實體安全與資安管理

報告人：花俊傑

課程大綱

- 資安事件案例分析
- 實體安全的資訊風險
- 實體及環境安全管理準則
- 災難處理應變程序

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

資安事件案例分析

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

案例一

地點：日本 三井住友銀行 倫敦分行

案情：

因數名竊賊假扮成清潔人員，

偷偷在處理國際轉帳事務的電腦內，

安裝了鍵盤側錄程式，

差點竊走4億美元存款。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

案例二

地點：巴西 中央銀行

案情：

因竊賊花了三個月時間挖掘地道，而被搬走約21億台幣的現鈔，但是金庫內的攝影機與偵測器，卻完全沒有發揮任何作用。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

案例三

地點：美國 國稅局

案情：

存放納稅人資料的26個電腦磁帶，

竟在市政府大樓內遺失。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

MIS小陳的故事

- 小陳是一家美容保養產品公司的MIS人員，隨著電視上有關美容保養的節目強力放送，使得美容DIY保養已蔚為風潮，公司從一開始接受傳真訂單銷售，到自行擴建了網路平台，短短幾年間就搖身一變成為以電子商務為主的網路購物公司，小陳也晉升成為一個MIS小組長。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

MIS小陳的故事(續)

- 在公司機房主機的硬碟裡面，存放著這幾年來所有的客戶與交易資料，小陳每天都小心翼翼地注意機房的溫溼度、空調與電力系統，來維持這小型資料中心的正常運作，為了避免閒雜人等或是竊賊進入機房，小陳也建議公司設置了安全鎖，並且要求進出的相關人員必須填寫進出登記簿。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

MIS小陳的故事(續)

- 不過，總務人員說，為了方便維護一些資設備，也必須擁有一把鑰匙，所以小陳將另一把機房鑰匙交給總務人員保管，他在鑰匙上貼了「機房」二字的標籤之後，就把它放置在桌上的文件盒裡，有委外維護的廠商需要進入機房時，只要向總務打聲招呼就能拿到鑰匙，總務並沒有仔細核對其身份，更沒有填寫進出登記簿，因為他認為只有公司的員工才需要去填寫。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

您發現可能的資安問題了嗎？

- 問題一：經過總務座位的任何一個人，都有機會輕易地取得這把上面清楚地標示著「機房」的鑰匙。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

您發現可能的資安問題了嗎？

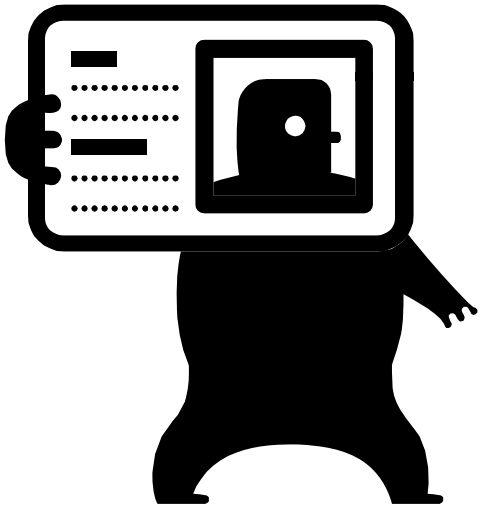
- 問題二：總務人員未核對廠商身份，只要有人偽裝成維護人員進入機房，企業的重要設備或是儲存的資料，就會成為待宰的羔羊。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

您發現可能的資安問題了嗎？

- 問題三：人員進出未加以記錄，出了事要如何追查？誰該負責？



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

小陳的故事告訴我們

- 機房鑰匙未妥善保管——

  顯示員工的資安教育訓練應加強，在企業的存取控制政策中，更應明訂鑰匙和通行碼保管人須善盡使用保管責任。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

小陳的故事告訴我們

- 未核對委外服務廠商的身份——

  顯示出人員管制有疏失，企業對於委外服務的廠商，必須要確認其維護人員是否有事先申請，並且取得了管理階層的授權，在核對身份無誤之後才能進行相關作業，並且最好要有專人陪同。

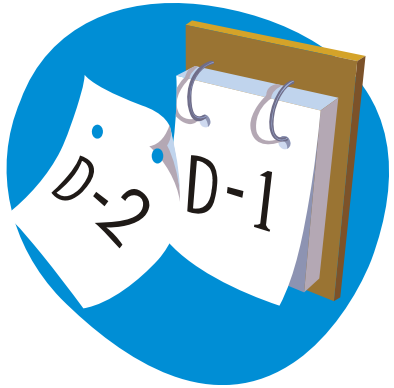


本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

小陳的故事告訴我們

- 出入人員未填寫登記簿—

顯示缺乏標準的作業程序(SOP)，就算來訪人員經過身份確認之後，也必須配戴清楚的身份識別標示，並且詳實記錄進出機房的日期與作業時間。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

實體安全的資訊風險

什麼是資訊？

- 對企業組織有價值的事物
- 資訊本身也是一種資產



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

資訊資產的類型

- 書面文件
- 電子檔案
- 傳輸中的資料
- 影片多媒體
- 進行中的對話



⇨ 不管資訊的形式是什麼，或者分享或儲存的方式是什麼，都應該受到適當的保護。

資訊是組織的無形資產

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

什麼是資訊安全？

- 保護資訊資產的機密性、完整性與可用性



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

資訊安全三要素

- 機密性(Confidentiality)

  資訊不可被未經授權的個人、實體、流程所取得或揭露



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

資訊安全三要素

- 完整性(Integrity)

  確保資訊的準確與完整



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

資訊安全三要素

- 可用性(Availability)

  資訊在需要時可被授權者存取及使用



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

資安風險來自於

- 有某項威脅，
  很可能會利用已存在的弱點，
  對於資訊資產的機密性、完整性、可用性
  造成危害。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

什麼是實體安全？

- 實體安全是為了避免自然或人為因素影響資訊安全，因此必須確保重要設施與資訊資產不會遭到無意或有意的洩漏、竊取與破壞。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

威脅有三種

一、外部：颱風、火災、雷擊、地震等。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

威脅有三種

二、內部：如電力、空調系統失效等。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

威脅有三種

三、人員：如偷竊、惡意破壞及門禁管制疏失等。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

損失有二種

- 一種是資產設備的失竊，會造成直接的財務損失。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

損失有二種

- 另一種則是重要資訊的遺失，
  輕則使商譽受損，
  重則甚至造成整個企業營運的中斷。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

面對外部威脅

- 針對外部威脅的預防，我們可以先從自然災害的評估著手，像是調查所在區域的颱風、地震頻率，以及救援單位能夠及時到場協助的時間。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

面對外部威脅(續)

- 另外，對於建築物本身的設計整建，是否使用防火建材、強化玻璃等，可以進一步要求對大樓結構進行強化，以抵擋自然災害的侵襲。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

面對內部威脅

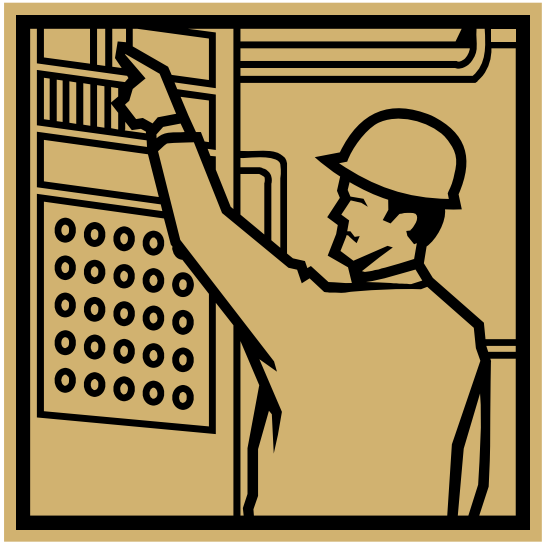
- 至於內部威脅的預防，主要是為了維持設備的正常運作，企業必須具備主要電力與備援電力獨立配電系統，另外像是針對突波與瞬間斷電的預防、總開關防護、發電機安置地點及供油儲存，也要有良好的規劃。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

面對內部威脅(續)

- 在空調系統方面，在機房內需要有恆溫、恆濕的溫濕度控制與空氣濾清裝置，對於大樓出入風口也要有妥善保護。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

面對人員威脅

- 許多企業對於所謂進出人員的管制，往往只是流於形式而已，這也是發生不當的內部資料存取與設備被竊的主要原因。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

面對人員威脅(續)

- 惡意人士只要透過社交工程(Social engineering)手法，像是冒充委外廠商的服務人員，或是尾隨在企業員工之後混入，甚至是假裝為同一公司員工，但是忘了帶門禁卡而請他人代刷，都可以輕易取得通行權進入企業內部環境。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

面對人員威脅(續)

- 依責任分散原則，以避免各項權限都集中在一人身上。
- 系統或網路管理人員在設定對於資訊的存取權限時，請務必遵循最小權限原則(Least Privilege)，讓員工不會接觸到不符合其職等權限的資訊，以避免資訊外洩的可能。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

員工資安管理注意事項

- 在人員聘雇方面，在錄用前、在職中及離職後需要注意的事項有：
  1. 人員招募時的注意事項
  2. 成為員工後的安全教育
  3. 離職人員處理的安全步驟

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

員工資安管理注意事項(續)

- 人員招募時的注意事項：

  若是職務涉及資訊安全或是敏感性的工作，應盡可能地去了解該人員的背景，例如詢問曾任職公司的人資部門或單位主管，也要確認該人員所提供的資料，像是離職證明與學歷資料是否屬實。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

員工資安管理注意事項(續)

- 成為員工後的安全教育：
  - 員工被正式錄用後，依員工的職務等級，要進行相關的資安教育訓練，使員工明瞭公司的資安政策與資安法令。
  - 正式員工須簽署同意遵守公司相關政策的規定，如網路、郵件、電話使用規範等，必要時還須簽署保密協定，同意即使在離職之後，不可對外洩露職務上所獲悉的商業機密。
  - 員工若從較低職等升遷至較高職等時，需要人資部門進行人員的背景審核，並且告知該職等所需遵守的資安規範。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

員工資安管理注意事項(續)

- 離職人員處理的安全步驟：
  - 從離職生效日開始，IT人員須將員工的帳號與資訊資產暫時停用，待確認所有檔案權限都順利移轉之後，再將該員工帳號和權限刪除。
  - 在員工離職當天，要收回各項實體設施的存取權限，像是職別證、門禁卡、Token、文件櫃鑰匙等。
  - 公告離職員工名單，尤其務必告知櫃檯接待人員，若是善意離職的員工，應由主管陪同離開原辦公處所，若是不太友善或是遭到革職的員工，則建議由警衛人員護送離開。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

實體及環境安全管理準則

實體安全管理要項

- 以下可作為執行實體安全管理時的參考：
  - 一、設定實體安全邊界
  - 二、進出人員管制措施
  - 三、設備安全管理
  - 四、機房之安全管理

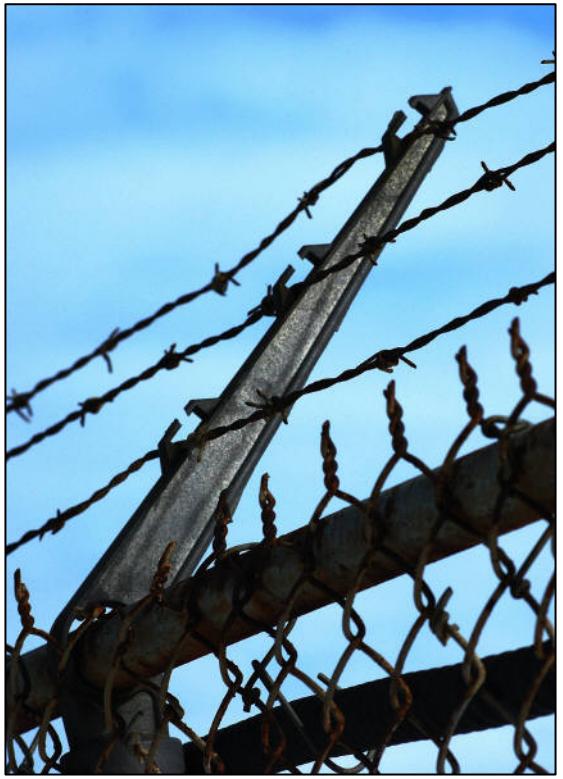


本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

一、設定實體安全邊界

- 建築物週圍可設立實體隔離設施
- 加強燈光照明系統
- 設置重點監視設備
- 保全人員巡邏



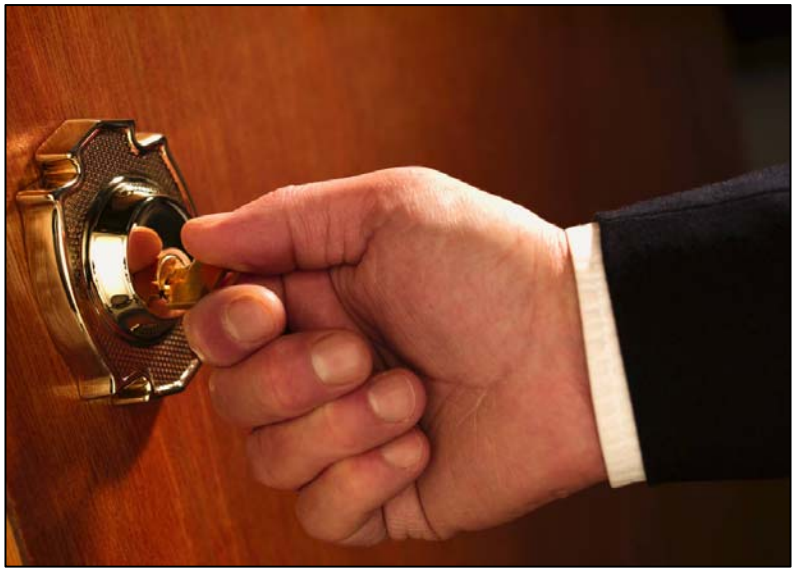


本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

一、設定實體安全邊界

- 對於無人門窗應予以上鎖，無人區域與重要設施，宜定時派人巡邏，或安裝防盜與監視系統。





本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

一、設定實體安全邊界

- 對於邊界進出口須設置警衛、檢查哨，並且進行人員及車輛進出管制。
- 識別方式可採取識別證、磁卡、生物辨識等。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

補充：關於身份識別

- What you have
- What you know
- What you are







本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

二、進出人員管制措施

- 來訪人員應要求出示身份識別，配戴身分識別標示，並記錄進出的日期與時間。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

二、進出人員管制措施

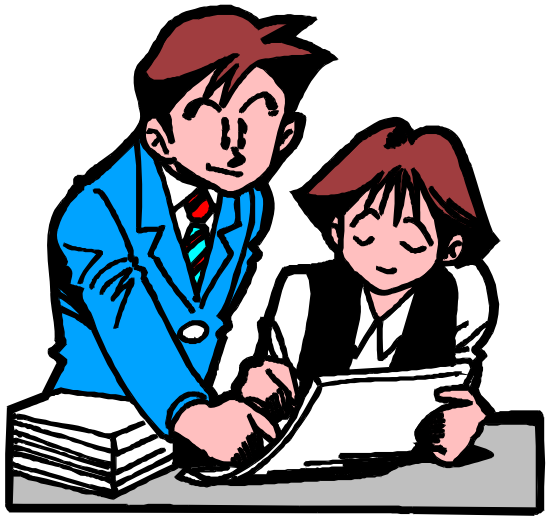
- 人員進出區域與動線需妥善規劃，來訪人員不應直接進入員工作業區域。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

二、進出人員管制措施

- 技術支援或維護服務人員，需事先取得授權才能進行作業，若需進入作業管制區，須經由專人陪同才能進入，或搭配可錄音錄影之監視系統。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

二、進出人員管制措施：

- 未經適當申請程序之人員，禁止留在辦公室單獨作業。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

二、進出人員管制措施：

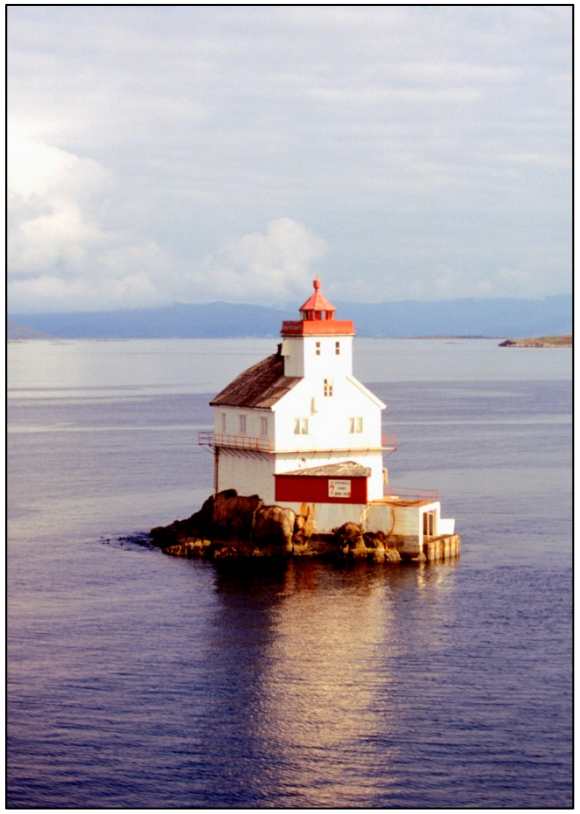
- 已調職或離職人員，
  禁止進入原工作之區域。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

三、設備安全管理

- 存放或處理敏感性資料的設備，應放置在可以監控的地點，並且提供足夠的電源供應，尤其是需要特別保護的設備，務必採取獨立區域存放。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

三、設備安全管理

- 設備所使用的通訊線路，必須採取隱藏或地下化的保護措施，以避免遭到資料截取與線路破壞。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

三、設備安全管理

- 設備的維護必須由授權的維護人員來進行，若是委由廠商維護，針對維修人員必須通過身份識別或是陪同進行。
- 在維護的過程中，必須將所排除的錯誤或是變更進行完整記錄，若需送回廠商處維修時，也必須按照設備攜出之規定進行，設備攜回或送修，應清除內含所有的敏感性資料。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

三、設備安全管理

- 在敏感區域，所有未經授權之資訊設備，皆不可攜入或攜出，需要攜入或攜出辦公室之設備則必須加以記錄檢查。





本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

三、設備安全管理

- 外勤人員所使用的筆記型電腦，必須安裝防毒或個人防火牆，並且提供適當的資料保護措施，並且要求不可將設備置於可能發生偷竊之地點。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

三、設備安全管理

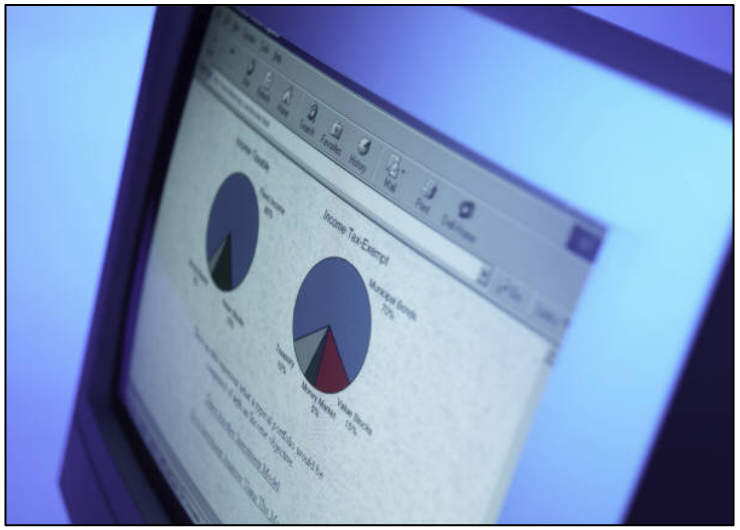
- 企業之無人設備需有使用保護機制，所列印之資訊應要求立即從印表機上取走，敏感資訊應採用受管制監控之設備來列印。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

三、設備安全管理

- 人員離開座位或是下班之後，辦公處所應實施桌面淨空政策，將文件與儲存媒體置於上鎖之櫃子，電腦螢幕應啟用螢幕保護程式。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

三、設備安全管理

- 需要報廢與再使用之資訊設備，必須針對其內含之儲存媒體，進行如低階格式化的資料刪除與重複覆寫，以確保資料能完全清除。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

四、機房之安全管理

- 機房設置地點需考量天災發生頻率，並避免鄰近火源、水源和交通頻繁地點。
- 機房之位置，應盡量避免過於明顯的標示，以免成為侵入和攻擊的目標。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

四、機房之安全管理

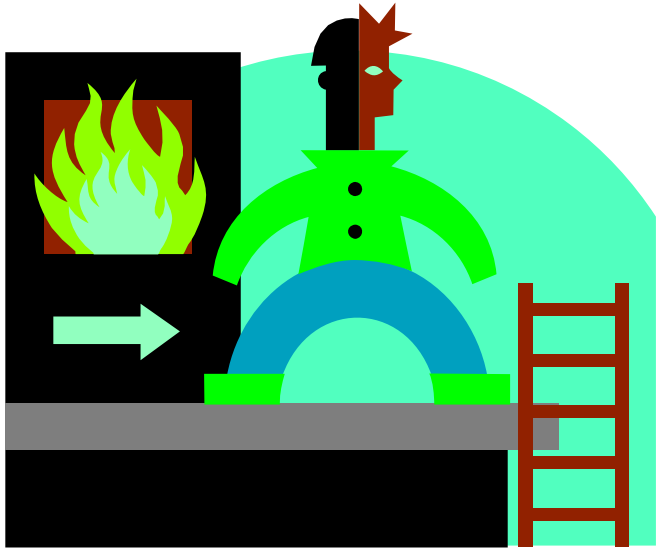
- 機房應具備門禁管制設備或上鎖，視情況設置監視設備，人員出入需取得授權並登記日期時間。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

四、機房之安全管理

- 機房需考慮採用如高架地板、隱藏佈線、地板承重度及排水、耐火等功能。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

四、機房之安全管理

- 機房應擁有獨立與備援之電力支援，對於重點設備應考慮優先供電設施及不斷電系統。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

四、機房之安全管理

- 危險及易燃性之物品，絕對不可存放在機房中。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

四、機房之安全管理

- 機房應裝置煙霧偵測器、溫度感知器等火警設備與空調系統，並且設置滅火器材以防止火災的發生。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

四、機房之安全管理

- 機房之備援設備，應存放一定之安全距離，以避免災害發生時一併遭到損毀。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

四、機房之安全管理

- 機房人員應熟悉緊急應變程序，並且定期實施消防演練，做好疏散及消防設備的使用測試。

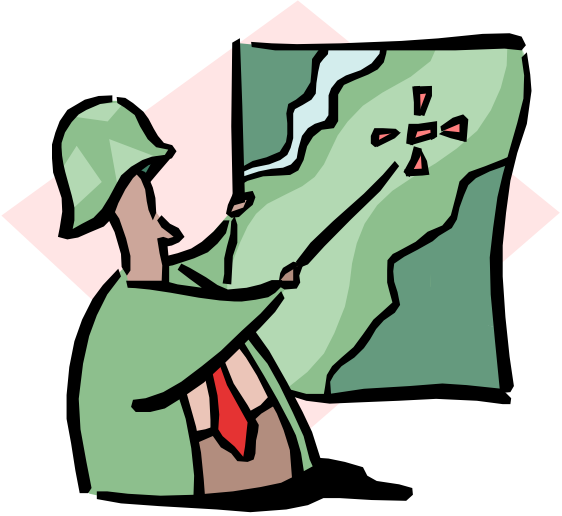


本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

災難處理應變程序

實體安全與營運持續

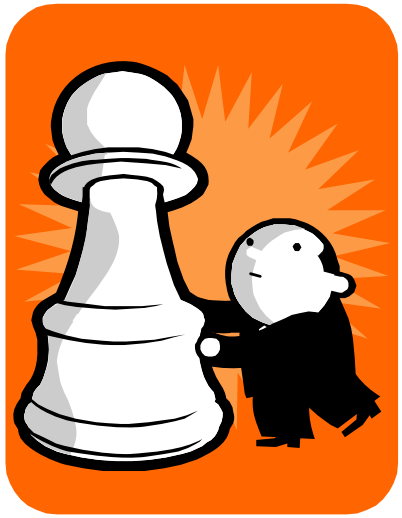
- 面對實體安全問題所造成的營運中斷，對資訊人員而言，最好的辦法就是在意外事件發生之前，根據各種可能的狀況，擬定好如何應對的策略。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

營運持續管理思考的方向

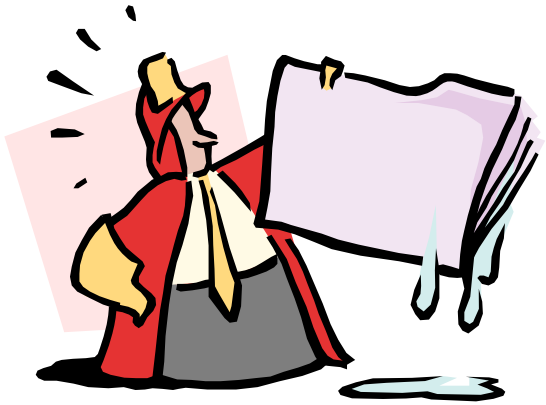
- 災難前，根據各種情況擬好應對策略
- 災難時，確保關鍵營運流程不會中斷
- 災難後，能夠在最短時間內回復作業



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

落實營運持續管理精神

- 一旦災難真的不幸發生，就可以根據這些事先定義的作業程序來緊急應變，以確保關鍵的業務運作不會因災害而中斷，並且在最短的時間內，盡快將所有系統和服務回復到正常運作。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

從國際標準看營運持續管理

- 目前，有關營運持續管理(BCM)的規範，英國的BS25999是個很好的參考，這項標準分為兩個部份：
  - BS25999-1是作為落實營運持續的參考手冊，對於營運持續管理系統，有完整的描述與實施說明；
  - BS25999-2則是對於營運持續的管理要求，同時也是一個可以作為驗證的標準。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

從國際標準看營運持續管理(續)

- 在BS25999標準中，它提供了整個營運持續管理實施的策略與框架，讓我們可以依照不同的產業屬性，擬訂有效的應對策略，目的就是要降低災難發生時的損失。
- 其中最重要的就是必須成立緊急應變小組，在災難發生的第一時間內，依照所擬定的緊急應變計劃來進行，避免人員、系統、組織受到更多的傷害。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

擬定災難緊急應變程序

- 以機房火災為例，在撰寫實體安全應變程序時，建議可從以下角度來思考：
- 偵測–

1. 煙霧警報器偵測到異常狀況
2. 由機房值班人員發現火警
3. 警衛室收到大樓火警警報



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

擬定災難緊急應變程序(續)

- 通報–
  1. 通知相關負責人員前來處理異常情況
  2. 確定為火災時，由值班人員或警衛室通知消防單位。
  3. 以廣播系統通報辦公處所人員儘速離開



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

擬定災難緊急應變程序(續)

- 判斷–

1. 機房人員必須進行初步判斷，因此，必須清楚定義事件的等級與對應的措施。
2. 是否可自行撲滅，或是針對異常事件進行持續監控，以採取更進一步的處理。
3. 處理時務必以人身安全為第一考量。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

擬定災難緊急應變程序(續)

- 處理–
  1. 移除火點附近的易燃物品
  2. 使用鄰近的滅火器滅火
  3. 關閉機房設備之電源或主電源
  4. 若備有自動滅火系統時，應按照標準操作程序進行。
  5. 消防人員前來處理時，應描述現場情況及注意事項。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

擬定災難緊急應變程序(續)

- 記錄–

機房人員務必牢記，所有的過程都必須要留下文件或記錄檔，以便進行後續的事件追蹤查核，並且作為日後改善的目標。

應填寫記錄包括：

1. 機房日誌
2. 機房異常事件處理記錄表
3. 機房火警緊急處理程序記錄表

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

總結

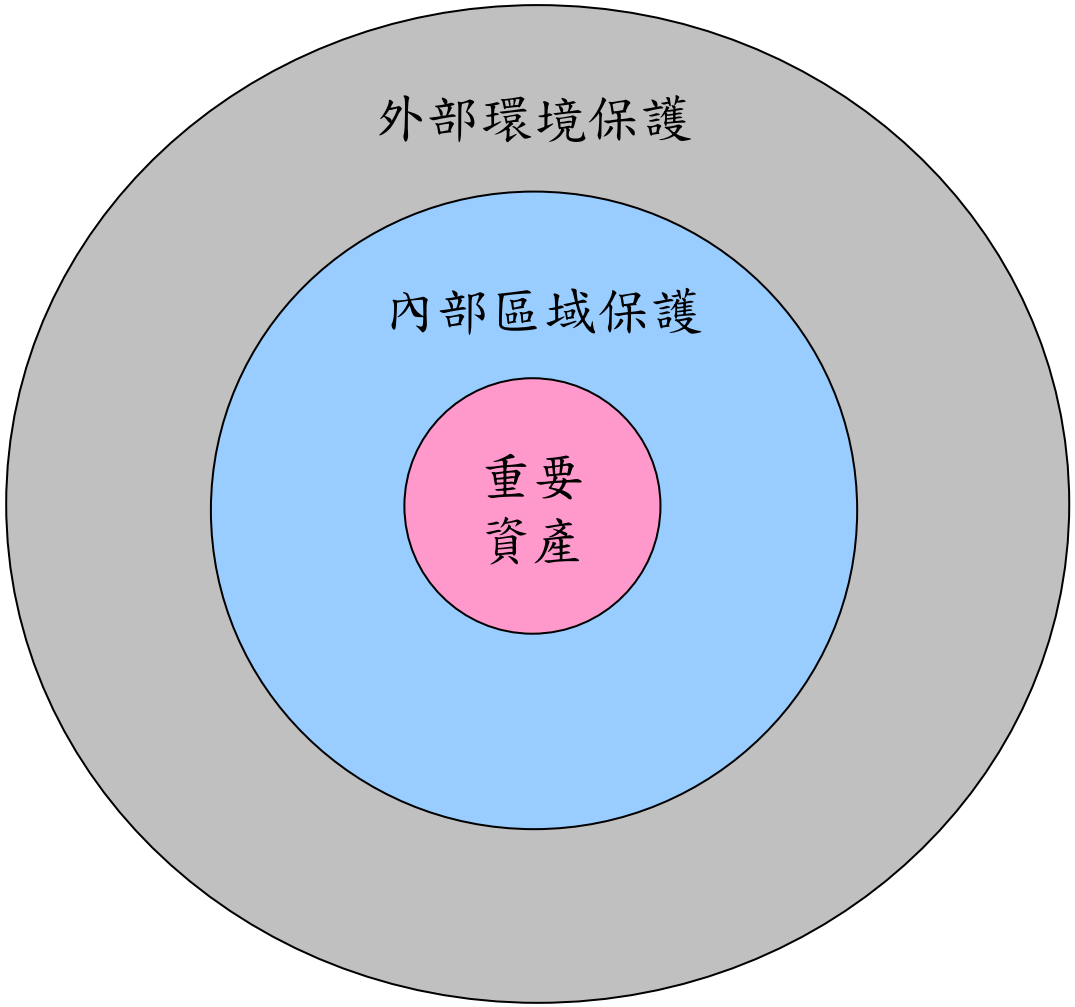
問題

- 為什麼您所建置的資安設備，像是防火牆、防毒牆、入侵防禦系統皆正常運作中，系統也沒有發現或回報任何異常狀況，但是重要企業資訊仍被駭客竊走？

答：因為檔案伺服器主機整台被偷走～

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

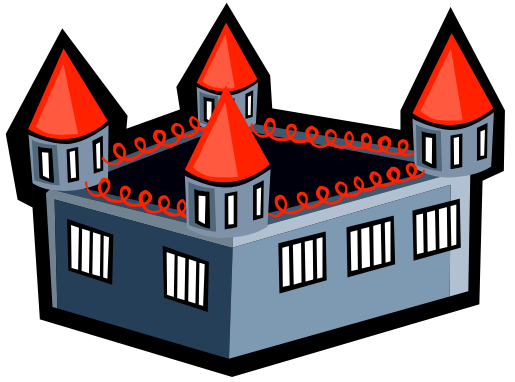
縱深防禦的概念



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

縱深防禦的概念(續)

- 第一步：評估有哪些屬於敏感的安全區域
- 第二步：依照不同安全等級的區域，選擇適當的安全控管措拖。
- 第三步：定期測試與稽核



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

選擇控制措施應考量

- 所需耗費成本
- 技術相容性、可擴充性
- 使用者接受度



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

國際標準是最佳參考指引

- 在ISO27001中，已針對實體及環境的安全管理，提供明確指引與實作建議，可避免關鍵設備或機密資訊受到不當的存取、損害與干擾，企業能夠藉由落實各項控制措施來降低可能發生的風險。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

資訊安全的最大問題來自於

“人”



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

落實實體安全與資安管理

- 資安管理的目標—

  讓資安意識成為組織文化的一環



資訊安全。
人人有責。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

問題與討論



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

Thank You!

聯絡人：花俊傑

Jackhwa@systex.com.tw

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。