國立中央大學電子計算機中心
「資訊安全管理系統顧問服務暨驗證範圍擴大案」

資安法令宣導及案例分析

專案主持人：吳國維 執行長

財團法人中華民國國家資訊基本建設產業發展協進會

課程大綱

- 資訊安全之概念說明
- ISMS/ISO27001簡介
- 資訊安全相關法律與安全倫理
- 數位蒐證與法律程序
- 案例說明與案例檢討
- 資安相關注意事項
- 同仁經驗分享

課程大綱

- 資訊安全之概念說明

資訊安全的最大威脅??→人員安全

- 根據Datapro Research Corporation的資安調查，約有5成的資安事件是由人為失誤所造成，加上離職員工或內部犯罪所佔1成，人為因素造成資安事件所佔的比例高達6成

資料來源:資安人 2006/9/8

什麼是資訊？

- 資訊對組織而言就是一種資產，和其他重要的營運資產一樣有價值，因此需要持續給予妥善保護
- 資產就是組織直接賦予價值，且需要受到保護的人、事、物

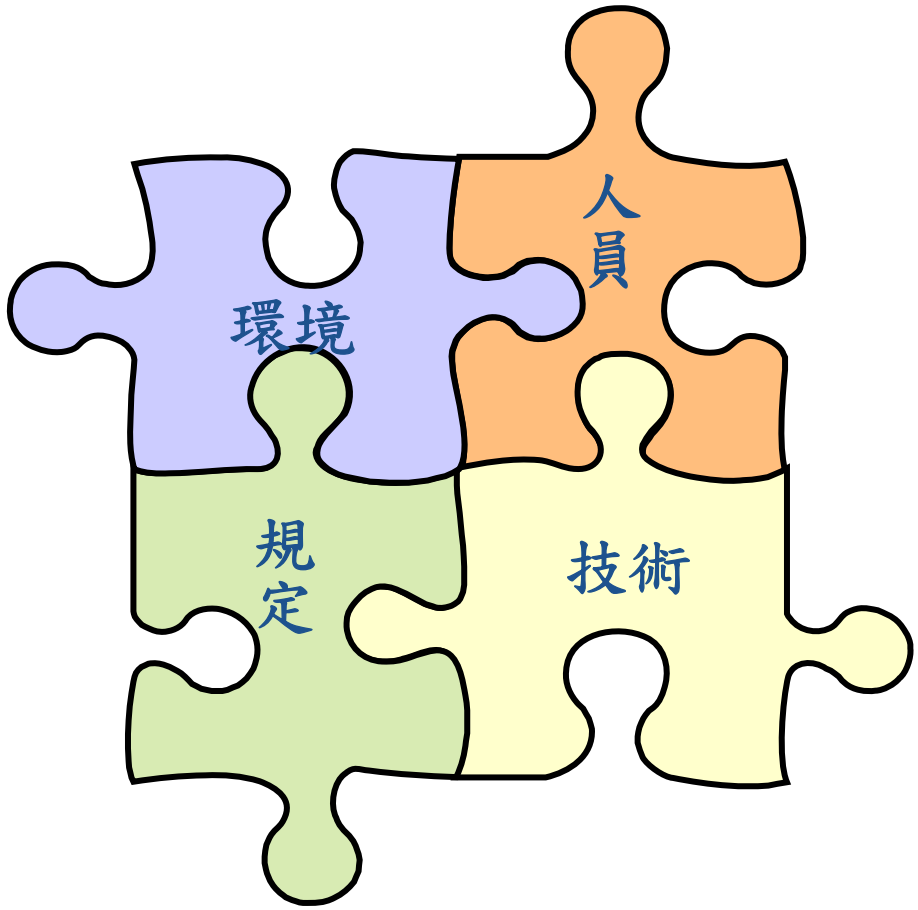
資訊安全管理制度為何

- 資訊安全管理制度 (Information Security Management System, ISMS)

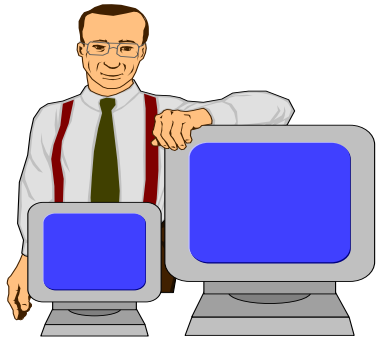
"The Information security management system is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, maintain and improve information security"

資訊安全範圍

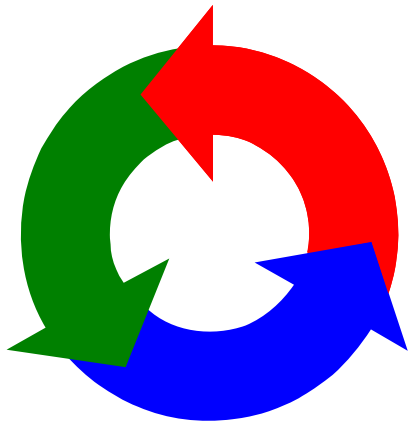
- 資訊使用之『環境』
- 資訊使用之『技術』
- 資訊使用之『規定』
- 資訊使用『人員』

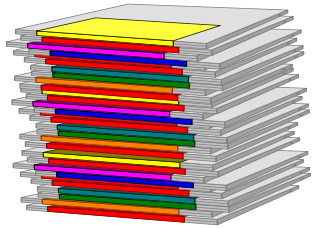


資訊安全管理重點

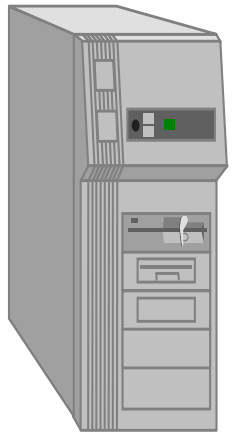


People





Process



Technology

資訊安全三大原則

- 機密性(Confidentiality)：
  確保只有經授權的人才可以取得資訊，避免資訊洩露。

- 完整性(Integrity)：
  確保資訊不受未經授權的竄改與資訊處理方法的正確性。

- 可用性(Availability)：
  確保經授權的使用者，在需要時可以取得資訊，並使用相關資產。

課程大綱

- ISMS/ISO27001簡介

ISO27001過去與現在

- **BS7799標準更新之歷史：**
  - 1995:英國公佈BS7799 Part I
  - 1998:英國公佈BS7799 Part II
  - 1999:英國公佈新版BS7799 Part I、Part II
  - 2000:ISO通過成為ISO/IEC 17799 Part I
  - 2002:BS7799:2-2002 -資訊安全管理系統驗證規範
  - 2005: ISO/IEC 17799:2005
  - 2005: ISO27001
- **BS7799:2-2005在10月15日成為國際標準 ISO27001**

ISO27001驗證全球推廣狀況

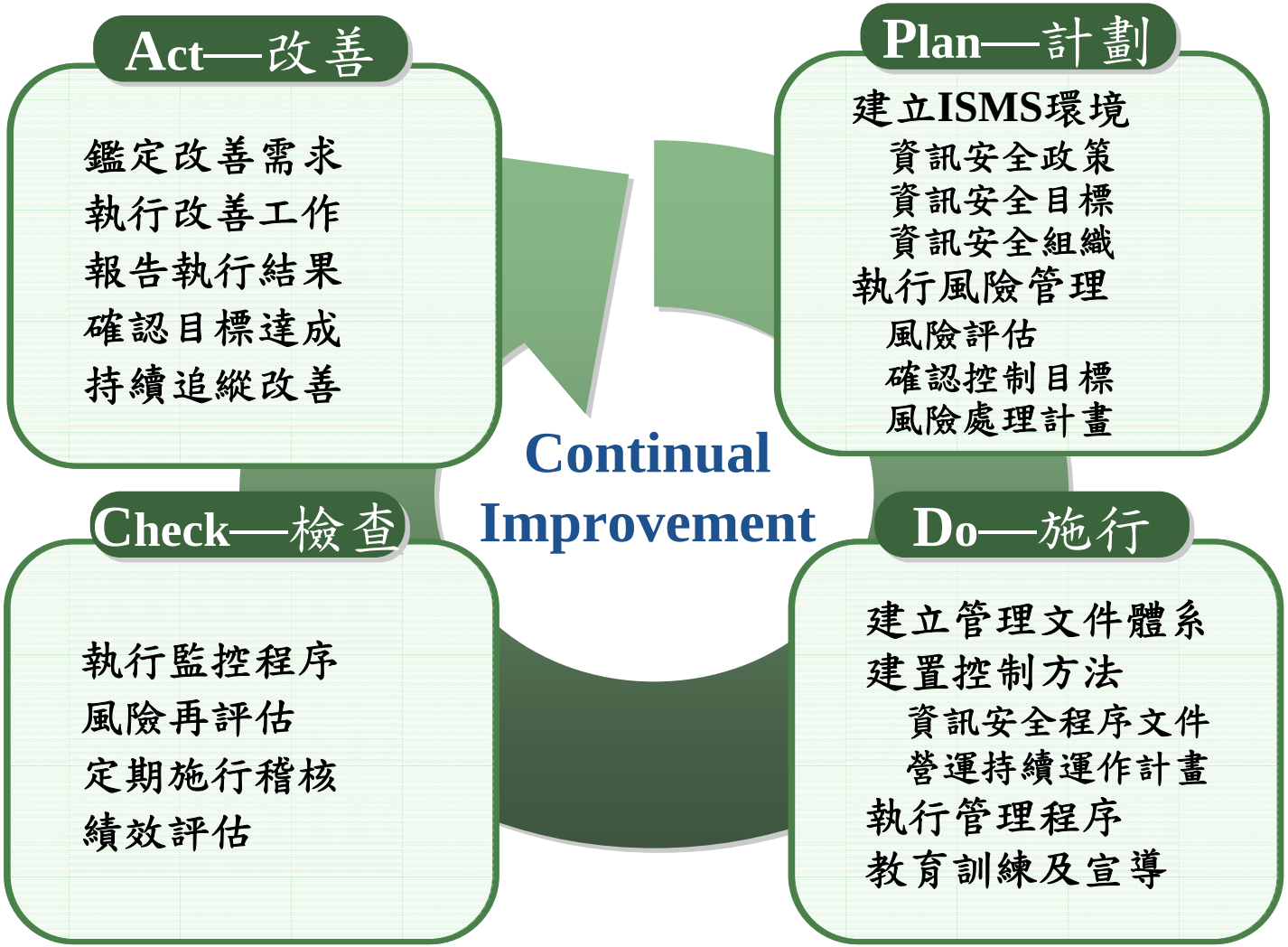
- 在政府帶動下，許多電信、金融與資訊服務，為能取得客戶信任，紛紛推動ISMS的建置
- 在法規要求以及客戶期望下，推行資訊安全管理制度已成為組織永續經營之必要工作

Top 10

日本	3273 *
印度	477
英國	401
臺灣	331
中國	205
德國	120
韓國	102
美國	95
捷克	82
匈牙利	65
Total	**5822**

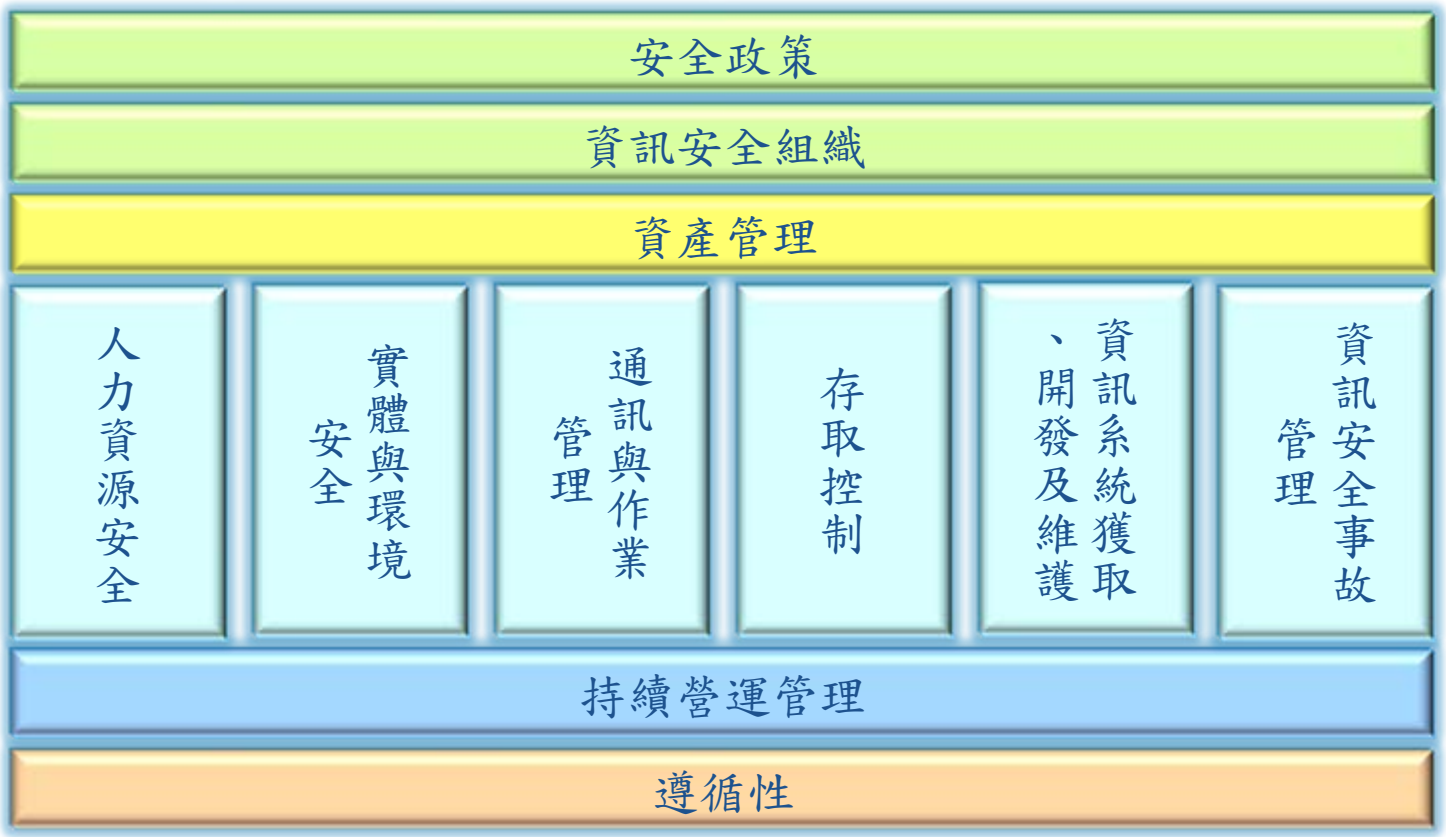
資料來源：http://www.iso27001certificates.com/ As of 2009/11

PDCA模型之應用



ISO27001涵蓋之內容

11 個領域、 39 個控制目標、 133 個控制要點



課程大綱

- 資訊安全相關法律與安全倫理

政府機關(構)資訊安全責任等級分級作業施行計畫
－各類資安系統等級應執行之工作事項

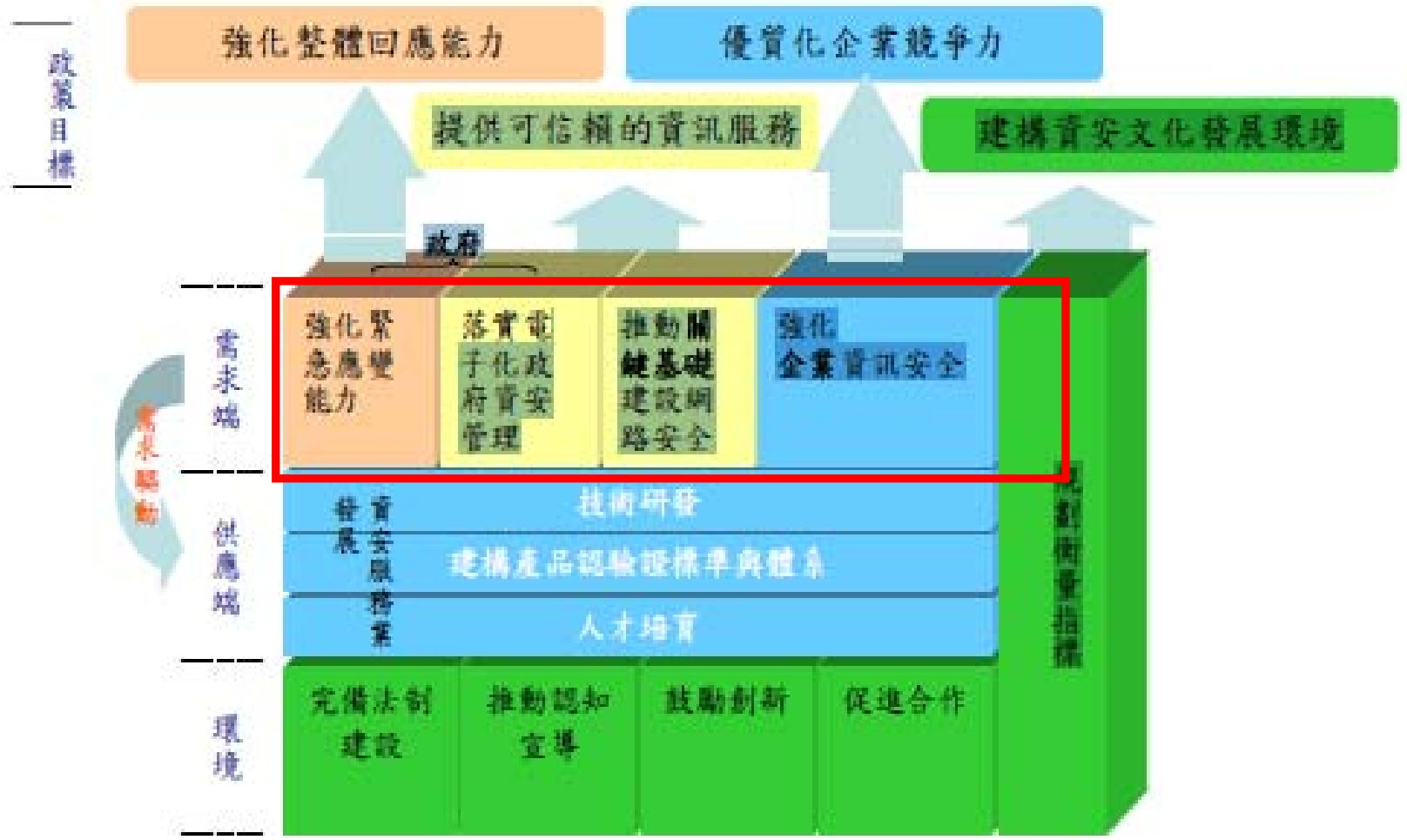
作業名稱 / 內容 / 等級	防護縱深	ISMS 推動作業	稽核方式	資安教育訓練(一般主管、資訊人員、資安人員、一般使用者)	專業證照	檢測機關網站安全弱點
A 級	NSOC 直接防護/自建 SOC、IDS、防火牆、防毒	通過第三者認証	每年至少執行二次內稽	每年至少（3,6,18,3 小時）	維持至少 2 張資安專業證照	每年兩次
B 級	SOC (Optional)、IDS、防火牆防毒、郵件過濾裝置	通過第三者認証(100 年)	每年至少執行一次內稽	每年至少(3,6,16,3 小時)	維持至少 1 張資安專業證照	每年一次
C 級	防火牆、防毒、郵件過濾裝置	自行成立推動小組規劃作業	自我檢視	每年至少(2,6,12,3 小時)	資安專業訓練	每年一次
D 級	防火牆、防毒、郵件過濾裝置	推動 ISMS 觀念宣導	自我檢視	每年至少(1,4,8,2 小時)	資安專業訓練	每年一次

中央大學

98~101資通安全推動計劃

98年~101年

資通安全推動計劃－發展藍圖



98~101資通安全推動計劃－目標

1. 強化整體回應能力

   當重大資安事件發生時，必須具備能在有限的時間內，採取緊急應變行動的能力，方能使災害損失降至可接受的程度，並確保核心業務的持續運作。

2. 提供可信賴的資訊服務

   高度資訊化社會，民眾對於政府與關鍵基礎建設的最基本期待在於兩者所提供的資訊服務是可以讓人安心且可信賴的。

3. 優質化企業競爭力

   透過資安來為組織的核心業務創造價值，並協助企業達成未來的競爭優勢，亦　為推動本方案的目標之一。

4. 建構資安文化發展環境

   a.推動「個人資料保護法」儘速完成立法

   b.提升全民資安認知

   c.資安關鍵指標的量化資訊、定性分析，可概略瞭解我國資安政策發展狀況、實施成效及趨勢。

資通安全相關法規

- 國家機密保護法
- 電子簽章法
- 刑法(防駭條款)
- 電腦處理個人資料保護法
- 檔案法
- 著作權法
- 機關公文電子交換作業辦法
- 智慧財產權 Intellectual Property Rights (IPR)

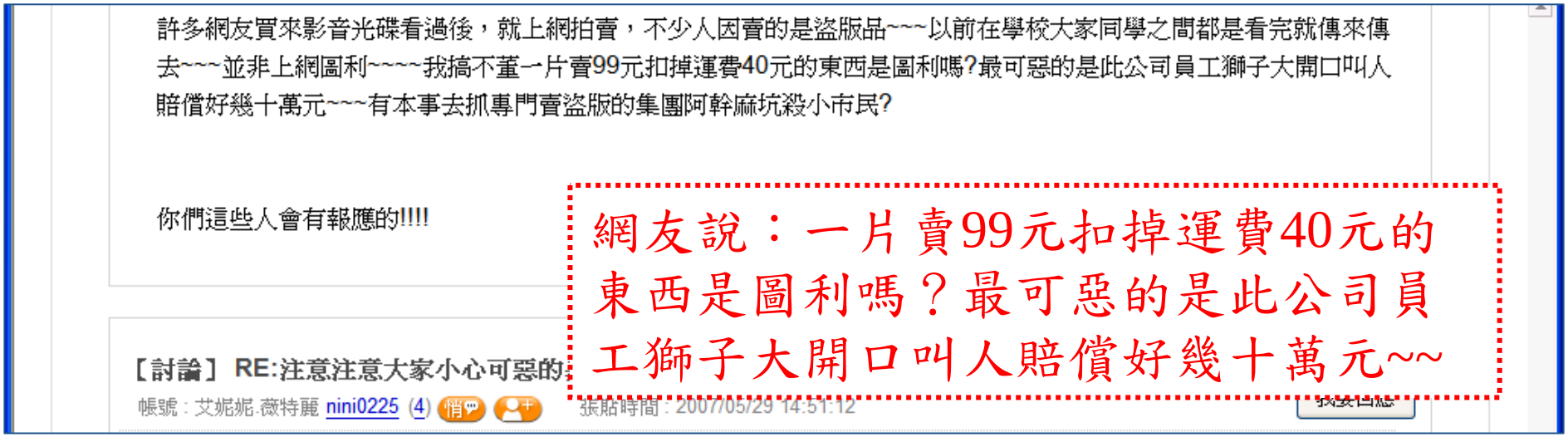
很多法令在法規資料庫可循!!~

著作權保護

- 尊重著作權很重要
- 使用合法軟體
- 尊重著作權
- 不散播非法資訊

販賣盜版光碟

- 很多網友反應，在網路上販賣盜版光碟，被代理商抓包索賠10~20萬元和解，許多網友不滿這家代理商用釣魚的方式，坑殺他們的荷包...



禁止真品平行輸入及侵害散布權

「小弟因看完一片香港正版的平行輸入真品DVD，在拍賣賣出，4月2日郵寄賣出，前兩天被自稱○○國際股份有限公司的法務代理商帶警察來家裡抓人...我真的傻眼！
在此之前我完全不知道原來正版的也有罪?? 而且只是販售一件真品平行輸入可以搞的像殺人強盜一般直接帶警察來家裡抓人？！」

違反著作權法第八十七條第一項第四款禁止真品平行輸入及第九十一條之一侵害散布權的規定

非正常使用行為

- 不刻意散播病毒
- 不刻意掃描網站
- 不攻擊他人網路
- 不拖垮他人網路
- 不闖網路空門
- 不大量、集中使用網路資源
- 不做網路監聽
- 不竊取名單(如2007年Gmail聯繫人名單漏洞)

著作權法修正案

- 行政院於98年5月13日公佈著作權法部分條文修正，第六章之一「網路服務提供者民事免責事由」或稱「 ISP責任避風港條款」
- 網路服務提供者包含：
  - 連線服務提供者(Hinet、Seednet、TANet等)
  - 快速存取服務提供者
  - 資訊儲存服務提供者(提供部落格、網路拍賣服務等)
  - 搜尋服務提供者(Google等搜尋引擎)

侵犯著作權行為

經著作權人舉證

- 使用者構成著作財產權之侵害，ISP構成共同侵權行為

ISP與使用者依法負民事連帶賠償責任

- 使用者　→依法負刑事責任：3年以下有期徒刑
- ISP行為人→依法負刑事責任：3年以下徒刑
- ISP(法人) →依法負刑事責任：罰金

避風港條款 & 三振條款

- 避風港條款
  - ISP業者只要採取「通知/取下」及「三振條款」等機制，對於別人利用其服務侵害著作權或受不當通知而取下網路資料，都可以不負法律責任，不用擔心隨時會捲入著作權人與網路使用者的爭訟
- 三振條款
  - 係指網路使用者若有三次涉及侵權情事，就會被終止網路服務，不能使用ISP業者提供的網路服務

何謂網路倫理？

- 網路是新興社會，容易匿名匿蹤，躲在終端機後，原有社會倫理被打破，大家需要調適，下位者上位者要互相尊重，需要重建網路倫理。
- 法律不易約束網路行為，要靠網路倫理自我約束。
- 不濫用網路特質，不利用網路技術做現實社會不會發生事，要靠網路倫理。

資料來源：交大計中劉大川

課程大綱

- 數位蒐證與法律程序

數位蒐證程序

- 何謂電腦鑑識?
  - 電腦鑑識是指數位證據的採證及鑑識的過程
  - 電腦鑑識與傳統的刑事鑑識工作差不多，都是證據的採集及分析。只是電腦鑑識的對象是電子資料，主要是用來協助執法人員偵辦電腦及網路犯罪。

資料來源:中央警察大學 王旭正

數位證據的來源

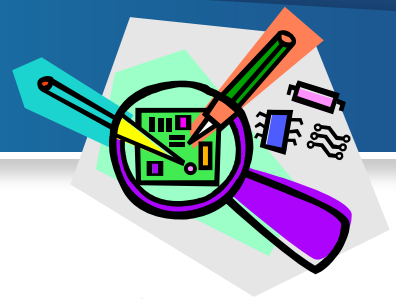
資料來源:調查局電腦犯罪防制科錢世傑先生

數位鑑識原則

- 事件現場蒐證原則
  - 保護第一手證據
- 數位證據擷取分析原則
  - 保持最原始蒐集之證物的完整性。
- 數位證據保存與保護原則
  - 實體的保護
  - 邏輯的保護
- 結果呈現原則
  - 陳述所發現的事實，而非負責鑑識人員的個人感覺、推測或主觀意見
  - 必須對技術名詞簡要清楚的解釋

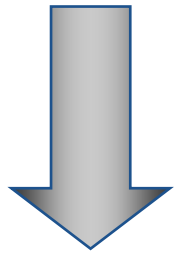
資料來源：成大博班生 林敬煌

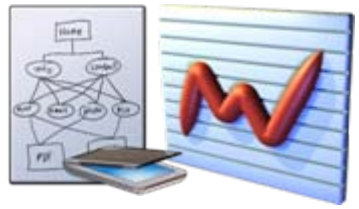
蒐證及法令程序



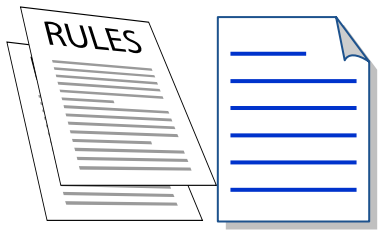
數位證據 → 蒐集 → 檢驗

數位蒐證與法律程序





分析 ← 報告 ← 法庭呈現



資料來源：調查局電腦犯罪防制科錢世傑先生

課程大綱

- 案例說明與案例檢討

- 拷貝正版光碟…？
- 提供MP3下載…？
- 複製他人著作…？

您確定也沒有下列行為嗎？

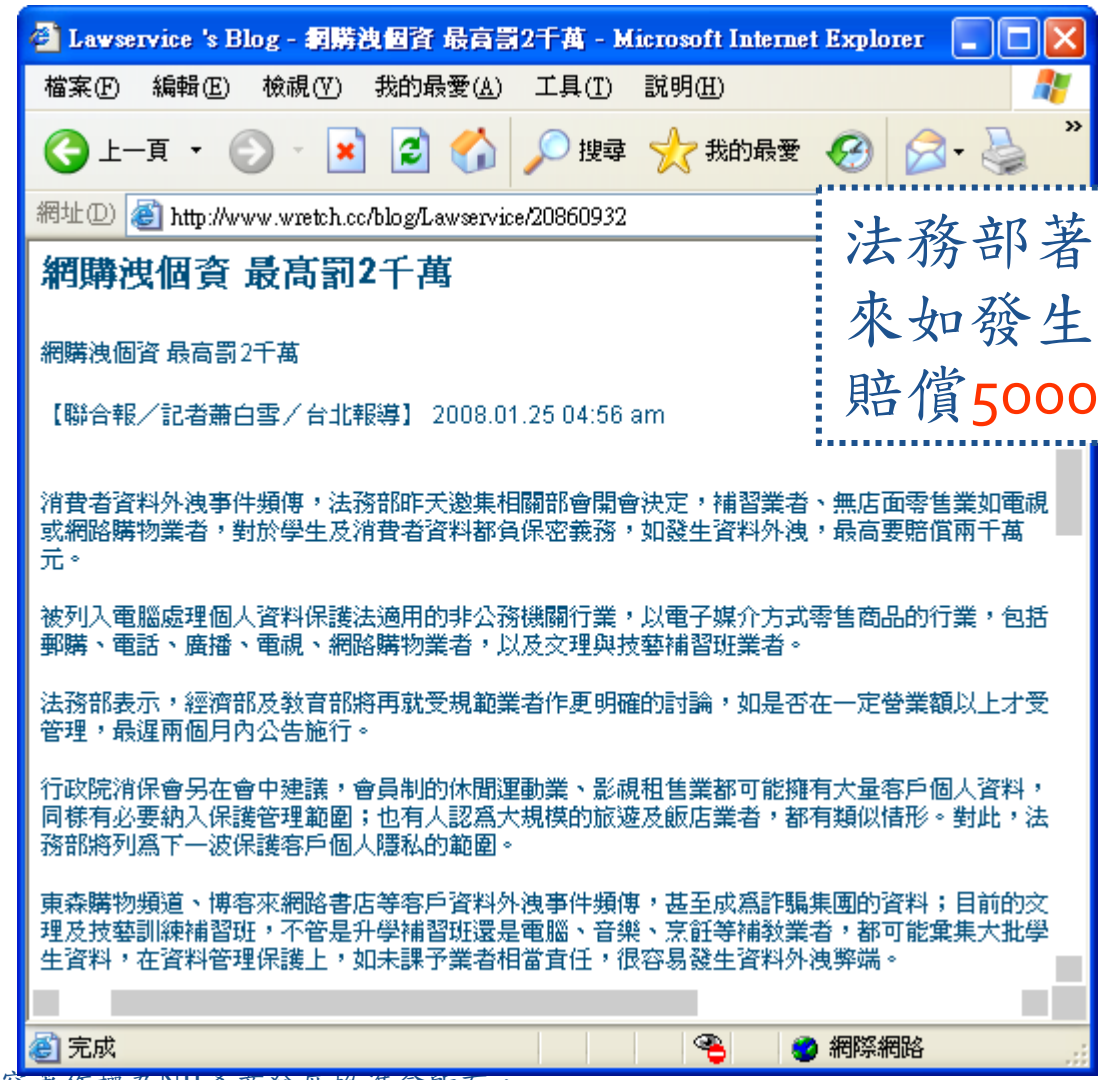
P2P軟體下載音樂、影音

IFPI查獲上百位大學生透過P2P軟體非法下載音樂，可能首次大規模對學生提告開

財團法人國際唱片業交流基金會

IFPI在網路上查察，發現有33校（多數是大學）、學術機構發生74件非法下載音樂或影片事件

洩個人資料將重罰2000萬(舊法)



法務部著手修法(個資法)，未來如發生資料外洩，最高要賠償5000萬！

案例：業界的個資外洩

新聞內容 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

上一頁 搜尋 我的最愛

網址(D) http://www.tvbs.com.tw/news/news_list.asp?no=suncomedy20070518 移至 連結

洩漏趙建銘資料　台新罰百萬、停卡

邱毅爆料總統兒子陳致中與女婿趙建銘申辦台新無限卡，金管會開鍘，對於台新銀行洩露客戶資料，按照銀行法處罰[illegible]萬，並且停止核發新卡至少1個月，台新銀行至少損失5千多萬，台新[illegible]示尊重處分，內部調查也大動作懲[illegible]名違反規定查詢客戶資料的員工，不過，仍舊沒有找到洩密者。

邱毅拿出這大疊資料，爆料陳致中和趙建銘特權辦卡，這可先讓台新銀行吃不完兜著走，因爲洩漏客戶資料，金管會開鍘，罰款200萬事小，甚至停止核發新辦信用卡，直到內部控管稽查制度改善。金管會副主委張秀蓮：「查(客戶)資料都要有密碼，控管不是很嚴格的話，才會有不該查的情況去查。」

台新銀行強調不會影響現有信用卡客戶權益，只不過，至少停發1個月的新卡，以2萬張的發卡量，平均每月刷2千1來算，至少損失5千多萬。台新銀行代理發言人李竝光：「對這項處分，我們尊

完成 網際網路

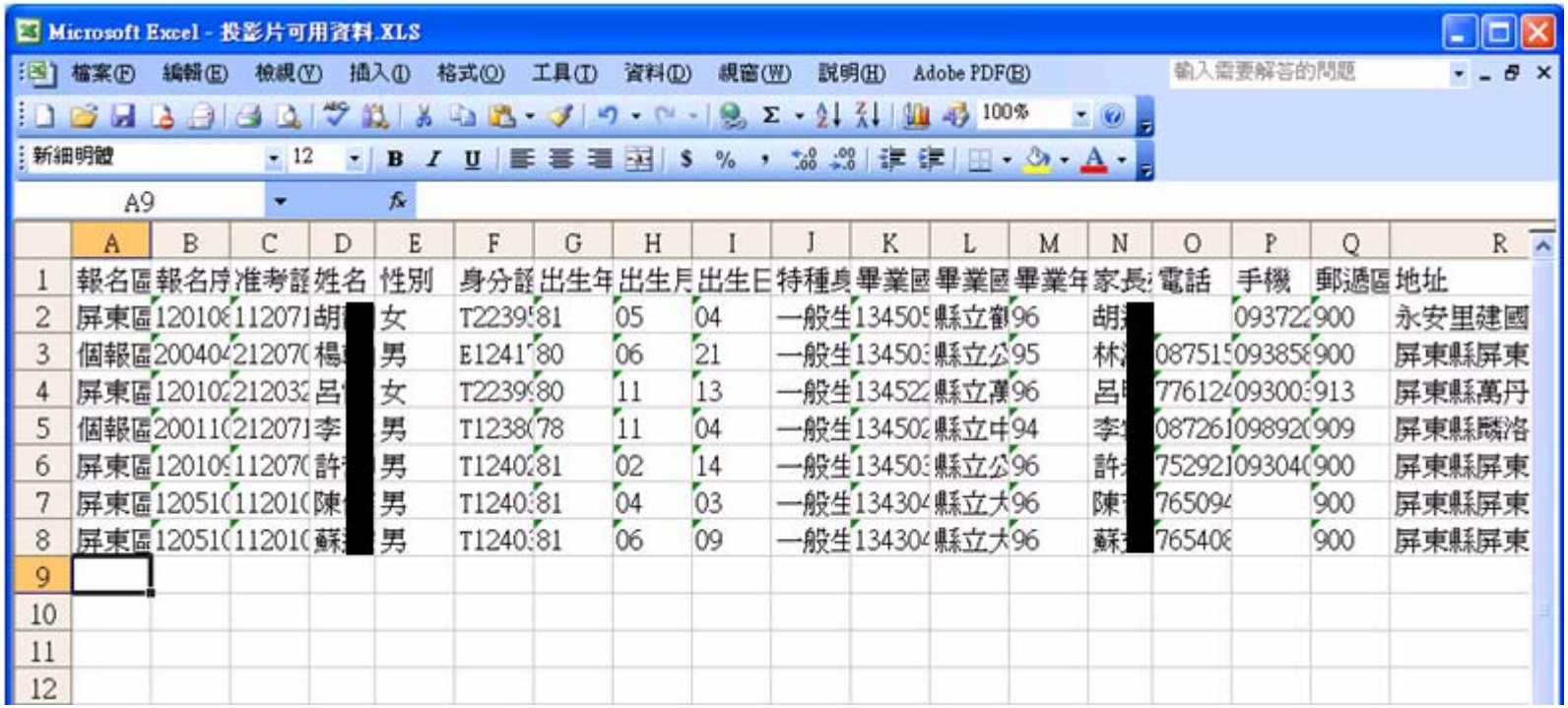
遭罰200萬；
停卡處分至少損失5,000多萬。

提醒您，真的沒有外洩個資？

搜尋網路上的公開個資

在入口網站上使用某些關鍵字搜尋…

詳細的各項個人與家庭資料



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	報名區	報名序	准考證	姓名	性別	身分證	出生年	出生月	出生日	特種身	畢業區	畢業區	畢業年	家長	電話	手機	郵遞區	地址
2	屏東區	120106	112071	胡[redacted]	女	T2239[redacted]81		05	04	一般生	134505	縣立[redacted]創	96	胡[redacted]		093722	900	永安里建國
3	個報區	200404	212070	楊[redacted]	男	E1241[redacted]80		06	21	一般生	134503	縣立[redacted]公	95	林[redacted]	087515	093858	900	屏東縣屏東
4	屏東區	120102	212032	呂[redacted]	女	T2239[redacted]80		11	13	一般生	134522	縣立[redacted]蕃	96	呂[redacted]	776124	093003	913	屏東縣萬丹
5	個報區	200110	212071	李[redacted]	男	T1238[redacted]78		11	04	一般生	134502	縣立[redacted]中	94	李[redacted]	087261	098920	909	屏東縣瑪洛
6	屏東區	120109	112070	許[redacted]	男	T1240[redacted]81		02	14	一般生	134503	縣立[redacted]公	96	許[redacted]	752921	093040	900	屏東縣屏東
7	屏東區	120510	112010	陳[redacted]	男	T1240[redacted]81		04	03	一般生	134304	縣立[redacted]大	96	陳[redacted]	765094		900	屏東縣屏東
8	屏東區	120510	112010	蘇[redacted]	男	T1240[redacted]81		06	09	一般生	134304	縣立[redacted]大	96	蘇[redacted]	765408		900	屏東縣屏東
9																		
10																		
11																		
12																		

課程大綱

- 資安相關注意事項

使用者責任

- 使用者的態度，對於有效防止非法的使用者存取，以保障安全的工作非常重要。
- 目標：防止未經授權的使用者存取資訊與資訊處理設施，以及使其遭受破壞或竊盜。
  - 通行碼的使用
  - 無人看管的使用者設備
  - 桌面淨空與螢幕淨空政策

通行碼的使用-密碼管理

- 定期更新密碼
- 定期檢查密碼
- 設定優質密碼
  - 避免使用重複數字/單位簡稱/詞語/生日
  - 數字字母符號穿插且不過於複雜
  - 避免重複使用密碼
- 不告訴他人密碼或寫下密碼
- 懷疑密碼外洩立即更新

無人看管的使用者設備

- 使用者應確保無人看守的設備獲得適當保護。

  安裝在公共區域的設備（如公用主機、印表機或伺服器），應有具體的保護：

  – 在活動完成時應終止對話，結束畫面。
  – 使用密碼保護的螢幕保護程式。
  – 活動結束時登出系統或主機，再關閉電腦。
  – PC或設備不用時，應使用密鑰鎖或其他安全控制措施，以防止他人非法使用。

桌面淨空與螢幕淨空政策

- 桌面淨空
  - 重要/機密文件不置於桌上
  - 重要/機密文件下班或離開辦公室前應鎖入安全空間
- 螢幕淨空
  - 設定螢幕保護程式
  - 設定保護密碼
  - 離開座位或暫時不使用時鎖定螢幕

網際網路管理要求

- 與網路服務的連接如果不安全，就會影響整個組織。
- 在敏感或重要業務應用或與處於高風險區域（如無法管理與控制的公共或外部區域）使用網路連接時，安全控制措施非常重要。
- 制定網路服務的使用政策要包含：
  - 允許存取的網路和網路服務。
  - 確定存取網路和哪種網路服務的授權程序。
  - 保護網路連接和服務存取的管理控制措施和程序。
  - 與存取控制政策取得一致性

公共區域無線上網安全性

- 選擇有加密功能的無線基地台
- 使用認證機制對使用人員做好身份管理
- 牽涉到高度機密之相關資訊，避免使用無線傳輸。

(資料來源：i-security-輕鬆學資安/資安小撇步 http://www.i-security.tw)

公共電腦使用安全

- 登入網路服務動作的保護
  - 使用公共電腦時，尤其要注意避免勾選任何的記住帳號或密碼的功能
- 使用公共電腦後，關閉網頁瀏覽器，清除個人相關資料
  - 清除網頁瀏覽記錄/網站上所留下的個人資料/電腦中的**cookie**/隱私權記錄/密碼記錄
- 盡量避免利用公共電腦上網處理重要或私密事務
- 特別注意坐在或站在你旁邊的人
- 更換密碼的頻率要更高

網路使用安全

- 確保網頁瀏覽器使用安全
  - 設定網頁瀏覽器安全性/隱私權
  - 設定信任的網站
- 遠離網路釣魚犯罪陷阱與騙局
  - 不回應不明公司/技術部門要求提供個人隱私或安全資訊
  - 不點選來路不明郵件的網頁連結
  - 不利用企業網路轉寄垃圾郵件

電子郵件的安全

- 安裝防毒軟體過濾郵件
- 不隨意開啟郵件附檔
- 防堵垃圾郵件
  - 絕對不回覆垃圾電子郵件訊息
  - 不購買垃圾電子郵件的廣告商品
  - 不轉寄串接式的電子郵件，(例如聲稱不轉寄給10 個人就會倒楣的電子郵件。)
  - 要寄送同一訊息給許多收件者時，可採用「密件副本」方式來進行
  - 刪除寄件者為空白的電子郵件
  - 使用垃圾電子郵件過濾軟體
- 垃圾郵件過濾簡易設定
  - 在Web 郵件上設定過濾垃圾郵件寄件者
  - 利用常見關鍵字過濾郵件

即時通訊軟體風險

- 存在的風險
  - 病毒威脅
  - 垃圾訊息
  - 檔案交換
  - 洩密
  - 工作效率的影響
- 常犯之錯誤
  - 盲目的檔案分享
  - 花費過多時間於私人聊天
  - 將個人帳號資訊以儲存密碼方式設定儲存
  - 任意將個人之連絡者清單給他人

即時通訊軟體使用安全

- 使用者
  - 登入密碼最好不要用「儲存密碼」記錄於系統內
  - 不任意傳遞與分享公司重要資訊或檔案
  - 不任意接收來路不明之分享檔案
  - 使用者必須秉持以公事使用之目的使用企業即時訊息
  - 隨時更新使用端程式

電腦作業威脅—電腦病毒

- 電腦中毒徵兆
  - 電腦系統運行速度異常緩慢
  - 上網速度越來越遲緩
  - 異常的系統訊息通知
  - 螢幕顯示異常，例如畫面突然一片空白
  - 來自防毒軟體的警告訊息
  - 電腦無故自動關機或不斷重新開機
  - 瀏覽器自動出現產品廣告或色情網頁
  - 網路流量異常，例如沒有使用網路服務或收發電子郵件，但網路的連線燈號卻一直閃爍

電腦作業威脅—電腦病毒

- 電腦病毒簡易處理步驟
  - 將中毒電腦離線網路作業
  - 設法使防毒軟體運作：
  - 以防毒軟體執行病毒的掃瞄與清除
  - 若防毒軟體無法正常執行，則執行以下替代方案：
    - 手動掃毒：
    - 使用未受病毒感染健康的電腦之防毒軟體來進行問題硬碟掃毒作業。
    - 透過免費線上掃毒資源，在不危害狀況下連線網路進行。

    http://housecall.trendmicro.com/
    http://www.symantec.com.tw/
  - 受感染的檔案並執行隔離或刪除動作
  - 未知病毒的處理方式：
    - 電腦病毒事件的通報，尋求資源協助。
    - 聯絡病毒軟體廠商協助。

電腦作業威脅—電腦病毒

- 電腦病毒的防範
  - 確認防毒軟體隨時運作
  - 勿隨意安裝未經許可的電腦軟體
  - 確保軟體在最新更新狀態
  - 使用有問題立即反應

電腦作業威脅—廣告/間諜軟體

- 廣告或間諜軟體的症狀
  - 沒有上網卻還是一直看見廣告視窗
  - 網路速度時快時慢
  - 首頁被更改成奇怪的網站
  - 視窗下方的工具列出現許多原本沒有的工具。
  - 瀏覽器多出沒有安裝過的工具列、搜尋工具，而且無法移除。
  - 電腦處理速度變慢或當機頻率增加。

電腦作業威脅—廣告/間諜軟體

- 間諜或廣告軟體的防範
  - 使用防火牆阻擋。
  - 關閉網路瀏覽器的ActiveX 功能。
  - 安裝封鎖彈跳視窗功能的工具， 例如Google Toolbar 。
  - 下載免費軟體前仔細閱讀所有相關資訊
  - 學習資料備份基本技巧
  - 使用反間諜軟體

刑事警察局惡意程式清除軟體「GK 1.0」
http://www.cib.gov.tw/news/news02_2.aspx?no=343

電腦作業威脅—駭客入侵

- 駭客入侵的徵兆
  - 檔案及資料庫內容遭到竊取或篡改
  - 不知名的IP來源與電腦連線
  - 系統中異常的服務程式
  - 異常通訊埠開啟
  - 稽核紀錄及檔案中的異常事件
  - 系統帳號的異常增加
  - 系統異常的訊息或行為
- 駭客入侵的簡易處理
  - 系統備份
  - 可能入侵途徑系統隔離
  - 蒐集入侵紀錄、檔案等軌跡
  - 追查駭客IP來源
  - 分析資料找出入侵方式
  - 報告相關單位
  - 適時尋求協助

駭客入侵的防範

- 即時更新修正檔
- 日常備份作業
- 設定自動時間校正作業
- 檢視權限設定
- 紀錄及檢視稽核軌跡

可攜式設備之安全管理要求

- 使用可攜式設備（如筆記型電腦、掌上型電腦、膝上型電腦和行動電話）時，應確保業務資訊不受損壞。
- 訂定可攜式設備連接網路的規則和公共場所中使用的指導說明，並提供適當保護連接網路的設施。
- 使用可攜式設備進行遠端存取時，必須先成功地進行身份識別和驗證並採用適當的存取控制機制。
- 在公共場所使用可攜式設備時應採用一定的保護措施，並防範被窺視，以避免儲存和處理的資訊遭到非法存取或洩密。
- 制定並即時更新用於防範惡意性軟體的程式。
- 準備對資訊備份的必要設施，並適當地保護備份的資訊，避免被盜或遺失。
- 應防止可攜式電腦化設備被盜，尤其是比如丟在汽車等其他交通工具、旅館、會議中心以及聚會場所內。
- 內含重要、敏感和/或關鍵業務資訊的設備不應無人看管。如果可能，應上鎖。應使用專用鎖來保障設備的安全。
- 進行可攜式設備的資安訓練，提高他們對可攜式設備可能帶來額外風險的防範意識，以及因應措施的認識。

資料備份

- 資料價值較高時應優先備份
- 擇適合之儲存媒介進行資料備份工作
- 按所欲備份的資料型態， 選擇方法進行備份 Ex.完全備份/ 選擇性備份/漸進式(增量)備份
- 備份的資料需定期做資料回復測試， 以確認備份資料的可用性

資訊儲存媒體的管理

- 儲存媒體的管理
  - 制定儲存媒體（如磁帶、磁片、盒式磁帶以及列印報告）的管理方法
  - 應明確記錄所有的管理步驟和授權級別
- 儲存媒體的報廢
  - 具敏感資訊的媒體應該進行安全保險的保存和處置。
  - 安全收集和報廢所有媒體。
  - 謹選具有經驗及技術的合格合約商。
  - 儘可能記錄敏感資料的報廢，並保留稽核追蹤。
- 儲存媒體的運送安全
  - 使用可靠的傳輸工具或投遞人。
  - 包裝應該可以保護不受運輸過程中事故造成損壞。
  - 依需要採取特殊的控制措施保護敏感資料免遭非法公開或修改。

軟體管理

- 安全要求分析與規格
- 系統文件管理
- 系統測試資料的保護
- 程式源碼的存取控制與集中管理、版本控制
- 測試資料的保護
- 軟體變更控制程序
- 委外的軟體開發管理
- 技術脆弱性控制，如：Code review、滲透測試
- Shareware 與 freeware 管理

課程大綱

- 同仁經驗分享

問題與討論

&