



「雲嘉區域網路中心」 個人資料保護法因應與介紹

NII產業發展協進會
吳昭儀 經理

課程大綱

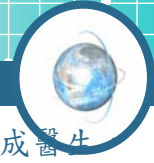


- 1 資訊安全事件與案例分析
- 2 個人資料保護法介紹
- 3 如何提升個人資料保護能量
- 4 資料保護工具說明



- 1 資訊安全事件與案例分析
- 2 個人資料保護法介紹
- 3 如何提升個人資料保護能量
- 4 資料保護工具說明

案例1-個人資訊外洩



一個醫療公司沒有嚴格的流程來規定和散佈或共享患者資訊。一個人冒充成醫生並向醫療公司要求患者Don Hammy的醫療資料，接待員並沒有對打電話的人提出疑問便告知Don Hammy有腦瘤。一週以後Don Hammy沒有獲得他申請的職位，並發現公司老闆打過電話了解他的醫療資訊。

❖ 法律認可義務

- 醫療公司沒有適當的政策和程序來保護患者資訊
- 雇主無權打這種電話，並不得用醫療資訊來拒絕潛在員工

❖ 未遵循的要求標準

- 敏感資訊由醫療公司員工釋放給未獲授權的人
- 雇主要求他無權獲得的資訊

❖ 可能造成的傷害和破壞

- 由醫療公司洩露的資訊帶給Don Hammy巨大困擾，並使他不能獲得特定工作
- 雇主根據他無權獲得的資訊作出決定。非法獲得的資料被用于決策過程

經過了長期的法律糾紛，Don Hammy最終贏得官司，戰勝腦瘤，買了一座小島，再也不用工作了。

資料來源：CISSP Certification All-in-One Exam Guide

案例2-駭客入侵



一個金融機構Cheapo公司購買了必要的應用軟體來提供客戶線上銀行交易，但沒有增加任何網路通訊和線上交易所必需的安全防衛措施。

在前2週裏，22位客戶的核算和存款帳戶被駭客攻擊，共損失439,344.09美元。

❖ 法律認可義務

- Cheapo 公司沒有安裝防火牆或IDS，鞏固持有客戶帳號資訊的資料庫，或對客戶交易使用加密保護
- Cheapo公司並未有效保護其客戶的資產

❖ 未遵循的要求標準

- 由於沒有建立適當的安全策略和計畫，也沒有使用必要的安全控制，Cheapo違反了12項管理金融機構的美國聯邦規範

❖ 可能造成的傷害和破壞

- 22個人損失439,344.09美元的事實與金融機構未執行線上銀行的規定及未曾實施應有的注意直接相關

最後，很多帳戶都被攻擊、金額被清空。人們對Cheapo公司共同起訴，很多人得回了他們大部份的錢，而原先的金融機構Cheapo公司現在只能賣玉米卷了。

資料來源：CISSP Certification All-in-One Exam Guide

All Rights Reserved by NII產業發展協進會

5

案例3-國內個資外洩新聞



❖ 補習班惡鬥偷個資 判賠1500萬

補習班惡鬥風波又一樁！台中康○○英語補習班被對手哥○○美語補習班控告以駭客方式竊取兩萬多筆客戶資料，哥○○公司提起二點四億多的附帶民事賠償，台中地院判決應賠償一千五百萬元。

康○○被控自九十五年十二月起，負責人余○○指示該公司程式設計及網路管理工程師許○○、游○○利用自己撰寫的程式，駭入哥○○電腦，竊取該公司客戶資料、客戶訪談記錄及相關營業資訊等紀錄。

游○○坦承，余○○指示他和許○○，進入哥○○系統取得客戶資料，用業務擴張之用。哥○○公司電腦資訊部邱姓員工也作證，入侵他的電子郵件必須知道其信箱，只有離職員工許○○擔任副總經理時，曾知悉其密碼。哥○○公司因此提起附帶民事賠償。

法官參考哥○○提供的廣告費用支出、自行陳報推估的來客成交率等資料，認定該筆客戶資料利益為一千二百萬元；另，康○○雇用哥○○公司離職員工，從事與該公司競爭之美語顧問營業，又共同竊取該公司營業秘密，其侵害行為屬典型同業競爭商業間諜模式，惡行非輕，懲罰性賠償金三百萬元，合計共應賠償一千五百萬元。

資料來源：[中時電子報20010-08-21](#)

All Rights Reserved by NII產業發展協進會

6

案例4-國內個資外洩新聞



❖ 啟能中心遭竊／七台電腦飛了／內有身障謀生個資

【記者羅正明／綜合報導】○○啟能發展中心昨天遭竊7台電腦，院內收容的76名身心障礙者個案資料全在裡面，相關輔導、就業紀錄也在其中，中心運作幾乎陷入癱瘓狀態，只期盼小偷可憐這些身障者，把電腦還給他們。

○○○說，失竊的電腦，價值21萬餘元，但裡頭的個案資料，包含個人基本資料、日常生活紀錄、輔導紀錄，這些都是訓練身障者謀生技能、自給自足、重新在社會站起來的重要參考依據，價值難以估算。

○○啟能發展中心期盼闖入偷他們電腦的小偷也能良心發現，趕快歸還，也呼籲善心人士捐輸電腦，協助他們重建資料檔案。



資料來源：TVBS-N 2007-09-03

All Rights Reserved by NII產業發展協進會

7

案例5-國內個資外洩新聞



❖ 團費刷卡洩個資 信用卡被盜刷

2010-08-30華視

知名雄○旅行社竟然傳出有員工盜刷客戶信用卡，這名宮姓員工利用客戶信用卡資料用傳真機回傳確認的方式，竟然就偷偷抄下客戶資料，到網路上盜刷客戶信用卡，刷了28名客戶資料，得手將近100多萬元。

客戶個人資料一張張的傳進來，信用卡資料就是像這樣被雄○旅行社內的員工偷看，然後上網盜刷。這個宮姓員工竟然利用自己的職務，看了起碼28名客戶信用卡資料然後上網盜刷，再將買來的東西變賣，得手百萬。真的是很可怕，只要這些信用卡資料一外漏，就可以上網盜刷，到底有什麼秘密，藏在信用卡裡。

仔細一看，這正面的信用卡號，然後卡片日期，最重要的是，背後小小的數字，叫做授權碼，有這三個要素，這名員工就可以在網路上盜刷客戶的卡片。不管是訂票，還是購物都可以刷，而且當你發現的時候，已經是月底看帳單的時候。

這是利用信用卡盜刷，刷卡時間跟對帳單時間差距，這名宮姓員工，刷了28名客戶資料都沒被發現，現在雖然已經被揪出來，旅行社也把這名員工開除，不過大公司內出現這樣的問題，客戶信用卡這麼隱私的資料外洩，雄獅旅行社的客戶個資保密的確出現了漏洞。

All Rights Reserved by NII產業發展協進會

8



遭駭客入侵 ○○教育局加強網路機密維護

【大紀元6月25日報導】（中央社記者陳朝福二十五日電）

○○市國中校務系統被駭客入侵，學生基本資料被竊，○○市政府教育局已與負責廠商聯繫，移除入侵程式，也將加強維護網路資訊機密。

教育局今天表示，○○市國中校務行政系統委由廠商服務，這次國中學生資料被駭客竊取，是這程式遭駭客侵入，所竊資料供補習班招生、宣傳、寄送資料等用途，目前調查尚無其他用途。

教育局已與負責廠商聯繫，將入侵程式移除，並修補程式漏洞，並加強網路安全，以維護學生權益。



❖ ○○部員工電郵密碼 Google全都露

2010-08-28自由時報

約兩千筆資料外洩 部長也在列

政府機構資安出現嚴重漏洞，網友爆料，○○部員工約兩千筆電子郵件的姓名、帳號與預設密碼，竟然可以透過Google搜尋到，連部長、前部長的帳號與預設密碼也全都露，資安專家認為，若資料落入有心人士手中，恐將嚴重威脅國家安全。



❖ 客戶資料外洩 ○○銀行遭罰400萬元

【聯合報／記者薛翔之／即時報導】2010.12.09 10:33 pm

駭客入侵！「風控模範生」○○銀行爆發逾萬筆客戶資料外洩案，金管會今天委員會會議決定處罰○○銀行新台幣400萬元；這也是網路銀行崛起後，首宗因駭客入侵、並遭處分的大規模案件。

金管會表示，○○銀行日前偵測發現，有木馬程式試圖進入網路銀行系統「活動」，由於銀行無法強化網路銀行資訊安全的內部控制作業，導致有特定IP位址成功登入銀行網路銀行。

金管會也指出，網路銀行的客戶存款，沒有異常，不過，有超過1萬筆的客戶資料外流。

金管會表示，網路駭客犯案手法，推陳出新，為確保金融機構資訊環境安全，銀行應落實資訊安全內部控制執行情形，務必作到「網銀安全零風險、金融資安百分百」，金管會也將資安，列為稽查重點。

課程大綱



- 1 資訊安全事件與案例分析
- 2 個人資料保護法介紹
- 3 如何提升個人資料保護能量
- 4 資料保護工具說明



- ❖ 立法院於**99年4月27日**，將電腦處理個人資料保護法，修訂並三讀通過為「個人資料保護法」
- ❖ 「個人資料保護法」**99年5月26日**總統府正式公布，施行日期由行政院定之。主要修訂方向為：
 - 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

個人資料保護法－範圍擴大



- ❖ 擴大適用行業
 - ✓ 原適用八大行業(徵信、醫院、學校、電信、金融、證券、保險及傳播業)。
- ❖ 個資新定義與科技演進結合
 - ✓ 原個資定義：姓名、生日、身份證字號、特徵、指紋、婚姻、職業等
 - ✓ 增加了護照號碼、犯罪前科、聯絡方式，並將原病歷擴大為需考量醫療、基因、性生活、健康檢查等。
- ❖ 調整資料儲存型式定義：
 - ✓ 原有對儲存於電磁紀錄物或其他類似媒體。
 - ✓ 調整為以自動化機器或非自動化個人資料之集合。

個人資料保護法—加強個資保護及通報因應



❖ 加強個資保護

- ✓ 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。（詳個資法第2章第18條）
- ✓ 非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。（詳個資法第3章第27條）

❖ 個資外洩時主動告知當事人

- ✓ 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。（詳個資法第1章第12條）

個人資料保護法—提高賠償責任與罰則



❖ 提高賠償責任與罰則

- ❖ 公務機關在非天災等不可抗力因素外，導致個資外洩而侵害當事人權益時，得依每人每一事件新台幣500元~20000元以下；若造成多數人權益受損時，則由2000萬調高至2億。（請詳第4章第28條）。

❖ 加重違反罰則

- ✓ 違反時仍為處以二年以下有期徒刑、拘役並由原有的4萬元以下罰金增加為20萬（請詳第5章第41條）；
- ✓ 增加意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而生損害於他人者，處5年以下有期徒刑、拘役或科或併科新臺幣100萬元以下罰金（請詳第5章第42條）。



個資法第二條

- 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

個資法第三條

- 當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：
 - 一、查詢或請求閱覽。
 - 二、請求製給複製本。
 - 三、請求補充或更正。
 - 四、請求停止蒐集、處理或利用。
 - 五、請求刪除。



個資法第五條

- 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。



個資法第六條

- 有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：
 - 一、法律明文規定。
 - 二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。

個資法第六條

- 三、當事人自行公開或其他已合法公開之個人資料。
- 四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。



個資法第七條

- 第十六條第七款、第二十條第一項第五款所稱書面同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，**單獨所為之書面意思表示**。

個資法第八條

- 當事人蒐集個人資料時，應明確告知當事人下列事項：
 - 一、公務機關或非公務機關名稱。
 - 二、蒐集之目的。
 - 三、個人資料之類別。
 - 四、個人資料利用之期間、地區、對象及方式。
 - 五、當事人依第三條規定得行使之權利及方式。
 - 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

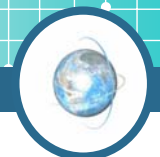


個資法第八條

- 有下列情形之一者，得免為前項之告知：
 - 一、依法律規定得免告知。
 - 二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
 - 三、告知將妨害公務機關執行法定職務。
 - 四、告知將妨害第三人之重大利益。
 - 五、當事人明知應告知之內容。

個資法第十條

- 公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：
 - 一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
 - 二、妨害公務機關執行法定職務。
 - 三、妨害該蒐集機關或第三人之重大利益。

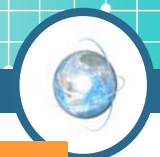


個資法第十二條

- 公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

個資法第十五條

- 公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：
 - 一、執行法定職務必要範圍內。
 - 二、經當事人書面同意。
 - 三、對當事人權益無侵害。

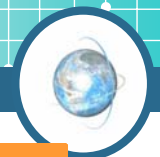


個資法第十七條

- 公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同：
 - 一、個人資料檔案名稱。
 - 二、保有機關名稱及聯絡方式。
 - 三、個人資料檔案保有之依據及特定目的。
 - 四、個人資料之類別。

個資法第十八條

- 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。



個資法第二十二條

- 中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。

個資法第二十七條

- 非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- 中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。



個資法第二十九條

- 非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。但能證明其無故意或過失者，不在此限。

個資法第五十條

- 非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應受同一額度罰鍰之處罰。



個資法第五十一條

- 有下列情形之一者，不適用本法規定：
 - 一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。
 - 二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。

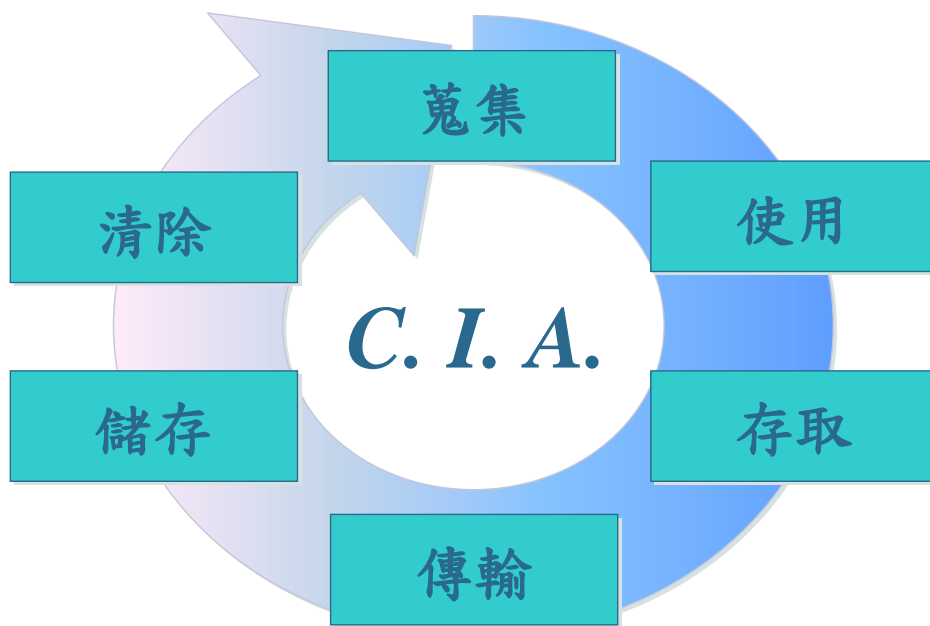
個資法第五十一條

- 公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。



- 1 資訊安全事件與案例分析
- 2 個人資料保護法介紹
- 3 如何提升個人資料保護能量
- 4 資料保護工具說明

個人資料生命週期管理 (Personal Data Life Management)



個人資料管理重點(一)



❖ 蒐集

- 蒐集個人資料之理由、方法與告知義務
- 確認個人資料之正確性及內容是否為法律定義之「得以直接或間接方式識別該個人之資料」

❖ 使用

- 符合法律之使用規範
- 符合組織政策之內部使用規範(例如：交叉行銷)

❖ 存取

- 存取個人資料之權限管理
- 委外或外包廠商之資訊安全管理

All Rights Reserved by NII產業發展協進會

個人資料管理重點(二)



❖ 傳輸

- 個人資料傳輸過程中之安全(加密或安全網路)

❖ 儲存

- 個人資料新增及修改之作業程序
- 存放個人資料場所及設備之安全管理
- 備份或歸檔後之資料安全

❖ 清除

- 個人資料刪除或銷毀之安全處理程序

❖ 其它

- 客訴、法律糾紛、懲處程序

All Rights Reserved by NII產業發展協進會



推動個人資料保護及管理制

實施個人資料管理及
保護教育訓練

評估可行之個人資料管理
及保護之技術方案

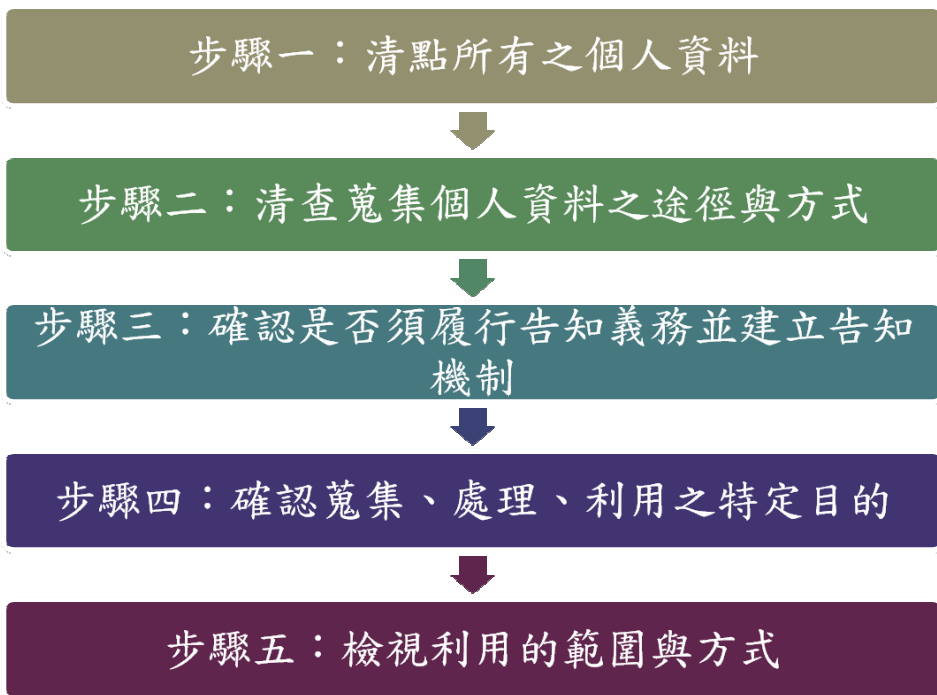
滿足基本
個人資料保護

確認組織個資保護達成狀況的十大問題

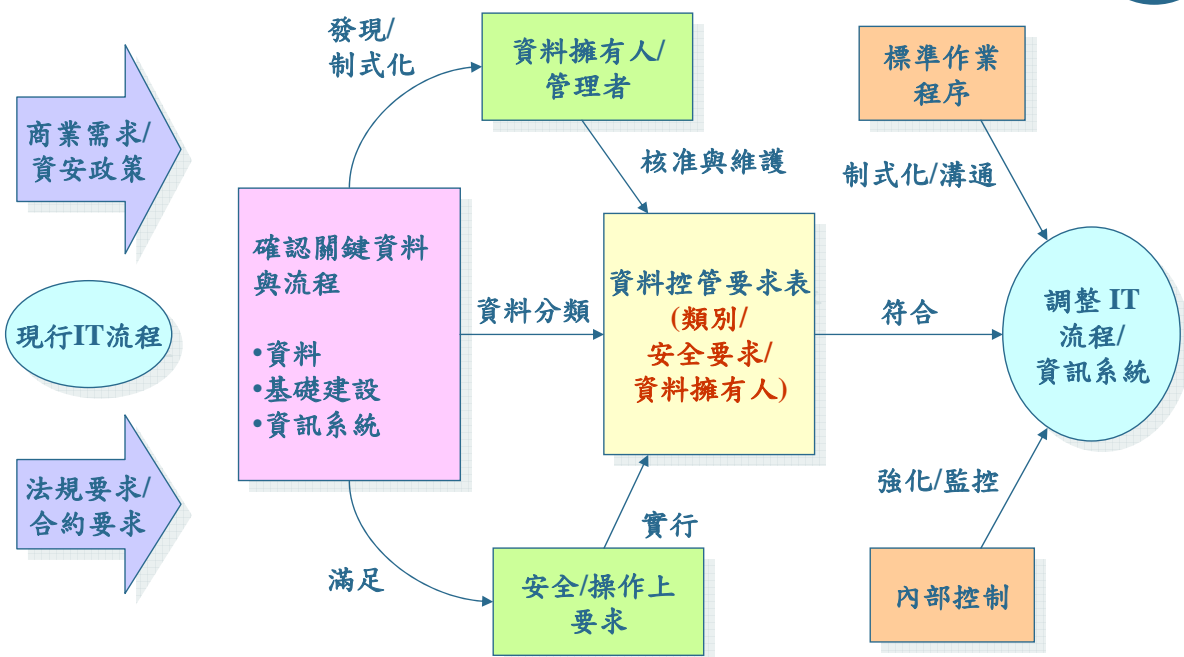


- ❖ 含有個人隱私資料的取得來源是否合法?(必要時取得當事人書面同意)
- ❖ 資料處理及利用範圍是否符合蒐集目的之必要範圍內?
- ❖ 組織成員是否能隨意取得、複製含有個人隱私資料?(由USB隨身碟帶出)
- ❖ 組織成員是否能隨意傳送含有個人隱私資料?(e-mail寄出)
- ❖ 組織是否有適當的控制措施防範駭客入侵?(建置防火牆、防毒軟體等)
- ❖ 個人資料之利用、修改、複製是否有留下稽核記錄?(啟用Log機制)
- ❖ 組織是否有適當的控制措施防範未經授權人員進入取得資料或操作系統?(實體安全控管)
- ❖ 組織是否有持續進行資訊安全認知訓練?
- ❖ 個人隱私資料存放位置及取用限制是否已經識別與規範?
- ❖ 個人隱私資料銷毀是否已建立適當的程序?

資料蒐集、處理、利用之自我檢查五步驟



個人資料管理流程圖





- 1 資訊安全事件與案例分析
- 2 個人資料保護法介紹
- 3 如何提升個人資料保護能量
- 4 資料保護工具說明

DLP資料外洩防護工具



- ❖ DLP(Data Loss Prevention)防止資料外洩解決方案須配合基本安全防護措施：例如：防火牆、防毒軟體、弱點修補、權限控管、資料復原系統使用，大致的概念如下：
 - 管控周邊裝置
 - 端點防止資料遺失，包括管控端點行為、加密軟體、與硬體加密方案
 - 閘道器網路防止資料遺失

DLP功能(以SmartIT為例)



(一) 外接式儲存媒體禁用



(二) 檔案抄寫



(三) 軟體禁用



(四) 網頁禁用



(五) 螢幕側錄



(六) IM對話紀錄稽核



(七) 印表機稽核



(八) 檔案加解密

All Rights Reserved by NII 產業發展協進會

DLP工具



- ❖ Bule Coat
- ❖ BorG DLP
- ❖ Check Point DLP
- ❖ FineArt X-Fort
- ❖ IP-guard
- ❖ McAfee DLP
- ❖ Symantec DLP
- ❖ SmartIT
- ❖ TrendMicro LeakProof
- ❖ Websense DLP

All Rights Reserved by NII 產業發展協進會



簡報完畢，敬請指教！