

The background is a vibrant green with a subtle gradient. In the upper left corner, there are several faint, white line-art icons: a key, a padlock, a shield, and a circular arrow. The top edge of the slide has a wavy, torn-paper-like effect. The text is centered in the middle of the slide.

A01-002

資訊安全概論

課程大綱

- 資訊安全導論
- 資訊安全法令與管理規範
- 資訊安全威脅
- 資訊安全基本防護
- 結論

The background is a vibrant green with a layered, wavy design. The top section features a horizontal band with faint, white line-art icons including a key, a padlock, a shield, a magnifying glass, a gear, and a square. Below this band, the background transitions into a series of horizontal, wavy bands of varying shades of green, creating a sense of depth and movement.

第一章 導論

資訊安全概念簡介(1/4)

“資訊對組織而言就是一種資產，和其它重要的營運資產一樣有價值，因此需要持續給予妥善保護。資訊安全可保護資訊不受各種威脅，確保持續營運，將營運損失降到最低，得到最豐厚的投資報酬率和商機。”

BS 7799標準定義

資訊安全概念簡介(2/4)

資訊安全的重要

- 企業資訊化的過程，資料以電腦處理、傳遞和儲存並不安全。
 - 會被攻擊
 - 會被入侵
 - 會被攔截
- 資料的不當揭露、破壞及無法正確提供服務將導致企業重大損失。

資訊安全概念簡介(3/4)

- 資訊安全

- 資訊安全是一種防止與偵測未經授權而使用、竊取、破壞您的資訊系統的一種過程與程序。
- 資訊安全的工作必需事先妥善規劃、確實謹慎實行各項必要的資訊安全措施，並且持續不斷的檢討修正實施，以確保隨著時間的演進，仍可以維持資訊的安全性。

資訊安全概念簡介(4/4)

- 安全管理概念

- 安全管理是將公司組織的風險降低到一個可以接受的程度並且持續維持這個可接受的程度的過程。
- 安全管理必需由上往下(Top-down)實施，由上層管理人員至一般員工必需參與。
- 為達到安全性管理目標，安全性管理的工作必需區分為下面三個控制層面：
 - 管理控制
 - 技術控制
 - 實體控制

資訊安全管理要件(1/7)

C. I. A.

資訊安全的基本功能及目的不外提供資料和資源的機密性、完整性、可用性。

- 安全性機制所提供的基本服務：

- Confidentiality (機密性)
- Integrity (完整性)
- Availability (可用性)

- 其它安全性服務

- Non-repudiation (不可否認性)
- Authentication (身分鑑別)
- Authority (存取權限控制)

資訊安全管理要件(2/7)

Confidentiality (機密性)

- Prevent disclosure of data.
- 確保資料傳遞與儲存的私密性。
- 避免未經授權的使用者有意或無意的揭露資料內涵。

例如資料於網路傳送時被攔截竊取，或公司不小心公佈不該公佈的訊息均是違反資料的機密性。

- 機密性資料傳遞和儲存時務必加密處理。
- 採用安全性協定 (eg. SSL、IPSec)

資訊安全管理要件(3/7)

Integrity (完整性)

- Prevent modification of data.
- 避免非經授權的使用者或處理程序篡改資料。
- 所使用的文件經傳送或儲存過程中必需證明其內容並未遭到竄改或偽造才能稱為完整性。

資訊安全管理要件(4/7)

Availability (可用性)

- Ensure reliable timely access to data.
- 讓資料隨時保持可用狀況。
- 企業資料必需即時並可靠的提供給企業內部各個層級的使用需求。
- 系統的高度可用性通常指的是必需確保不能中斷服務。

資訊安全管理要件(5/7)

Non-repudiation (不可否認性)

- 防止存心不良的使用者否認其所做過的事，包括送出信件，接收文件，存取資料等。
- 即交易的收發雙方參與安全管制並無法否認執行過的交易
- 例如數位簽署就具備不可否認性。

資訊安全管理要件(6/7)

Authentication(身分鑑別)

- 辨別資訊使用者的身份
- 即可以記錄資訊是被誰使用過
- 例如帳號、身份字號、員工編號。

資訊安全管理要件(7/7)

Authority(存取權限控制)

- 依照身份給予適當的權限。
- 例如：銀行的櫃臺是不被允許進入保險櫃，僅有組長以上的權限才能進入。

資訊安全防護體系(1/2)

現行對於資訊安全的保護機制其實與古代的防禦機制是沒有差別的。

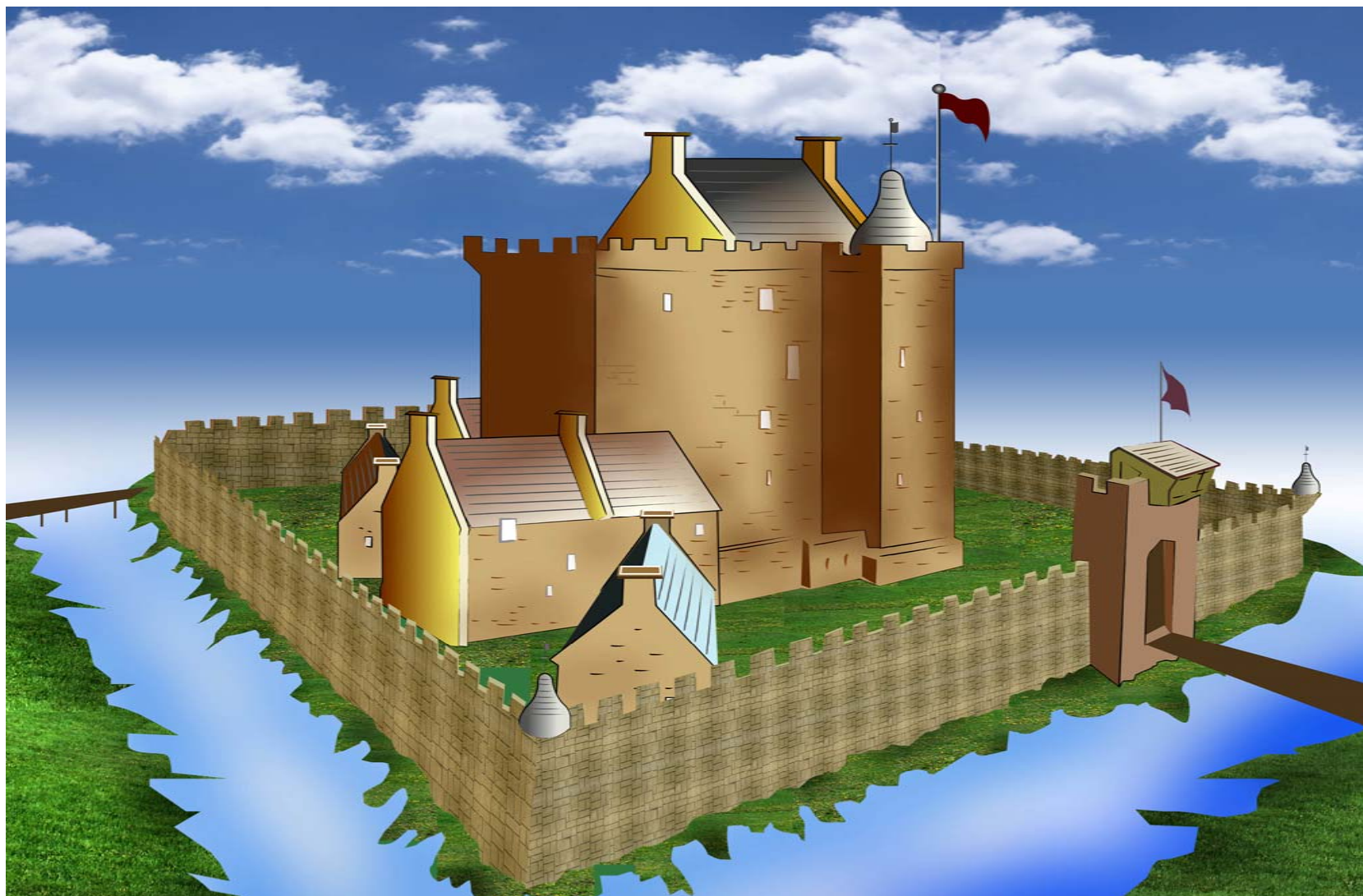
- 在古代，為了抵禦外侮，領主都會建立城堡。城堡有高大的城牆，牆上面有兵士巡邏。城牆外，有些會挖護城河，用來防止地道攻擊，也避免近距離的攀城攻擊。有些重要的城池還會有內外城牆之分。
- 城堡對外的出入就是經過長長的城門。城門除了厚重的大門外，有些還在裡面設機關，前後端可能會加上急降式柵門，用意是來困住入侵者。城門官兵必要時會檢驗證件。

資訊安全防護體系(2/2)

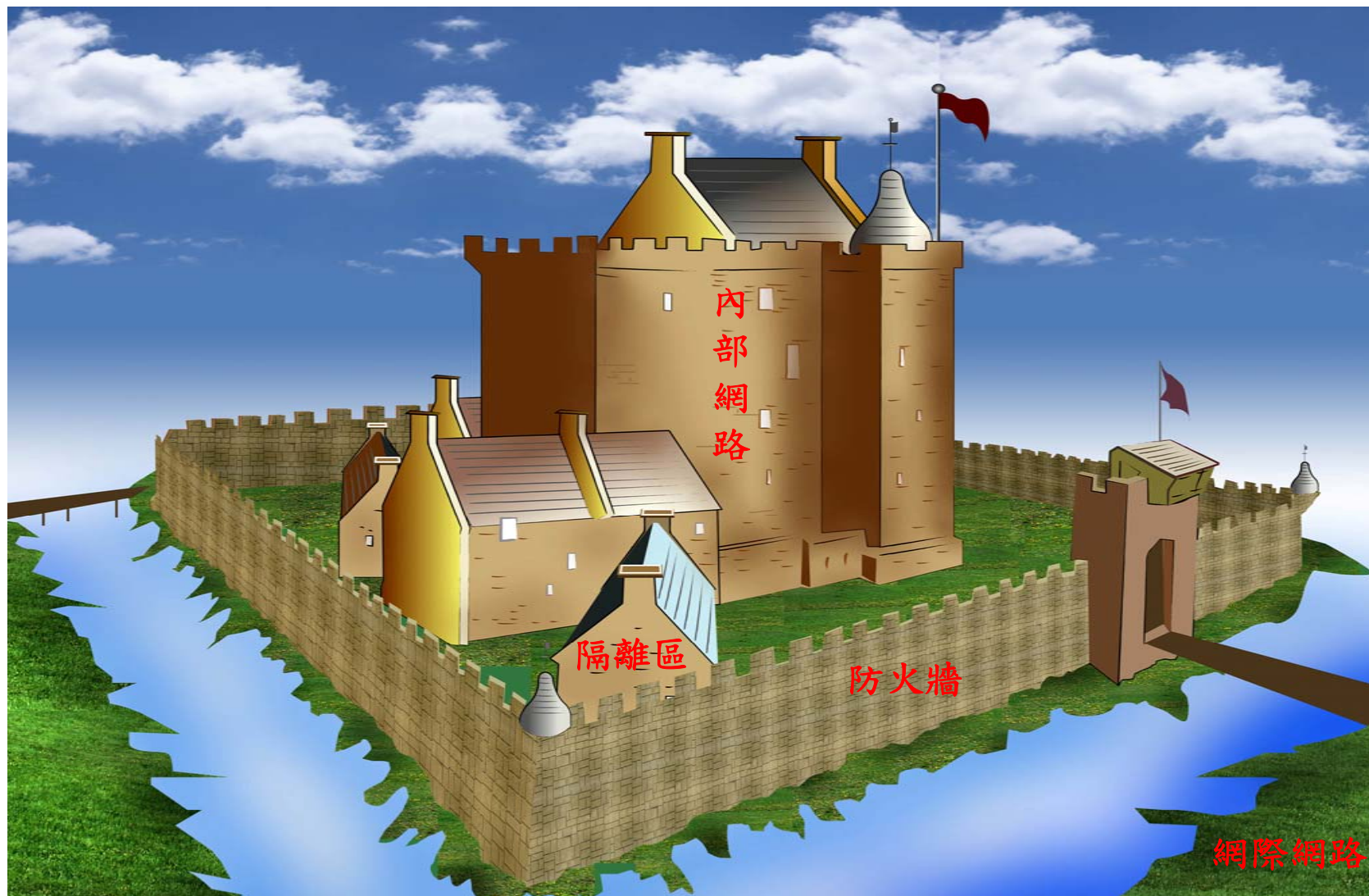
現行對於資訊安全的保護機制其實與古代的防禦機制是沒有差別的。

- 在現在，為了抵禦外來的威脅，企業都會定義資訊安全邊界。使用防火牆來保護邊界內的資源，**防火牆內還會使用入侵偵測系統來避免內部的威脅**。有些重要的單位還會有內外網路之分。
- 要進出防火牆的網路封包都會經過防火牆的檢驗，合法的封包才能進出。

資訊安全防護體系(古代)



資訊安全防護體系(現在)



安全四階

整個資訊安全防護體系其實是要達到四個目的：

- 嚇阻(Deter)

讓入侵者在面對目標時，會因為風險或代價太大而心生畏懼，因而打消入侵行為。

- 偵測(Detect)

當入侵發生時，能夠及時發現。

- 阻延(Delay)

使入侵行為困難，必須使用工具，耗費更多的時間和精力，以增加其被發現的機會。

- 禁制(Deny)

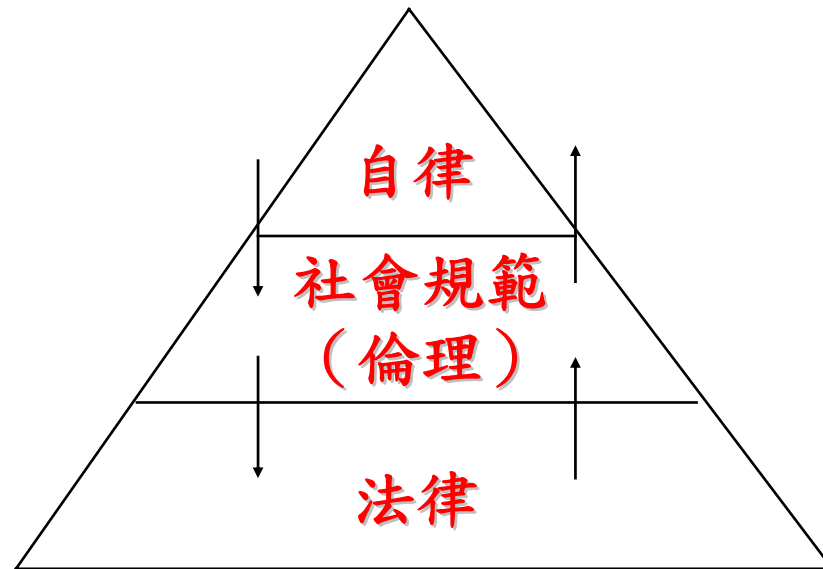
就是阻止入侵行為。

The background is a light green gradient with a darker green border. In the top left corner, there are faint, stylized icons representing a key, a padlock, and a shield. The main title is centered in a dark green, serif font.

第二章 資訊安全法令與管理規範

法令、調查及道德守則(1/10)

- 資訊倫理
- 資訊法律
- 電腦犯罪調查



法令、調查及道德守則(2/10)

資訊倫理的定義

- 資訊人員使用或製造資訊產品時，在面臨資訊相關之『**倫理議題**』上的權利與義務，以及賦予此倫理議題在決策或行動上之是非善惡的判斷基準。
- 資訊倫理大師 **Mason** 提出的四大議題：**PAPA**
 - 隱私權 (Privacy)
 - 精確性 (Accuracy)
 - 財產權 (Property)
 - 存取權 (Accessibility)

法令、調查及道德守則(3/10)

資訊隱私權

- 當事人對個人資料的主動支配權
- 議題：
 - 私人哪些資訊必須取得當事人同意，才可公開？
 - 雇主可對員工進行哪些形式的監視？
 - 哪些資訊可以自行保有，而不被強制公開？
 - 個體的哪些資訊需保存於資料庫中，且應保持何種程度之安全性？

法令、調查及道德守則(4/10)

資訊精確性

- 資訊的真實性，資訊品質的保障
- 議題：
 - 誰應當對所收集資訊的確實性、真實性及正確性負責？
 - 如何確認資訊將被適當地處理或正確地表達給使用者？
 - 如何確認資料庫內、資料傳輸及資料處理時的錯誤為偶發而非有意圖者？
 - 對於資訊錯誤誰要負責？受損害一方應如何受到補償？

法令、調查及道德守則(5/10)

資訊財產權

- 資訊擁有者對於該資訊具有持有、處置及利用之權力。
- 議題：
 - 誰擁有該資訊？
 - 其交換之公平價格為何？
 - 誰擁有資訊管道？
 - 如何處理軟體侵權？
 - 資訊管道之存取如何分配？

法令、調查及道德守則(6/10)

資訊存取權

- 個人或組織有權利可以取用什麼樣的資訊？可以在何種情況及保障下取用資訊？
- 議題：
 - 誰被允許存取資訊？
 - 允許資訊存取的所需資訊為何？
 - 電腦存取權要如何給無資格之員工？
 - 存取資訊所需之設備要提供給哪些對象？
 - 在何種情況或保護下，個人或組織有權利或特權獲得所需資訊？

法令、調查及道德守則(7/10)

- 法律：社會的最後一道防線
- 人為生存而守法，非為守法而生存
- 一般分類
 - 民法 (Civil Law; tort)
私法，規範私人間一般社會生活的法律
 - 刑法 (Criminal Law)
罪刑法定主義
 - 行政法 (Administrative/Regulatory Law)
規定與人民的權利義務事項
- 各國資訊相關法律：
 - 智慧財產權法 (Intellectual Property Law)
 - 資料保護法 (Information Privacy Law)
 - 電子監控法 (Electronic Monitoring)

法令、調查及道德守則(8/10)

電腦犯罪類型：

DoS、DDoS、偷竊密碼、網路入侵、訊息竊取、社會工程（利用社交能力擷取資訊）、不當內容、詐欺（利用電腦、網路）、軟體財產權、蓄意資訊收集（垃圾等）、惡意程式、IP假冒、偵探、偽裝、侵佔、欺騙、恐怖活動…等。

法令、調查及道德守則(9/10)

電腦犯罪特色:

- 調查和起訴時間緊迫
- 資訊大部分是不可觸及
- 調查會影響一個組織的正常商業活動
- 證據收集困難。
- 犯罪資料與正常商業資料可能在一部電腦上
- 可能需要電腦專家協助
- 犯罪地區可能廣達數個地理區隔，而有不同的司法管轄權。
- 大部分的司法權都已擴展包含電子資訊的財產權

法令、調查及道德守則(10/10)

電腦犯罪調查進行：

- 和法律執行單位聯絡（如偵九隊）
- 決定何時帶進法律執行單位
- 建立電腦犯罪的報告方法
- 建立處理此報告的程序
- 規劃進行調查
- 將資深管理者和相關部門參與調查
- 確保證據的收集、確認和保護

現行法規(1/2)

- 刑法妨害電腦使用罪專章
- 國家機密保護法
- 電腦處理個人資料保護
- 通訊保障及監察法

現行法規(2/2)

- 刑法妨害電腦使用罪專章(刑法第三十六章妨害電腦使用罪)
 - 刑法第三十六章妨害電腦使用罪，是用來規範駭客的行為，並且讓執法人員有法可辦。
- 國家機密保護法
 - 建立國家機密保護制度，確保國家安全及利益。
- 電腦處理個人資料保護法
 - 為規範電腦處理個人資料，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。
- 通訊保障及監察法
 - 為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序。

現行行政規定

- 行政院及所屬各機關資訊安全管理要點
- 行政院及所屬各機關資訊安全管理規範

行政院及所屬各機關資訊安全管理要點

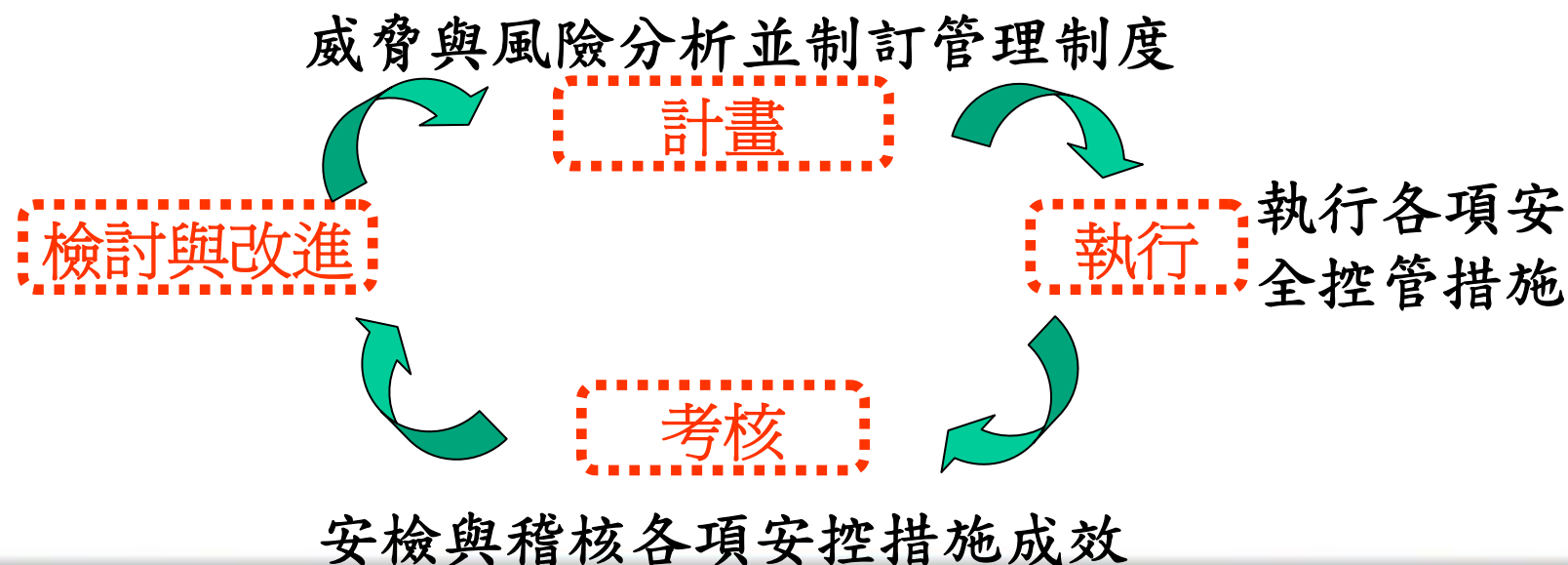
- 行政院為推動各機關強化資訊安全管理，建立安全及可信賴之電子化政府，確保資料、系統、設備及網路安全，保障民眾權益，特訂定本要點。
- 各機關應就下列事項，訂定資訊安全計畫實施，並定期評估實施成效：
 - (一) 資訊安全政策訂定。
 - (二) 資訊安全權責分工。
 - (三) 人員管理及資訊安全教育訓練。
 - (四) 電腦系統安全管理。
 - (五) 網路安全管理。
 - (六) 系統存取控制管理。
 - (七) 系統發展及維護安全管理。
 - (八) 資訊資產安全管理。
 - (九) 實體及環境安全管理。
 - (十) 業務永續運作計畫管理。
 - (十一) 其他資訊安全管理事項。

行政院及所屬各機關資訊安全管理規範

- 88/11/16行政院研考會（88）會訊字第05787號函頒。
- 依據「**行政院及所屬各機關管理安全要點**」中所要求必須訂定資訊安全計畫的事項之詳細實施規範說明。

資訊安全架構與標準(1/2)

- 資訊安全管理制度(Information Security Management System)：針對組織內部所使用之資訊，實施全面性之管理，以妥善保護資訊之機密性(Confidentiality)，完整性(Integrity)與可用性(Availability)並降低資安事件之衝擊至可承受之範圍。
- 資訊安全管理制度可分為PDCA四大部份，循環執行，不斷改進。



資訊安全架構與標準(2/2)

國際與國內資訊安全標準與法令

BS7799 / ISO17799	英國國家標準協會, 資訊安全管理機制 http://www.bsi.org.uk/
COBIT	國際電腦稽核協會, 資訊技術控制架構, http://www.isaca.org/
NIST	美國國家標準與技術協會, http://csrc.nist.gov/nistpubs/800-14.pdf
BIS Basel II	國際清算銀行/新巴塞爾資本管理協定 New Basel Capital Accord
我國政府規範	『行政院所屬各機關資訊安全管理實施基準/要點』 『財政部暨所屬機關資訊安全管理基準』 『金融機構辦理電子銀行業務安全控管作業基準』
我國法令要求	銀行法, 營業秘密法, 個資法, 刑法電腦犯罪
Electronic Banking Control	美國聯邦存款保險公司電子銀行控制架構評估—稽核規範

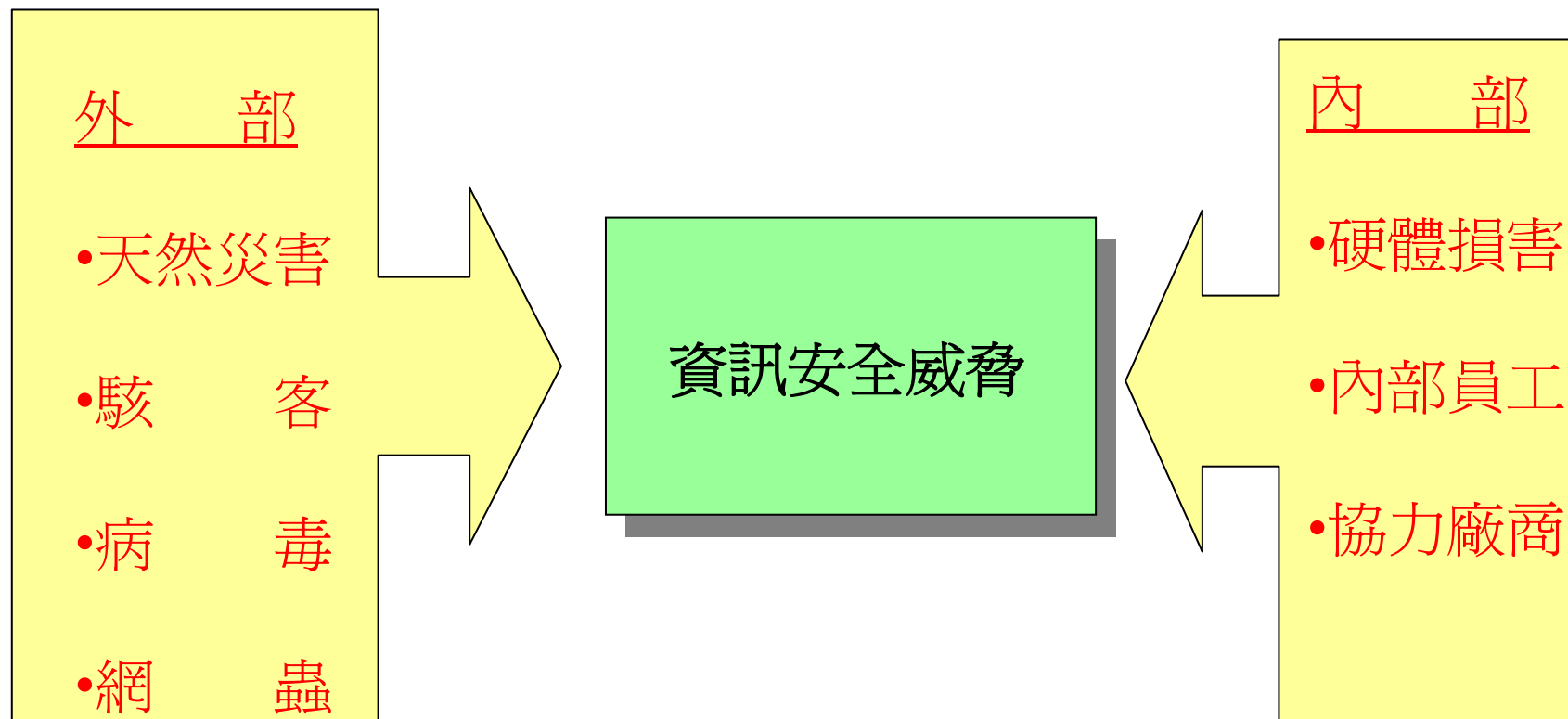
BS 7799(CNS17799/17800)

- 為目前國際上最知名的安全規範，而且已被ISO (International Organization for Standardization) 接納成為國際標準
- 台灣的國家標準CNS 17799、CNS 17800，就是參考BS7799的Part 1和Part2並加以中文化。
- 主要以ISMS風險評估管理架構進行安全管理，涵蓋所有的安全議題，是一套相當複雜的資訊安全應用與稽核的標準。



第三章 資訊安全的威脅

資訊安全的威脅



何謂風險？

- 安全威脅來自何處？
 - 攻擊類型、攻擊方式、攻擊位置
 - 內部隱憂外部威脅
 - 蓄意、故意、無意
 - 人為、自動
 - 天然災害、人為疏失
- 沒有一天是安全的

實體VS數位的威脅

- 來自實體入侵、破壞、偷竊等實際行為，而造成資訊洩漏、損毀、不堪使用等威脅。如：直接偷走硬碟、允許任何人進入機房，導致間諜可以直接從伺服器主機複製其所要的資訊等。
- 來自通訊時因竊聽、擷取通尋中的資訊，而造成資訊洩漏、損毀、不堪使用等威脅。如：監聽網路通訊，從中竊取帳號密碼、攔截電子郵件並加以竄改等。

網路VS系統的威脅

- 透過網路進行入侵系統、破壞、偷竊等行為，而造成系統、資訊洩漏、損毀、不堪使用與無法提供服務等威脅。如：離職員工入侵電腦偷走設計圖、駭客入侵刪除重要資訊或偷走商業機密等。
- 透過系統的弱點（設計上或設定上的錯誤、疏忽等），而造成系統、資訊洩漏、損毀、不堪使用與無法提供服務等等的威脅。如：駭客位於系統進行分散式阻斷服務攻擊（Distributed Denied of Services），利用Buffer Overflow入侵系統取得權限或使應用程式、系統當機等。

內部VS外部的威脅

- 有的時候威脅來自於內部的員工，員工盜賣內部資料、內部大樓配電盤失火，而造成資訊洩漏、損毀、不堪使用與無法提供服務等等的威脅。
- 其他的時候，威脅卻總是來自於非公司員工所發起的。例如商業間諜、網路駭客、電腦病毒演化等。

天然災害VS人為破壞的威脅

- 天然災害：
 - 火山爆發、海嘯、颱風、地震、蟲害。
- 人為破壞：
 - 駭客、恐怖份子、工業間諜、政府、惡意的程式

風險來自於哪裡？(1/2)

電腦環境的潛在風險：

風險的類型	範例
天災與實體	火災、水災、風災、地震 停電
非蓄意	未被告知的員工 未被告知的客戶
蓄意	駭客 恐怖份子 工業間諜 政府 惡意的程式

風險來自於哪裡？(2/2)

電腦環境的潛在弱點：

風險的類型	範例
實體	門未鎖
天然	火災、水災、風災、地震 停電
硬體與軟體	軟體版本過期、韌體過舊
媒體	電子干擾
通訊	沒有加密傳輸
人為因素	疏失

攻擊來自於哪裡？

- 所謂攻擊並非真正明刀明槍的攻擊，甚至可以為偽裝攻擊、傾聽攻擊、大家一起攻擊…
- 防禦的手法永遠比不上攻擊的腳步
 - 被攻擊再來防禦
 - 防禦有漏洞
 - 防禦不堪負荷
 - 被自己人攻擊
- 攻擊者不一定每次走相同手法

人為破壞(1/6)

- 駭客
- 病毒
- 後門程式
- 電腦蠕蟲
- 社交工程

人為破壞(2/6)

駭客：

- 駭客(Hacker)其實是一位以電腦工作來展示其強大程式技巧的人。其目的在於，測試自己的功力，並竊取他人的運算資源，以作為向更高難度目標攻擊的踏板。
- 駭客與非法入侵或闖入電腦系統的人不同，有時會被誤稱。其不同點在於，駭客入侵系統是為了追求知識，而非藉此牟利，更不會故意毀壞他人資料。

人為破壞(3/6)

病毒：

- 病毒是一種程式，一種會將自己附加在其它程式裡面的軟體，當附加程式被執行的時候，病毒程式也跟著啟動。
- 病毒具有傳播和感染的特性，可能會造成系統損害、刪除程式或者資料。病毒通常會附著在可執行檔或開機磁片、磁碟，甚至硬碟分割磁區，不過必須附加在其它程式中才能感染另一台電腦，某些病毒也會藉著電子郵件 (E-mail) 感染其它電腦。

人為破壞(4/6)

後門程式：

後門程式就不像電腦病毒一樣會感染其他檔案，後門程式通常都會以一些特殊管道進入使用者的電腦系統中，然後伺機執行其惡意行為（如格式化磁碟、刪除檔案、竊取密碼等），**Back Office**後門程式便是一個案例，透過該程式電腦駭客便有機會入侵主機竊取機密資料。

人為破壞(5/6)

電腦蠕蟲：

電腦蠕蟲像蠕蟲般在電腦網路中爬行，從一台電腦爬到另外一台電腦，最常用的方法是透過區域網路（**LAN**）、網際網路（**Internet**）或是 **E-mail** 來散佈自己。著名的電腦蠕蟲『**VBS_LOVELETTER**』就是一個例子。

人為破壞(6/6)

社交工程：

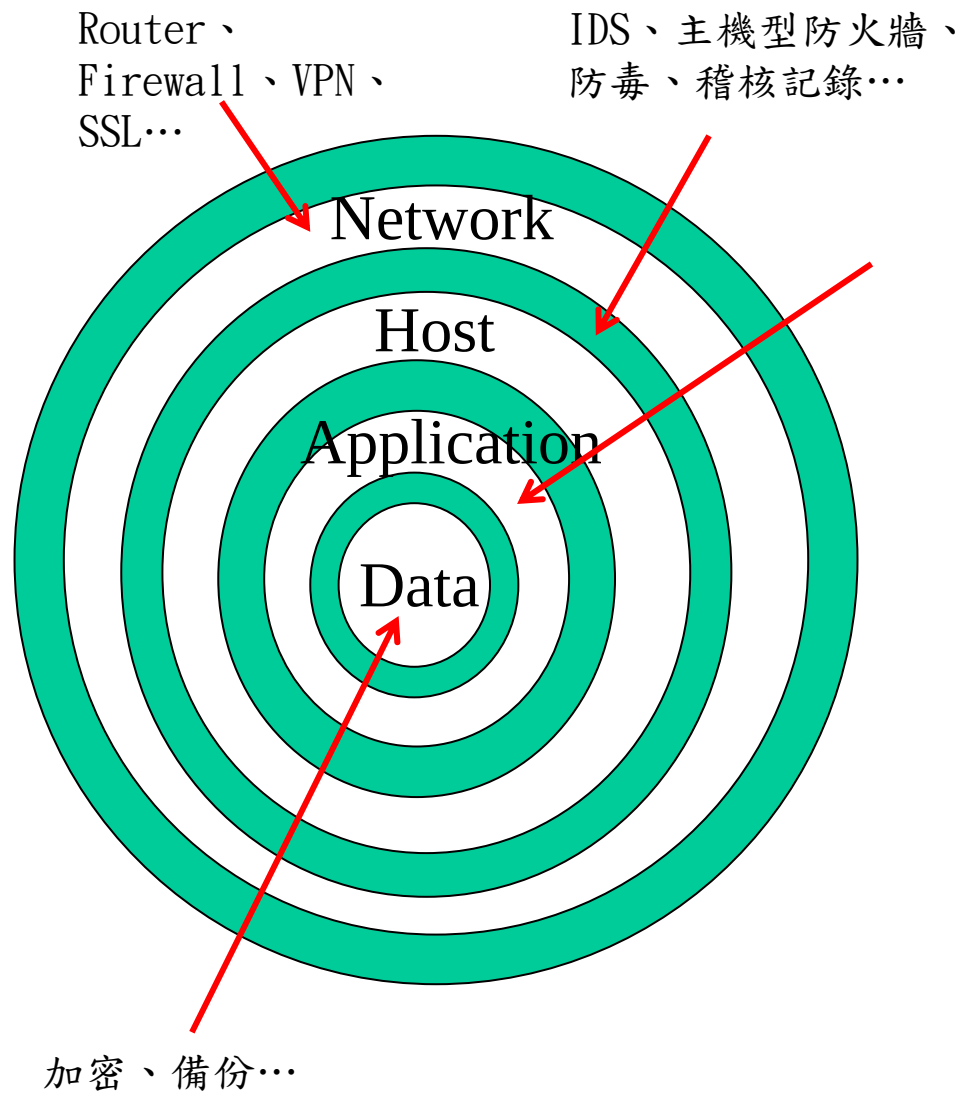
社交工程是一種攻擊行為，攻擊者利用人際關係間的互動特性所發展出來的攻擊法；通常攻擊者若無法直接取得主機 (Host) 內部資料時，會利用電子郵件 (E-mail) 或者電話，謊稱是某家網際網路服務供應商 (ISP) 的工程師，以維修測試系統的理由，騙取總機的重要資料 (Data)，再利用這些資料取得主機的最高權限，利用該台主機對其他系統出攻擊，或者乾脆將主機內部資料佔為己有。

The background is a light green gradient with a darker green border. In the top left corner, there are faint, stylized icons: a key, a padlock, a shield, and a document with a checkmark. The main title is centered in the middle of the page.

第四章

資訊安全基本防護概念

分層防禦



防禦方法

- 資料保護
- 傳輸保護
- 系統防護
- 入侵偵測
- 存取控制/入侵防護
- 系統管理

The background is a vibrant green with a layered, wavy design. At the top, there is a horizontal band containing several faint, white line-art icons: a key, a padlock, a shield, a speech bubble, a gear, and a square. Below this band, the green background transitions into a lighter shade with soft, white wavy lines that create a sense of depth and movement. The overall aesthetic is clean and modern.

第五章 結論

結論

維護安全的體認：

- 攻擊的發生無所不在與無法預測
- 內部才是攻擊的主力
 - 正面
 - 觀念灌輸
 - 教育訓練
 - 獎勵措施
 - 負面控制
 - 系統控制
 - 稽核
- 資訊安全是必須靠單位內的每一份子來共同維護