

USB病毒防範與解除

ccjh.kl.edu.tw/modules/tad_book3/html_all.php

USB病毒防範與解除

USB Virus Killer

快速移除USB病毒的小程式。

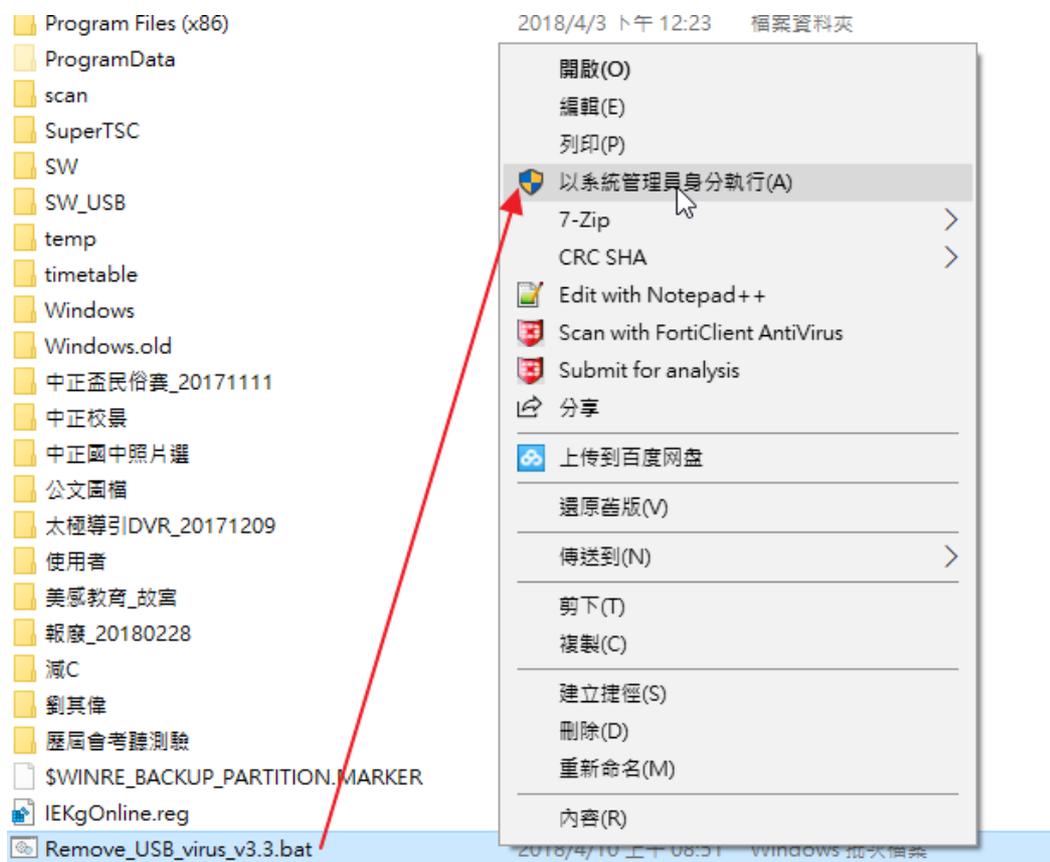
下載後解壓縮，直接點擊USBVirusKiller.exe即可。

USB_Virus_Killer

解除Helper.vbs等變種的USB病毒的批次檔(壓縮檔)。

Remove_USB_Virus

下載後於解壓縮檔案，於*.bat上點擊滑鼠右鍵，選取「以系統管理員身份執行」，如下圖：



於如下畫面處點擊你所想要執行的選項：

```
C:\WINDOWS\System32\cmd.exe
=====捷徑病毒修復程式說明=====
編輯者：Lun 2017.12.06  版本：v3.3
適用狀況：所有檔案皆變為捷徑檔、隨身碟點開變為捷徑。
修復程式僅會刪除病毒檔案，其餘非病毒相關檔案並不影響。
程式請以→右鍵→"系統管理員身分執行"
    ※本程式不負擔任何資料遺失或異常之責任，重要資料應自行養成備份習慣。
=====程式將開始執行=====
功能：
1.自動移除並修復(預設)
2.移除電腦中病毒
3.修復隨身碟
4.關閉程式
    ※若要修復檔案，請務必確認此程式已放在隨身碟根目錄下。
輸入欲執行編號或直接按 ENTER 執行預設
工作編號：
```

USB病毒防範與解除

3. USB病毒的徵狀

最重要的判斷依據，就是隨身碟（硬碟、記憶卡...），本來的檔案或資料夾全變成「捷徑」。如下圖示例：

當然，這種情形下，檔案根本無法開啟，通常病毒會將自己隱藏起來，如果使用者點擊捷徑，就會將病毒複製到硬碟並執行，最後整台電腦的C:\下所有的資料夾或檔案可能都變成「捷徑」。



USB病毒防範與解除

4. 防範USB病毒-Fortinet Antivirus

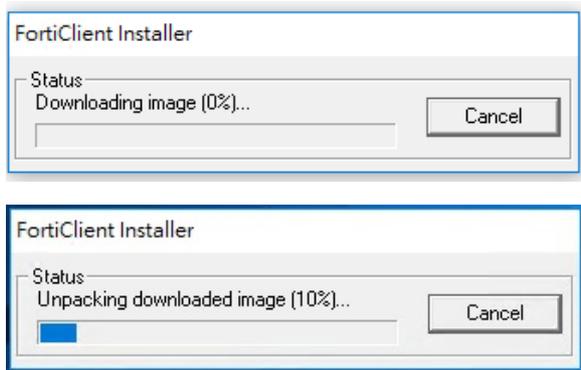
Forticlient Antivirus為著名資安公司 - Fortinet所出品的一套免費版的防毒軟體。在Windows Server上也可以安裝。

官方下載點

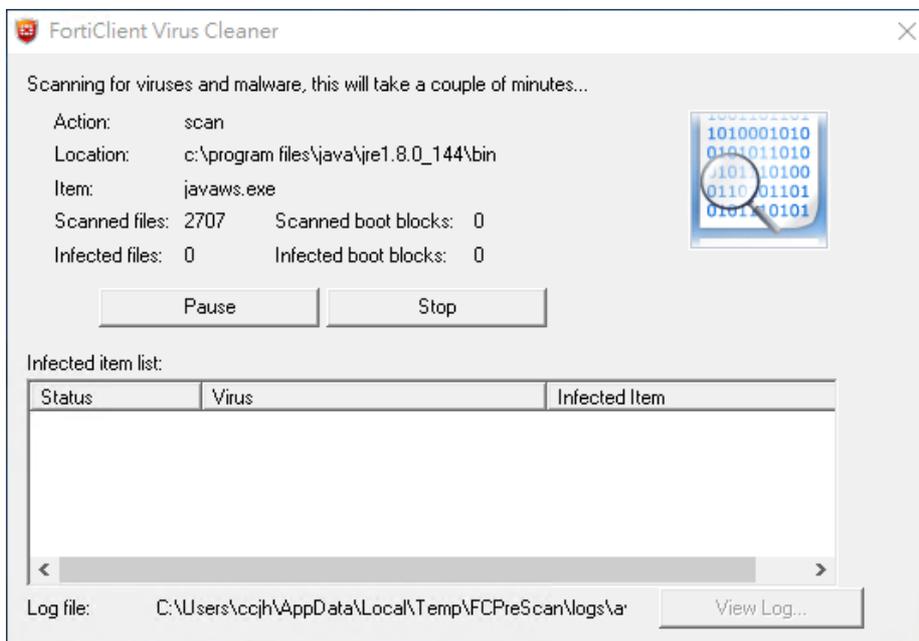
下載後，於FortiClientOnlineInstaller.exe點擊滑鼠左鍵進行安裝。出現如下畫面，請點擊「是」。



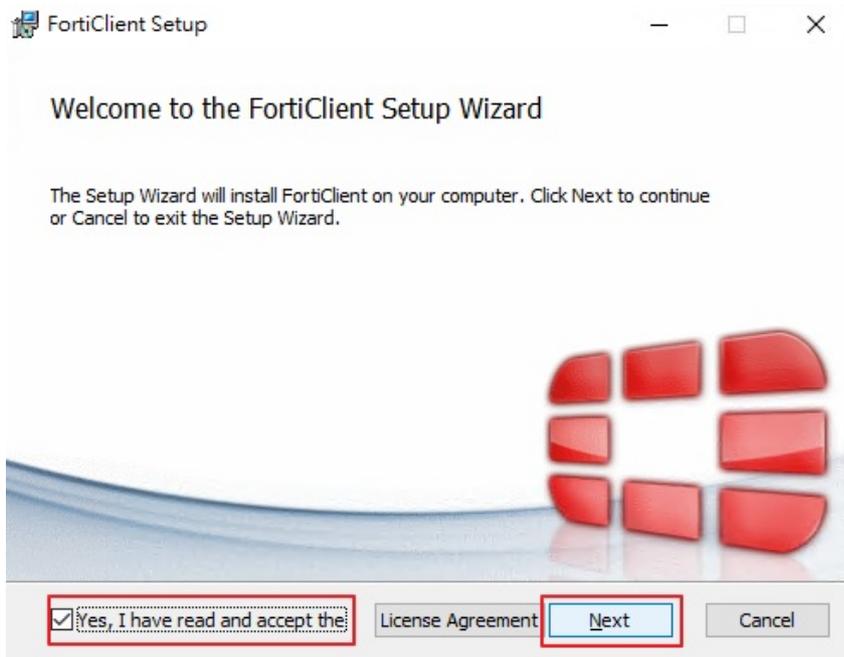
安裝時電腦需要連上網路，安裝程式會下載安裝檔，下載完畢後會進行解壓縮。如下圖。



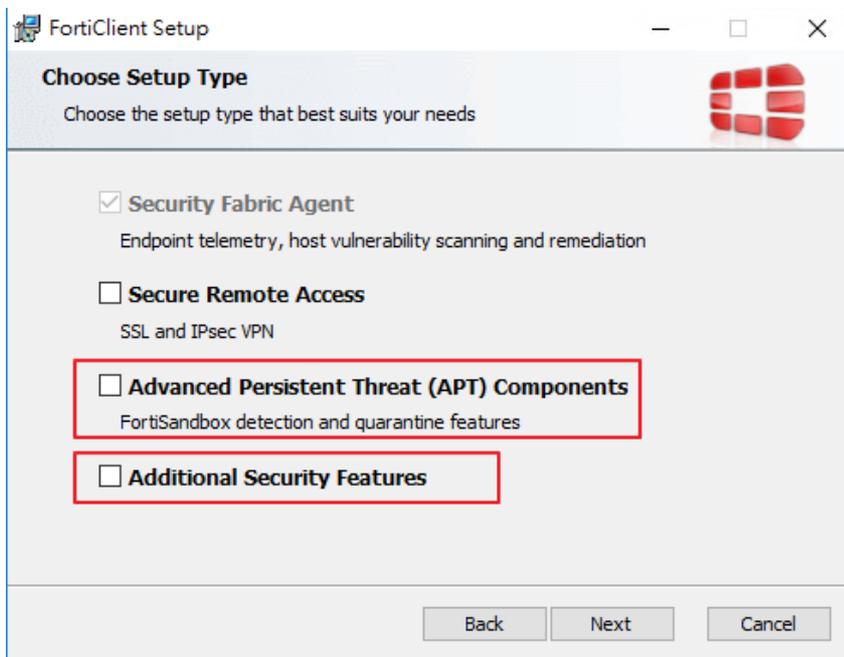
在進行安裝主程式前，會對Windows系統進行掃毒的動作。如下圖。



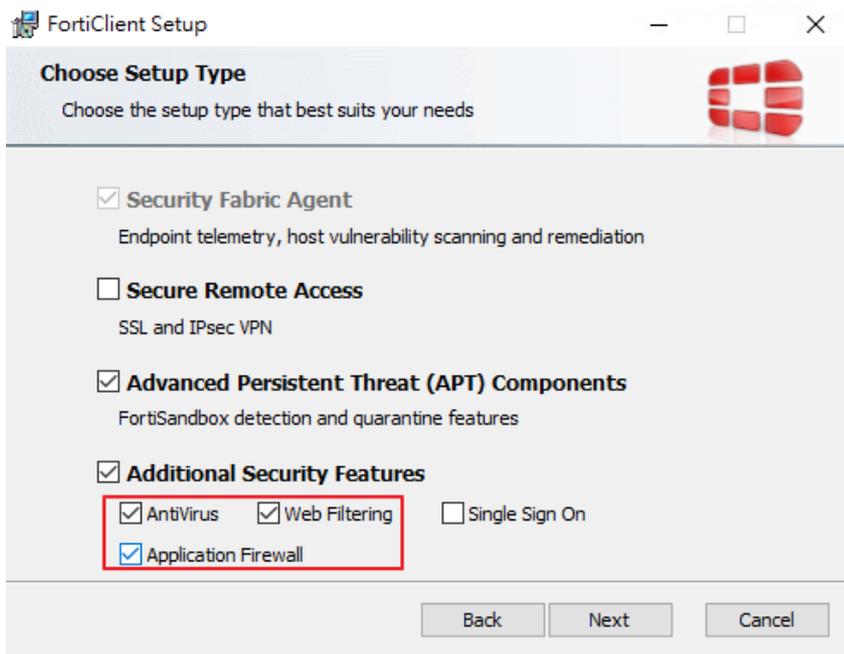
掃毒完畢，會出現如下畫面，請勾選如下圖所示紅色框線處，再點擊Next。



接著會出現如下畫面。

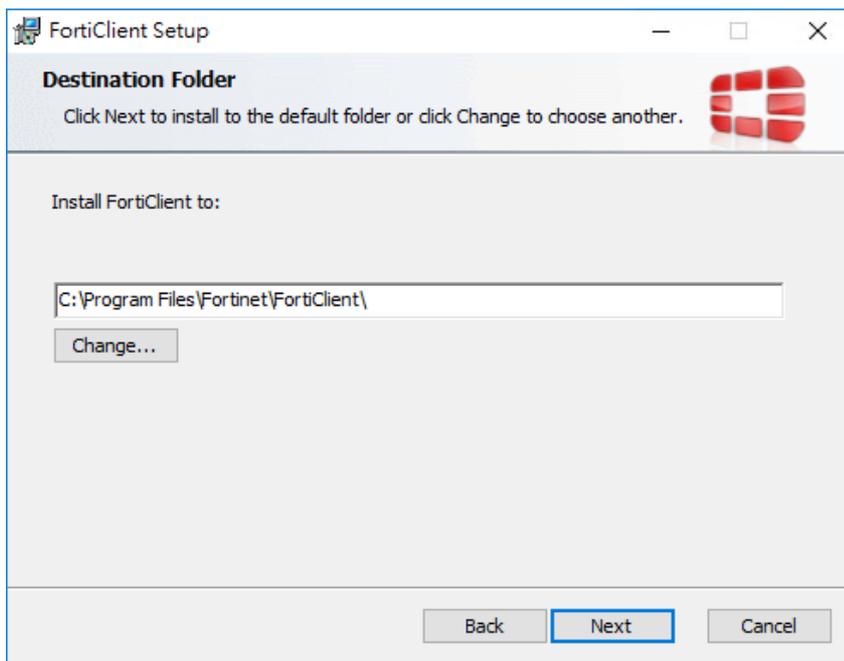


將圖示上APT與Additional Security Features兩處勾選起來，接著點擊Next。

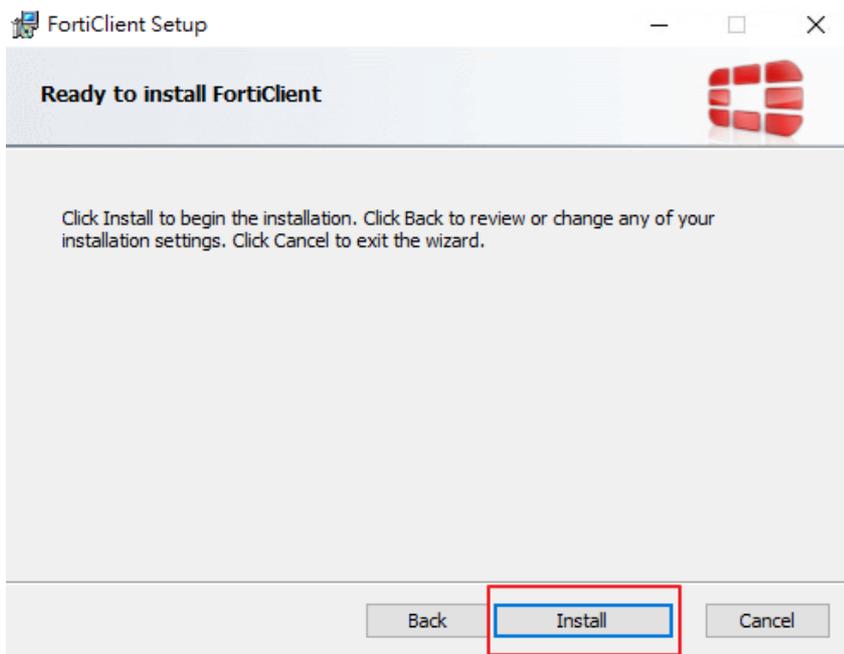


於Additional Security Features處，勾選Antivirus、Web Filtering與Application Firewall，以對Windows進一步的防護。

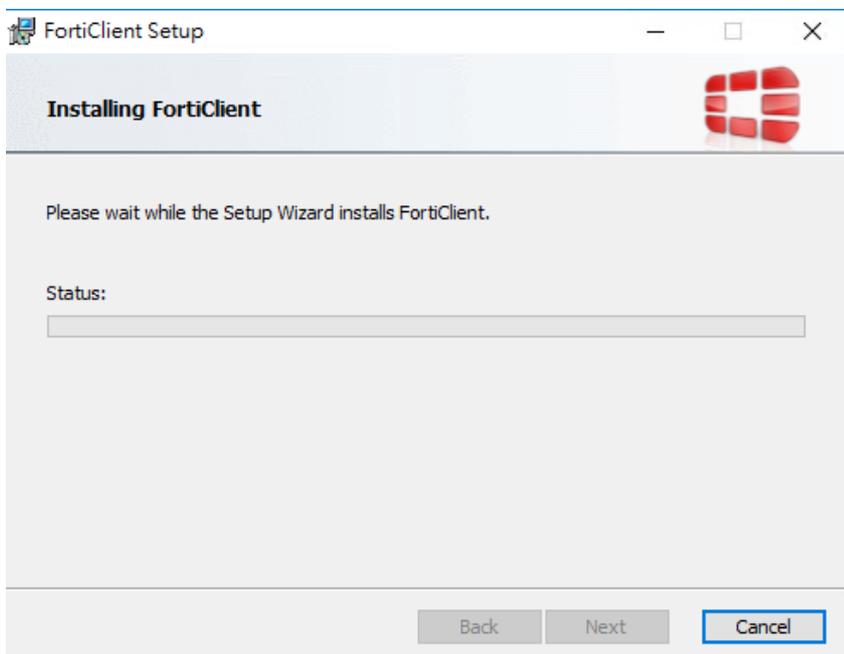
點擊Next後出現如下畫面，要求設定安裝路徑，維持預設值即可。



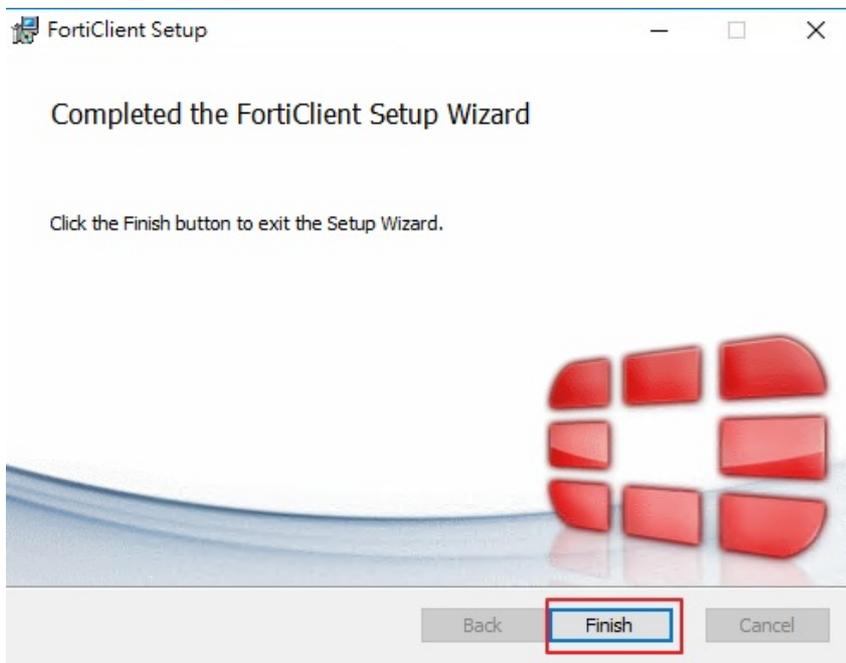
點擊Next後，於如下畫面時點擊Install。



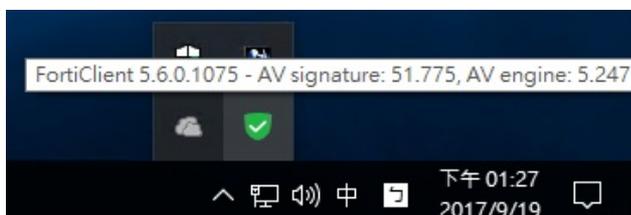
安裝過程如下圖。



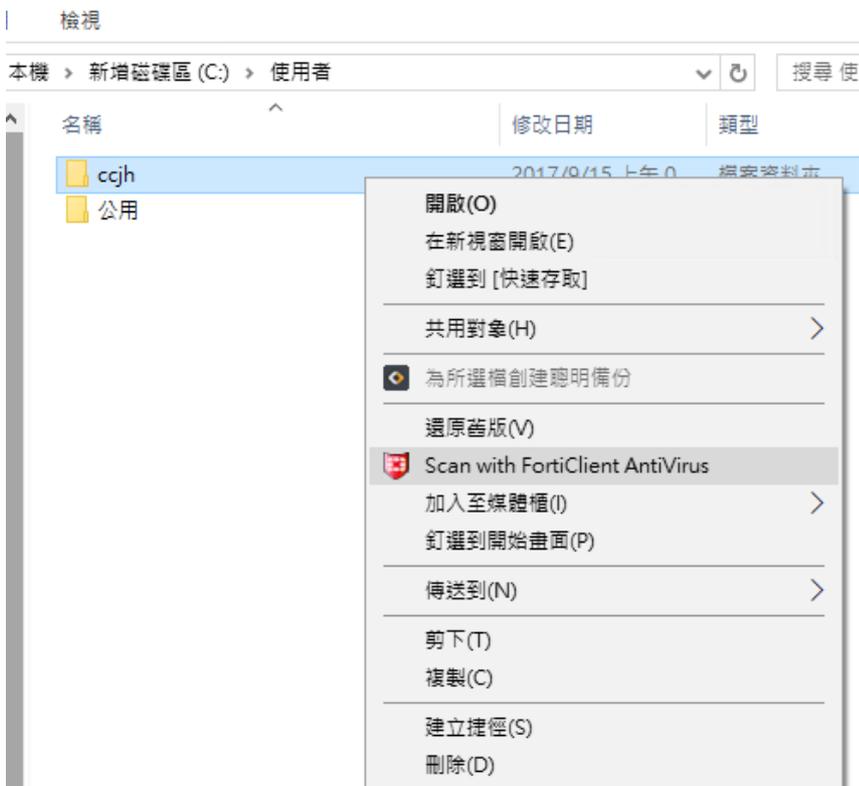
安裝完畢後點擊Finish，如下圖。



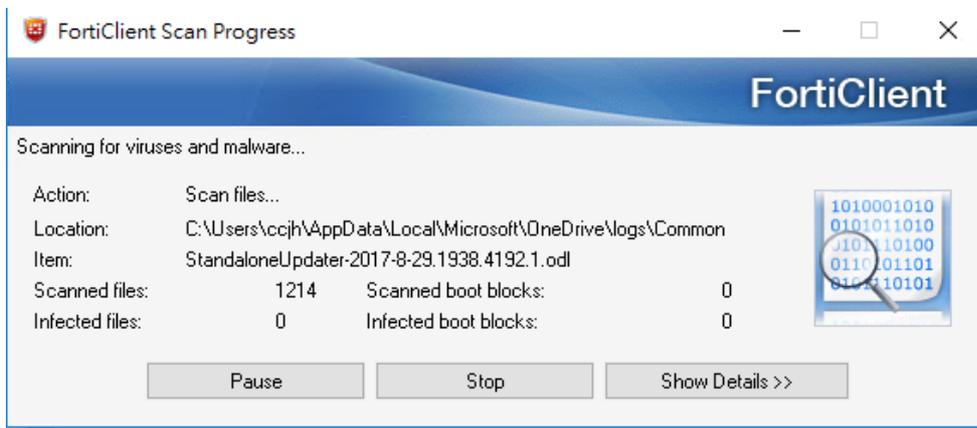
安裝完畢後，Windows右下角會出現如下圖示。



掃毒方式 - 選取要掃描的目錄或磁碟，點擊滑鼠右鍵，如下所示。



點擊Scan with FortiClient Antivirus即可進行掃毒。如下畫面。



經實際測試，FortiClient Antivirus的防護能力不差，而且它主要針對「行為」，如企圖寫入系統的惡意程式，或企圖呼叫Explorer執行隨身碟中惡意的Script，它可直接檔下不良意圖的動作，但掃毒能力平平，不算太優。綜合而論，比微軟內建的Defender好很多，加上是免費的，而且安裝完畢後，操作介面會變成繁體中文，相當親民好上手。特此推薦。

USB病毒防範與解除

5. 防範USB病毒-USB Disk Security

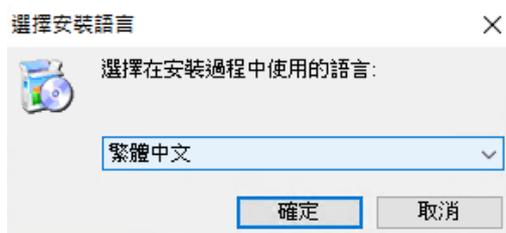
如果有一套程式或軟體，當隨身碟一插入電腦的USB時就能自動掃毒，將有問題的檔案移除，那一定可以省下日後一支支隨身碟掃毒的麻煩與風險，以下介紹zbsware這公司所出品的一套免費，專們主動掃除USB病毒的小程式。經王言俊老師實戰測試，發現可以解掉令人困擾的隨身碟病毒。這個小程式，不但是繁體中文，而且可在隨身碟病毒進入系統前就先解掉，它可以和其它的防毒軟體和平共存，更重要的，它是免費的。

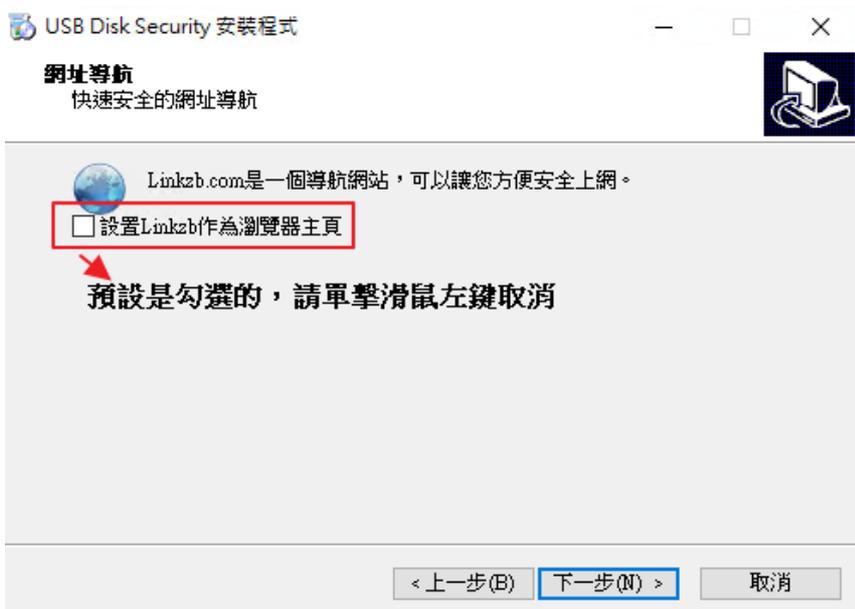
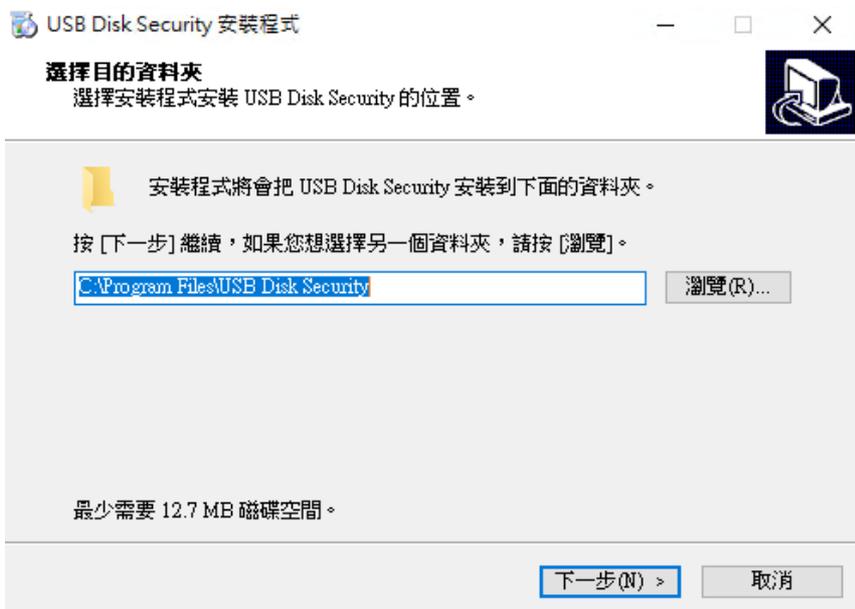
1. 下載網址：[Usb Disk Security](#)

2. 點擊USBGuard6.5.0.0.exe，如下圖，請單擊滑鼠左鍵，點擊「是」。

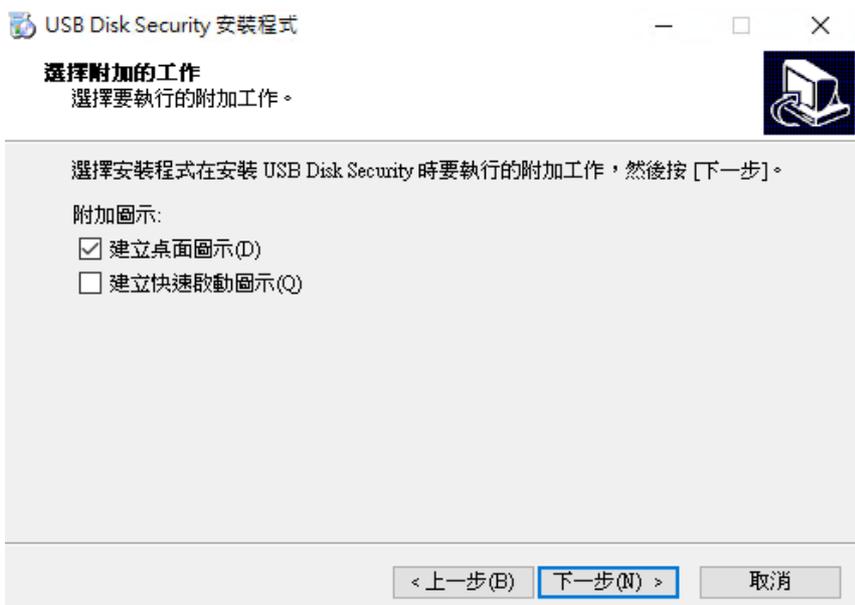


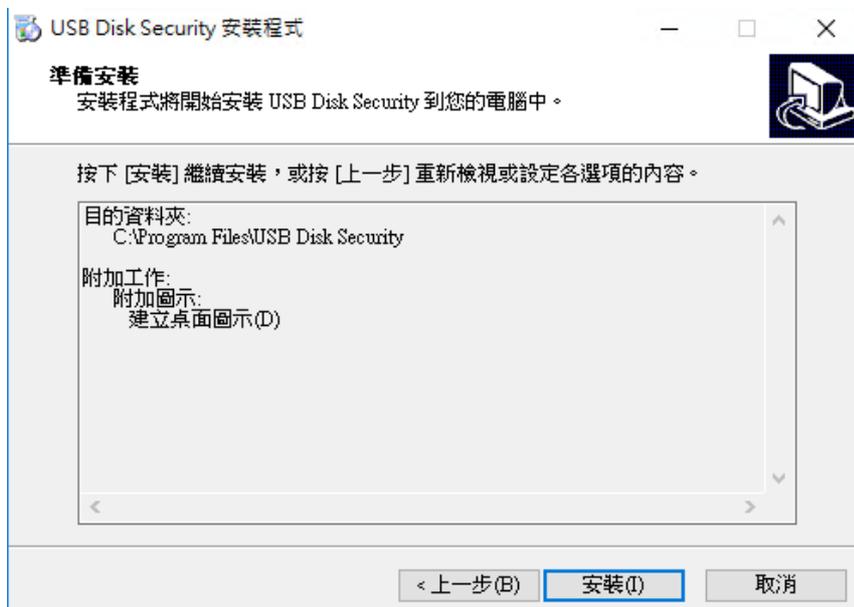
以下的畫面，直接單擊滑鼠左鍵，點擊「確定」或「下一步」或「安裝」以進行安裝。





至此畫面時，預設會將 Linkzb 作為瀏覽器的主頁，請單擊滑鼠左鍵取消。



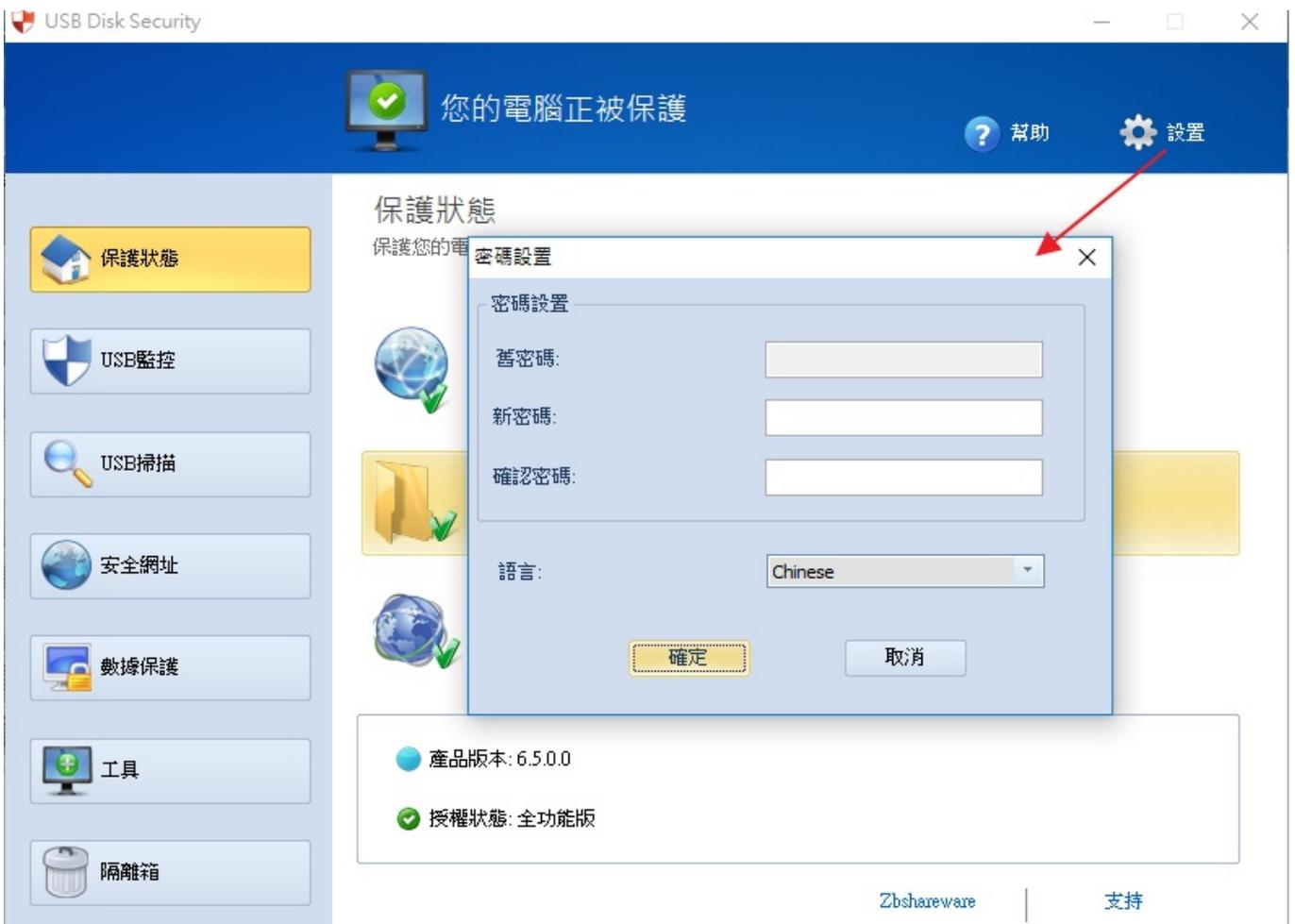


點擊「完成」即完成安裝，同時會啟動USB Disk Security執行程式以常駐於系統中，如下圖所示。

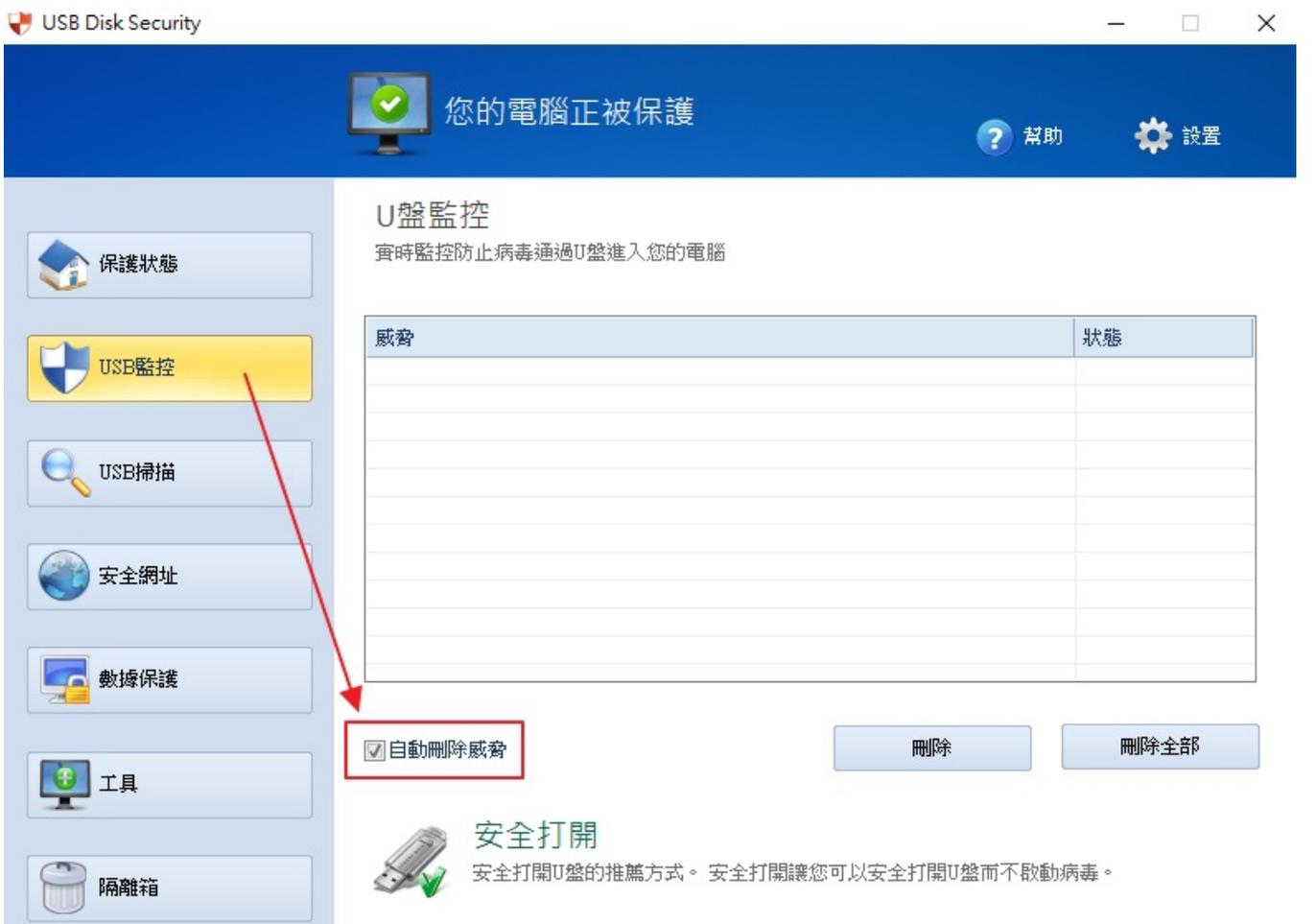


3. USB Disk Security的使用：

其實這個小程式不用什麼設定，可於「設置」處設定密碼，避免因公用電腦不小心被使用者關閉了。



USB監控：預設可自動將掃描到的隨身碟病毒掃掉。



USB掃描：可點擊如下方「USB免疫」，不過是否真的有效，不得而知。

您的電腦正被保護

? 幫助
 ⚙️ 設置

保護狀態

USB監控

USB掃描

安全網址

數據保護

工具

隔離箱

U盤掃描

掃描您的U盤以發現是否有威脅

威脅	狀態

掃描
停止
刪除
刪除所有

USB免疫

禁止PC和U盤的自動運行功能以防止病毒入侵電腦

安全網址：

您的電腦正被保護

? 幫助
 ⚙️ 設置

保護狀態

USB監控

USB掃描

安全網址

數據保護

工具

隔離箱

安全網址

可以在訪問任意網址前確定安全，並讓您方便快捷地訪問常用網址。

網址導航

安全快捷地訪問網址

網址掃描

輸入網址確定是否安全

VirusTotal

檢查網址

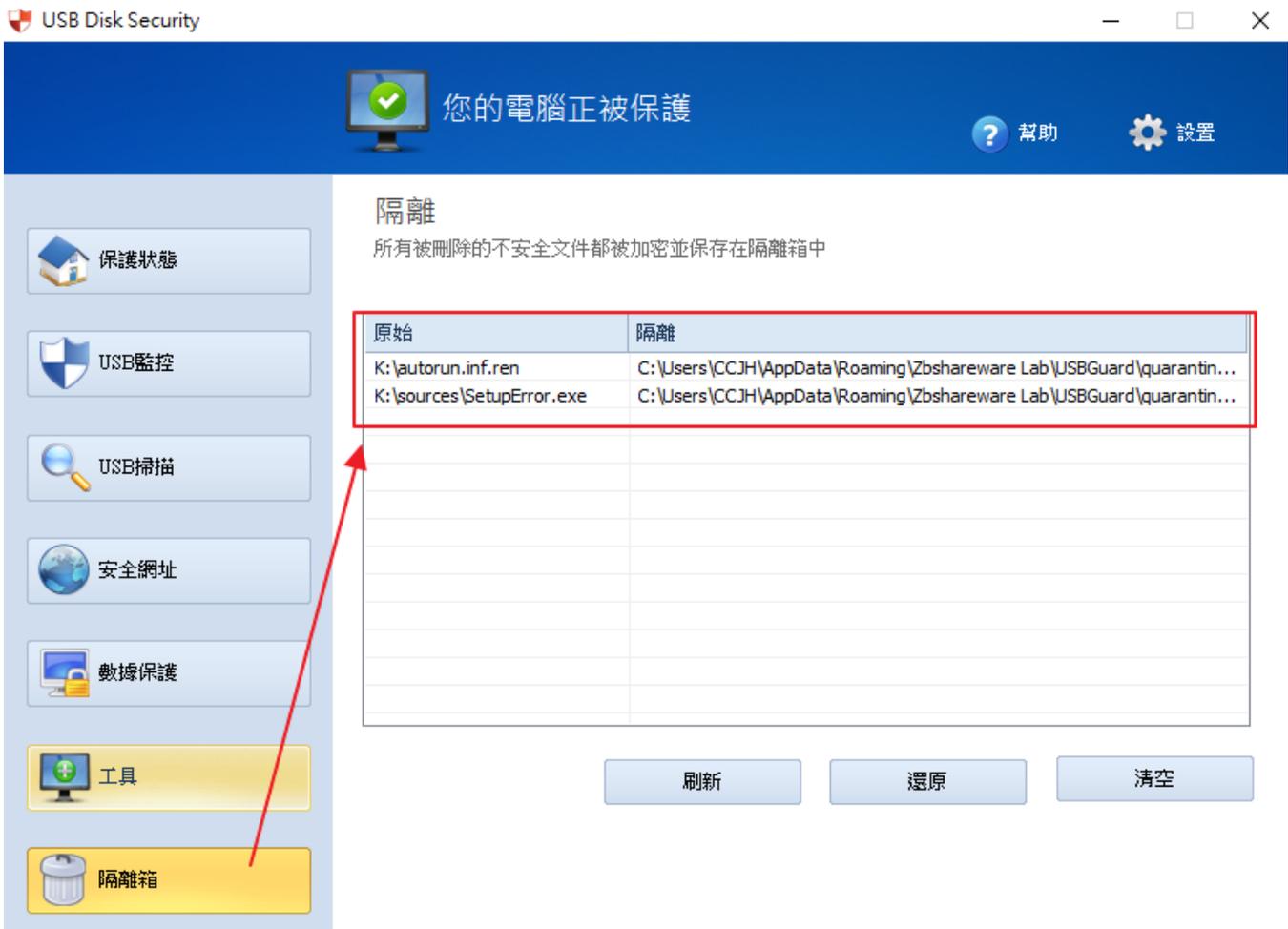
數據保護：可設定USB碟只供讀取或防止未授權的人使用。各位可自己試試看。

The screenshot shows the USB Disk Security application window. The title bar reads "USB Disk Security" and "您的電腦正被保護" (Your computer is protected). The interface is in Chinese. On the left is a navigation pane with buttons for "保護狀態" (Protection Status), "USB監控" (USB Monitoring), "USB掃描" (USB Scanning), "安全網址" (Safe Sites), "數據保護" (Data Protection), "工具" (Tools), and "隔離箱" (Quarantine). The "數據保護" button is highlighted in yellow. Two red arrows point from this button to the "U盤只讀控制" (USB Read-Only Control) and "U盤控制" (USB Control) sections in the main area. The main area has a blue header with a green checkmark icon and the text "您的電腦正被保護". Below the header, the "數據防洩漏" (Data Leakage Prevention) section is active, with the subtitle "防止您的數據被其他人竊取" (Prevent your data from being stolen by others). It contains two sub-sections: "U盤只讀控制" (USB Read-Only Control) with the description "防止未授權人拷貝您的數據到U盤" (Prevent unauthorized users from copying your data to USB) and a "鎖定" (Lock) button; and "U盤控制" (USB Control) with the description "防止未授權的人在您的電腦使用U盤" (Prevent unauthorized users from using USB on your computer) and a "鎖定" (Lock) button.

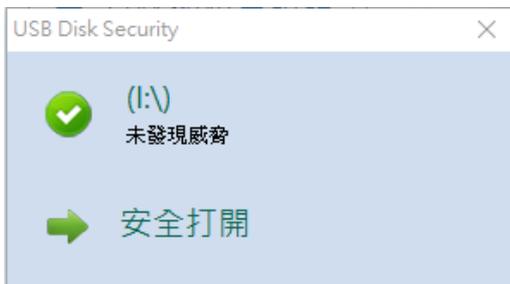
工具：可進行硬碟清理、系統修復與設定一開機就啟動的程式列表。

The screenshot shows the USB Disk Security application window. The title bar reads "USB Disk Security" and "您的電腦正被保護" (Your computer is protected). The interface is in Chinese. On the left is a navigation pane with buttons for "保護狀態" (Protection Status), "USB監控" (USB Monitoring), "USB掃描" (USB Scanning), "安全網址" (Safe Sites), "數據保護" (Data Protection), "工具" (Tools), and "隔離箱" (Quarantine). The "工具" button is highlighted in yellow. The main area has a blue header with a green checkmark icon and the text "您的電腦正被保護". Below the header, the "系統工具" (System Tools) section is active, with the subtitle "恢復惡意修改並可以刪除垃圾文件" (Restore malicious modifications and delete junk files). It contains three sub-sections: "硬盤清理" (Disk Cleanup) with the description "刪除垃圾文件並清理IE緩存文件夾" (Delete junk files and clean up IE cache folders) and a bell icon; "修復系統" (Repair System) with the description "你可以修復系統以還原被病毒做的惡意修改" (You can repair the system to restore malicious modifications made by viruses) and a wrench icon; and "自動運行列表" (Automatic Startup List) with the description "顯示隨 Windows 啟動的程式" (Show programs that start with Windows) and a gear icon.

隔離箱：可將不安全的檔案，如：autorun.inf或有疑慮的執行檔放入隔離箱中。



當USB隨身碟或外接式硬碟插入電腦的USB時，系統會自動掃毒，並於螢幕右下角彈出如此小視窗。



這樣各位就可以點擊安全打開，或逕行從檔案總管、我的電腦中開啟USB碟。

USB病毒防範與解除

6. 隨身碟內容變成捷徑的處理

如果隨身碟（含可攜式硬碟）已受病毒感染，檔案或資料夾會變成捷徑，如果點擊該捷徑，會將病毒寫入Windows系統，則該電腦就會受隨身碟病毒感染，最後感染每一支插入該電腦USB的隨身碟。

如果隨身碟內的病毒已被清除，但檔案或資料夾仍是捷徑，這樣子資料仍然無法被讀取，可循下列方式解決。

以Win10為例，於  輸入命令提示字元，並於其上單擊滑鼠右鍵，選擇以「系統管理員身份」執行，如下所示。



```
cmd 系統管理員: 命令提示字元
Microsoft Windows [版本 10.0.15063]
(c) 2017 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\WINDOWS\system32>
```

假設USB隨身碟的路徑是i，於提示字元輸入i，再按下Enter。

於i:\>，輸入 **attrib -s -r -h * /S /D** 將被隨身碟病毒隱藏的檔案與資料夾回復。

切記，資料回復後，將隨身碟中所有的捷徑刪除。