基本目標

- 過濾封包以阻止網路駭客的入侵。
- 作為所有封包進出的門戶。
- 過濾系統安全政策所禁止的網路服務。
- 保護企業內部網路，避免來自網際網路的入侵。
- 當外部使用者存取高度機密檔案時，先加以記錄並通知系統管理者。
- 調節網路交通流量。

ISBN 978-986-457-047-8

14.2.4 防火牆的主要問題

- 較難提供全面性的安全
- 無法提供資料隱密性
- 無法確認資料來源的認證性
- 無法預防內部威脅
- 無法保護那些不經過防火牆的網路連結

ISBN 978-986-457-047-8

14.3 資訊的加密系統與數位簽章

- 資訊加密的主要機制
- 數位簽章與資訊安全
- 數位信封與傳輸層安全性協定(TLS)

ISBN 978-986-457-047-8

14.3.1 資訊加密的主要機制(1/3)

- 加密
  - 加密(Encryption)，指的是：將原始文件轉換成亂碼，而唯有使用解密(Decryption)的金鑰(Key)才能讀出原文的程序。
- Key
  - 指的是：一長串的文字、符號、數字的組合這些參數，用來啟動指揮轉換程式來轉換原始的文件，使得原始文件變成亂碼。

ISBN 978-986-457-047-8

14.3.1 資訊加密的主要機制(2/3)

- 對稱式加密法
  - 對稱式加密法(Symmetric Encryption)，此為傳統的加密法，其特色是買賣雙方同時持有一個同樣的Key來加密和解密（圖14-6是對稱式的加密法），所使用的Key稱為秘密金鑰(Secret Key)。

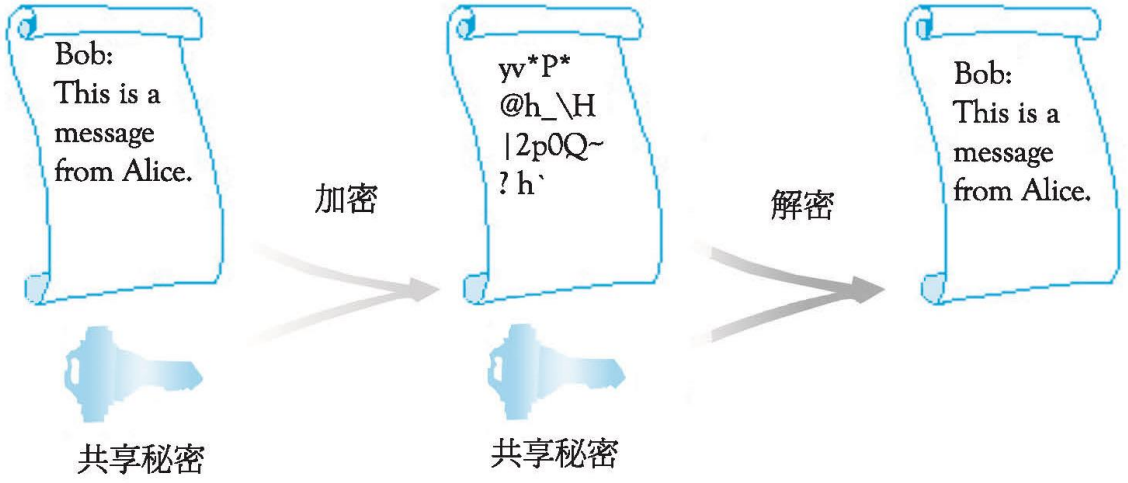


圖 14-6 資訊的加密與解密

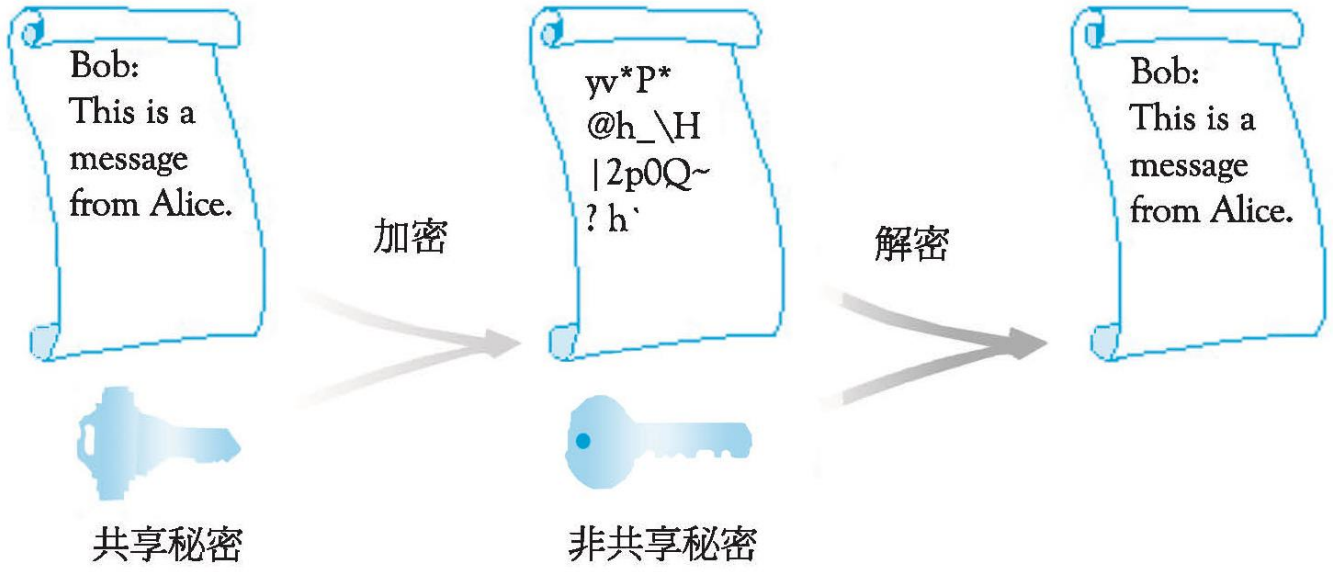
ISBN 978-986-457-047-8

14.3.1 資訊加密的主要機制(3/3)

- 非對稱式加密法
  - 非對稱式加密法(Asymmetric Encryption)，此為1976年，由Diffe及Hellman所發明的新加密機制，又稱之為公鑰的基礎設施(Public Key Infrastructure, PKI)。此法的特色主要是使用兩把對應配對的Key，即公鑰(Public Key)與私鑰(Private Key)，互相可加密／解密對方，也就是以Public Key加密後可以使用Private Key將其解開，而使用Private Key加密後也可以使用Public Key將其解開，兩者是一對的。

ISBN 978-986-457-047-8

圖14-7 非對稱式的加密法



ISBN 978-986-457-047-8

14.3.2 數位簽章與資訊安全(1/2)

- 數位簽章(Digital Signature, DS)，簡單的說，指的是：利用PKI的機制來保護資料傳遞的隱密性與不可否認性的一種通訊安全機制。而支援數位簽章的主要機制，包括下列幾點：
  - 碎映函式
    - 所謂碎映函式(Hash Function)，指的是：對於任一長度的訊息，將其映射成一個固定長度（例如128 Bits）的數值，而且其是多對一的映射，無法由其輸出值計算出原本的訊息的一種函式。
  - 數位簽章
    - 傳送者將文件經特別碎映函式運算後產生一獨特的號碼(128 Bits)，稱之為訊息摘要(Message Digest)，再利用傳送方的Private Key對此摘要加密，謂之數位簽章(DS)。

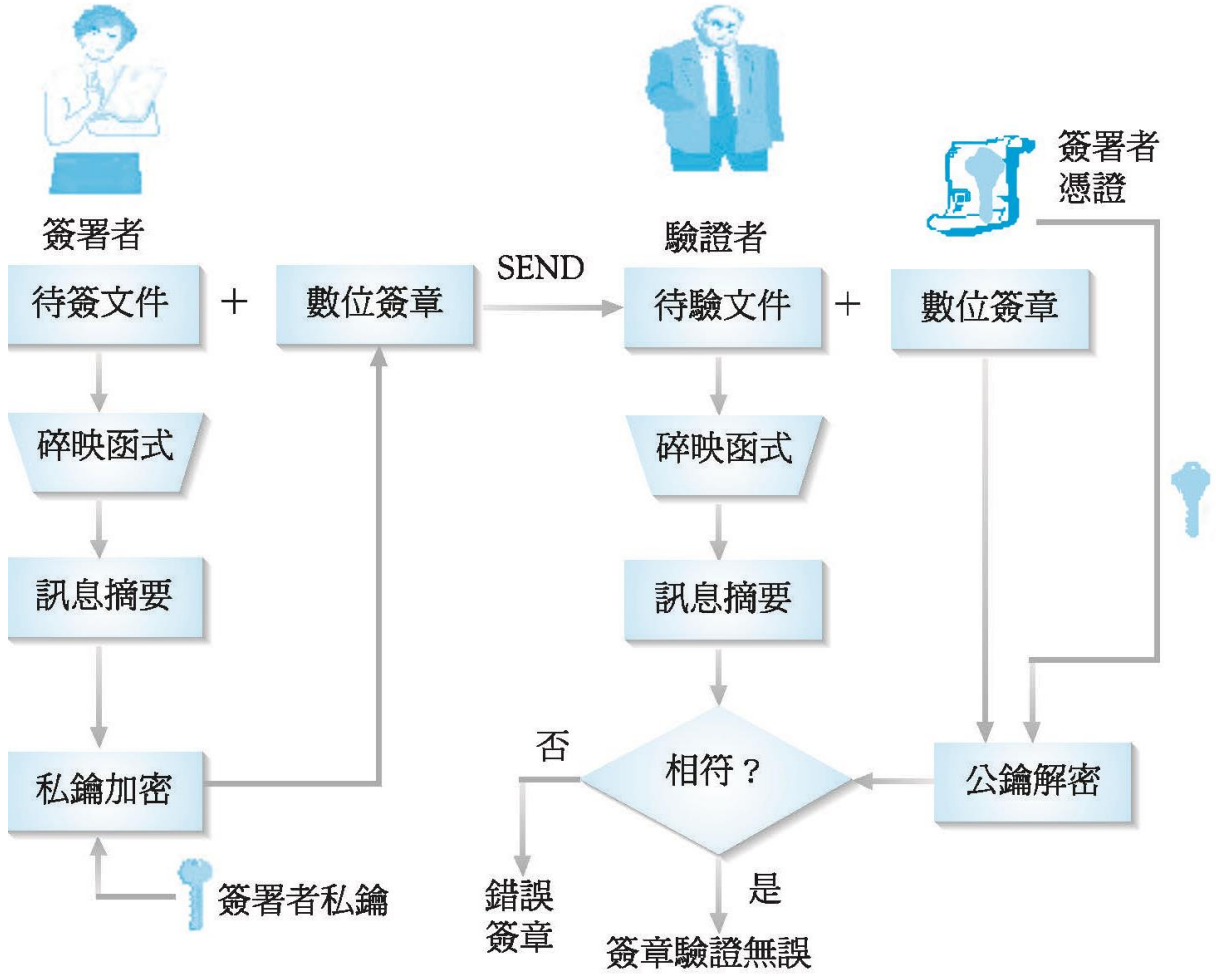
ISBN 978-986-457-047-8

14.3.2 數位簽章與資訊安全(2/2)

- 電子認證中心
  - 所謂電子認證中心(Electronic Certificates Authority, CA)，指的是：一個有公信力的第三者，要在EC上交易的個人或企業必須在CA認證身分後，再核發電子憑證(Electronic Certificate)及 Public Key 與 Private Key。CA最主要的任務是管理買賣雙方的認證問題。

ISBN 978-986-457-047-8

圖14-8 數位簽章流程



ISBN 978-986-457-047-8

14.3.3 數位信封與傳輸層安全性協定義(TLS)

- 數位信封
  - 數位信封，簡單的說，指的是：利用速度較快、較不安全的對稱式加密法的秘密金鑰來對大量的文章內容加密，之後利用較安全的PKI來對秘密金鑰加密（由於其數量很小，因此不會妨害傳輸速度），而其主要的利用方法即是所謂的TLS。
  - TLS：傳輸層安全性協定(Transport Layer Security, TLS)是數位信封的應用（其前身為Secure Sockets Layer, SSL）。在瀏覽器、電子郵件、即時通訊、VoIP、網路傳真等應用程式中，廣泛支援這個協定。主要的網站，如Google、Facebook等也以這個協定來建立安全連線，傳送資料。目前已成為網際網路上保密通訊的工業標準。

ISBN 978-986-457-047-8

14.4 組織整體的資訊安全策略與活動

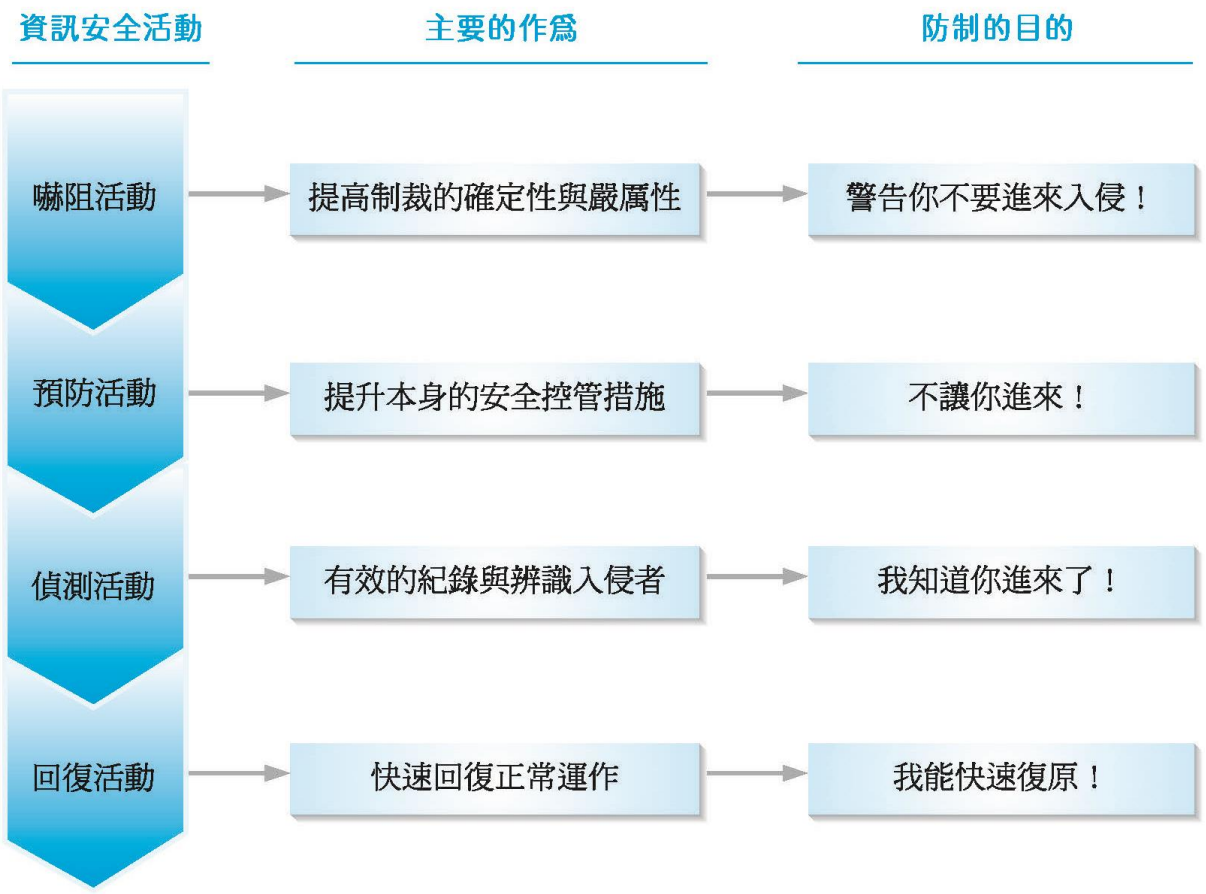


圖 14-10 資訊安全的四大活動與目的

ISBN 978-986-457-047-8

14.4.2 嚇阻活動

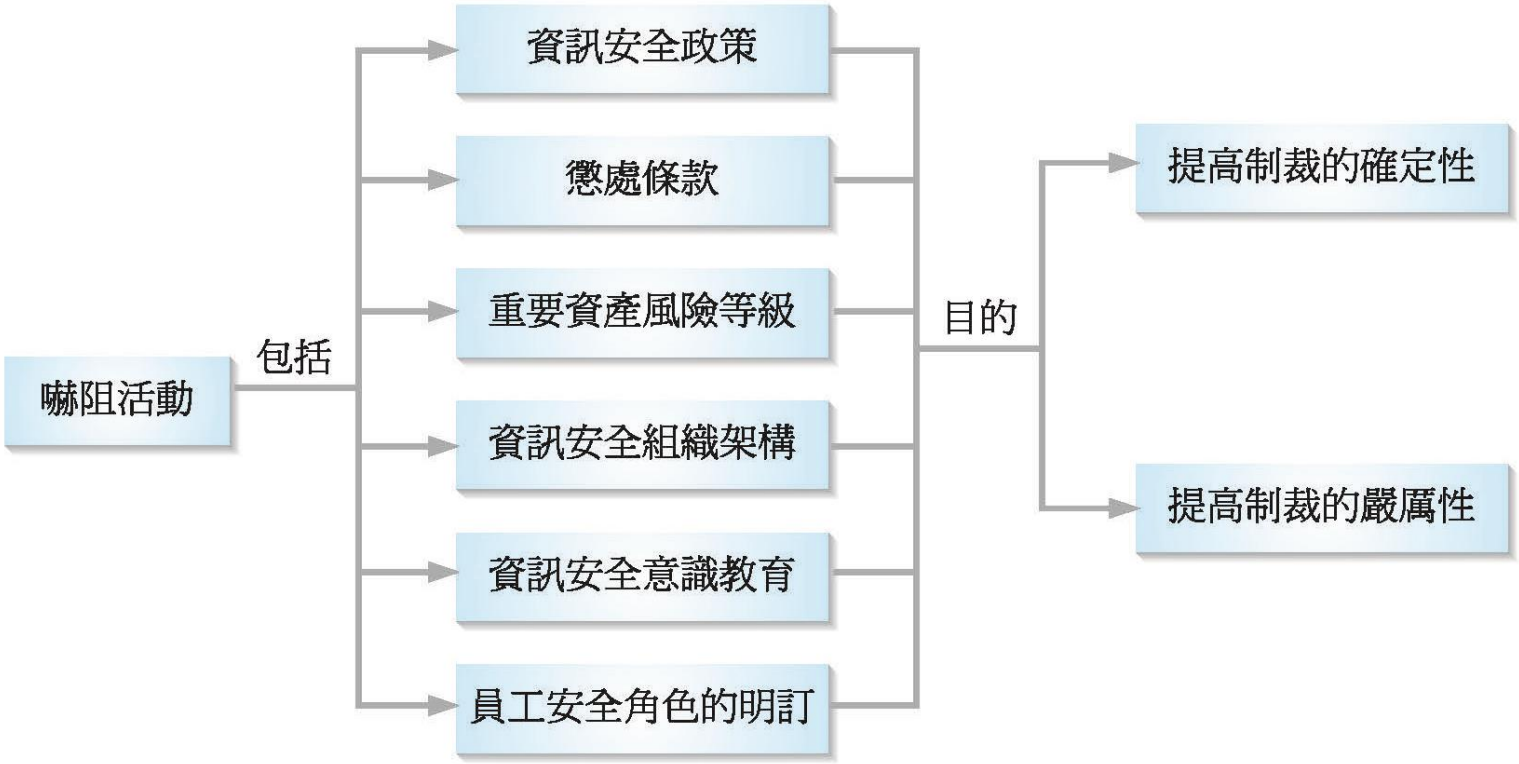


圖 14-11 嚇阻的主要活動與目的

ISBN 978-986-457-047-8

14.4.3 預防活動

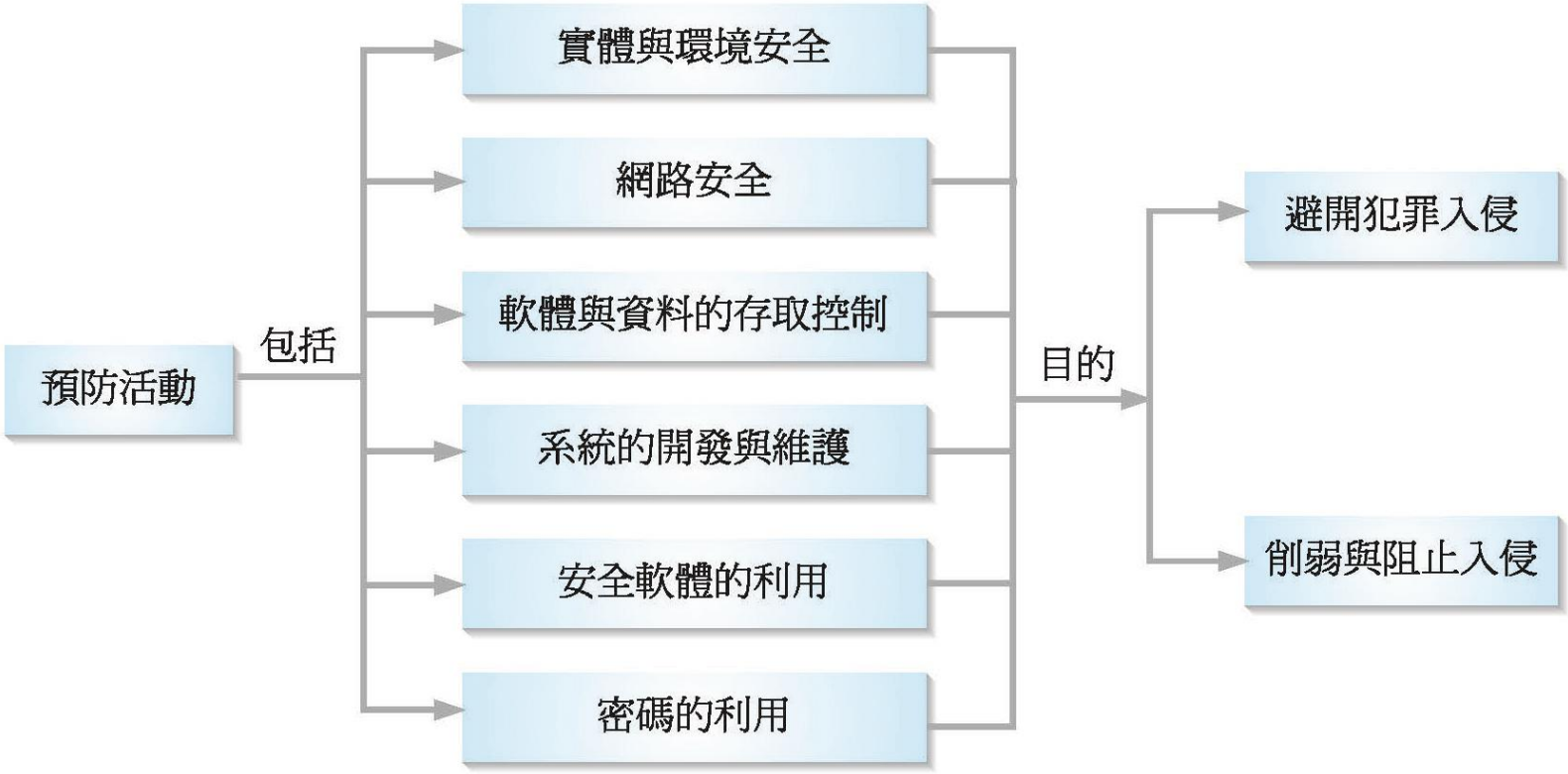


圖 14-12 預防的主要活動與目的

ISBN 978-986-457-047-8

14.4.4 偵測活動

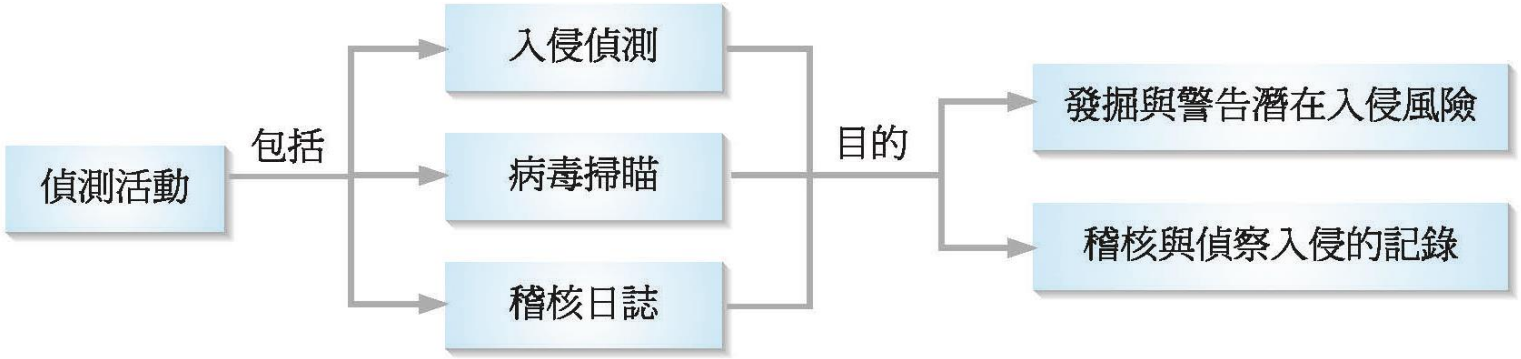


圖 14-13 偵測的主要活動與目的

ISBN 978-986-457-047-8

14.4.5 回復活動

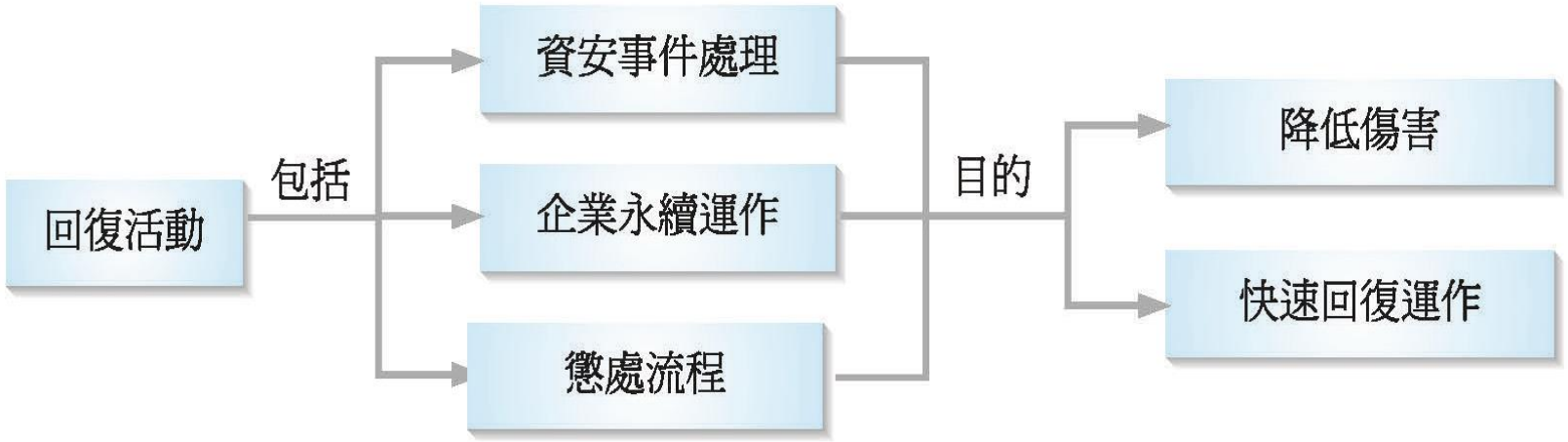


圖 14-14 回復的主要活動與目的

ISBN 978-986-457-047-8

14.4.6 四個資訊安全活動之整合

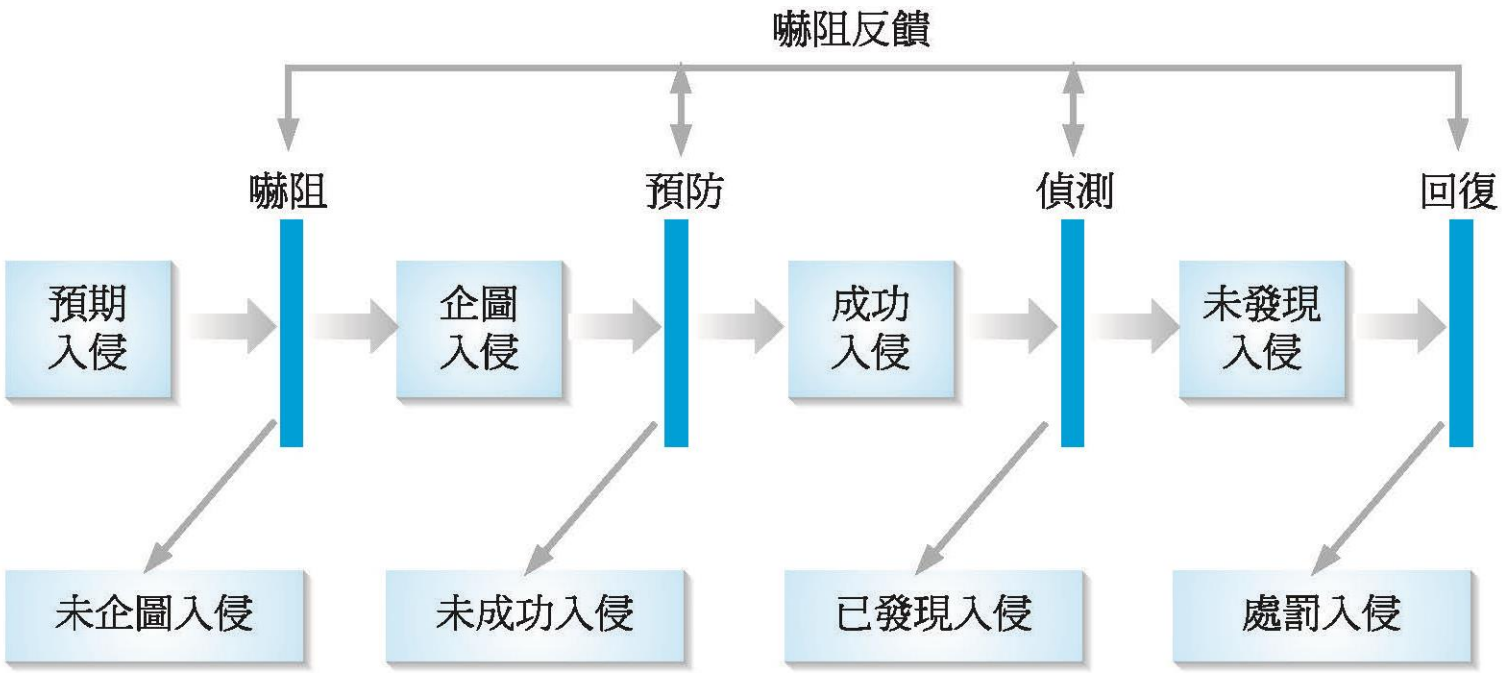


圖 14-15 四個資訊安全活動的流程

ISBN 978-986-457-047-8

14.5.1 隱私權的倫理議題(1/3)

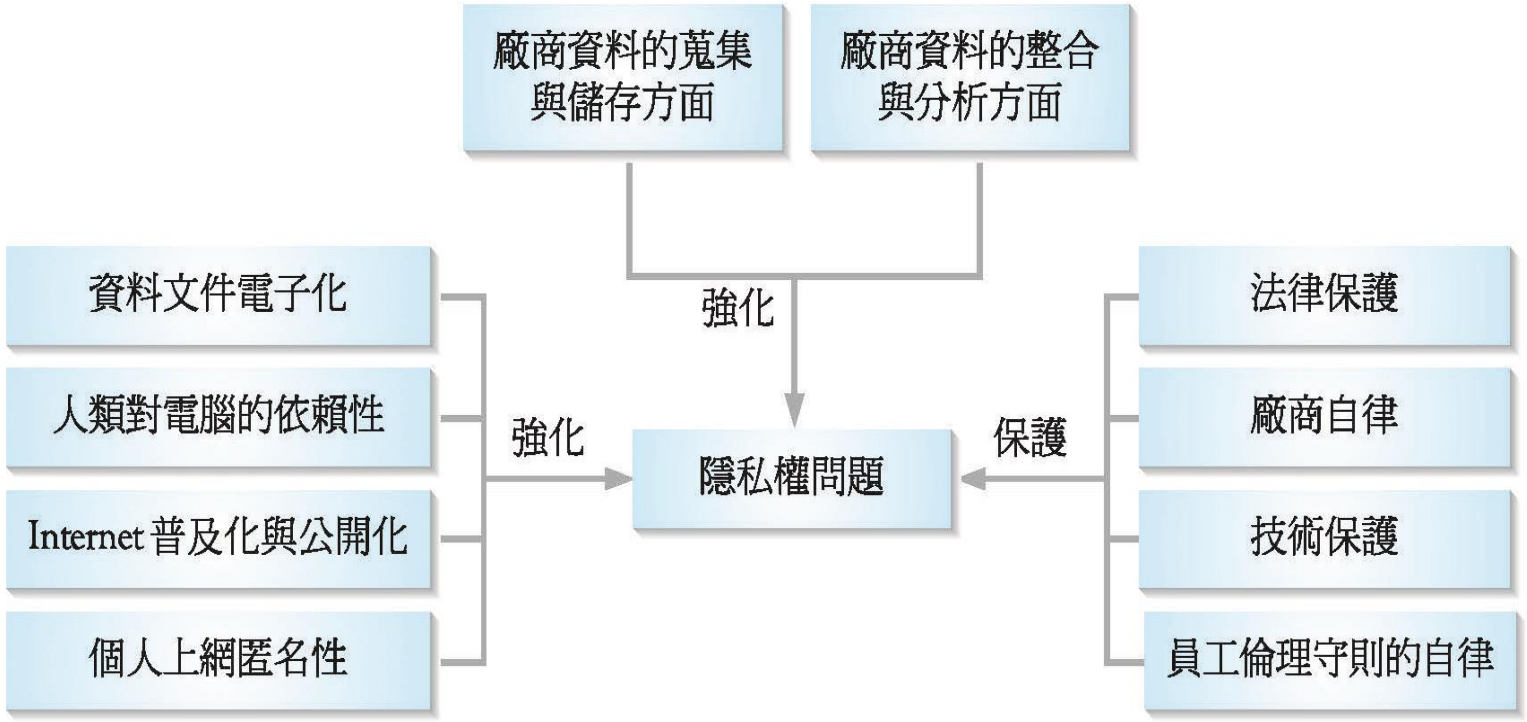


圖 14-16 隱私權的主要分析架構圖

ISBN 978-986-457-047-8

14.5.1 隱私權的倫理議題(2/3)

- 法律保護：例如各地區個資法與資訊安全新規範
  - 歐盟的通用資料保護法(General Data Protection Regulation, GDPR)於2018年5月25日正式實施，被稱為史上最嚴格的個資法案對於擁有歐盟公民個資資料的組織有著嚴格的規範，若沒有執行個資保護風險評估、沒有任命資料保護長、72小時沒有即時通報、違法向第三國傳輸個資，違反者可罰2,000萬歐元或全球營業額4%罰鍰。
  - 台灣《資通安全管理法》於2018年5月1日通過制定，要求各公務機關需設置資安長，推動及監督資安事務，經行政院核定的關鍵基礎設施提供者應訂定資安計畫，且若未通報資安事件，可罰30萬至500萬元的罰款。

ISBN 978-986-457-047-8

14.5.1 隱私權的倫理議題(3/3)

- 廠商自律
  - 選擇不加入(Opt-out)
  - 選擇加入(Opt-in)
- 技術保護
- 員工倫理守則的自律

ISBN 978-986-457-047-8

14.5.2 資訊的正確性倫理議題(1/4)

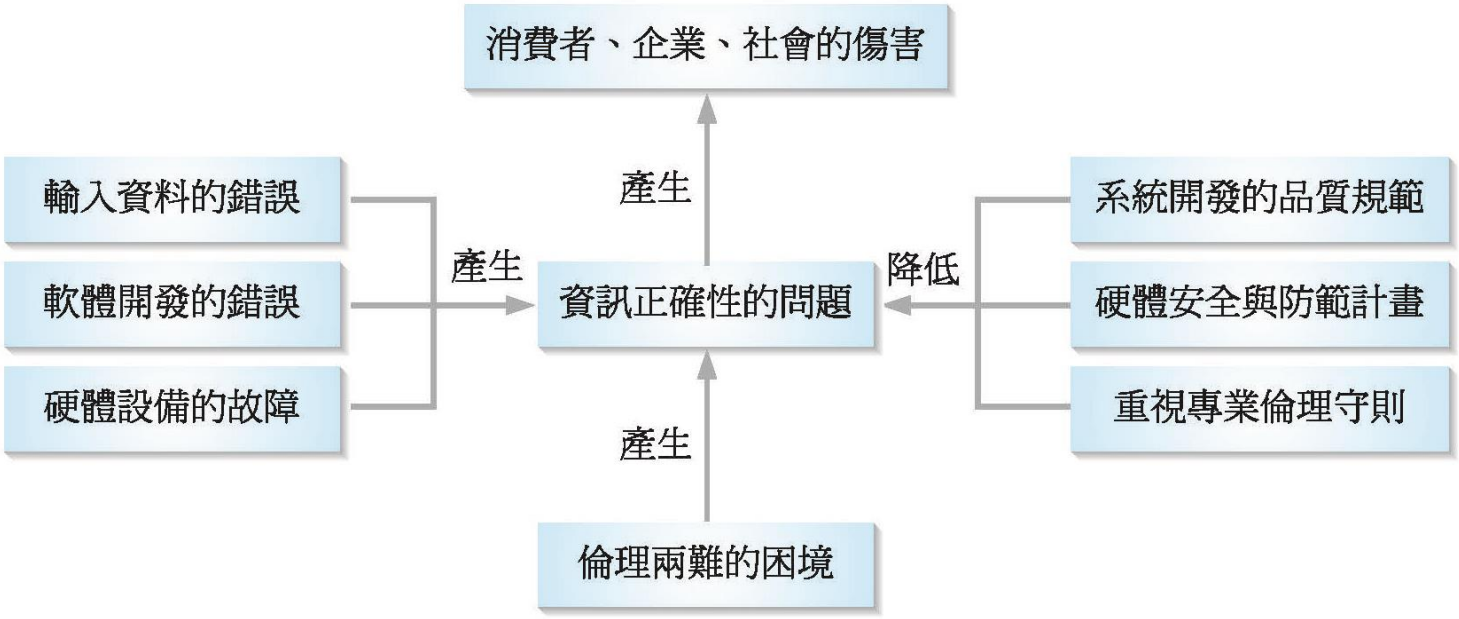


圖 14-17 資訊正確性議題的主要分析架構

ISBN 978-986-457-047-8

14.5.2 資訊的正確性倫理議題(2/4)

- 資訊的正確性(Information Accuracy)指的是資訊的提供者有提供正確資訊的義務；資訊的不正確性會對個人、社會甚至國家安全產生很大的傷害，例如：
  - 股票營業員錯誤輸入100倍的買賣交易金額。
  - 銀行錯誤植入民眾存款的金額。
  - 醫院錯誤輸入病人用藥的品項。
  - 司法單位錯誤植入犯罪者的身分。
  - 銀行系統當機，使得銀行用戶無法提款。
  - 網路上散播不實的謠言。

ISBN 978-986-457-047-8

12.5.2 資訊的正確性倫理議題(3/4)

- 資訊正確性的基本概念與重要性
  - 由於資訊化的普及，如若資訊的不正確性會對個人、社會甚至國家安全產生很大的傷害，例如：
    - 股票營業員錯誤輸入100倍的買賣交易金額。
    - 銀行錯誤植入民眾存款的金額。
    - 醫院錯誤輸入病人用藥的品項。
    - 司法單位錯誤植入犯罪者的身分。
    - 銀行系統當機，使得銀行用戶無法提款。
    - 網路上散播不實的謠言。

ISBN 978-986-457-047-8

12.5.2 資訊的正確性倫理議題(4/4)

- 資訊正確性的問題產生原因與防範措施
  - 系統開發的品質規範
  - 硬體安全與防範計畫
  - 重視專業倫理守則
- 資訊正確性的倫理兩難

ISBN 978-986-457-047-8

12.5.3 財產權(Property)的倫理議題(1/2)

- 科技上的保護：數位內容權利管理
  - 所謂數位內容權利管理(Digital Right Management, DRM)：泛指智財權的所有者用來控制與管制合法存取有智財權數位產品的所有一切技術謂之。
- 社會宣導與教育
- 立法上的保護

ISBN 978-986-457-047-8

12.5.3 財產權(Property)的倫理議題(2/2)

圖 14-18 智財權議題的主要分析架構

ISBN 978-986-457-047-8

14.5.4 資訊存取權的倫理議題(1/2)

- 資訊存取權的基本概念
- 資訊存取權的重要倫理原則：FIP原則
  - 告知／察覺原則(Notice/Awareness Principle)：指的是任何網站在搜尋消費者資料之前，必須明確的說明其資訊使用政策。
  - 選擇／同意原則(Choice/Consent Principle)：資料蒐集的使用者必須提供一個選項，讓消費者能自由決定其所輸入的資料。

ISBN 978-986-457-047-8

14.5.4 資訊存取權的倫理議題(2/2)

- 存取／參與原則(Access/Participate Principle)：資料蒐集的使用者必須提供一個方便快捷的管道讓消費者能隨時去檢視、審閱其本身資料的正確性與完整性。
- 安全原則(Security Principle)：資料蒐集的使用者本身必須採取負責的措施來保證消費者資料的正確性並保障資訊安全。
- 強化原則(Enforcement Principle)：FIP原則必須要強化與落實，無論是透過業者本身的自律自我規範，或政府立法管制，並也要立法讓消費者因受到傷害而能得到補償。