臺中市雅潭地政事務所

資訊安全教育訓練

ISMS 導入及資安防護

106年3月14日16日

臺中市雅潭地政事務所

課程內容

課程名稱	講師
ISMS導入	資訊課 胡英嬌課長
資安防護	
問題與討論	
課程評量	

訓練目的

- 強化同仁及志工資訊安全認知。
- 配合地政局導入資訊安全管理系統(簡稱ISMS)。
- 107年3月20日及21日地政局及抽中的5個地所，必須接受ISMS外部稽核複評，請同仁一定要事先做好準備。

107年外部稽核日程表

時　間	3月20日	3月21日
08:30-09:30	地政局啟始會議	
09:30-12:30	A-地政局	A-大里
	B-中興	B-太平
12:30-13:30	休息時間	休息時間
13:30-16:30	A-中山	A-地政局
	B-雅潭	B-地政局
16:30-17:30		地政局結束會議

ISMS導入

- 什麼是資訊安全管理系統(ISMS)
- 國際標準要求(C, I, A)
- 個人資料保護法規定(L)
- 政府機關資安責任等級區分

什麼是資訊安全管理系統(ISMS)

- 資訊安全是組織要隨時保持資訊之機密性 (C) 、完整性 (I) 及可用性 (A)。
  - 機密性 ：確保只有獲得授權的使用者，才可以存取資訊。
  - 完整性：資訊在傳送或儲存過程中，內容未遭到竄改或偽造。
  - 可用性：資料或系統必須即時提供給獲得授權的使用者使用。

什麼是資訊安全管理系統(ISMS)

- ISMS是一組合適的控制措施，這個控制措施包括政策、過程、程序、組織結構及軟硬體功能。
- 將一組合適的控制措施導入組織裡的每一個單位，通過第三方驗證，取得ISMS國際認證證書，就是ISMS導入。

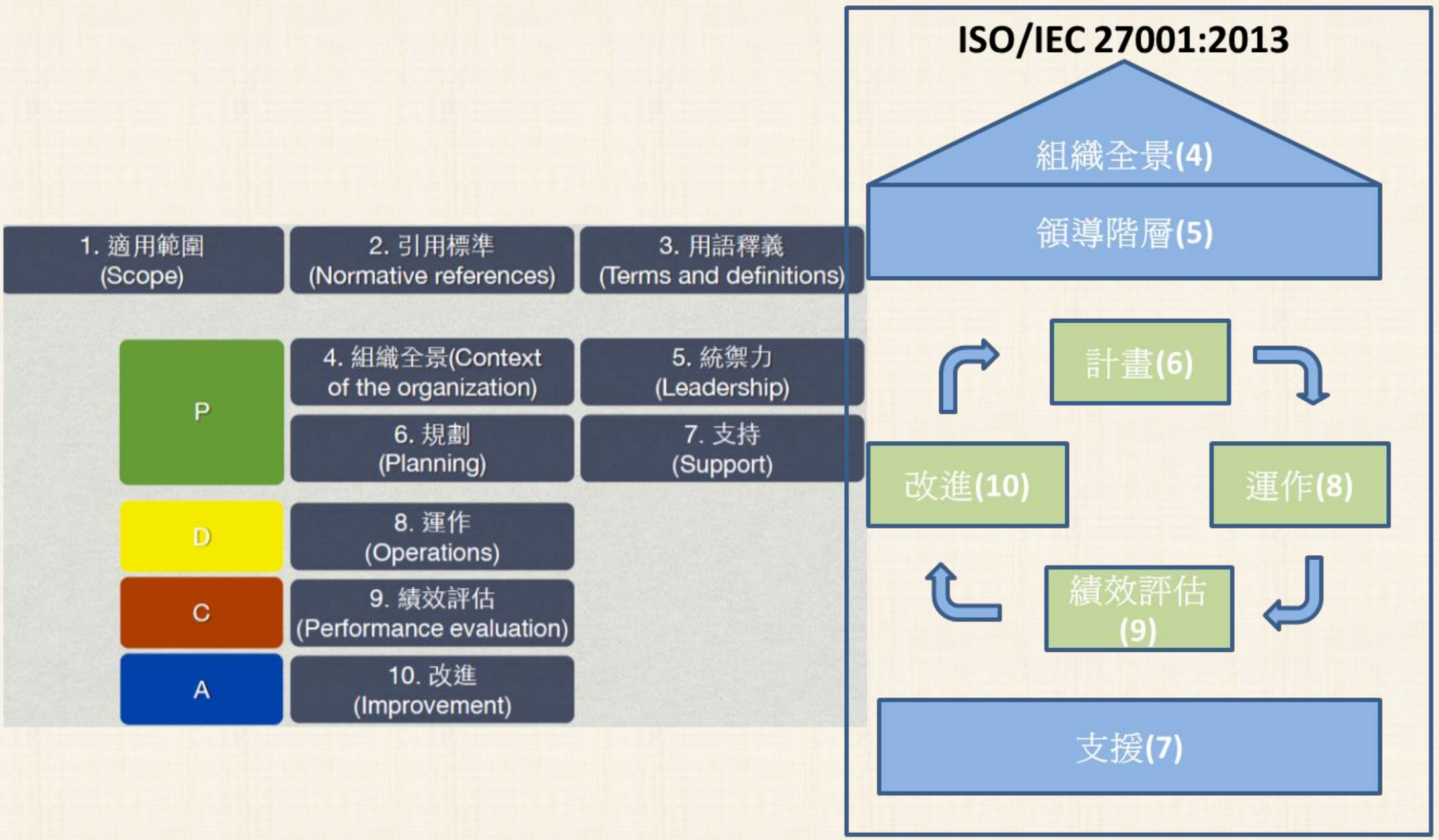
國際標準要求（C, I, A）

- ISO27001:2013

  規定必須在組織的背景下建立控制措施，維護和不斷改進資訊安全管理系統。

- **這些規定包括資訊安全風險評估和根據組織需求制定的資訊安全風險處理方法。**
- **在ISMS導入的過程中，主文第4 到第10章規定的要求，是不可排除的（需全部達到要求），否則無法通過驗證。**

ISO/IEC 27001:2013



個人資料保護法規定（L）

隱私權	個人資料（個資）
●不受干擾的權利、對個人領域事務的控制權。 ●如「孤獨權」、「匿名權」、「秘密權」、「保留權」、「通訊隱私權」、「領域隱私權」、「身體隱私權」、「資訊隱私權」。	● 個資法訂立個資成立的條件：足資識別該個人之資料。 ● 姓名因有同名同姓還不算個資。 但： 姓名+出生日期 姓名+住址 姓名+電話號碼 姓名+車牌號碼 只要能透過組合找到唯一的那個人就是個資。

擁有最多個資的單位

單位別	個資來源	個資檔案
1.政府單位	民眾	● 地籍資料 ● 戶籍資料 ● 人事單位員工資料 ● 個資備份儲存資料
2.教育單位	學生	● 學籍資料
3.醫療單位	病患	● 醫療資料

公務機關洩漏個資的損害賠償責任

法源	受保護資料	賠償金額（新臺幣）	賠償上限（新臺幣）
● 電腦處理個人資料保護法	只限電腦處理的個資	2萬元~10萬元/每人每一事件	以2千萬元為限。
● 個人資料保護法（101/10/01施行）	電腦處理及紙本的個資均受到保護	5百元~2萬元/每人每一事件	以2億元為限。但所涉利益超過2億元者，以所涉利益為限。

政府機關資安責任等級區分

等級	政府機關
A	1.總統府、國安會、立法院、司法院、考試院、監察院、行政院及直轄市政府。 2.立法院、司法院、考試院、監察院及行政院等所屬二級機關、相當二級機關之獨立機關。但其業務或組織單純者，得報經其上級機關核准，調整為B級或C級。 3. 凡涉及外交、國防、國土安全，及掌理全國財政、經濟、警政等重要業務之機關，如外交部領事事務局、內政部警政署刑事警察局等。 4.負責能源、水資源、通訊傳播、交通、金融、緊急救援、高科技園區等關鍵資訊基礎設施之營運機關，如交通部民用航空局飛航服務總臺、臺北市自來水事業處等。 5.保有全國性個人資料檔案之機關，如勞動部勞工保險局、衛生福利部中央健康保險署等。
B	1.縣（市）政府。 2.凡涉及社會秩序及人民財產業務之機關，如地方政府警察局、地方政府地政事務所等。 3.保有區域性或地區性個人資料檔案之機關，如財政部各區國稅局、地方政府戶政事務所等。
C	其他政府機關及地方政府民意機關。

B級政府機關資通安全責任等級應辦事項

年度 / 等級	104	105	106	107
B	1. 每年至少1次內稽 2. 每年至少辦理1次網站安全弱點檢測 3. 每年資安人員(資訊人員)至少1人次須接受12小時以上資安專業課程訓練或資安職能訓練 4. 每年一般使用者與主管至少須接受3小時資安宣導課程並通過課程評量 5. 每年維持至少1張國際資安專業證照與1張資安職能訓練證書之有效性			
	1. 完成資訊系統分級 2. 指派資安專責人力1人 3. 防毒、防火牆、郵件過濾裝置、IDS/IPS、Web應用程式防火牆(機關具有對外服務之核心資訊系統)	1. 每2年至少辦理1次核心資訊系統持續運作演練 2. 完成資訊系統資安防護基準要求 3. SOC監控 4. 每2年至少辦理1次系統滲透測試、 5. 每2年至少辦理1次資安健診	至少2項核心資訊系統完成ISMS導入	至少2項核心資訊系統通過第三方驗證

第三方驗證受稽方應配合事項

- 地政局97年9月即建立 ISO27001:2005 資訊安全管理制度並驗證通過
- 104年轉版 ISO27001:2013 並驗證通過
- 106年6月擴大驗證，地政局及11地所已共同取得一張ISMS國際認證證書。
- 107年3月20日~21日地政局及5地所接受外部稽核追蹤審核，以達驗證持續有效。
- 相關文件持續依現況修正，修正重點依驗證範圍修正至各所通用：
  - 適用性聲明書
  - 資安文件總覽表
  - 適用性法規登記表

第三方驗證受稽方應配合事項

- 推派資安推動小組成員，包含資安長1名、資安聯絡人2名(主辦及協辦)及內稽人員2名。
- 資安推動小組成員參與建置作業與教育訓練，文件修訂討論、利害關係方調查、風險評鑑報告與資產清查、機房管理紀錄、內部稽核與管理審查執行。
- 機房安全整備：
  - 勿堆放易燃物(紙箱)。
  - 勿於機房內飲食(防治蟲鼠害)。
  - 纜線整理(佈纜安全)。
  - 氣體滅火消防設備。
  - 環境安全(溫溼度控管、進出管制權限/ 登記)。

第三方驗證受稽方應配合事項

- **實體與環境安全防護：**
  - **防止組織場所與資訊遭未經授權的人存取、損害及干擾。**
  - **防止資產之遺失、損害、遭竊或破解，並防止組織運作中斷。**
  - **保持紙本及可攜式媒體桌面淨空及電腦螢幕淨空。**
  - **設備安置及保護、資產攜出、無人看管之使用者設備管理。**
  - **專用電腦插座不可以使用其他非電腦之電子產品。**

第三方驗證受稽方應配合事項

- 組織應評估資訊安全績效和ISMS的有效性：
  - 組織應在計畫的時間間隔進行內部稽核，根據提供的資訊判斷是否安全的管理系統。

    稽核員訓練➡各所相互內稽➡內部稽核報告
  - 最高管理者應在計畫的時間間隔審查組織的ISMS ，以確保其持續的適用性，充分性和有效性。

    各所提供執行成果➡地政局管理審查會➡會議記錄

資訊安全政策與目標

- 臺中市政府地政局之資訊安全管理系統以ISO27001：2013標準為建置基準，驗證適用範圍為地籍管理服務之地政業務，包含地政整合系統、土地管理集中資料庫同步異動系統和機房的運行和維護。
- 資訊安全政策為『地政資訊E網通』。
- 資訊安全目標為『達成資訊系統之機密性(C)、完整性(I)、可用性(A)與法規遵循性(L)』。

資訊安全管理系統全景

- 臺中市政府地政局依據「資訊系統分級與資安防護基準作業規定」進行資訊系統分析，評估各資訊系統發生資安事件時，對機密性(C) 、完整性(I) 、可用性(A)及法律遵循性(L)四大影響構面之衝擊程度以識別出各資訊系統業務屬性與安全等級，以建立臺中市政府地政局資訊安全管理系統全景。
- 在機關全景內建立、實作、維持及改進資訊安全管理系統。

重要核心資訊系統風險值計算

- 依據「資訊系統分級與資安防護基準作業規定」之影響構面安全等級設定原則，嚴重性分別為：普(1)；中(2)；高(3)。
- 評估機關內部經驗及外部事件，對發生四大影響構面事件的可能性，分別為：幾乎不可能發生(1)；有可能發生(2)；幾乎確定會發生（３）。
- 經核定之重要核心資訊系統依其衝擊影響構面嚴重性(S)及發生之可能性(P)，評估其風險等級。

重要核心資訊系統風險值計算

- **機關最高風險值RV (9)=嚴重性S(3)×可能性P (3) 。**

可能性 P / 嚴重性 S	幾乎不可能(1)	有可能(2)	幾乎確定(3)
非常嚴重（3）	中（3）	高（6）	**極高(9)**
嚴重（2）	低(2)	中（4）	高（6）
輕微（1）	低(1)	低(2)	中（3）

重要核心資訊系統風險處理

- 應依資訊系統【高】、【中】、【普】等級，執行相對應之防護基準 。
- 除執行相對應之防護基準外，亦應依資訊安全管理系統之安全控制措施進行選用及實施。
- 當風險評估完畢後完成風險評鑑報告，管理審查會議應就該次風險評鑑報告提出一適當之風險可接受值，當計算之風險值大於可接受風險值時，應訂定風險處理計畫。

風險評鑑結果

- 2項重要核心資訊系統風險評估結果
  - 風險本質

    地政局 - 集中資料庫同步異動系統：高風險等級(6分)

    各地所 - 地政整合系統WEB版：中風險等級(4分)
  - 殘餘風險

    經研擬風險處理對策後，在發生機率上均可明顯降低。其殘餘風險：

    集中資料庫同步異動系統：中風險等級(3分)

    地政整合系統WEB版：低風險等級(2分)
  - 106年度核定機關可接受風險值為4分

風險評鑑結果

- 目前風險處理對策已有效降低風險值，其殘餘風險值3分(集中資料庫同步異動系統)為中風險等級，已低於機關核定之可接受風險值4分以下，符合要求。
- 依據「資訊系統分級與資安防護基準作業規定」目前執行高安全等級防護措施，並且實施資訊安全管理系統各項安全管控措施，不需進行額外風險處理計畫。

107年內部稽核日程表

內稽日期	內稽時間	受稽方	現場諮詢及協助	內稽稽核方
1月12日	14:00-17:00	中正	顧問公司-楊顧問	中山、東勢稽核員
1月15日	14:00-17:00	中山		大里、太平稽核員
1月16日	09:00~12:00	雅潭		中興、東勢稽核員
1月19日	09:00~12:00	豐原		清水、大里稽核員
1月23日	09:00~12:00	中興		雅潭、豐原稽核員
1月23日	14:00-17:00	清水		太平、大甲稽核員
1月24日	09:00~12:00	龍井		清水、中興稽核員
1月25日	14:00-17:00	大里		中正、龍井稽核員
1月26日	09:00-12:00	太平		中興、中山稽核員
1月30日	14:00-17:00	東勢		豐原、雅潭稽核員
1月31日	09:00~12:00	大甲		龍井、中正稽核員
2月5日	09:00-17:00	地政局		顧問公司+地政局稽核員

內部稽核應矯正事項

- 矯正措施1：印表機及傳真機部分未落實適當保護措施。
- 矯正前：因列印人員座位
離印表機或傳真機較遠，
因此列印文件後未立即取走。

內部稽核應矯正事項

- 矯正後：印表機及傳真機貼有警語-列印或傳真後請立即取走資料。
- 請同仁列印或傳真後，務必立即取走資料，不要把資料放在印表機及傳真機。

內部稽核應矯正事項

- 矯正措施2：抽查個人電腦發現未落實螢幕淨空政策。
- 矯正前：為方便使用，電腦螢幕桌面放置常用資料夾。

內部稽核應矯正事項

- 矯正後：屬於公務文件及資料夾不再放置電腦螢幕桌面。
- 請同仁屬於公務文件及資料夾不要放置電腦螢幕桌面。

管理審查會議決議

- 107年資訊安全政策延續106年為『地政資訊E網通』，資訊安全目標為『達成資訊系統之機密性、完整性、可用性與法規遵循性』。
- 本年度可忍受風險值維持4分。
- 資訊安全目標達成計畫如下表。

臺中市政府地政局及各地所資訊安全目標達成計畫表--107年度

資安目標	監 控 事 項	有效性量測	定　義	執 行 方 式
機密性	不得有任何資料外洩之事件發生。	0次/月	來源:技服中心及民眾通報	依據臺中市政府監控紀錄、機關機房紀錄統計、民眾通報案件
完整性	同步異動資料傳輸失敗次數	≦3次/季	超過60分鐘,為機關內設備造成之原因	依設備紀錄每月傳輸失敗次數
可用性	地政系統應用程式伺服器可用性	≦2次/月	超過60分鐘無法自行排除	統計服務中斷次數
完整性	防毒伺服器病毒碼軟體更新	≧2次/月	地政內網	依據設備紀錄檢查，至少每兩週一次達成符合性
機密性	惡意郵件郵件開啟率	≦6%		依據每半年臺中市政府測試結果

臺中市政府地政局及各地所資訊安全目標達成計畫表--107年度

資安目標	監 控 事 項	有效性量測	定　義	執 行 方 式
機密性	惡意郵件連結或附加檔案點閱率	≦5%		依據每半年臺中市政府測試結果
完整性	電腦防毒偵測病毒入侵次數	≦5台/月	地政內網	依據每月防毒月報統計
可用性	防火牆異常狀態	≦1次/月	超過60分無法自行排除	每週檢視防火牆紀錄
機密性	資安監控APT攻擊事件	≦1件/季	經監控發現APT攻擊成功行為	依據每月臺中市政府監控通知統計或機關機房資安防禦紀錄經判定為攻擊行為成功者
法規遵循性	對適用之法規進行查詢	1次/年		每年更新「適用法規登記表」

管理審查會議決議

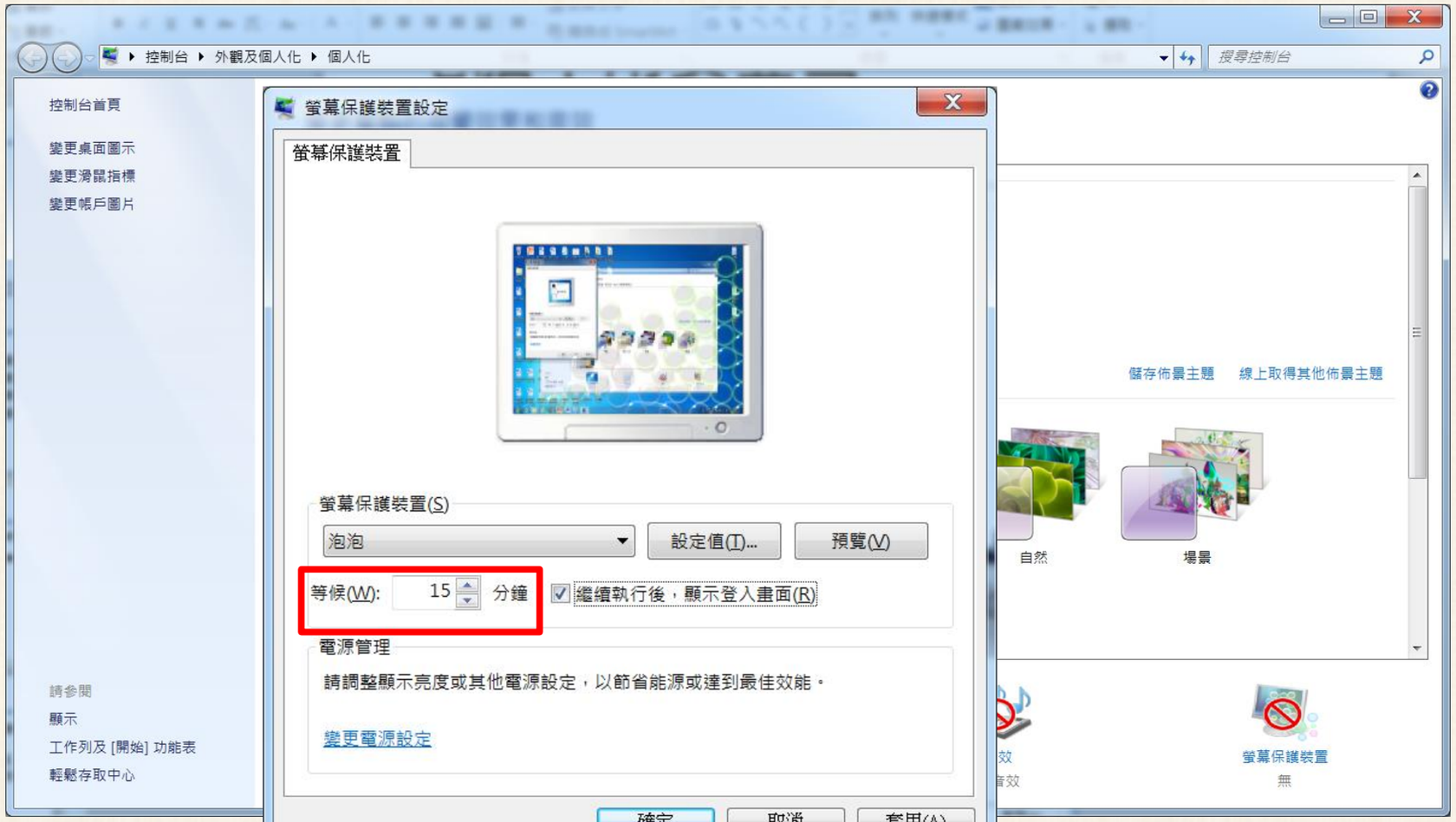
- 地政局及各地所於106年6月1日通過ISMS第三方驗證，取得證書。依規定每年必須接受外部稽核複評，每三年重新驗證。本年度預定3月20日及21日接受外部稽核，除地政局外，另抽5個地政事務所為受稽機關。請各地政事務所加強準備相關文件，以供外部稽核員查核之用
- 外部稽核前注意事項

資安防護

- 電腦不用要登出
- 機密資料要保護
- 密碼設定要穩固
- 重要資料要備份
- 電腦防毒要更新
- 應用系統要更新
- 上網瀏覽要提防
- 電子郵件要過濾
- USB使用要謹慎

電腦不用要登出

- 使用者個人電腦啟用螢幕保護程式之密碼鎖定功能(設定15分鐘以內)。
- 每月不定期稽核1次以上，防止其他使用者操作。



機密資料要保護

- 機密及敏感文件不可遺留於辦公桌上，必須存放安全場所並加以上鎖。
- 作廢敏感文件不得回收再利用。
- 電腦螢幕不可放置公務文件及資料夾。
- 供民眾使用的外網電腦，關閉網路芳鄰資料分享。
- 印表機、傳真機列印後，立即取走資料。

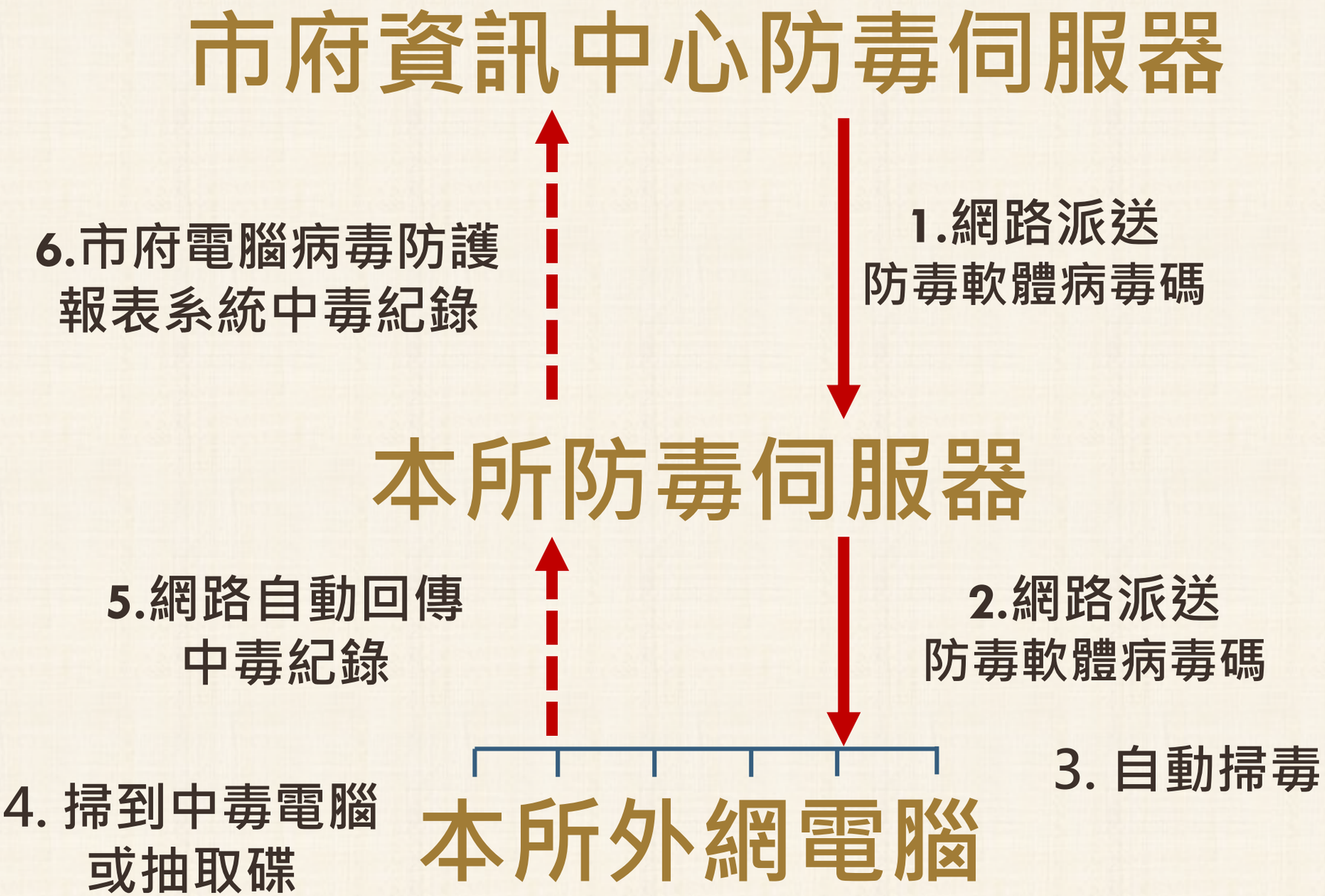
密碼設定要穩固

- 較佳的設密碼原則（5要）：
  - 密碼要至少8碼，包含英文大小寫、數字及特殊符號，且密碼不包含帳號。
  - 密碼要任何沒有意義的組成。
  - 密碼要記得住，最好能夠自己迅速的不看鍵盤就可以打出來（別人偷看想記的時間都來不及）。
- 至少每3個月更改一次密碼。

重要資料要備份

- 定期備份資料：
  - 預防重要資料或設備損壞遺失。
  - 預防勒索軟體加密。
  - 確保可用性。
- 遵守3-2-1備份原則：
  - 3份備份（至少1份處於離線狀態）。
  - 2種儲存媒體。
  - 至少1個不同的存放地點。

電腦防毒要更新


市府資訊中心防毒伺服器
1.網路派送
防毒軟體病毒碼
6.市府電腦病毒防護
報表系統中毒紀錄
本所防毒伺服器
2.網路派送
防毒軟體病毒碼
5.網路自動回傳
中毒紀錄
3. 自動掃毒
4. 掃到中毒電腦
或抽取碟
本所外網電腦

應用系統要更新

- 作業系統或應用程式設計上有漏洞。
- 駭客經常透過漏洞來入侵電腦。
- 更新作業系統或應用程式的修補程式。

  (自動更新會關閉可能的安全性漏洞，

  協助防止來自駭客的病毒和攻擊)
- 不要安裝未經驗證安全的軟體。
- 使用合法版權軟體。

上網瀏覽要提防

- 釣魚網站是駭客誘騙電腦使用者透過電子郵件或網站提供個人或財務資訊的一種手段。
- 常見釣魚方式：假網頁、電子郵件、社交軟體。
- 點選網站要確認網址，以免誤入釣魚網站（偽冒網站）陷阱。

例如：原來是

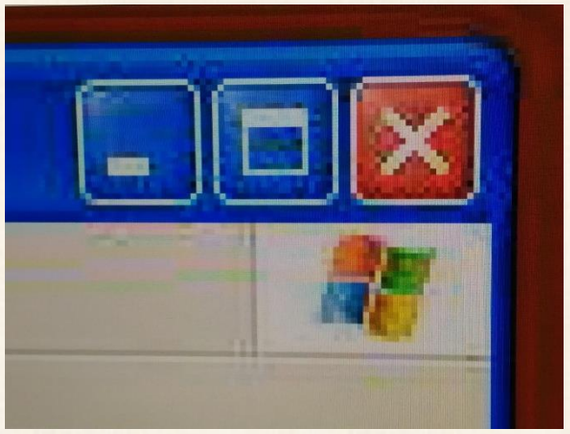
- www.abc.com.tw 偽冒成 www.abc.com
- www.land.com.tw偽冒成 www.1and.com.tw。

上網瀏覽要提防

- 選擇加密網站HTTPS瀏覽。

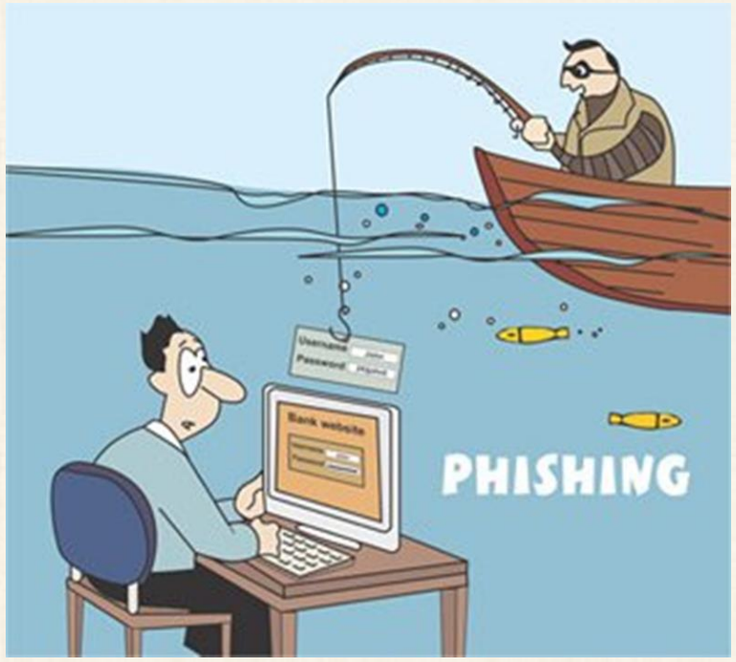
HTTPS 是一種網際網路通訊協定，可確保資料在使用者的電腦和網站之間傳輸時，保有完整性和機密性。

- 不要輕易按下同意與接受的按鈕。
- 絕對不按[同意] 或[確定] 按鈕來關閉視窗，務必使用視窗角落的紅色[X] 按鈕。



電子郵件要過濾

- **提高收發電子郵件警覺性：**
  - 確認寄件來源及寄件者。
  - 確認郵件主旨及郵件內容。
  - 是否與業務相關。
  - 不開啟連結是否有影響。
  - 審慎查證寄件者。



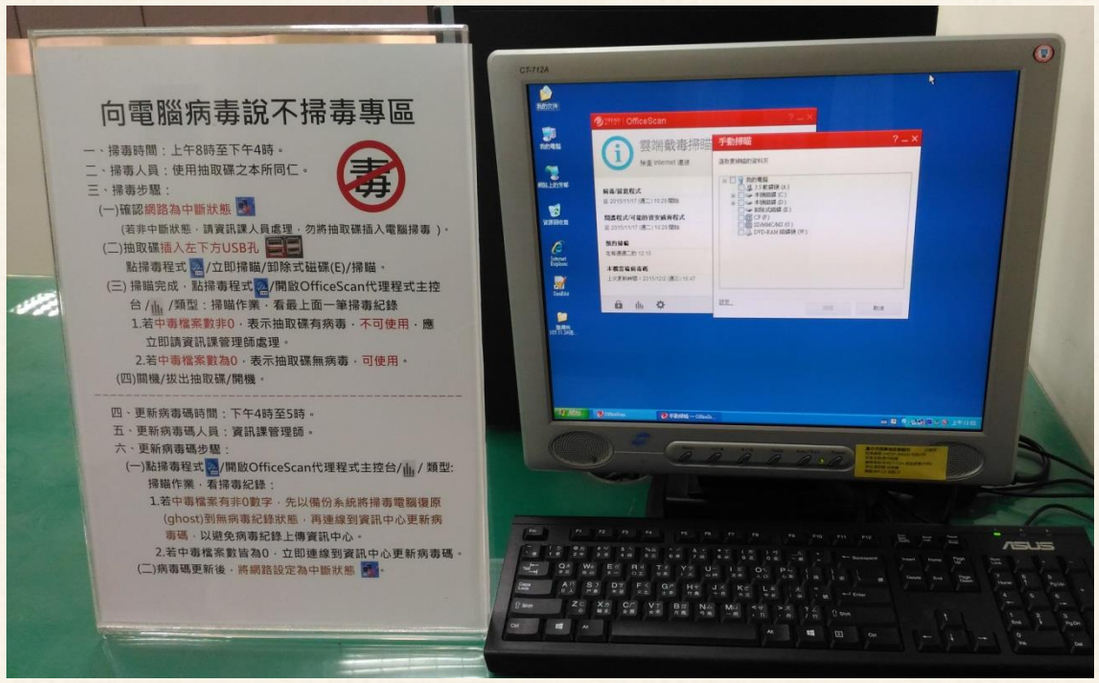
- **發現疑似網路釣魚郵件，儘速刪除勿開啟。**
- **關閉郵件預覽視窗。**
- **以純文字開啟信件。**
- **使用公務電子信箱收發公務所需資訊。**

USB使用要謹慎

- USB等可攜式媒體資安威脅:
  - 遺失洩漏資訊
  - 傳播病毒
- 防範方式：
  - 小心保管，避免遺失。
  - 使用前，先掃毒。
  - 盡量不要使用別人的USB傳來傳去。

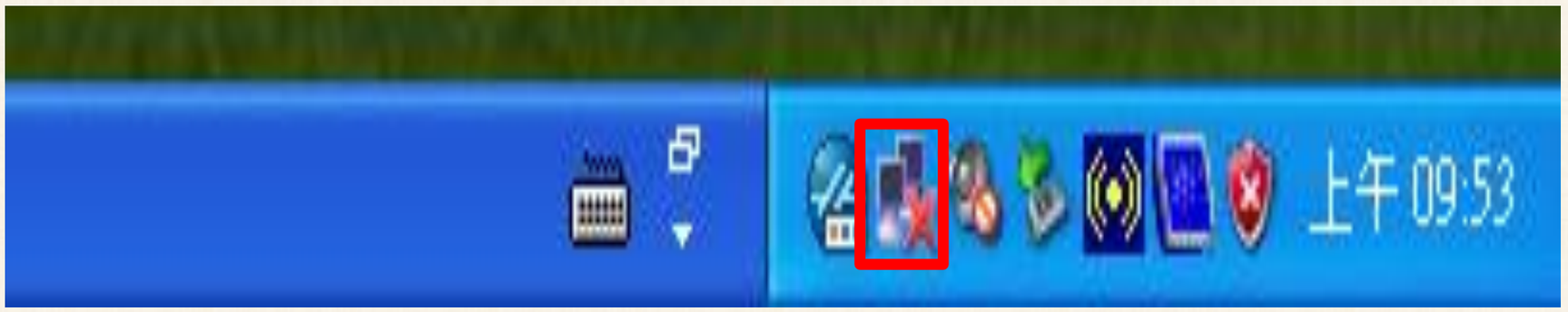
向電腦病毒說不掃毒專區

- 1樓設置「掃毒專區」，供同仁使用抽取碟（USB）前掃毒。
- 掃毒專用電腦採離線掃毒，不掃毒時與臺中市政府資訊中心連線更新病毒碼。



掃毒專區掃毒步驟

(一)確認網路為中斷狀態

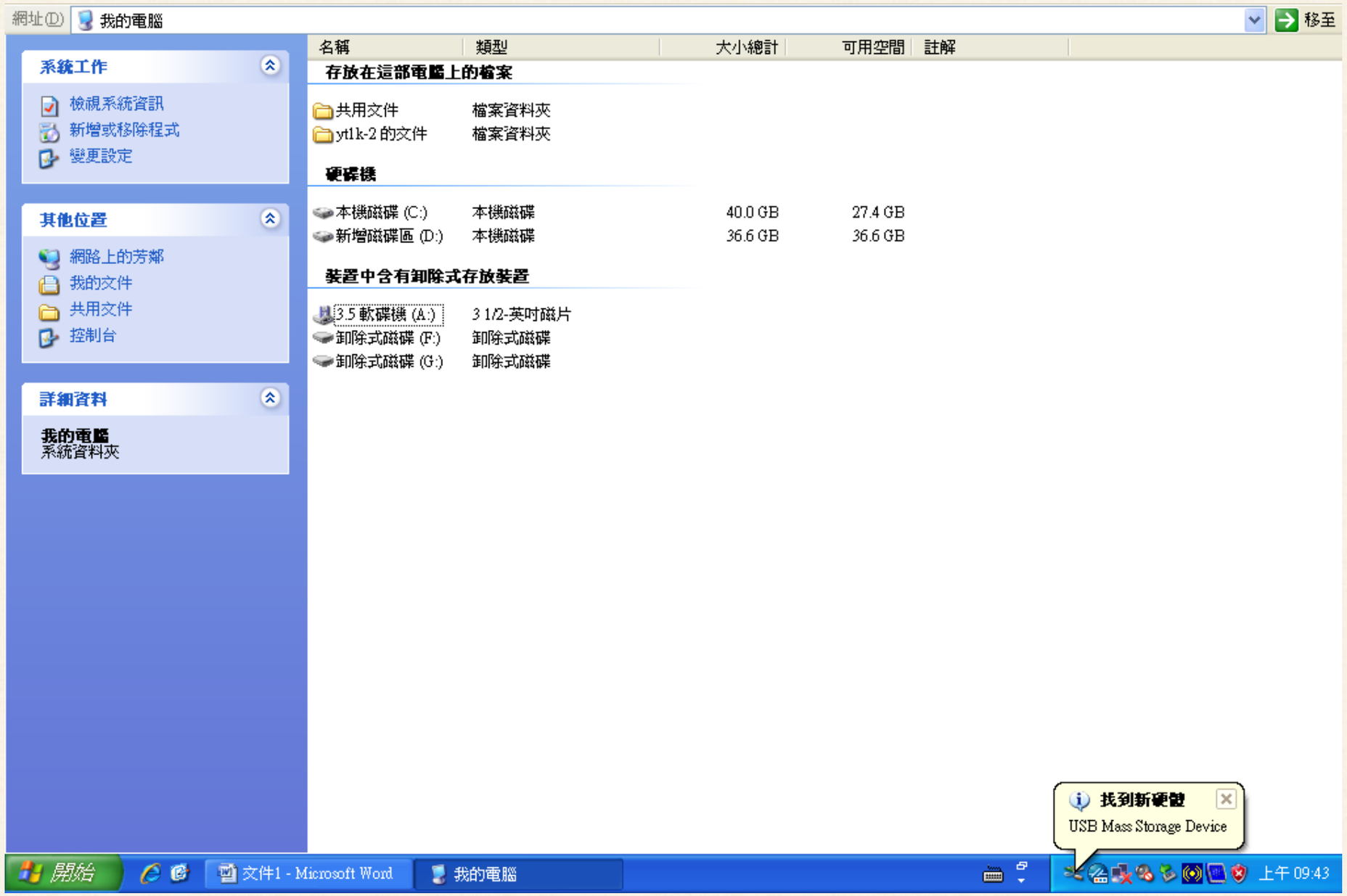


掃毒專區掃毒步驟

(二)抽取碟插入左下方 USB 孔

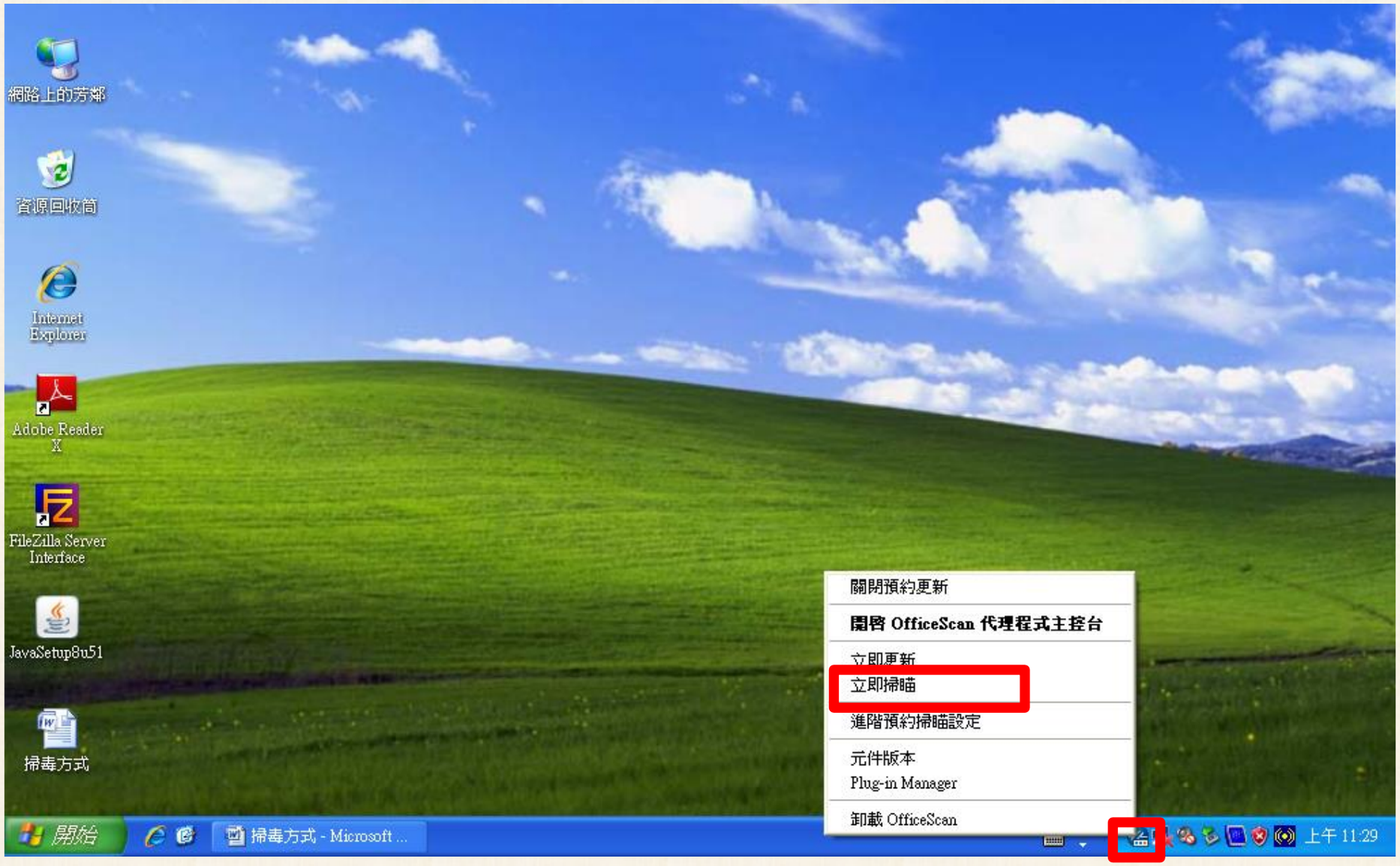
掃毒專區掃毒步驟

找到新硬體



掃毒專區掃毒步驟

點掃毒程式 /立即掃瞄



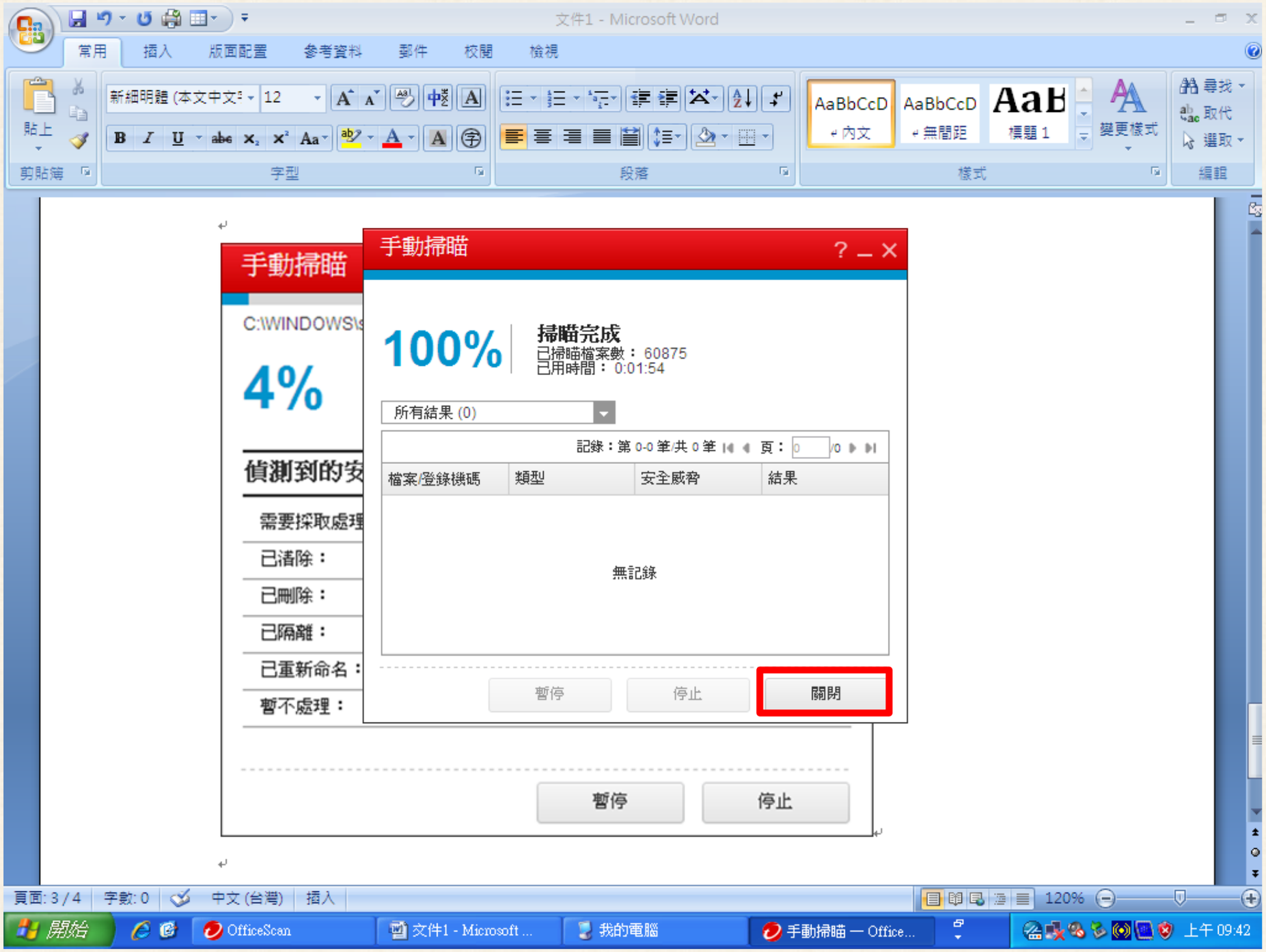
掃毒專區掃毒步驟

勾選卸除式磁碟(E)/掃瞄

掃毒專區掃毒步驟


手動掃瞄
C:\WINDOWS\system32\imm32.dll
4%
正在掃瞄...
已掃瞄檔案數： 0
已用時間： 0:00:08
偵測到的安全威脅： 0
需要採取處理行動： 0
已清除： 0
已刪除： 0
已隔離： 0
已重新命名： 0
暫不處理： 0
暫停
停止

掃毒專區掃毒步驟


文件1 - Microsoft Word
常用
插入
版面配置
參考資料
郵件
校閱
檢視
貼上
剪貼簿
新細明體 (本文中文)
12
字型
段落
AaBbCcD
內文
AaBbCcD
無間距
AaB
標題 1
變更樣式
樣式
尋找
取代
選取
編輯
手動掃瞄
C:\WINDOWS\s
4%
偵測到的安
需要採取處理
已清除：
已刪除：
已隔離：
已重新命名：
暫不處理：
暫停
停止
手動掃瞄
100%
掃瞄完成
已掃瞄檔案數： 60875
已用時間： 0:01:54
所有結果 (0)
記錄：第 0-0 筆/共 0 筆
頁：
檔案/登錄機碼
類型
安全威脅
結果
無記錄
暫停
停止
關閉
頁面: 3 / 4
字數: 0
中文 (台灣)
插入
120%
開始
OfficeScan
文件1 - Microsoft ...
我的電腦
手動掃瞄 — Office...
上午 09:42

掃毒專區掃毒步驟

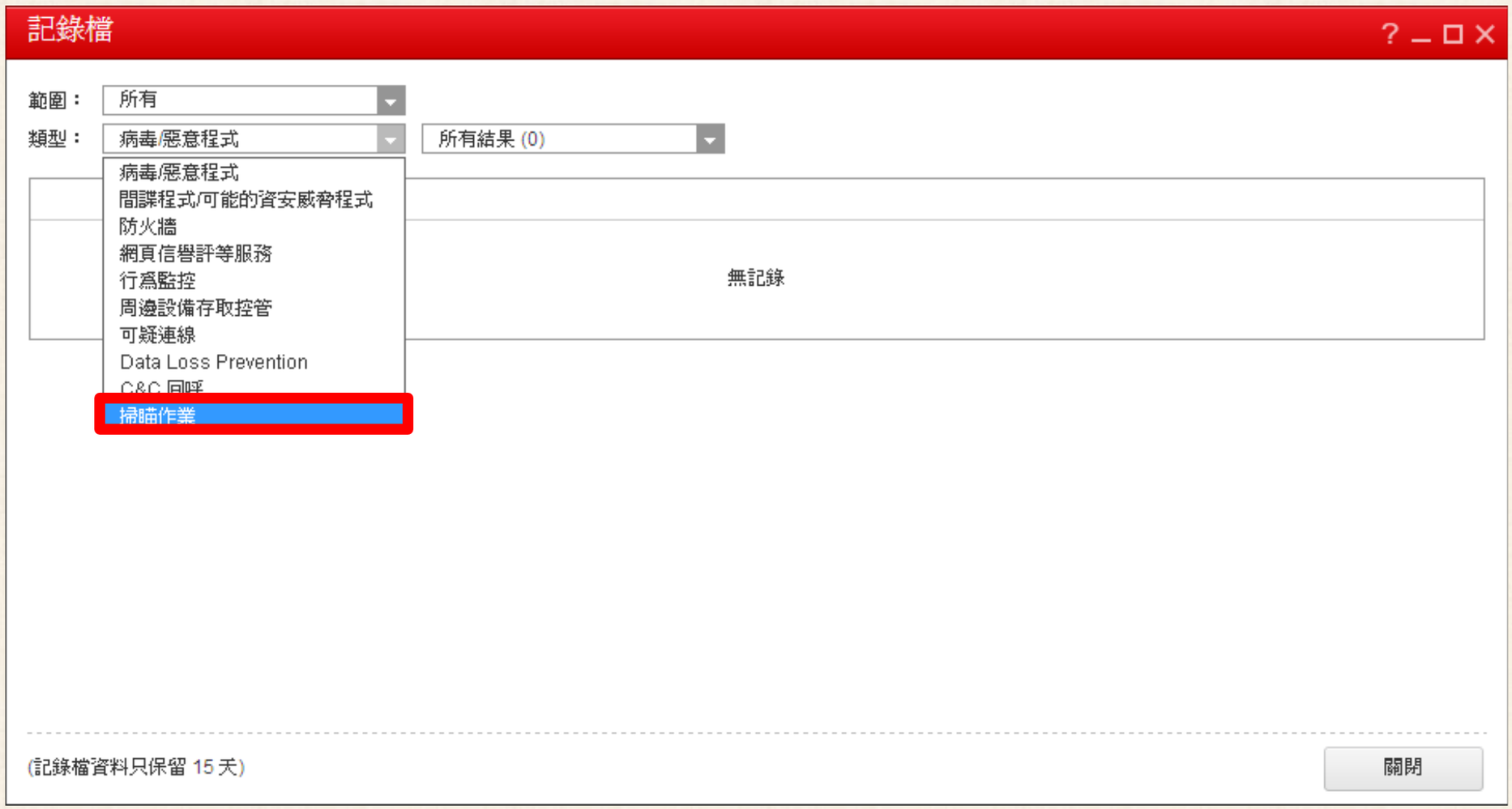
(三) 掃瞄完成，點掃毒程式 /開啟 OfficeScan 代理程式主控台

掃毒專區掃毒步驟

點 記錄檔

掃毒專區掃毒步驟

類型：掃瞄作業

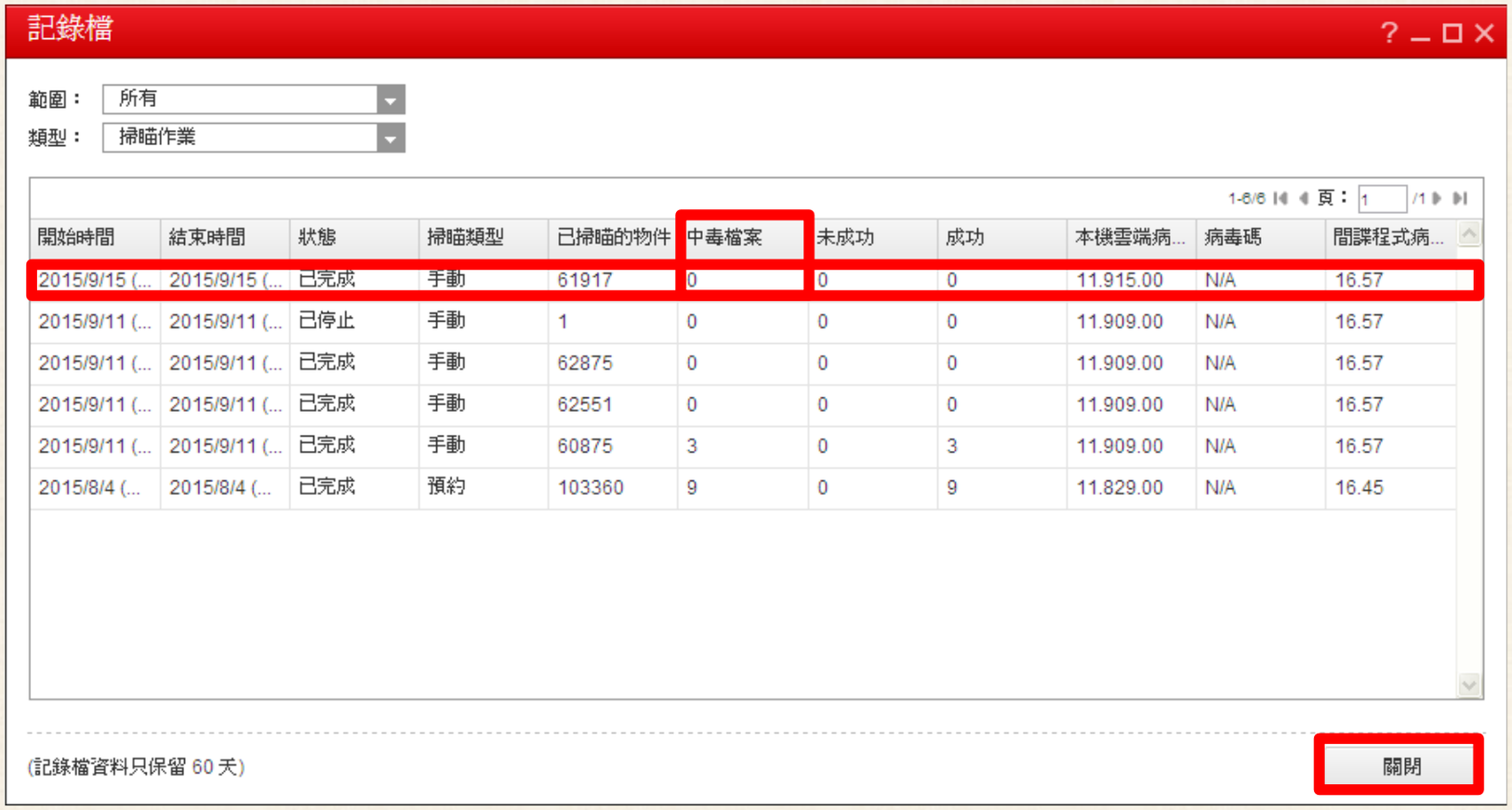


掃毒專區掃毒步驟

看最上面一筆掃毒紀錄：

1.若中毒檔案數非 0，表示抽取碟有病毒，不可使用，
　應立即請資訊課管理師處理。

2.若中毒檔案數為 0，表示抽取碟無病毒，可使用。



(四)關機/拔出抽取碟/開機。

認證抽取碟之分配

- 本所抽取碟認證數，依地政局規定不能超過16個(全所83個員額的5分之1)。
- 各單位分配之抽取碟數量：

單位	主任室	秘書室	會計室	人事室	第一課	第二課	第三課	第四課	資訊課
數量	1	1	1	1	3	3	2	2	2

電腦中毒禁用抽取碟

- 資訊課管理師每日上網查詢本所電腦有無列入臺中市政府資訊中心電腦中毒清單，並記載於機房工作日誌。
- 本所電腦列入電腦中毒清單，不論是否因使用抽取碟中毒，該電腦均禁用抽取碟3個月；若因使用抽取碟中毒，則取消抽取碟認證，3個月內不得遞補其認證缺額。

ISMS導入及資安防護

問題與討論