C07-101

電腦病毒原理與防治

單元1：
電腦威脅的來源與途徑

電腦威脅的來源

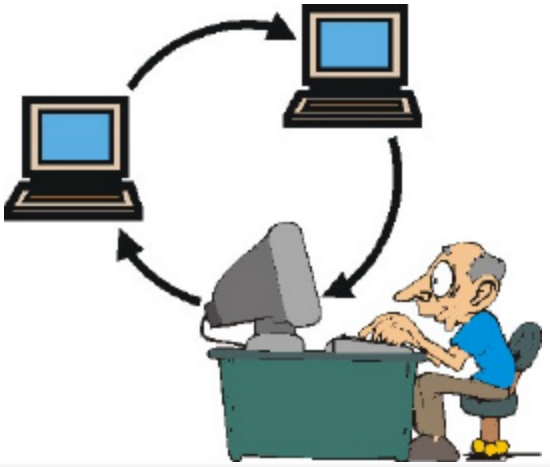
- TCP/IP通訊協定本身的問題
- 作業系統的弱點
  - 身分驗證
  - 授權
- 網路應用程式的瑕疵
  - IIS
  - IE、Outlook
- 惡意程式的傳播與誤用
- 網路與資訊系統管理不當

電腦威脅的共通特徵

- 來自於組織內部及單位以外的網路
- 降低工作同仁的生產力
- 佔用與消耗電腦系統資源
- 對資訊資產造成嚴重的損毀與危害
- 常在毫無預警的情況下進入系統

電腦威脅的種類

- 天災與實體
  - 水災、火災、風災、地震、停電……
- 非蓄意
  - 員工或客戶的不當操作……
- 蓄意
  - 偷竊、駭客、恐怖份子、工業間諜、惡意程式……

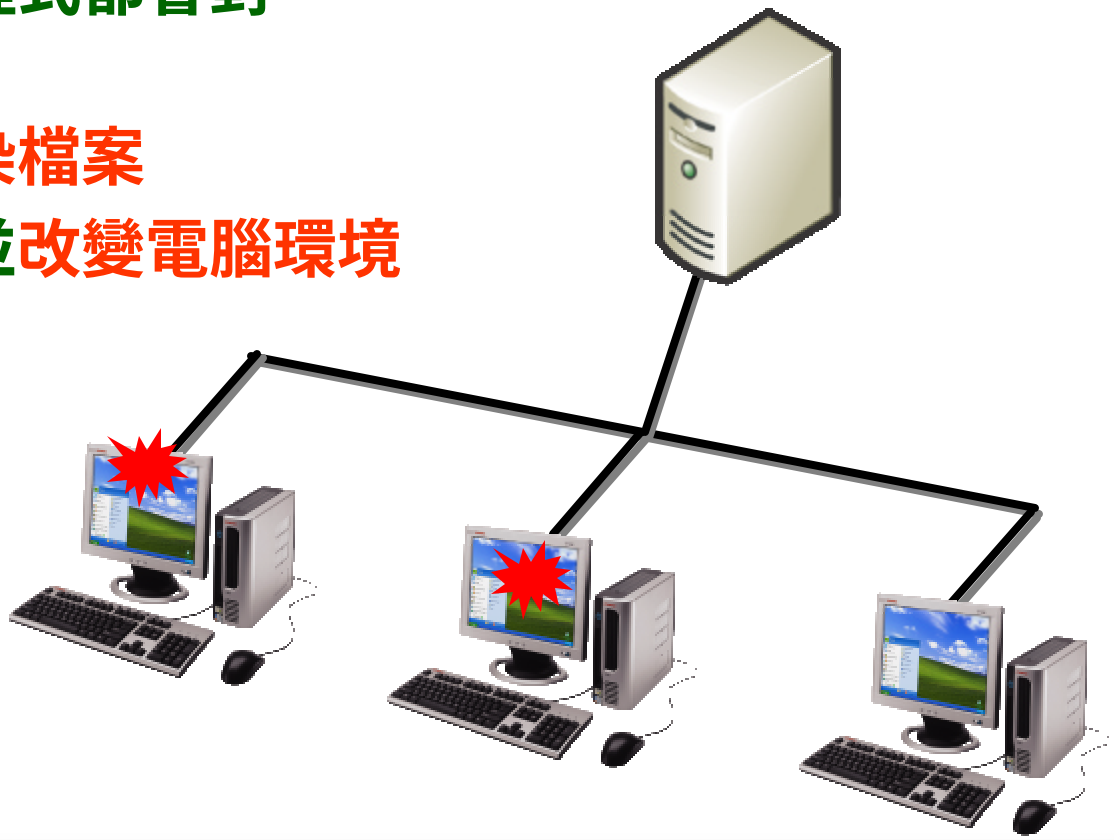


電腦威脅的途徑

- 各種儲存媒體
  - 磁碟片、行動碟、拇指碟
- 透過 Internet
  - 電子郵件、網頁瀏覽、即時應用程式
- 區域網路
  - 網路芳鄰、檔案共享、文件傳播

惡意程式總結與形式 (1/2)

- 惡意程式(Malware)就是…
  - 對系統造成危害的一支程式或程式碼
  - 並不是所有惡意程式都會對系統造成危害
  - 有能力刪除或感染檔案
  - 可藉由系統感染並改變電腦環境
  - 瓦解組織單位的電腦安全性



惡意程式總結與形式 (2/2)

- 常見電腦的威脅
  - 電腦病毒
  - 電腦蠕蟲
- 電腦的威脅通常結合上述數種可能
  - 電腦蠕蟲與電腦病毒的結合 — 梅莉莎
  - 電腦蠕蟲與特洛伊木馬 — 探險蟲
- 二十一世紀惡意程式的新類型
  - 間諜軟體 (SpyWare)
  - 網路釣魚 (Phishing = Phone + Fishing)

電腦病毒介紹

- 電腦病毒是一種惡意程式，會將程式自我複製或感染電腦中其他正常的程式、或破壞電腦系統，導致電腦無法正常運作。
- 動機不同，所造成的損害也不同
  - 無聊、愛現、炫耀能力
  - 惡作劇、好奇
  - 破壞資料與系統、報復
  - 竊取資料、謀求利益等等

惡意程式比較表

	電腦病毒	木馬程式	電腦蠕蟲
感染其他檔案	○	X	X
被動散播自己	○	○	X
主動散播自己	X	X	○
造成程式增加數目	一般電腦使用率提高，受感染檔案數目則增加	不增加	視網路連結狀況而定，連結範圍愈廣，散佈的數目多
破壞能力	視寫作者而定	視寫作者而定	X
對組織的影響性	中	低	高

感染電腦病毒的徵兆

- 電腦執行程式的速度變慢，或是莫名其妙的當機。
- 螢幕上出現一些開玩笑或警告的字語、畫面、或邀你玩遊戲，甚至發出音樂或怪聲。
- 突然找不到硬碟、檔案異常變大或變小，硬碟可使用空間異常減少。
- 檔案的名稱、日期或屬性無故被更改、多出一些不明檔案、或是在正常使用狀況下，產生記憶體不敷使用的異常情形。

感染電腦病毒的結果

- 程式檔案無法使用
- 資料檔案遭到破壞或刪除
- 硬碟損毀無法啟動
- 持續自動重新開機
- 網路癱瘓
- 伺服器癱瘓
- BIOS資料損毀無法啟動

單元2：資安威脅實例與電腦病毒型態

現今資訊安全威脅實例

現今資訊安全威脅的實例 (1/4)

新電腦病毒 專攻視窗2000

美國今天又傳出新的電腦病毒作祟，主要攻擊目標是使用微軟視窗 (Windows 2000) 作業系統的電腦，至少125家全球知名的企業機構遭殃。

根據CNN報導，全美裝有Windows 2000，或沒有更新XP作業系統的電腦，今天都遭到一種新電腦病毒攻擊，包括：CNN，ABC，紐約時報，美國國會山莊，和舊金山國際機場都成了受害者，德國和亞洲也有災情傳出。

資料來源：台視新聞網站 940917

現今資訊安全威脅的實例 (2/4)

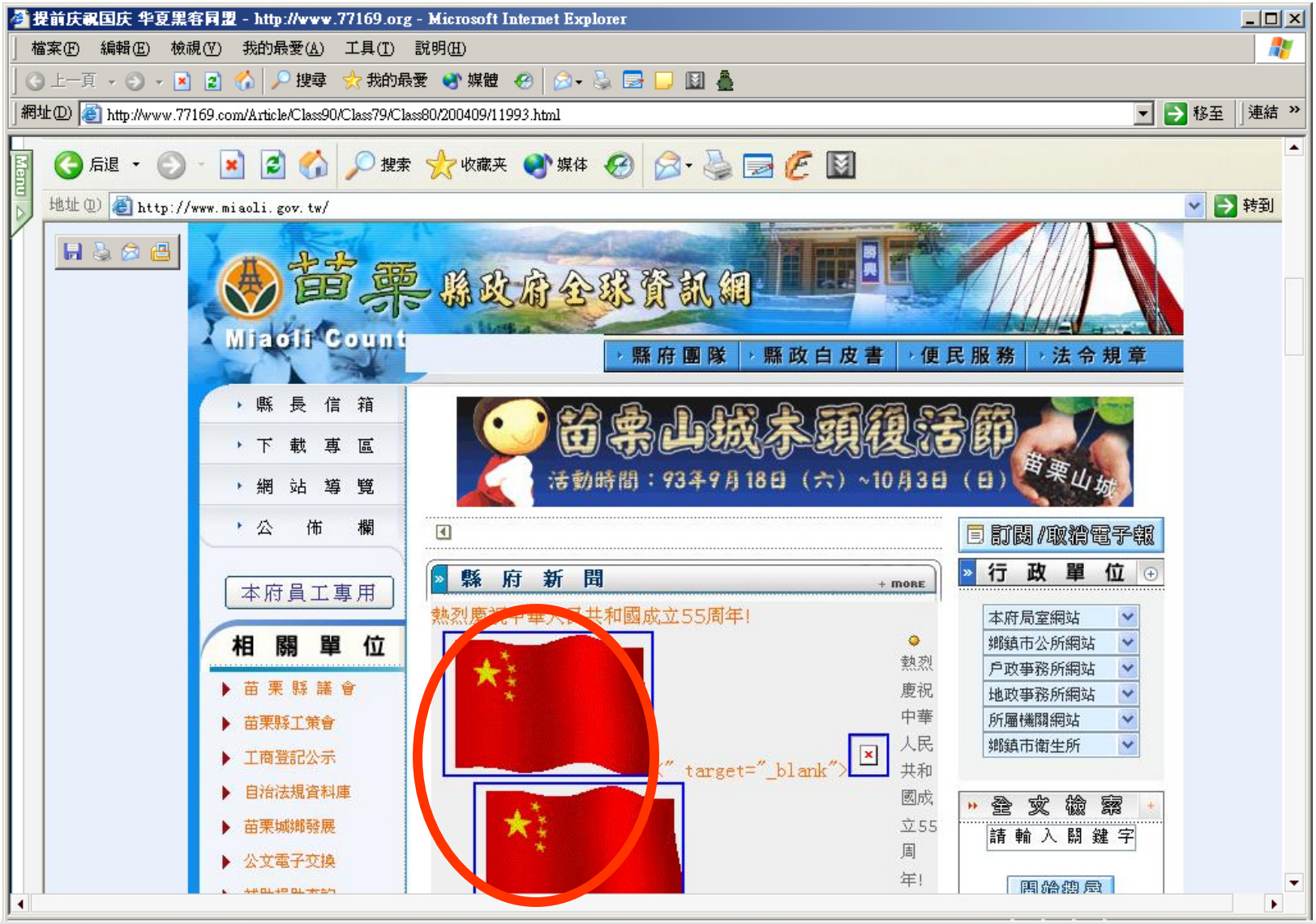
亂按8個YES之後網路免費電影檔案送上病毒

想急著看「酒井若菜清涼比基尼秀」網路免費電影嗎？但是電影播映前，卻有連續視窗跳出來告知需要獲得授權才能看，於是猴急地連按8個「YES」，不但電影沒看成，還奉上「間諜軟體」和「木馬程式」，資訊安全專家說，碰到這種情形，千萬別動，趕快退出並刪除這個檔案。

資訊安全廠商趨勢科技表示，P2P 是間諜軟體最新的寄身途經之一，間諜軟體Media tickets就是利用網友無法抗拒免費電影下，藉著蠕蟲 (米塔病毒 WORM_MYTOB.AR)和木馬 (TROJ_QLOWZONES) 進入受害系統後，間接找到新投宿標的。

資料來源：中央通訊社 940907

現今資訊安全威脅的實例 (3/4)



現今資訊安全威脅的實例 (4/4)

首支手機感染電腦病毒現身！
趨勢：目前未發現大規模感染

第一隻經由手機感染電腦病毒現身！趨勢科技Trend Labs日前發現一支臥底手機病毒SYMBOS_CARDTRP.A會透過藍芽感染智慧型手機，緊接著擴散到手機記憶卡中，更嚴重的是，若使用者將記憶卡資料存取至電腦中，便入侵電腦，藉此安裝後門程式。

趨勢科技表示，此隻病毒因感染症狀不一，中毒者多誤以為手機故障而不自覺。雖目前在全球尚未發現有大規模傳染，但從其透過手機感染電腦的新手法，則為新型態混合型病毒拉起警報。趨勢科技建議使用者在使用MMS與藍芽傳輸裝置接收時需更加謹慎，同時提醒使用者下載手機防毒軟體並定期更新電腦病毒碼，以防範駭客入侵。

資料來源：東森新聞報 940923

電腦病毒成長統計

- 2000年
  - 資安單位統計：全球電腦病毒的成長率約為：222%
  - 情書病毒(ILOVEYOU)造成全球87.5億美元損失
- 2001 – 思坎(Sircam)、紅色警戒(CodeRed)病毒
- 2002 – 娜妲(Nimda) 、疾風病毒…
- 2003 – SQL Worm…
- 2004 – 殺手(Sasser)病毒…
- 2005 – 3721間諜軟體…

平均一個寬頻用戶每天會被10個駭客攻擊！

80億美元

你確定自己安全嗎?

單元2：資安威脅實例與電腦病毒型態

電腦病毒概述

電腦病毒的種類 (1/2)

- 開機型病毒 (例如：米開朗基羅)
  - 躲藏在軟碟或是硬碟啟動磁區，殺傷力居冠，結局通常是全毀
- 檔案型病毒 (例如：維也納)
  - 寄居在執行檔 (副檔名 .COM或 .EXE)
  - 著名的有黑色星期五 (發作時執行的程式會遭刪除)
- 混合型病毒 (例如：大榔頭)
  - 兼具開機型及檔案型病毒特性，不僅感染執行檔，也感染啟動磁區 (例如 Hare野兔病毒，軟碟開機後C:消失)

電腦病毒的種類 (2/2)

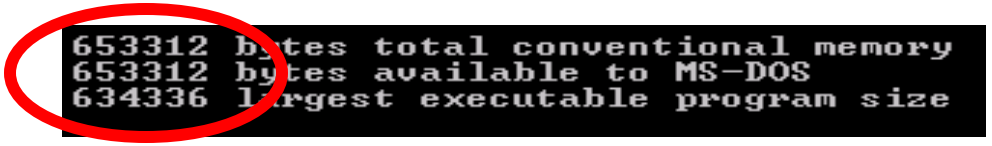
- 網路系統病毒 (例如：疾風)
  - 專門攻擊網路作業系統，破壞伺服器上的檔案。
- 千面人病毒 (例如：Whale)
  - 每繁殖一次就產生新病毒碼，防毒軟體較難防禦。
- 巨集病毒 (例如：Taiwan No.1)
  - 隱藏於具有撰寫巨集能力的軟體檔案裡(Office文件例如：Word & Excel) 最具代表性的就是Taiwan No.1 (出現心算畫面，猜錯開啟20個文件檔案)。
  - 透過其他應用程式之巨集語言來散播。
  - 不會感染程式或啟動磁區。

開機型病毒的特色

- **感染MBR** (Master Boot Record)
- **複製資訊在啟動磁區**(MBR)**中**
- **複製病毒本身到硬碟**
- **會刪除硬碟本身的資料**
- **是最常見的病毒型態**
  - **不包括：**Windows NT, 2000, XP, Server 2003 **家族**

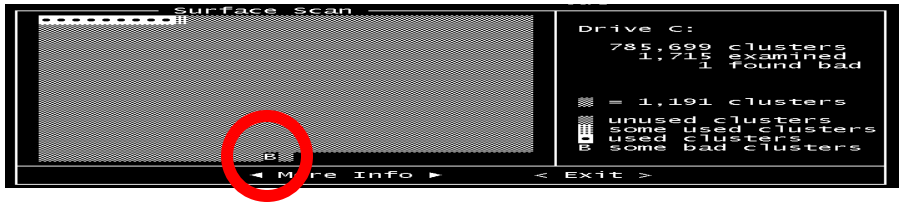
被感染開機型病毒的症狀 (1/2)

- 可用的記憶體少於640k



- 寫入錯誤(不當保護)

- 壞軌出現



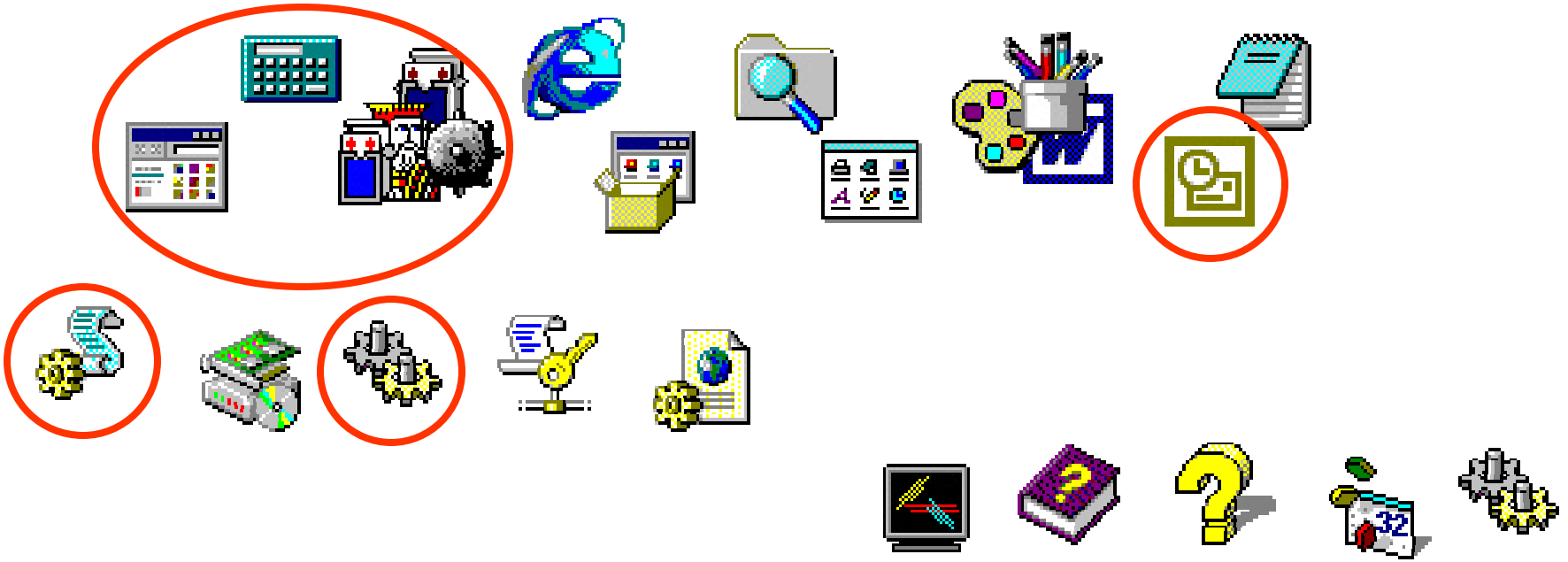
- 無法開機

被感染開機型病毒的症狀 (2/2)

- 變更檔案大小
- 最後的修改時間不正確
- 系統效能降低
- 網路流量突然增加
- 檔案或程式被破壞

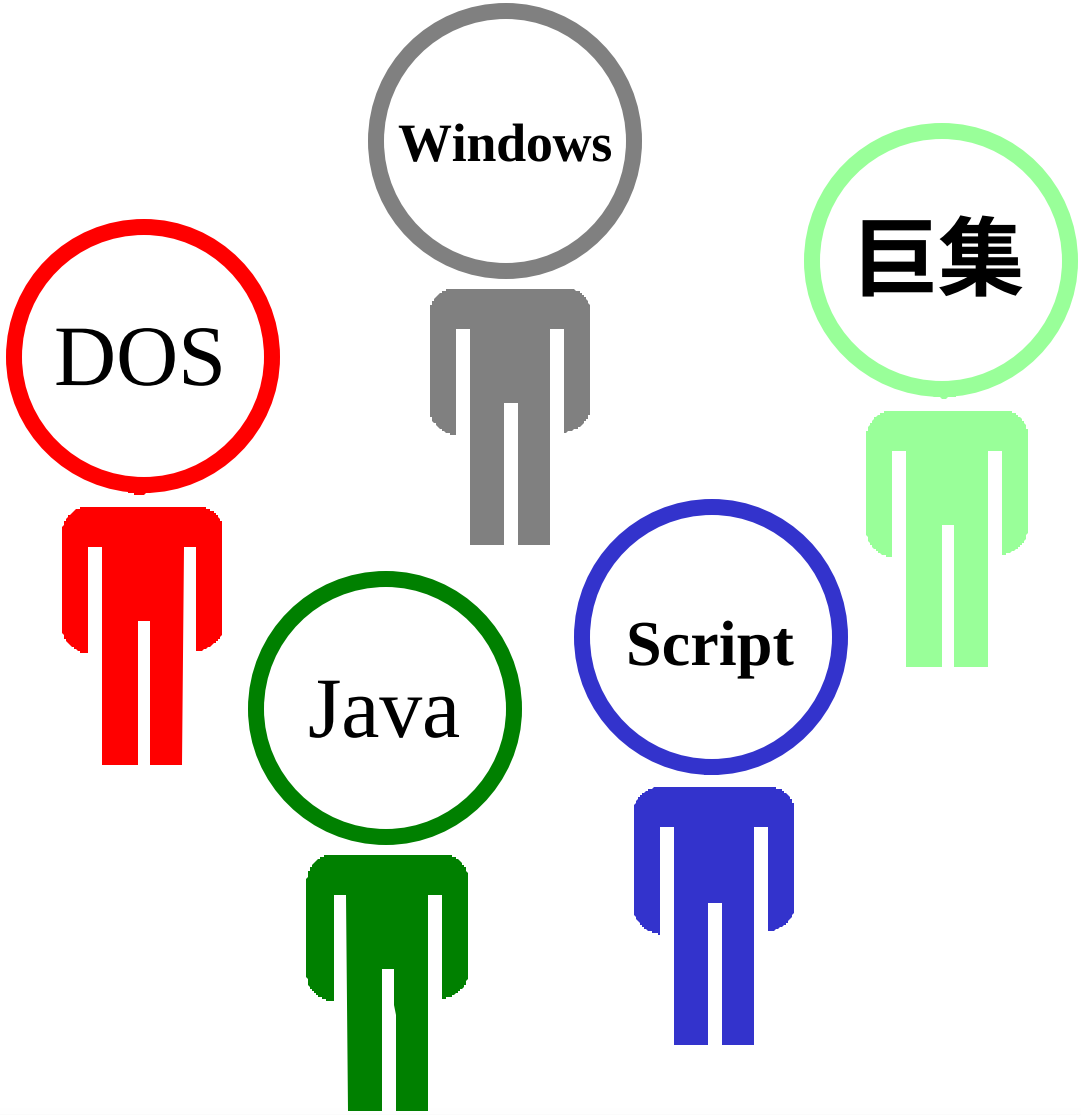
檔案型病毒的特色

- 感染可執行的程式或檔案
- 依賴作業系統開機後才能被啟動
- 利用已感染的程式或檔案進行散佈(傳播)



檔案型病毒的種類

- DOS 病毒
- Windows 病毒
- **巨集病毒**
- Script 病毒
- Java **程式病毒**



複合型病毒的特色

- 兼具開機型與檔案型病毒的特色
- 多種散佈途徑
- 不易被發現、移除或清除

傳統型病毒特色

- 傳統型病毒(開機型、檔案型、混合型等病毒)的共同特色，就是一定有一個「寄主」程式。
  - 所謂寄主程式就是指那些讓病毒窩藏的地方。
  - 最常見的就是一些可執行檔，像是副檔名為.EXE及.COM的檔案。
- 隨著Office文件的普及與其所提供的強大巨集功能，使其相關巨集病毒也愈來愈多。因此應注意：是否允許檔案開啟時對巨集的相關執行動作。

新一代病毒特色

- 新一代病毒完全不需要依靠寄主的程式，如果一定要說其寄生所在，最佳的答案應該就是「Internet」吧！
  - JavaScript和ActiveX，這兩個語言都相繼地被有心人士「點召」，成為新一代病毒的溫床。
  - JavaScript和ActiveX的執行方式，是把程式碼寫在網頁上，當你連上這個網站時，瀏覽器就把這些程式碼抓下來，然後用使用者自己系統裡的資源去執行它。
  - 可是如此一來，使用者就會在神不知鬼不覺的狀態下，執行了一些來路不明的程式。

單元3：
電腦病毒的防護

懷疑中毒的處理方式

- 電腦上的防毒軟體，平時應該注意：
  - 定期更新的動作是否完整
  - 排程(預約)掃毒 與 即時防護的機制
  - 相關日誌檔案的內容是否有所異常
  - 做好備份動作(記錄管理員帳號名稱與密碼)
- 日誌異常或防毒軟體發出通知時，應該注意：
  - 立即向上回報狀態，避免狀況蔓延擴散
  - 執行：即時掃毒或即時防護程式並確定生效運作
  - 不幸中毒檔案應直接解毒或是執行相關隔離

中毒後的解決方法

- 先行參考各家防毒軟體公司的產品說明或教育訓練介紹
- 檢查感染何種病毒與病毒相關資訊
  - 迅速地隔離受感染的網路區段、抑制疫情擴散
- 進行救援動作
  - 報請專業人員尋找源頭並正確清除相關病毒程式
- 使用系統還原功能
  - 格式化硬碟(包含MBR啟動磁區)
- 中毒後使用平時備份資料回復

平日應做好的救援準備

- 養成良好的備份習慣，可使用光碟燒錄片或是其它種類的儲存媒體將資料備份
- 準備救援磁片，例如：原版產品光碟(序號)與修補檔(Servise Pack)、正版應用程式、開機片、Ghost等軟體
- 格式化硬碟的準備，整體重新安裝的準備，系統片、驅動程式以及應用軟體等

防範電腦中毒的原則

- 不使用盜版軟體或來路不明的軟體
- 避免使用在公共電腦用過的儲存媒體
- 沒有存取網路的時候離線
- 檢視副檔名
- 安裝一套合法的防毒軟體, 並時常更新病毒碼
- 開啟電子郵件的附加檔案前, 可開啟防毒軟體的掃描功能掃描
- 關閉電子郵件軟體的預覽郵件功能
- 利用瀏覽器的安全設定功能來防範

資訊安全的環節

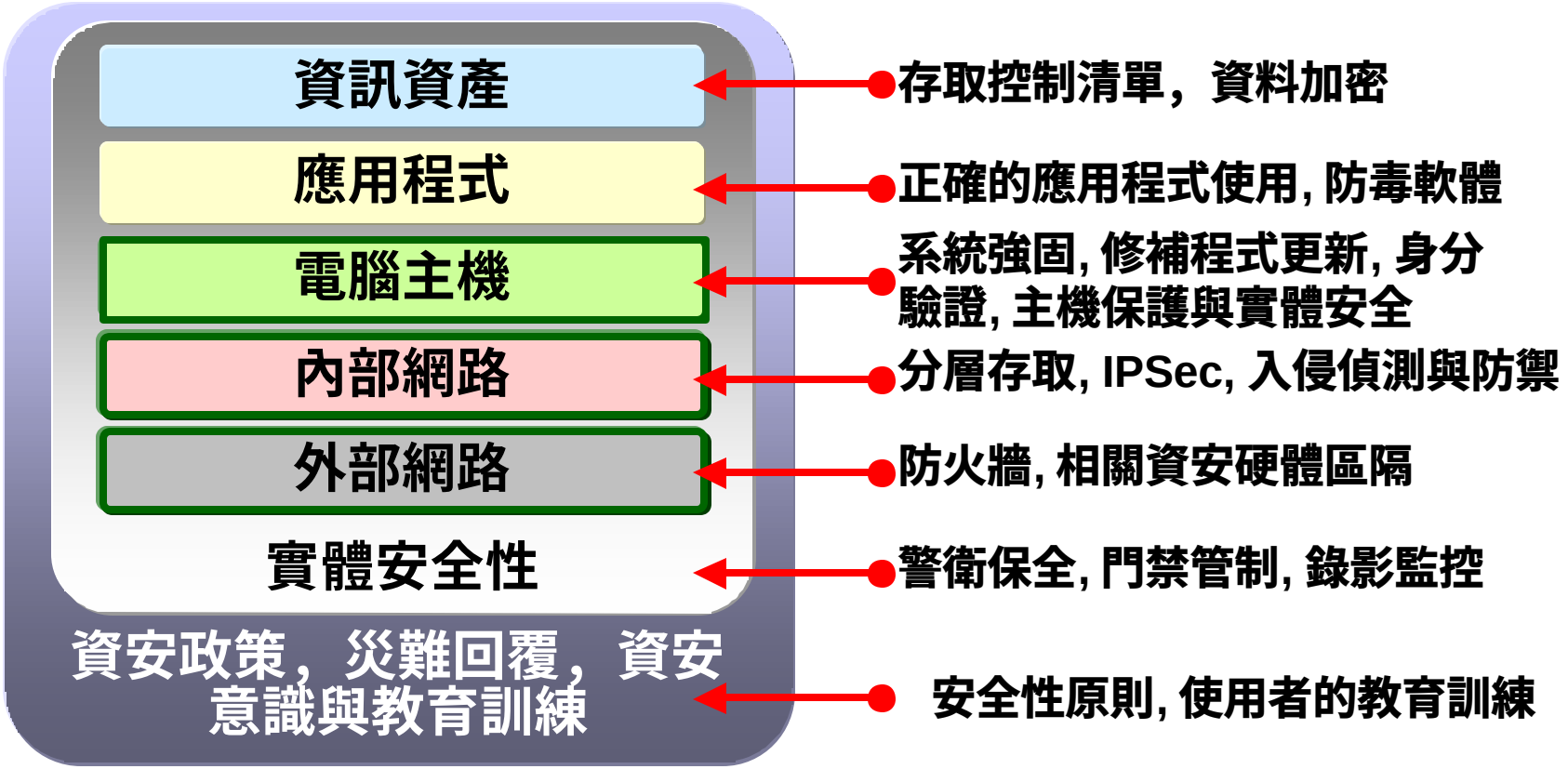
WetWare：泛指程式人員、作業人員、系統管理人員等與電腦接觸的「人」

電腦病毒防範的觀念

- 是一種人人有責的意識
  - 良好正確的使用習慣，例如：強固密碼、定期換密碼
- 妥善的應用工具
  - 停用：不需要的服務
- 進階相關設定
  - 不能用預設值以一套萬
  - 各種機器角色應界定相關的安全設定
- 善用既有的工具
- 安全是一種相對性的成效，沒有絕對的產品！！

縱深防禦觀念 - Defense in Depth

- 建議分層防禦
  - 增加入侵者被偵測機會
  - 降低被入侵成功機會



病毒威脅的防範

- 防火牆的架設
  - 成立有效區隔的安全區間
  - 有效執行不同的安全政策
- 確保電腦更新
  - 降低系統的弱點
  - 減少應用程式的缺失
- 安裝防毒軟體
  - 偵測、清掃、隔離中毒的對象
  - 一致性安全防護
- 執行必要的防範程序
  - 關閉非必要之網路服務功能
  - 整合入侵偵測、防毒程式、防火牆、木馬偵測
  - 確認密碼強度、定期換密碼