



第 061 期 中華民國 106 年 7 月 1 日

發行人：韓孟麒主任 總編輯：李慎芬組長 主編：簡國璋

服務與維修專線：2885

【服務公告】

1. 教育部社交工演練已經落幕 (簡國璋 撰稿)

教育部進行之社交工程演練，已於 6 月 30 日結束，感謝全校同仁的配合。電子計算機中心(以下簡稱本中心)希望同仁們，未來仍舊以謹慎的態度，來使用電子郵件；也就是：非確認安全之郵件，切勿輕易開啟。尤其近來勒索病毒猖獗，真的須要非常地小心，避免您的電腦檔案，遭受重大的損害。

2. 落實對外網站「提供下載的可編輯文件應支援 ODF 文書格式」之任務 (簡國璋 撰稿)

本中心針對教育部所推行之 ODF-CNS15251 標準，舉辦了三場教育訓練，經董瑞生老師的詳細講授後，同仁們應該大都對 ODF 有初步的認識，且能夠將 Word 之 docx 檔與 Open Document Format 之 odt 檔，進行基本的轉檔與內容修正。因此，本中心要求各教育行政單位，於 106 年 7 月 31 日前，完成對外網站(指不限定特定身分均可瀏覽的網站)「提供下載的可編輯文件應支援 ODF 文書格式」之任務，應不成問題。屆時，各單位也應完成自我檢查與彙報，秘書室與本中心，將於 106 年 8 月 31 日前，派員檢查各網站，希望也能 100%達標，以符合教育部的要求。

3. 學務處課外活動指導組於社團負責人大會中，大力宣導使用 ODF-CNS15251 標準 (簡國璋 撰稿)

學務處課外活動指導組，於本學期之期末社團負責人會議暨社員大會中，宣導教育部所推動之 ODF-CNS15251 標準，並且以「有獎問答」之方式進行，寄望藉由社團之力量，能將 ODF 的使用推廣更順利。是日，黃明雪組長，與同學互動活絡，同學們在組長的宣導中，都能深刻體會政府的用心，因為多一項文書軟體工具使用的學習，將來在使用上，會給大家帶來更方便的選擇；活動之進行，如下圖所示。



【技術分享】

TCP 445 通訊埠的關閉方式 (簡國璋 撰稿)

近日，新的一波變種勒索病毒 Petya 正四處肆虐中，相較於五月間造成全球恐慌的 WannaCry 勒索病毒，Petya 的散播管道主要有兩種：

1. 同樣是利用微軟的安全弱點：MS17-0106 Eternalblue 來針對使用者進行攻擊，不同於 WannaCry 的地方，Petya 入侵電腦後，會修改電腦硬碟中的主要開機磁區(Master Boot Record, MBR)的設定，而且建立電腦排程於一小時內重新開機，開機時會於電腦螢幕跳出勒索訊息視窗，讓使用者無法進行任何操作。
2. 駭客會利用微軟官方的 PsExec 遠端執行工具，以「進階持續性滲透攻擊」(Advanced Persistent Threat, APT)的手法進行入侵，一旦入侵成功，將可以潛伏於內部網路中並感染控制內部重要伺服器，進一步發動勒索病毒攻擊。

對此，本中心建議本校同仁應採取以下防範措施來避免感染：

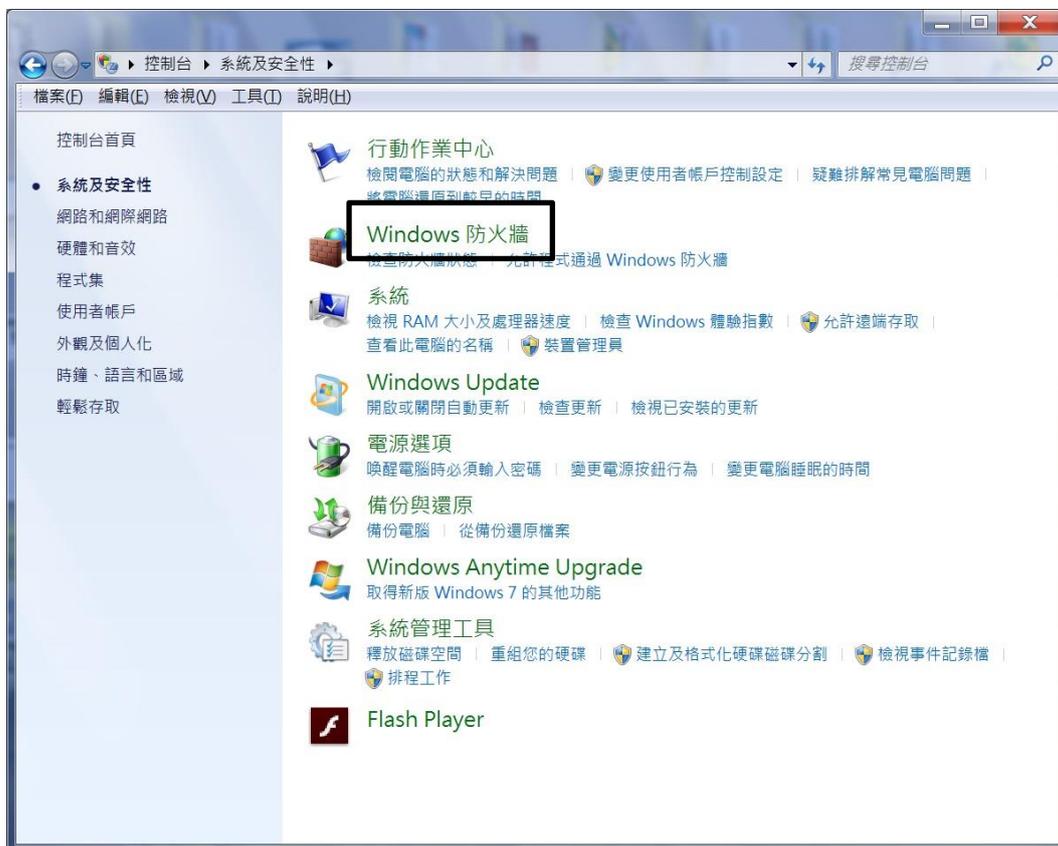
1. 套用安全性弱點 MS17-010 EternalBlue (<https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx>)修補更新。
2. 停用 TCP 連接埠 445。

停用 TCP 連接埠 445 的步驟如下：

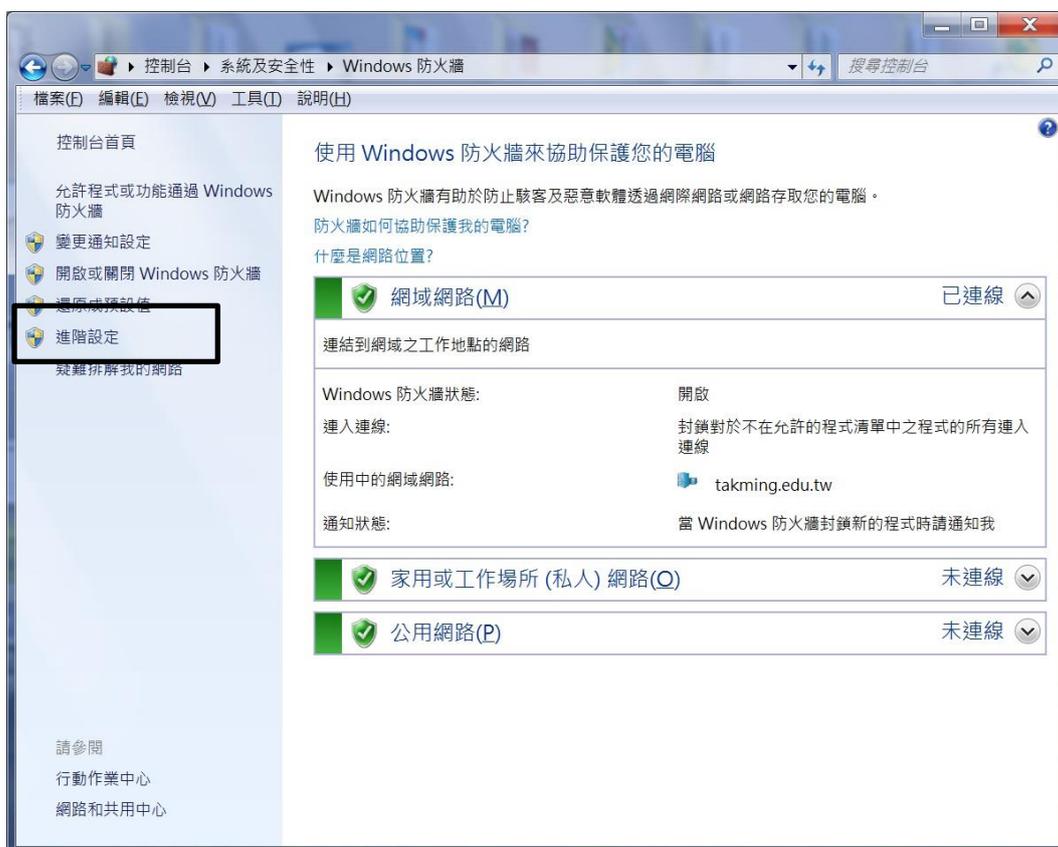
步驟 1、開啟「控制台」，選擇「系統及安全性」，如下圖所示。



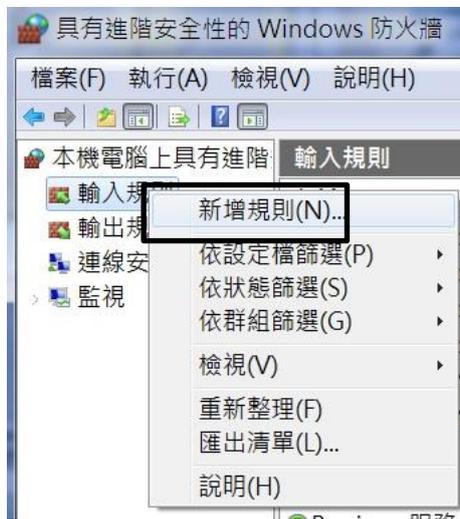
步驟 2、選擇「Windows 防火牆」，如下圖所示。



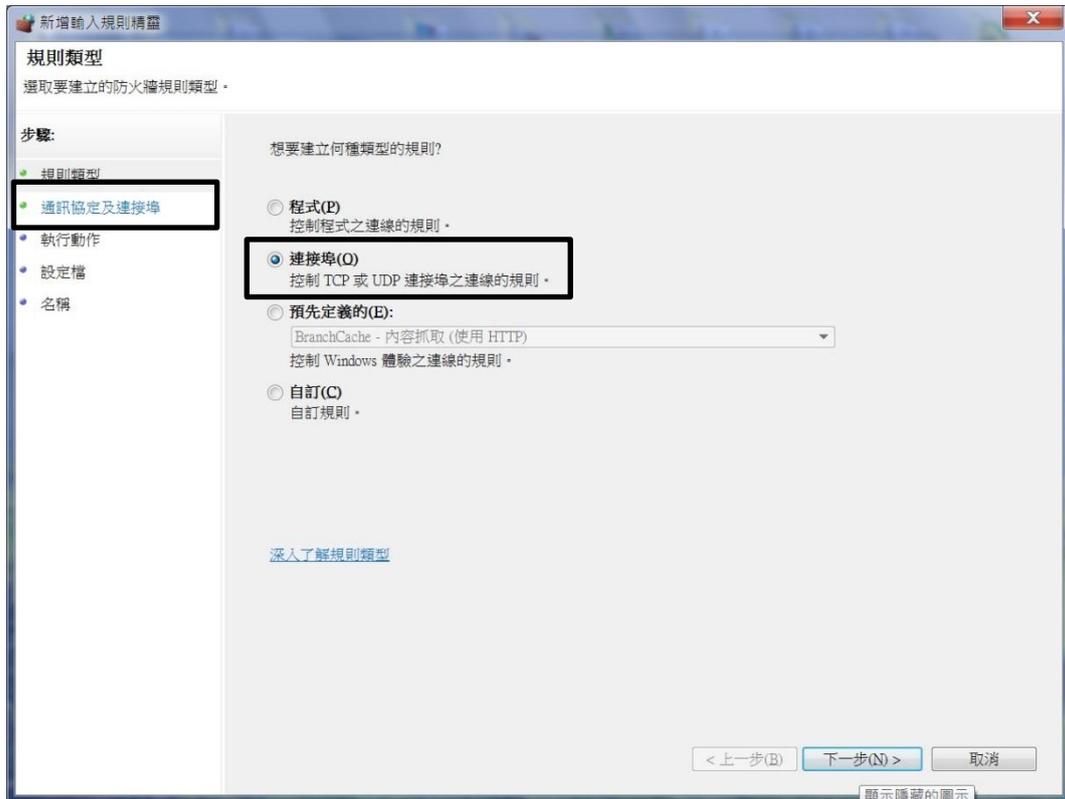
步驟 3、選擇「進階設定」，如下圖所示。



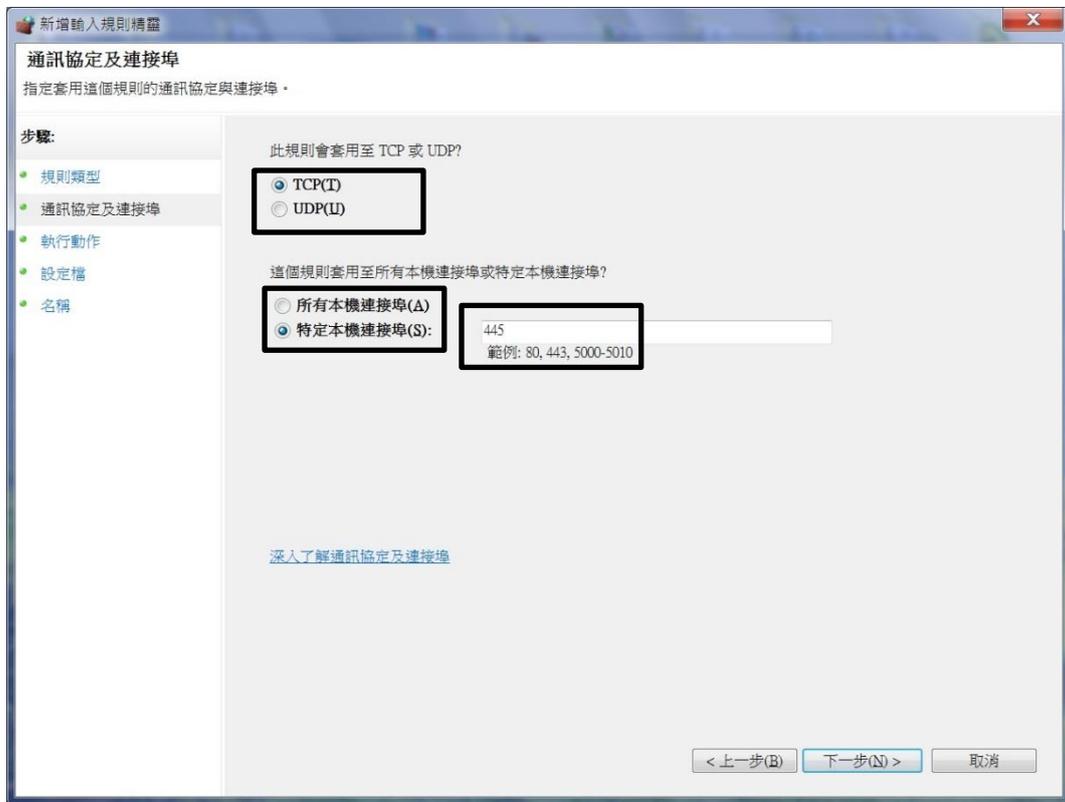
步驟 4、選擇「輸入規則」、「新增規則(N)...」，如下圖所示。



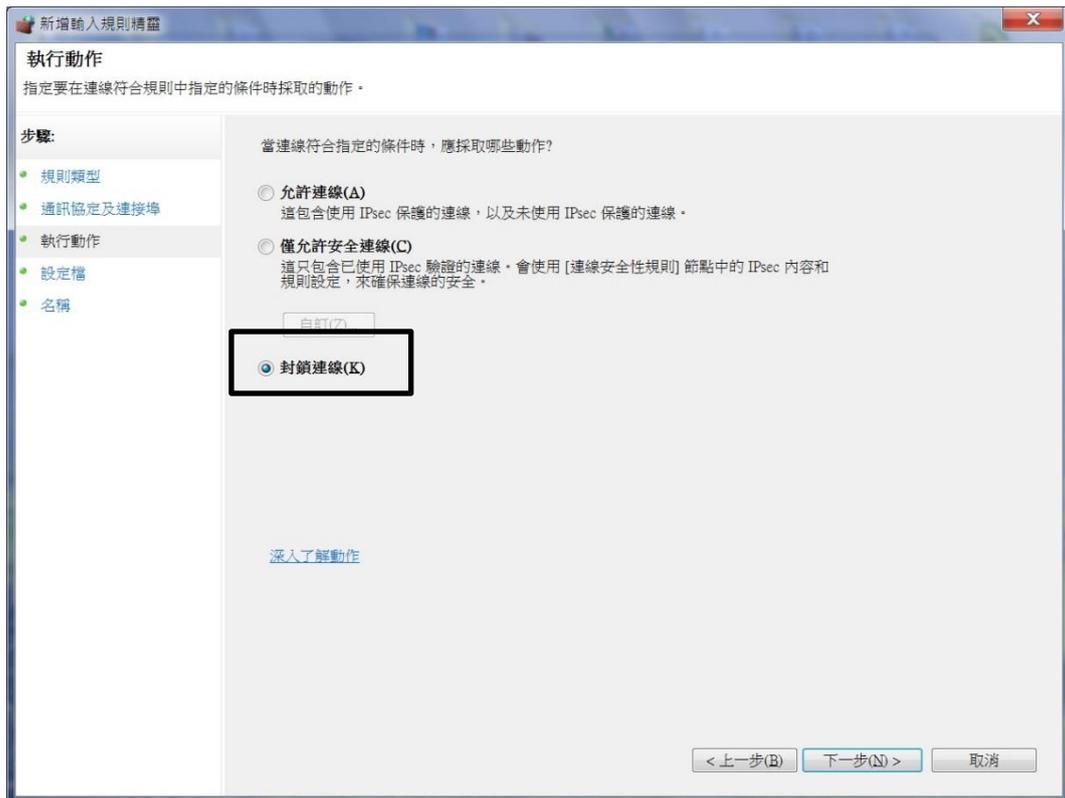
步驟 5、選擇「連接埠」後，點選「通訊協定及連接埠」，如下圖所示。



步驟 6、點選「TCP」和「特定本機連接埠」，輸入 445，按下「下一步」，如下圖所示。



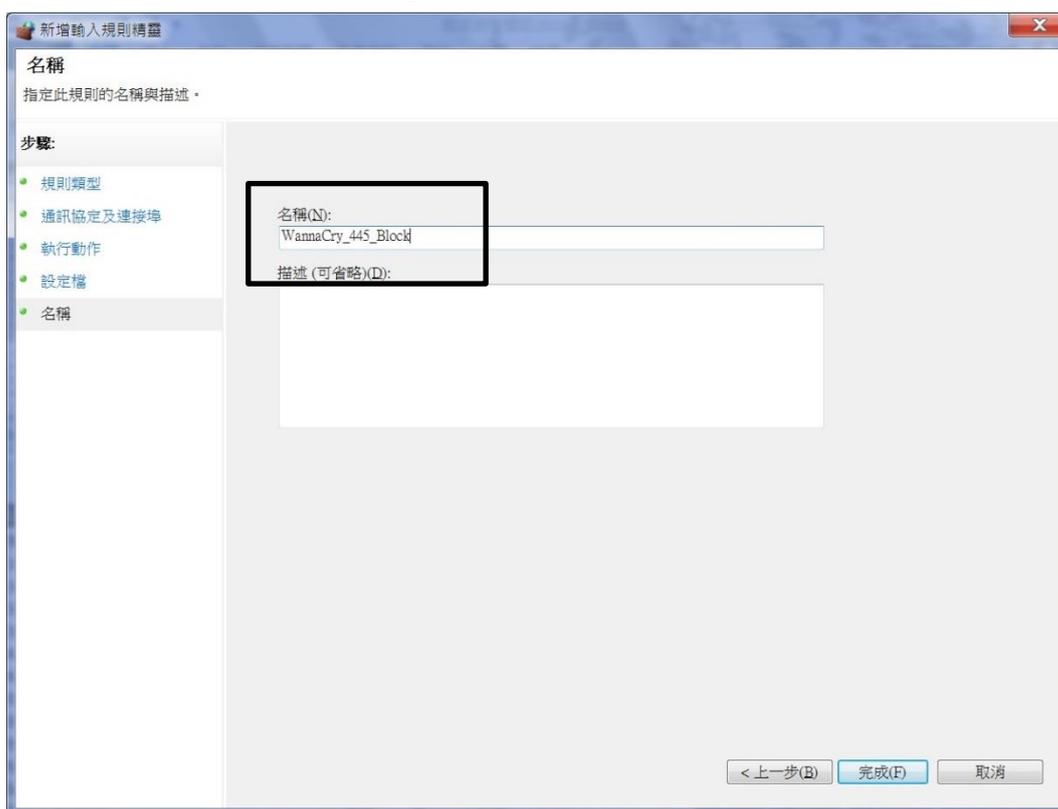
步驟 7、點選「封鎖連線」，按下「下一步」，如下圖所示。



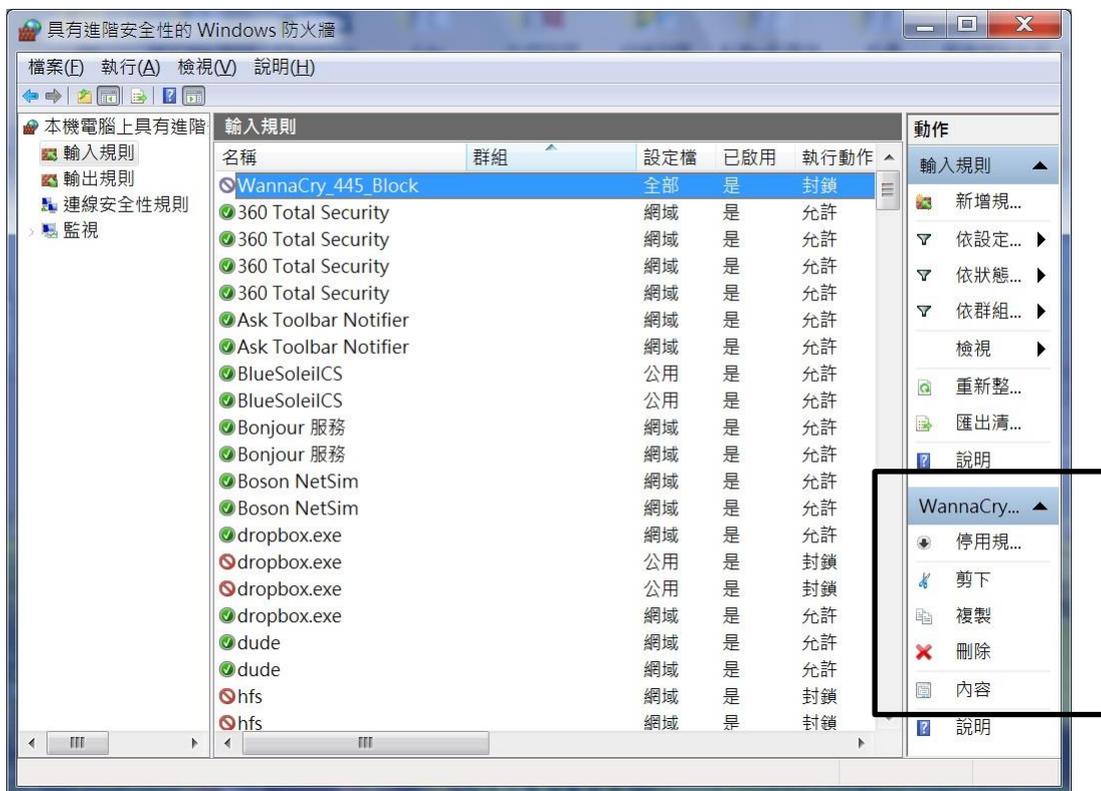
步驟 8、將「網域」、「私人」與「公用」都勾選，按下「下一步」，如下圖所示。



步驟 9、輸入足以辨識的名稱，按下「完成」，如下圖所示。



步驟 10、可以看到新增了一條規則，若是不再需要，隨時可將其刪除，如下圖所示。



【一般宣導】

1. 敬請尊重智慧財產權，有關校園網路使用規範、智慧財產權之宣導及注意事項，請多予關注，相關網址如下：<http://www.takming.edu.tw/cc/>。檢舉信箱：abuse@takming.edu.tw 或 netcc@takming.edu.tw。
2. 請勿安裝來路不明之非法軟體，以免觸法。
3. 查閱相關電腦技術資料，網址：<http://www.takming.edu.tw/cc/resources/document.htm>
4. ODF 園地：<http://www.takming.edu.tw/cc/resources/odf.htm>