電子資料安全防護介紹

資訊中心楊士毅
99.04.14

資料來源:
國家資通安全會報技術服務中心
教育部校園資訊安全服務網

資料數位化

- 修改、複製、散佈--彈指間
- 資料量龐大

電子資料

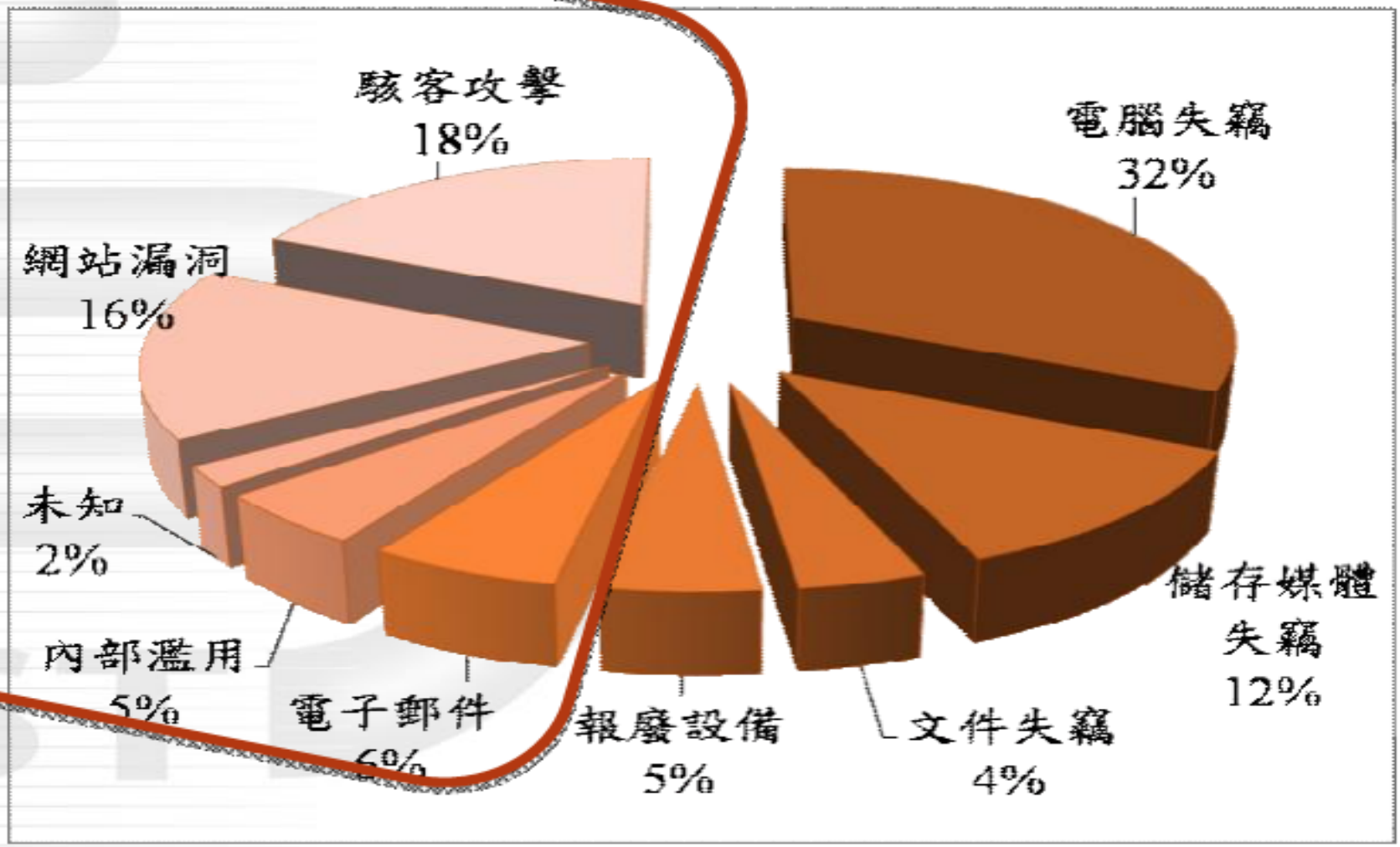
- 價值
- 威脅
- 風險
- 保護措施

資訊價值

- 公務機敏資料
- 個人隱私資料
- 智慧財產
- 無價之寶

威脅

- 資料遺失統計



資料來源：attrition.org

資料外洩風險

臺視全球資訊網 www.ttv.com.tw TTV 台視新聞

台視首頁 新聞首頁 台視財經 一週氣象 RSS

王宇婕、段旭明、第二回、省錢大作戰、蘇珊娜、桃

財經速報：清算結束營業或脫手出售？通用汽車雙管齊下

政治 財經 社會 醫藥 消費 娛樂 國際 綜合 文化 體育 影音

網售東森8千個資 每筆五毛　資料外洩 東森購物:交警處理　會員頻傳遭詐騙 藝人也受害

2009/06/11

推薦 列印 轉寄 討論

快速瀏覽　更多..

東森購物台又發生了客戶個人資料外洩事件，八千筆的個人資料在網路上外洩，包括客戶姓名、信用卡號，身份證字號通通都有，每筆在二手市場網站上只賣0.5元，公然販售客戶的信用卡資料這實在是茲事體大，東森購物強調，目前已經報案，請警方協助調查。

拿出報案單，東森購物現在又傳出有八千筆的個人資料在網路上通通曝光。

面對資料外洩風險

- 避免–不做資料交換
- 降低–採取保護措施
- 轉移–委外簽約保險
- 接受–善後

如果是您，會如何處理？

- 今天長官要出差至外地，需要李小龍儘速提供業務部分相關機敏資料。
  - USB
  - NB
- 今天李小龍出差到外地，北部長官一小時後要參加會議，急需李小龍業務部分相關機敏資料。
  - 驅車速回
  - 告訴同事自己電腦帳密，請同事轉交
  - 找網咖上網，把資料寄給長官

如果是您，會如何處理？

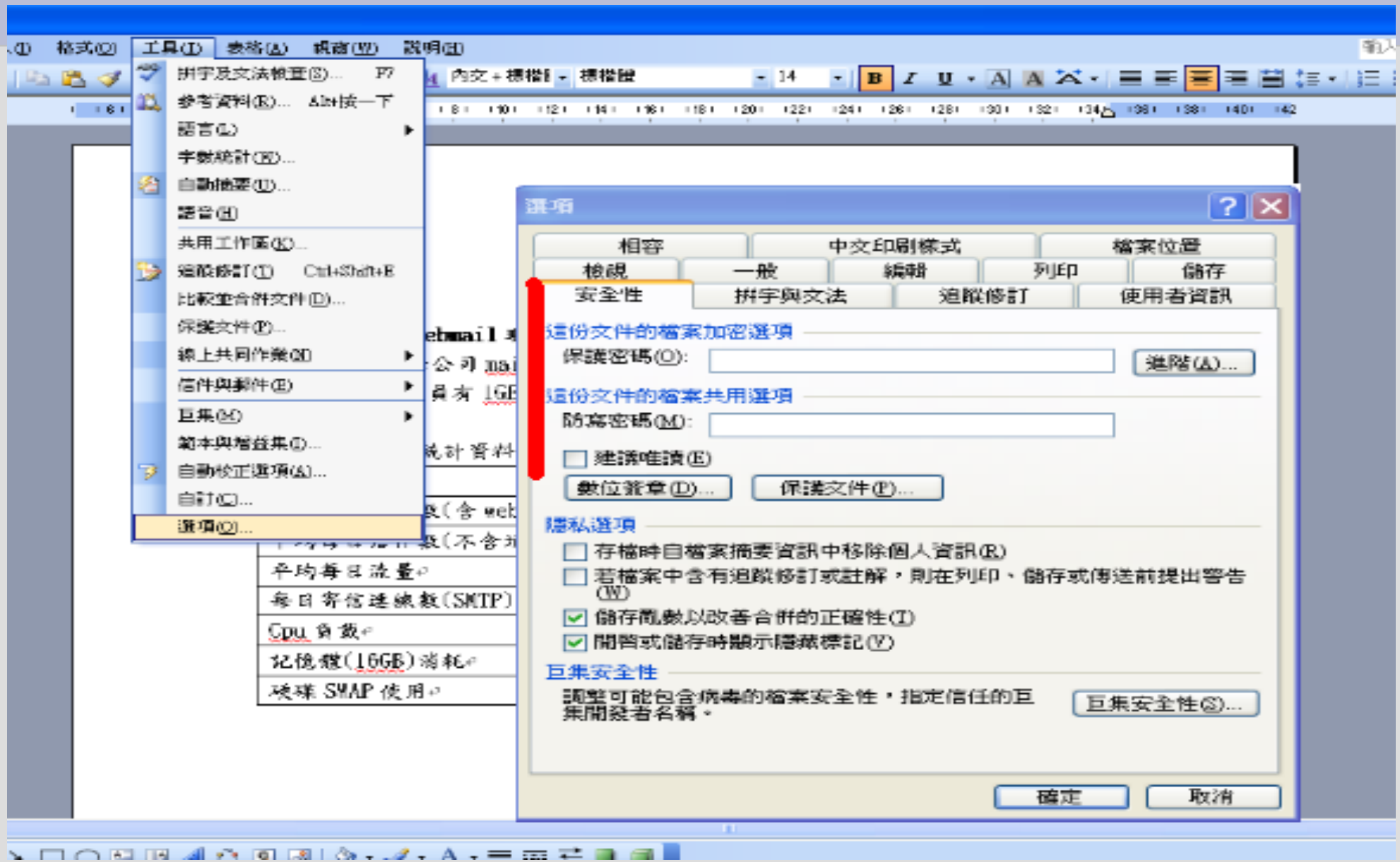
- 接到電話對方自稱教育部，請您傳送受輔導學生名冊。
  - 確認？
  - 加密？
  - 傳送

個人資料防護工具

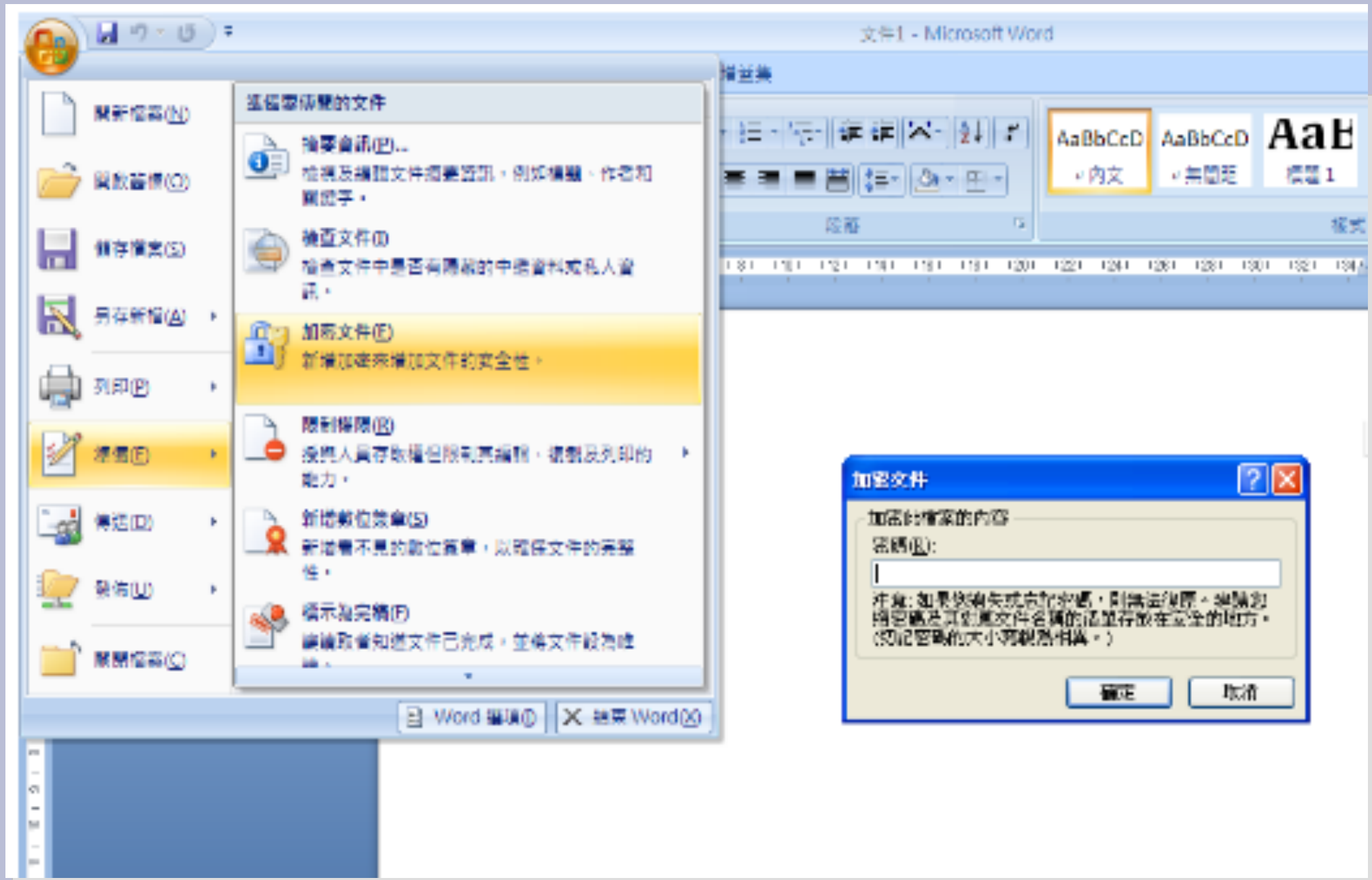
檔案加密管理–增加讀取的困難

- 文書編輯器加密–MSoffice、Openoffice、Pdf
  - 單一檔案
- 壓縮加密–7–zip–數個檔案或目錄
- 磁區加密–TrueCrypt–掛載磁碟
- 硬體晶片加密
- 檔案內容編碼–單一檔案
- 傳輸加密–SSL
- PKI金鑰簽章加密–自然人憑證
- 密碼管理–keepass

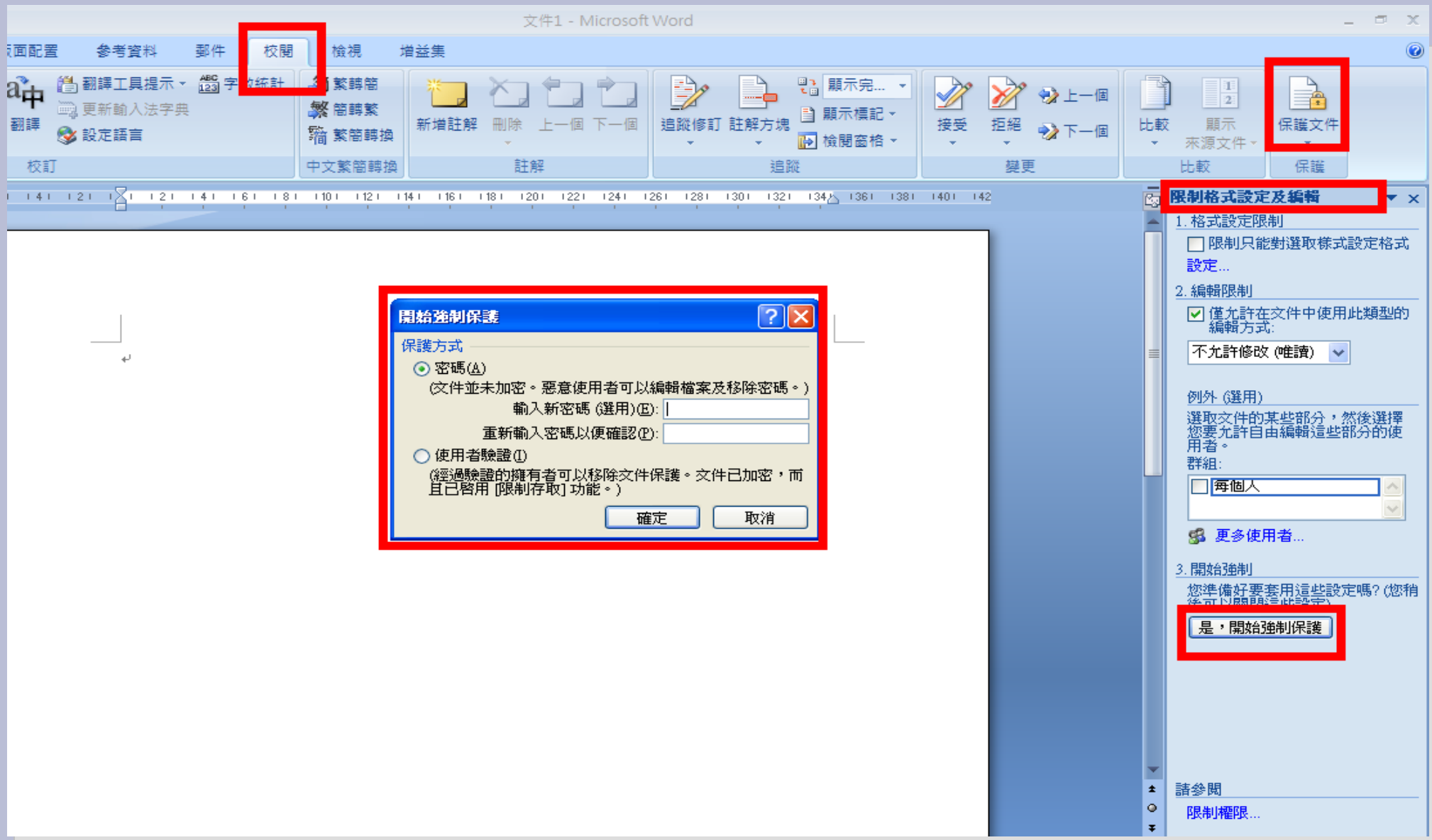
文書編輯器加密-word2003



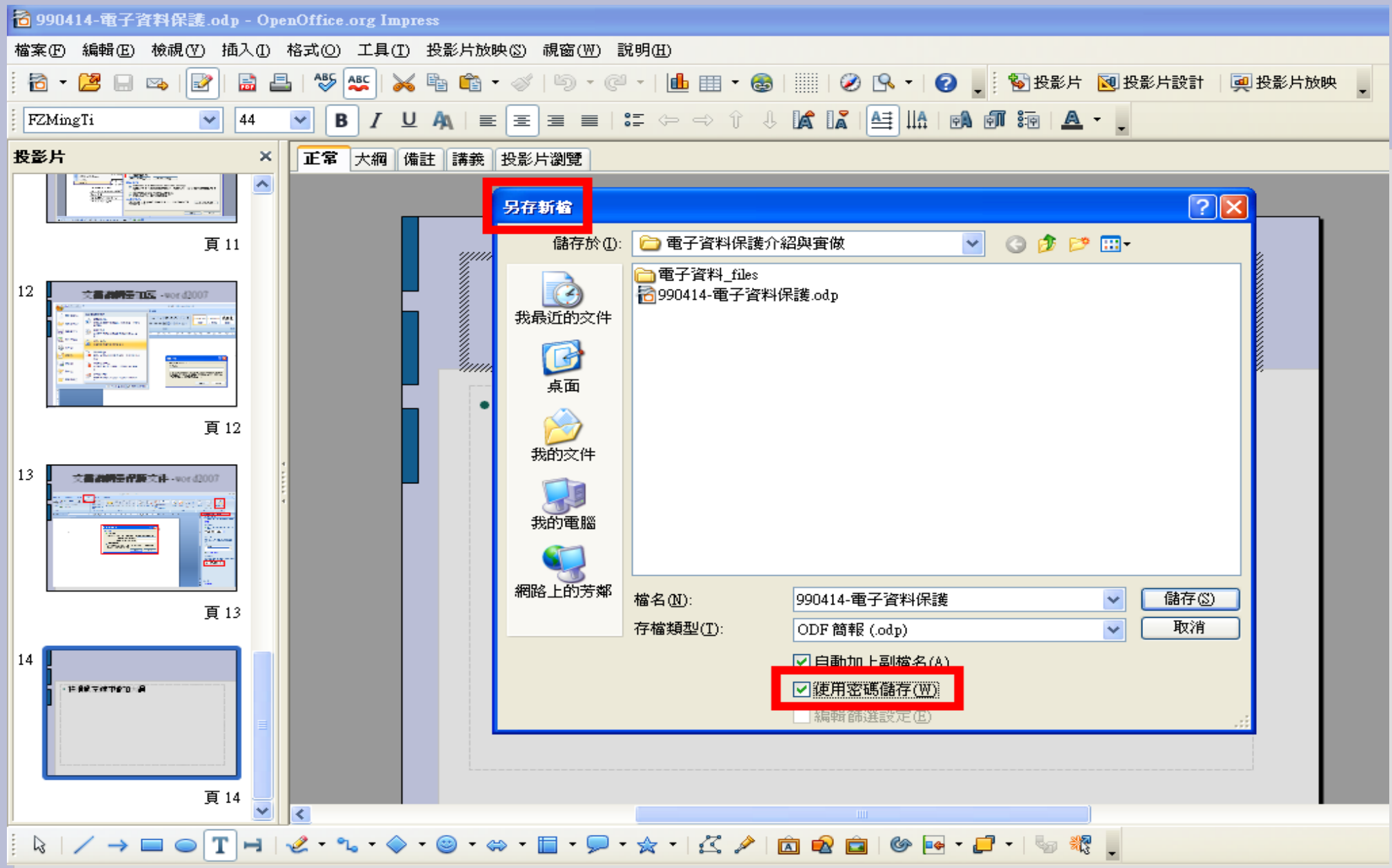
文書編輯器加密–word2007



文書編輯器保護文件-word2007

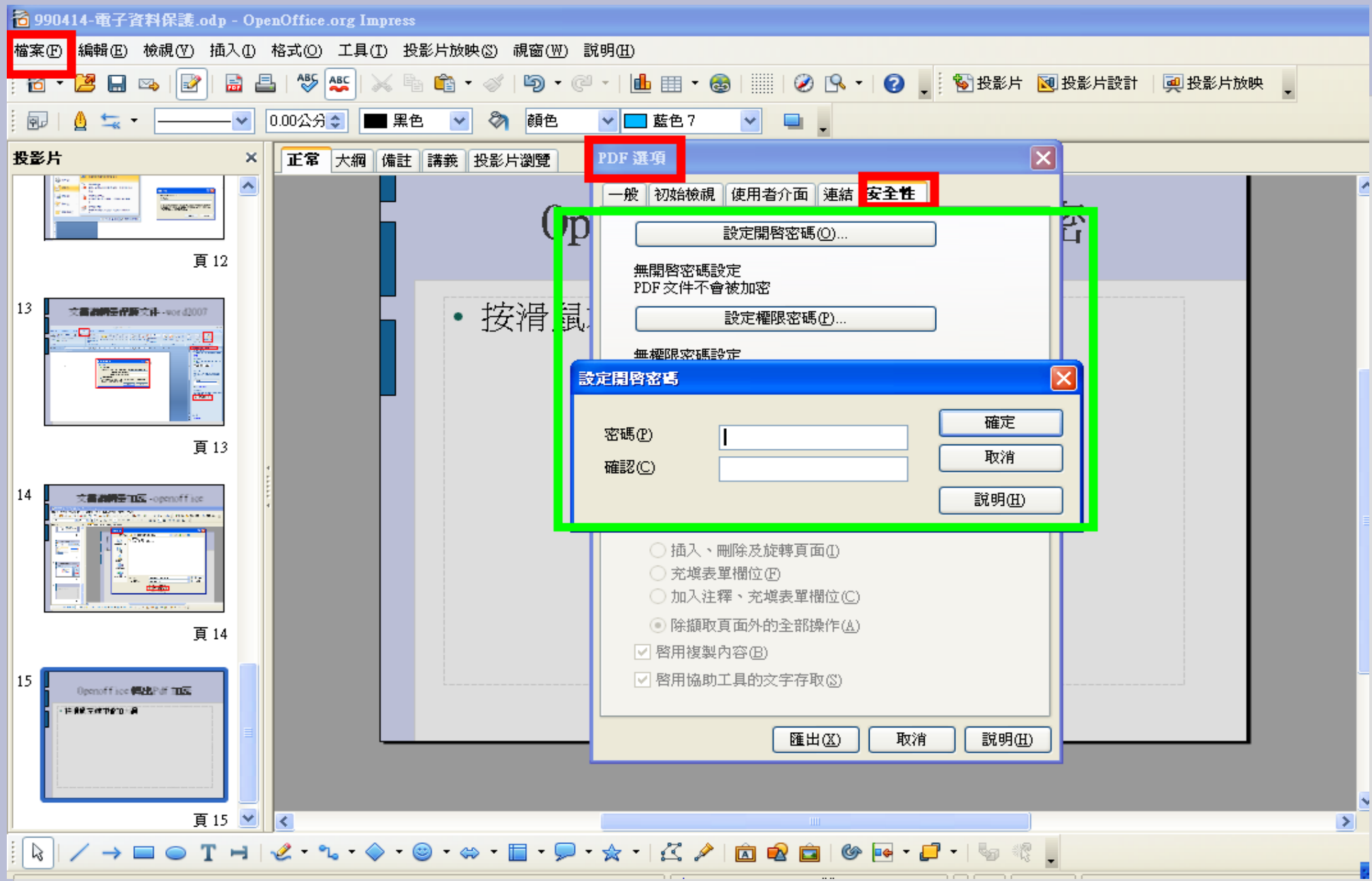


文書編輯器加密-Openoffice

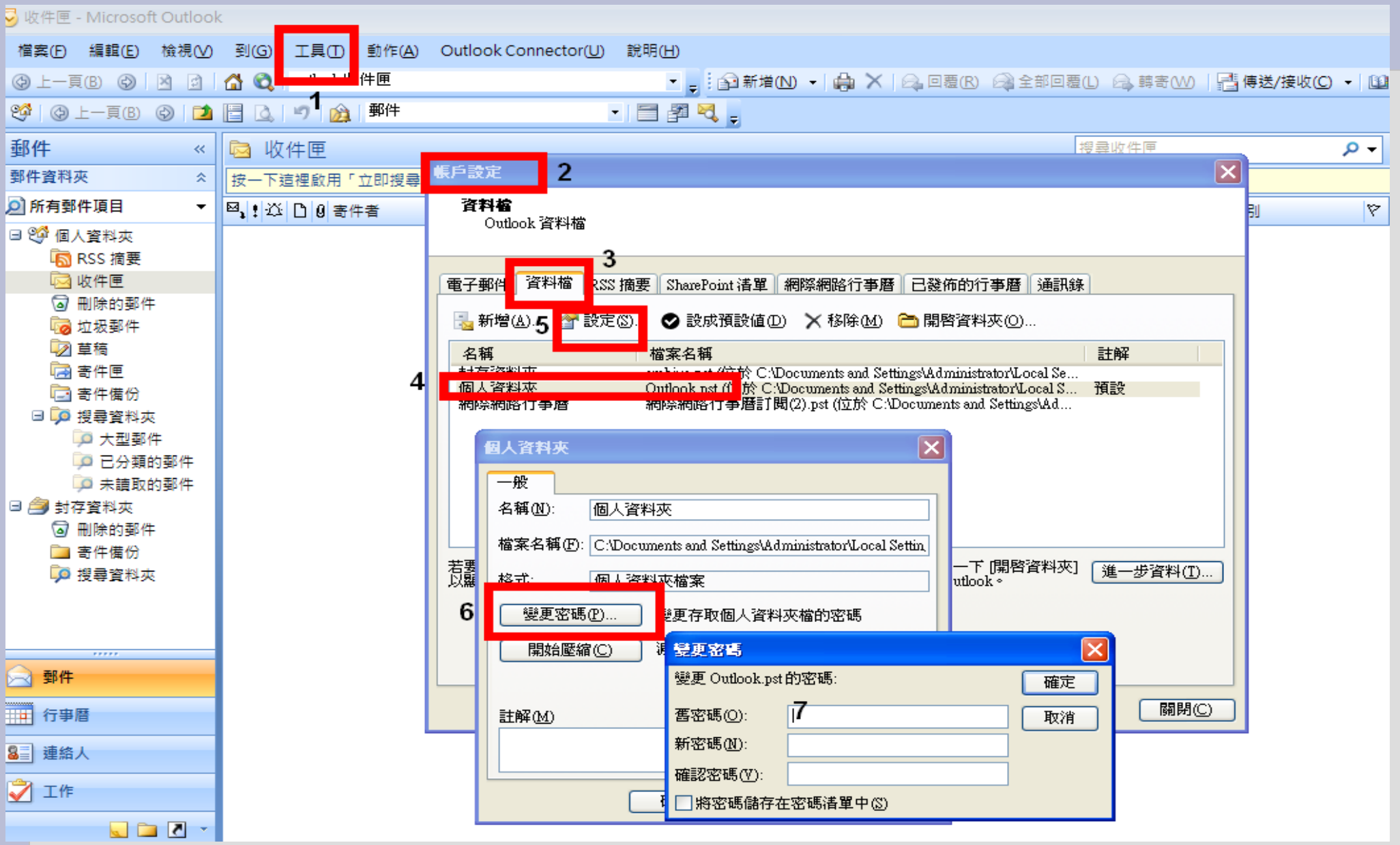


http://zh.openoffice.org/new/zh_tw/downloads.html

Openoffice轉出Pdf加密

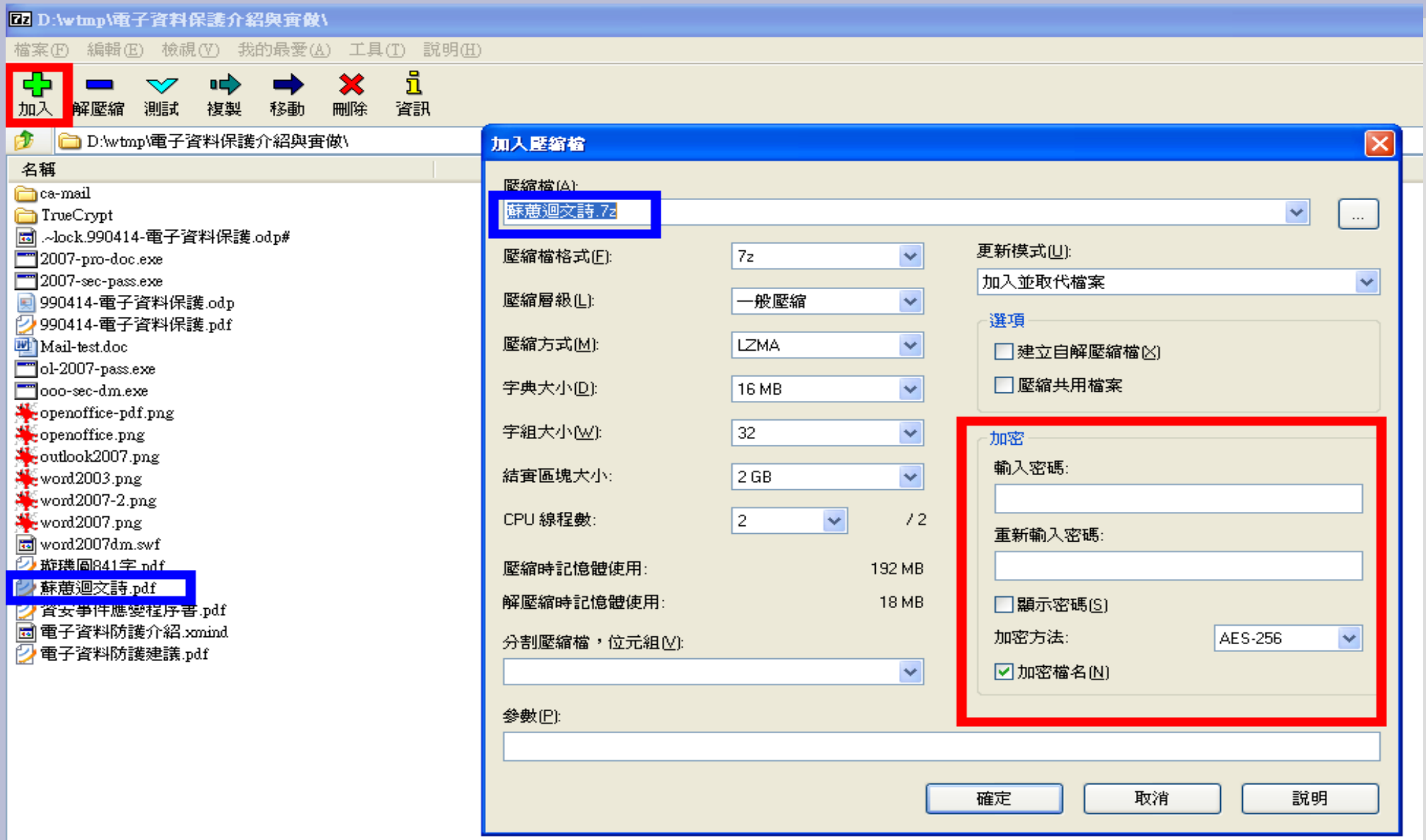


Outlook2007帳戶檔案加密



7-ZIP壓縮加密

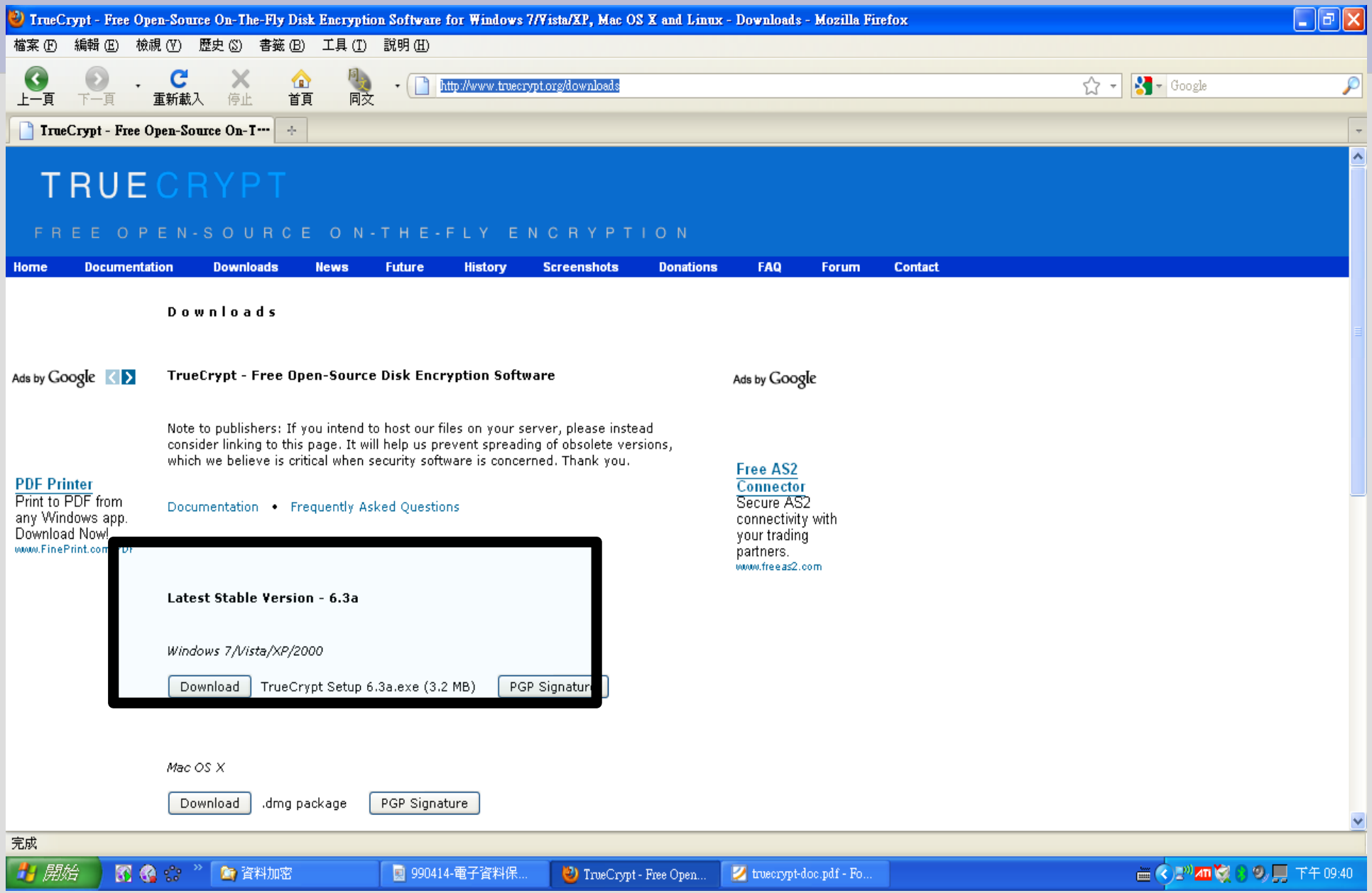
http://www.7-zip.org



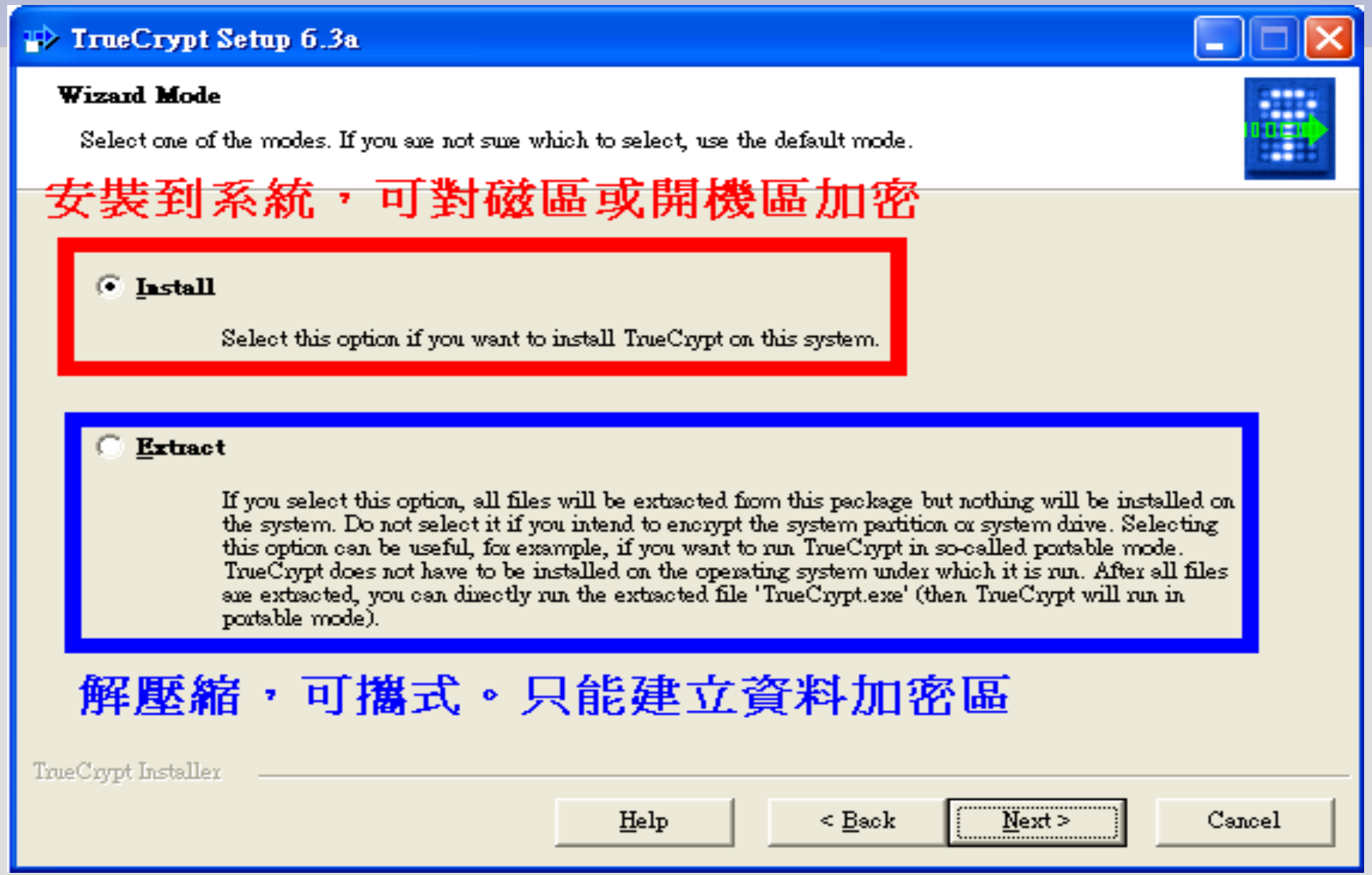
磁區加密管理–TrueCrypt

- TrueCrypt是一個免費的磁碟加密軟體，支援多種加密演算法如：AES、Serpent、Twofish等；另外在Windows、Mac OS X、OpenSuse與Ubuntu多種平台皆可使用。使用者可以決定安裝或者直接使用，其原理是利用在硬碟上新增一個類似「映像檔」的加密磁區，使用時只需掛載它，將需要加密的檔案移入其中，最後將其卸載，完成加密手續。
- **http://www.truecrypt.org/downloads**

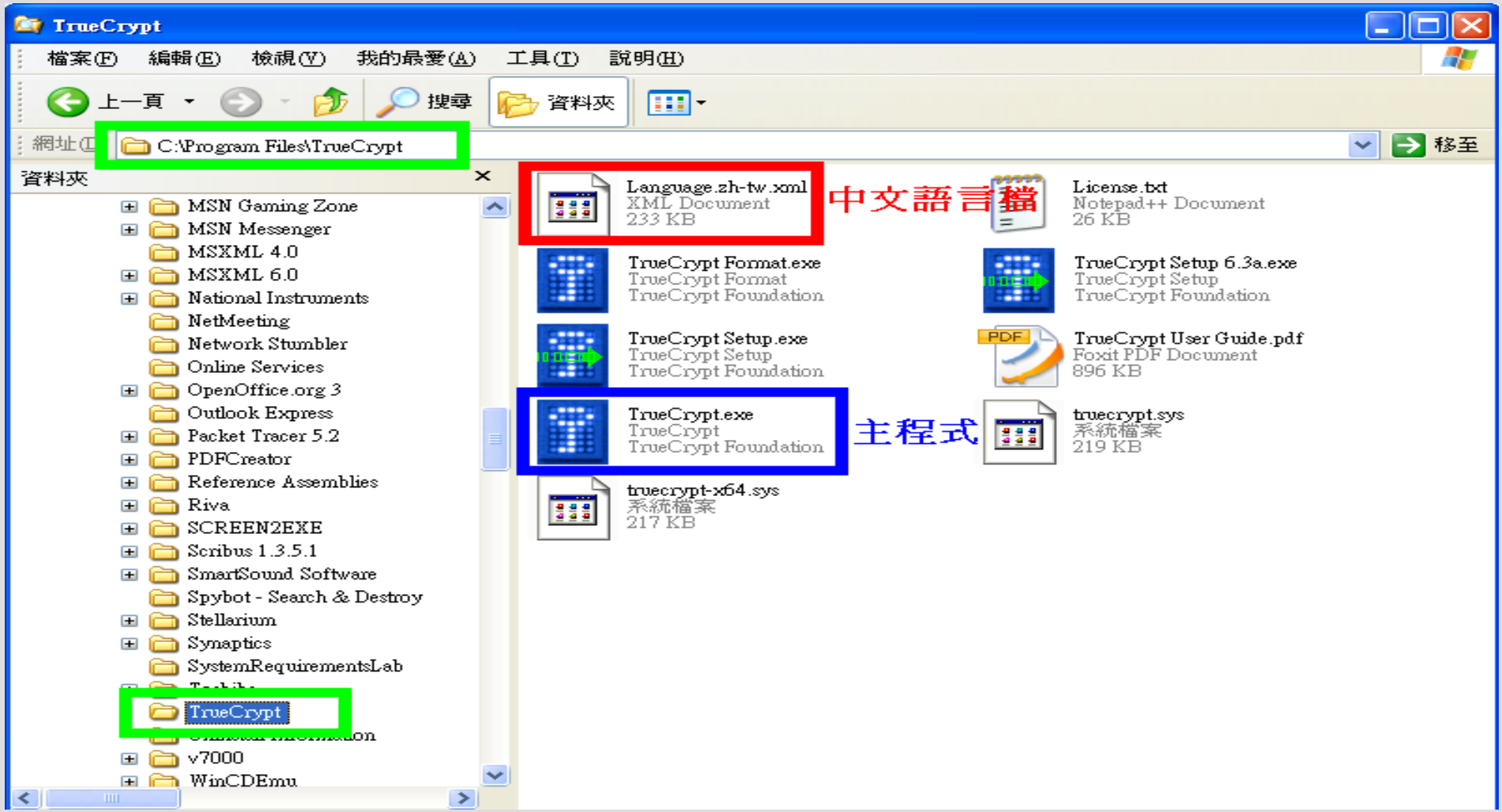
TrueCrypt-主程式



TrueCrypt-安裝



中文化http://www.truecrypt.org/localizations
解壓縮產生的Language. zh-tw. xml
檔案複製至TrueCrypt資料夾內



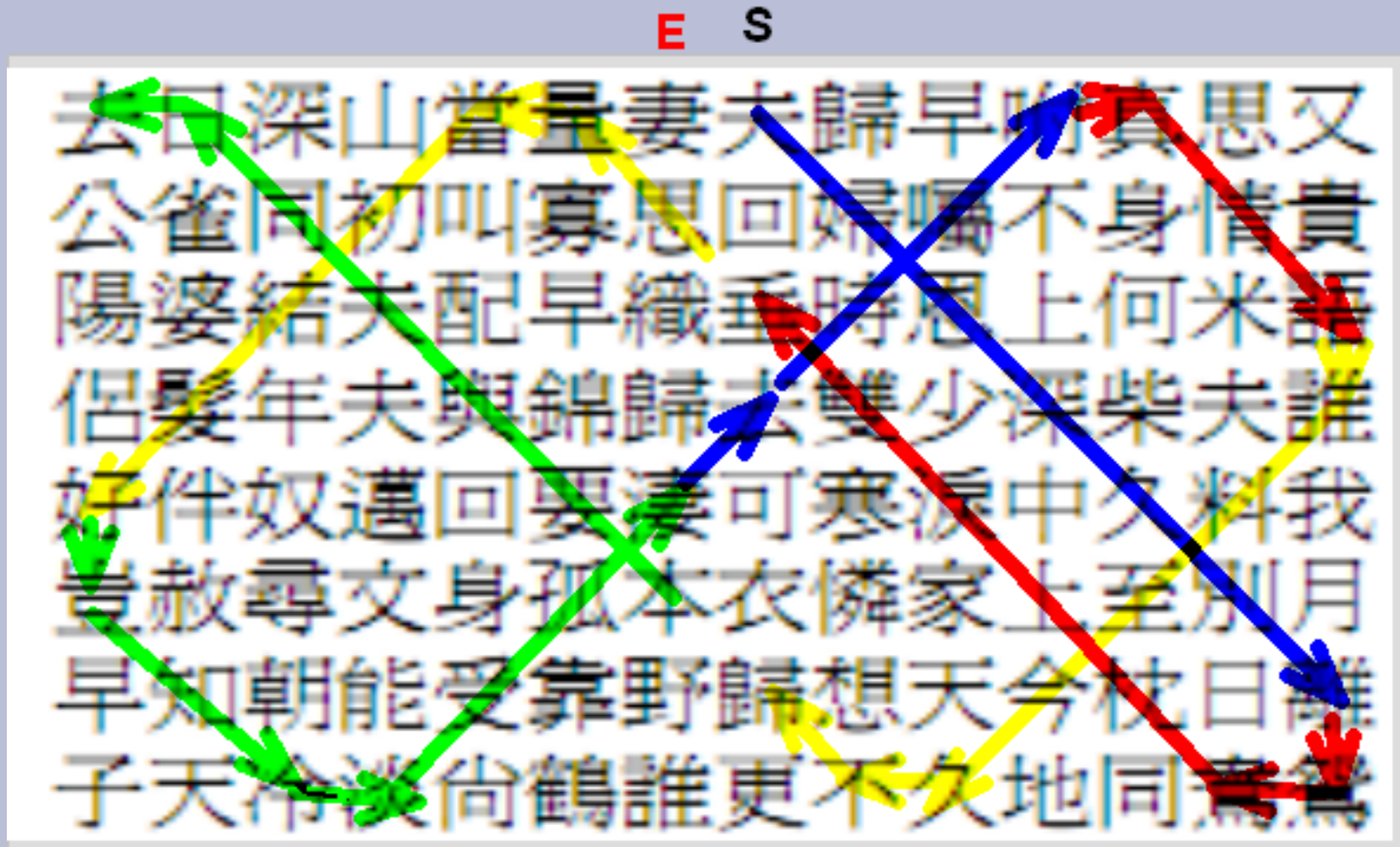
TrueCrypt-注意事項

- 設定的密碼必須牢牢記住，否則，萬一密碼忘記或遺失，所加密過的資料將無法解開，反而造成使用上的困擾–密碼要20~65個字元
- 資料加密磁區格式影響加密區大小
  - 採FAT需小於4GB
  - NTFS才能大於4GB
- 可以密碼與金鑰檔混合使用
- 掛載前需要在TrueCrypt的主畫面中選擇「選擇磁碟機」
- 不用時，請記得卸載磁碟區，將虛擬磁碟機卸載下來

硬體加密

- 採購具有加密功能的設備

內容編碼、傳輸加密



內容解碼

夫婦恩深久別離，鴛鴦枕上淚雙垂。
思量當初結髮好，豈知冷淡受孤淒。
去時囑咐真情語，誰料至今久不歸。
本要與夫同日去，公婆年邁身靠誰？
更想家中柴米貴，又思身上少寒衣。
野鶴尚能尋伴侶，陽雀深山叫早歸。
可憐天地同日月，我夫何不早歸回？
織錦迴文朝天子，早赦奴夫配寡妻。

PKI金鑰簽章加密

- 自然人憑證-不含重大個資
- GPG-GNU Privacy Guard-使用Openpgp加密技術的軟體-http://www.gnupg.org/
- 公共金鑰/私人密鑰 是一種加密/解密的方法，您可以把它們視成一對用來加密解密的『鑰匙』。簡單得說，被公共金鑰　所加密的訊息，只有私人密鑰能解開，同時，被私人密鑰所加密的訊息，也只有公共金鑰能解開
- 透過公認單位(內政部)確認寄件者與收件者，避免社交工程攻擊

一堆密碼記不住

- 把密碼貼在螢幕旁、藏在鍵盤下...
- 密碼原則

結論

- 隨身碟(行動裝置)具有輕、薄、短、小的優點，但這項優點也可能變成缺點，隨身碟體積小容易遺落，並同時造成資料遺失與外洩
- 使用隨身碟(行動裝置)應謹記下列原則:
  - 不儲存機敏性資料，如必須儲存應加密，並於使用後將資料立即刪除
  - 妥善保管避免遺失
- 在辦公室裡更要提防個人電腦或伺服器裡的機敏資料被有心人士利用隨身碟輕易盜拷
- 平常除需養成螢幕淨空與機敏資料加密等習慣
- 防範社交工程攻擊