

農委會農業金融局 下半年度主管人員訓練



資安趨勢及個資案例宣導

實施日期：107年7月25日、107年9月26日

授課講師：SOC部 陳成聰 經理

簡報大綱

一

資訊安全

二

資安趨勢

三

個人資料保護

四

神鬼駭客

五

ODF

六

Q&A

農委會農業金融局

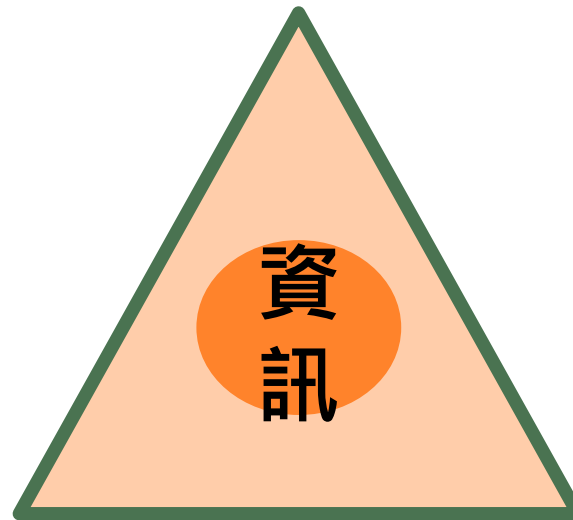
一．資訊安全

一 · 資訊安全

➤ 何謂資訊安全？

保護資訊的**機密性**、**完整性**與**可用性**;另外也涉及如：不可否認性、驗證性、可歸責性、及可靠性等特性。

Confidentiality 機密性

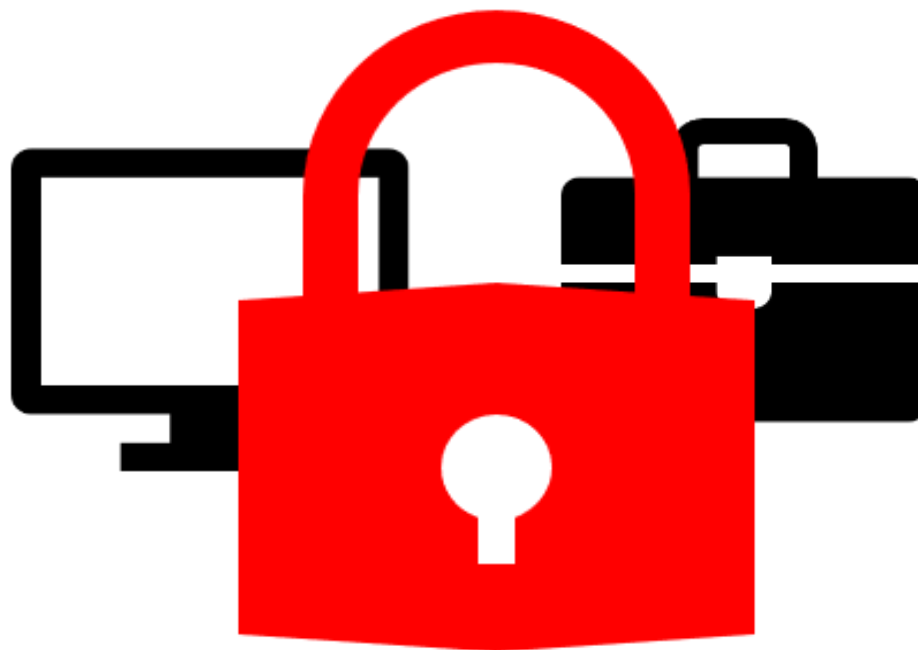


Availability 可用性

Integrity 完整性

一 · 資訊安全

➤ 何謂機密性？



上鎖了嗎？

一 · 資訊安全

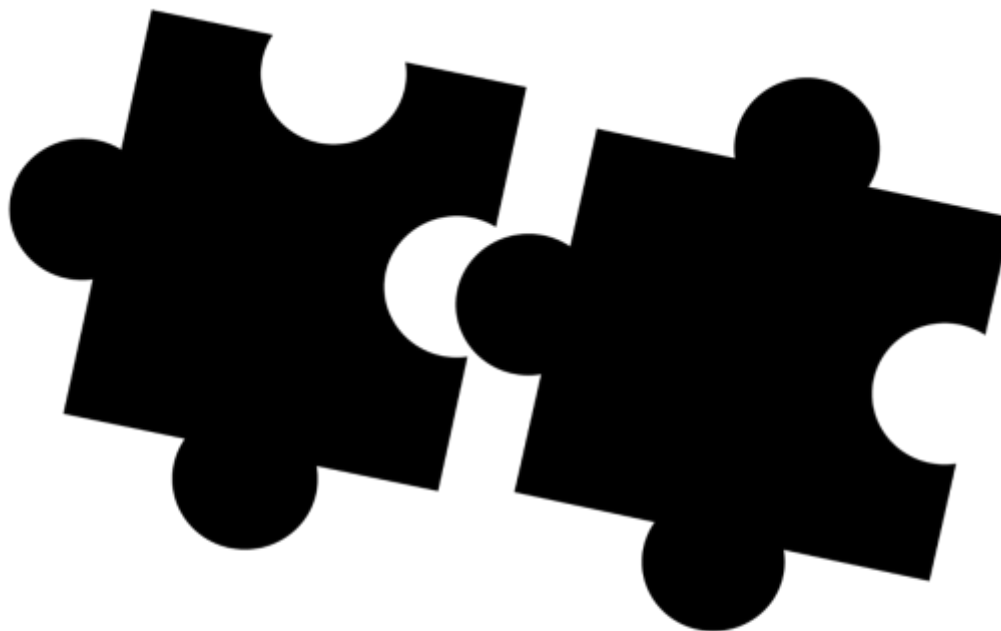
➤ 何謂可用性?



能正常使用嗎?

一 · 資訊安全

➤ 何謂完整性?



有被竄改嗎?

一 · 資訊安全

➤ 為什麼需要資訊安全？



博愛座 —— 人人可坐
但請記得
讓給需要的人



© 2018 TSC

博愛座 —— 人人可坐
但請記得
讓給需要的人



© 2018 TSC

一 · 資訊安全

➤ 資訊安全的迷失

1. 我的單位已經百分之百的安全！
2. 單位資訊沒有價值，有需要保護嗎？
3. 朋友、同事、長官寄來的信一定安全嗎？

一．資訊安全

➤ 資安宣導短片 - 一分半看懂資安



農委會農業金融局

二 · 資安趨勢

二 · 資安趨勢

➤ 資通安全管理法最受爭議的條文

第十八條

中央目的事業主管機關因查核資通安全維護計畫發現重大缺失，或遇重大資通安全事件，認有必要時，得進入受查核之非公務機關場所檢查；非公務機關及相關人員不得規避、妨礙或拒絕；參與檢查之人員就因而知悉之他人秘密資訊，應負保密義務。

➤ 資通安全管理法立委質詢



二 · 資安趨勢

- 一級關鍵基礎設施業者名單公布，加重遭駭知情不報者處罰
- 目前行政院資安處只有公布一級關鍵基礎設施業者的名單
1. 能源部分：臺電及中油等公營事業。
 2. 水資源：臺北翡翠水庫管理局政府機關。
 3. 通訊傳播：中華電信、新世紀資通、台固、全球光網、國際環球及亞太電信等民間企業。
 4. 交通：民航局臺北國際航空站及民航局高雄國際航空站等政府機關。
 5. 公營事業則有臺鐵、臺北捷運、臺灣港務公司和桃園機場等公營事業，以及高鐵和高雄捷運等民間企業。
 6. 金融與銀行領域：中央銀行公營事業及財金資訊公司
 7. 中央與地方政府：國家發展委員會及故宮等兩個政府機關。

二 · 資安趨勢

➤ 資安管理六子法出爐 政院將辦十場座談會

- 行政院資通安全處決定自二月起，在全台各地舉辦十場座談會，廣徵各界意見。
- 行政院在提出「資通安全管理法草案」後，進一步草擬完成「資通安全事件通報及應變辦法」等六項「資通安全管理法草案」子法。
- 這六項子法為：
 1. 「資通安全管理法施行細則」
 2. 「資通安全責任等級分級辦法」
 3. 「資通安全事件通報及應變辦法」
 4. 「資通安全維護計畫實施情形稽核辦法」
 5. 「資通安全情資分享辦法」
 6. 「公務機關人員資訊安全事件獎懲辦法」

二 · 資安趨勢

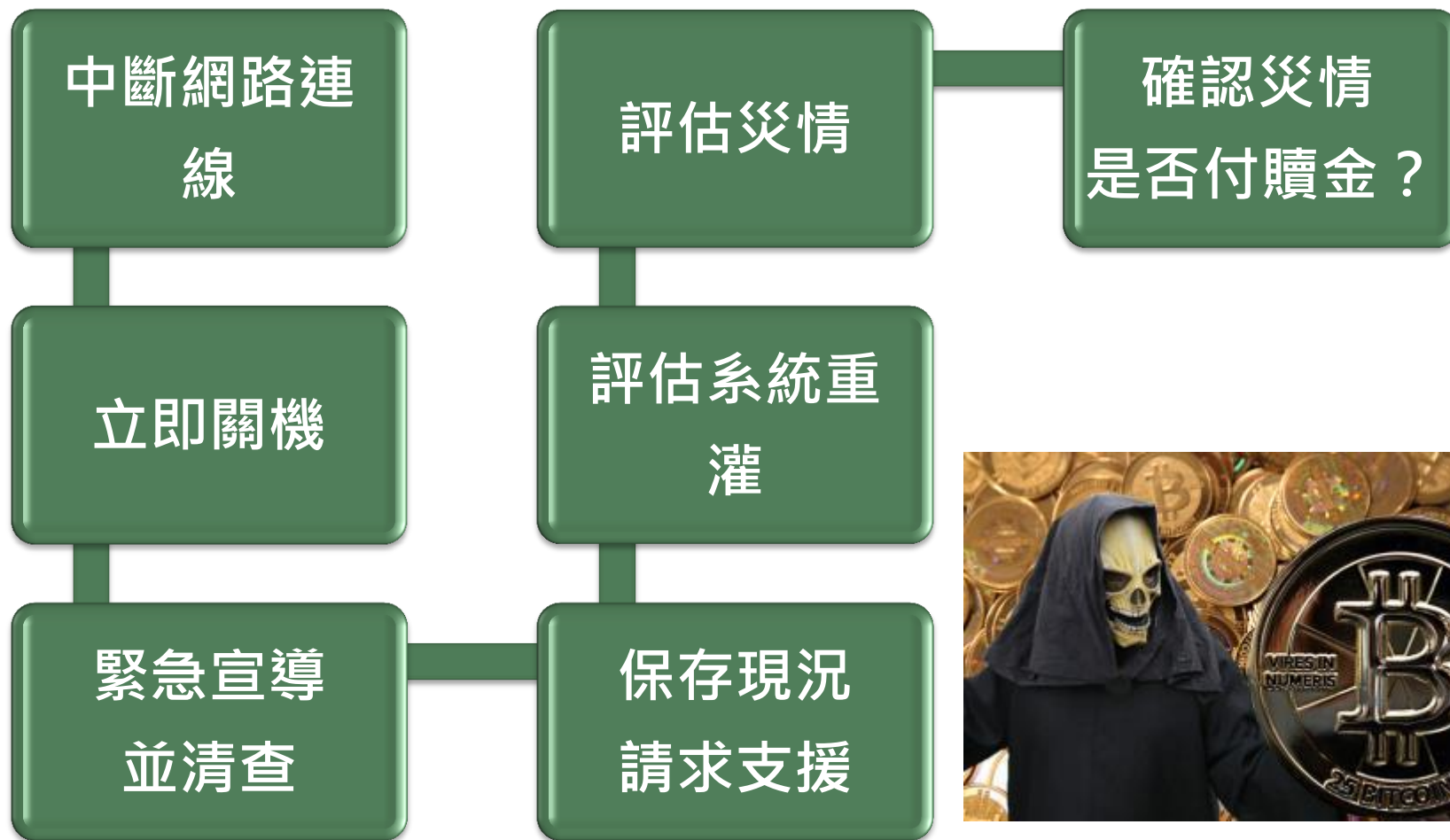
- **IoT仍是潛在威脅**
- 隨著聯網裝置的日益普及與運算能力的提昇，IoT設備仍然成為企業，甚至是個人的潛在威脅。
- 例如像心律調整器的生理監視裝置就可能會遭駭客攔截，而這類生物駭客的案例可能在醫療與穿戴裝置中真實上演。

二 · 資安趨勢

- 勒索軟體攻擊目標多元
- 連銀行、醫院、電力公司等關鍵基礎設施都受到影響
- 駭客會更進一步鎖定可帶來更高利益的特定企業進行攻擊
- Fortinet甚至提到雲端服務商可能成為勒索病毒的攻擊對像，因為其雲端服務的特性將會造成大量企業與客戶的營運中斷，而藉此讓駭客獲得巨額的報酬
- IBM則認為勒索軟體會朝大量攻擊發展，而以IoT設備為目標，用低於重新購買聯網設備的較少贖金對受害者進行勒索

二 · 資安趨勢

➤ 中勒索軟體的因應方法：



資料來源 <http://www.ithome.com.tw/tech/101366>

二 · 資安趨勢

➤ 社交工程的基本防護

- 執行各種作業系統、應用軟體的更新及設定。
- 必須安裝防毒軟體，並確實更新病毒碼。
- 密碼設定要符合**複雜度**的要求。
- 不要輕易相信電話中任何非經正式授權的請求。
- 不要任意安裝未經授權的軟體。
- 小心釣魚網站、詐騙廣告的陷阱。
- 不使用公務信箱作為登入的帳號。
- 不於社群網路中談論有關公務之相關內容。
- 修改個人資料的隱私設定(提供**最少**個資為宜)。
- 不要輕易點選陌生的加好友請求。
- 不任意點選社群網路聊天室或電子郵件的連結。

二 · 資安趨勢

➤ 正確地使用電子郵件

- 關閉郵件預覽功能。
- 除非相當確定信件的來源，否則決不輕易開啟或點擊信件裡的附件檔案或超連結。
- 不要將電子郵件密碼告知任何人，即使是系統管理者。
- 不要將電子郵件帳號轉借他人使用。
- 不要使用電子郵件傳輸任何不當資訊，包括不法、暴力、色情、違法交易、侵犯隱私或威脅他人的資料。
- 不要轉寄不明網路謠言及發送廣告信。
- 轉寄前先將他人郵件地址刪除，避免他人郵件地址傳出。
- 同時寄件給多人時，為保護各收信人資訊，最好使用「密件副本」方式傳送。

二 · 資安趨勢

利用社交工程攻擊手法-關鍵基礎建設

伊朗新聞通訊社周日（9/26）報導，當地境內首座核能發電廠受到Stuxnet蠕蟲感染，該發電場負責人Mahmoud Jafari已證實此事，但表示僅有部份員工電腦受到感染，而非主要系統。伊朗已派遣專家移除發電廠員工電腦中的病毒，而即將上線營運的核能發電系統並無大礙。



農委會農業金融局

三．個人資料保護

三、個資法之立法目的

- 避免人格權受侵害
- 促進個人資料合理利用



三、個資法-第三條

第 3 條

當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

- 一、查詢或請求閱覽。
- 二、請求製給複製本。
- 三、請求補充或更正。
- 四、請求停止蒐集、處理或利用。
- 五、請求刪除。

資料來源：[全國法規資料庫](#)

三、個資法-第六條

第 6 條

有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

- 一、法律明文規定。
- 二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 三、當事人自行公開或其他已合法公開之個人資料。
- 四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。

資料來源：[全國法規資料庫](#)

三、個資法-第五十二條

第 52 條

第二十二條至第二十六條規定由中央目的事業主管機關或直轄市、縣（市）政府執行之權限，得委任所屬機關、委託其他機關或公益團體辦理；其成員因執行委任或委託事務所知悉之資訊，負保密義務。
前項之公益團體，不得依第三十四條第一項規定接受當事人授與訴訟實施權，以自己之名義提起損害賠償訴訟。

資料來源：[全國法規資料庫](#)

三、實例分享-個資過度保護



資料來源：[youtube](https://www.youtube.com/watch?v=...)

三、防範資料外洩的基本原則

- 資料的鑑別並分級分類
- 除非必要，否則不蒐集機敏資料(不蒐集就沒有外洩風險)
 - 最小蒐集原則
- 除非必要，否則已經不需要的機敏資料應立即清除(保存時間越長，外洩風險越高)
 - 最短保存期限

三、個人資料保護作法

- 個人資料資訊分類分級，依等級不同採取不同管控措施
 - 加密機制
 - 存取權限
 - 必要時採取網路隔離。
- 筆記型電腦、行動隨身碟等儲存設備因攜帶方便、容易遺失，應設定密碼保護或資料加密，並儘可能避免存放機密公務資料，並妥善保管。
- 避免將個人基本資料放於網路上流傳或散播。

三 · 個人資料保護

➤ 史上最嚴資料保護令GDPR 來了！



資料來源：<https://www.microsoft.com/taiwan/security/gdpr/>

農委會農業金融局

四 · 神鬼駭客

四 · 神鬼駭客

➤ 駭客假稱給你藍勾勾！這些網紅、藝人IG帳號都被盜

社群網站像是Facebook或是IG，都會特別標記公眾人物「藍色勾勾」，認證是本人帳號，但最近傳出有不肖駭客假冒官方寄信，說要提供藍勾勾認證，要求一些網紅或藝人提供帳號密碼，被害人不察因而上當，不但沒得到認證，整個帳號都被盜用，包括Youtuber蔡哥、藝人四葉草都受害。



四 · 神鬼駭客

➤ 駭客2度入侵日本401家飯店系統 32萬人個資、信用卡號碼被盜

許多國人喜愛到日本旅遊，近日卻傳出日本有401家飯店的房客資料遭盜，共計高達32萬筆，其中包含房客的姓名、電話以及住址等個資，更有訂房旅客的信用卡號碼慘遭外洩，儘管飯店高層緊急出面道歉，但負責訂房系統維護的法國技術商Fastbooking卻仍未提出解決辦法。



王子飯店共有12多萬筆的客戶個資被盜。（圖／王子飯店官網）

四 · 神鬼駭客

➤ 新興詐欺手法專案報告

編號	標題	發布日期
1	有沒有這麼好康？辦門號換現金！	107-06-28
2	107/6/18-6/24民眾通報高風險賣場(平臺)	107-06-28
3	購物停、看、聽~一頁式廣告詐騙！	107-06-27
4	外國朋友要小心！照過來~~~	107-06-21
5	網路論壇尋芳!? 潛藏在吸睛照片背後的威脅與詐騙	107-06-20
6	暑假將至！您在尋找工作機會嗎???	107-06-19
7	107/6/4-6/10民眾通報高風險賣場(平臺)	107-06-19
8	臉書購物沒保障!您貪他的利，他要您的本!	107-06-19
9	假網拍詐騙：熱門秒殺級演唱會門票！	107-06-13

四 · 神鬼駭客

➤ 假星巴克粉絲團 留言就送免費一年咖啡兌換券



四 · 神鬼駭客

➤ MyGoPen麥勾騙阿！



四 · 神鬼駭客

➤ 行動裝置的安全防護 - 基本認知

- 安裝行動裝置防毒軟體
- 設定行動裝置密碼、自動鎖定功能
- 請勿修改或破解行動裝置之安全措施(如：越獄)
- 請勿利用行動裝置進行重要交易行為
- 不理會陌生人的訊息(如：LINE、Facebook等)
- 不任意點選來路不明的網頁連結、簡訊連結，如果是好友送來的訊息，建議改用另外的方式(打電話、email)與對方聯絡，確定這個連結是安全、沒有問題的之後再開
- 設定不具個人識別的裝置名稱

四 · 神鬼駭客

➤ 行動裝置的安全防護 - 基本認知

- 儘量避免離開視線或交由陌生人操作
- 充電儘量使用座充變壓器，避免連接電腦
- 不上可疑網站，不下載可疑APP
- 取消電信小額付款機制
- 需要使用小額付款的使用者，應啟用「即時消費通知」，若發現詐騙發生，請務必報警，才可當作是被詐騙證明，要求電信業者不能列入帳單或是可到臨櫃辦簽結退款
- 使用任何通訊軟體與社群軟體，勿使用懶人密碼
- 不隨意提供個人資訊，也不隨意轉寄簡訊

四 · 神鬼駭客

- 行動裝置的安全防護 - APP下載與使用
 - 僅安裝來自可信任來源之軟體
 - 留意該APP 的星級評價、總下載次數
 - 觀察使用者對該APP之評論
 - 注意軟體存取權限設定
 - 軟體定期更新修補程式



農委會農業金融局

五 · ODF

五 · ODF簡介

➤ ODF相關網站

- ODF研習資料：<https://ppt.cc/fDr5yx>
- 國發會以Libre office為藍本，所開發之ODF文件應用工具（NDCODFApplicationTools），下載網址：
<https://www.ndc.gov.tw/cp.aspx?n=32A75A78342B669D&s=41F160FA9EF25A20>

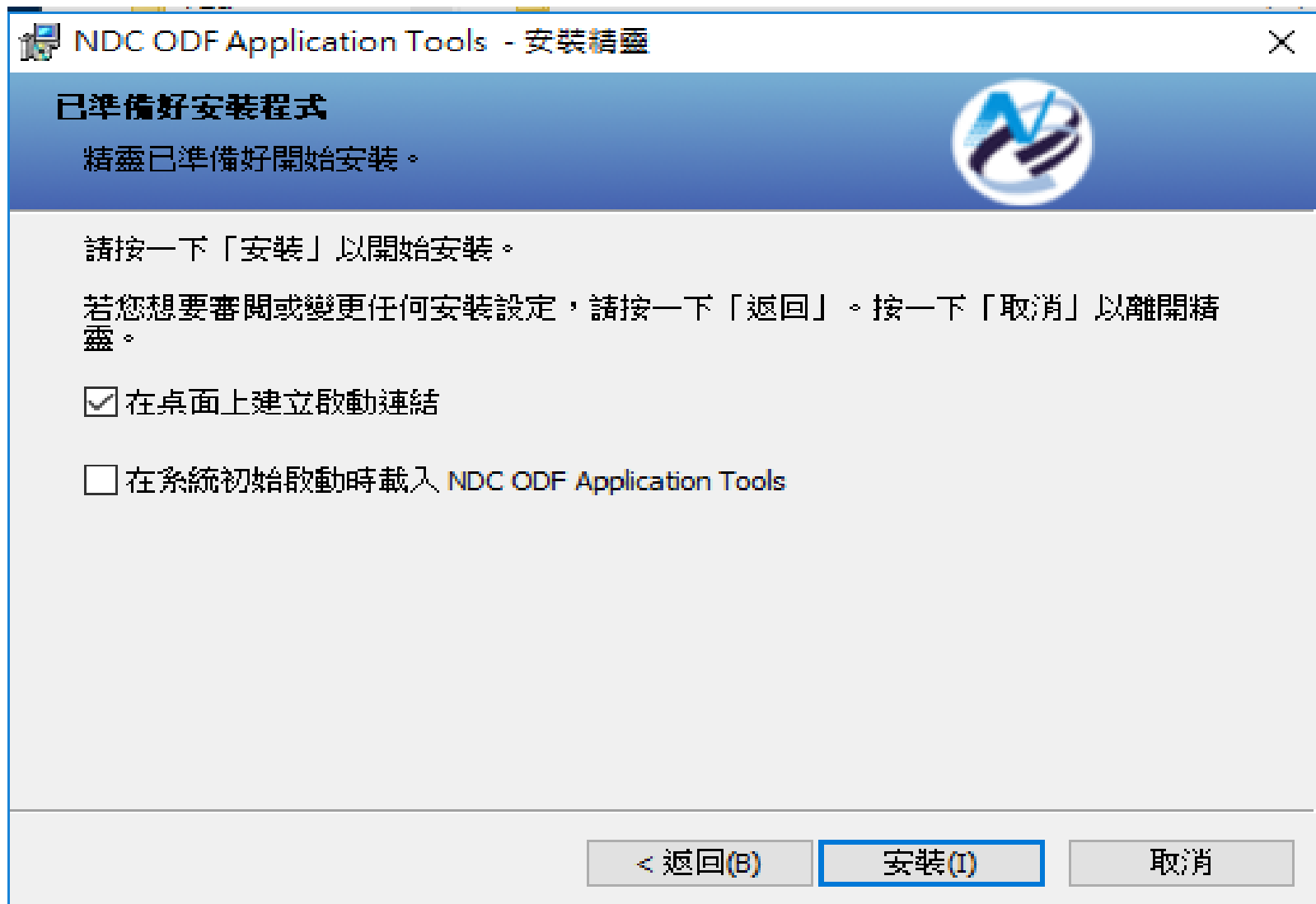
五 · NDCODF安裝說明



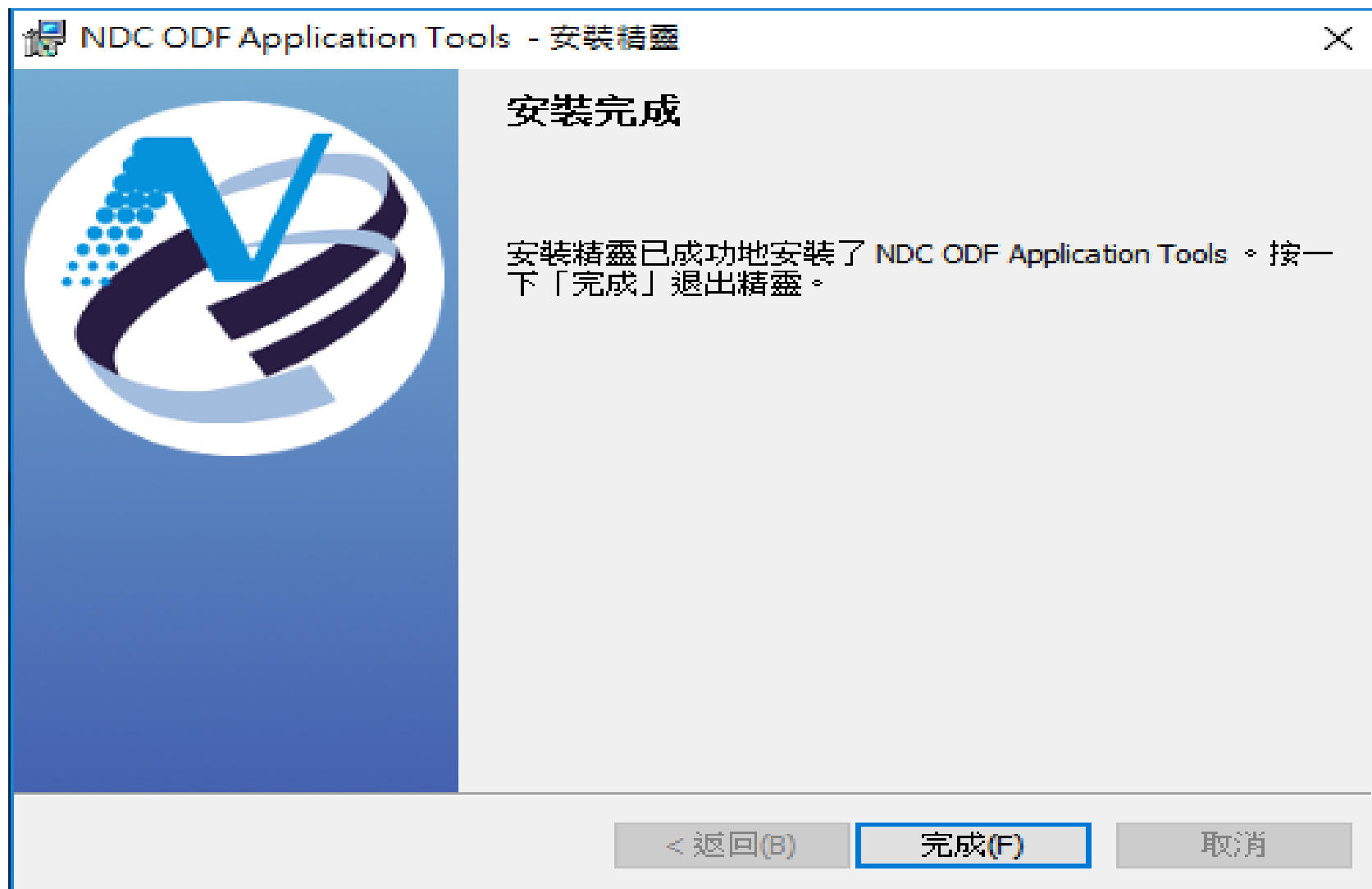
五 · NDCODF安裝說明



五 · NDCODF安裝說明



五 · NDCODF安裝說明



五 · 注意事項（一）

➤ 如果檔案是.docx（或doc）檔

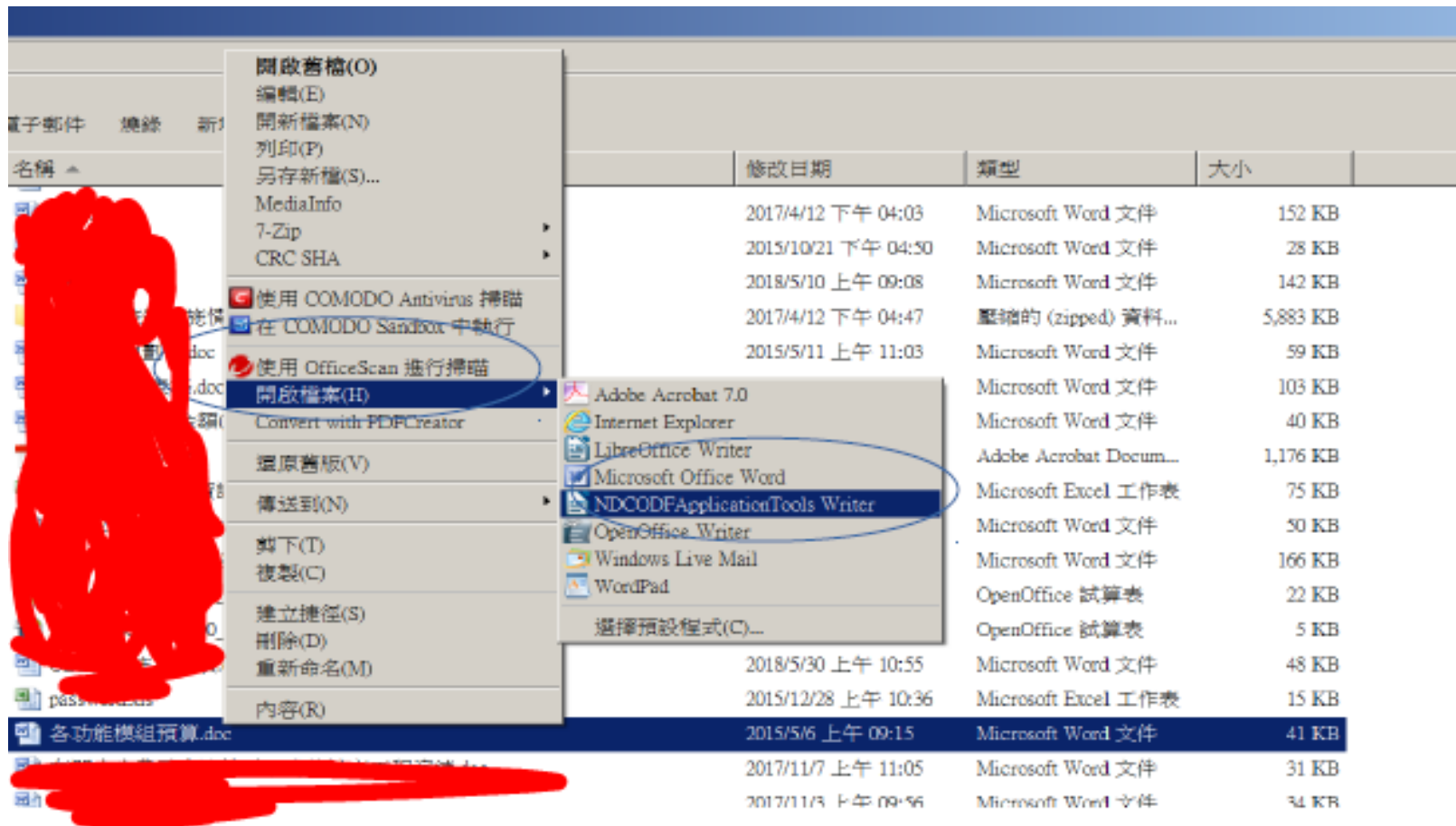
- 千萬不要用Word打開，以另存檔案方式存.odt檔。
- 建議直接以Writer開啟.docx（或doc）檔案，用Writer存成.odt檔案。

➤ 如果檔案是Word存的.odt檔

- 以Wtrier開啟.odt檔案。
- 可以在功能選單找到格式\頁面\文字網格\不使用網格，設定格式。

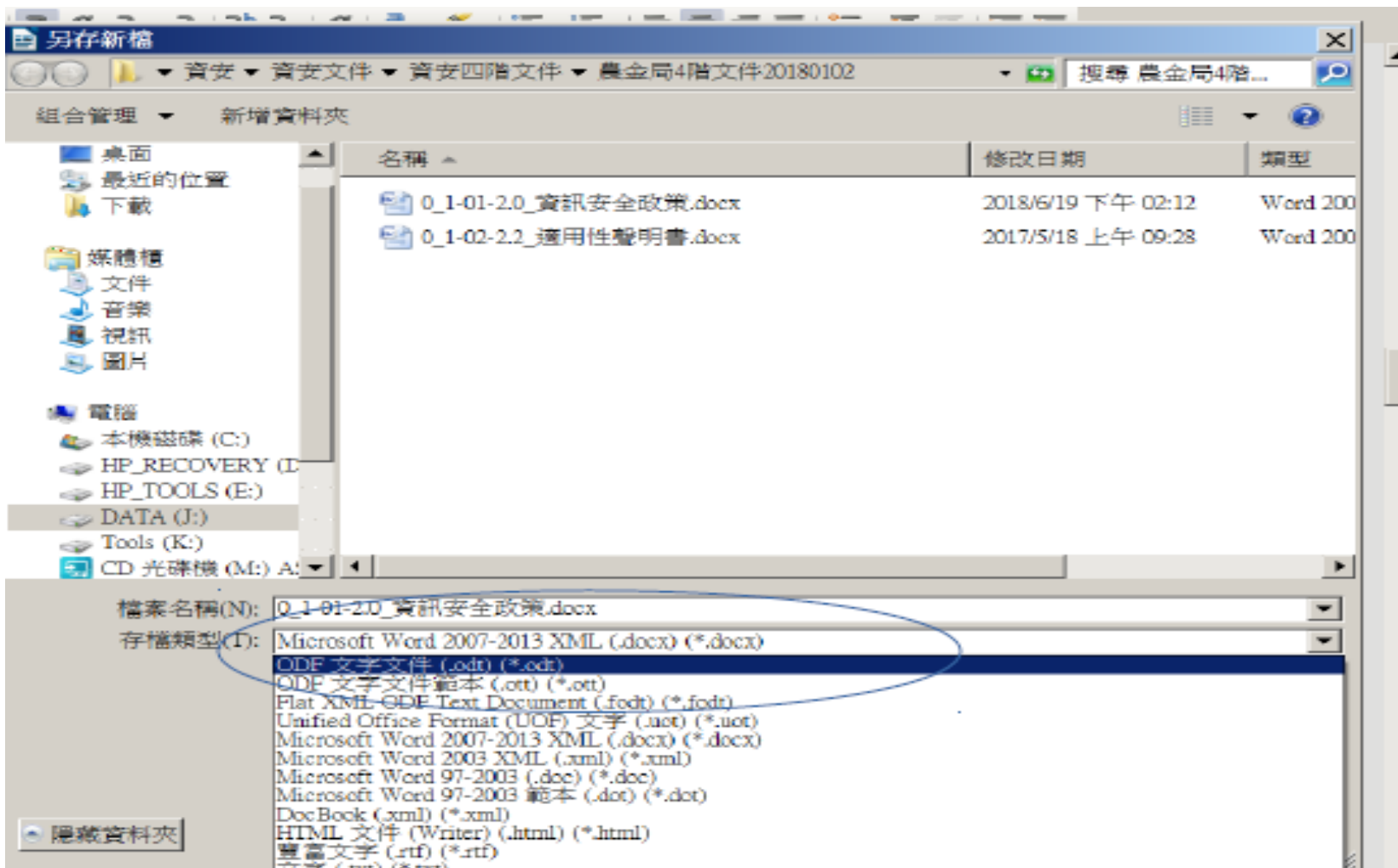
五 · 轉檔示範

- 以Writer開啟.docx (或doc) 檔案(滑鼠右鍵選開啟檔案 (H) 選NDCODFAApplicationTools writer或OpenOffice writer)



五 · 轉檔示範

➤ 另存新檔，存成.ODT格式



五·開啟檔案及調整格式

➤以Wtrier開啟.odt檔案

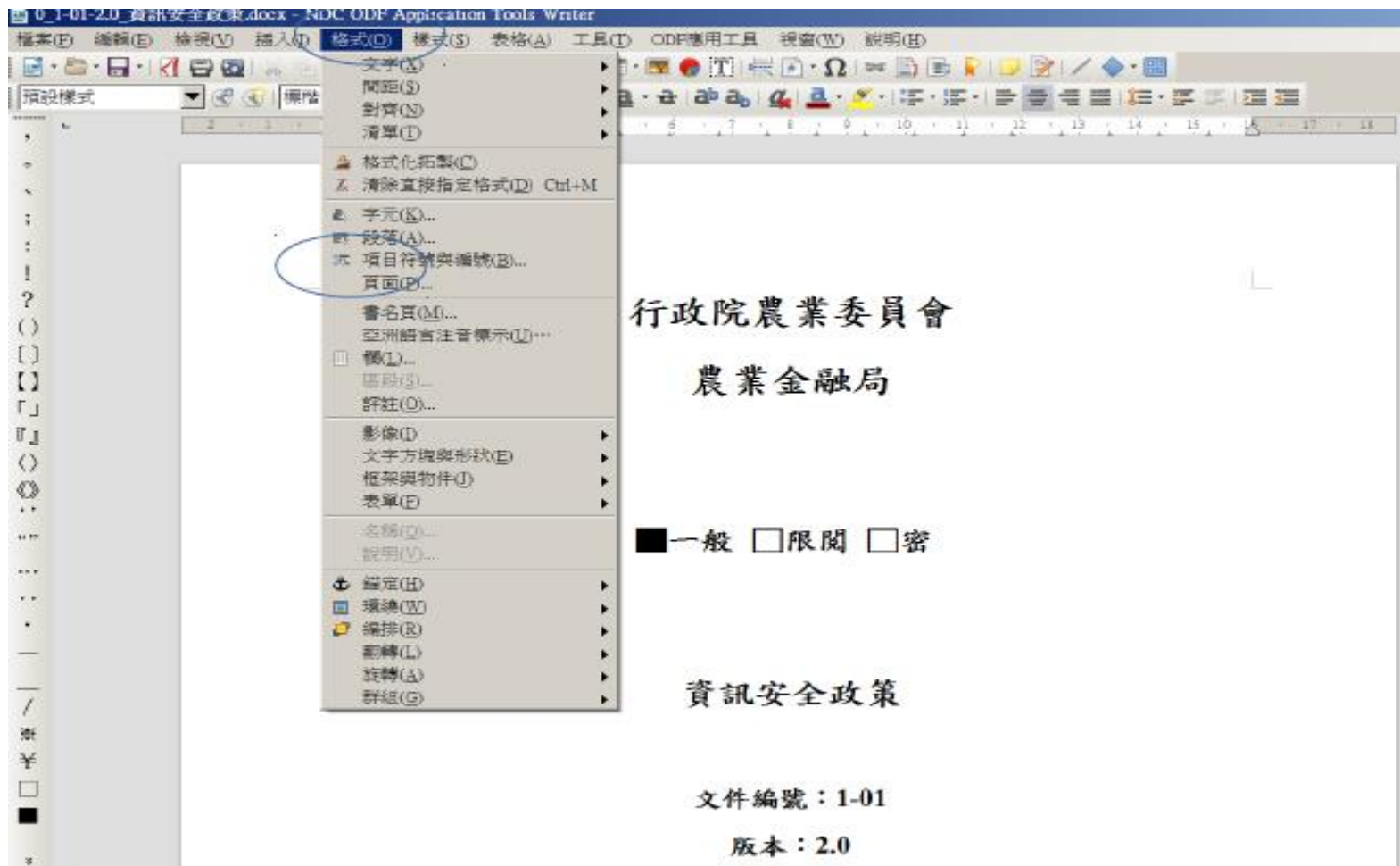


版本修訂紀錄表

文件版本	修訂日期	修訂內容	修訂單位
1.0	95.05.24	文件初版	第一組
1.1	100.05.02	修訂文件安全等級	第一組
1.2	102.01.24	增訂『七、(一).3.(4)重要系統日誌至少保存半年』	第一組

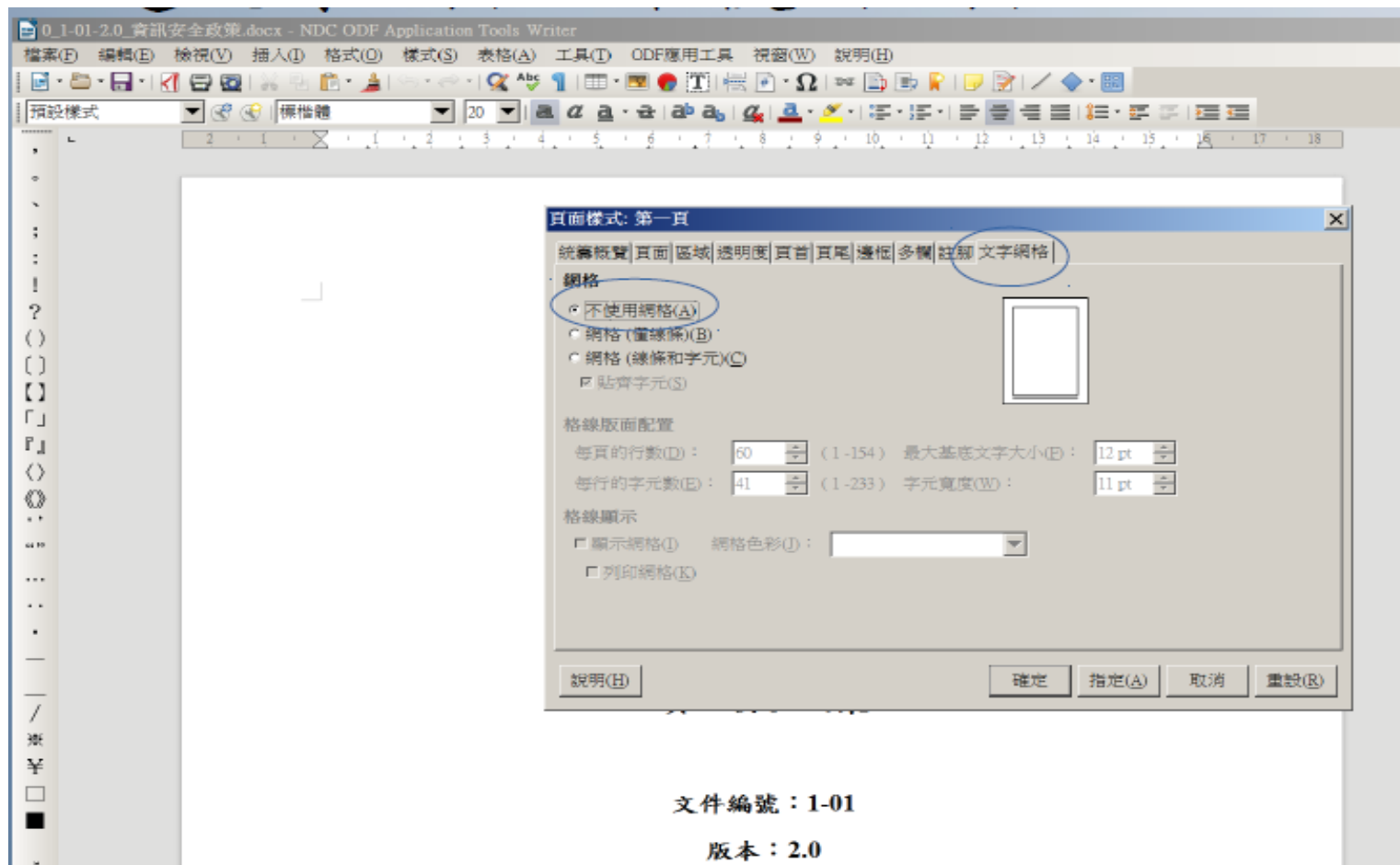
五 · 開啟檔案及調整格式

➤ 選格式\頁面



五 · 開啟檔案及調整格式

➤ 選文字網格\不使用網格



五 · 注意事項（二）

- 如果是xlsx（xls），請以Calc開啟xlsx（xls）檔案，用Calc存成.ods檔案。
- 如果是pptx（ppt），請以Impress開啟.pptx（或ppt）檔案，用Impress存成.odp檔案。
- 以上說明均適用於NDCODFApplicationTools、LibreOffice或OpenOffice，同仁可自行選擇。

五 · 注意事項（三）

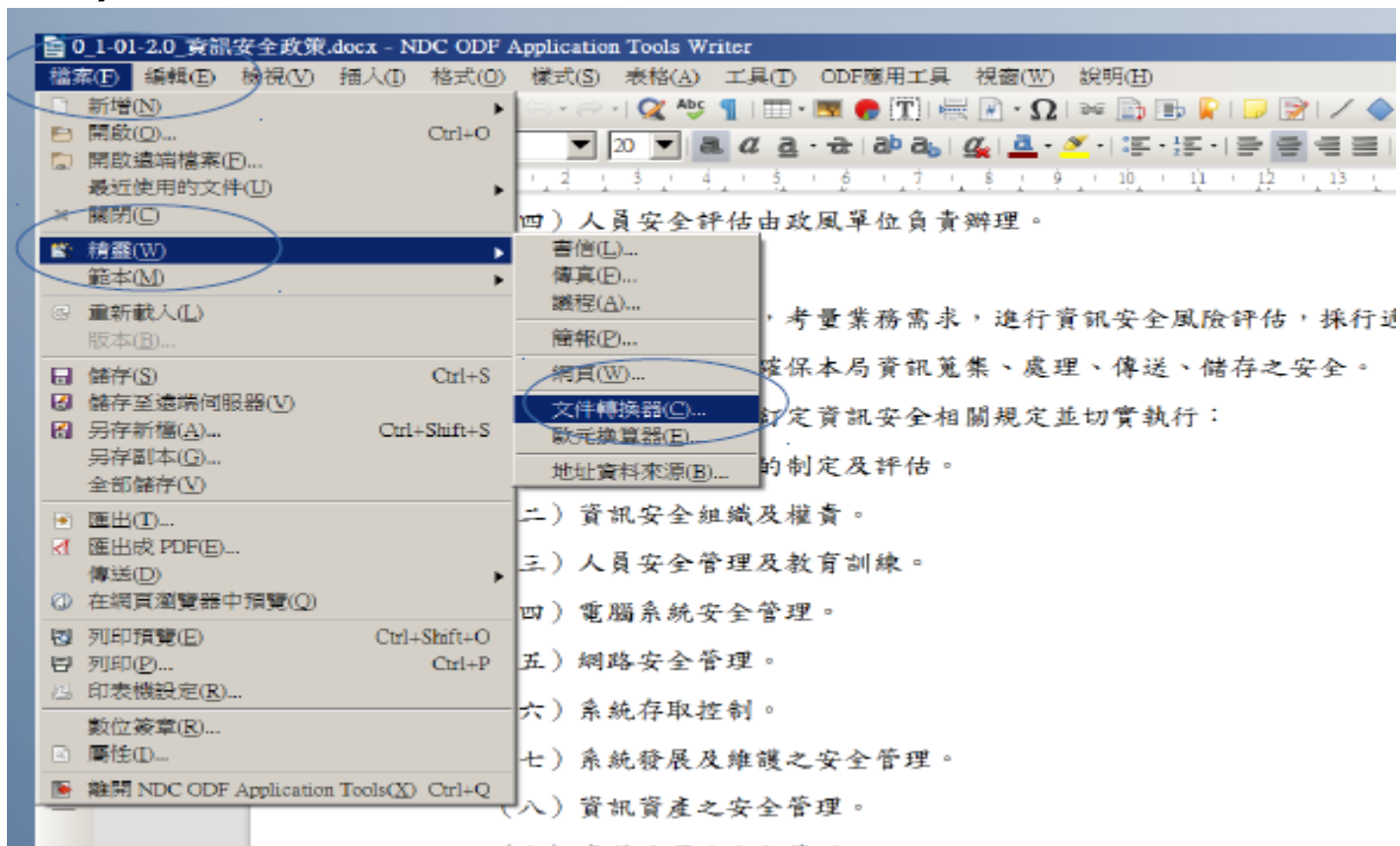
- 有許多OFFICE 2007之後的新功能轉換成ODF是會出錯的，而ODF功能與OFFICE 2003相容度較高，所以建議先將OFFICE 2007之後的檔案（docx、xlsx及pptx等），先轉存成OFFICE2003（doc、xls及ppt等），避免在轉成ODF時，因為不支援新功能而造成的異常問題，但是利用Office另存新檔功能來轉儲存成ODF文件，儲存後格式跑掉的情形比較嚴重，所以轉檔還是建議使用ODF軟體，像是NDCODFApplicationTools、LibreOffice或OpenOffice來做轉檔會比較穩定，在存檔時預設的檔案類型即為ODF格式。

五 · 批次轉檔示範

- 多檔案同時需要轉換為ODF格式時，可利用工具協助批次轉檔。
- 前置作業：建議可建一個暫存目錄（如AAA），將欲轉為ODF格式檔之MS-Office各種檔案（如docx、xlsx及pptx等）先存入該目錄，再建一個暫存目錄（如BBB），用來放置轉為ODF格式檔之檔案。

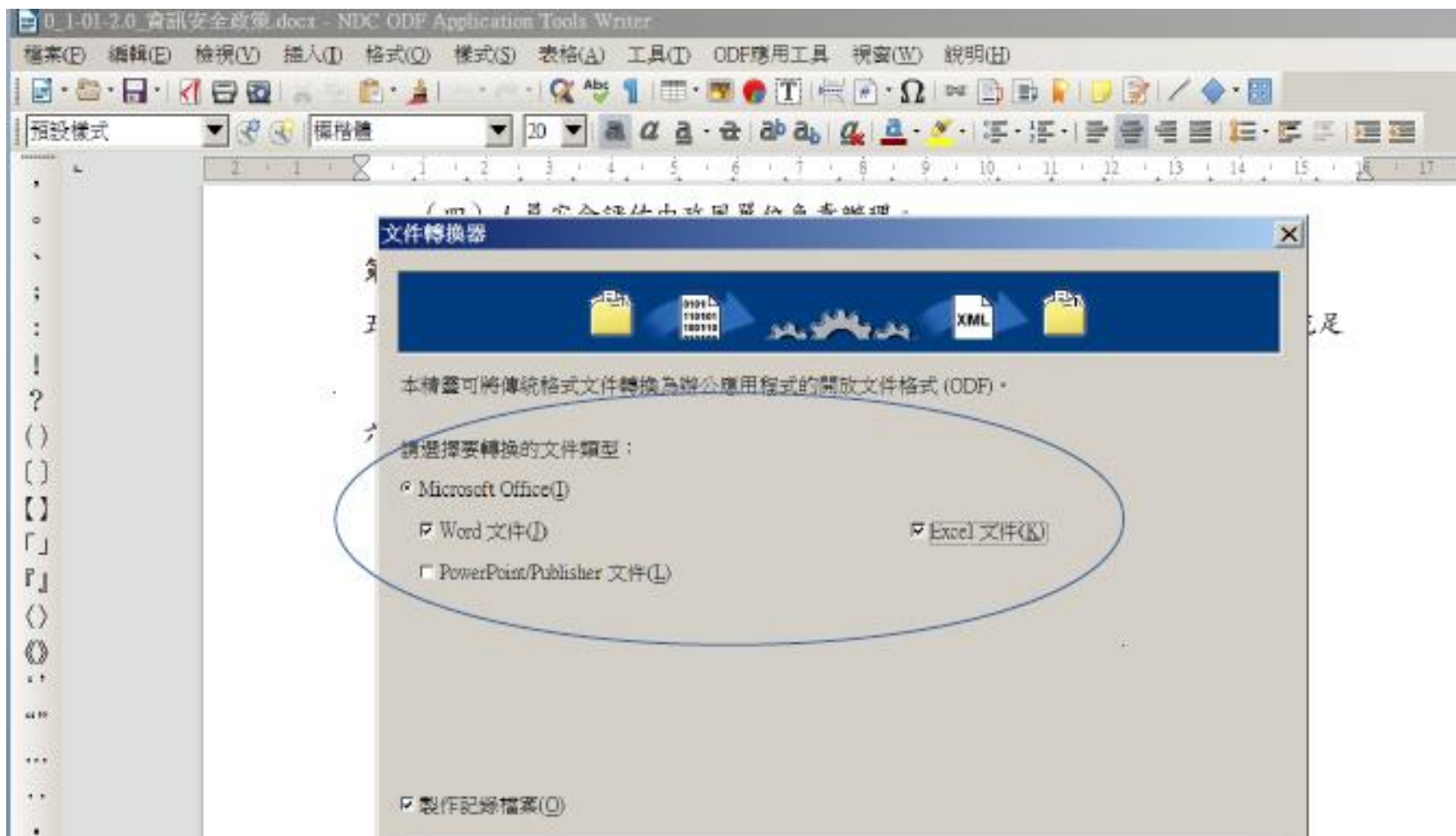
五 · 批次轉檔示範

- 選檔案>精靈>文件轉換器 (以國發會 NDCODFApplicationTools 為例，Openoffice 請選擇文件篩選器)



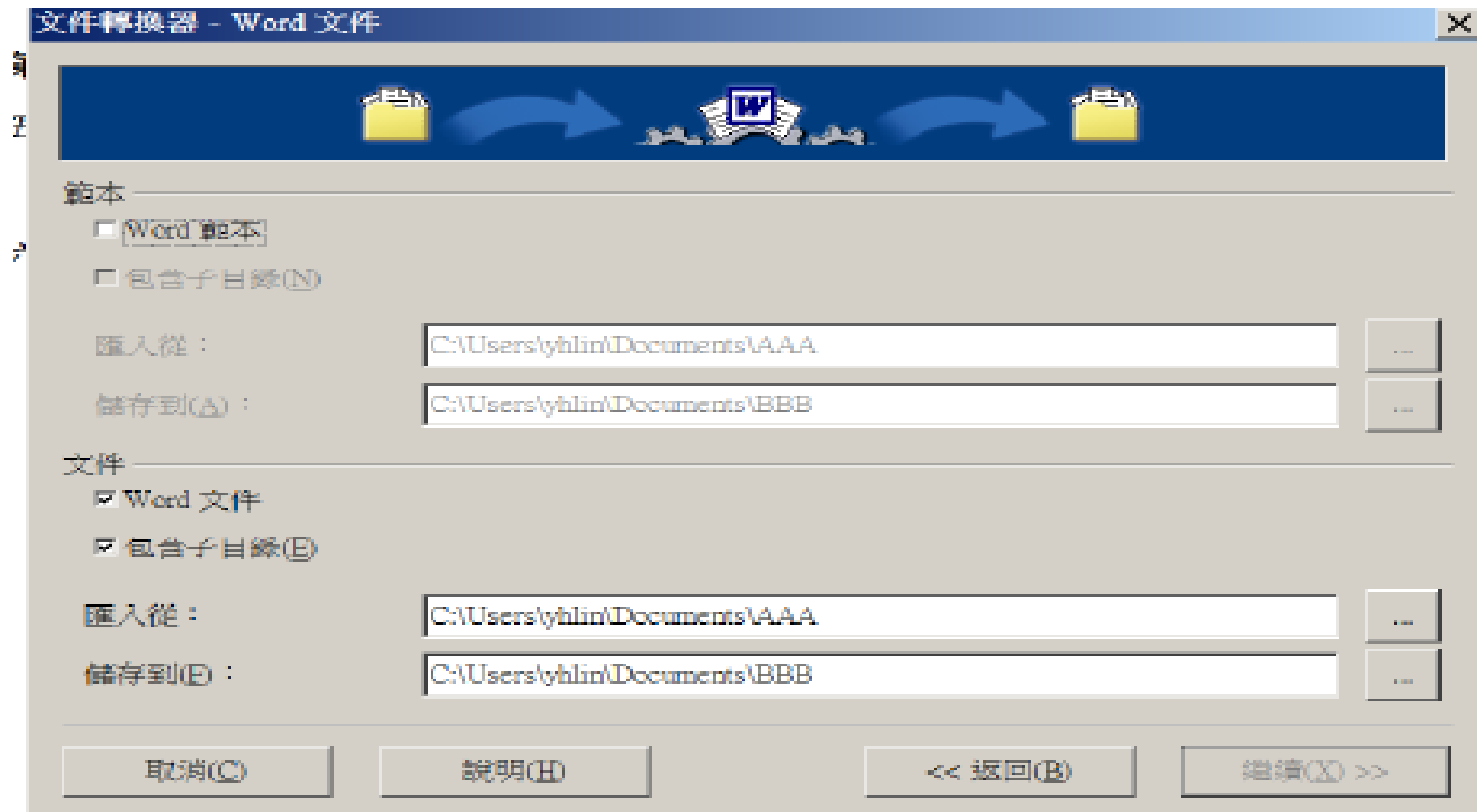
五 · 批次轉檔示範

- 選擇想要轉換之文件類型後，按繼續



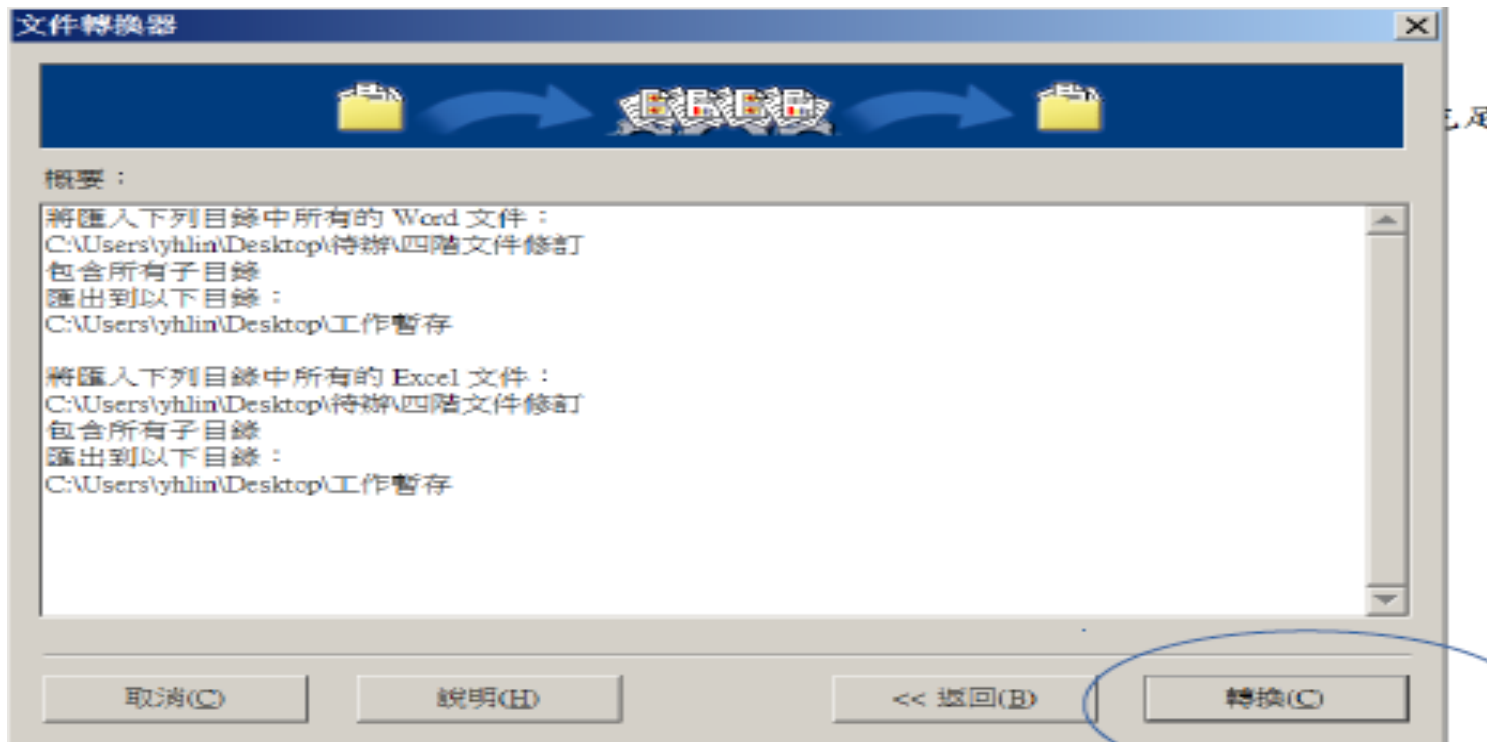
五 · 批次轉檔示範

- 文件>勾選word文件及包含子目錄>然後在「匯入」輸入剛剛存入檔案之AAA目錄之路徑，在「儲存到」輸入剛剛建好之AAA目錄之路徑，按繼續



五 · 批次轉檔示範

- 如果AAA目錄中有多種格式（如docx、xlsx或pptx），精靈會自動判斷，並會出現前述對話框（只是原本word文件處會變成EXCEL或POWERPOINT文件），請依前述方式輸入檔案路徑即可，全部輸入完，系統會出現以下對話框，按「轉換」就開始批次轉檔。



五 · ODF結語

- 若以微軟Office建立文件時，如有轉檔需求時，應儘量避免使用特殊功能（如SmartArt、巨集或3D動畫等）。
- 批次轉檔後，請打開檔案確認文字及格式是否正確，作適當之微調。
- NDCODFApplicationTools、LibreOffice或OpenOffice為免費軟體，功能上已可應付日常工作所需，同仁在家亦可自行下載安裝使用，可省掉購買微軟Office的費用，推行ODF格式檔案，是國家政策，便於未來資料交換，建議同仁爾後直接以ODF的免費軟體編輯文件，省去轉檔困擾。

農委會農業金融局

六 · Q&A



TSC – FB Site



TSC – Blog Site

