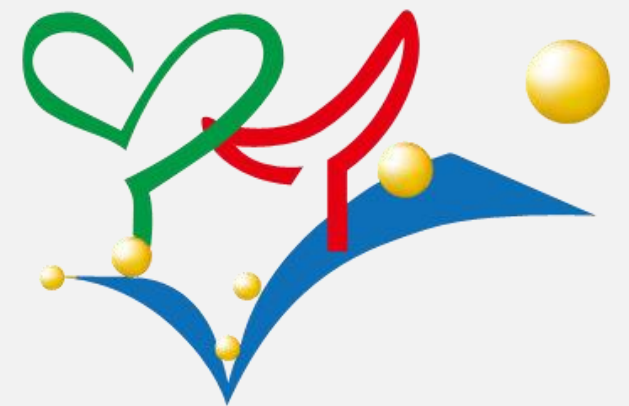


臺中市雅潭地政事務所

資安防護與花博相本操作

106年10月20日



臺中市雅潭地政事務所

課程內容

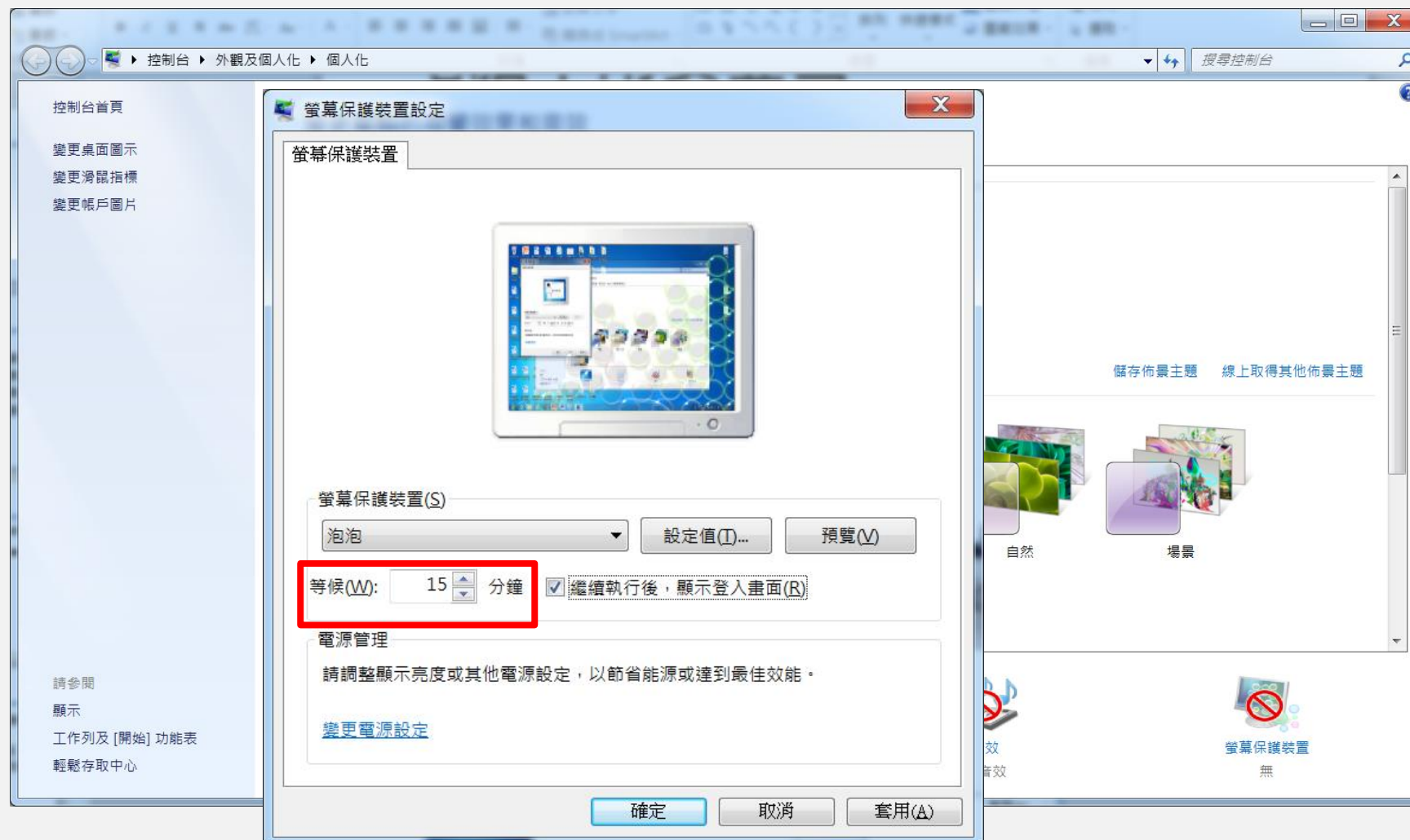
課程名稱	講師
資安防護	資訊課 林志忠管理師
花博相本操作	
問題與討論	
資安防護課程評量	

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。

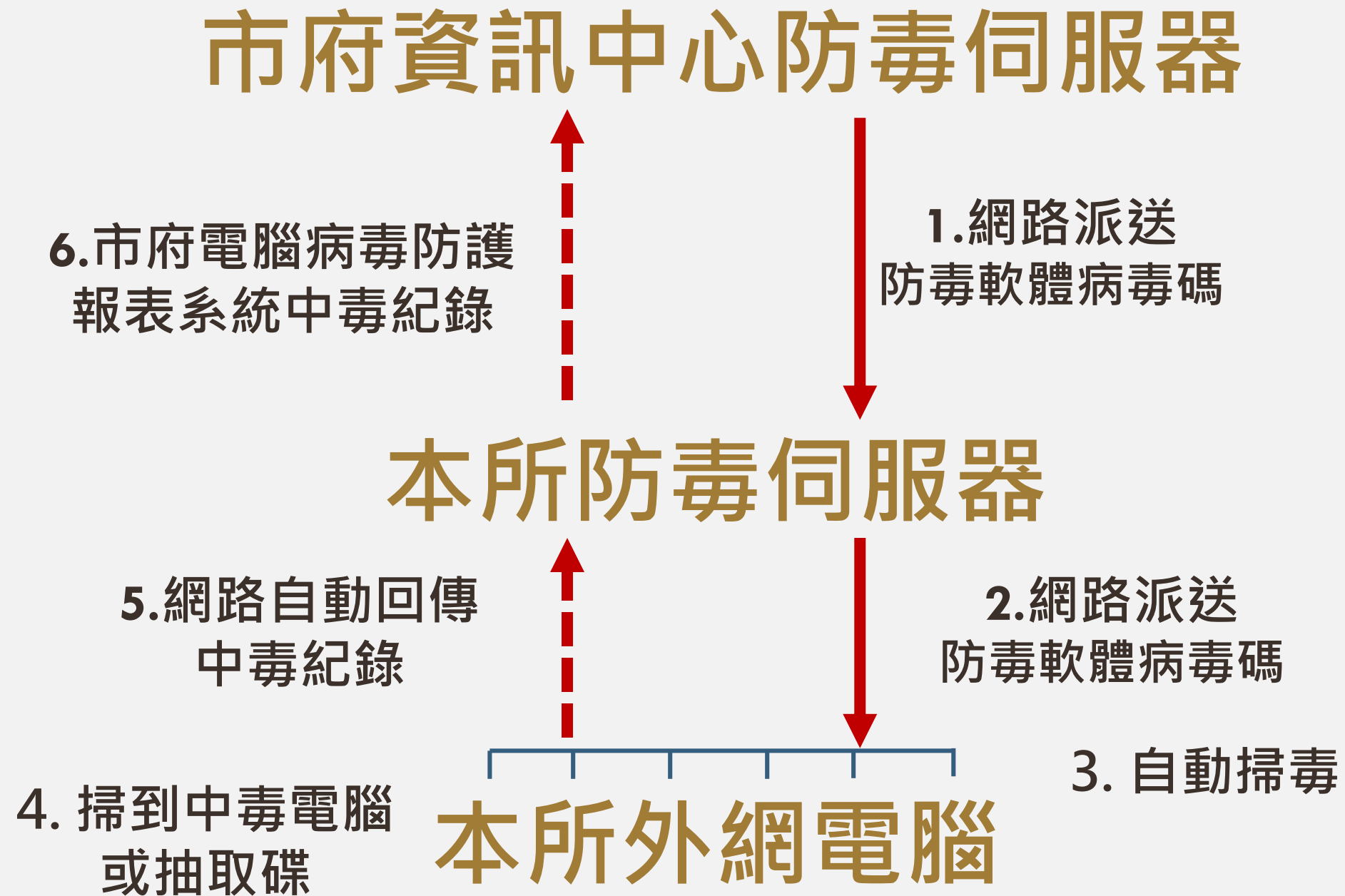
密碼設定要穩固

- 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



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

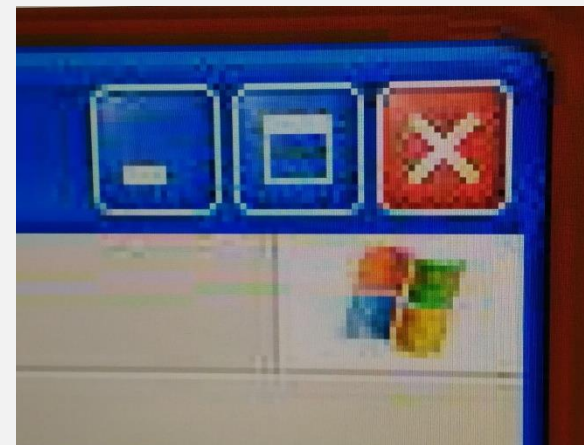
上網瀏覽要提防

- 選擇加密網站HTTPS瀏覽。



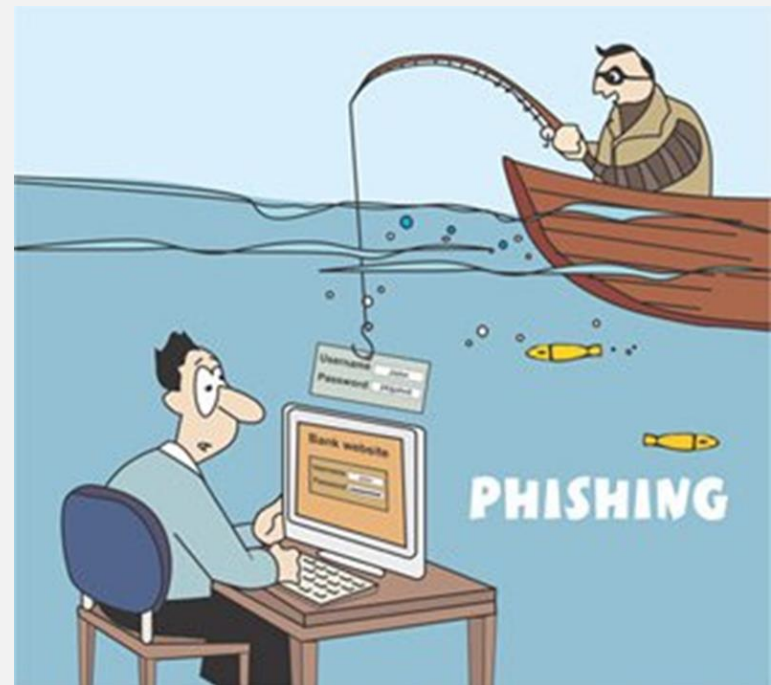
HTTPS 是一種網際網路通訊協定，可確保資料在使用者的電腦和網站之間傳輸時，保有完整性和機密性。

- 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。

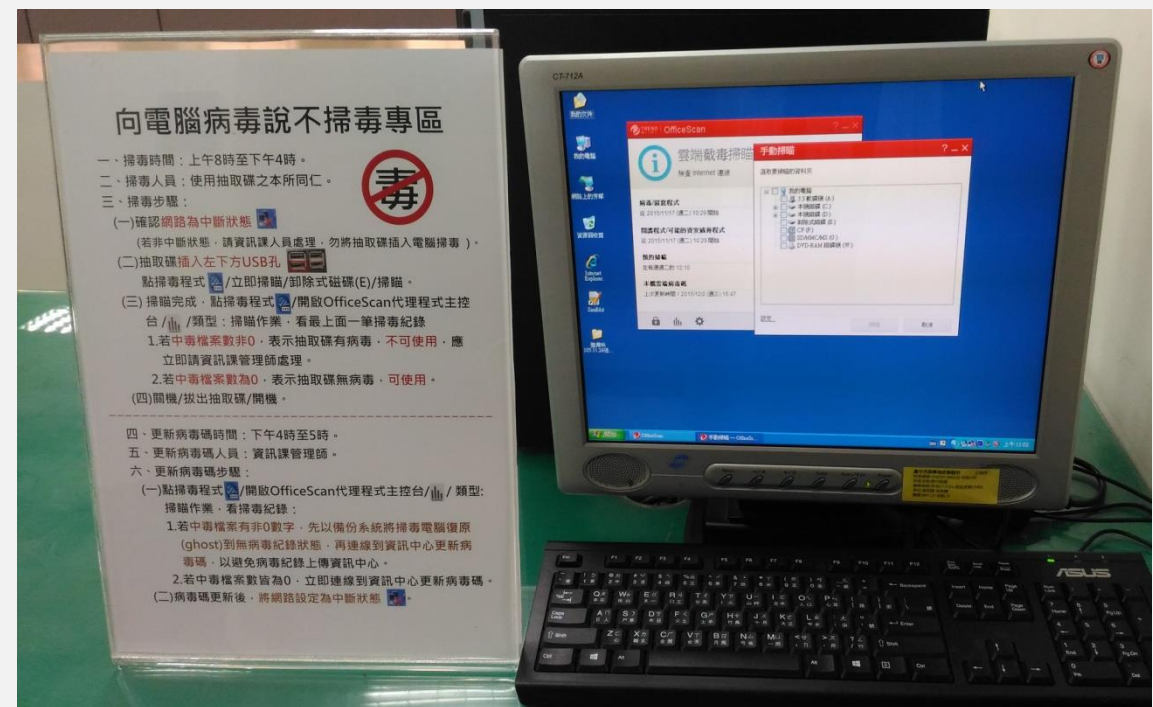
USB使用要謹慎

- 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。



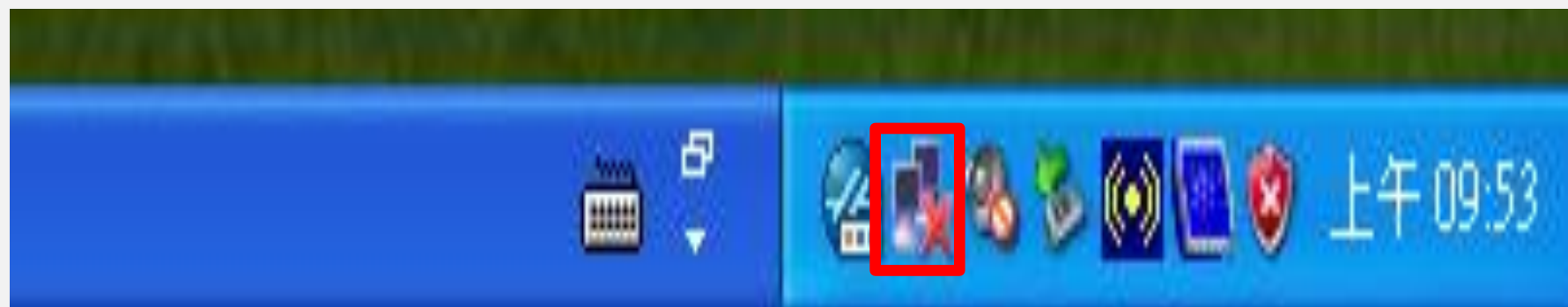
向電腦病毒說不掃毒專區

- 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

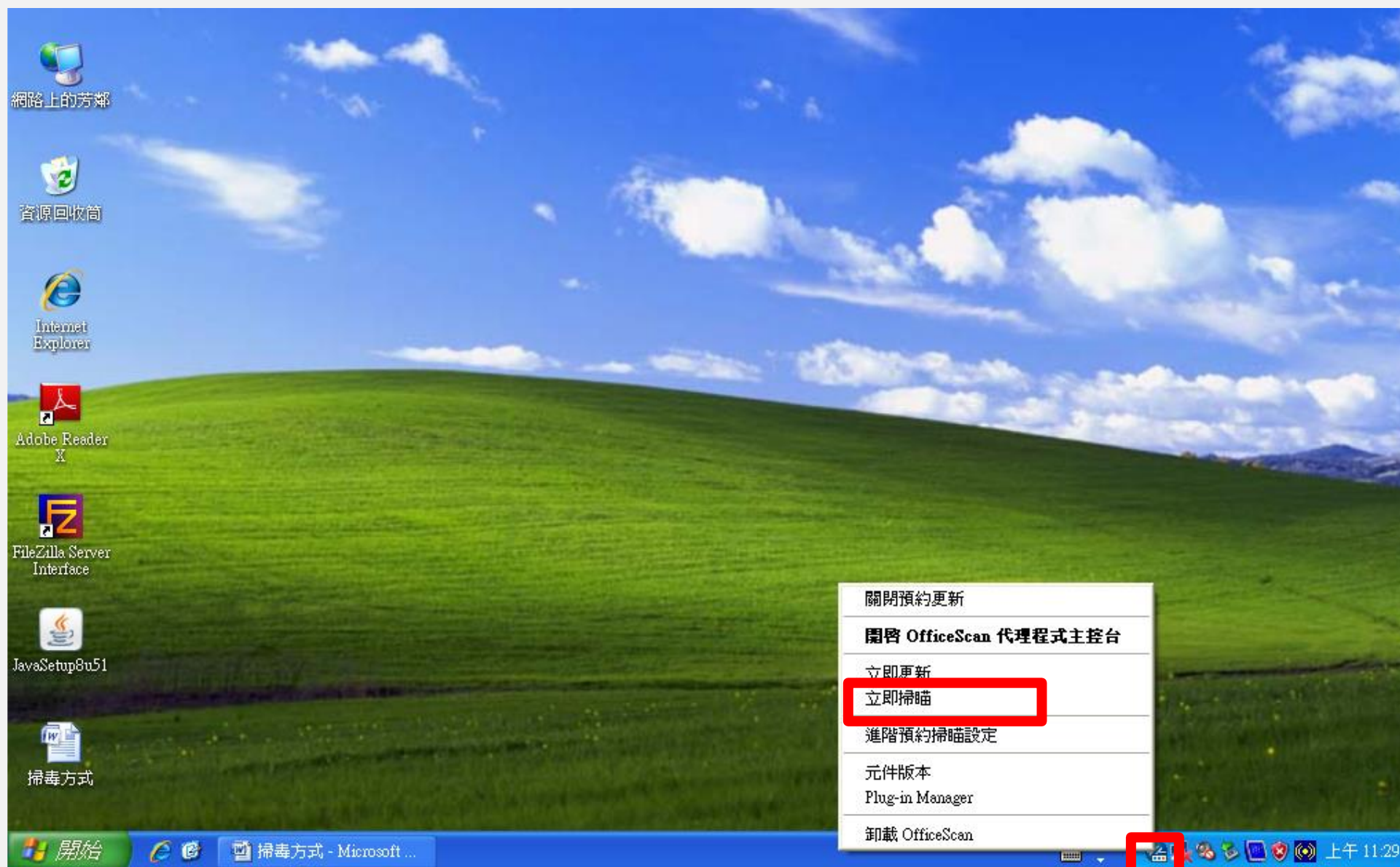
The screenshot shows the Windows XP 'My Computer' window. The address bar shows '我的電腦'. The left sidebar has sections for '系統工作', '其他位置', and '詳細資料'. The main pane displays a table of storage devices:

名稱	類型	大小總計	可用空間	註解
存放在這部電腦上的檔案				
共用文件	檔案資料夾			
yt1k-2 的文件	檔案資料夾			
硬碟機				
本機磁碟 (C:)	本機磁碟	40.0 GB	27.4 GB	
新增磁碟區 (D:)	本機磁碟	36.6 GB	36.6 GB	
裝置中含有卸除式存放裝置				
3.5 軟碟機 (A:)	3 1/2-英寸磁片			
卸除式磁碟 (F:)	卸除式磁碟			
卸除式磁碟 (G:)	卸除式磁碟			

In the bottom right corner, a notification bubble titled '找到新硬體' (Find New Hardware) indicates a 'USB Mass Storage Device' has been detected. The taskbar at the bottom shows the Start button, open applications (Microsoft Word), and the system tray with the time '上午 09:43'.

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

手動掃描

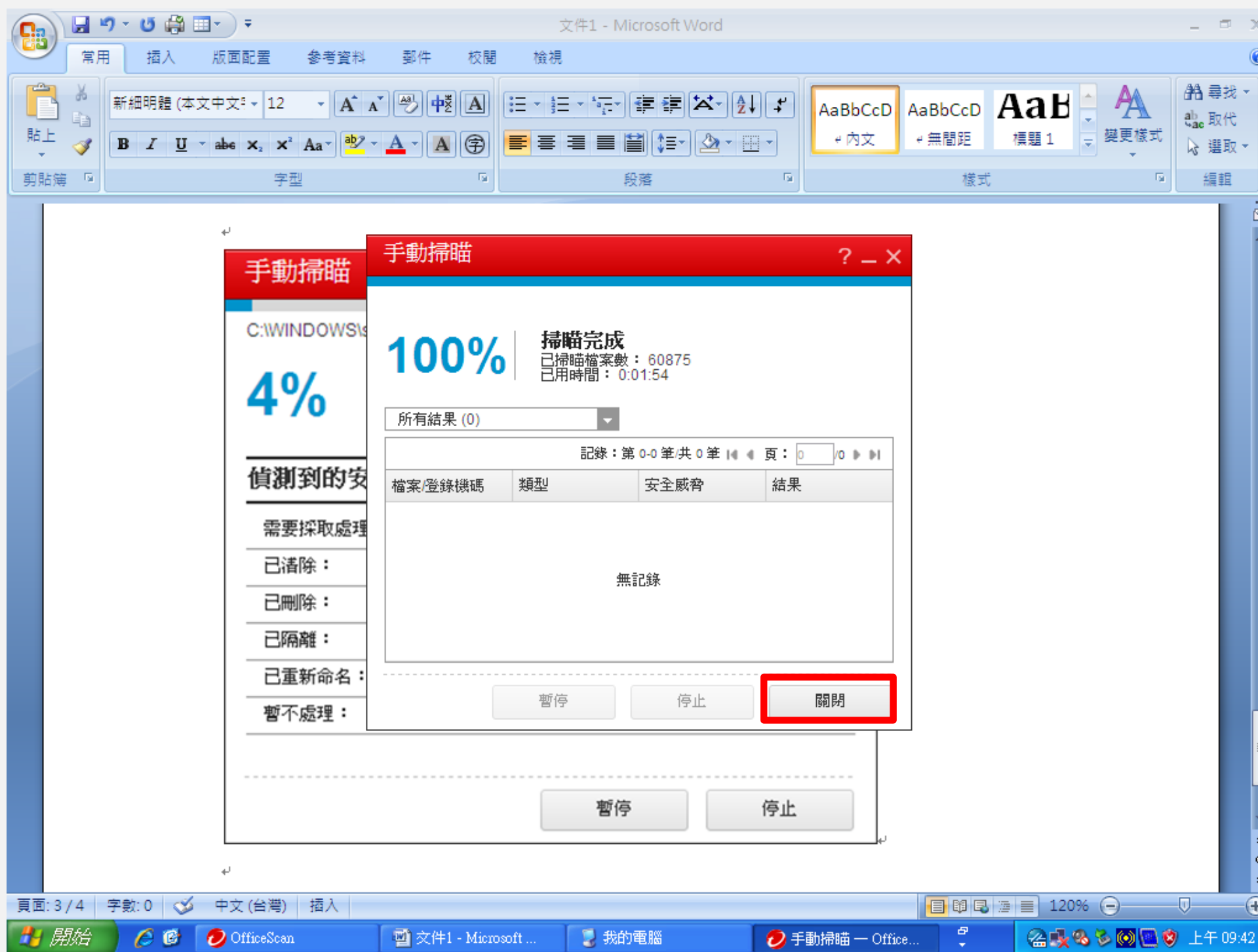
C:\WINDOWS\system32\imm32.dll

4% | **正在掃描...**
已掃描檔案數：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



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

點山記錄檔



TREND MICRO | OfficeScan ? _ X

雲端截毒掃瞄無法使用
檢查 Internet 連線

病毒/惡意程式 0
從 2015/8/31 (週一) 11:12 開始

間諜程式/可能的資安威脅程式 0
從 2015/8/31 (週一) 11:12 開始

預約掃瞄 已啟動
在每週週二的 12:10

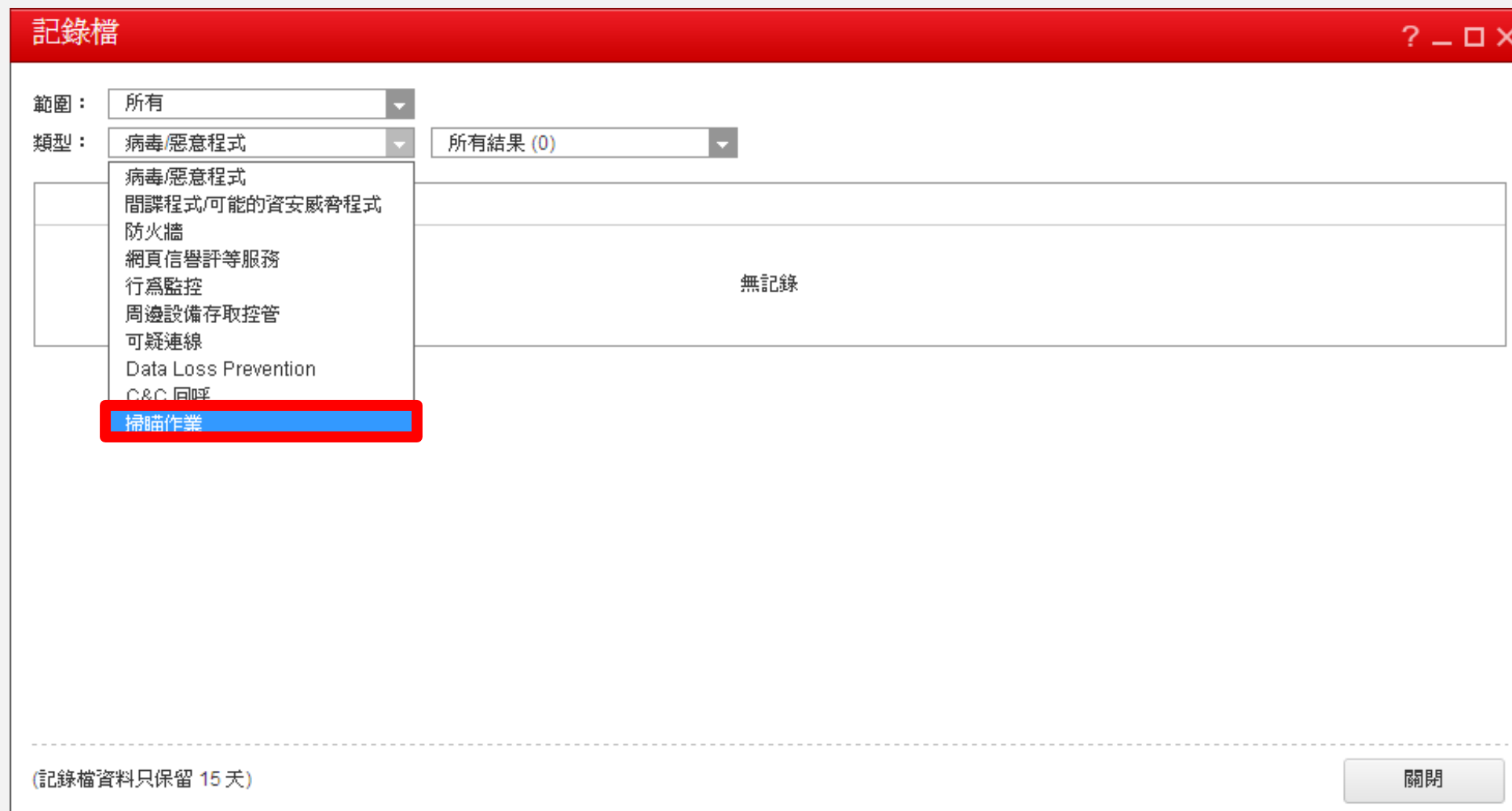
本機雲端病毒碼 11.915.00
上次更新時間：2015/9/15 (週二) 10:28

記錄檔

掃瞄
更新

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。

記錄檔

範圍： 所有

類型： 掃描作業

1-8/8 頁： 1 / 1

開始時間	結束時間	狀態	掃描類型	已掃描的物件	中毒檔案	未成功	成功	本機雲端病...	病毒碼	間諜程式病...
2015/9/15 (...)	2015/9/15 (...)	已完成	手動	61917	0	0	0	11.915.00	N/A	16.57
2015/9/11 (...)	2015/9/11 (...)	已停止	手動	1	0	0	0	11.909.00	N/A	16.57
2015/9/11 (...)	2015/9/11 (...)	已完成	手動	62875	0	0	0	11.909.00	N/A	16.57
2015/9/11 (...)	2015/9/11 (...)	已完成	手動	62551	0	0	0	11.909.00	N/A	16.57
2015/9/11 (...)	2015/9/11 (...)	已完成	手動	60875	3	0	3	11.909.00	N/A	16.57
2015/8/4 (...)	2015/8/4 (...)	已完成	預約	103360	9	0	9	11.829.00	N/A	16.45

(記錄檔資料只保留 60 天)

關閉

(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。

資安防護及花博相本操作

問題與討論