國中小學資安認知及資安推廣活動種子教師巡迴教育訓練

主辦單位：教育部

執行單位：安侯企業管理股份公司

臺灣知識庫股份有限公司

99年9-10月

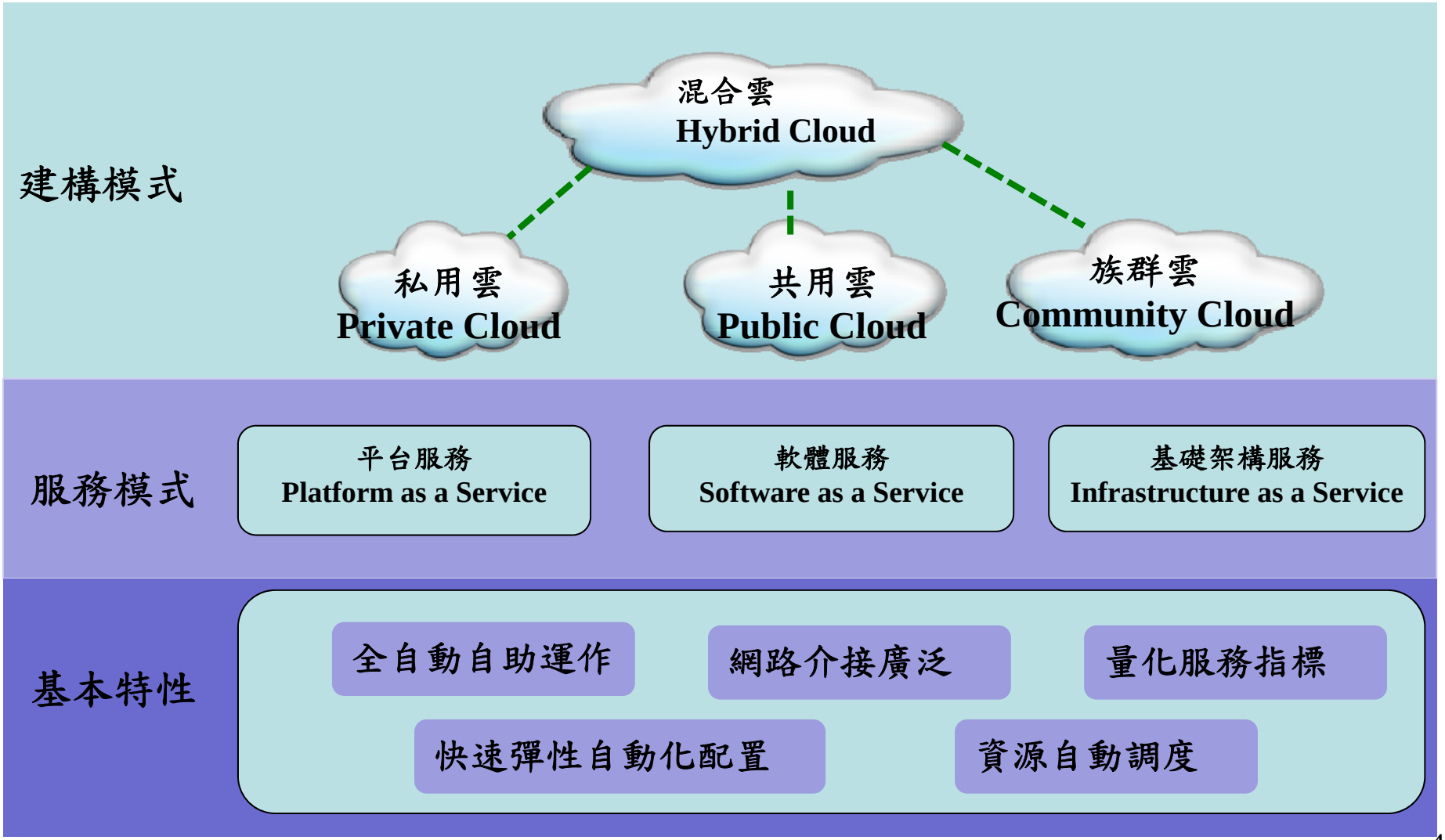
簡報大綱

- 資訊安全上雲端
- 資訊安全案例探討
- 個人資料保護法探討
- Q&A

簡報大綱

- 資訊安全上雲端
- 資訊安全案例探討
- 個人資料保護法探討
- Q&A

何謂雲端運算(Cloud Computing)



雲端服務模式與優勢

雲端服務模式	雲端服務優勢
• **軟體服務化 (SaaS)** —透過網際網路存取雲端的應用程式 —全功能環境 —資料內容、展現、軟體及管理 • **平台服務化 (PaaS)** —將客戶開發的應用程式部署到雲端的服務 —軟體開發架構、中介軟體、資料庫、訊息傳遞 • **基礎架構服務化 (IaaS)** —處理器、儲存、網路以及其他資源的租用服務 —電力、空調、網路、硬體等	• 一切都能行動化 •協同作業 •輕易蒐集資料 •可調節的商業應用程式負載 •執行速度快 •擁有較高階的儲存結構 •成本降低（維護硬體、電費耗用、程式開發） •系統的容錯率較高 •快速分享

教育體系雲端服務運用的可能方向

- 將教學與學習相關運用資訊(例如：課程教材，測驗評量，學習成果)，持續累積儲存在雲端服務之資料中心，成為教育知識管理中心
- 老師與學生透過終端設備與連網服務，從教育體系雲端服務來取得教學相關資訊與學習運用資訊，讓老師教學與學生學習可以獲得更多運用彈性，不受到時空限制
- 整合現有電子化教室(例如電子白板、電腦、廣播教學設備與電子書包)與教育體系雲端服務，透過結合既有軟硬體與雲端服務內容提供，讓教學方式更多元化，學習成效更提升

從資訊安全觀點看雲端服務

- **雲端服務之威脅**
  - 掌控到雲端的連線
    - 讓使用者在連上網頁應用程式時，先轉往地下惡意網站，然後才到達自己的網頁應用程式頁面。
  - 攻擊雲端本身
    - 攻擊者有可能利用標準的殭屍網路/傀儡網路 Botnet 來讓雲端基礎架構上的主機超載而癱瘓。
  - 雲端服務業者資料外洩
    - 直接從雲端擷取有價值的資料 ，例如：信用卡、身分證號碼、登入帳號密碼等等。

運用雲端服務資訊安全原則（一）

- **識別資訊資產特性**
  - 機密性(Confidentiality)
  - 完整性(Integrity)
  - 可用性(Availability)
- **評估需求選擇服務**
  - SaaS
    - 整合度高、最複雜、不易擴充
    - 安全控管由供應商負責
  - PaaS
    - 介於Saas與IaaS之間
  - IaaS
    - 軟體功能彈性最佳
    - 安全控管由客戶負責

運用雲端服務資訊安全原則（二）

- **資安風險管理**
  - 弱點掃瞄(Vulnerability scan)與滲透測試(Penetration test)
  - 弱點、威脅及衝擊衡量
  - 程序安全性規範
- **法規遵循與稽核**
  - SLA(Service Level Agreement)
  - 執行稽核活動
  - 簽定權責歸屬合約
- **備份**
  - 備份在不同資料中心以確保資料運作的高可靠性

簡報大綱

- 資安訊安全上雲端
- 資訊安全案例探討
- 個人資料保護法探討
- Q&A

實例一：知名社群網站變更密碼通知

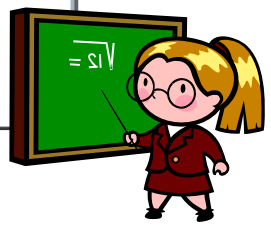
- **資安案例**

近期有垃圾郵件假借知名社群網站帳號通知的名義，信件內容謊稱：為了確保帳號安全，要求用戶重新設定知名社群網站帳號，而使用者若想要知道其重新設定的帳號，就必須先開啟郵件中的附件檔案，來誘使知名社群網站使用者開啟郵件中夾帶檔案。而實際上這個附件檔中隱藏了一個名為「Trojan Bredolab」的木馬程式。

資料出處：資安人 2009/10/30

資安觀點

- 至**知名社群網站**頁面變更密碼
- 帳戶已被盜用或無法重設密碼，可與該業者聯絡。
- 安裝防毒軟體，並定期更新病毒碼



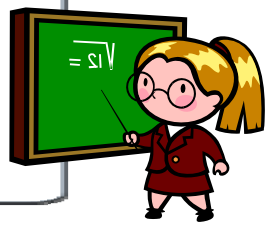
實例二：受害人無「話」可說

- **資安案例**

美國聯邦調查局（FBI）今天發表聲明指出，詐騙集團有新招術，就是針對受害者手機、家用或公司電話發動上百通來電阻斷通話管道，同一時間卻盜領受害者銀行帳戶。這種把受害人打電話對外求證、求援的通話管道通通切斷的詐騙伎倆，FBI稱為「**電話阻斷服務式攻擊**」（**telephone denial-of-service attack**）。到今年4月為止這種攻擊方式越來越常見，在美國東部幾州都有案例發生，受害者以一般民眾及中小企業居多。 資料出處：2010/6/22 中央社

資安觀點

- 避免暴露或張貼過多個人隱私或機敏性資料到網路上
- 經常性地更新網路銀行密碼



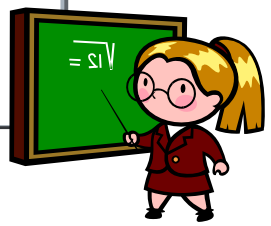
實例三：事故通報單回收訂飲料

- **資安案例**

  幫同事訂飲料，可能因此丟掉飯碗！發生旅客在車上昏迷、送醫後不治意外，員工事後竟將旅客死亡事故通報單回收用來訂飲料，導致旅客資料外流。事件的處理過程通報單，日前卻被員工回收用來「訂飲料」，紙張背面寫滿「LR去S」、「紅茶半S少I」等訂飲料資訊，訂完飲料後，這張單子就被棄置地上，導致旅客猝死事件曝光、當事人資料外流。　資料出處：2010/3/8 自由時報

資安觀點

- 如公務上公文或表單不再需要或作廢，應統一集中管理處理或者當下立即使用碎紙機進行銷毀，避免機敏文件不當洩漏



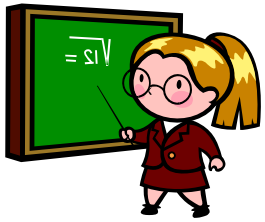
實例四：入侵電腦選課 女大生被訴

- **資安案例**

大學的邱姓女學生因和林姓同學發生爭執，竟然以林女在學校的帳號、密碼進入該校選課系統，將其所選的2門科目辦理退選，致使林女喪失上課權利，檢方偵辦之後，依無故侵入他人電腦罪將邱女起訴。　資料出處：2009/12/1 自由時報

資安觀點

- 密碼應保持適當長度，建議應在6個字元以上
- 定期更換密碼一次(例如每季或每半年)
- 密碼更改時新密碼不應與前一次密碼有重複，密碼設定應有數字與英文字母夾雜，建議可包括特別字元
- 避免將帳號、密碼記錄於書面或張貼於容易洩漏之場所
- 當有跡象足以顯示密碼可能遭破解或被竊取時，應立即變更密碼



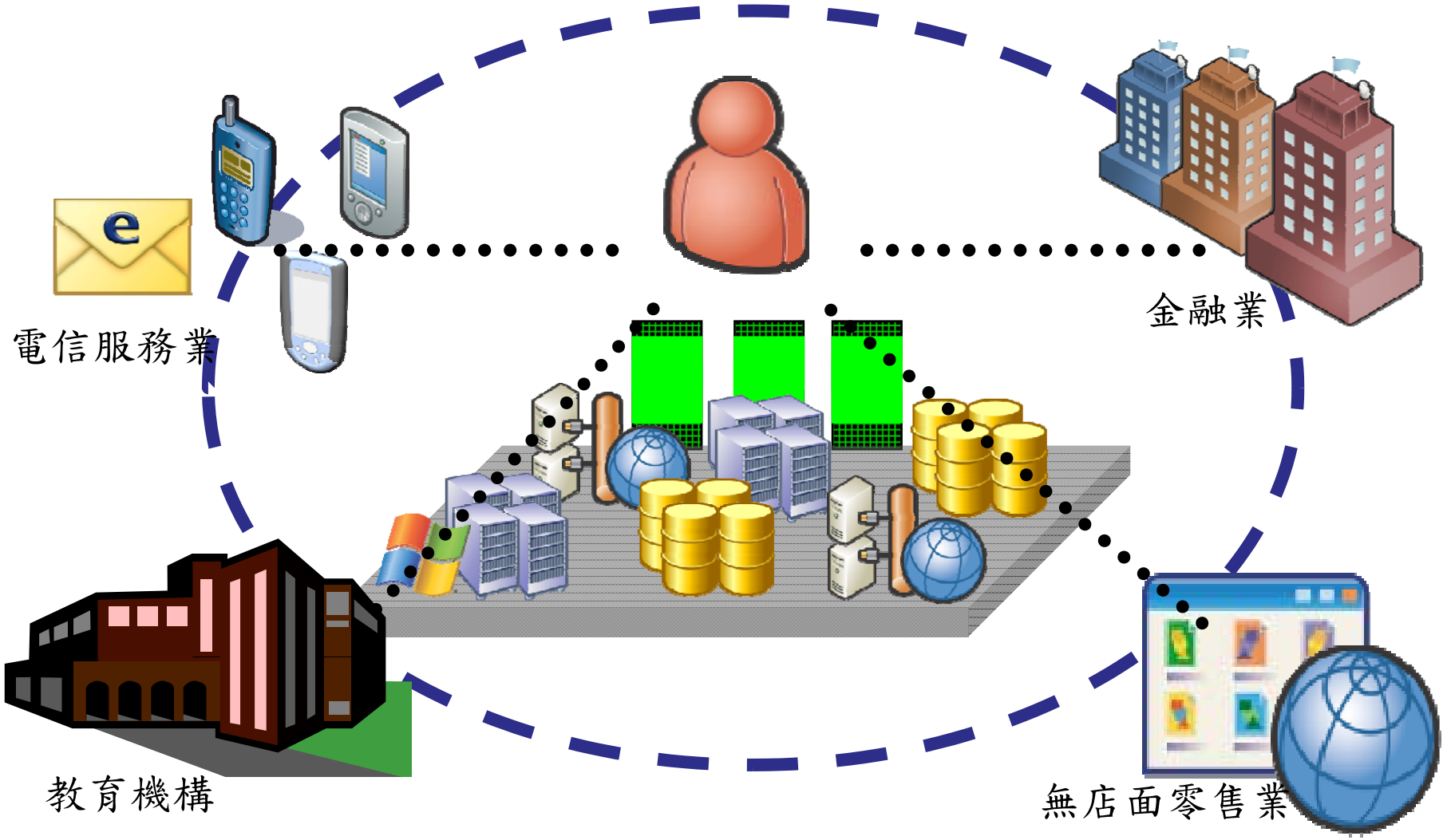
駭客入侵常見手法（影片展示說明）

- 發送垃圾郵件
  - 匿名信件
  - 夾帶惡意程式檔案
  - 網路連結
- 網站尋找獵物
  - 交友社群網站
  - 論談網站
  - 購物網站
- 檔案分享
  - 非法下載網站
  - 檔案分享軟體（例如：BT、Flashget、FOXY、FTP等）

簡報大綱

- 資訊安全上雲端
- 資訊安全案例探討
- 個人資料保護法探討
- Q&A

無所不在的個人資料



個資的價值

一個存有個資的小小隨身碟＝台北帝寶豪宅

- 假設每筆求償金額為10,000元台幣。若有20,000筆資料遭竊或不慎外洩，求償金額將可達10,000x20,000= 200,000,000（台幣2億元）
- 也就是2萬筆個人資料的價值，約等於台北市帝寶豪宅一戶(120坪含雙車位)

人手一支的USB隨身碟，至少可儲存個資檔案數萬至數百萬筆

姑且不論資料本身的附加價值，僅幾萬筆個資盜失所造成的損害賠償金額，就已等同於1戶以上帝寶豪宅價值

台灣富豪珍藏的台北帝寶豪宅，每戶至少價值1.5 - 2億以上

99年5月公告之新版個資法第二十八條—公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。

被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。

依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。

實例一：個人隱私於網站外洩

案例說明：

A機關於辦理某計畫，甄試業務員，不過甄試結束後竟然發現甄試人員的身份證字號、電話、學歷、地址等個人資料，全被登錄上網，儘管該機關已經立即將網頁移除，不過仍可於著名搜尋引擎網站上，依然可以找到暫存檔。

資安事故原因分析

資料管理人員未考量個人資料之敏感性，即公告於公開網站，遭搜尋引擎列入查詢

預防措施

1.提高人員個資保護認知
2.必要公布之敏感資料應加密保護，並利用電子憑證等認證方式限制存取權限
3.審視單位個人資料保護之規範，制訂控制措施

實例二：系統開發疏失導致隱私外洩

案例說明：

B機關於建置之專案補助研究計劃查詢資料庫中，民眾發現只要把滑鼠游標移到姓名的連結上，瀏覽器左下方就會出現該生的身分證字號，總計有一萬八千名學生的個資可供查詢。經媒體投訴，B機關查證後才發現程式有漏洞，已緊急修補。

資安事故原因分析

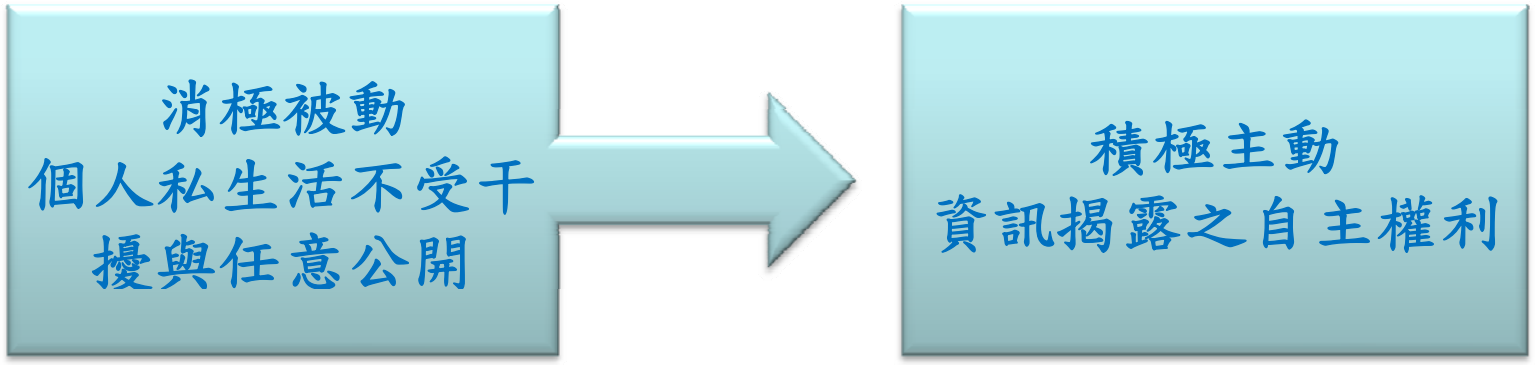
資訊系統於開發過程中，未考量及確認相關的安全要求及測試，導致開發上程式的疏失洩漏個人資料

預防措施

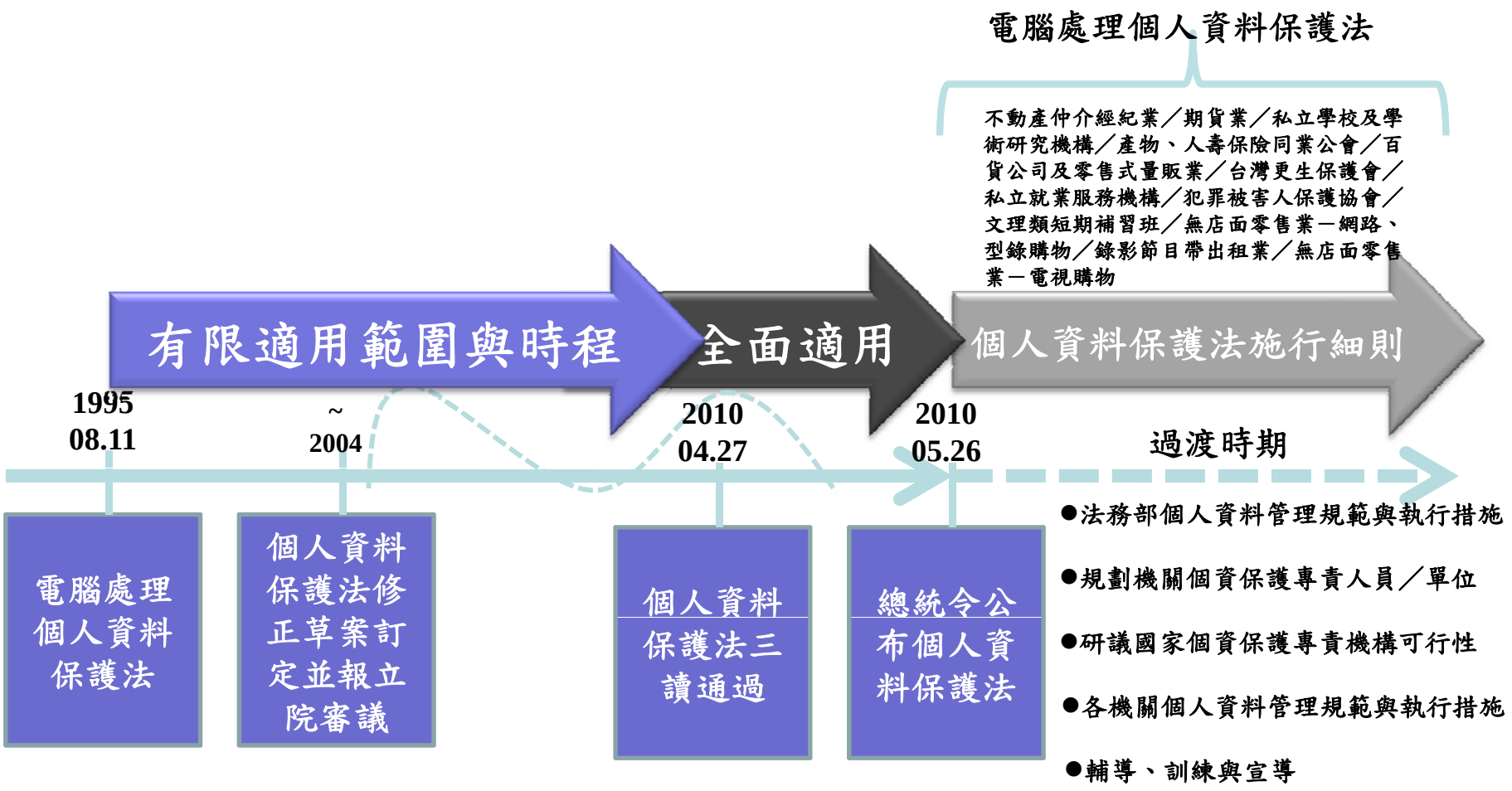
制訂資訊系統變更或上線之安全要求，並落實程式及資料之安全控制程序、測試與稽核

資訊隱私權概念

- 資訊隱私權
  - 個人自主控制個人資料之權利（資訊自決權）
  - 個人有決定是否接露個人資料、及在何種範圍內、於何時、以何種方式、向何人接露之決定權。
  - 個人對其個人資料之使用有**知悉與控制權及資料記載錯誤之更正權**。（釋字第603號）



個人資料保護法修正歷程與重要政策



個人資料保護法修訂方向

- 修法背景：
  - 法務部為因應急速變遷之社會環境，近年來彙整國內學界與實務界之修法建議，並參考其他國家之個人資料保護相關法令，針對原「電腦處理個人資料保護法」進行修訂
  - 99年4月由立院三讀通過後，已於99年5月由總統府公告
  - 修訂法案共有56條，名稱修訂為「個人資料保護法」
- 修正方向：
  - 擴大保護客體
  - 普遍適用主體
  - 增修行為規範
  - 強化行政監督
  - 妥適調整罰則
  - 促進民眾參與

個資法施行細則修訂方向

項次	個資法施行細則修訂方向
1	將明訂公部門各機關資料保護政策，並特別考慮明確保護個人資料自主決定權與個人資料合理流通之並重等議題。
2	將針對不確定法律概念之內容，如識別、刪除等技術性概念，或書面同意等程序性概念，給予程度性或定義性之明確規範，或標準化作業流程。
3	將明訂委託關係之責任，如受託者個資保護責任應明訂於委託契約、受託者員工教育訓練措施，或委託者之行政檢查義務。
4	將明訂安全維護事項（或計畫）之標準，如個資管理流程、資安管理流程與水準等。
5	將確定公務機關執行個資保護之協調聯繫機制。
6	將明訂依據個資法第十七條所規範，公務機關所持有個資類別等依法應公告事項之公告期限。

個人資料保護控管程序

- 一般個人資料（組合後足以識別特定個人）：姓名、出生年月日、身分證字號、護照號碼、特徵、指紋、家庭、教育、聯絡方式、財務狀況等
- 特種個人資料：醫療、 基因、性生活 、健康檢查、犯罪資料

蒐集		■ 直接或間接方式取得個人資料 ■ 特種資料不得任意蒐集 ■ 對當事人告知之義務 ■ 當事人同意/拒絕之機制
處理		■ 建立或利用個人資料檔案所為之紀錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結、或內部傳送 ■ 銷毀：違反法律規定、特定目的消失、期限屆滿 ■ 查詢：當事人行使權力之機制
利用		■ 組織將個人資料作跨國(境)之處理或利用內部資料傳送—處理 ■ 將個資提供第三人—利用
國際傳輸		■ 將個人資料作跨國(境)之處理或利用 ■ 在個人資料受保護之前提下跨國傳輸

教育部現階段之因應作為

- 正研擬個人資料保護之相關辦法，未來將要求機關學校（含公私立學校）配合遵守，亦或是由各機關學校修改、引用適當之項目
- 針對C、D級機關學校(主要是技術學院、專科學校以及高中職)已選出26所學校，後續將於99年9月到12月針對**資訊安全管理與個人資料保護作業**進行稽核
- **如想要更了解個人資料保護相關工作事項，建議可參考「教育機構個人資料保護工作事項」**

蒐集階段之提醒事項

提醒事項	參考範例/建議做法
個人資料如何取得（含教職員生）？	教職員人事資料、學生資料
個人資料取得其形式為何？	紙本、電子形式
個人資料取得的管道是否安全？	檔案加密、加密通道
如何確認所取得之個人資料正確性？	人工檢查
醫療、健康狀況原則上不得蒐集，惟因學校保健室提供相關服務，在施行細則公佈前，以妥善儲存為重點。	N/A

處理階段之提醒事項

提醒事項	參考範例/建議做法
確認具有查詢、調閱或更正權限之人員，是否為其職務所需，並經主管審核、確認？	帳號、權限之申請紀錄
存放個人資料之主機、個人電腦，其管理者帳號是否有共用帳號？	各自持有自己的管理者帳號、通行碼
個人資料於內部傳送時是否安全？	彌封、檔案加密
是否召開資安管理與個資保護之相關會議，並留下稽核軌跡？	會議簽到表、會議紀錄
機關副首長是否擔任召集人，統籌跨單位之資源運用？	會議簽到表、會議紀錄

儲存階段之提醒事項

提醒事項	參考範例/建議做法
存放個人資料之主機與PC安全性？	作業系統、應用程式、防毒軟體是否定期更新
存放個人資料之主機、PC之環境？	門禁控管、共用設施安全
個人資料是否備份？備份之可讀性？	定期回復測試
備份資料（含異地備份）存放環境之安全性？	門禁控管、公用設施安全
紙本形式之個人資料是否妥善保管？	門禁控管、公用設施安全

銷毀階段之提醒事項

提醒事項	參考範例/建議做法
個人資料保存年限？	依照校內規範、相關法令法規要求來辦理
個人資料銷毀、刪除之方式？	實體破壞、電子刪除
個人資料如保存期限屆滿，是否需要傳送至外部，或進行銷毀、刪除？	依照校內規範、相關法令法規要求來辦理
若個人資料需傳送之外部，其傳送方式是否安全？	彌封（掛號）、檔案加密、加密通道
（其它項目）人員是否持續施予資安教育訓練？	針對個資保護辦理相關課程

教育體系資訊安全教育資源

- 教育部校園資訊安全服務網

  http://cissnet.edu.tw/download_tanet.aspx

  - 教育部 TANet 網路中心導入資訊安全管理制度計畫教育訓練教材
  - 教育部提昇校園資訊安全服務計畫 - ISMS 相關教育訓練教材
  - 資訊安全技術教育訓練教材
  - 教育部所屬館所資訊安全稽核教育訓練教材
  - **資安認知教育訓練教材**
    - **各級學校教職人員資安認知課程教材**
    - **各級學校主管資安認知課程教材**
    - **電子郵件使用資安認知課程教材**
    - **上列三份線上教材另已上傳到教育部數位學習服務平台，可供學習參考運用，網址如右：https://ups.moe.edu.tw**
  - 其他教育訓練教材

Q & A

簡報完畢，敬請指教