

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

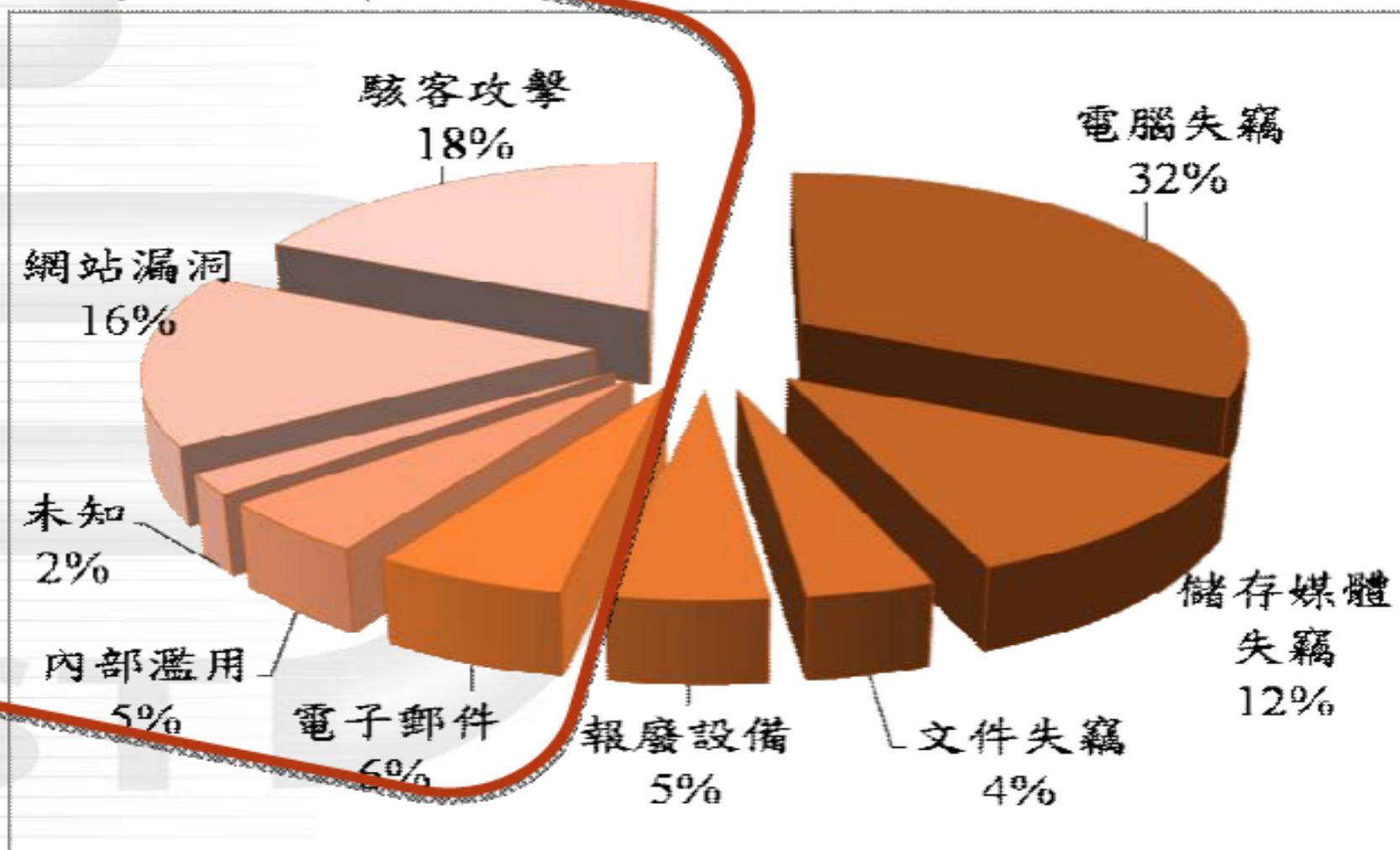
- .價值
- .威脅
- .風險
- .保護措施

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、桃園

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 東森購物個資外洩

97年購物完
8月接到自稱客服人員電話
被騙 5萬元

香港 7-29 會員頻傳遭詐騙 藝人也受害

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？

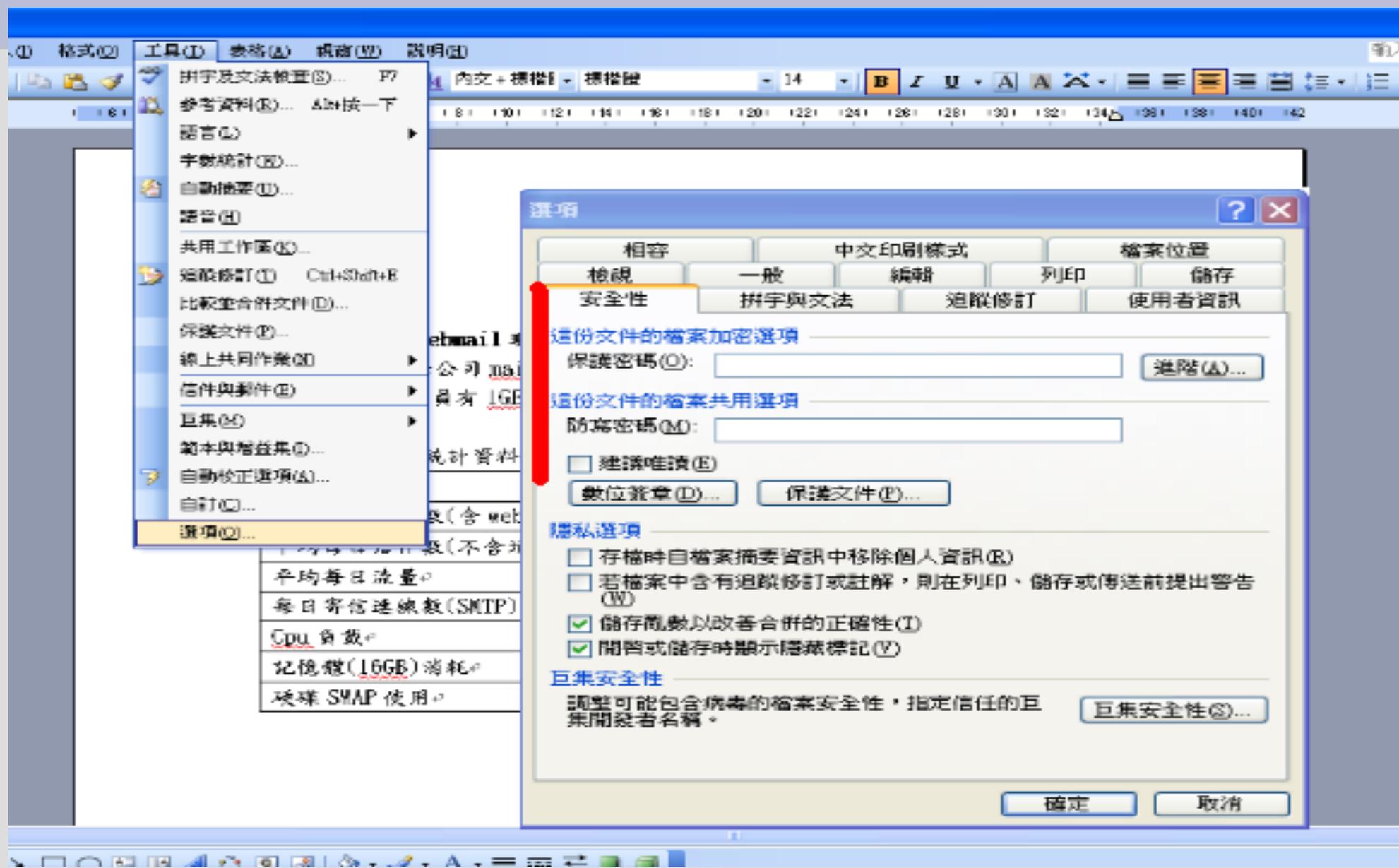
• 傳送

個人資料防護工具

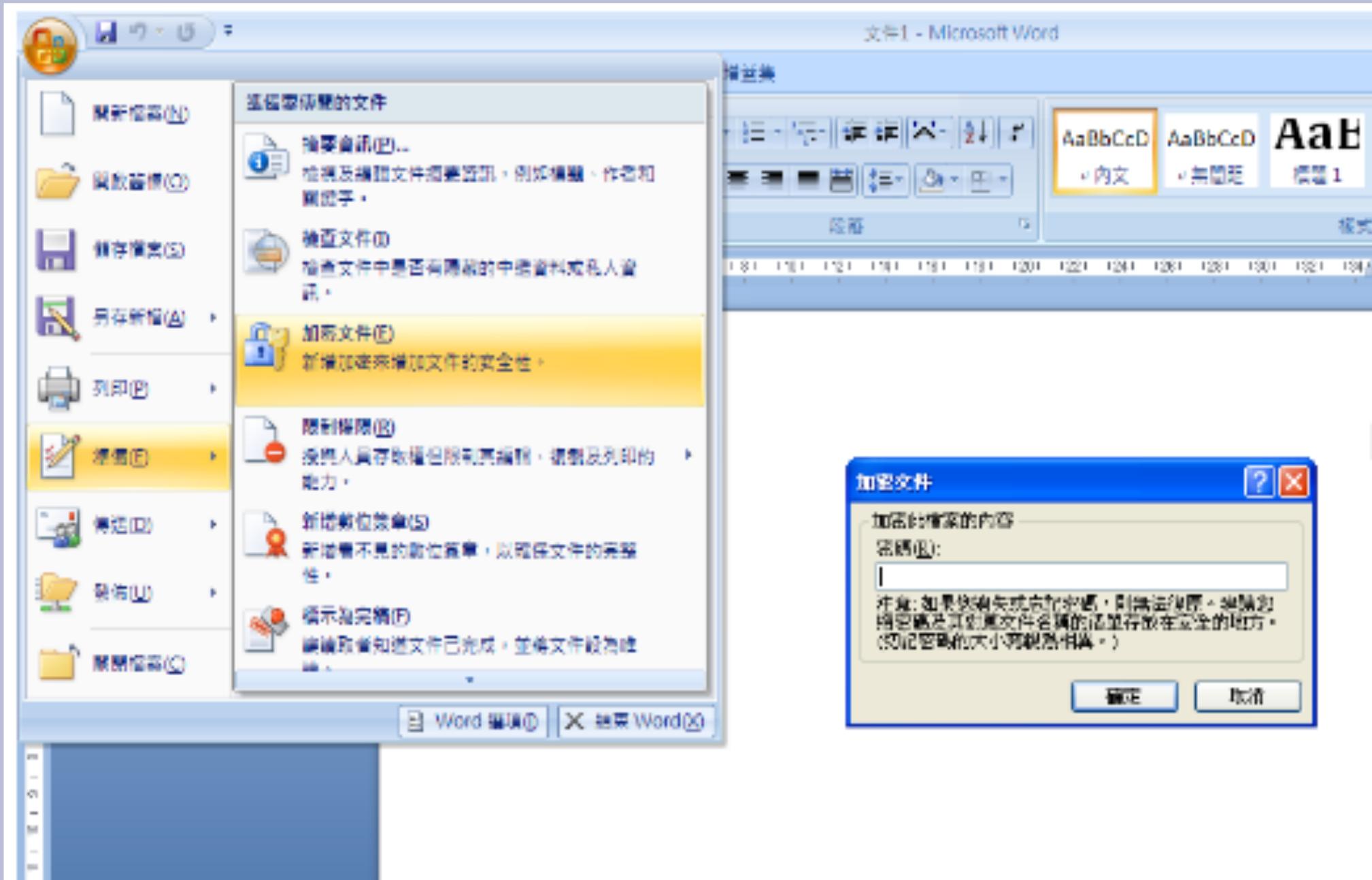
檔案加密管理-增加讀取的困難

- . 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

文件1 - Microsoft Word

校閱

保護文件

開始強制保護

保護方式

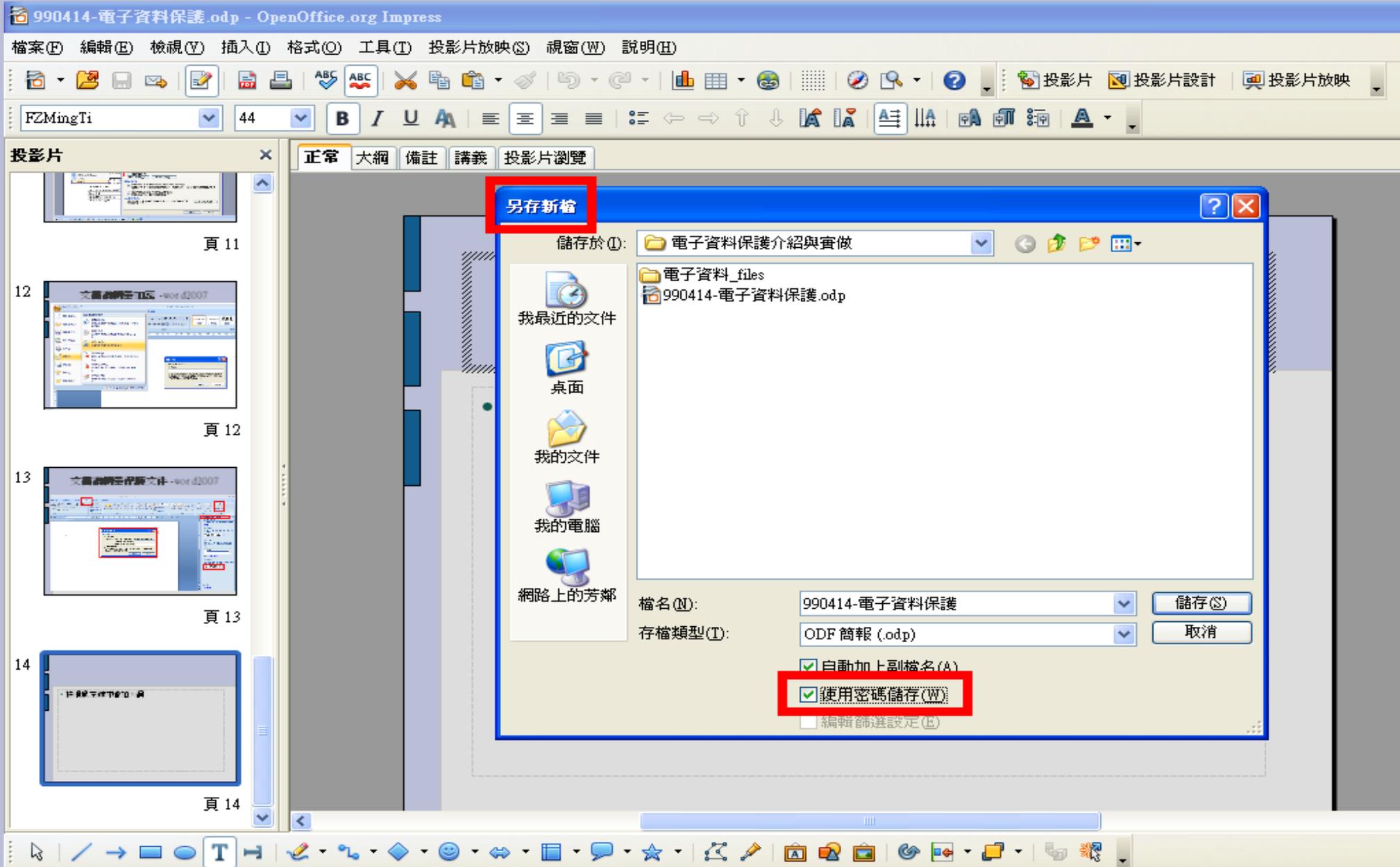
- 密碼 (A)
(文件並未加密。惡意使用者可以編輯檔案及移除密碼。)
輸入新密碼 (選用)(E):
重新輸入密碼以便確認 (E):
- 使用者驗證 (I)
(經過驗證的擁有者可以移除文件保護。文件已加密，而且已啟用 [限制存取] 功能。)

確定 取消

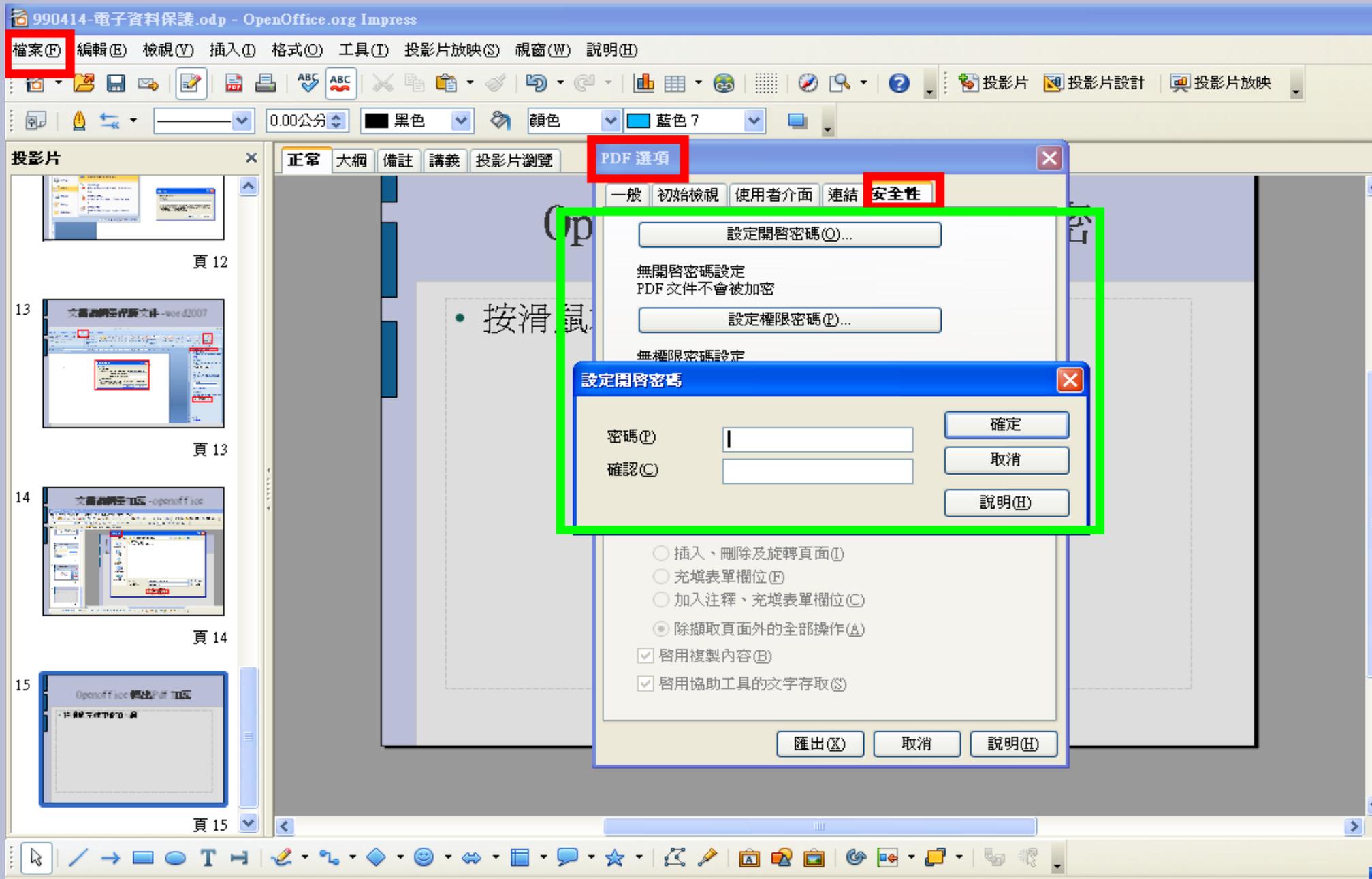
限制格式設定及編輯

- 格式設定限制
 - 限制只能對選取樣式設定格式設定...
- 編輯限制
 - 僅允許在文件中使用此類型的編輯方式。
不允許修改 (唯讀)
- 開始強制
 - 您準備好要套用這些設定嗎? (您稍後可以關閉這些設定)
 - 是，開始強制保護**

文書編輯器加密-Openoffice



Openoffice轉出Pdf加密



Outlook2007帳戶檔案加密

收件匣 - Microsoft Outlook

檔案(F) 編輯(E) 檢視(V) 到(G) 工具(T) 動作(A) Outlook Connector(U) 說明(H)

1

2 帳戶設定

3

4

5

6

7

資料檔
Outlook 資料檔

電子郵件 資料檔 RSS 摘要 SharePoint 清單 網際網路行事曆 已發佈的行事曆 通訊錄

新增(A) 設定(S) 設成預設值(D) 移除(M) 開啓資料夾(O)...

名稱	檔案名稱	註解
封存資料夾	Outlook.pst (位於 C:\Documents and Settings\Administrator\Local Se...	
個人資料夾	Outlook.pst (位於 C:\Documents and Settings\Administrator\Local S...	預設
網際網路行事曆	網際網路行事曆訂閱(2).pst (位於 C:\Documents and Settings\Ad...	

個人資料夾

一般

名稱(N): 個人資料夾

檔案名稱(F): C:\Documents and Settings\Administrator\Local Settin

格式: 個人資料夾檔案

變更密碼(P)... 變更存取個人資料夾檔案的密碼

開始壓縮(C) 開始壓縮

註解(M)

變更密碼

變更 Outlook.pst 的密碼:

舊密碼(O): 17

新密碼(N):

確認密碼(Y):

將密碼儲存在密碼清單中(S)

確定

取消

關閉(C)

7-ZIP 壓縮加密

<http://www.7-zip.org>

The screenshot shows the 7-Zip application window with the 'Add to Archive' dialog box open. The main window displays a file list in the left pane, with '蘇蕙迴文詩.pdf' selected. The dialog box contains the following settings:

- 壓縮檔(A): 蘇蕙迴文詩.7z
- 壓縮檔格式(E): 7z
- 壓縮層級(L): 一般壓縮
- 壓縮方式(M): LZMA
- 字典大小(D): 16 MB
- 字組大小(W): 32
- 結實區塊大小: 2 GB
- CPU 線程數: 2 / 2
- 壓縮時記憶體使用: 192 MB
- 解壓縮時記憶體使用: 18 MB
- 分割壓縮檔, 位元組(V):
- 參數(P):

The '加密' (Encryption) section is highlighted with a red box and includes:

- 輸入密碼: [Empty text box]
- 重新輸入密碼: [Empty text box]
- 顯示密碼(S)
- 加密方法: AES-256
- 加密檔名(N)

At the bottom of the dialog box are buttons for '確定' (OK), '取消' (Cancel), and '說明' (Help).

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 - Free Open-Source On-The-Fly Disk Encryption Software for Windows 7/Vista/XP, Mac OS X and Linux - Downloads - Mozilla Firefox

檔案 (E) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (I) 說明 (H)

上一頁 下一頁 重新載入 停止 首頁 同文

<http://www.truecrypt.org/downloads>

TrueCrypt - Free Open-Source On-T...

TRUECRYPT

FREE OPEN-SOURCE ON-THE-FLY ENCRYPTION

Home Documentation Downloads News Future History Screenshots Donations FAQ Forum Contact

Downloads

Ads by Google [TrueCrypt - Free Open-Source Disk Encryption Software](#)

Note to publishers: If you intend to host our files on your server, please instead consider linking to this page. It will help us prevent spreading of obsolete versions, which we believe is critical when security software is concerned. Thank you.

Documentation • [Frequently Asked Questions](#)

Latest Stable Version - 6.3a

Windows 7/Vista/XP/2000

[Download TrueCrypt Setup 6.3a.exe \(3.2 MB\)](#) [PGP Signature](#)

Mac OS X

[Download .dmg package](#) [PGP Signature](#)

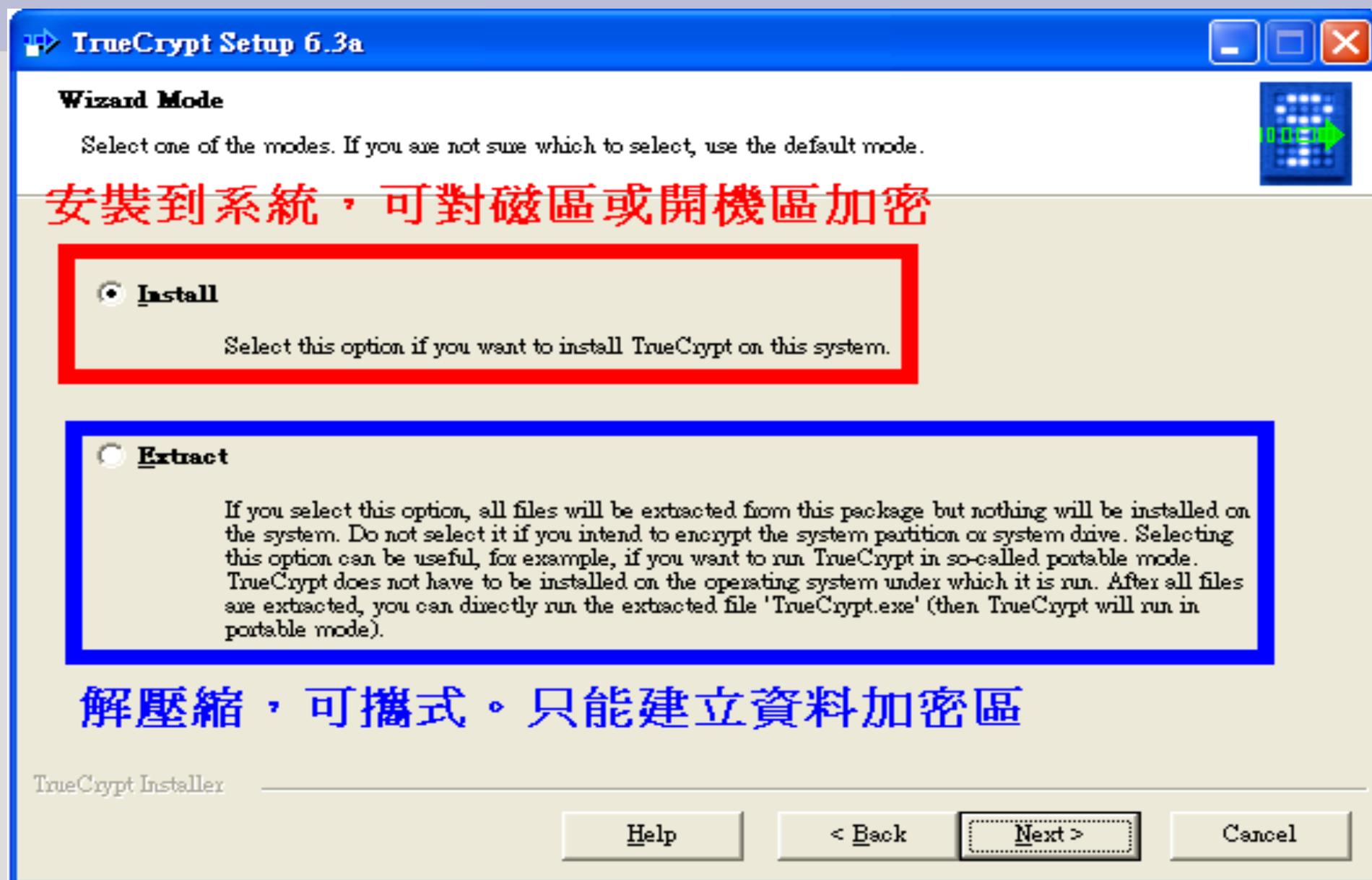
PDF Printer
Print to PDF from any Windows app. Download Now! www.FinePrint.com

Free AS2 Connector
Secure AS2 connectivity with your trading partners. www.freeas2.com

完成

開始 資料加密 990414-電子資料保... TrueCrypt - Free Open... truecrypt-doc.pdf - Fo... 下午 09:40

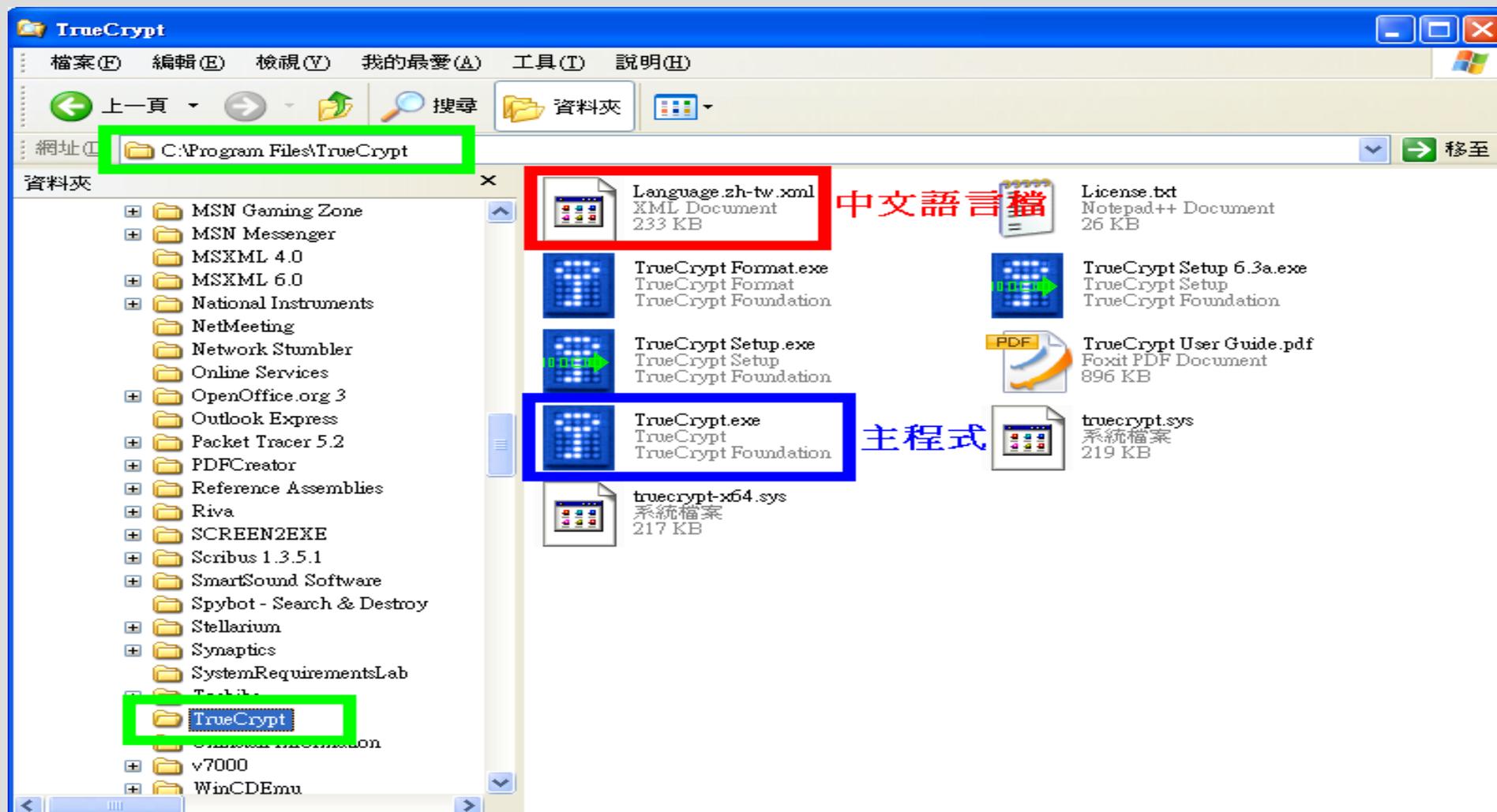
TrueCrypt-安裝



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

E S

去日深山當量妻夫歸早啣真思又
公雀同初叫寡思回婦囑不身情貴
陽婆結夫配早織垂時恩上何米語
侶髮年夫與錦歸去雙少深柴夫誰
好伴奴邁回要湊可寒淚中久料我
豈赦尋文身孤本衣憐家上至別月
早知朝能受靠野歸想天今枕日離
子天冷淡尚鶴誰更不久地同焉焉

The image shows a 10x8 grid of Chinese characters. Colored arrows trace a path through the characters, starting from the top-left and ending at the bottom-right. The path is composed of green, yellow, blue, and red arrows. The green arrows form a large 'X' shape, connecting the top-left to the bottom-right and the top-right to the bottom-left. The yellow arrows form a path that starts at the top-left, goes to the top-right, then down to the bottom-right, and finally to the bottom-left. The blue arrows form a path that starts at the top-right, goes to the bottom-right, then up to the bottom-left, and finally to the top-left. The red arrows form a path that starts at the top-right, goes to the bottom-right, then up to the bottom-left, and finally to the top-left.

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