



政府機關資安弱點通報機制(VANS) 實作訓練

行政院國家資通安全會報技術服務中心

課程簡介

- 本單元課程時間總計**3**小時
- 目標：協助機關具備執行資訊資產弱點管理與安全性更新管理之能力
- 課程重點
 - 資訊資產弱點管理說明與實作
 - 安全性更新管理說明與實作
- 實作產出
 - 資訊資產弱點管理實作結果
 - 安全性更新管理實作結果

課程行政事項

- 上課時間安排
 - 09:00~09:15：政府機關資安弱點通報系統說明
 - 09:15~11:30：政府機關資安弱點通報系統實作
 - 11:30~12:00：問題討論
- 課程進行中，為確保學習效果請勿使用3C產品
- 本課程含公務人員終身學習時數3小時，請記得簽到
- 上課中有任何需求，請告知行政人員或講師

課程大綱

- 前言與法規政策說明
- 政府機關資安弱點通報系統說明
- 政府機關資安弱點通報系統實作
 - 資訊資產與已安裝KBID盤點作業
 - 資訊資產與已安裝KBID正規化作業
 - 實作練習1
 - 資訊資產與已安裝KBID登錄作業
 - 實作練習2
 - 弱點通知與修補作業
 - 實作練習3
 - 資訊資產與已安裝KBID更新作業
 - 實作練習4

課程大綱

- 前言與法規政策說明
- 政府機關資安弱點通報系統說明
- 政府機關資安弱點通報系統實作
 - 資訊資產與已安裝KBID盤點作業
 - 資訊資產與已安裝KBID正規化作業
 - 實作練習1
 - 資訊資產與已安裝KBID登錄作業
 - 實作練習2
 - 弱點通知與修補作業
 - 實作練習3
 - 資訊資產與已安裝KBID更新作業
 - 實作練習4

前言

- 不定期爆發之重大弱點，若未能即時反應，將嚴重影響機關業務正常運作，亦可能造成機關形象受損
- 當弱點爆發時，如能確實掌握機關資通系統與使用者電腦情況，即可快速因應，將損害降至最低

快速反應

- 如何在弱點發布後，快速反應所面臨的威脅與掌握受影響版本

確認範圍

- 如何在確認受影響版本後，可確實掌握受影響範圍

應變處理

- 如何在確認受影響範圍後，快速因應處理

事後追蹤

- 如何在應變處理後，持續追蹤弱點修補情形

資通安全管理法相關規定(1/3)



- 資通安全管理法第十條/第十六條第二項
 - 公務機關/關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施**資通安全維護計畫**
- 資通安全管理法施行細則第六條規範資通安全維護計畫應包含之項目
 - 第六款規範機關應**盤點資通系統**，並標示核心資通系統與相關資產
 - 第七款規範機關應**建立相關風險評估機制**，以針對盤點之資產進行資通安全風險評估

資通安全管理法

政府機關

- **Windows**平台**資通系統**與**使用者電腦**之**軟體**資產

- Windows平台資通系統與使用者電腦之**硬體**資產
- 類Unix平台資通系統與使用者電腦之**軟、硬體**資產
- 辦公室事務設備之**韌體**資產

弱點告警方式



弱點比對通知



重大漏洞
警訊通知

資通安全管理法相關規定(2/3)



- 依「資通安全責任等級分級辦法」，資安責任等級A級、B級、C級之公務機關及關鍵基礎設施提供者應導入資安弱點通報機制

制度面向	辦理項目	資安責任等級	辦理內容
技術面	資安弱點通報機制	A、B級 公務機關	一、初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料
		A、B級 特定非公務機關	一、關鍵基礎設施提供者初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式完成提交資訊資產盤點資料 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料

資通安全管理法相關規定(3/3)



制度面向	辦理項目	資安責任等級	辦理內容
技術面	資安弱點通報機制	C級 公務機關	<p>一、初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料</p> <p>二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料</p>
		C級 特定非公務機關	<p>一、關鍵基礎設施提供者初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料</p> <p>二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料</p>

國家資通安全發展方案

- 「**國家資通安全發展方案(110年至113年)**」策略三之「**1-2 建立資通系統弱點之主動發掘、通報及修補機制**」工作項目之分年重要進程

110年

- A級公務機關完成導入資安弱點通報機制

111年

- B級公務機關完成導入資安弱點通報機制
- A級CI提供者完成導入資安弱點通報機制

112年

- C級公務機關完成導入資安弱點通報機制
- B級CI提供者完成導入資安弱點通報機制

113年

- C級CI提供者完成導入資安弱點通報機制

課程大綱

- 前言與法規政策說明
- 政府機關資安弱點通報系統說明
- 政府機關資安弱點通報系統實作
 - 資訊資產與已安裝KBID盤點作業
 - 資訊資產與已安裝KBID正規化作業
 - 實作練習1：資訊資產正規化
 - 實作練習2：已安裝KBID正規化
 - 資訊資產與已安裝KBID登錄作業
 - 實作練習3：資訊資產登錄
 - 弱點通知與修補作業
 - 資訊資產與已安裝KBID更新作業
 - 實作練習4：弱點修補規劃與更新
 - 實作練習5：已安裝KBID更新

政府機關資安弱點通報機制

- 政府機關資安弱點通報機制(Vulnerability Alert and Notification System, VANS)結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實資通安全管理法之資產盤點與風險評估應辦事項
 - 定期蒐集資通系統與電腦所使用之資訊資產項目及版本，建立資訊資產清冊，以達到降低風險與管控成本等目標
 - 將資訊資產清冊與弱點資料庫比對，以掌握所使用資訊資產是否存在已公開揭露之弱點資訊



● 確認資訊資產弱點

- 蒐集政府機關使用之軟體資訊，並與國際權威弱點資料庫進行比對，當使用軟體存在重大弱點時，即時得知與應變處理

● 降低重大弱點管控與追蹤之成本

- 利用弱點資料庫搭配自動比對方式，提供政府機關相關弱點資訊與自我檢查機制

● 追蹤資訊資產弱點修補情形

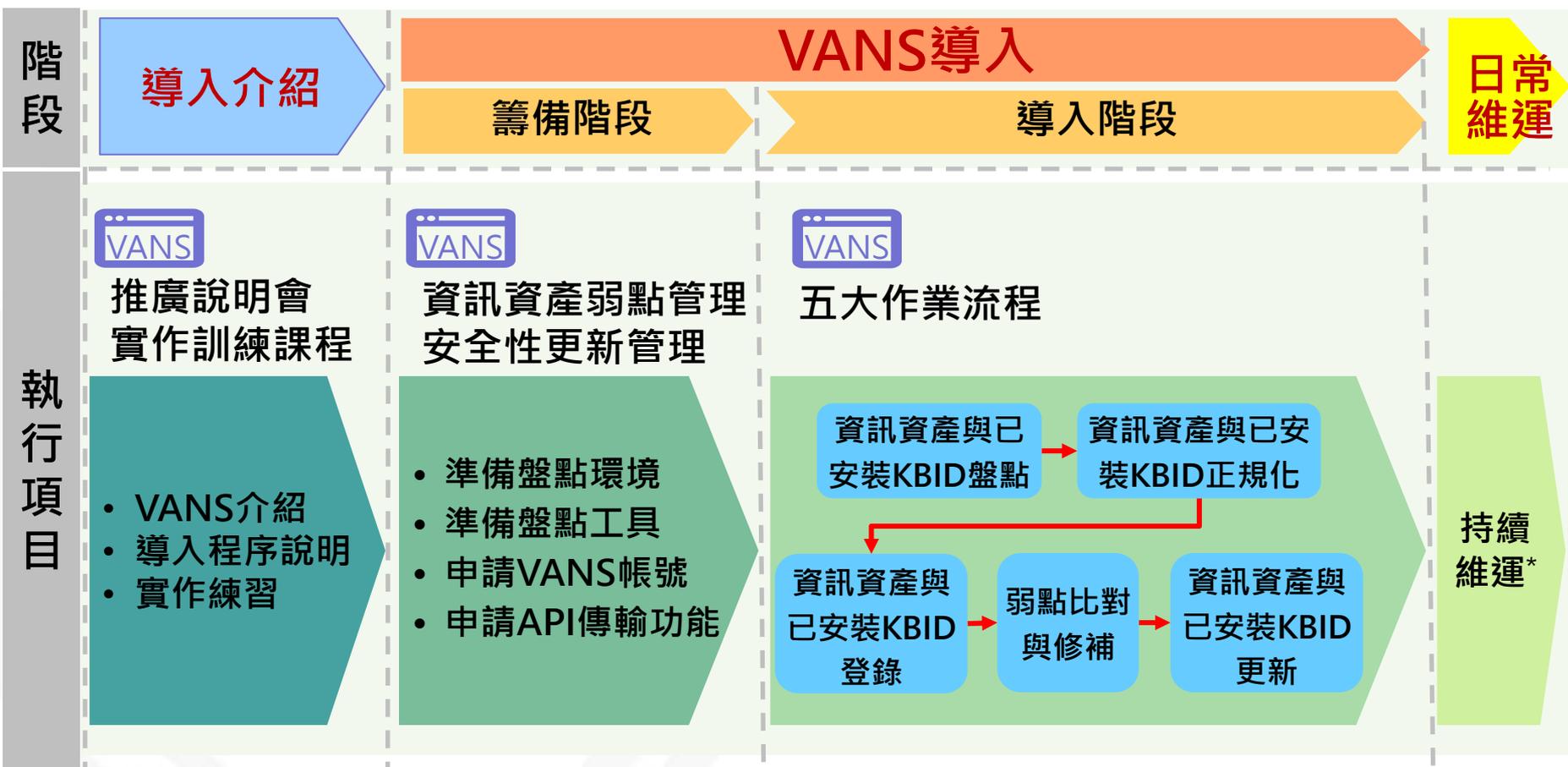
- 依照機關訂定之風險值門檻，及時提醒資訊資產風險情形，並進行弱點評估與修補作業

● 強化安全性更新落實情形

- 搭配上傳已安裝安全性更新，以協助機關確認微軟資產之安全性更新缺漏項目，更精準呈現微軟弱點修補情形



VANS機制導入作業流程

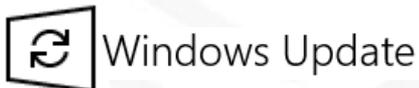
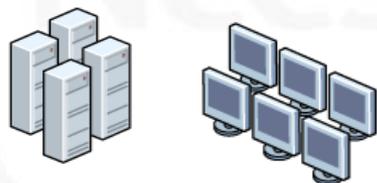


*持續維運：包含定期執行及不定期執行(例如資產異動時)

系統介紹



- VANS系統提供機關登錄資訊資產，藉由系統自動與NVD弱點資料庫比對，羅列出資訊資產之弱點，俾利機關掌握可能面臨之資安風險，以強化資訊資產之資安管理



政府機關資安弱點通報系統 (VANS)

[一般權限帳號登入](#) [機關管理者帳號登入](#)

公告
為提升安全性，本系統已將HTTPS加密等級提升至TLS 1.1以上，再請留意瀏覽器需支援TLS 1.1以上方可瀏覽本系統，謝謝。

聯絡資訊如下：
行政院國家資通安全會報技術服務中心(技服中心)
服務電話：(02)6631-6458
服務信箱：VansService@nccst.nat.gov.tw

機關管理者帳號

iAuth個人帳號

密碼

[登入](#) [申請個人帳號](#) [忘記密碼](#)

資訊資產盤點標的

- 蒐集範圍：Windows平台資通系統與使用者電腦之軟體資產



應用程式

應用程式或網站伺服器

程式語言執行環境

網站採用第三方元件

開發框架

資料庫

- Adobe
- Apache

- Microsoft Office
- ...



作業系統

Windows Server

Windows

Windows Server 2012 R2

Windows Server 2016 Datacenter

Windows 8

Windows 10 Professional

- 軟體名稱
- 開發廠商名稱

- 版本資訊
- 軟體安裝數量

資訊資產呈現方式(1/2)

- **Common Platform Enumeration(簡稱CPE)**，為美國國家標準技術研究所(NIST)所提出標準化方式，用以描述與識別企業內的應用程式、作業系統及硬體設備等資訊資產，最新版本為2.3
- **CPE條目格式**
 - 主要分為三大類：作業系統(o)、應用程式(a)及硬體(h)
 - 主要資訊：廠商名稱(vendor)、產品名稱(product)、產品版本(version)、產品更新(update)、產品版次(edition)、語系(language)

弱點呈現方式

- Common Vulnerabilities and Exposures(簡稱 CVE)羅列各種資安弱點，並給予編號以便查閱
- CVE目標為將所有已知弱點與相關風險資訊標準化，俾利於各個弱點資料庫與安全工具之間統一弱點相關資料
- 現由美國非營利組織MITRE所屬之National Cybersecurity FFRDC負責營運維護
- 每一個CVE都賦予一個專屬編號，格式如下：

-CVE-YYYY-NNNN

西元紀年 流水號

- **National Vulnerability Database(簡稱NVD)**為NIST所建置，專門用來蒐集各種弱點資訊之資料庫網站
 - 自MITRE取得CVE列表，並增加修補建議連結、嚴重性評分(CVSS分數)及影響等級等資訊
 - 建立CPE與CVE對應關係，以解決弱點與資訊資產之對應關係
 - VANS系統每天更新1次資產與弱點資訊

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

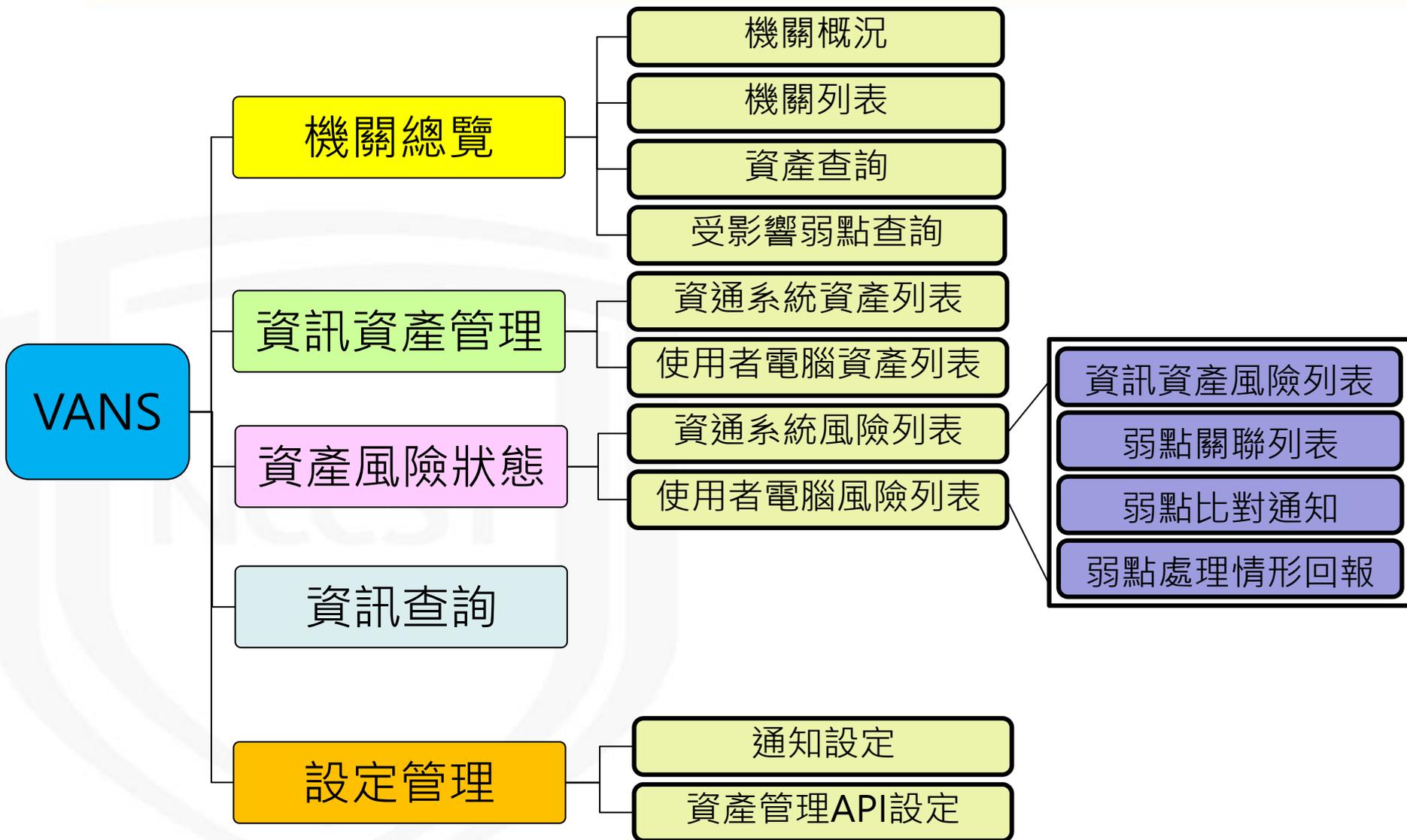


微軟安全性更新

- 微軟系列軟體之弱點多數透過安裝安全性更新進行修補，而不會改變軟體版本資訊
 - CPE條目僅包含軟體版本等資訊，無法有效判斷是否完成弱點修補
- 藉由盤點已安裝安全性更新(KBID)，以了解資通系統與使用者電腦安全性更新實際情況
 - 協助管理者**確認微軟系列產品安全性更新缺漏項目**，以強化**安全性更新落實情形**
 - 重大弱點爆發時，可**確認未安裝安全性更新之資通系統與使用者電腦數量與範圍**，並進行應變處理



系統功能總覽



系統介面說明

系統名稱

全螢幕 登出

政府機關資安弱點通報系統



登入人員

機關總覽 > 機關概況

功能路徑

顯示/隱藏
功能選單列

- 首頁
- 機關總覽
 - 機關概況
 - 機關列表
 - 資產查詢
 - 受影響弱點查詢
- 資訊資產管理
- 資產風險狀態
- 資訊查詢
- 設定管理

功能選單列

功能頁面

檢視方式

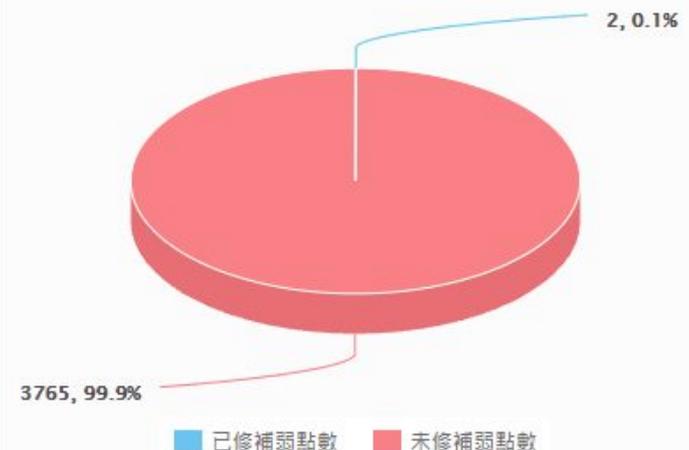
資通系統

使用者電腦

資通系統資產類別統計



資通系統弱點處理情形(CVE)



服務申請流程

聯絡資訊
服務電話：(02)6631-6458
服務信箱：VansService@nccst.nat.gov.tw



申請個人帳號

- 於iAuth系統申請個人帳號

資安人員身分驗證系統(iAuth系統)
<https://www.ncert.nat.gov.tw/iAuth2/>



機關提出申請

- 於iAuth系統提出**VANS**帳號申請
- 於VANS專區下載並填寫**機關管理者帳號申請(異動)單**，完成後Email予資安處



參閱操作手冊

- 操作諮詢
- 服務說明

技服中心VANS專區
<https://www.nccst.nat.gov.tw/Vans?lang=zh>



開始使用服務

- 資料建立
- 弱點比對

VANS系統
<https://vans.nccst.nat.gov.tw/>

VANS帳號管理(1/2)

● 管理者帳號權限異動

- 單一機關至多**2個**機關管理者帳號
- 有異動需求時，請填寫**機關管理者帳號申請(異動)單**，完成後Email予資安處，審核通過後，技服中心將協助進行後續處理

● 閒置帳號鎖定

- 若iAuth帳號長達**180天**未有登入行為，則將進入**鎖定狀態**，無法登入系統進行操作
- 重新啟用步驟如下圖

說明帳號遭閒置鎖定，並提供：

- 機關名稱
- iAuth帳號名稱
- 人員姓名
- 連絡電話
- Email



資料核對無誤後，協助啟用帳號



VANS帳號管理(2/2)

- 機關登入VANS系統分為下列兩種帳號

機關管理者帳號



- ✓ 檢視機關總覽
- ✓ 資訊資產與已安裝KBID管理
- ✓ 弱點管理
- ✓ 資訊查詢
- ✓ 檢視**機關各帳號**資產異動紀錄
- ✓ **申請API介接IP並重新產生API Key**

一般權限帳號



- ✓ 檢視機關總覽
- ✓ 資訊資產與已安裝KBID管理
- ✓ 弱點管理
- ✓ 資訊查詢
- ✓ 檢視**自身**帳號資產異動紀錄
- ✓ **檢視API Key**

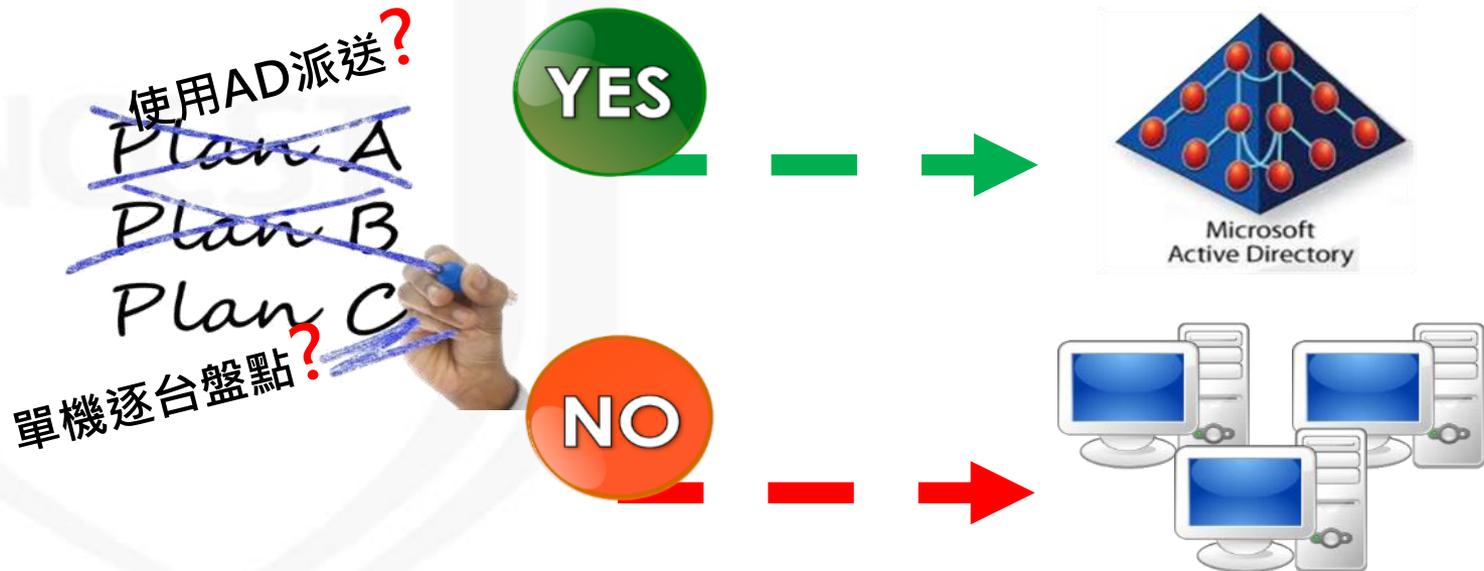
課程大綱

- 前言與法規政策說明
- 政府機關資安弱點通報系統說明
- 政府機關資安弱點通報系統實作
 - 資訊資產與已安裝KBID盤點作業
 - 資訊資產與已安裝KBID正規化作業
 - 實作練習1
 - 資訊資產與已安裝KBID登錄作業
 - 實作練習2
 - 弱點通知與修補作業
 - 實作練習3
 - 資訊資產與已安裝KBID更新作業
 - 實作練習4

執行規劃

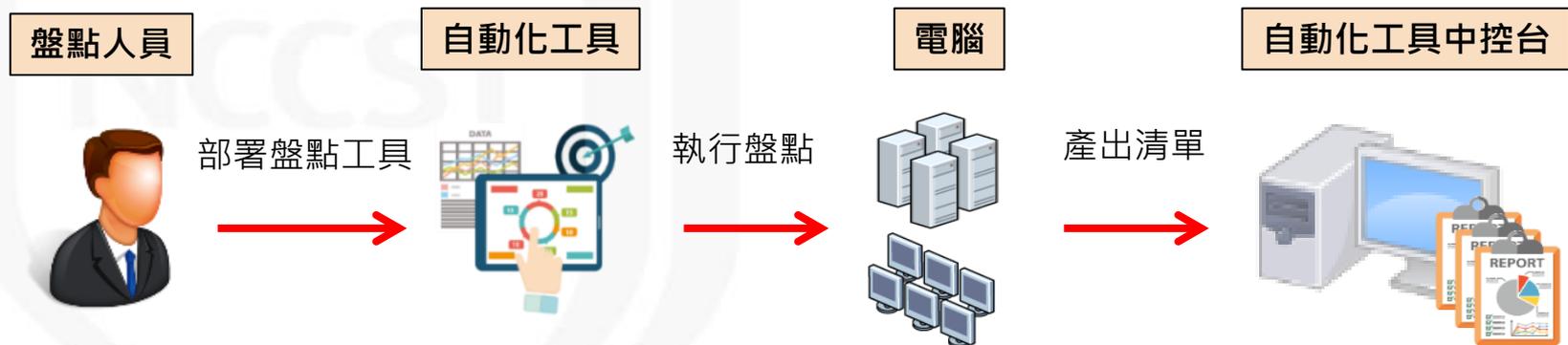
- 依據機關環境擬定導入執行規劃

- 執行範圍：本部/本部與所屬、資通系統/使用者電腦
- 執行時程：人力評估、導入測試起訖時間、正式導入起訖時間
- 執行方式：單機/AD派送GPO執行、第三方工具執行



情境說明(1/3)

- 定期透過**自動化工具**或**系統指令**進行資訊資產與已安裝KBID之盤點與正規化，以利後續可登錄至VANS系統
- 可依機關資訊環境自由選擇合適之**資料蒐集方式**
— 透過**自動化工具盤點**



情境說明(2/3)

—透過系統指令批次盤點

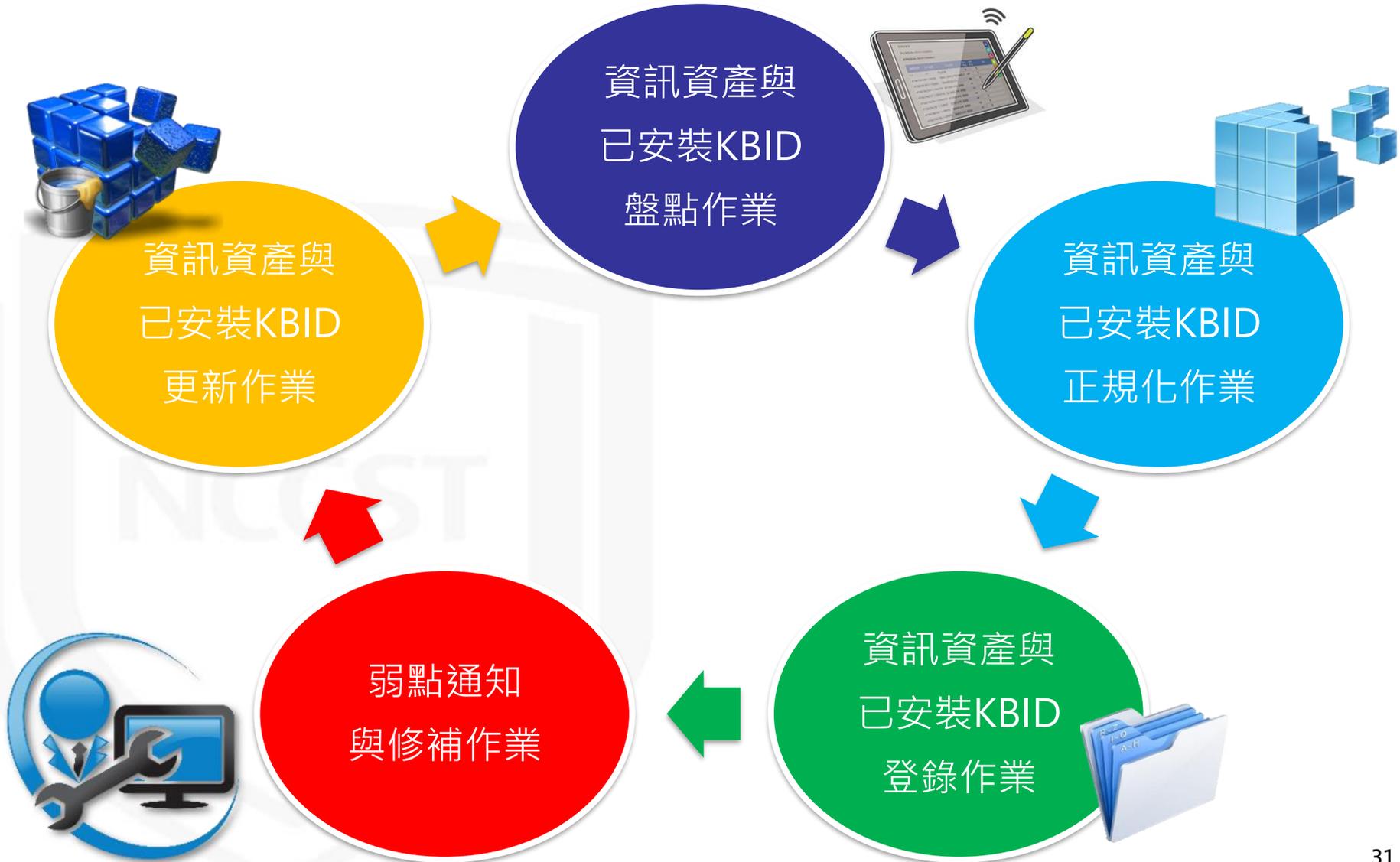


情境說明(3/3)

—透過系統指令單機盤點



導入作業流程



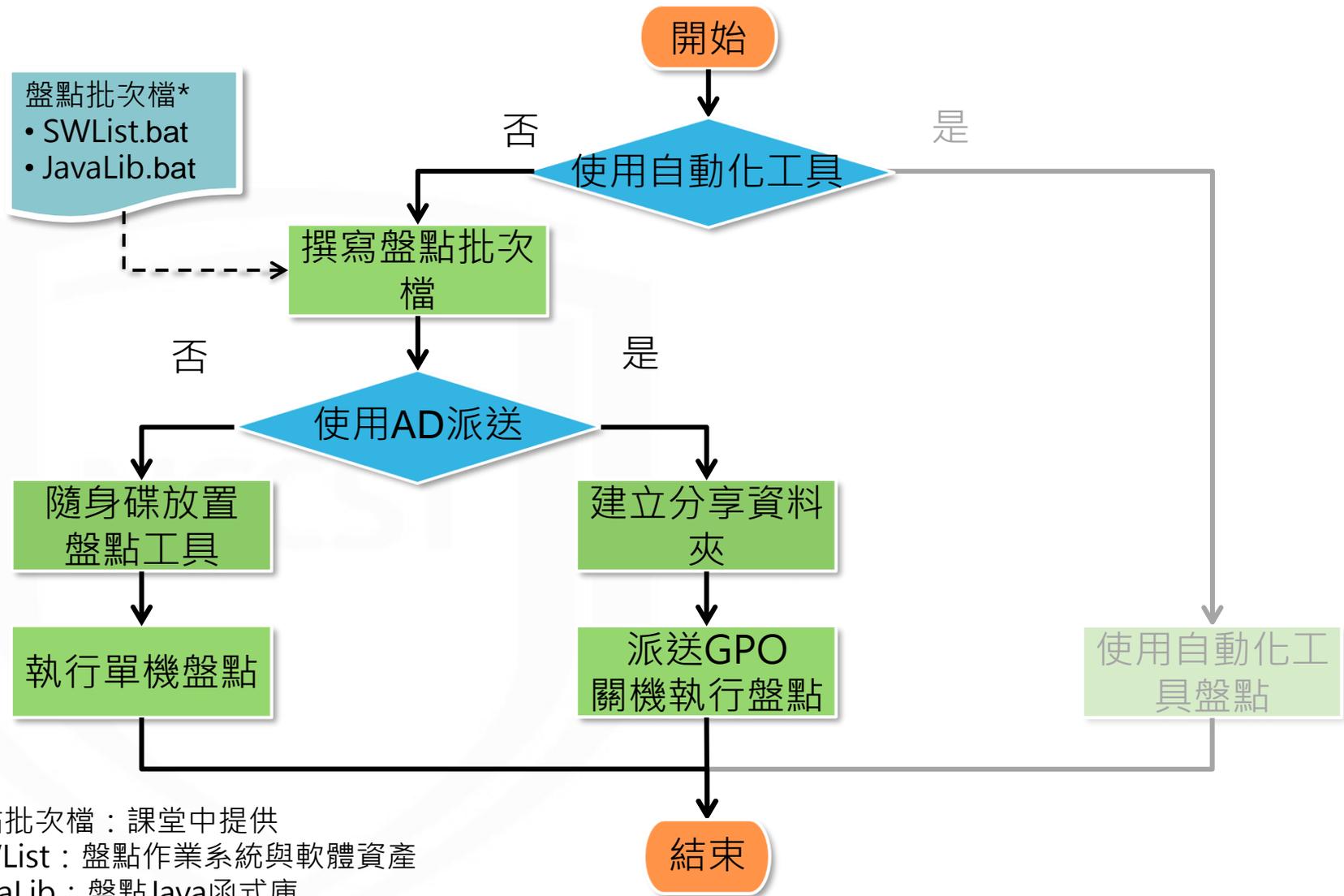
導入作業流程說明重點

編號	流程名稱	教材編排方式
1	資訊資產與已安裝KBID盤點作業	先說明手動盤點、正規化及登錄作業方式，再說明透過工具進行盤點、正規化及登錄作業方式
2	資訊資產與已安裝KBID正規化作業	
3	資訊資產與已安裝KBID登錄作業	
4	弱點通知與修補作業	說明透過VANS系統網頁介面進行修補與更新
5	資訊資產與已安裝KBID更新作業	

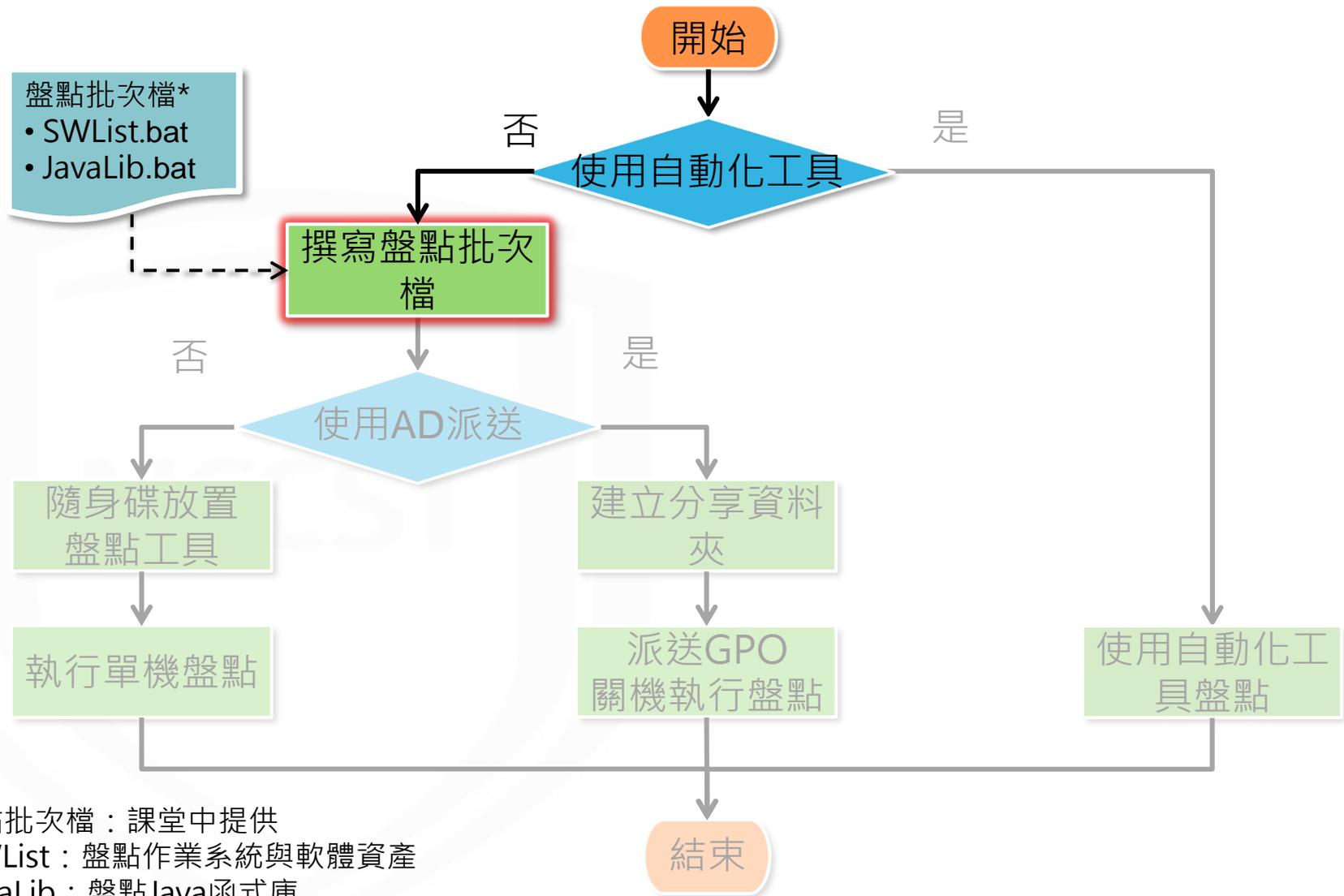
導入作業流程



盤點作業流程



盤點作業流程



*盤點批次檔：課堂中提供
1.SWList：盤點作業系統與軟體資產
2.JavaLib：盤點Java函式庫

撰寫盤點批次檔(1/2)

- 登錄機碼值(reg query)

- 藉由查詢登錄機碼值，可列出作業系統資訊、已安裝軟體清單及 Office 相關產品之已安裝 KBID

- Windows 管理工具(簡稱 WMI)

- 運用 Windows 平台作業系統進行檔案管理與操作之技術，讓使用者可透過 WMI 管理本機與遠端電腦，可用以盤點已安裝 KBID



撰寫盤點批次檔(2/2)

- 命令提示字元指令

- 若機關環境有使用Java函式庫時，可透過此批次檔執行盤點
- Tomcat Java函式庫路徑預設位置如下圖
 - cd C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\docs\WEB-INF\lib\

```
JavaLib_v1.0.bat
1 FOR /F "tokens=2 delims=[]" %%a in ('ping -4 -n 1 %computername% ^|
  findstr [') do set NetworkIP=%%a
2
3 rem ===切換至Java函式庫位置，準備執行盤點作業===
4 cd C:\Program Files\Apache Software Foundation\Tomcat
  9.0\webapps\docs\WEB-INF\lib\
5
6 rem ===列出Java函式庫，並產出csv格式檔案至公用文件資料夾===
7 dir *.* /S /B /ON > %~dp0\3.Javalib\3.javaoutput_%computername%_
  %DATE:~0,4%%DATE:~5,2%%DATE:~8,2%.csv
```



命令提示
字元指令



Java函式庫

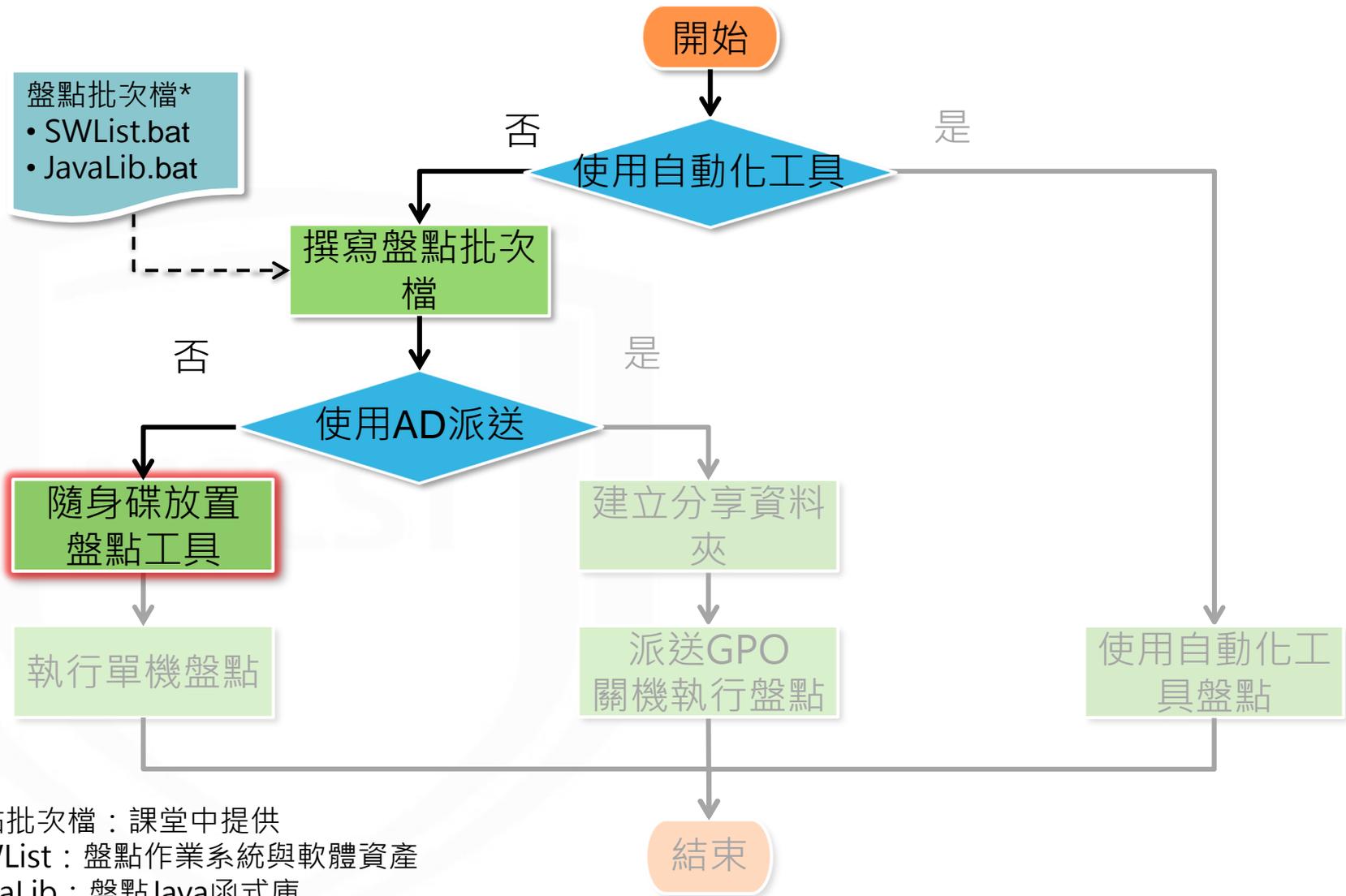


Java函式庫清單

透過系統指令單機盤點

NCCST

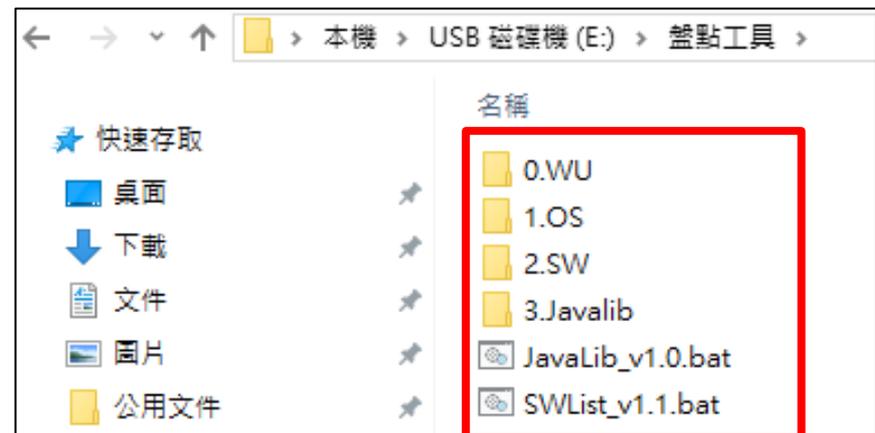
盤點作業流程



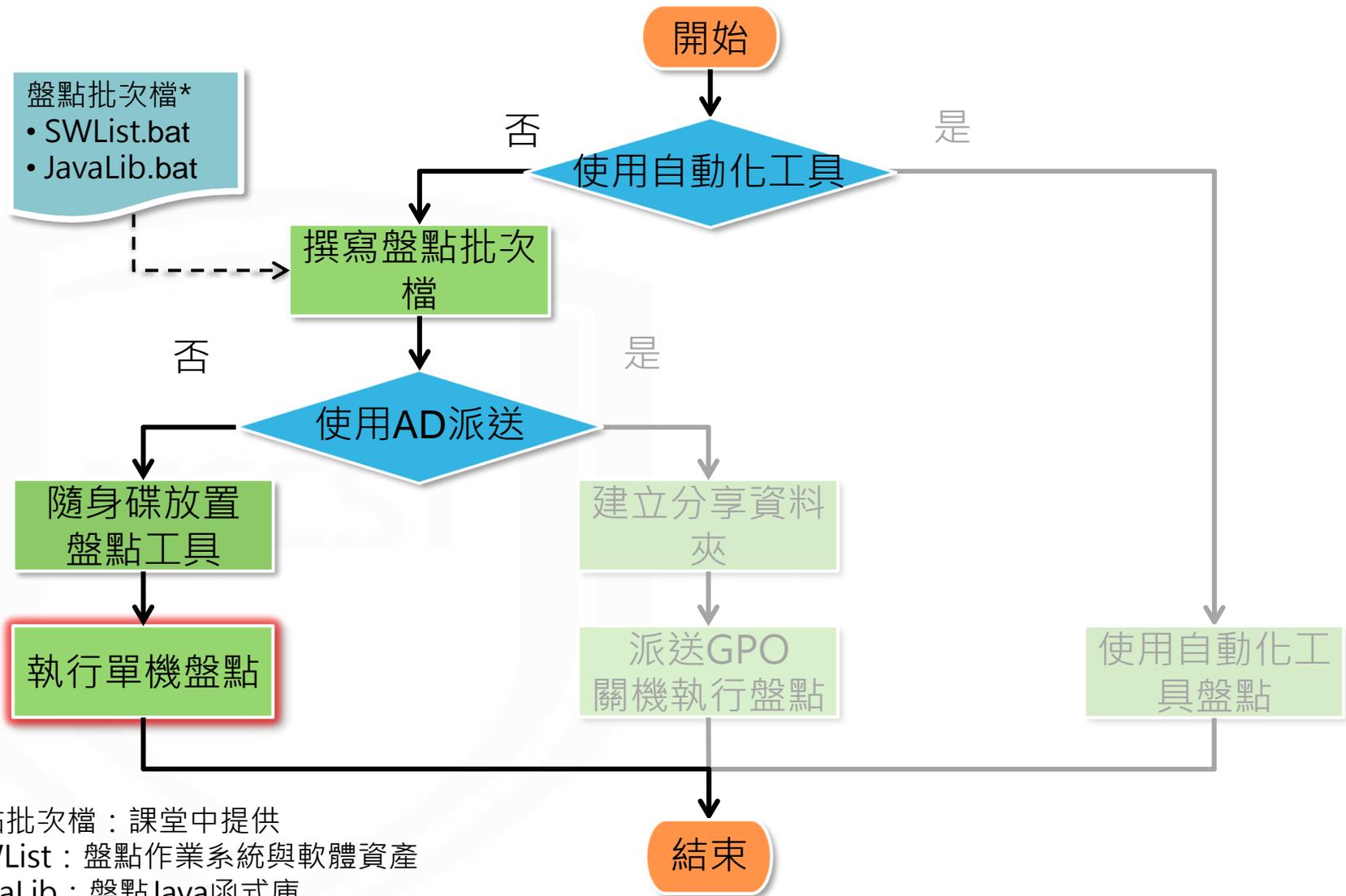
*盤點批次檔：課堂中提供
1.SWList：盤點作業系統與軟體資產
2.JavaLib：盤點Java函式庫

隨身碟放置盤點工具

- 於隨身碟建立資料夾放置盤點批次檔與存取結果資料夾，依欲盤點之資訊資產執行盤點批次檔。
 - SWList.bat：盤點作業系統、軟體及已安裝KBID
 - JavaLib.bat：盤點Java函式庫
 - 0.WU資料夾：存取已安裝安全性更新盤點清單之資料夾
 - 1.OS資料夾：存取作業系統盤點清單之資料夾
 - 2.SW資料夾：存取軟體資產盤點清單之資料夾
 - 3.JavaLib資料夾：存取Java函式庫盤點清單之資料夾

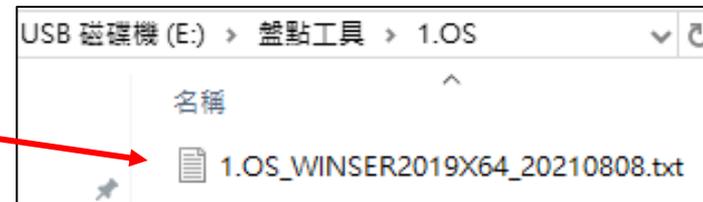
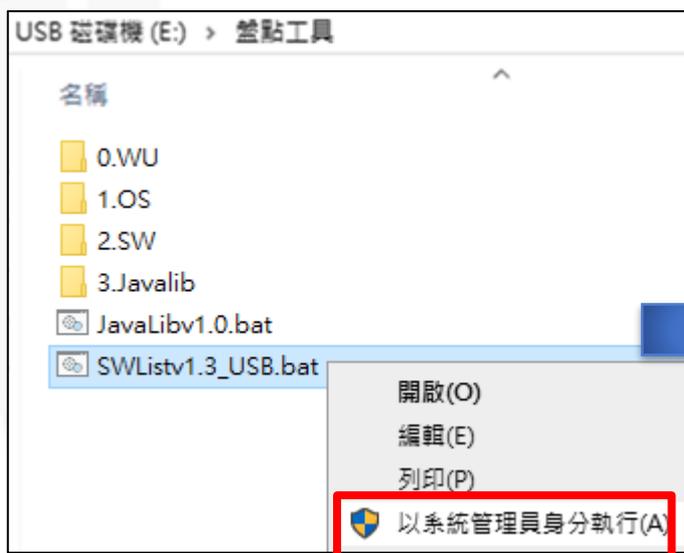


盤點作業流程



執行單機盤點(1/2)

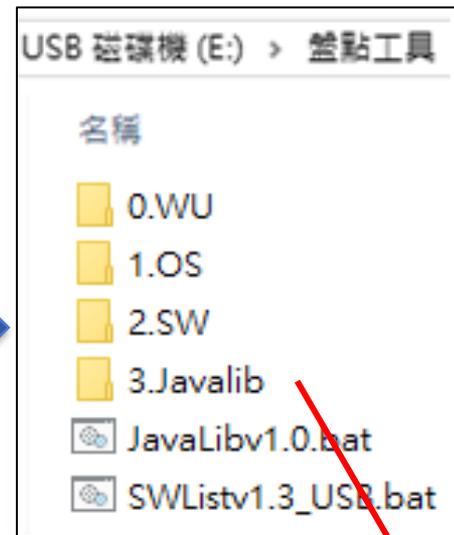
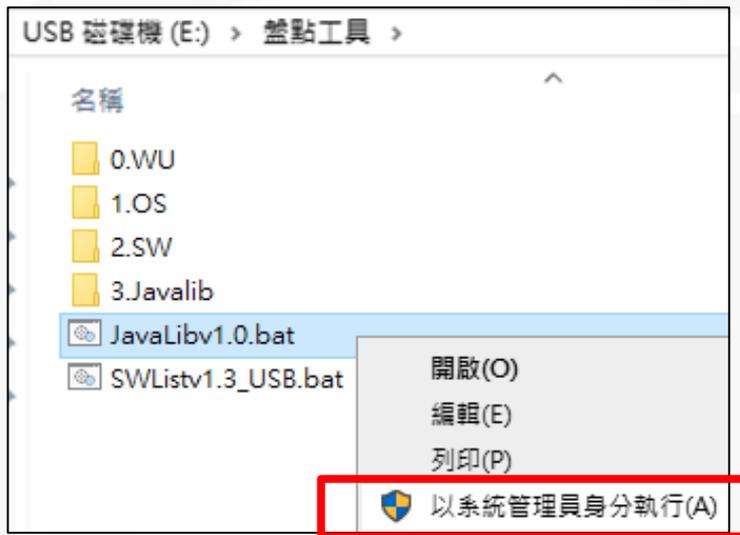
- STEP1：以系統管理員身分執行SWList批次檔
- STEP2：檢視盤點結果資料夾，分別為已安裝KBID清單、作業系統資訊及軟體盤點清單



盤點完成視窗自動關閉

執行單機盤點(2/2)

- STEP3 : 以系統管理員身分執行JavaLib批次檔
- STEP4 : 檢視盤點結果資料夾內含Java函式庫清單



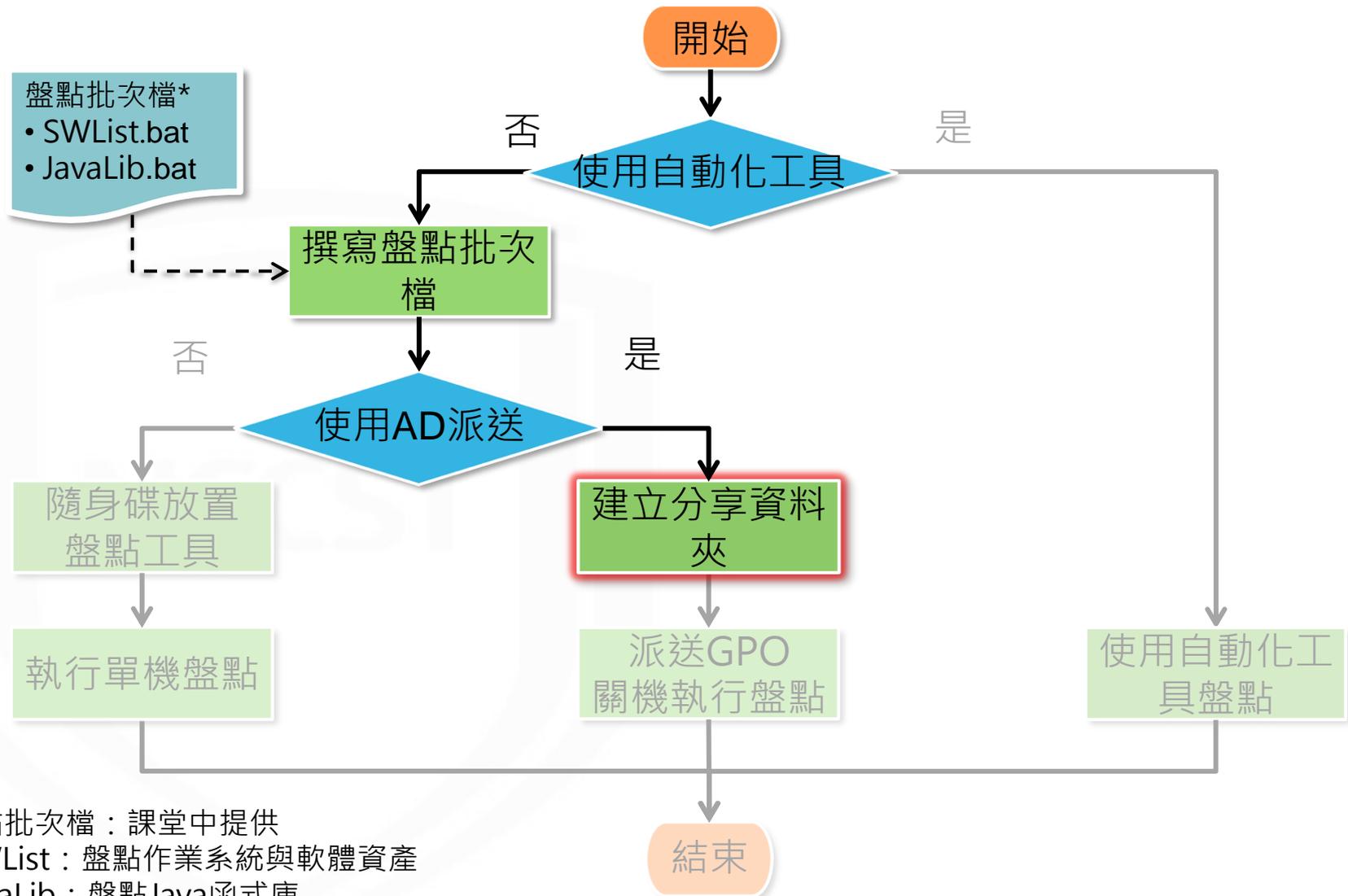
盤點完成視窗自動關閉



透過系統指令批次盤點

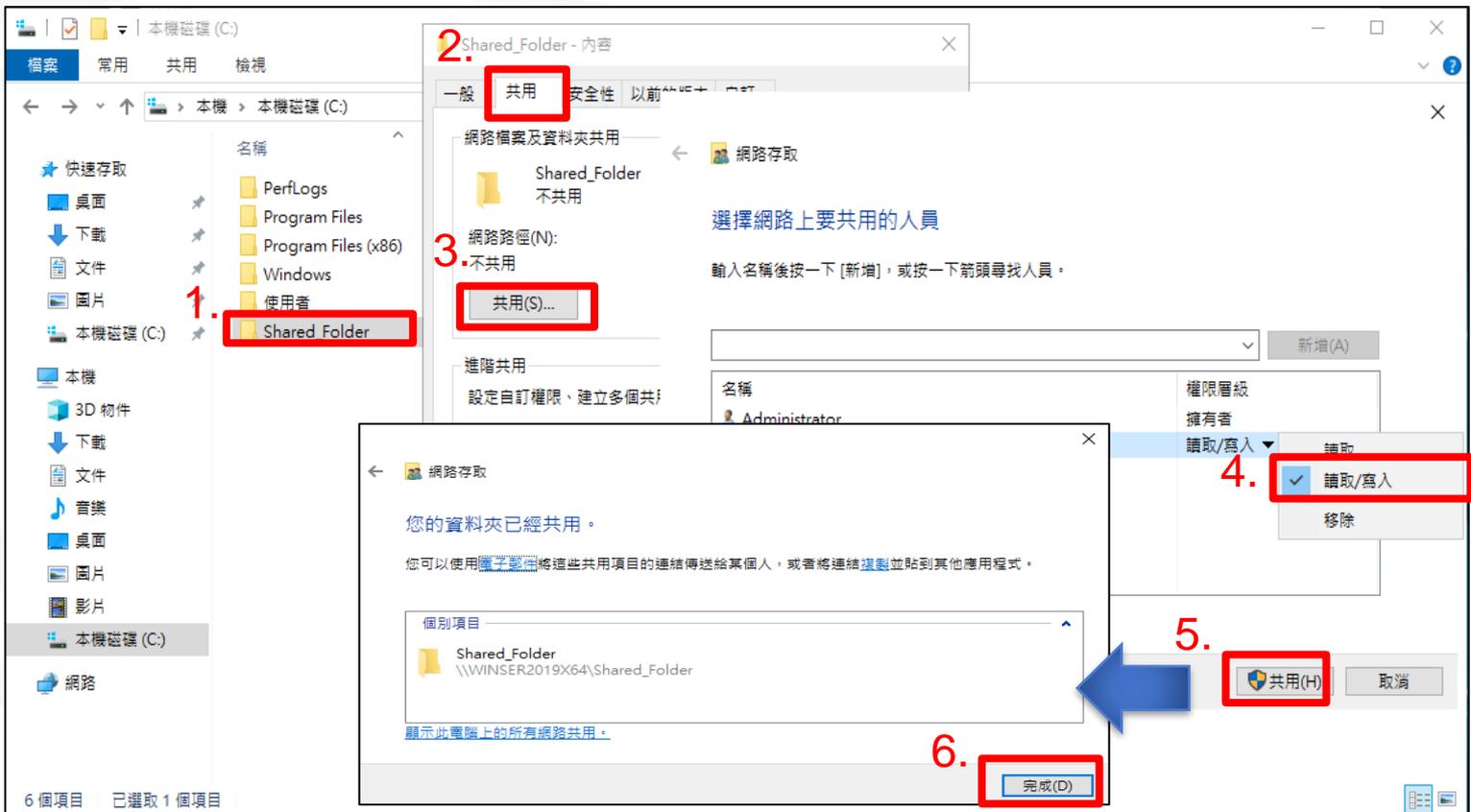
NCCST

盤點作業流程



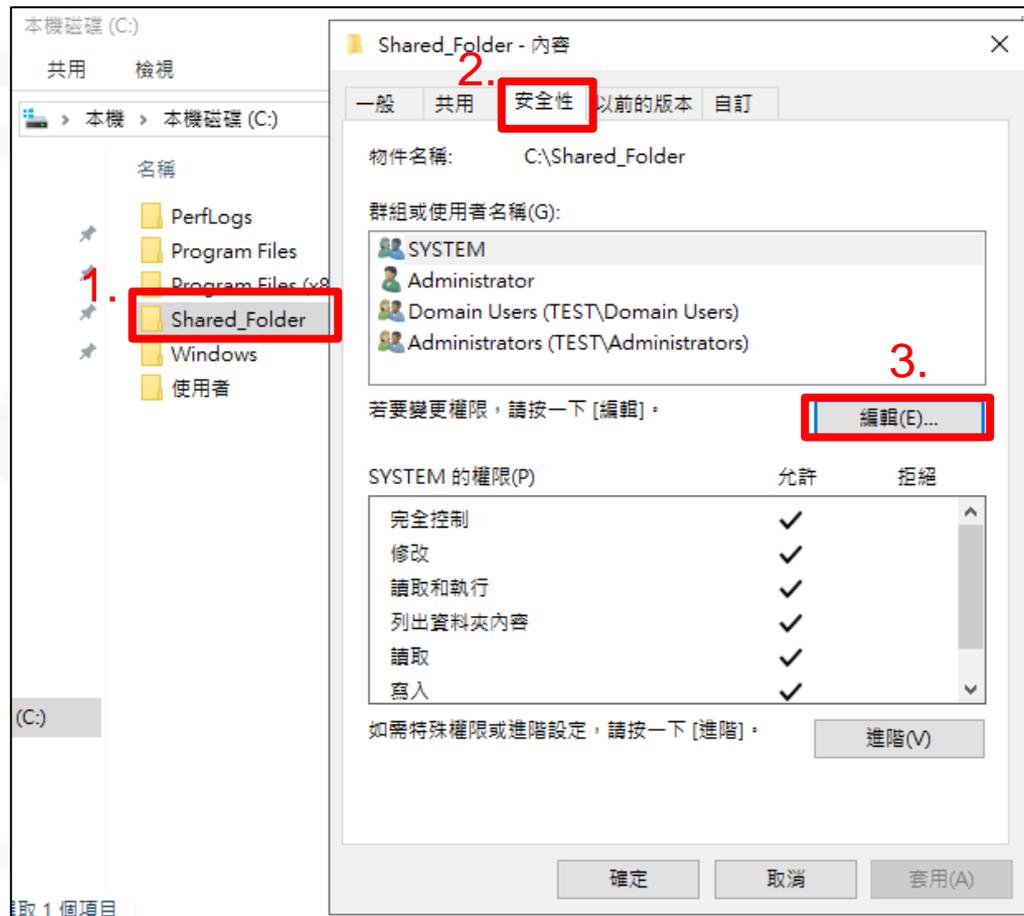
AD主機建立分享資料夾(1/3)

- STEP1：於AD主機建立分享資料夾(Shared_Folder)
- STEP2：點選右鍵內容，接著點選共用頁籤，設定 Domain Users可「讀取/寫入」此資料夾



AD主機建立分享資料夾(2/3)

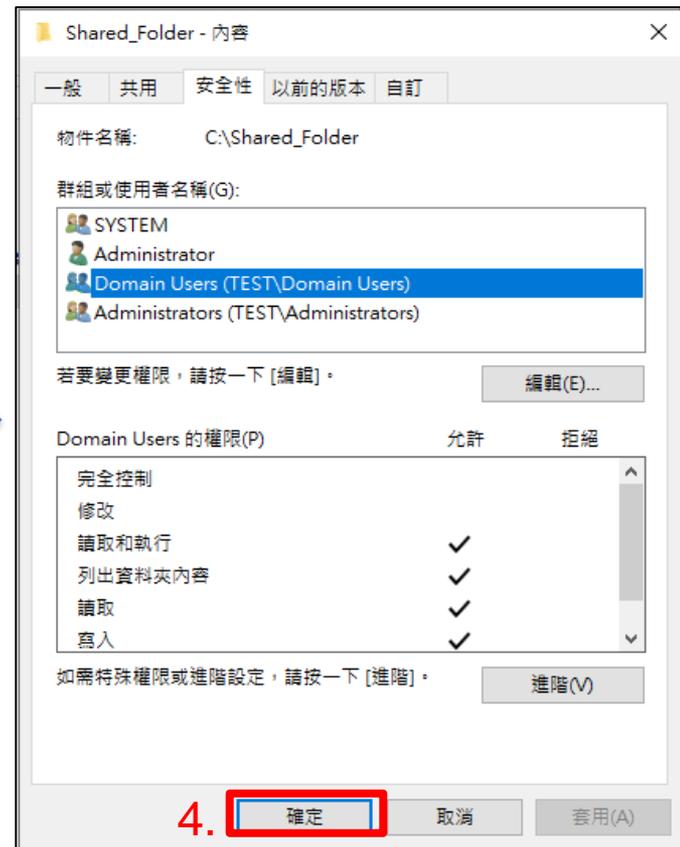
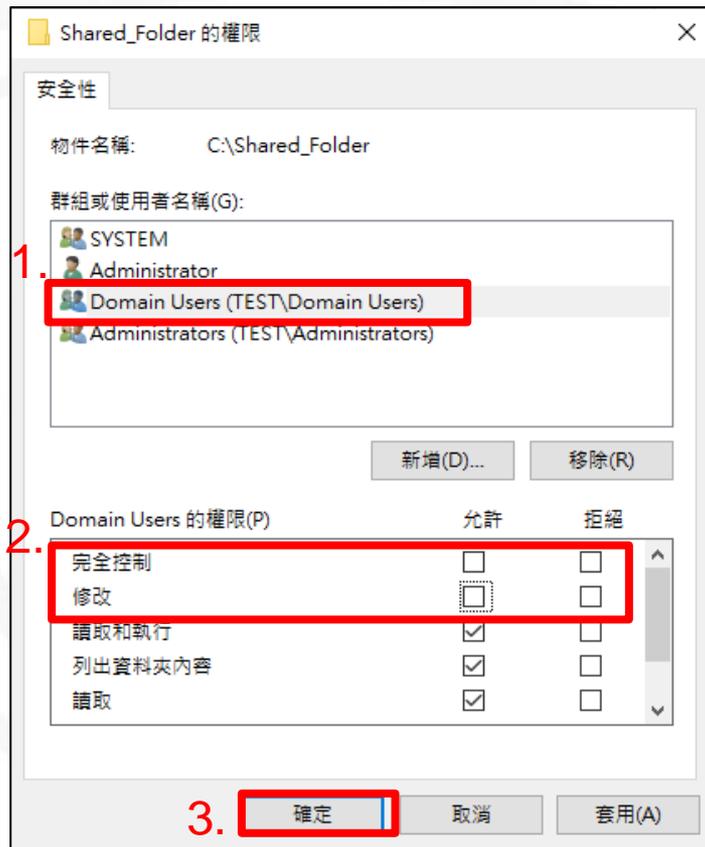
- STEP3：避免網域使用者誤刪檔案，需限縮其存取權限，切換至**安全性**頁籤，並點選編輯



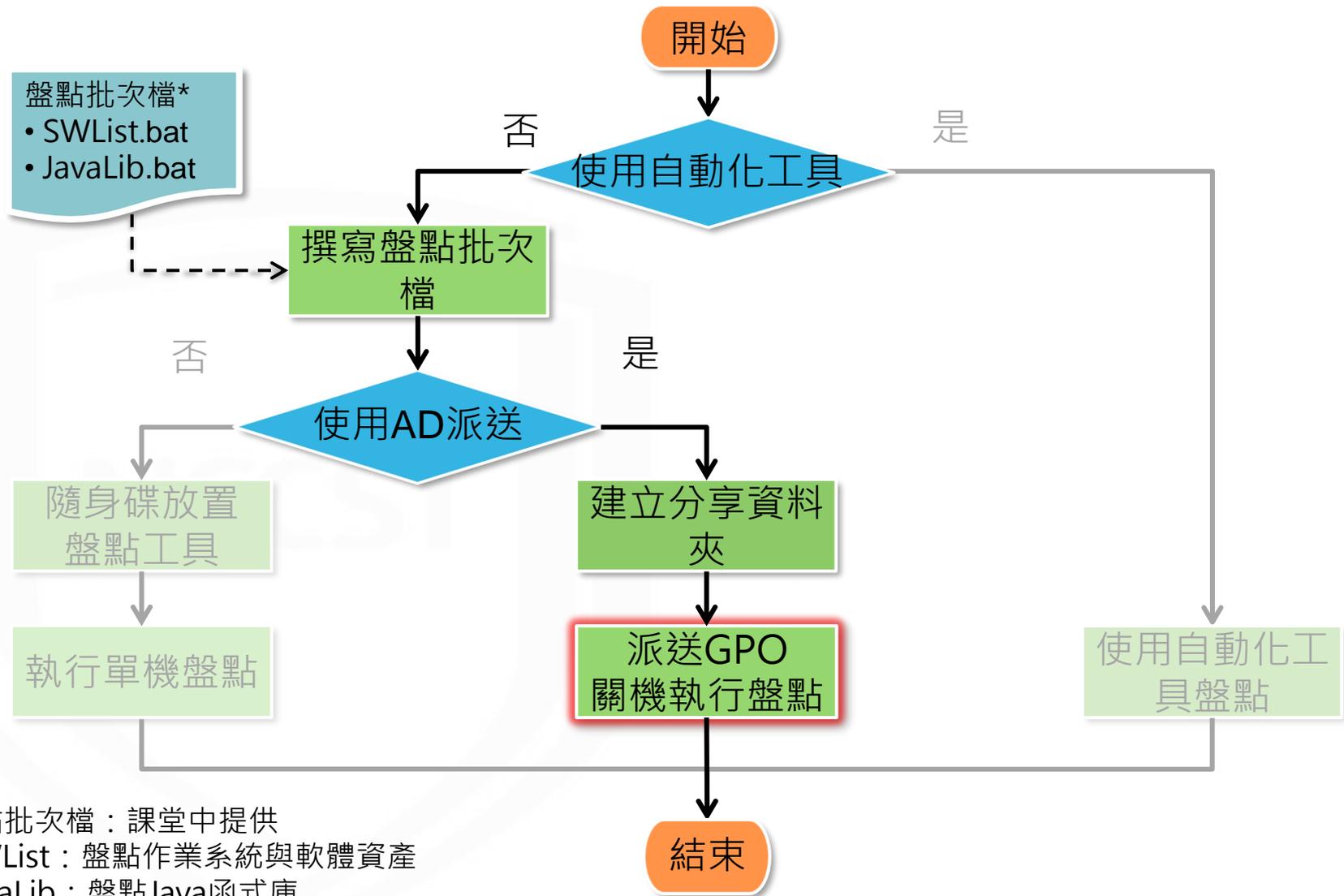
AD主機建立分享資料夾(3/3)



- STEP4：選取Domain Users並移除「完全控制」與「修改」權限，使Domain Users僅能讀取或寫入資料，但不可修改與刪除



盤點作業流程



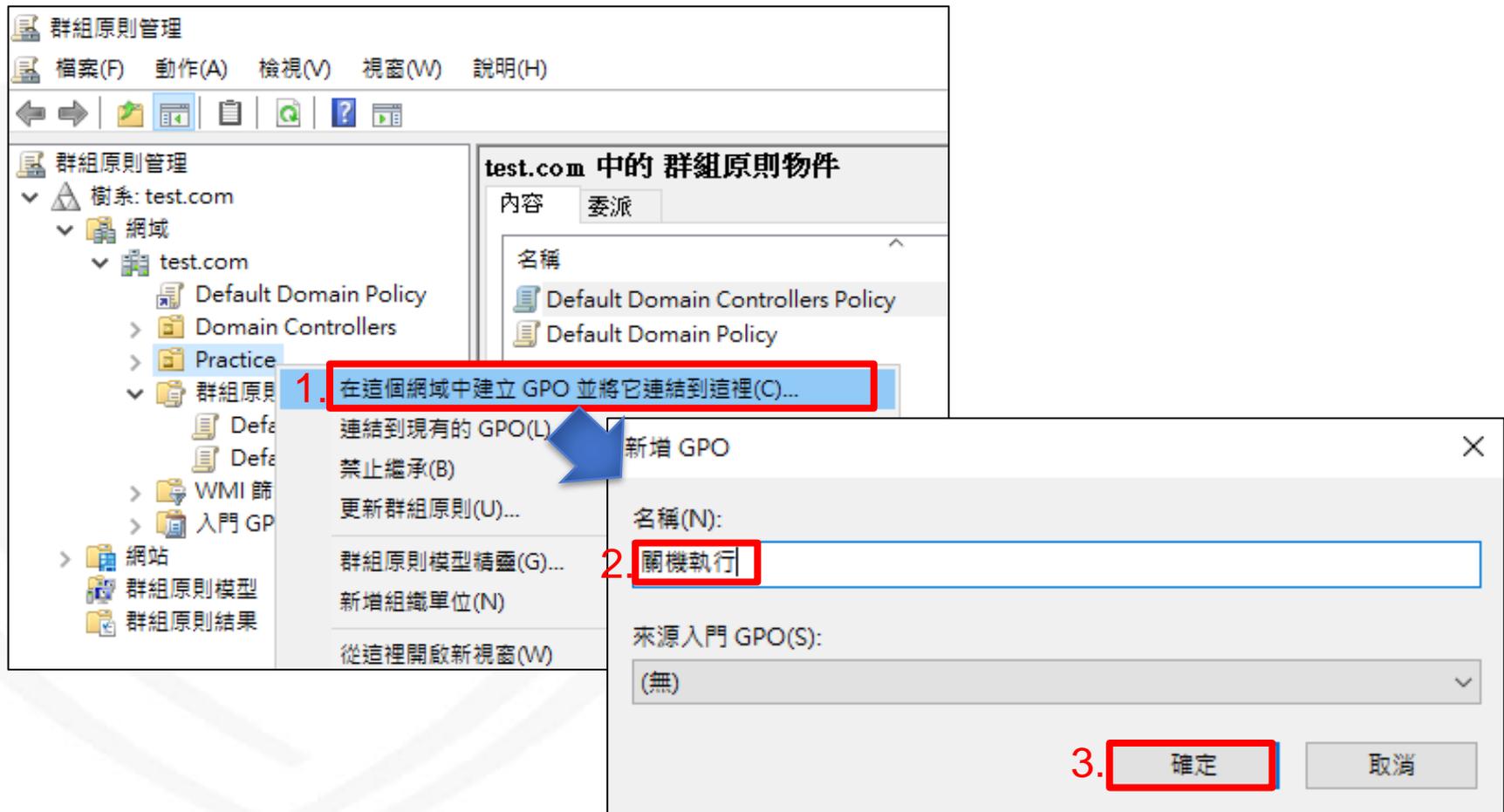
*盤點批次檔：課堂中提供

1.SWList：盤點作業系統與軟體資產

2.JavaLib：盤點Java函式庫

派送GPO-關機執行(1/5)

- 在目標OU點選右鍵並建立GPO
 - 新增「關機執行」GPO



The screenshot shows the Group Policy Management console for the test.com domain. The left pane shows the tree structure with 'test.com' selected. The right pane shows the 'test.com 中的 群組原則物件' (Group Policy Objects in test.com) list. A context menu is open over the 'test.com' folder, and the '在此網域中建立 GPO 並將它連結到這裡(C)...' (Create GPO in this domain and link it here) option is selected. A blue arrow points from this option to the '新增 GPO' (New GPO) dialog box. In the dialog box, the '名稱(N):' (Name) field contains '關機執行' (Shutdown Execution). The '來源入門 GPO(S):' (Source Starter GPO(S)) dropdown is set to '(無)' (None). The '確定' (OK) button is highlighted with a red box.

1. 在這個網域中建立 GPO 並將它連結到這裡(C)...

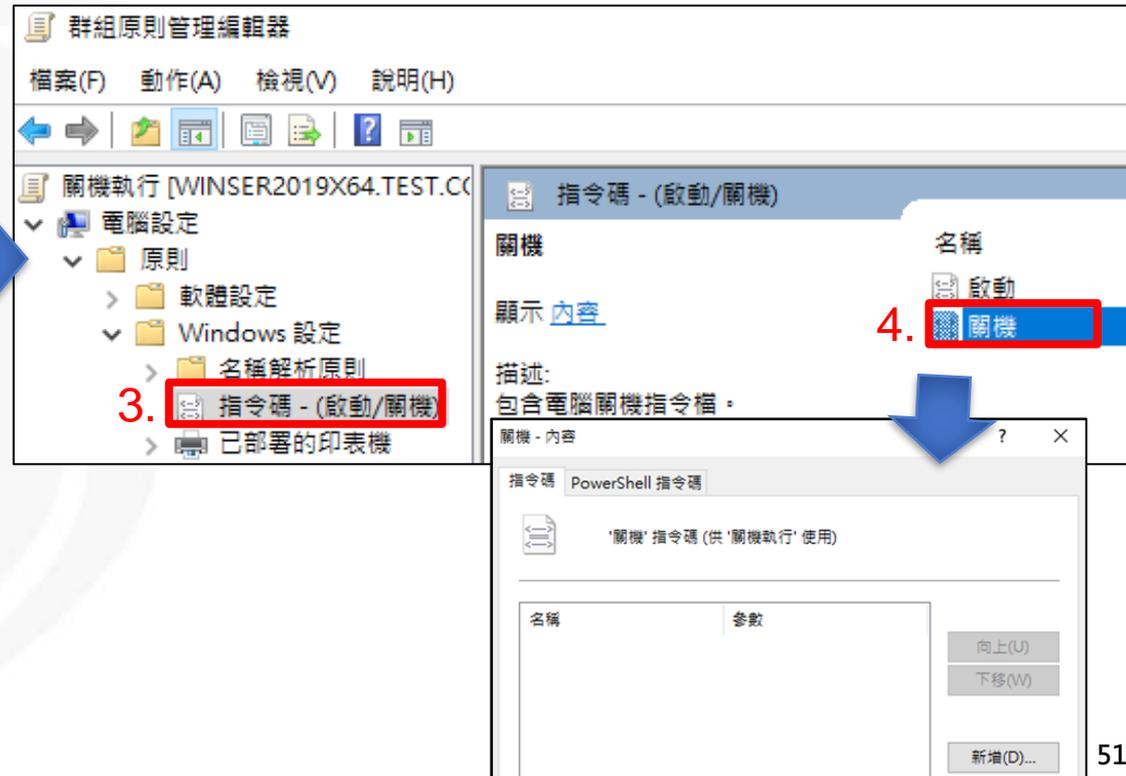
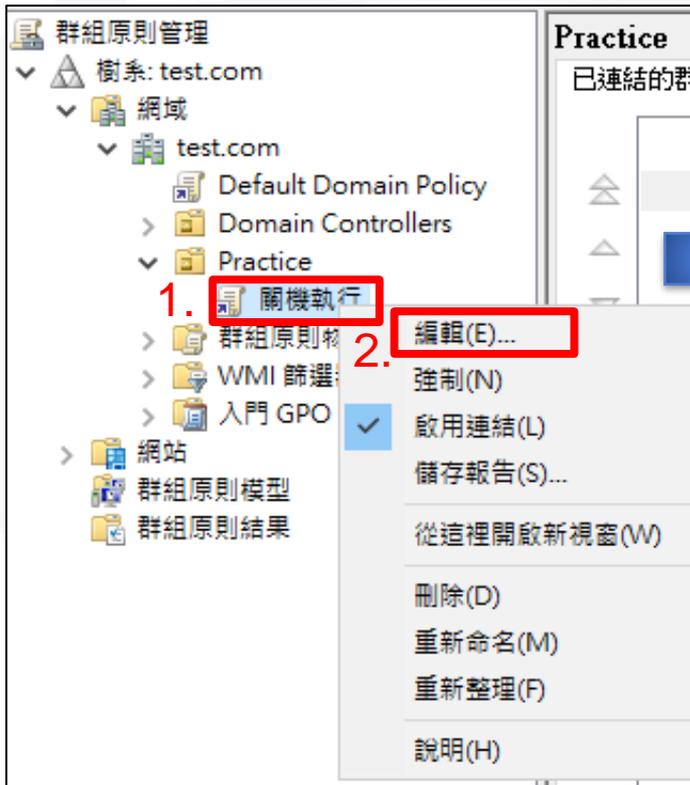
2. 關機執行

3. 確定

派送GPO-關機執行(2/5)

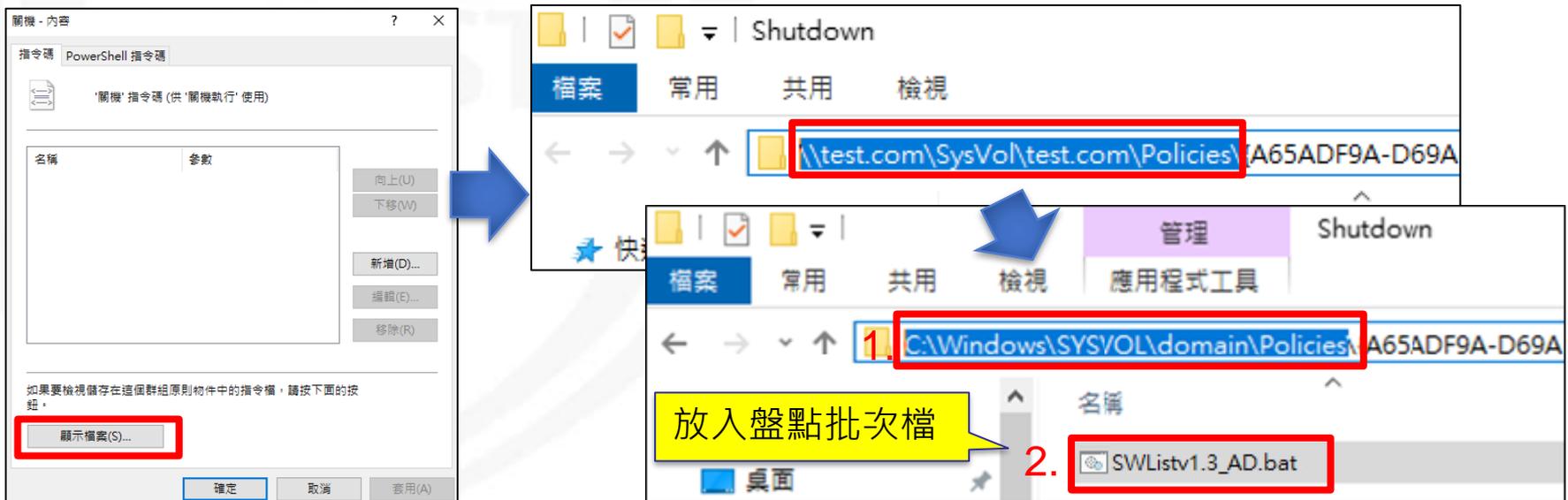
- 編輯GPO，於電腦關機時執行檢測批次檔

- 點選剛建立的「關機執行」GPO，按右鍵選擇編輯
- 路徑為：電腦設定\原則\Windows設定\指令碼 - (啟動/關機)\關機
- 點擊「關機」並編輯「關機-內容」



派送GPO-關機執行(3/5)

- 點選「顯示檔案」，準備放入檢測批次檔
- 因作業系統預設不允許複製檔案至網路位置，須將資料夾路徑改為本機路徑，放入盤點批次檔後即可關閉
 - 由「**\\[網域名稱]\SysVol\[網域名稱]\Policies\{關機執行GPO_GUID}\Machine\Scripts\Shutdown**」
 - 改成「**C:\Windows\SYSVOL\domain\Policies\{關機執行GPO_GUID}\Machine\Scripts\ Shutdown**」



The image shows a sequence of steps to modify a Group Policy Object (GPO) path. On the left, the 'Group Policy Editor' window is open to the 'Scripts' section. The 'Show files' button is highlighted with a red box. A blue arrow points from this button to the File Explorer window. The File Explorer window shows the path '\\test.com\SysVol\test.com\Policies\A65ADF9A-D69A'. A red box highlights this path. A second blue arrow points to the path 'C:\Windows\SYSVOL\domain\Policies\A65ADF9A-D69A', which is also highlighted with a red box and labeled '1.' with a yellow callout box that says '放入盤點批次檔'. A third red box highlights the file 'SWListv1.3_AD.bat' in the file list, labeled '2.'.

派送GPO-關機執行(4/5)



- 選擇關機執行的檔案

- 選擇「新增」後，點選「瀏覽」並選取前一步驟放入的盤點批次檔

1. 新增(D)...

2. 瀏覽(B)...

3. SWListv1.3_AD.bat

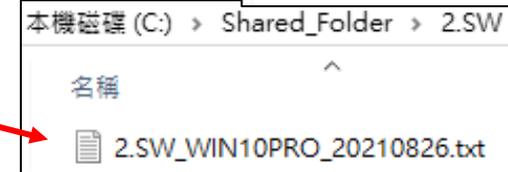
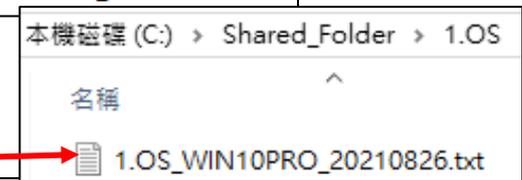
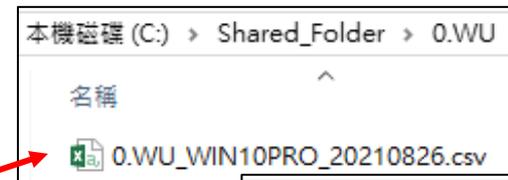
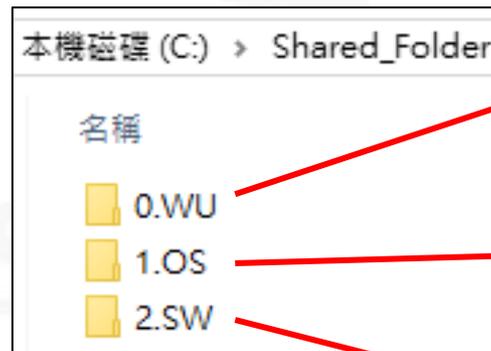
4. 開啟(O)

5. 確定

派送GPO-關機執行(5/5)

- 電腦關機時，將自動執行盤點
- 盤點結果將產出至本機之「共用文件」中，並自動回存至AD主機「Shared_Folder」資料夾

AD主機



執行盤點電腦



導入作業流程

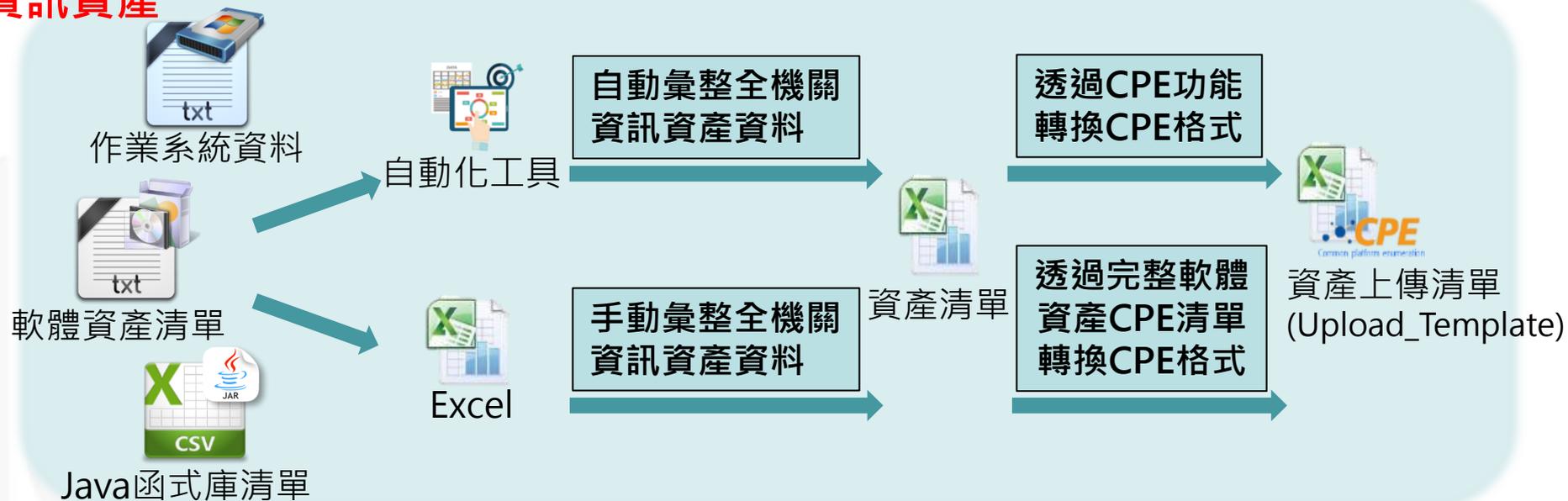


資訊資產與已安裝KBID正規化



- 透過自動化工具或Excel彙整為全機關資料，並將資訊資產轉換為CPE格式

資訊資產



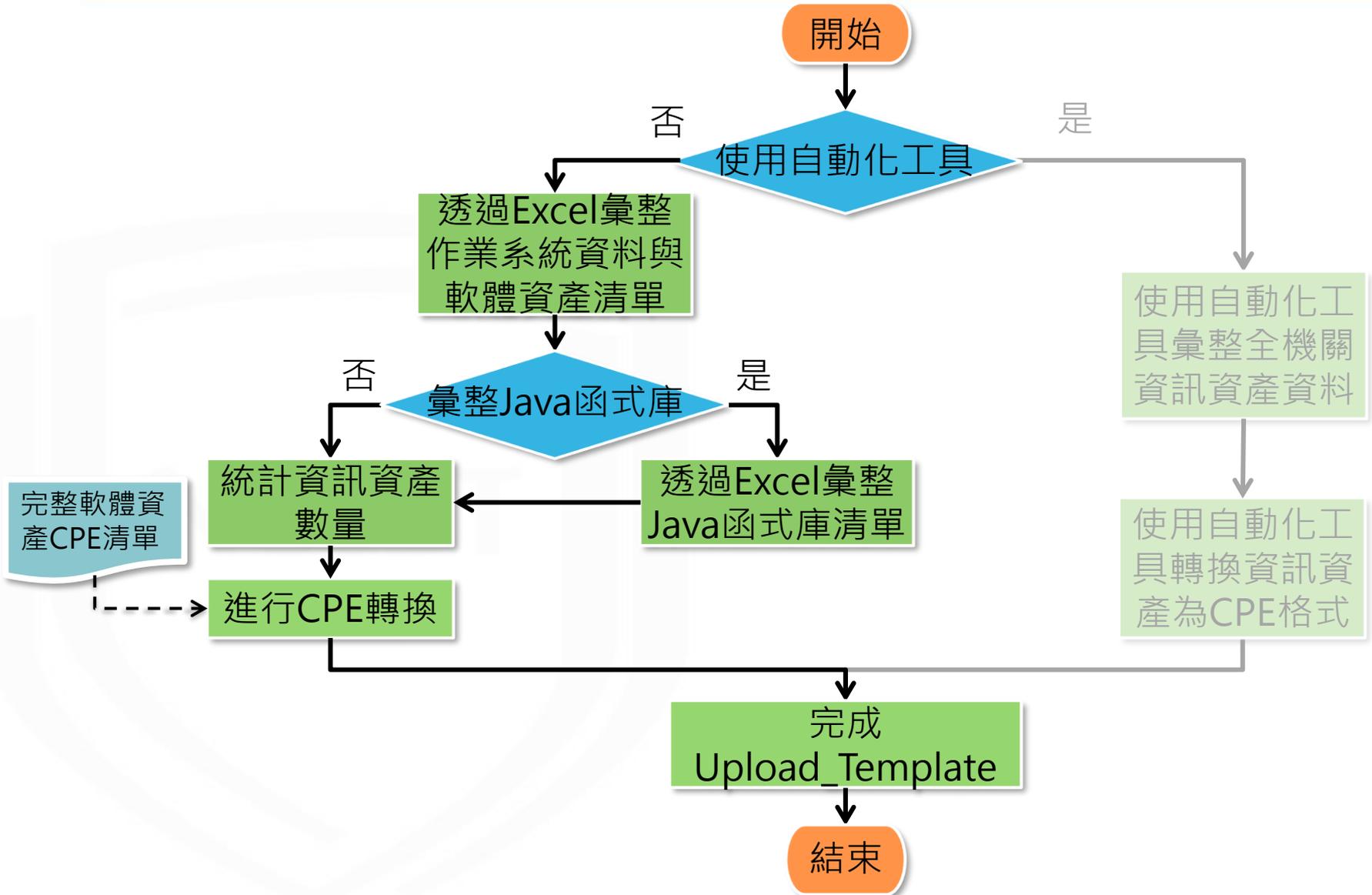
KBID



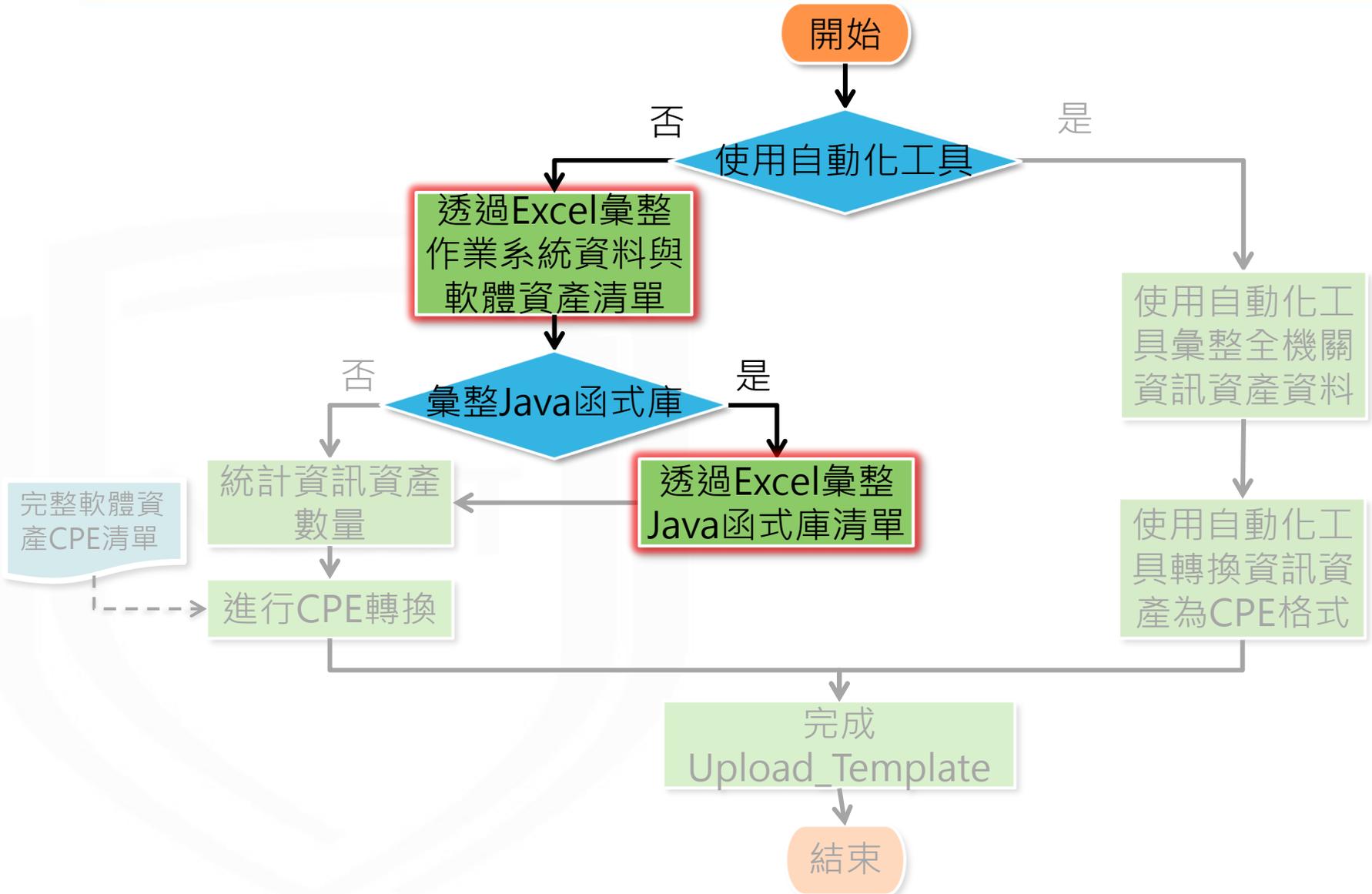
資訊資產正規化作業

NCCST

資訊資產正規化作業流程



資訊資產正規化作業流程



Excel彙整功能介紹

- Microsoft Power Query for Excel可在各種不同的資料來源中合併或精簡資料



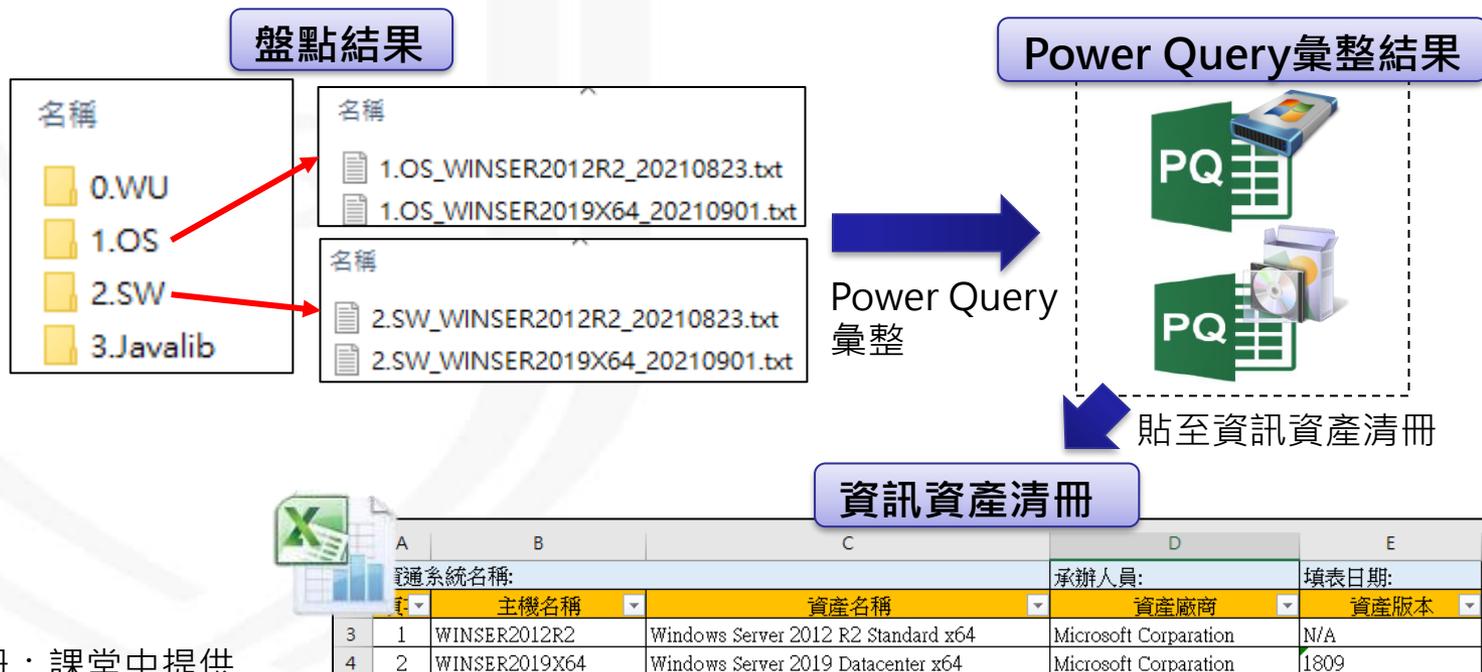
- 適用於32位元與64位元平台
- 支援作業系統版本
 - Windows 7/8/8.1/10
 - Windows Server 2008 R2/2012
- 支援Office版本
 - Microsoft Office 2010 Professional Plus(需另行安裝套件)
 - Microsoft Office 2013 (需另行安裝套件)
 - Power Query內建於Excel 2016、2019中，功能名稱為「取得及轉換」
- 須Internet Explorer 9以上之版本

- 下載網址：

- <https://www.microsoft.com/zh-TW/download/details.aspx?id=39379>

彙整資訊資產清單

- 透過Power Query分別彙整歸類後作業系統與軟體資產之盤點結果
 - 若欲了解彙整步驟，請參閱「政府機關資安弱點通報系統操作手冊v1.8」
- 將作業系統與軟體資產彙整結果，整合至資訊資產清冊*，以留存查看

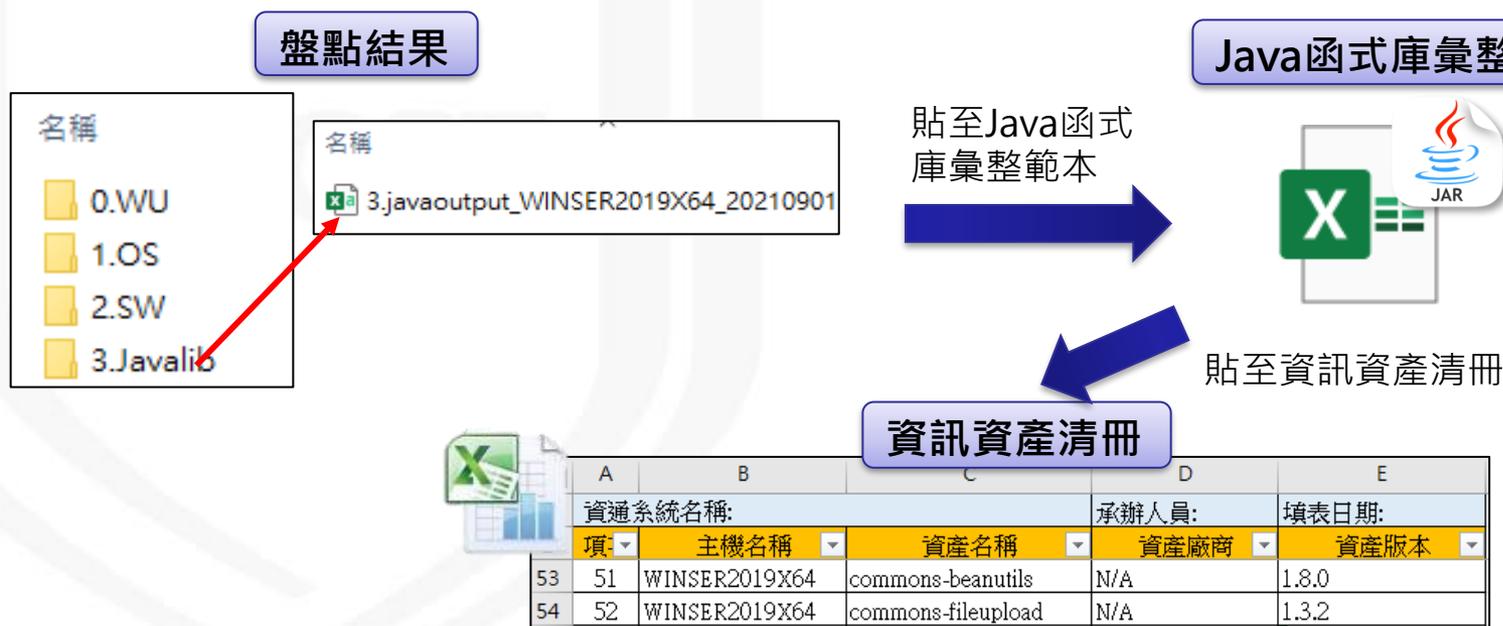


*資訊資產清冊：課堂中提供

彙整資訊資產清單_Java函式庫

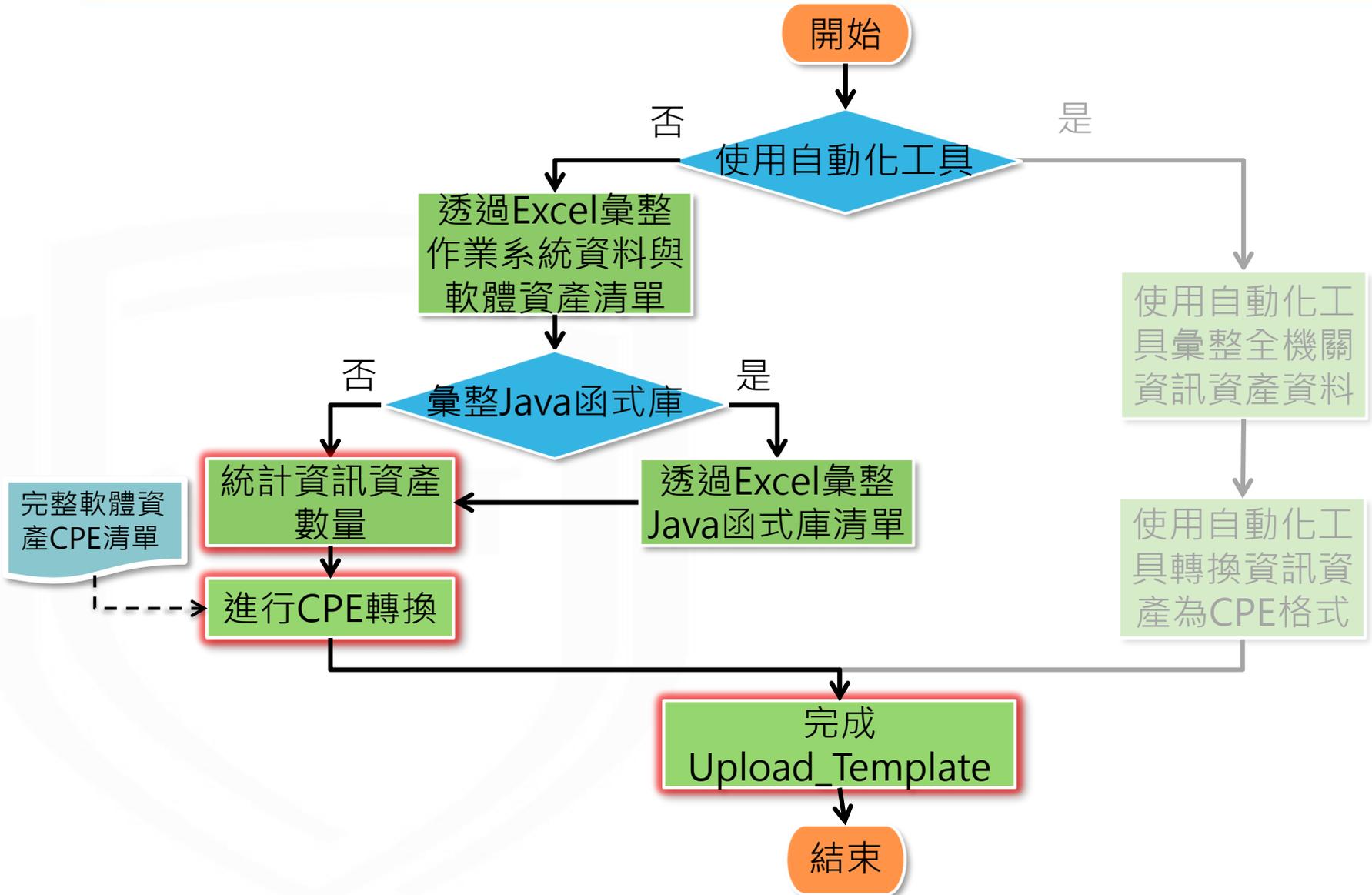


- Java函式庫盤點清單彙整至Java函式庫彙整範本*，以取得Java函式庫名稱與Java函式庫版本
- 將Java函式庫彙整結果，整合至資訊資產清冊*，並補充主機名稱與資產廠商資訊



*Java函式庫彙整範本：課堂中提供

資訊資產正規化作業流程



完成Upload_Template

- 統計資訊資產數量
 - 資訊資產清冊自動計算資產數量
 - 利用移除重複項功能，以避免上傳相同之資訊資產
- 進行CPE轉換
 - 將資訊資產清冊彙整至Upload_Template*
 - 於完整軟體資產CPE清單*搜尋，並於Upload_Template填入資訊資產對應之CPE格式，若無則填入N/A
- 完成Upload_Template
 - 填寫機關OID與機關名稱



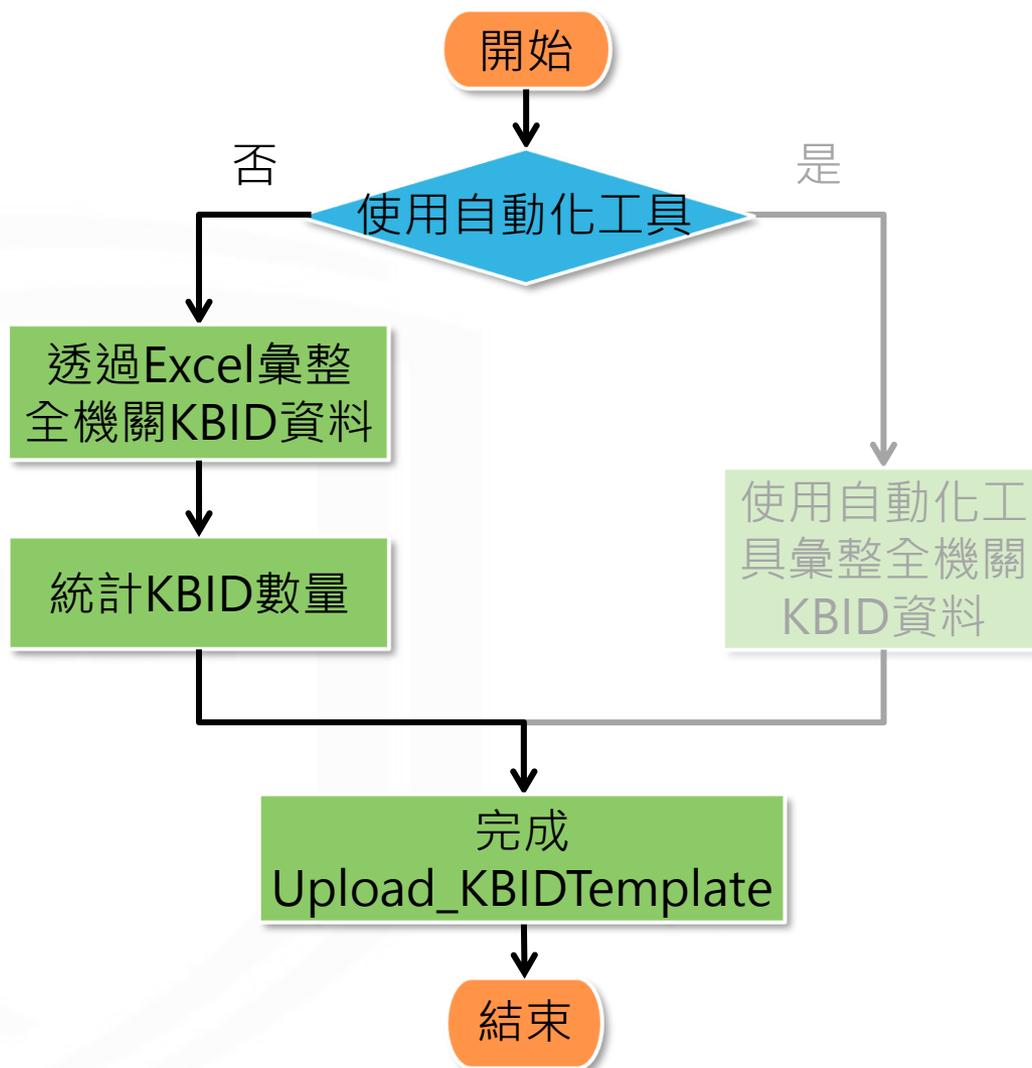
*Upload_Template：於VANS系統下載

*完整軟體資產CPE清單：於VANS系統下載

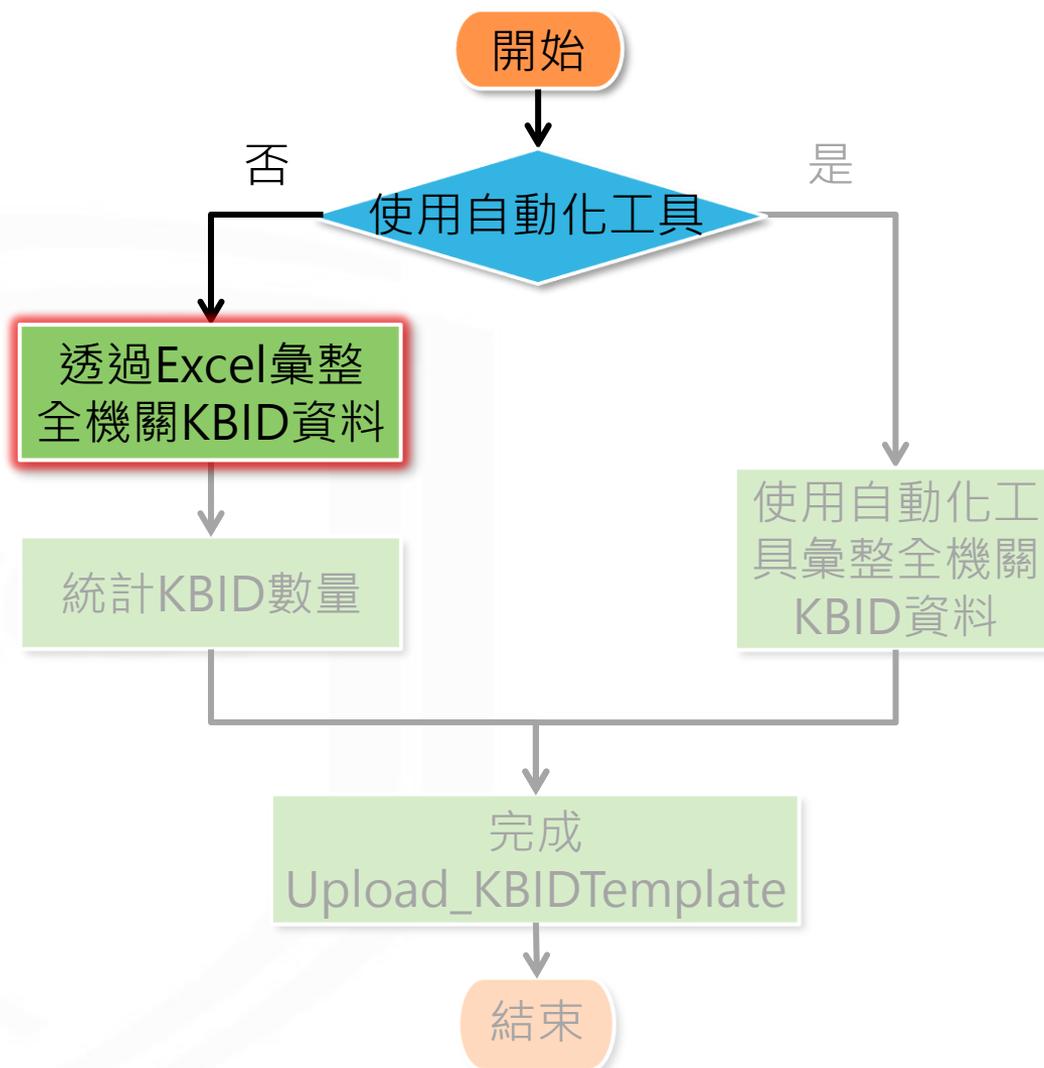
已安裝KBID正規化作業

NCCST

已安裝KBID正規化作業流程

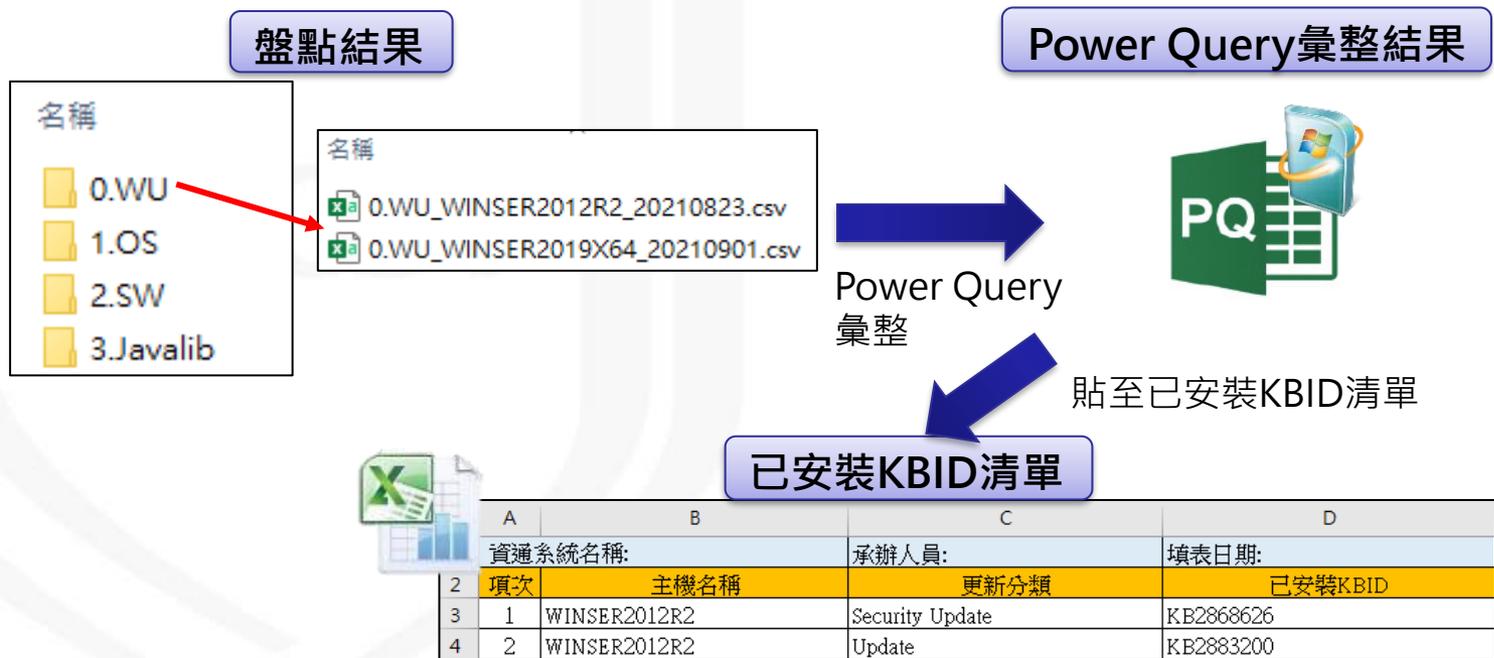


已安裝KBID正規化作業流程



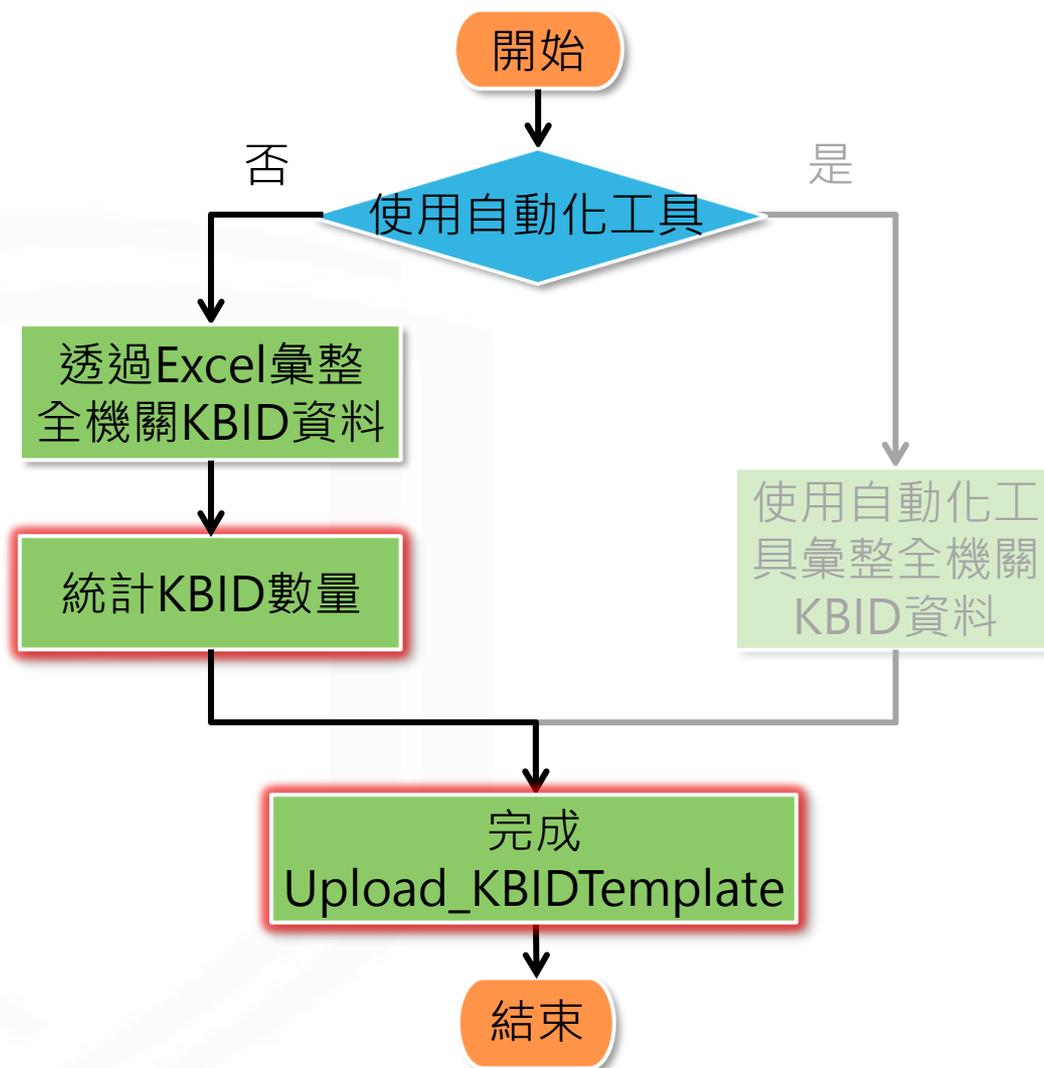
彙整KBID清單

- 透過Power Query彙整歸類後已安裝KBID之盤點結果
 - 若欲了解彙整步驟，請參閱「政府機關資安弱點通報系統操作手冊v1.8」
- 將已安裝KBID彙整結果，整合至已安裝KBID清單*，以留存查看



*已安裝KBID清單：課堂中提供

已安裝KBID正規化作業流程



完成Upload_KBIDTemplate

- 統計KBID數量

- 已安裝KBID清單自動計算KBID數量
- 利用移除重複項功能，以避免上傳相同之KBID

- 完成Upload_KBIDTemplate

- 將已安裝KBID清單彙整至Upload_KBIDTemplate*
- 填寫機關OID與機關名稱



實作練習1

NCCST

實作練習1 (環境說明)

● VANS系統_實作站

– 登入資訊

- 網址：已儲存於瀏覽器「我的最愛列」
- 帳號：student01~45
- 密碼：1111

– 首次登入設定

- 通知設定：ON
- 分數設定：4.0
- 電子郵件設定：請輸入欲接收弱點通知之電子郵件

– 機關資訊

- 機關OID：student01~45
- 機關名稱：student01~45

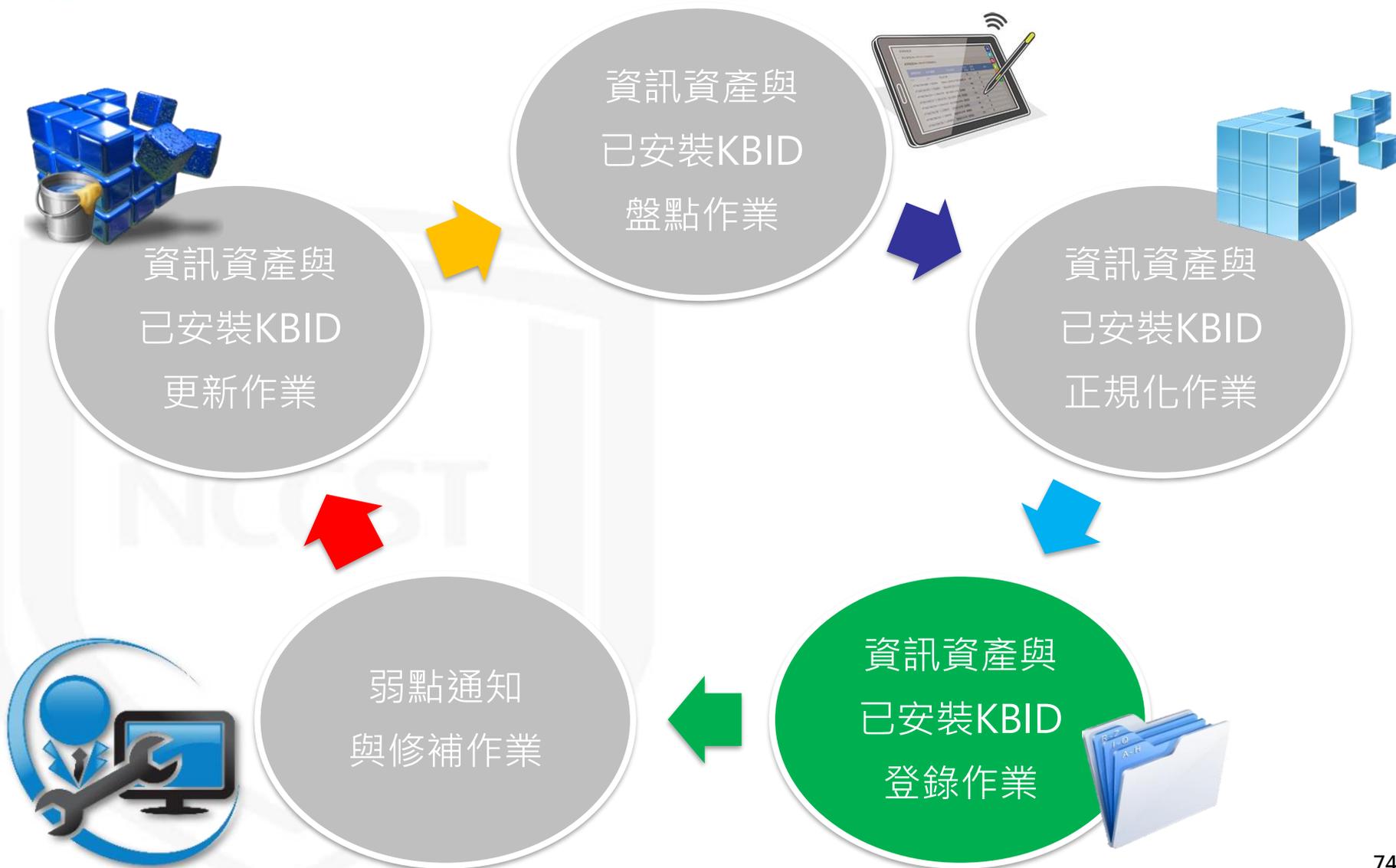


實作練習1

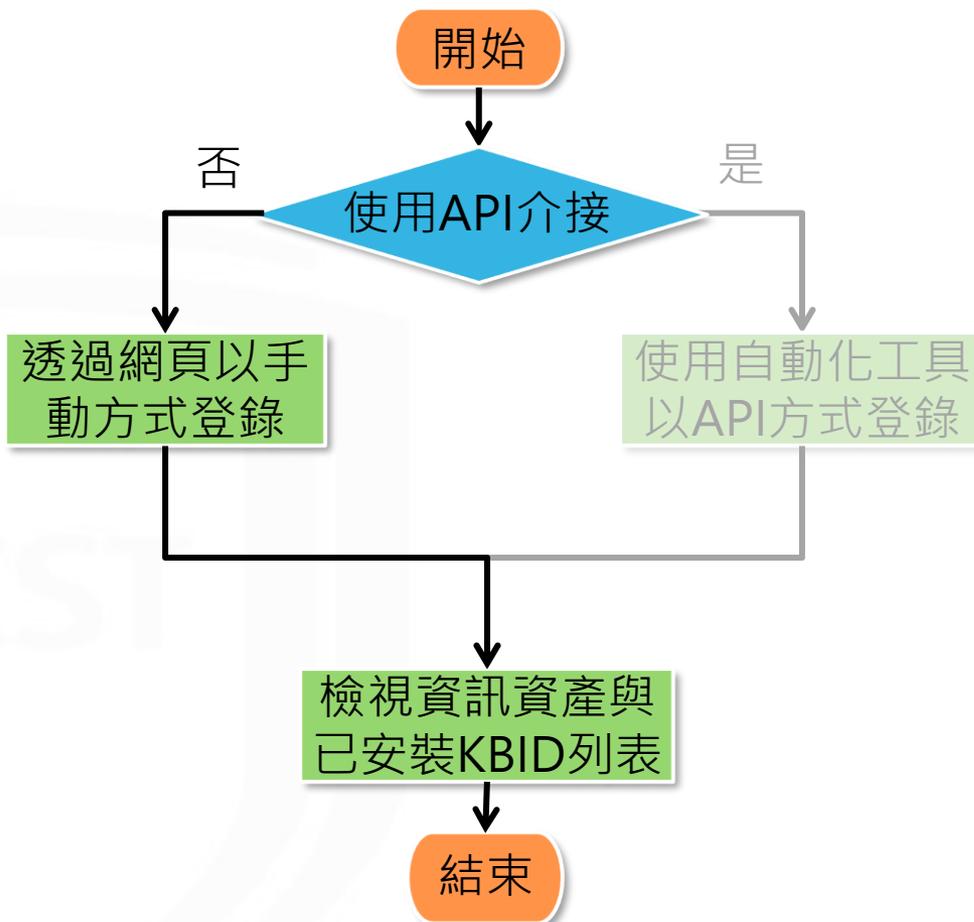
- 請將「實作練習1」提供之Upload_Template與Upload_KBIDTemplate完成正規化作業
- 本項練習時間**20分鐘**

項次	參考頁數	執行項目	產出項目/執行結果
1	P.63	登入VANS系統下載 完整資產CPE清單	完整資產CPE清單
2	P.63	開啟Upload_Template (路徑：學員資料夾\01.實作練習\實作練習1\Upload_Template.xlsx) <ul style="list-style-type: none"> ● 針對前3筆軟體資產進行正規化 ● 針對前3筆Java函式庫清單進行正規化 ● 完成Upload_Template 	Upload_Template
3	P.69	開啟KBID上傳清單 (路徑：學員資料夾\01.實作練習\實作練習1\Upload_KBIDTemplate.xlsx) <ul style="list-style-type: none"> ● 完成KBID上傳清單 	Upload_KBIDTemplate.xlsx

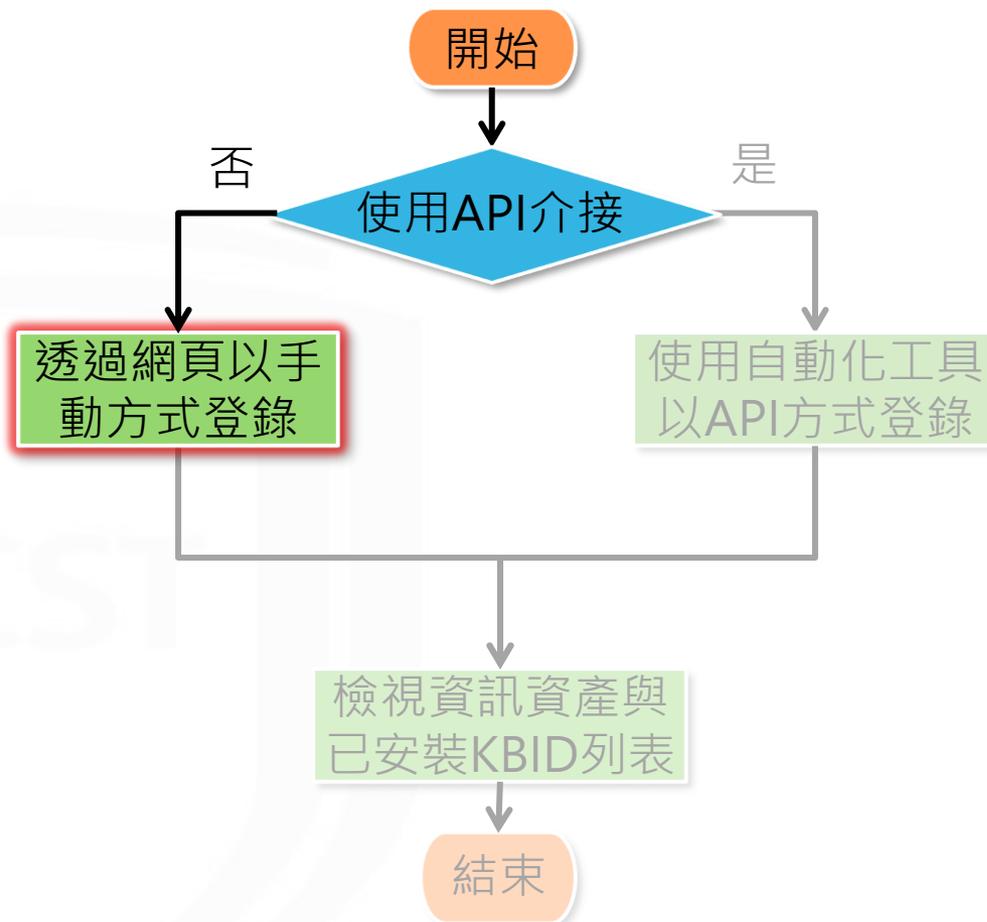
導入作業流程



登錄作業流程



登錄作業流程



網頁登錄-資訊資產(1/2)

- STEP1：於VANS系統點選資產清單上傳
 - 資訊資產管理 > 資通系統資產列表/使用者電腦資產列表
- STEP2：選取已完成之**上傳清單**



The screenshot illustrates the process of uploading an asset list in the VANS system. It is divided into two parts:

Top Screenshot: Shows the navigation menu on the left with "資訊資產管理" (Information Asset Management) highlighted in a red box. The main content area shows the breadcrumb "資訊資產管理 > 資通系統資產列表" (Information Asset Management > Information Communication System Asset List). Below this, there are three buttons: "CPE清單 / 範本下載" (CPE List / Download Template), "資產 / 已安裝KBID上傳" (Assets / Upload Installed KBID), and "資產清單匯出" (Export Asset List). The "資產 / 已安裝KBID上傳" button is highlighted in a red box, and a tooltip below it says "資產清單上傳" (Upload Asset List) and "已安裝KBID清單上傳" (Upload Installed KBID List).

Bottom Screenshot: Shows the "資產清單上傳" (Upload Asset List) page. The breadcrumb is "資訊資產管理 > 資通系統資產列表 > 資產清單上傳". There is a checkbox for "資產CPE清單上傳" (Upload Asset CPE List). Below it, a red box highlights the "選擇檔案" (Select File) button next to the text "Upload_Template.xlsx". A note below the button reads: "※使用Excel編輯ODS檔案可能引起相容性問題，如發生異常請嘗試以其他格式上傳。" (Note: Using Excel to edit ODS files may cause compatibility issues. If an abnormality occurs, please try uploading in another format.). An "上傳" (Upload) button is located at the bottom right.

網頁登錄-資訊資產(2/2)

- STEP3：點選「上傳」，等待系統解析清單
- STEP4：待收到解析完成通知信，即完成登錄

資訊資產管理 > 資通系統資產列表 > 資產清單上傳

資產CPE清單上傳

選擇檔案 Upload_Template.xlsx

※使用Excel編輯ods檔案可能引起相容性問題，如發生異常請嘗試以其他格式上傳。

上傳

上傳清單成功，系統正在解析清單中，解析完成後將會寄發郵件通知

回列表頁

2021/8/23 (週一) 下午 11:35

VANS <vans@nccst.nat.gov.tw>

[VANS]資通系統資訊資產清單解析完成

敬啟者 您好

此為「政府機關資安弱點通報系統」之通知郵件。

貴機關之所以收到此通知信件，在於貴機關於 VANS 系統上傳之資訊資產清單已解析完成，請至 VANS 系統檢視資訊資產清單登錄結果。

謝謝。

VANS 系統網頁連結：
<https://vans.nccst.nat.gov.tw/>

如有任何疑問，聯絡資訊如下：
行政院國家資通安全會報技術服務中心(技服中心)
服務電話：(02)6631-6458
服務信箱：VansService@nccst.nat.gov.tw

網頁登錄-已安裝KBID(1/2)

- STEP1：於VANS系統進行已安裝KBID清單上傳
– 資訊資產管理 > 資通系統資產列表/使用者電腦資產列表
- STEP2：瀏覽並上傳已完成之**上傳清單**



The screenshot illustrates the navigation process in the VANS system. On the left, a sidebar menu shows '資訊資產管理' (Information Asset Management) highlighted with a red box. Below it, '資通系統資產列表' (Communication System Asset List) and '使用者電腦資產列表' (User Computer Asset List) are also visible. The main content area shows the breadcrumb '資訊資產管理 > 資通系統資產列表' and a sub-section '上傳資通系統已安裝KBID清單' (Upload Communication System Installed KBID List). Three buttons are present: 'CPE清單 / 範本下載' (CPE List / Template Download), '資產 / 已安裝KBID上傳' (Assets / Installed KBID Upload), and '資產清單匯出' (Asset List Export). A dropdown menu is open under the second button, showing '資產清單上傳' (Asset List Upload) and '已安裝KBID清單上傳' (Installed KBID List Upload), with the latter highlighted by a red box. A blue arrow points down to the next screen, which shows the '已安裝KBID清單上傳' (Installed KBID List Upload) page. This page has a sub-section '已安裝KBID清單上傳' and a file upload area with a red box around the '選擇檔案' (Choose File) button and the filename 'Upload_KBIDTemplate.xlsx'. A note below the filename states: '※使用Excel編輯ods檔案可能引起相容性問題，如發生異常請嘗試以其他格式上傳。' (Using Excel to edit ods files may cause compatibility issues, if an abnormality occurs, please try uploading in another format). An '上傳' (Upload) button is located at the bottom right.

網頁登錄-已安裝KBID(2/2)

- STEP3：點選「上傳」，等待系統解析請單
- STEP4：待收到解析完成通知信，即完成登錄

資訊資產管理 > 資通系統資產列表 > 已安裝KBID清單上傳

已安裝KBID清單上傳

選擇檔案 Upload_KBIDTemplate.xlsx

※使用Excel編輯ods檔案可能引起相容性問題，如發生異常請嘗試以其他格式上傳。

上傳

上傳清單成功，系統正在解析清單中，解析完成後將會寄發郵件通知

回列表頁

2021/8/25 (週三) 上午 02:52

VANS <vans@nccst.nat.gov.tw>

[VANS]資通系統已安裝KBID清單解析完成

敬啟者 您好

此為「政府機關資安弱點通報系統」之通知郵件。

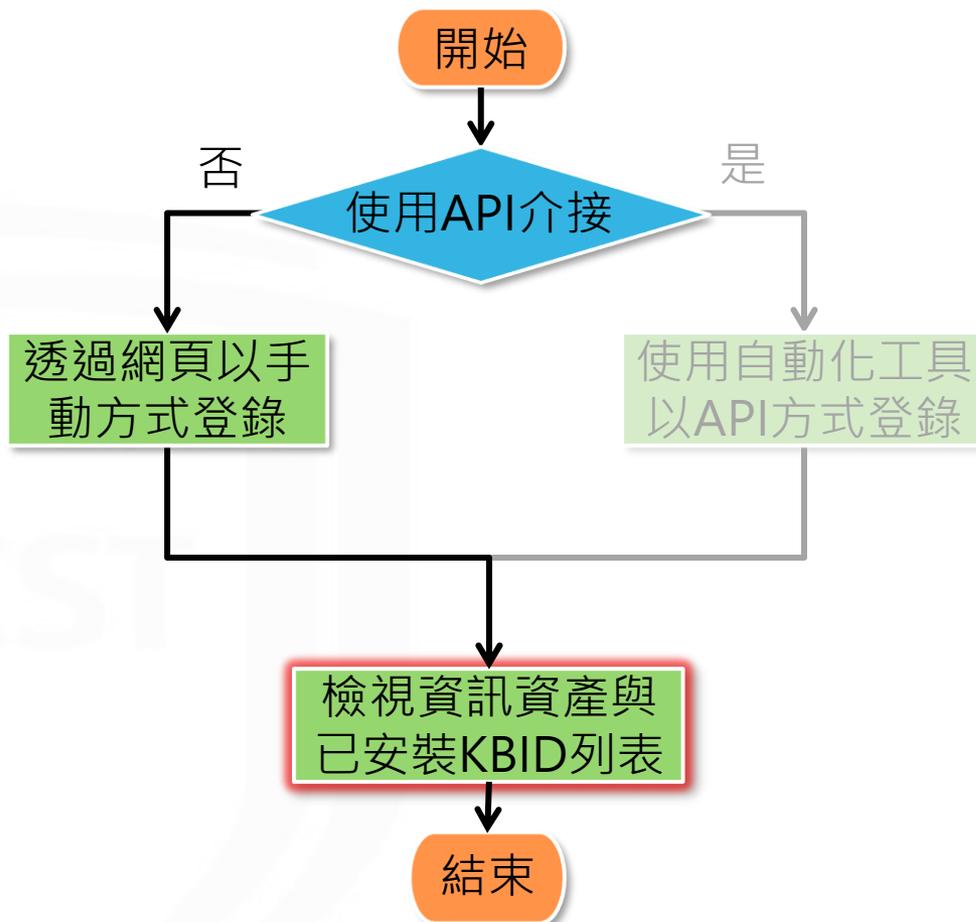
貴機關之所以收到此通知信件，在於貴機關於 VANS 系統上傳之已安裝 KBID 清單已解析完成，請至 VANS 系統檢視已安裝 KBID 清單登錄結果。

謝謝。

VANS 系統網頁連結：
<https://vans.nccst.nat.gov.tw/>

如有任何疑問，聯絡資訊如下：
行政院國家資通安全會報技術服務中心(技服中心)
服務電話：(02)6631-6458
服務信箱：VansService@nccst.nat.gov.tw

登錄作業流程



檢視資訊資產與已安裝KBID列表

- 可於**資訊資產管理**查看已登錄之資產項目
 - 資訊資產管理 > 資通系統資產列表/使用者電腦資產列表
- 點選右邊「**切換至已安裝KBID列表**」可檢視已安裝KBID項目

資訊資產管理 > 資通系統資產列表

CPE清單 / 範本下載 | 資產 / 已安裝KBID上傳 | 資產清單匯出

切換至已安裝KBID列表

資訊資產列表

資產名稱	資產廠商	資產版本	CPE2.3
Apache Tomcat 9.0 Tomcat9 (remove only)	The Apache Software Foundation	9.0.16	cpe:2.3:a:apache:tomcat:9.0.16:*:*:*:*:*
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beanutils:1.8.0:*:*:*:*:*

資訊資產管理 > 資通系統資產列表

CPE清單 / 範本下載 | 資產 / 已安裝KBID上傳 | 資產清單匯出

切換至資訊資產列表

已安裝KBID列表

新增已安裝KBID

搜尋

KBID	數量	受影響產品名稱	刪除
KB2868626	1	詳細清單	刪除
KB2883200	1	詳細清單	刪除
KB2887595	1	詳細清單	刪除

實作練習2

NCCST

實作練習2

- 請將「實作練習1」建立之Upload_Template執行登錄作業
- 本項練習時間**5分鐘**

項次	參考頁數	執行項目	產出項目/執行結果
1	P.76~77	上傳Upload_Template至VANS系統	於資產列表檢視登錄資產

NCCST

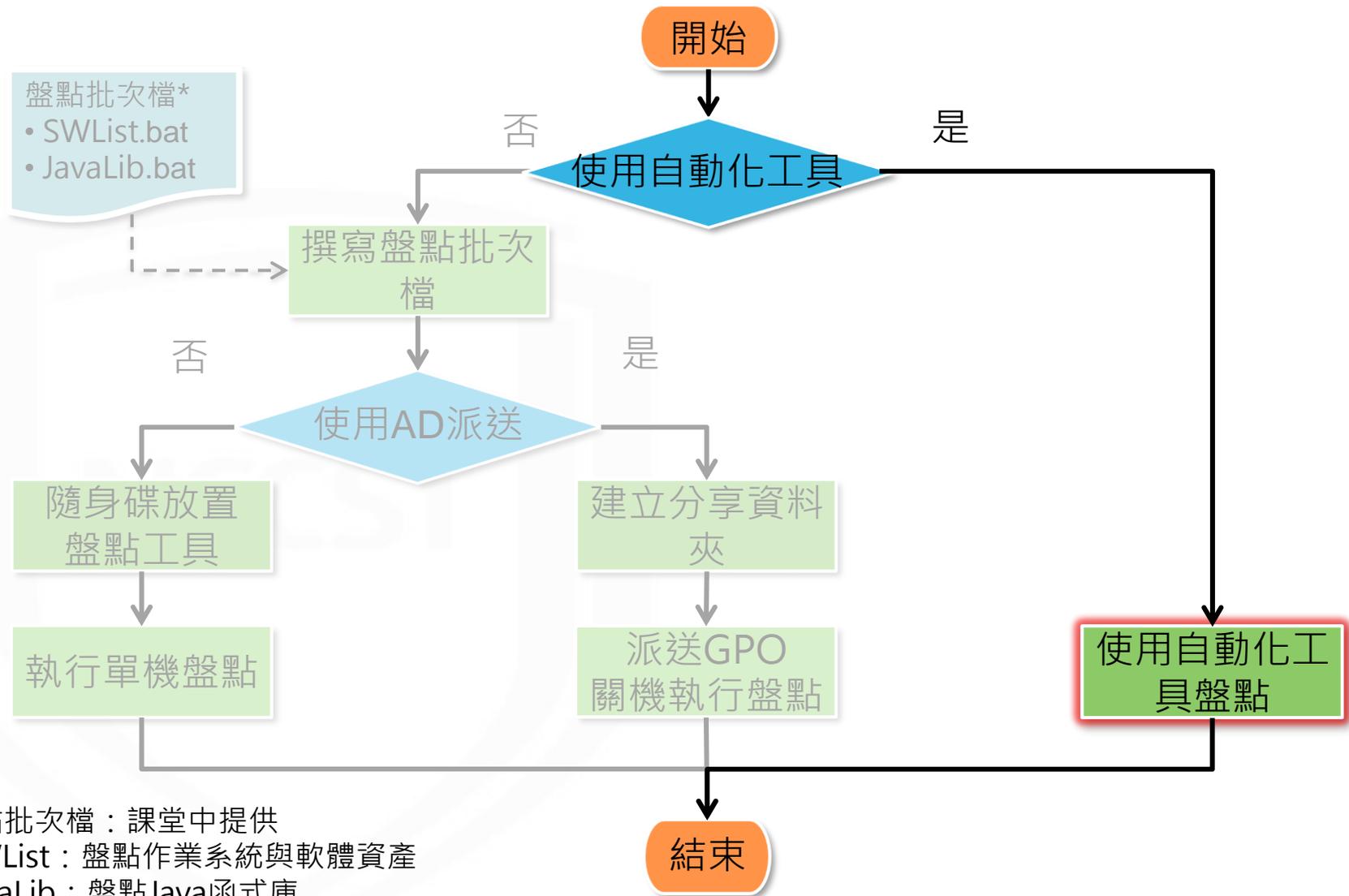
使用自動化工具

NCCST

導入作業流程

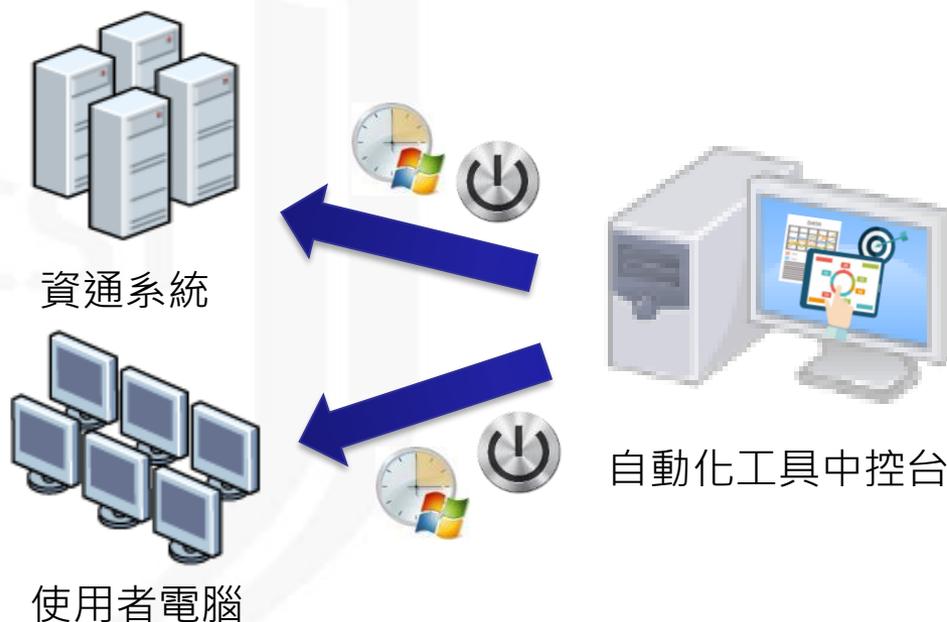


盤點作業流程



運用自動化工具盤點

- 於資通系統與使用者電腦部署**自動化工具**
- 透過設定排程或指定條件觸發時，進行**資訊資產**
與已安裝KBID盤點



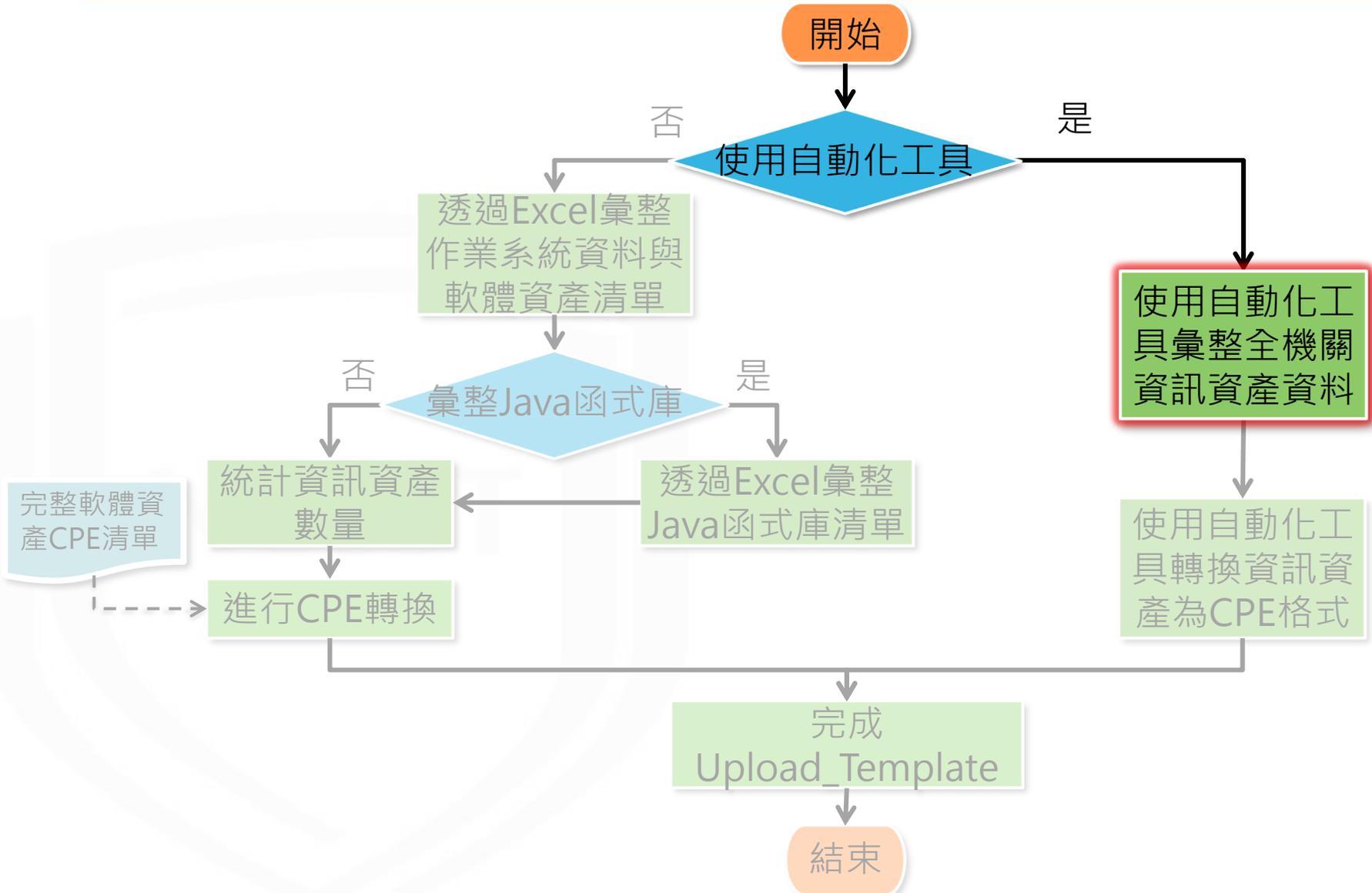
導入作業流程



資訊資產正規化作業 (自動化工具)

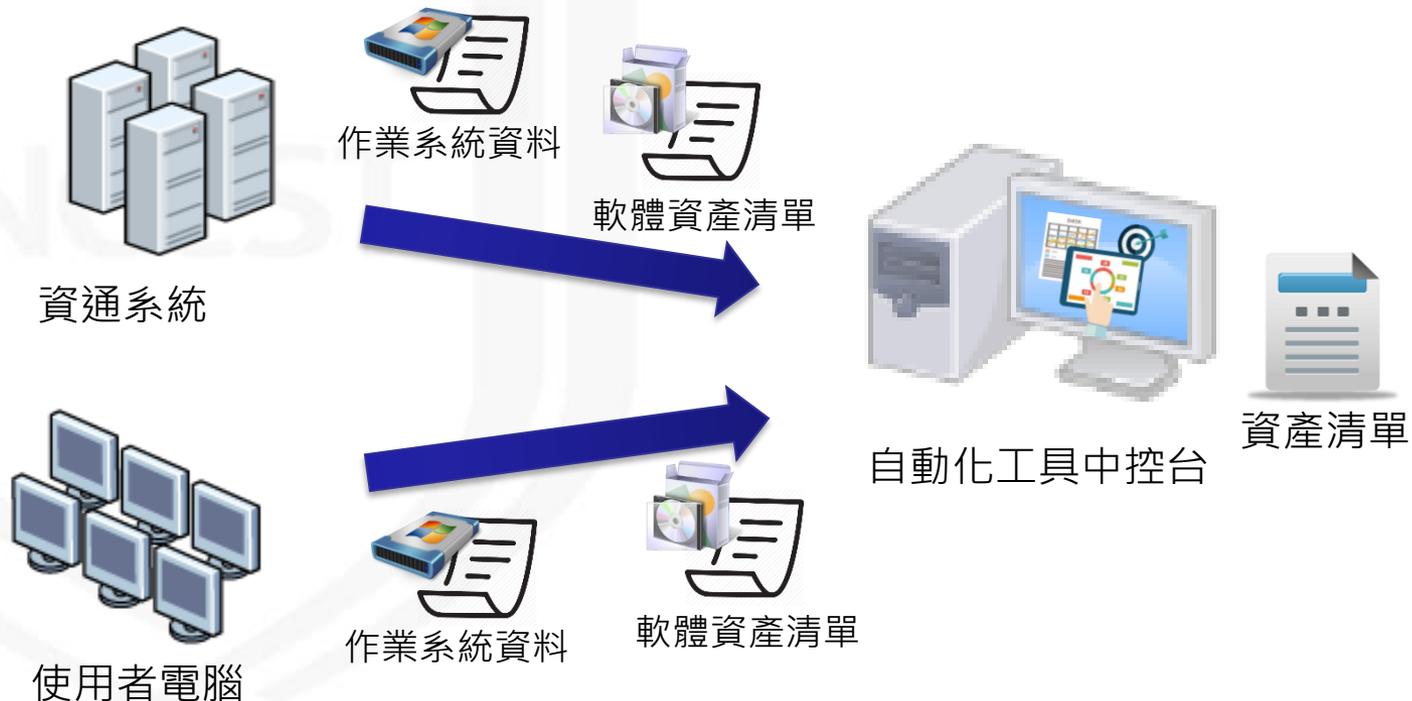
NCCST

資訊資產正規化作業流程

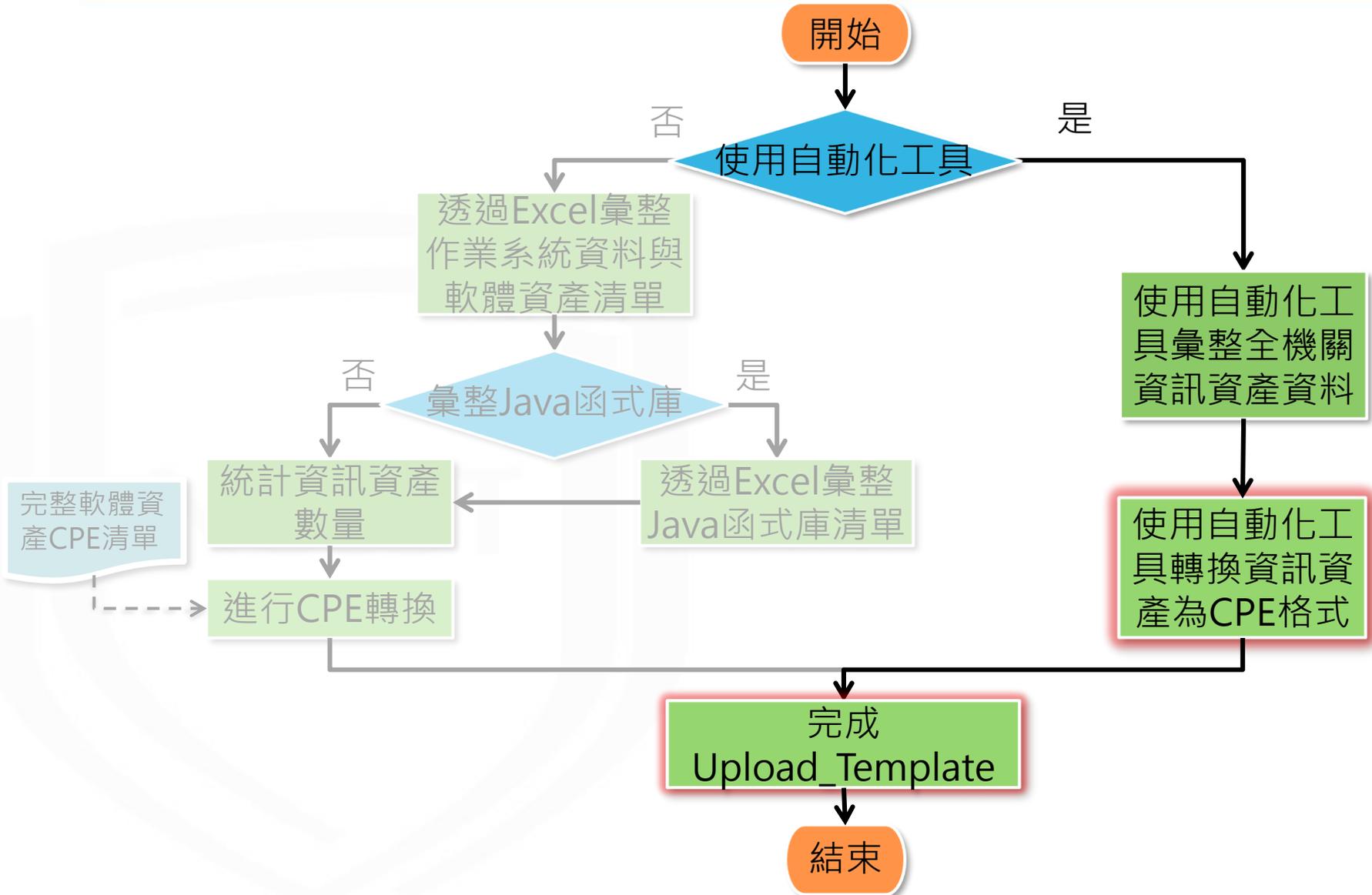


使用自動化工具彙整資訊資產

- 自動蒐集資通系統與使用者電腦作業系統、軟體資產及已安裝KBID等內容
- 自動去識別化整併為全機關資產清單，並提供反查對照功能，便於機關管理資產清單
- 透過排程定時回傳盤點結果予自動化工具中控台



資訊資產正規化作業流程



使用自動化工具轉換資訊資產格式

- 自動更新NVD最新CPE條目，並將常見資產格式轉換為CPE格式
- 自動依據VANS系統所需上傳之欄位格式完成 Upload_Template



自動化工具中控台



資產清單



轉換CPE功能

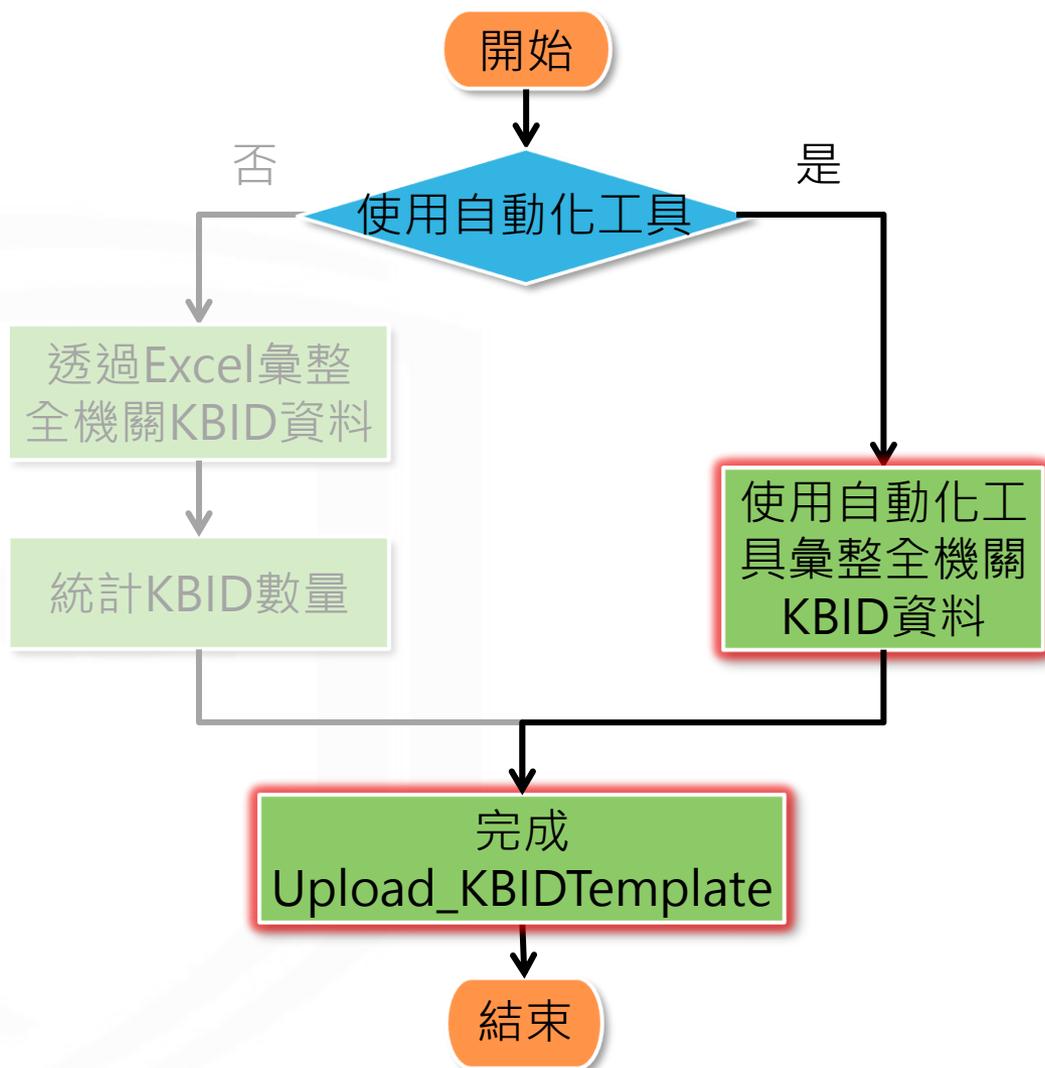


Upload_Template

已安裝KBID正規化作業 (自動化工具)

NCCST

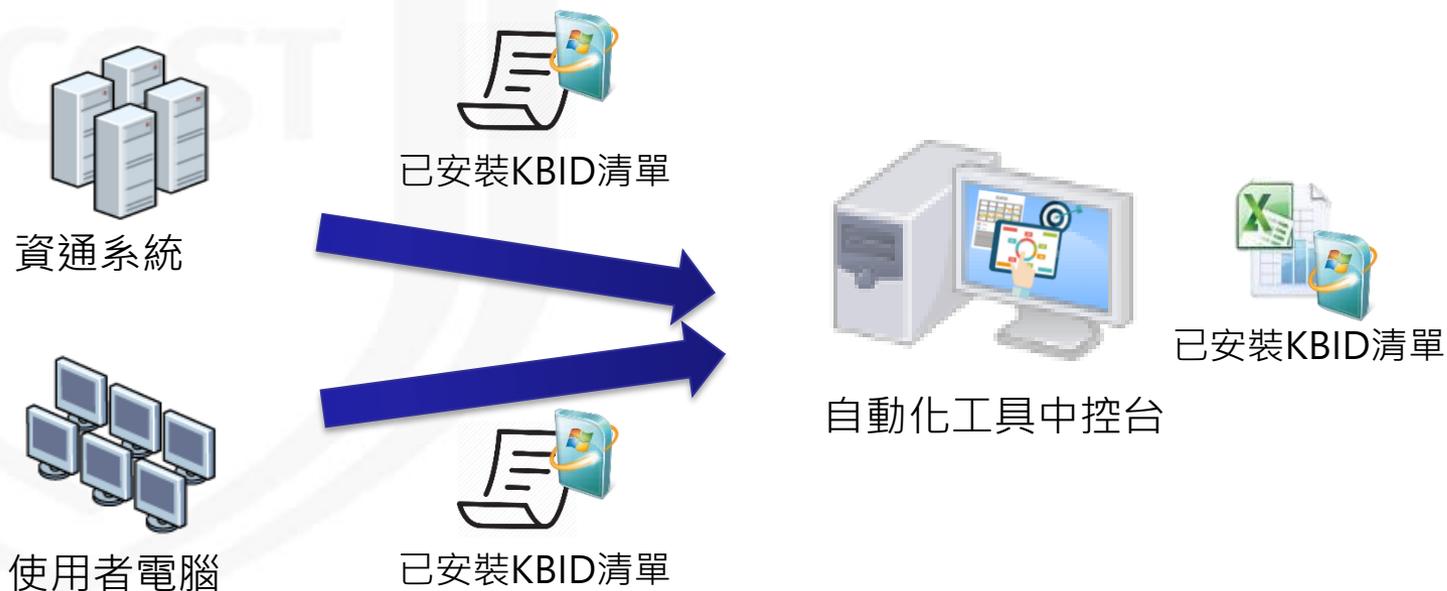
已安裝KBID正規化作業流程



使用自動化工具彙整已安裝KBID



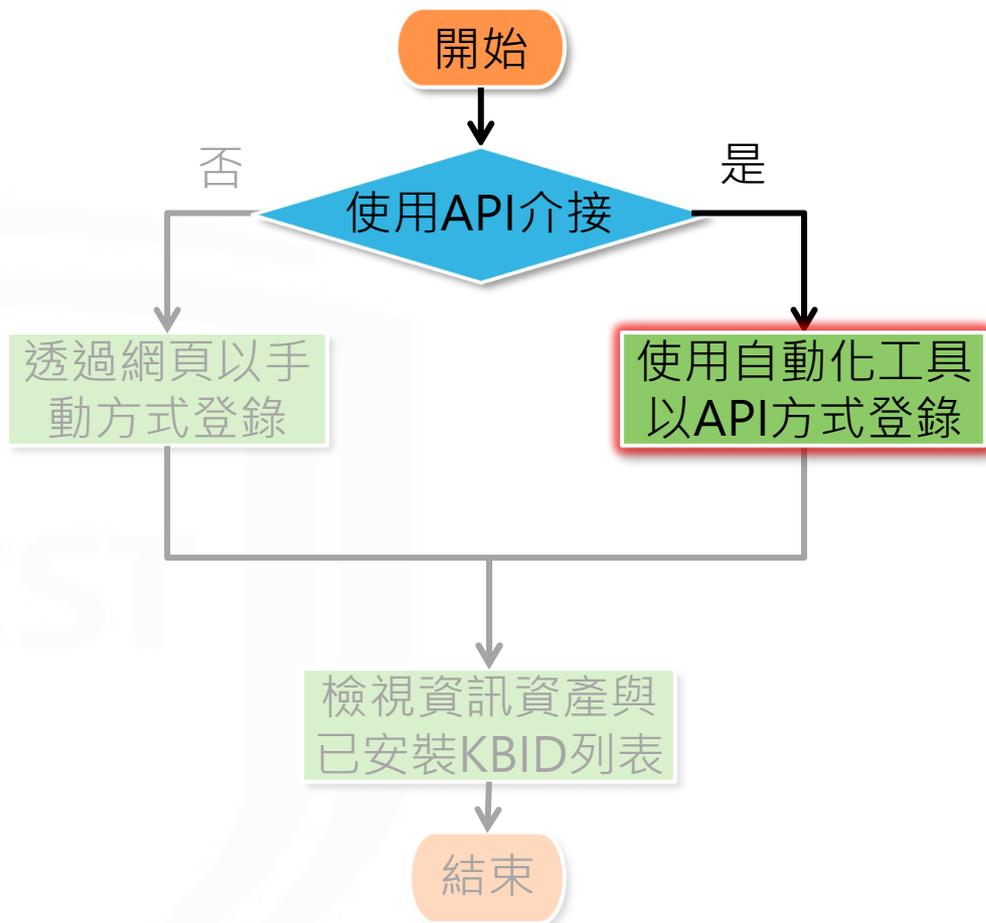
- 自動化蒐集與彙整資通系統與使用者電腦之已安裝KBID
- 透過排程定時回傳盤點結果予自動化工具中控台
- 自動去識別化整併為全機關已安裝KBID清單，並提供反查對照功能，便於機關管理已安裝KBID清單
- 完成已安裝KBID清單



導入作業流程



登錄作業流程



使用自動化工具以API方式登錄(1/3)



- 前置作業申請-於VANS系統申請API Key
 - STEP1：以系統管理者帳號登入VANS系統
 - STEP2：設定管理>資產管理API設定
 - STEP3：點選「重新產生API Key」



使用自動化工具以API方式登錄(2/3)



● 前置作業申請-填寫API介接IP申請單

- STEP1 : 以系統管理者帳號登入VANS系統
- STEP2 : 設定管理 > 資產管理API設定
- STEP3 : 輸入欲申請之IP，並送出
- STEP4 : 於VANS專區下載API介接申請表單填寫並核章，完成後提供資安處審核(<https://www.nccst.nat.gov.tw/Vans?lang=zh>)

設定管理 > 資產管理API設定

機關資產管理API key

使用以下API key存取系統

IP設定

請輸入欲申請之IP

送出

已申請IP地址	狀態	刪除
---------	----	----

政府機關資安弱點通報機制(VANS)專區

政府機關資安弱點通報機制(Vulnerability Alert and Notification System, 簡稱VANS)結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實資通安全管理法之資產盤點與風險評估應辦事項。

歡迎透過意見信箱提供您的寶貴意見！

申請作業表單 教育訓練教材 數位教材影片 FAQ

帳號申請說明文件
政府機關資安弱點通報系統(VANS系統)帳號申請說明文件v1.0_1100408.pdf
SHA256:MvVITjVzF/CvIFzC+4ojJ6dAEJ8NuxnZSmejR7BGuzl=

帳號申請表單
附表-政府機關資安弱點通報系統(VANS系統)機關管理者帳號申請(異動)單v1.3_1100419.xlsx
SHA256:p21gleXAZncLPjDH7vF0oIjcZmV/iaBE5yJBTrH7SbM=

API介接申請表單
政府機關資安弱點通報系統(VANS系統)API介接申請(異動)單v1.2_1100419.xlsx
SHA256:nQG92BL9q/twJLJxPsLUF9RawMhLQ6veWCA7oQcmbk8=

使用自動化工具以API方式登錄(3/3)



- 待收到審核結果通知信，說明IP完成開通時，即可使用自動化工具以API方式登錄資訊資產與已安裝KBID

API Key

機關資訊

API傳輸網址



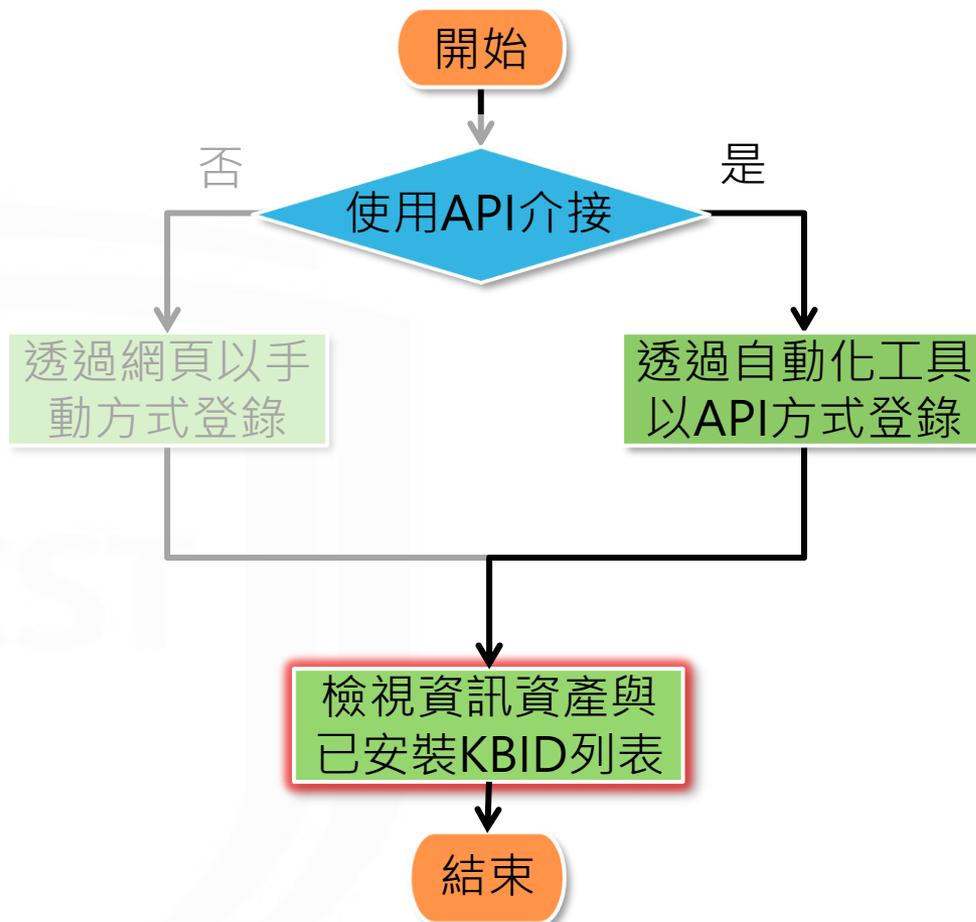
自動化工具



VANS系統



登錄作業流程



檢視資訊資產與已安裝KBID列表

- 可於**資訊資產管理**查看已登錄之資產項目
 - 資訊資產管理 > 資通系統資產列表/使用者電腦資產列表
- 點選右邊「**切換至已安裝KBID列表**」可檢視已安裝KBID項目



資訊資產管理 > 資通系統資產列表

CPE清單 / 範本下載 資產 / 已安裝KBID上傳 資產清單匯出 **切換至已安裝KBID列表**

資訊資產列表

資產名稱	資產廠商	資產版本	CPE2.3
Apache Tomcat 9.0 Tomcat9 (remove only)	The Apache Software Foundation	9.0.16	cpe:2.3:a:apache:tomcat:9.0.16:*:*:*:*:*
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beanutils:1.8.0:*:*:*:*:*



資訊資產管理 > 資通系統資產列表

CPE清單 / 範本下載 資產 / 已安裝KBID上傳 資產清單匯出 **切換至資訊資產列表**

已安裝KBID列表 新增已安裝KBID

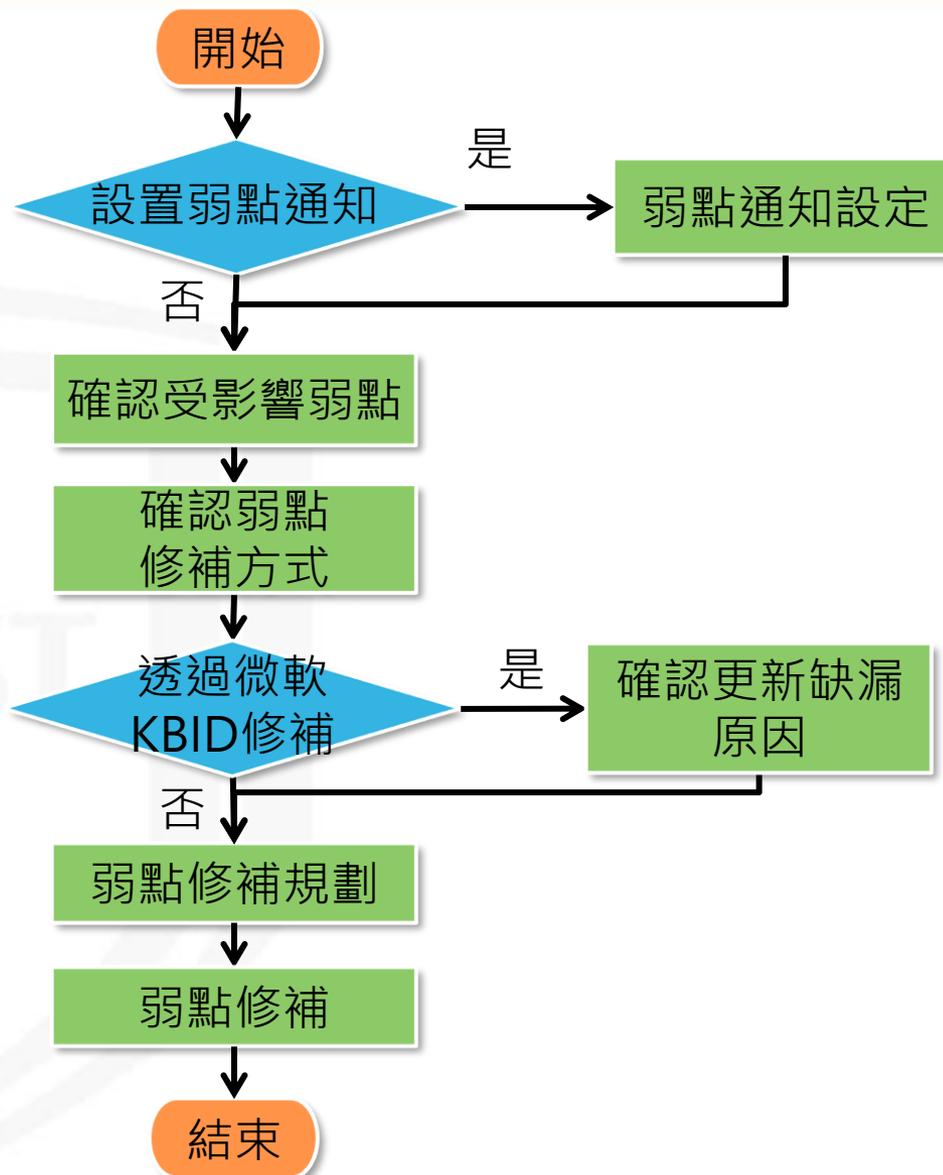
搜尋

KBID	數量	受影響產品名稱	刪除
KB2868626	1	詳細清單	刪除
KB2883200	1	詳細清單	刪除
KB2887595	1	詳細清單	刪除

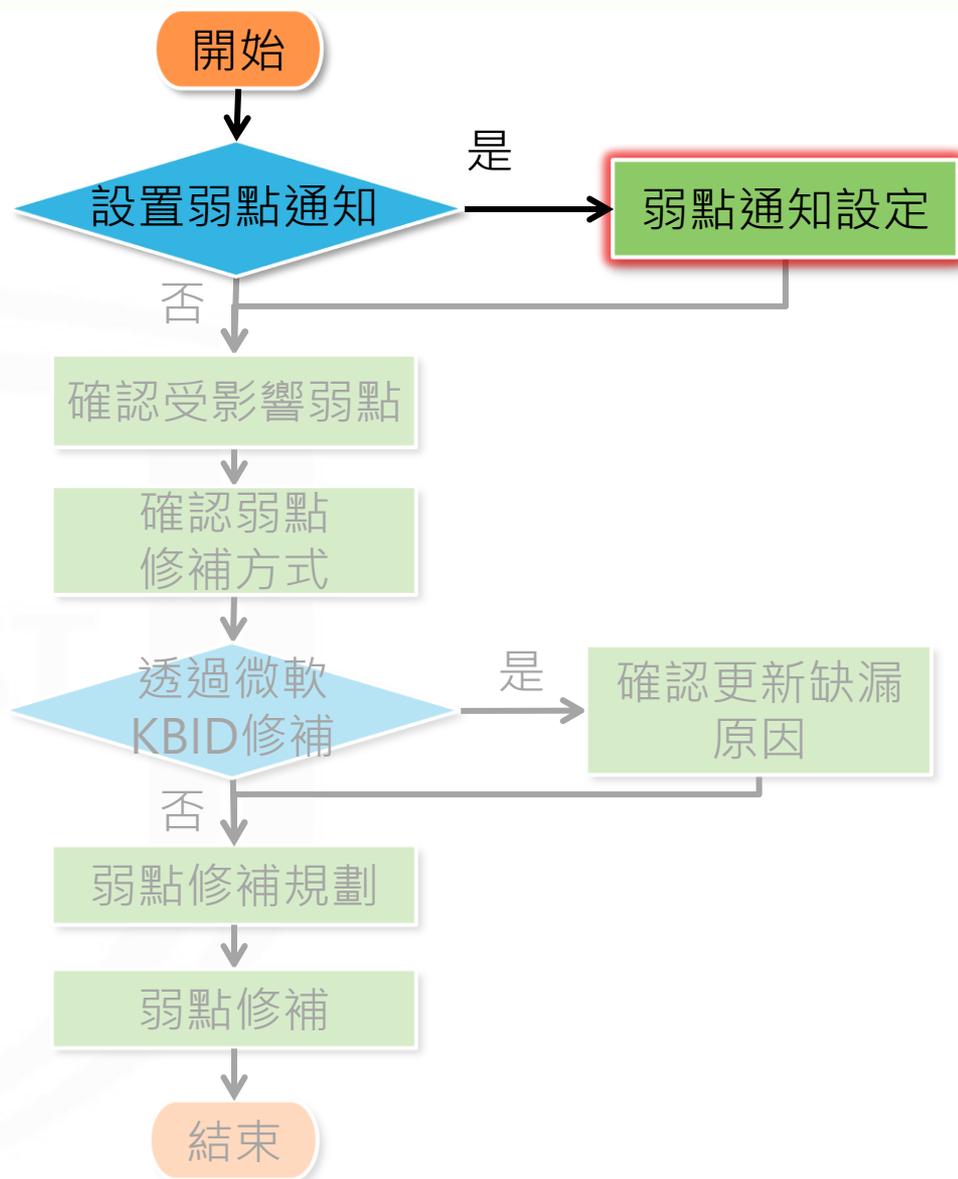
導入作業流程



弱點通知與修補規劃作業流程



弱點通知與修補規劃作業流程



弱點通知設定(1/3)

- 首次登入VANS系統，需先進行弱點通知設定
 - 弱點通知設定包含通知開關、CVSS分數門檻及接收通知Email

政府機關資安弱點通報系統

student2

設定 > 弱點通知設定

弱點通知設定

i 由於您為首次登入本系統，請完成以下設定，以便後續進行系統通知

請選擇當系統比對到您的軟體資產具有弱點時，是否發送電子郵件通知。

OFF **通知開關**

請輸入當弱點嚴重程度達幾分(含)以上時，發送電子郵件通知。(嚴重程度為1-10分，10分為滿分)

調整設定CVSS分數門檻

請輸入電子郵件信箱資訊，以便後續接收系統通知。

設定接收通知Email

+ 新增電子郵件欄位

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

可參考ISMS弱點修復基準
設置CVSS分數門檻

弱點通知設定(2/3)

- 後續變更弱點通知設定，可於通知設定調整
 - 設定管理 > 通知設定



Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

可參考ISMS弱點修復基準
設置CVSS分數門檻

弱點通知設定(3/3)

- 資訊資產與NVD弱點資料庫自動比對後，若有開啟弱點通知功能，VANS系統將於比對出高於CVSS分數門檻之弱點時寄送通知信

- 寄送通知信予**接收通知Email**
- 於VANS系統上顯示**弱點比對通知**

敬啟者 您好：
此為「政府機關資安弱點通報系統」之通知郵件。

貴機關之所以收到此通知信件，在於貴機關於 VANS 系統所登錄之資訊資產，經過系統比對弱點資料庫後，發現存有風險項目，建議貴機關對資訊資產風險進行修補，以避免資安風險。修補作業完成後，再煩請貴機關至 VANS 系統進行資訊更新，以協助本中心掌握修補情況。謝謝。

VANS 系統網頁連結：
<https://vans.nccst.nat.gov.tw/>

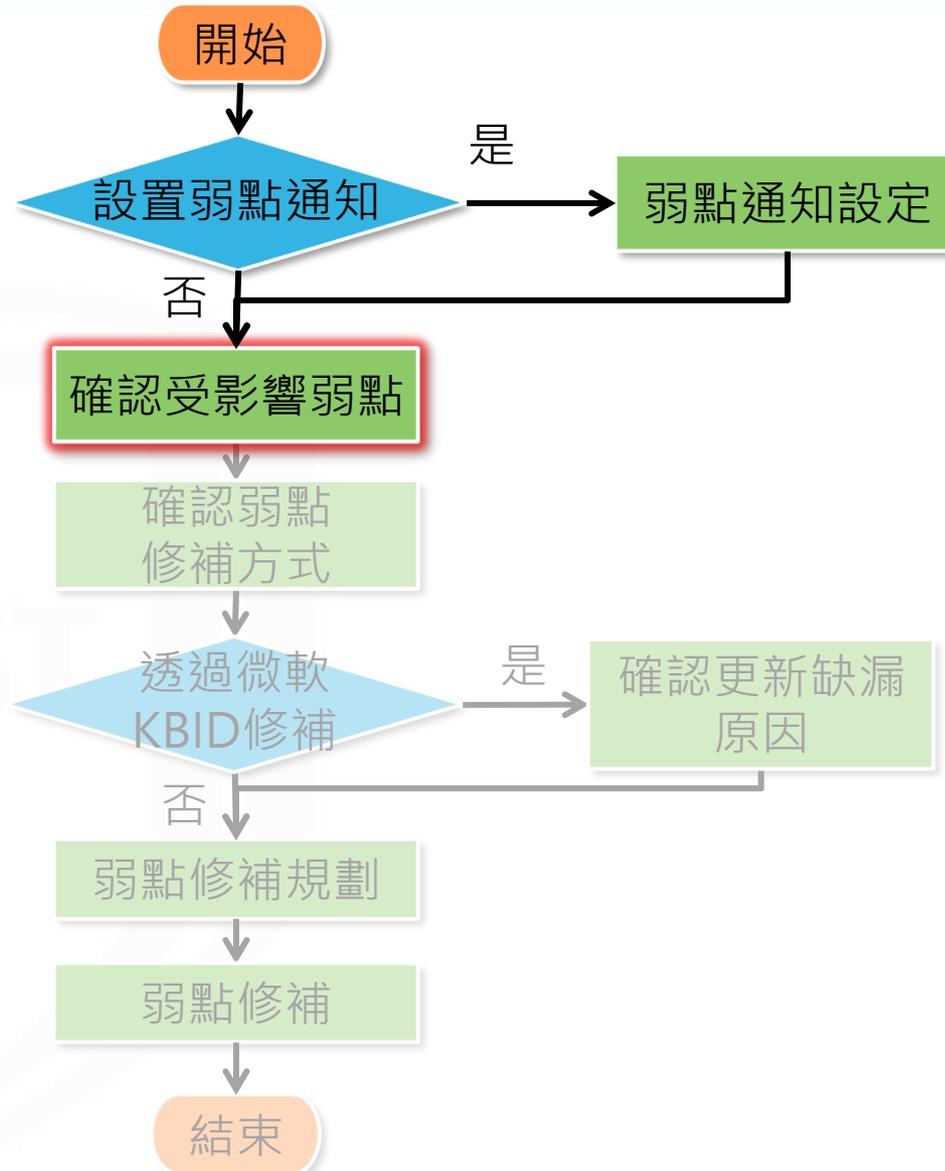
如有任何疑問，聯絡資訊如下：
行政院國家資通安全會報技術服務中心(技服中心)
服務電話：(02)6631-6458
服務信箱：VansService@nccst.nat.gov.tw

- 同一項資產的同一個弱點只會於**首次比對到時進行1次通知**，之後**不會再出現相同之弱點通知**



通知時間	資產數量	弱點數量	詳細資訊	通知顯示	
2019-11-17 00:37:17	1	171	開啟	ON	<input type="checkbox"/>
2019-11-08 16:39:21	28	456	開啟	ON	<input type="checkbox"/>

弱點通知與修補規劃作業流程



確認受影響弱點-資訊資產風險列表



● 於資訊資產風險列表，檢視各資訊資產存在之弱點

– 資產風險狀態 > 資通系統風險狀態 / 使用者電腦風險狀態 > 資訊資產風險列表

- 首頁
- 機關總覽
- 資訊資產管理
- 資產風險狀態
 - 資通系統風險狀態
 - 資訊資產風險列表**
 - 弱點關聯列表
 - 弱點比對通知
 - 弱點處理情形回報
- 使用者電腦風險狀態
- 資訊查詢
- 設定管理

資產風險狀態 > 資通系統風險狀態 > 資訊資產風險列表

下載弱點清單 上傳弱點改善措施

全部 技服中心

資訊

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	風險指數	弱點數量	未填寫改善措施數量	弱點資訊
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beanutils:1.8.0:*:*:*:*:*	1	7.50	2	2	詳細資訊
commons-fileupload	N/A	1.3.2	cpe:2.3:a:apache:commons_fileupload:1.3.2:*:*:*:*	1	7.50	1	1	詳細資訊

Apache

詳細資訊

填寫勾選改善措施 全部勾選 全部取消

	CVE編號	CVSS	發佈時間	更新時間	改善措施
<input type="checkbox"/>	CVE-2019-10086	7.5	2019-08-21 05:15:00	2021-07-21 07:15:00	填寫改善措施
<input type="checkbox"/>	CVE-2014-0114	7.5	2014-04-30 18:49:00	2021-01-27 02:15:00	填寫改善措施

顯示第 1 到第 2 項記錄，總共 2 項記錄

關閉

確認受影響弱點-弱點關聯列表



- 若欲查詢特定弱點，透過弱點關聯列表搜尋CVE編號或查詢弱點爆發時間區間，以確認受影響之資訊資產與範圍
 - 資產風險狀態 > 資通系統風險狀態/使用者電腦風險狀態 > 弱點關聯列表

資產風險狀態 > 資通系統風險狀態 > 弱點關聯列表

技服中心

請輸入CVE編號

查詢

起始時間 2021-07-01

結束時間 2021-09-01

查詢

資訊

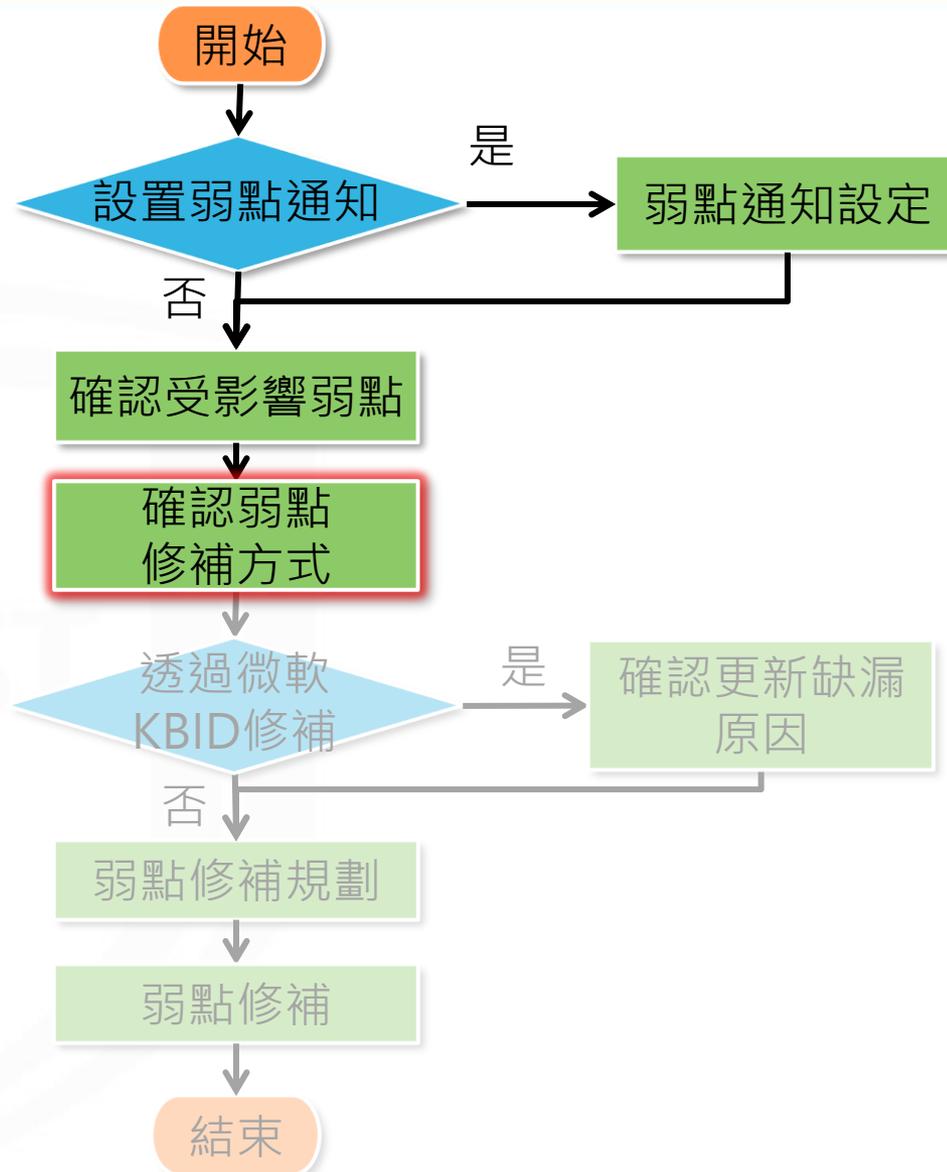
CVE-2021-34510 CVSS Score: 4.6 發布時間: 2021-07-15 02:15:00 更新時間: 2021-08-19 01:08:00

影響資產名稱	影響資產廠商	影響資產版本	影響CPE2.3	比對時間
Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763	cpe:2.3:o:microsoft:windows_server_2019:-:*:*:datacenter:*x64:*	2021-08-18 05:03:28

顯示第 1 到第 1 項記錄，總共 1 項記錄

CVE-2021-30640 CVSS Score: 6.4 發布時間: 2021-07-12 11:15:00 更新時間: 2021-08-10 11:08:00

弱點通知與修補規劃作業流程



確認弱點修補方式(1/4)

- 可至NVD官網確認弱點修補方式
- 以資訊資產風險列表為例，點選「詳細資訊」檢視JDK 1.8.0 Update 202之弱點資訊

資產風險狀態 > 資通系統風險狀態 > 資訊資產風險列表

[下載弱點清單](#)
[上傳弱點改善措施](#)
全部
技服中心

資訊

搜尋

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	風險指數	弱點數量	未填寫改善措施數量	弱點資訊
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beanutils:1.8.0:****:*	1	7.50	2	2	詳細資訊
commons-fileupload	N/A	1.3.2	cpe:2.3:a:apache:commons_fileupload:1.3.2:****:*	1	7.50	1	1	詳細資訊
Java 8 Update 202 (64-bit)	Oracle Corporation	8.0.2020.8	cpe:2.3:a:oracle:jdk:1.8.0:update202:****:*	1	7.00	34	34	詳細資訊
Microsoft Office 專業增強版 2019 - zh-tw	Microsoft Corporation	16.0.14228.20250	cpe:2.3:a:microsoft:office:2019:****:~:*	1	7.10	184	184	詳細資訊

確認弱點修補方式(2/4)

- 點選弱點編號，可查看弱點描述與相關連結

詳細資訊

CVE編號	CVSS	發布時間	更新時間	改善措施	填寫勾選改善措施	全選
CVE-2014-0429	10	2014-04-16 08:55:00	2018-01-05 10:29:00	填寫改善措施	<input type="checkbox"/>	
CVE-2014-0432						
CVE-2014-0446						



CVE資訊

[查看弱點描述](#) 關閉

CVE-2014-0429 NVD-CWE-noinfo

Summary Unspecified vulnerability in Oracle Java SE 5.0u61, 6u71, 7u51, and 8; JRockit R27.8.1 and R28.3.1; and Java SE Embedded 7u51 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.

[NVD官網弱點說明連結](#) <https://nvd.nist.gov/vuln/detail/CVE-2014-0429> [查看NVD官網說明](#)

CVSS Score: 10

Access Vector

AccessComplexity: LOW

AccessVector: NETWORK

Authentication: NONE

確認弱點修補方式(3/4)

- 參閱NVD官網建議弱點修補方式

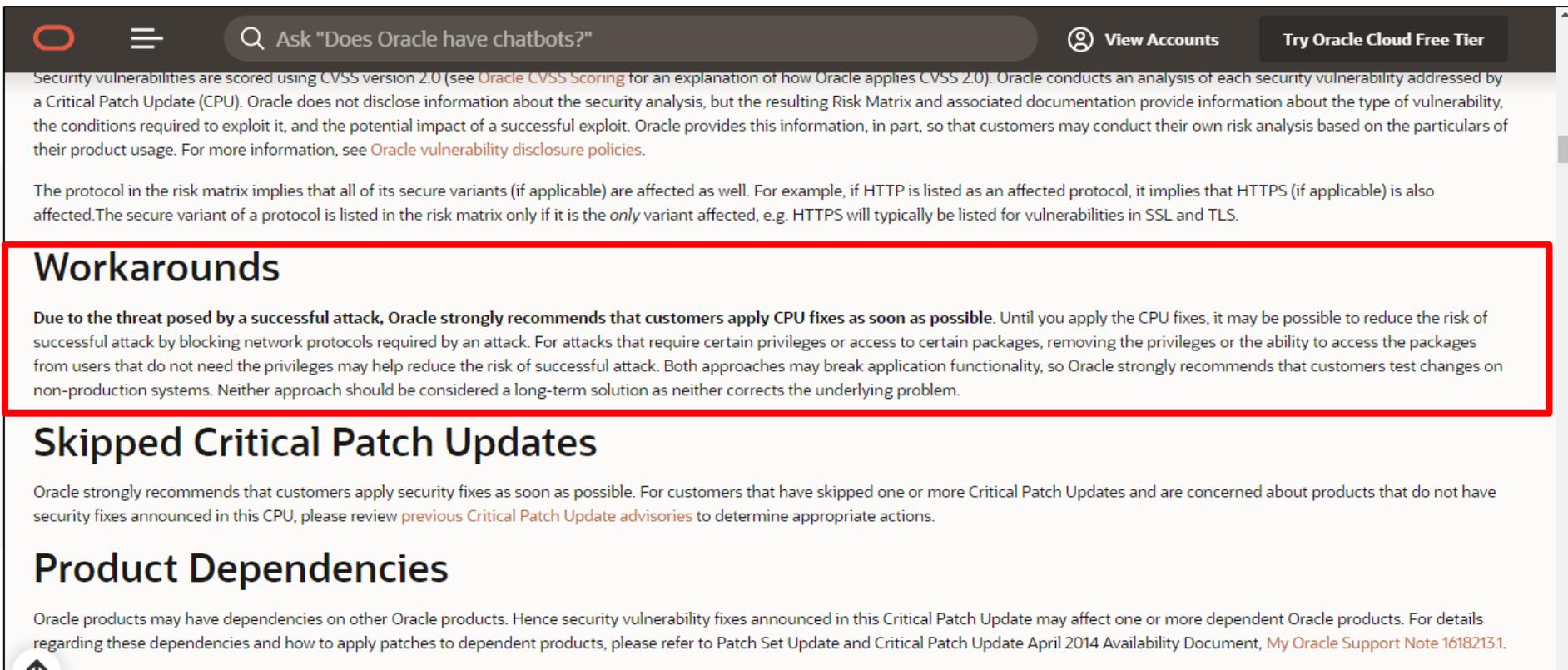
References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10698	
http://marc.info/?l=bugtraq&m=140852974709252&w=2	
http://rhn.redhat.com/errata/RHSA-2014-0675.html	
http://rhn.redhat.com/errata/RHSA-2014-0685.html	
http://security.gentoo.org/glsa/glsa-201406-32.xml	
http://security.gentoo.org/glsa/glsa-201502-12.xml	
http://www.debian.org/security/2014/dsa-2912	原廠說明連結
http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html	Vendor Advisory
http://www.securityfocus.com/bid/66856	

確認弱點修補方式(4/4)

- 透過弱點詳細資訊中的連結，查閱原廠或相關廠商建議弱點修補方式



Security vulnerabilities are scored using CVSS version 2.0 (see [Oracle CVSS Scoring](#) for an explanation of how Oracle applies CVSS 2.0). Oracle conducts an analysis of each security vulnerability addressed by a Critical Patch Update (CPU). Oracle does not disclose information about the security analysis, but the resulting Risk Matrix and associated documentation provide information about the type of vulnerability, the conditions required to exploit it, and the potential impact of a successful exploit. Oracle provides this information, in part, so that customers may conduct their own risk analysis based on the particulars of their product usage. For more information, see [Oracle vulnerability disclosure policies](#).

The protocol in the risk matrix implies that all of its secure variants (if applicable) are affected as well. For example, if HTTP is listed as an affected protocol, it implies that HTTPS (if applicable) is also affected. The secure variant of a protocol is listed in the risk matrix only if it is the *only* variant affected, e.g. HTTPS will typically be listed for vulnerabilities in SSL and TLS.

Workarounds

Due to the threat posed by a successful attack, Oracle strongly recommends that customers apply CPU fixes as soon as possible. Until you apply the CPU fixes, it may be possible to reduce the risk of successful attack by blocking network protocols required by an attack. For attacks that require certain privileges or access to certain packages, removing the privileges or the ability to access the packages from users that do not need the privileges may help reduce the risk of successful attack. Both approaches may break application functionality, so Oracle strongly recommends that customers test changes on non-production systems. Neither approach should be considered a long-term solution as neither corrects the underlying problem.

Skipped Critical Patch Updates

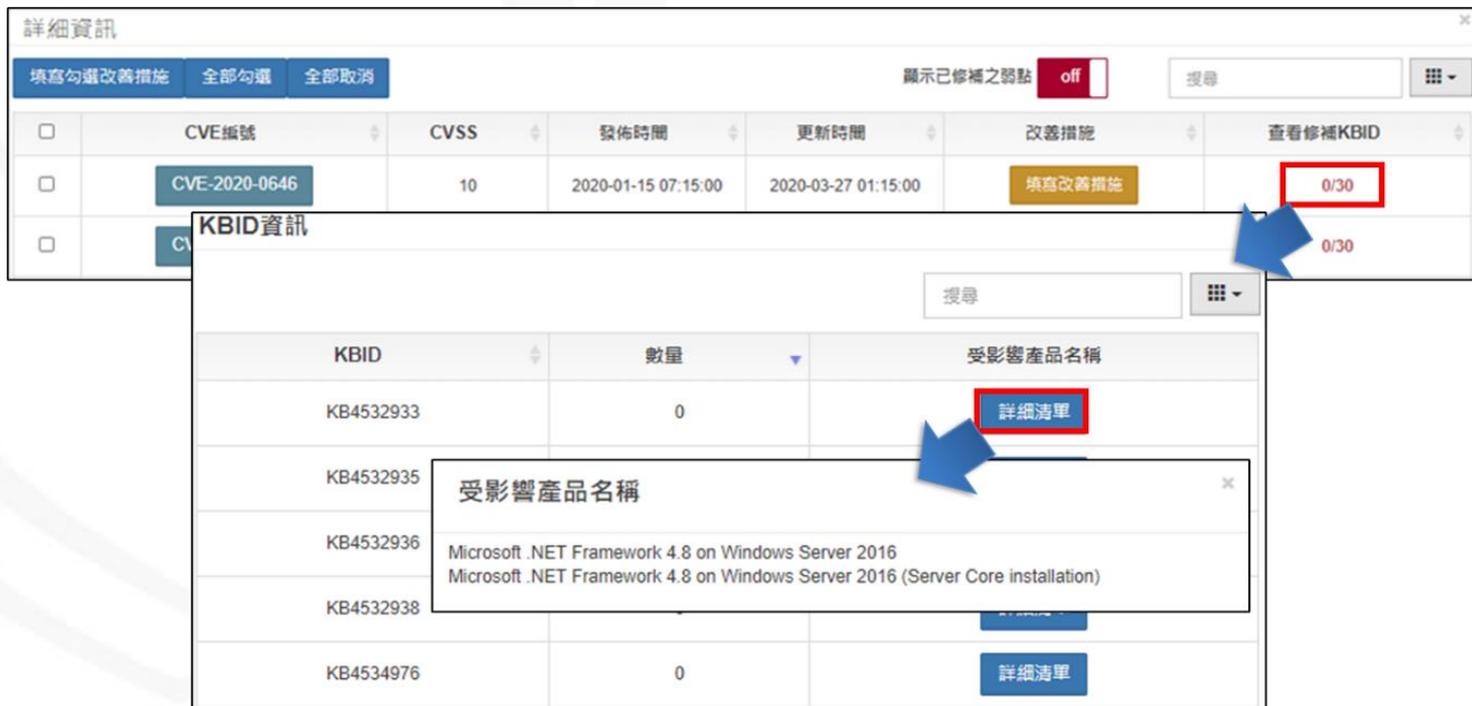
Oracle strongly recommends that customers apply security fixes as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security fixes announced in this CPU, please review [previous Critical Patch Update advisories](#) to determine appropriate actions.

Product Dependencies

Oracle products may have dependencies on other Oracle products. Hence security vulnerability fixes announced in this Critical Patch Update may affect one or more dependent Oracle products. For details regarding these dependencies and how to apply patches to dependent products, please refer to Patch Set Update and Critical Patch Update April 2014 Availability Document, [My Oracle Support Note 1618213.1](#).

確認弱點修補方式-微軟類

- 微軟類之CVE，可透過詳細資訊中的「查看修補KBID」欄位
 - 呈現已安裝KBID與應安裝KBID數量
 - 紅色為尚有缺漏KBID，綠色為完成安裝KBID
 - 點選檢視可修補該弱點之KBID

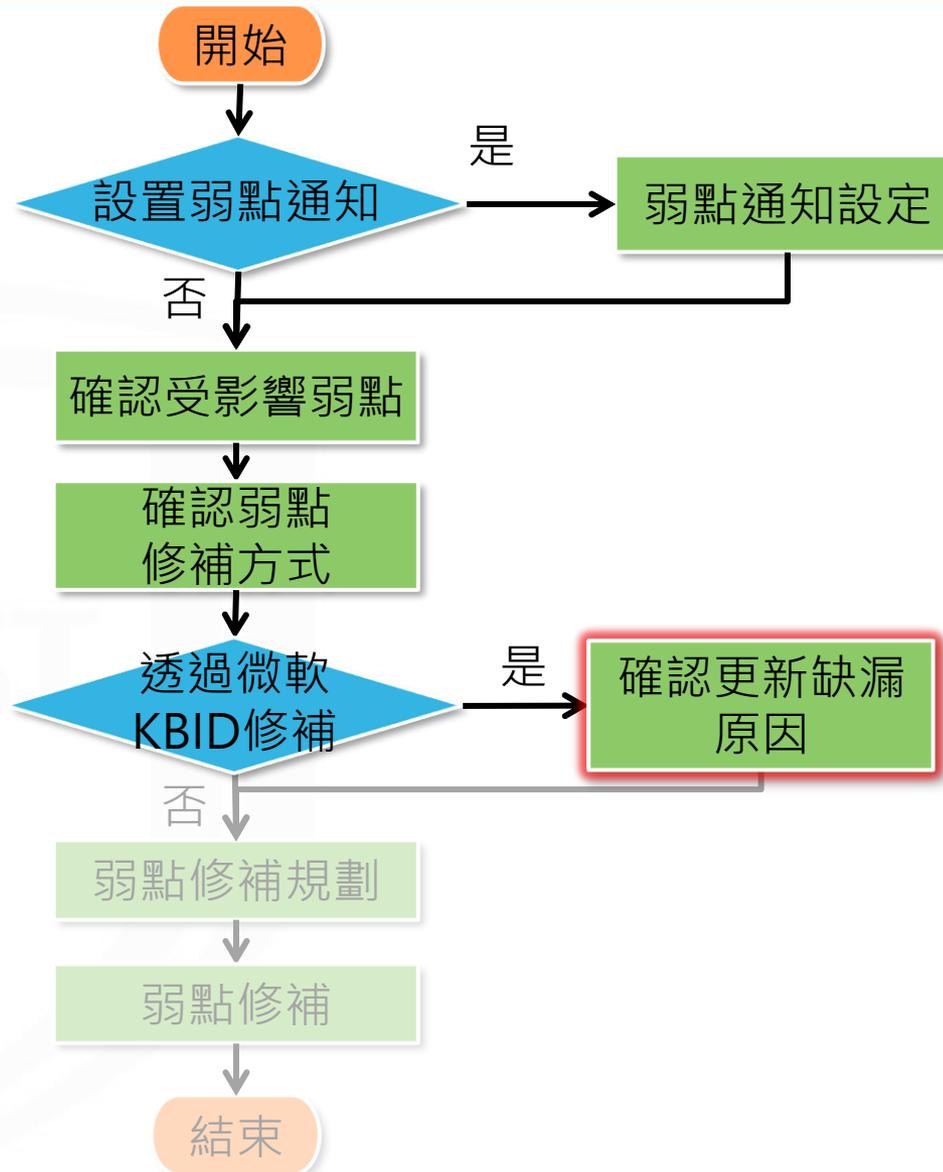


The screenshot displays a web interface for vulnerability management. The top section, titled '詳細資訊' (Detailed Information), shows a table of CVEs. The first row is for CVE-2020-0646, with a CVSS score of 10, published on 2020-01-15, and updated on 2020-03-27. The '查看修補KBID' (View KBID) column shows '0/30' in red, indicating that no KBIDs are currently installed for this CVE. A blue arrow points from this '0/30' to a second window titled 'KBID資訊' (KBID Information). This window shows a table of KBIDs with columns for 'KBID', '數量' (Quantity), and '受影響產品名稱' (Affected Product Name). The first row is for KB4532933, with a quantity of 0. A red box highlights the '詳細清單' (Detailed List) button next to it. A second blue arrow points from this button to a third window titled '受影響產品名稱' (Affected Product Name), which lists the affected products: 'Microsoft .NET Framework 4.8 on Windows Server 2016' and 'Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)'. A third blue arrow points from this window back to the 'KBID資訊' window.

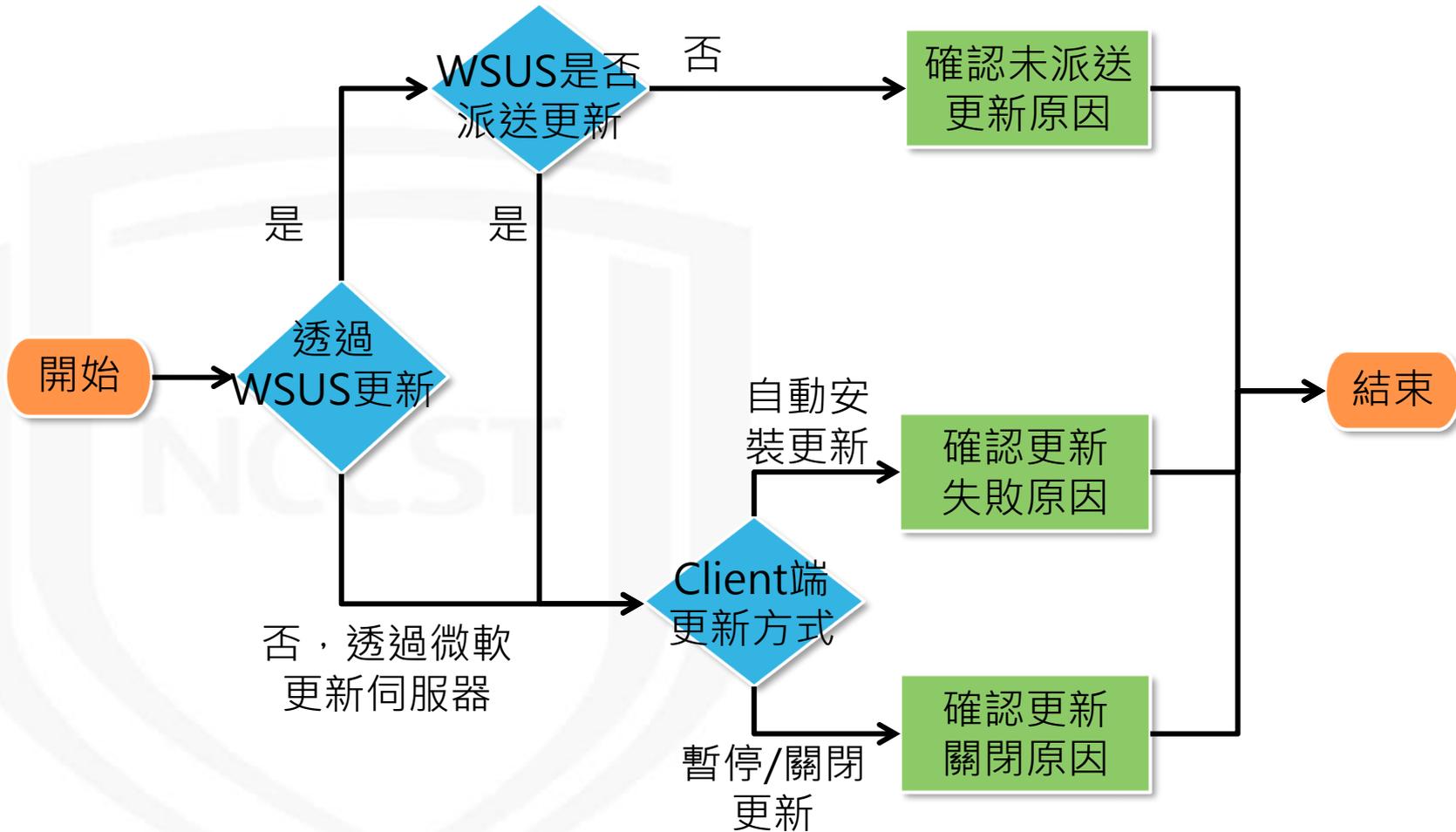
CVE編號	CVSS	發佈時間	更新時間	改善措施	查看修補KBID
CVE-2020-0646	10	2020-01-15 07:15:00	2020-03-27 01:15:00	填寫改善措施	0/30

KBID	數量	受影響產品名稱
KB4532933	0	詳細清單
KB4532935		受影響產品名稱
KB4532936		Microsoft .NET Framework 4.8 on Windows Server 2016 Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)
KB4532938		
KB4534976	0	詳細清單

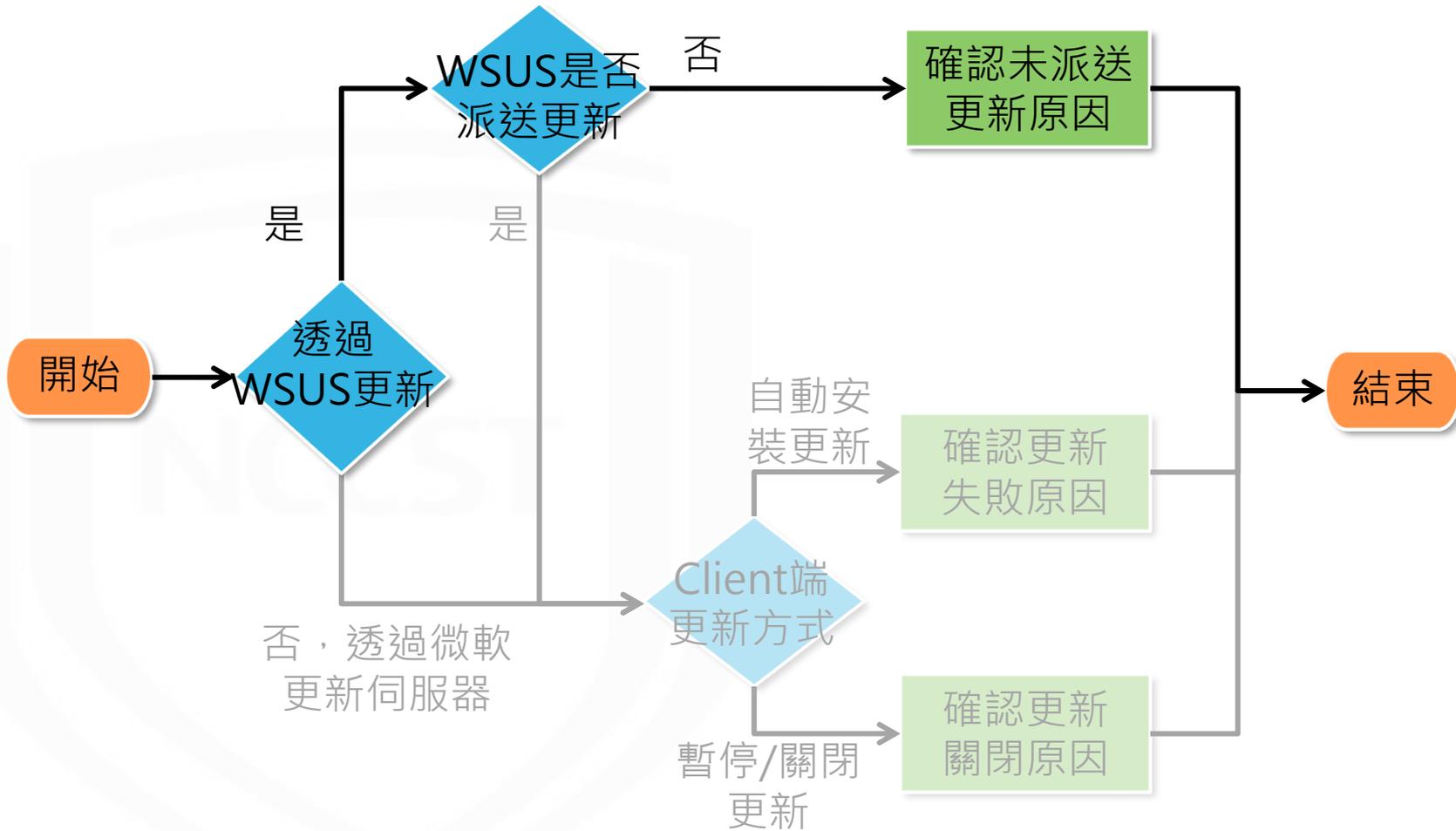
弱點通知與修補規劃作業流程



確認更新缺漏原因



確認更新缺漏原因



確認WSUS更新派送狀態(1/2)



- 若透過WSUS派送更新，需至WSUS伺服器確認

下列設定

- 可搭配資訊資產清單或資產管理系統，確認機關內**所有微軟系列品項**，確保**完整勾選所需之產品**
- 確認有勾選「**安全性更新**」類別

選項 > 產品和分類 > 產品

您可以指定要對它同步處理更新的产品。

產品(P):

- Windows 10 Version 1803 and Later Upgrade & Servicing Drivers
- Windows 10, version 1809 and later, Servicing Drivers
- Windows 10, version 1809 and later, Upgrade & Servicing Drivers
- Windows 10, version 1903 and later, Servicing Drivers
- Windows 10, version 1903 and later, Upgrade & Servicing Drivers
- Windows 10, version 1903 and later
- Windows 10, Vibranium and later, Servicing Drivers
- Windows 10, Vibranium and later, Upgrade & Servicing Drivers
- Windows 10
- Windows 2000
- Windows 7
- Windows 8 Dynamic Update
- Windows 8 Embedded
- Windows 8 Language Interface Packs

所有產品，包括未來要加入的產品。

確定 取消 套用(A)

選項 > 產品和分類 > 分類

您可以指定您要同步處理哪些分類的更新。

分類(C):

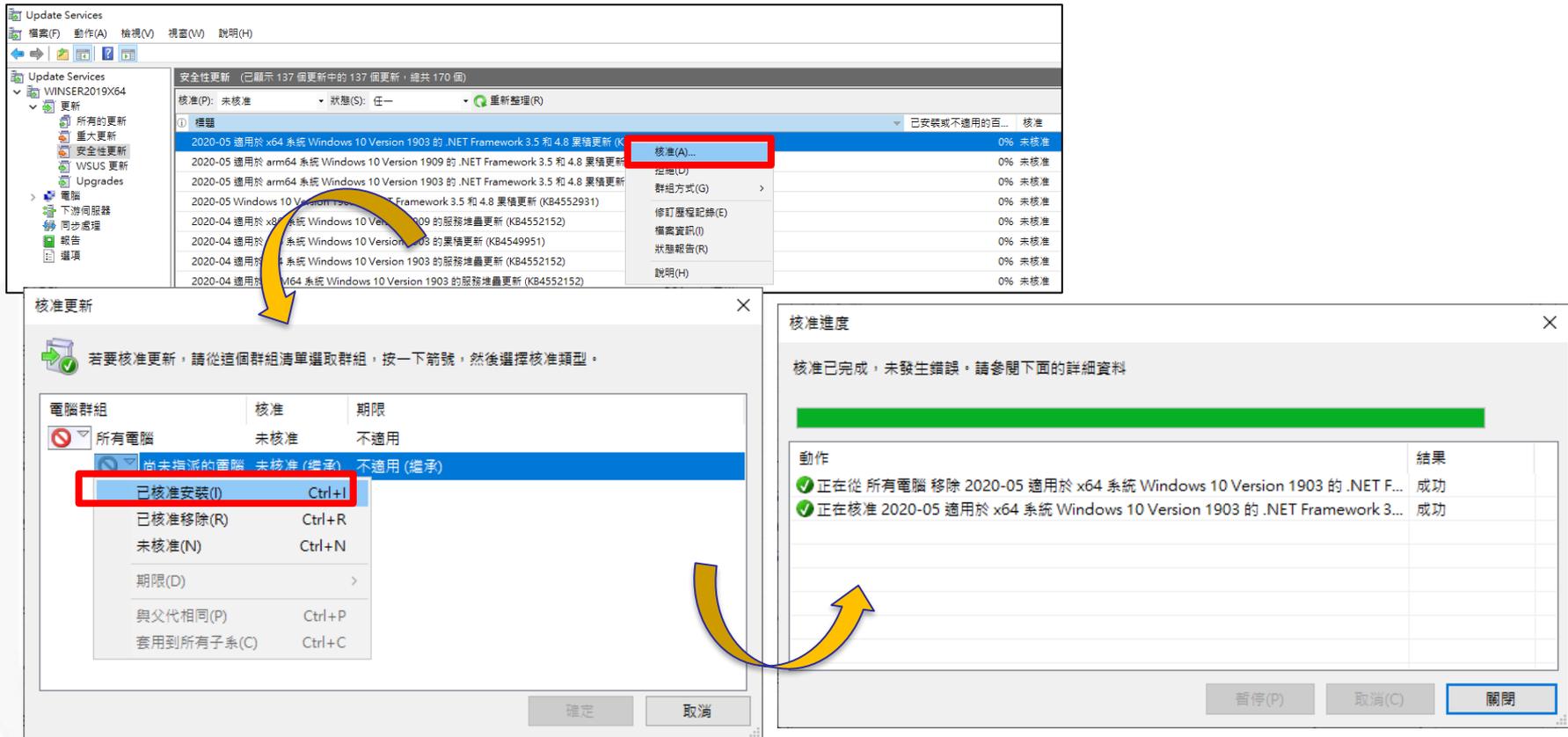
- 所有分類
- Service Pack
- Upgrades
- 工具
- 功能套件
- 安全性更新
- 更新
- 更新彙總套件
- 定義更新
- 重大更新
- 驅動程式
- 驅動程式集

所有分類，包括未來要加入的分類。

確定 取消 套用(A)

確認WSUS更新派送狀態(2/2)

- 確認缺漏更新是否已於WSUS核准派送

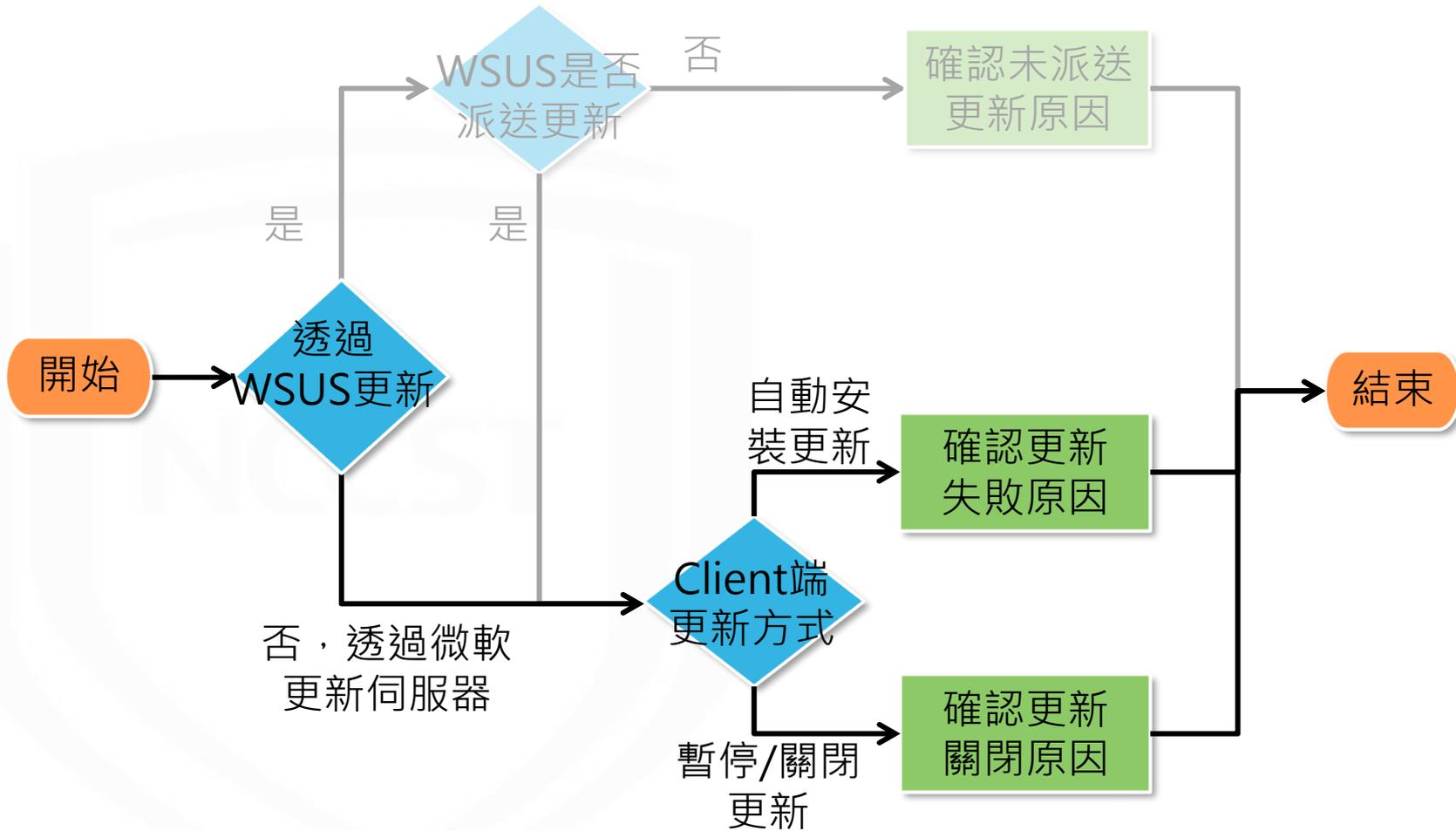


The screenshot illustrates the process of approving updates in the WSUS console. The main window shows a list of updates, with the context menu for '2020-05 適用於 x64 系統 Windows 10 Version 1903 的 .NET Framework 3.5 和 4.8 累積更新 (KB4552152)' open, highlighting the '核准(A)...' option. A yellow arrow points from this option to the '核准更新' dialog box. In this dialog, the '尚未指派的管理' group is selected, and the '已核准安裝(I)' option is highlighted with a red box. Another yellow arrow points from this option to the '核准進度' dialog box. The progress dialog shows a green progress bar and a table of actions:

動作	結果
正在從 所有電腦 移除 2020-05 適用於 x64 系統 Windows 10 Version 1903 的 .NET F...	成功
正在核准 2020-05 適用於 x64 系統 Windows 10 Version 1903 的 .NET Framework 3...	成功

- 若上述確認完畢後，仍有缺漏更新，則需確認是否為Client端問題

確認更新缺漏原因



確認Client端更新狀態

- Client更新失敗時，建議臨機於「Windows Update」頁面查看更新失敗之更新項目與錯誤代碼，並至微軟官方頁面查詢錯誤代碼含意，並尋找解決方案
 - <https://docs.microsoft.com/zh-tw/windows/deployment/update/windows-update-error-reference>
- 另需確認Client端更新是否遭關閉或暫停，而導致未正常更新



Microsoft | Docs 文件 Learn Q&A 程式碼範例

文件 / Windows / 部署

依元件的 Windows 更新錯誤代碼

2018/09/18

適用對象：Windows 10

本節列出 Microsoft Windows Update

透過Ctrl+F搜尋錯誤代碼

自動更新錯誤

錯誤碼	訊息	描述
0x80243FFF	WU_E_AUCLIENT_UNEXPECTED	有另一個WU_E_AUCLIENT_*錯誤代碼未涵蓋的使用者介面錯誤。
0x8024A000	WU_E_AU_NOSERVICE	自動更新無法服務傳入的要求。

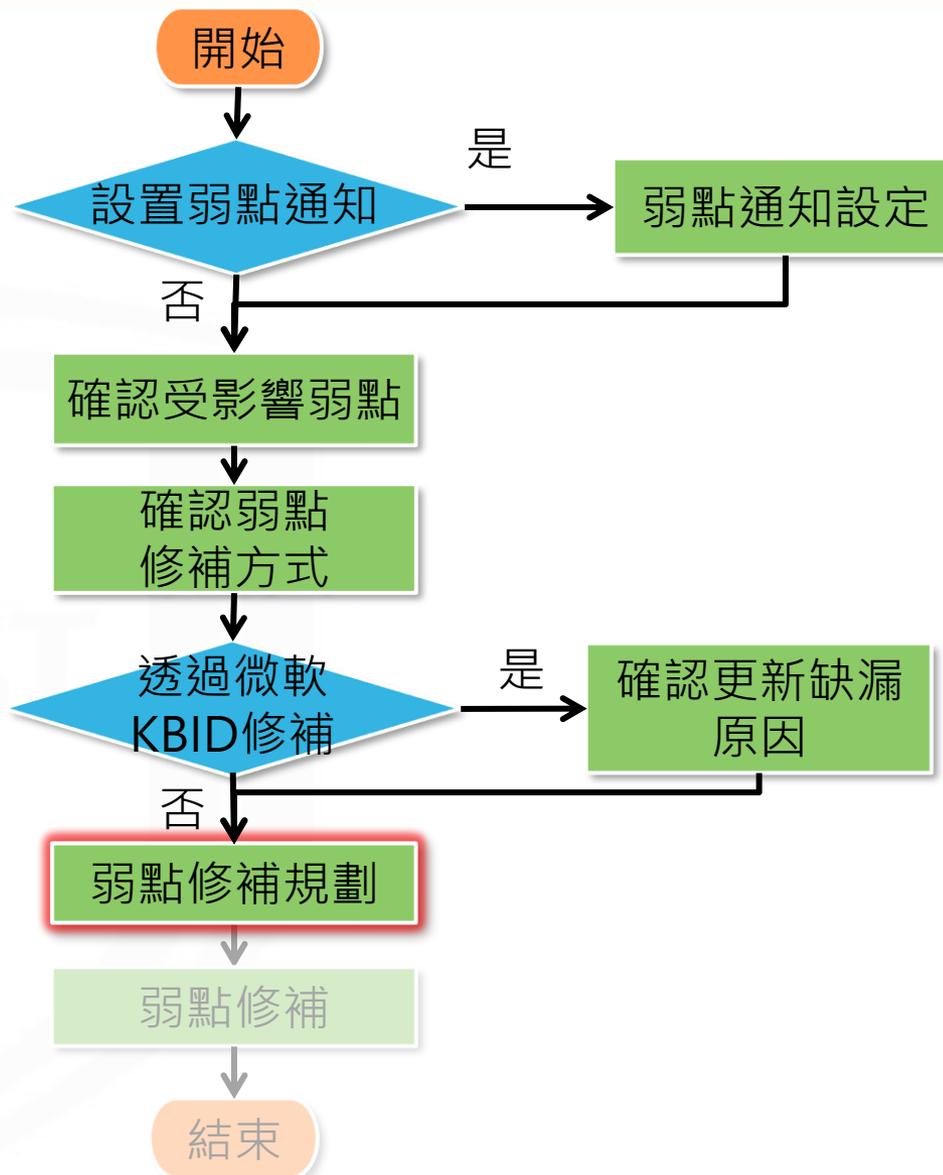
此頁面有所助益嗎？
Yes
No

本文內容

- 自動更新錯誤
- Windows Update UI 錯誤
- 庫存錯誤
- 運算式計算機錯誤
- 報告錯誤
- 重新導向程式錯誤

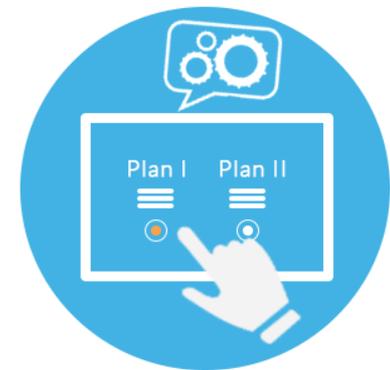
下載 PDF

弱點通知與修補規劃作業流程



弱點修補規劃(1/6)

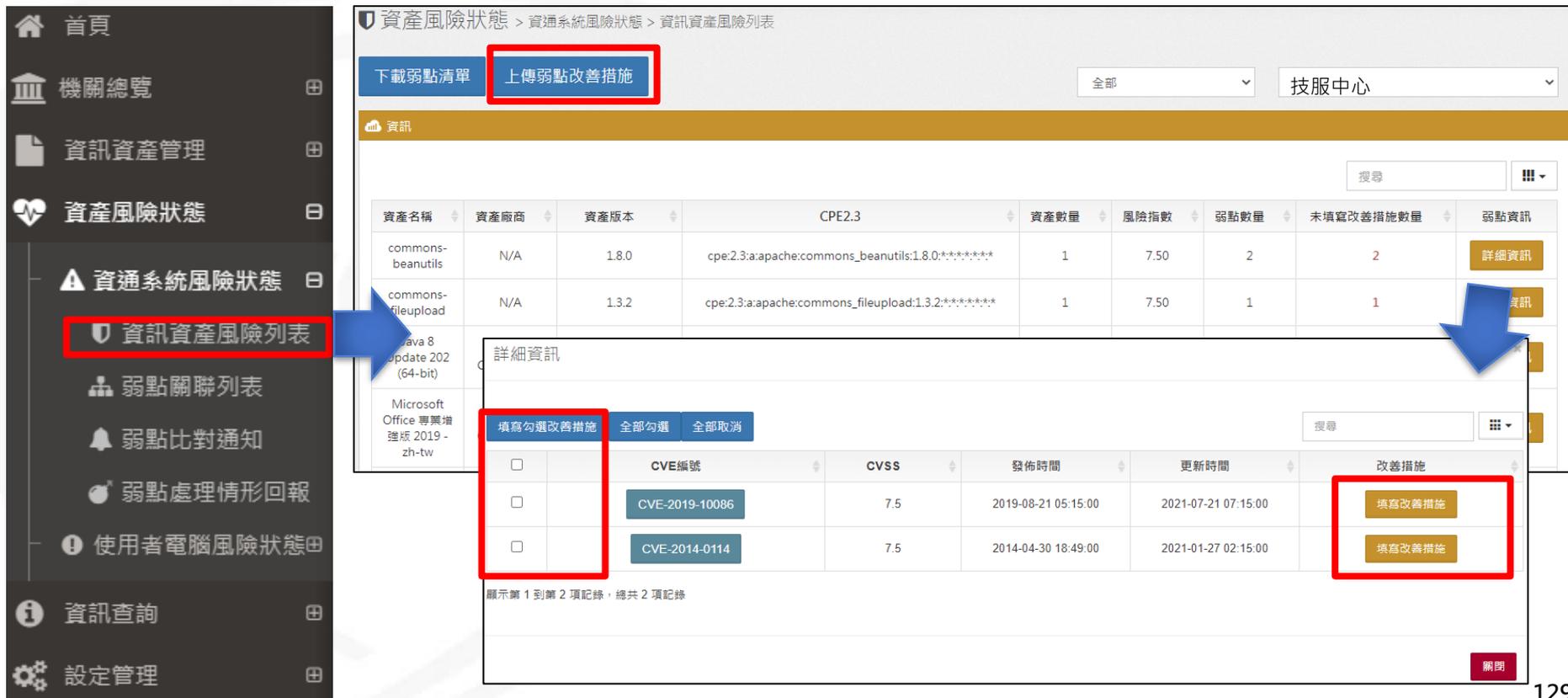
- 依據機關ISMS政策訂定弱點修復基準與修復時程，若無法立即修補、安裝安全性更新或須接受風險之弱點，可針對該風險填寫改善措施
- 針對達到弱點修復基準之弱點進行修補規劃
 - 確認是否可透過更新方式修補弱點？
 - 是否有其他替代修補措施？
 - 預計修補時程



弱點修補規劃(2/6)

- 改善措施填寫方式分為單筆填寫、批次填寫及上傳更新

– 資產風險狀態 > 資通系統風險狀態 / 使用者電腦風險狀態 > 資訊資產風險列表



The screenshot displays the '資訊資產風險列表' (Information Asset Risk List) interface. The left sidebar contains navigation options, with '資訊資產風險列表' highlighted. The main content area shows a table of assets with columns for name, vendor, version, CPE2.3, quantity, risk index, number of vulnerabilities, and number of remediation measures. A red box highlights the '上傳弱點改善措施' (Upload Vulnerability Remediation Measures) button. Below the table, a '詳細資訊' (Detailed Information) modal is open, showing a table of vulnerabilities with columns for CVE ID, CVSS, release time, update time, and remediation measures. A red box highlights the '填寫勾選改善措施' (Fill/Select Remediation Measures) checkbox and the '填寫改善措施' (Fill Remediation Measures) button. A blue arrow points from the sidebar menu to the main table, and another blue arrow points from the table to the detailed information modal.

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	風險指數	弱點數量	未填寫改善措施數量	弱點資訊
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beanutils:1.8.0:*****	1	7.50	2	2	詳細資訊
commons-fileupload	N/A	1.3.2	cpe:2.3:a:apache:commons_fileupload:1.3.2:*****	1	7.50	1	1	資訊

填寫勾選改善措施	CVE編號	CVSS	發佈時間	更新時間	改善措施
<input type="checkbox"/>	CVE-2019-10086	7.5	2019-08-21 05:15:00	2021-07-21 07:15:00	填寫改善措施
<input type="checkbox"/>	CVE-2014-0114	7.5	2014-04-30 18:49:00	2021-01-27 02:15:00	填寫改善措施

弱點修補規劃(3/6)

- 單筆填寫：可針對各弱點進行弱點修補規劃

- STEP1：確認弱點後，點選「填寫改善措施」，針對該弱點進行修補規劃
- STEP2：點選「送出」即完成填寫改善措施
- 填寫改善措施請避免使用 >、<、&、"或'"等特殊字元



詳細資訊

填寫勾選改善措施 全部勾選 全部取消

搜尋

<input type="checkbox"/>	CVE編號	CVSS	發佈時間	更新時間	改善措施
<input type="checkbox"/>	CVE-2019-10086	7.5	2019-08-21 05:15:00	2021-07-21 07:15:00	填寫改善措施
<input type="checkbox"/>	CVE-2014-0114	7.5			填寫改善措施

顯示第 1 到第 2 項記錄，總共 2 項記錄

填寫改善措施

請勿使用 >、<、&、"或'" 字元填寫改善措施

送出

關閉

弱點修補規劃(4/6)

- 批次填寫：可針對同樣修補方式之弱點進行批次弱點修補規劃
 - STEP1：確認弱點後，勾選右方的方格並點選**填寫勾選改善措施**，以進行多筆CVE之弱點修補規劃
 - STEP2：點選「送出」即完成填寫改善措施
 - 填寫改善措施請避免使用 >、<、&、"或'等特殊字元)

詳細資訊

填寫勾選改善措施 全部勾選 全部取消

搜尋

	CVE編號	CVSS	發佈時間	更新時間	改善措施
<input checked="" type="checkbox"/>	CVE-2019-10086	7.5	2019-08-21 05:15:00	2021-07-21 07:15:00	填寫改善措施
<input checked="" type="checkbox"/>	CVE-2019-10086	7.5	2019-08-21 05:15:00	2021-07-21 07:15:00	填寫改善措施
<input checked="" type="checkbox"/>	CVE-2019-10086	7.5	2019-08-21 05:15:00	2021-01-27 02:15:00	填寫改善措施

顯示第 1 到第 2 項記錄，總共 2 項記錄

填寫改善措施

請勿使用 >、<、&、"、' 字元填寫改善措施

送出 關閉

弱點修補規劃(5/6)

- 上傳更新：將弱點比對結果匯出並填寫改善措施後，上傳弱點清單登錄弱點修補規劃
 - 「下載弱點清單」功能可匯出弱點比對結果，並通知相關長官、資通系統/使用者電腦負責人或廠商
 - 可於CVSS分數欄位篩選，針對達弱點修復基準之弱點進行修補
 - 若改善措施為「尚未填寫」則表示尚未對該弱點進行修補規劃

資產風險狀態 > 資通系統風險狀態 > 資訊資產風險列表

下載弱點清單

上傳弱點改善措施

全部

資訊	G	H	I	J	K	L	M	N	O	
資產名稱	CPE2.3	CVE編號	CVSS	發布時間	更新時間	弱點說明	NVD弱點說明連結	KBID修補情形	改善措施	
	1	CPE2.3	CVE編號	CVSS	發布時間	更新時間	弱點說明	NVD弱點說明連結	KBID修補情形	改善措施
	2	microsoft.office:2019:*	CVE-2019-1449	10.0	2019/11/13 03:15:00	2020/08/25 01:37:00	ms, and Office LPAC P	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補
	3	microsoft.office:2019:*	CVE-2021-1716	9.3	2021/01/13 04:15:00	2021/01/15 03:35:00	on Vulnerability This	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補
	4	microsoft.office:2019:*	CVE-2021-1715	9.3	2021/01/13 04:15:00	2021/03/04 22:51:00	on Vulnerability This	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補

G	H	I	J	K	L	M	N	O	
CPE2.3	CVE編號	CVSS	發布時間	更新時間	弱點說明	NVD弱點說明連結	KBID修補情形	改善措施	
2	microsoft.office:2019:*	CVE-2019-1449	10.0	2019/11/13 03:15:00	2020/08/25 01:37:00	ms, and Office LPAC P	gov/view/vuln/detail?v	N/A	尚未填寫
3	microsoft.office:2019:*	CVE-2021-1716	9.3	2021/01/13 04:15:00	2021/01/15 03:35:00	on Vulnerability This	gov/view/vuln/detail?v	N/A	尚未填寫
4	microsoft.office:2019:*	CVE-2021-1715	9.3	2021/01/13 04:15:00	2021/03/04 22:51:00	on Vulnerability This	gov/view/vuln/detail?v	N/A	尚未填寫

弱點修補規劃(6/6)

- 從「資訊資產風險列表」之「處理情形」檢視各軟體資產尚未填寫修補規劃之弱點數量
 - 資產風險狀態 > 資通系統風險狀態/使用者電腦風險狀態 > 資訊資產風險列表

資產風險狀態 > 資通系統風險狀態 > 資訊資產風險列表

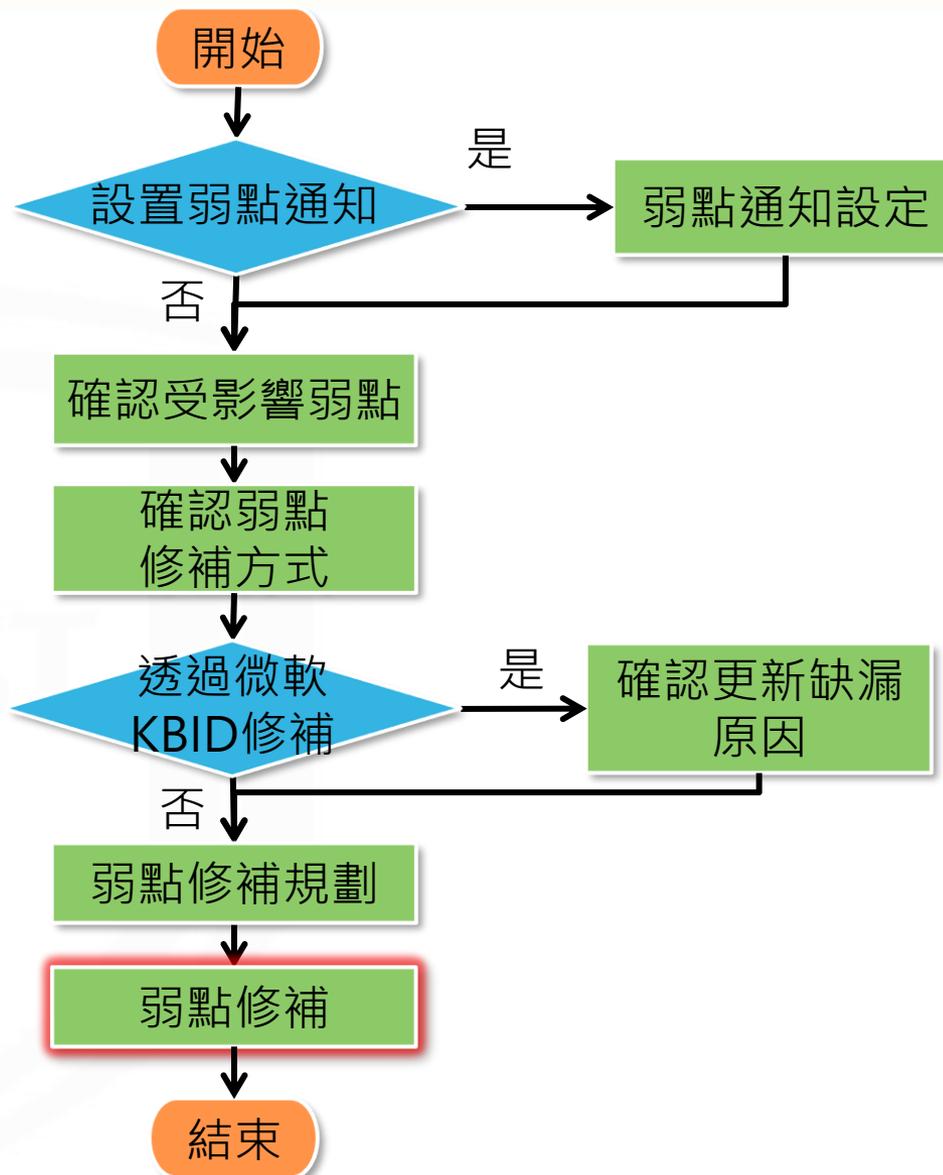
[下載弱點清單](#)
[上傳弱點改善措施](#)
全部
技服中心

資訊

搜尋

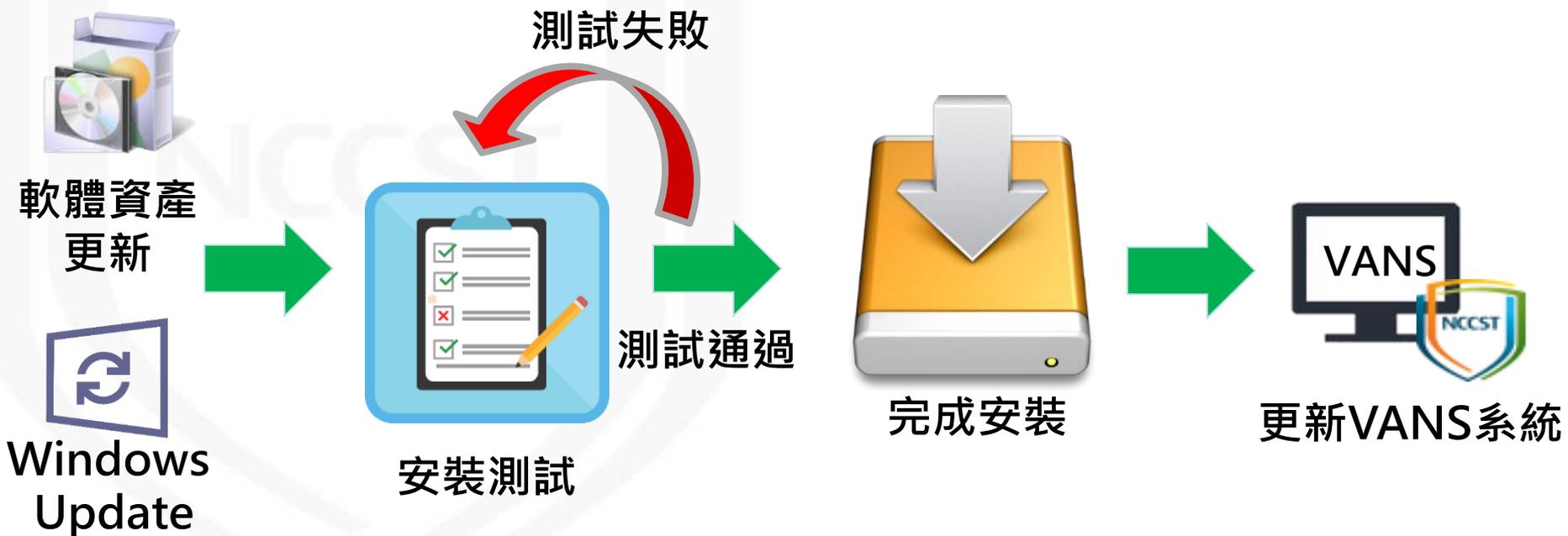
資產名稱	資產廠商	資產版本	CPE2.3	資產數量	風險指數	弱點數量	未填寫改善措施數量	弱點資訊
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beanutils:1.8.0:****:*	1	7.50	2	2	詳細資訊
commons-fileupload	N/A	1.3.2	cpe:2.3:a:apache:commons_fileupload:1.3.2:****:*	1	7.50	1	1	詳細資訊
Java 8 Update 202 (64-bit)	Oracle Corporation	8.0.2020.8	cpe:2.3:a:oracle:jdk:1.8.0:update202:****:*	1	7.00	34	34	詳細資訊
Microsoft Office 專業增強版 2019 - zh-tw	Microsoft Corporation	16.0.14228.20250	cpe:2.3:a:microsoft:office:2019:****:-:*	1	7.10	184	184	詳細資訊

弱點通知與修補規劃作業流程



弱點修補

- 異動軟體版本與派送安全性更新前，建議進行測試以確認安裝更新後，日常作業與服務仍可正常運作
- 修補完成後，更新VANS系統之資訊資產與已安裝KBID，以檢視弱點修補情形



實作練習3

NCCST

實作練習3

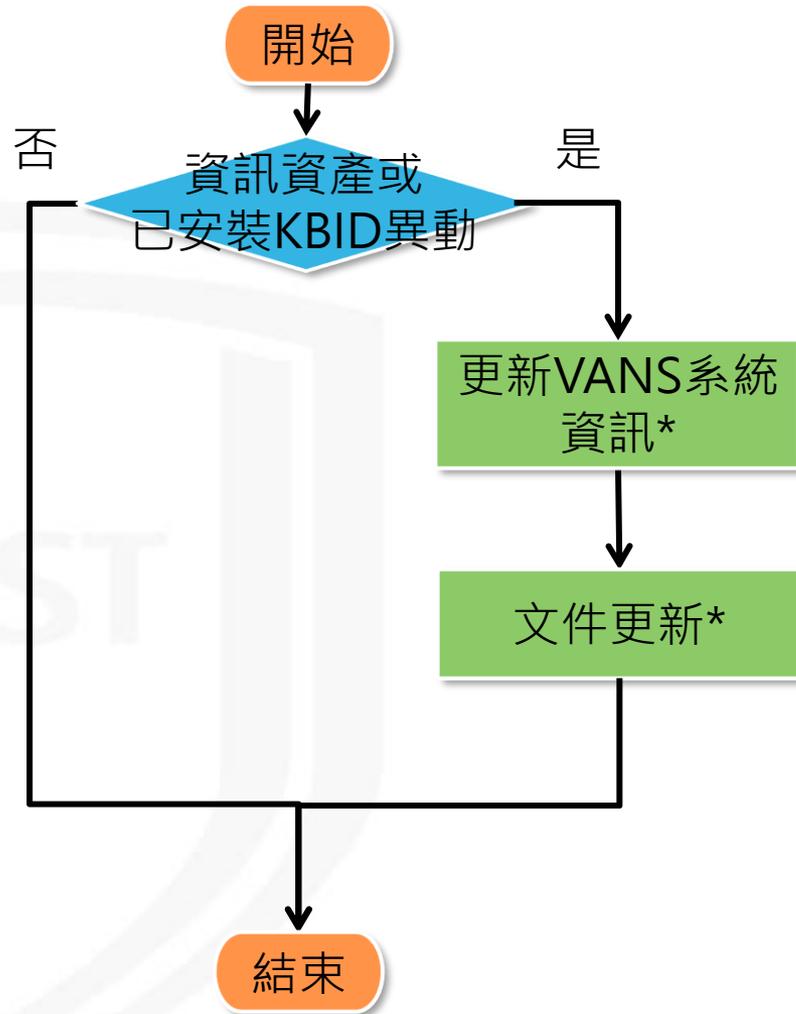
- 檢視弱點通知，並進行弱點修補規劃
- 本項練習時間**20分鐘**

項次	參考頁數	執行項目	產出項目/執行結果
1	P.109	接收弱點通知	檢視設定接收通知之信箱
2	P.111、 P.114~117、 P.129	於 資訊資產風險列表 檢視 Apache Tomcat 9.0之弱點，透過查詢建議修補方式填寫改善措施	<ul style="list-style-type: none"> • 填寫弱點清單中的改善措施 • 改善措施範例： 因系統服務使用，故須請系統維護負責人評估後再進行版更作業
3	P.111、 P.114~118、 P.129	於 資訊資產風險列表 檢視 Windows Server 2012 R2之弱點，查詢CVE-2021-34448，透過查詢建議修補方式填寫改善措施	<ul style="list-style-type: none"> • 填寫弱點清單中的改善措施 • 改善措施範例： 安全性更新預計測試7天後進行全機關派送

導入作業流程



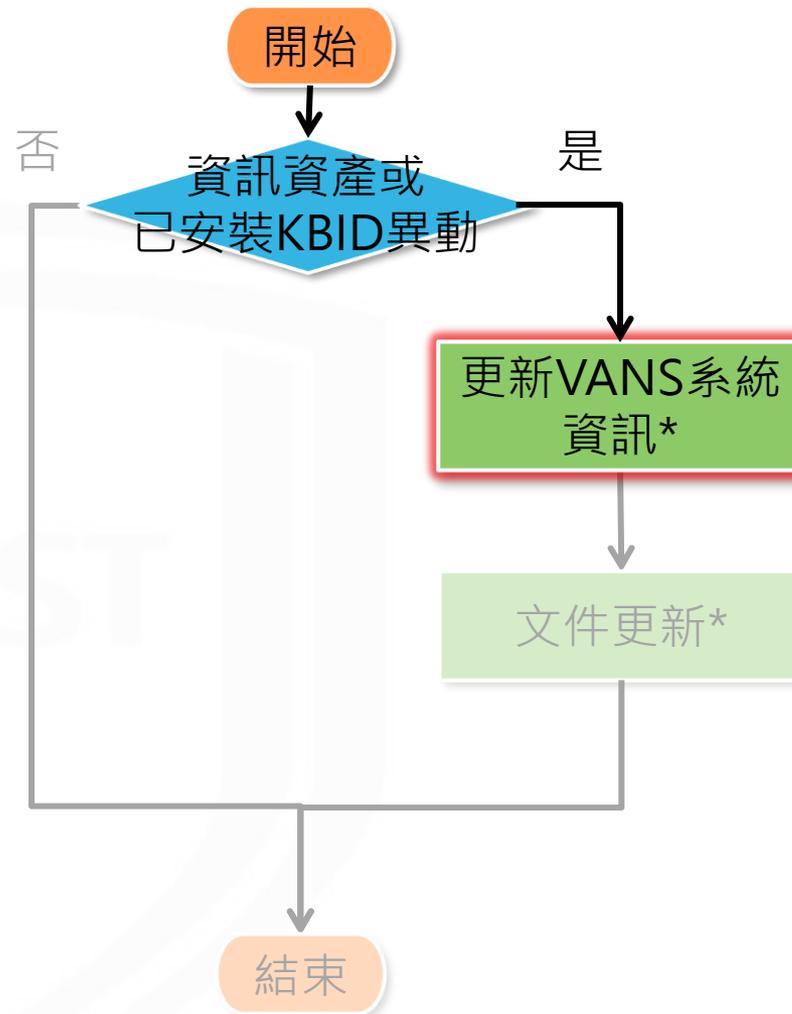
資訊資產與已安裝KBID更新作業流程



*更新VANS系統資訊：
新增、修改及刪除VANS
系統資訊

- *文件更新：
- 1.更新資訊資產清冊
 - 2.更新已安裝KBID清單
 - 3.重新匯出資訊資產清單
 - 4.重新匯出弱點清單

資訊資產與已安裝KBID更新作業流程



*更新VANS系統資訊：
新增、修改及刪除VANS
系統資訊

- *文件更新：
- 1.更新資訊資產清冊
 - 2.更新已安裝KBID清單
 - 3.重新匯出資訊資產清單
 - 4.重新匯出弱點清單

更新VANS系統資訊-批次更新

- 弱點修補後，若資訊資產或版本有異動，請至VANS系統**更新資訊資產內容**，以維持資料有效性
- 可下載已登錄至VANS系統之資訊資產接續處理，節省資訊資產更新耗費之時間



資訊資產管理 > 資通系統資產列表

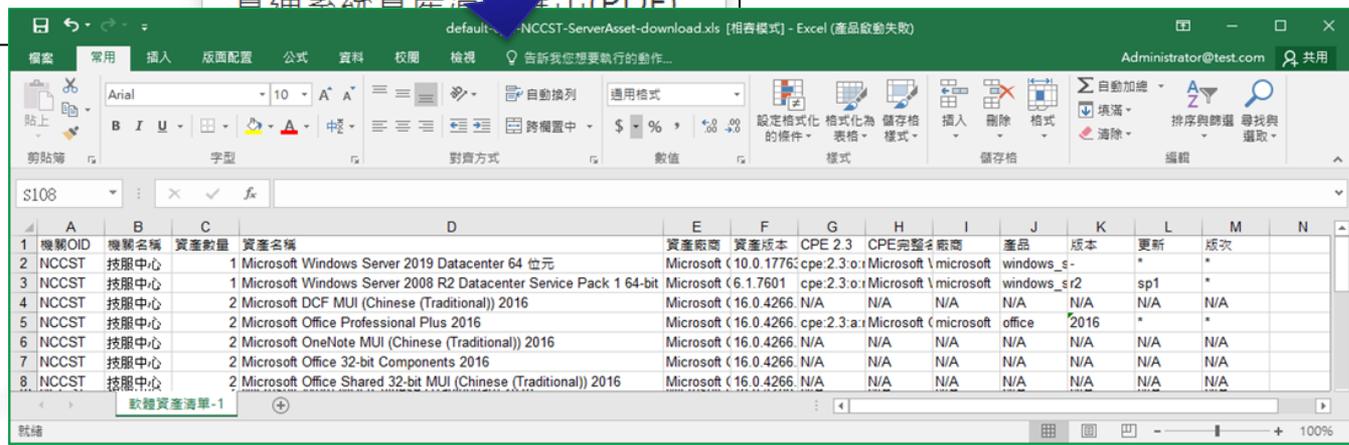
下載已登錄之資訊資產清單，以利進行後續編輯

CPE清單 / 範本下載 ▾ 資產 / 已安裝KBID上傳 ▾ 資產清單匯出 ▾

資訊資產列表

資通系統資產清單匯出(Excel)

資通系統資產清單匯出(PDF)



1	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	機號OID	機號名稱	資產數量	資產名稱	資產廠商	資產版本	CPE 2.3	CPE完整名稱	產品	版本	更新	版次		
2	NCCST	技服中心	1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft	(10.0.17763)	cpe:2.3:o:Microsoft	Microsoft \microsoft	windows_s-		*	*		
3	NCCST	技服中心	1	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit	Microsoft	(6.1.7601)	cpe:2.3:o:Microsoft	Microsoft \microsoft	windows_s12		sp1	*		
4	NCCST	技服中心	2	Microsoft DCF MUI (Chinese (Traditional)) 2016	Microsoft	(16.0.4266)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	NCCST	技服中心	2	Microsoft Office Professional Plus 2016	Microsoft	(16.0.4266)	cpe:2.3:a:Microsoft	(microsoft	office	2016	*	*		
6	NCCST	技服中心	2	Microsoft OneNote MUI (Chinese (Traditional)) 2016	Microsoft	(16.0.4266)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
7	NCCST	技服中心	2	Microsoft Office 32-bit Components 2016	Microsoft	(16.0.4266)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8	NCCST	技服中心	2	Microsoft Office Shared 32-bit MUI (Chinese (Traditional)) 2016	Microsoft	(16.0.4266)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

更新VANS系統資訊-單筆更新(1/2)



● 編輯資訊資產

- 透過網頁頁面進行單筆資訊資產編輯與刪除
- 更新資產時，僅可變更資產之版本、版次及數量

The screenshot displays the '資訊資產管理' (Information Asset Management) interface. A modal window titled '更新資產' (Update Asset) is open, allowing for the modification of an asset's details. The main interface shows a table of assets with columns for '資產名稱' (Asset Name), '資產廠商' (Asset Vendor), and '資產版本' (Asset Version).

資產名稱	資產廠商	資產版本
Apache Tomcat 9.0 Tomcat9 (remove only)	The Apache Software Foundation	9.0.16
commons-beanutils	N/A	1.8.0

The '更新資產' dialog box contains the following fields:

- 廠商 (Vendor): apache
- 產品 (Product): commons-beanutils
- 版本 (Version): 1.8.0
- 更新 (Update): *
- 版次 (Edition): *
- 資產數量 (Asset Quantity): 1

Buttons in the dialog include '更新資產' (Update Asset) and '取消' (Cancel). A blue arrow points from the '更新資產' button to the '編輯' (Edit) button in the table's action column. The '編輯' and '刪除' (Delete) buttons for the first row are highlighted with a red box.

更新VANS系統資訊-單筆更新(2/2)



● 編輯已安裝KBID

- 透過網頁頁面進行單筆已安裝KBID新增與刪除
- 更改KBID數量可先點選刪除，再點選新增已安裝KBID輸入KBID與已安裝數量

資訊資產管理 > 資通系統資產列表

CPE清單 / 範本下載 ▾ 資產 / 已安裝KBID上傳 ▾ 資產清單匯出 ▾ 切換至資訊資產列表

已安裝KBID列表

KBID	數量
KB2868626	1
KB2883200	1

新增已安裝KBID

KBID: KB2868626

已安裝KBID數量: 3

新增已安裝KBID

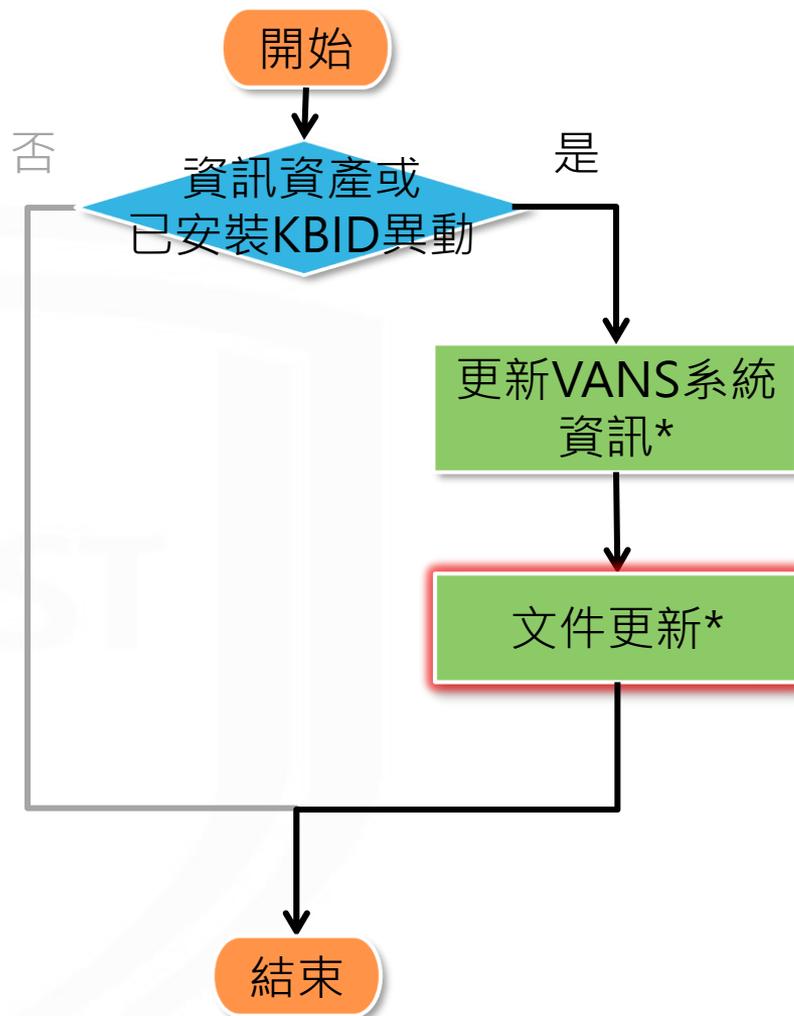
取消

刪除

刪除

刪除

資訊資產與已安裝KBID更新作業流程



*更新VANS系統資訊：
新增、修改及刪除VANS
系統資訊

- *文件更新：
- 1.更新資訊資產清冊
 - 2.更新已安裝KBID清單
 - 3.重新匯出資訊資產清單
 - 4.重新匯出弱點清單

文件更新-資訊資產清單匯出

● 資訊資產清單匯出(PDF)

– 有資料留存與備查需求時，可以PDF格式匯出已登錄VANS系統之資訊資產

資訊資產管理 > 資通系統資產列表

下載已登錄之資訊資產清單，以利進行後續編輯

[CPE清單 / 範本下載](#)
[資產 / 已安裝KBID上傳](#)
[資產清單匯出](#)

[資通系統資產清單匯出\(Excel\)](#)
[資通系統資產清單匯出\(PDF\)](#)

機關OID	機關名稱	資產數量	資產名稱	資產廠商	資產版本	CPE 2.3	CPE完整名稱	廠商	產品	版本	更新	版次
NCCST	技服中心	1	Apache Tomcat 9.0 Tomcat9 (remove only)	The Apache Software Foundation	9.0.16	cpe:2.3:a:apache:tomcat:9.0.16:*:*:*:*:*:*	Apache Software Foundation Tomcat 9.0.16	apache	tomcat	9.0.16	*	*
NCCST	技服中心	1	commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons-beanutils:1.8.0:*:*:*:*:*	Apache Software Foundation Commons BeanUtils 1.8.0	apache	commons-beanutils	1.8.0	*	*
NCCST	技服中心	1	commons-fileupload	N/A	1.3.2	cpe:2.3:a:apache:commons-fileupload:1.3.2:*:*:*:*:*	Apache Software Foundation Commons FileUpload 1.3.2	apache	commons-fileupload	1.3.2	*	*
NCCST	技服中心	1	commons-io	N/A	2.2	N/A	N/A	N/A	commons-io	2.2	N/A	N/A
NCCST	技服中心	1	commons-lang	N/A	2.4	N/A	N/A	N/A	commons-lang	2.4	N/A	N/A

文件更新

- 依據弱點修補規劃執行資訊更新或下架後，進行下列文件更新作業
 - 更新資訊資產清冊與已安裝KBID清單
 - 於VANS系統匯出更新後之弱點清單，並進行弱點修補規劃

資訊資產清冊

	A	B	C	D	E	F
1	資產數量	資產名稱	資產廠商	資產版本	TEMP	資產數量
2	1	Windows Server 2012 R2 Standard x64	Microsoft Corporation	N/A	Windows Server 2012 R2 Standard	1
3	1	Windows Server 2019 Datacenter x64	Microsoft Corporation	1809	Windows Server 2019 Datacenter	1
4	1	Microsoft Visual C++ 2008 Redistributable	Microsoft Corporation	9.0.30729.6161	Microsoft Visual C++ 2008 Redistributable	1
5	2	Microsoft Silverlight	Microsoft Corporation	5.1.50918.0	Microsoft Silverlight	2
6	1	VMware Tools	VMware, Inc.	11.0.0.14549434	VMware Tools VMware, Inc. 11.0.0.14549434	1

弱點清單

	G	H	I	J	K	L	M	N	O
1	CPE2.3	CVE編號	CVSS	發布時間	更新時間	弱點說明	NVD弱點說明連結	KBID修補情形	改善措施
2	microsoft.office:2019:*	CVE-2019-1449	10.0	2019/11/13 03:15:00	2020/08/25 01:37:00	... and Office LPAC P...	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補
3	microsoft.office:2019:*	CVE-2021-1716	9.3	2021/01/13 04:15:00	2021/01/15 03:35:00	on Vulnerability This	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補
4	microsoft.office:2019:*	CVE-2021-1715	9.3	2021/01/13 04:15:00	2021/03/04 22:51:00	on Vulnerability This	gov/view/vuln/detail?v	N/A	已安排駐點廠商協助測試更新，確認安裝後不影響系統運作，將以手動方式更新完成修補

實作練習4

A large, faint watermark of the NCCST logo is centered on the page. It features a shield shape with the acronym "NCCST" written in a light gray font inside.

實作練習4

- 登錄已安裝KBID，並確認弱點修補情形
- 本項練習時間**15分鐘**

項次	參考頁數	執行項目	產出項目/執行結果
1	P.169~175	參考附件4，將 Upload_KBIDTemplate.json 登錄至 VANS 系統	檢視已安裝KBID列表
2	P.131	<ul style="list-style-type: none"> 於資訊資產風險列表匯出弱點清單，搜尋並檢視 CVE-2021-34448 是否完成修補 安全性更新請參考 KBID 修補情形欄位 	弱點清單

	G	H	I	J	K	L	M	N	O
1	CPE2.3	CVE編號	CVSS	發布時間	更新時間	弱點說明	NVD弱點說明連結	KBID修補情形	改善措施
2	microsoft.office:2019:*	CVE-2019-1449	10.0	2019/11/13 03:15:00	2020/08/25 01:37:00	... and Office LPAC P	gov/view/vuln/detail?	N/A	尚未填寫
3	microsoft.office:2019:*	CVE-2021-1716	9.3	2021/01/13 04:15:00	2021/01/15 03:35:00	on Vulnerability This	gov/view/vuln/detail?	N/A	尚未填寫
4	microsoft.office:2019:*	CVE-2021-1715	9.3	2021/01/13 04:15:00	2021/03/04 22:51:00	on Vulnerability This	gov/view/vuln/detail?	N/A	尚未填寫

Q1 VANS與弱點掃描之差異？

項目	VANS	弱點掃描
資訊蒐集方式	透過作業系統內建工具或第三方軟體，產出已安裝資訊資產清單	透過網路遠端執行掃描
弱點查詢方式	將登錄至VANS之資訊資產項目與版本進行弱點比對	透過弱掃軟體plugin進行弱點偵測
比對範圍	登錄至VANS之所有資訊資產	目標主機對外服務使用套件
時間性	下列情境會觸發1次弱點比對，最低觸發間隔為2小時 <ul style="list-style-type: none">每日與NVD更新後機關資產異動後	定期執行掃描

Q2 VANS系統資產更新時，能否只上傳新增的資產項目？

– 透過上傳清單(Upload_Template.xls)更新資產時，會以最新上傳清單覆蓋既有資產，故須以完整資產內容進行上傳

常見問答(2/2)



Q3 如何得知哪些資產較危險，應立即處理？

- 弱點比對結果會顯示各資產風險指數，計算方式為將各資訊資產比對到的每個弱點CVSS分數加總平均，風險指數較高者建議優先處理

Q4 上傳資產清單時，VANS系統支援哪些格式？

- VANS系統可接受上傳之檔案格式包含Excel活頁簿(*.xlsx)、Excel 97-2003活頁簿(*.xls)及OpenDocument試算表(*.ods)等3種，機關可透過上述格式上傳資產清單

Q5 相同弱點只會通知一次呢？還是會持續寄通知信？

- VANS機制主要提供機關即時掌握弱點、有效修補弱點及做好弱點管理，進而降低資安風險，相同弱點僅會通知一次



參考資料

A large, faint watermark of the NCCST logo is visible in the background on the left side of the slide. It features the same shield shape and "NCCST" text as the header logo, but in a light gray color.

NCCST

參考資料(1/2)



- Windows Management Instrumentation
 - <https://docs.microsoft.com/zh-tw/windows/desktop/wmisdk/wmi-start-page>
- How to find the Windows version using Registry?
 - <https://mivilisnet.wordpress.com/2020/02/04/how-to-find-the-windows-version-using-registry/>
- Microsoft Docs - Dir
 - <https://docs.microsoft.com/zh-tw/windows-server/administration/windows-commands/dir>
- NVD官方網站
 - <https://nvd.nist.gov/>
- Excel從右向左查找
 - <http://www.gocalf.com/blog/excel-find-from-right.html>

參考資料(2/2)

- 用來描述 Microsoft 軟體更新標準術語的說明
 - <https://support.microsoft.com/zh-tw/help/824684/description-of-the-standard-terminology-that-is-used-to-describe-micro>
- Microsoft Power Query for Excel
 - <https://www.microsoft.com/zh-TW/download/details.aspx?id=39379>
- 關於 Excel 中的 Power Query
 - <https://support.office.com/zh-tw/article/Power-Query-%E5%BF%AB%E9%80%9F%E5%85%A5%E9%96%80-7104fbee-9e62-4cb9-a02e-5bfb1a6c536a>
- 瞭解如何在 Power Query (合併多個)
 - <https://support.office.com/zh-hk/article/%E5%90%88%E4%BD%B5%E5%A4%9A%E5%80%8B%E8%B3%87%E6%96%99%E4%BE%86%E6%BA%90%E7%9A%84%E8%B3%87%E6%96%99-Power-Query-70cfe661-5a2a-4d9d-a4fe-586cc7878c7d>

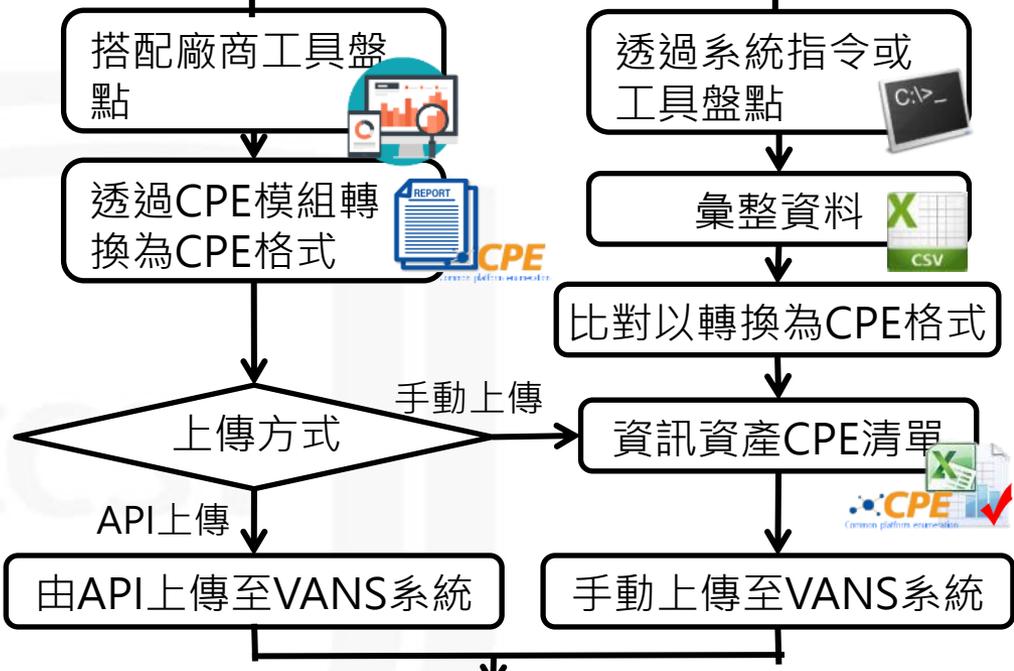
附件

A large, faint watermark of the NCCST logo is visible on the left side of the page. It features a shield shape with the acronym "NCCST" in the center, rendered in a light gray color.

附件1.資訊資產弱點管理總覽



透過合作廠商工具產出CPE格式報表，並可透過API上傳至VANS系統



透過AD派送批次檔方式盤點軟體資產資訊，再以PowerQuery擴充套件彙整



VANS系統

附件2

WMI Windows Installer提供者 安裝步驟

NCCST

安裝WMI Windows Installer(1/7)



- 若作業系統為Windows Server 2003，須安裝「WMI Windows Installer提供者」，否則指令無法運作

A screenshot of a Windows command prompt window titled "命令提示字元 - wmic". The window shows the following text:

```
C:\Documents and Settings\Administrator>wmic
wmic:root\cli>/output:"C:\Documents and Settings\install-apps.txt" product list full
節點 - III-020370ED6AA
錯誤:
代碼 = 0x80041010
描述 = 無效的類別
設備 = WMI
wmic:root\cli>
```

The error message is highlighted with a red rectangular box. The error details are: 節點 - III-020370ED6AA, 錯誤: (Error:), 代碼 = 0x80041010 (Code = 0x80041010), 描述 = 無效的類別 (Description = Invalid class), and 設備 = WMI (Device = WMI).

安裝WMI Windows Installer(2/7)



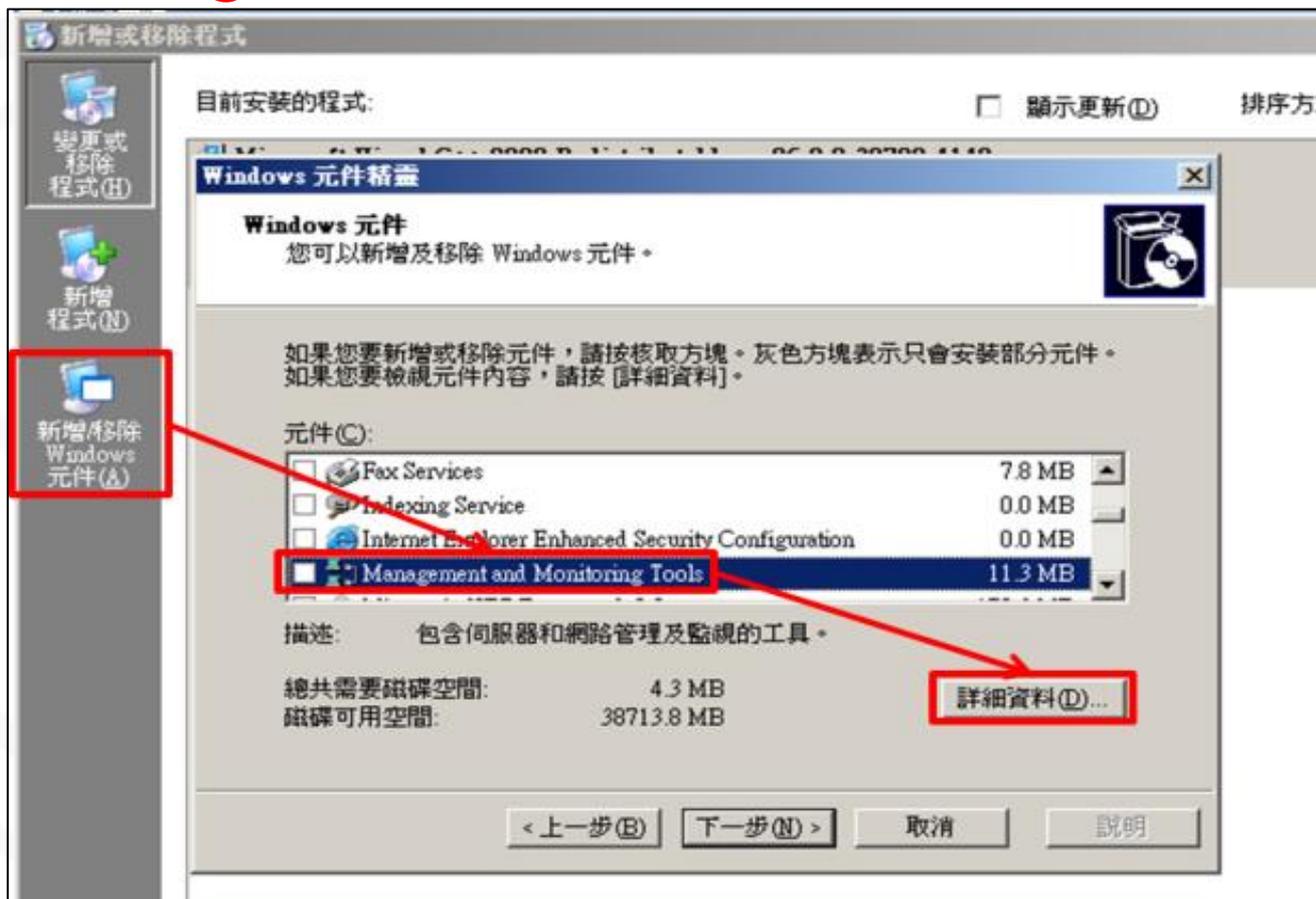
- 安裝WMI Windows Installer提供者的步驟如下：
- 步驟一：進入控制台的「新增或移除程式」



安裝WMI Windows Installer(3/7)



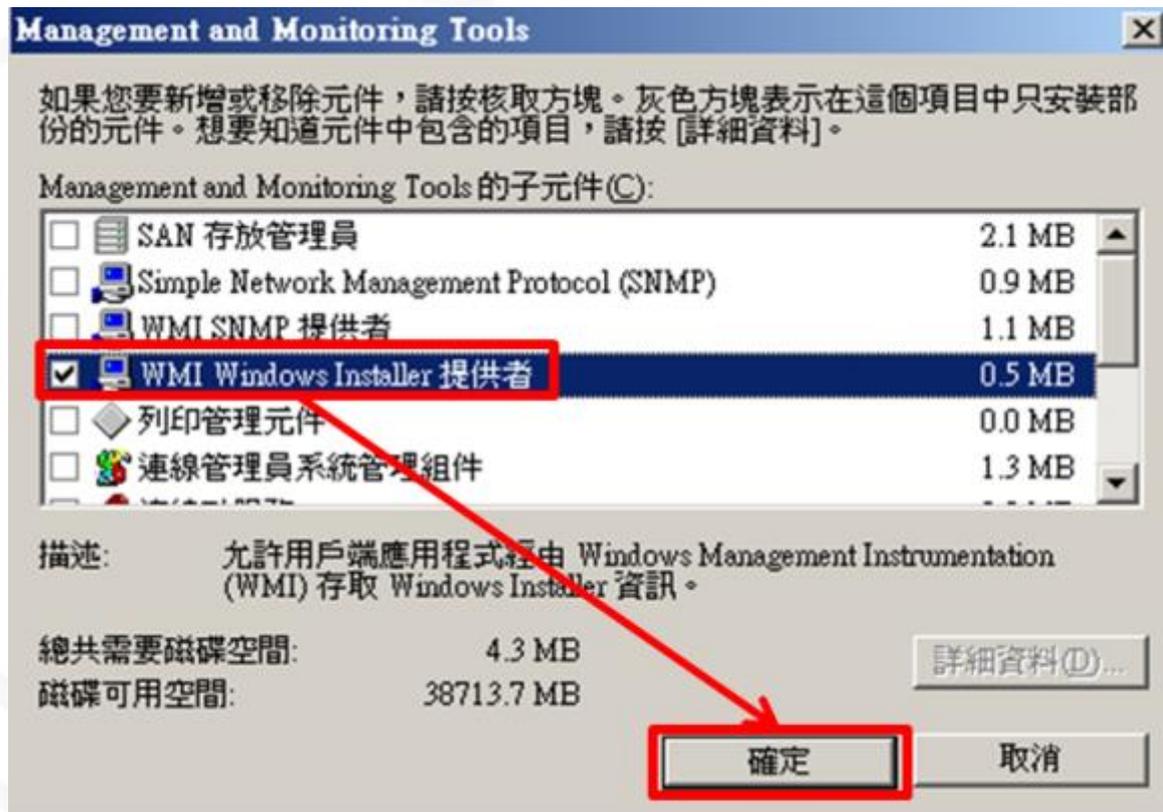
- 步驟二：點選「新增/移除Windows元件」。於Windows元件精靈視窗中，選擇「Management and Monitoring Tools」，並點選「詳細資料」按鈕



安裝WMI Windows Installer(4/7)



- 步驟三：於「Management and Monitoring Tools」對話方塊中，勾選「WMI Windows Installer提供者」，並點選「確定」

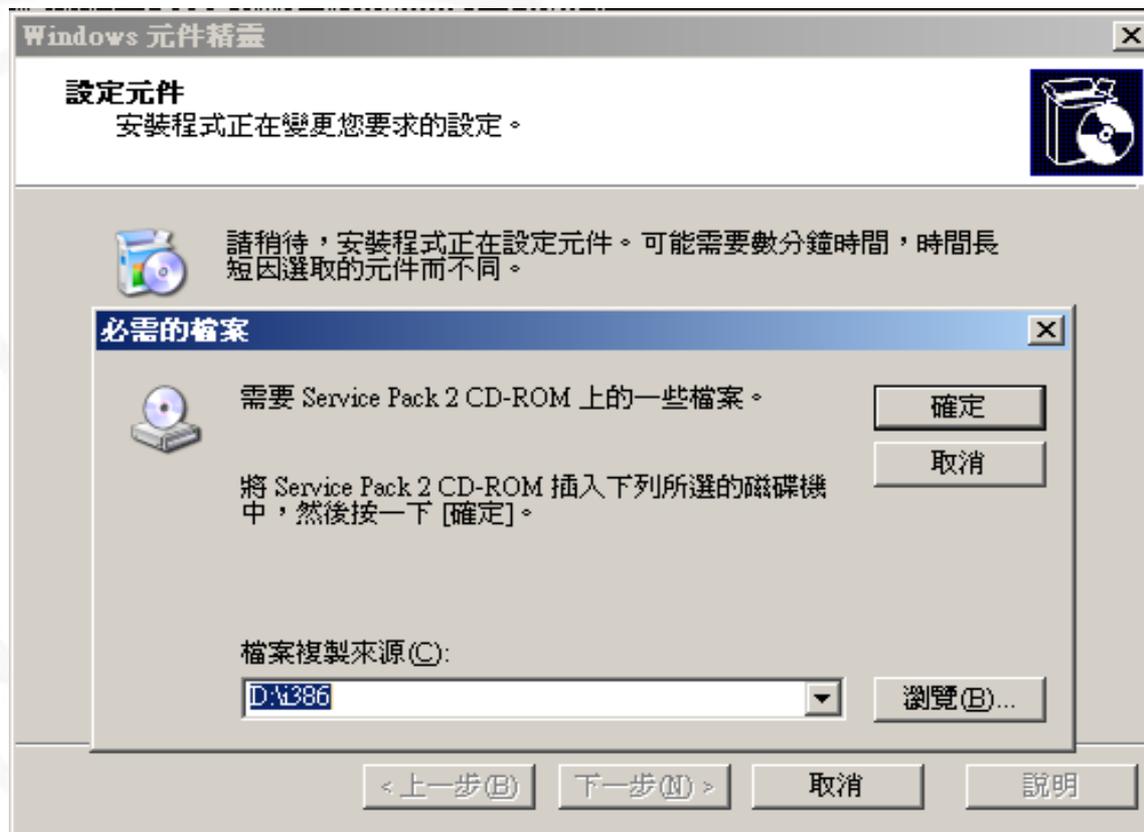


安裝WMI Windows Installer(5/7)



- 步驟四：點選「下一步」後，即會開始安裝「WMI Windows Installer提供者」

–備註：安裝時需要Windows Server 2003之安裝映像檔



安裝WMI Windows Installer(6/7)



- 步驟五：完成安裝



安裝WMI Windows Installer(7/7)



- 步驟六：安裝完成後，即可執行WMIC

The screenshot shows a Windows Explorer window displaying the file 'install-apps.txt' in the 'C:\Documents and Settings\All Users\Documents' folder. A red box highlights this file, with a red '2.' next to it. Overlaid on this is a Command Prompt window titled '命令提示字元 - wmic'. The Command Prompt shows the command 'wmic' being entered at the prompt 'C:\Documents and Settings\Administrator>'. The output of the command is 'wmic:root\cli>/output: "C:\Documents and Settings\All Users\Documents\install-ap', which is also highlighted with a red box and a red '1.' next to it.

名稱	大小	類型	修改日期	屬性
My Music		檔案資料夾	2017/8/14 上午 10:15	
install-apps.txt	1 KB	文字文件	2017/9/25 下午 08:59	A

```
C:\Documents and Settings\Administrator>wmic
wmic:root\cli>/output: "C:\Documents and Settings\All Users\Documents\install-ap
wmic:root\cli>
```

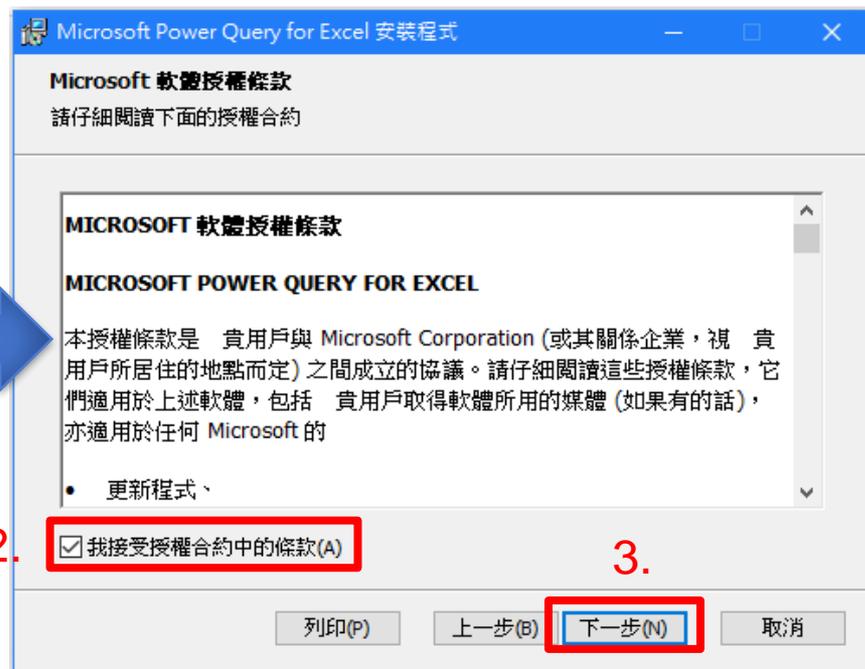
附件3

Microsoft Power Query for Excel 安裝步驟

NCCST

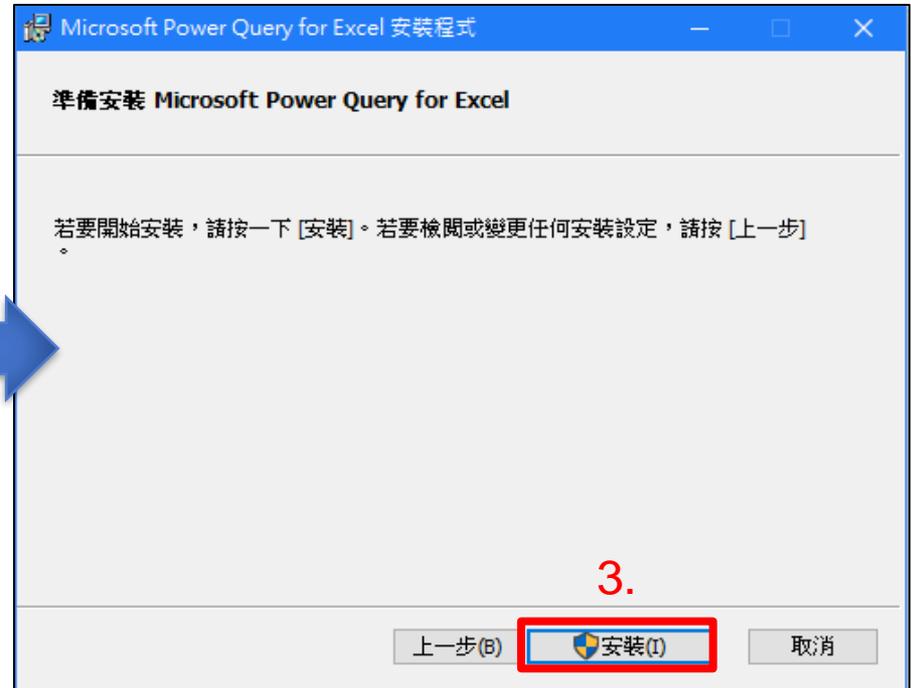
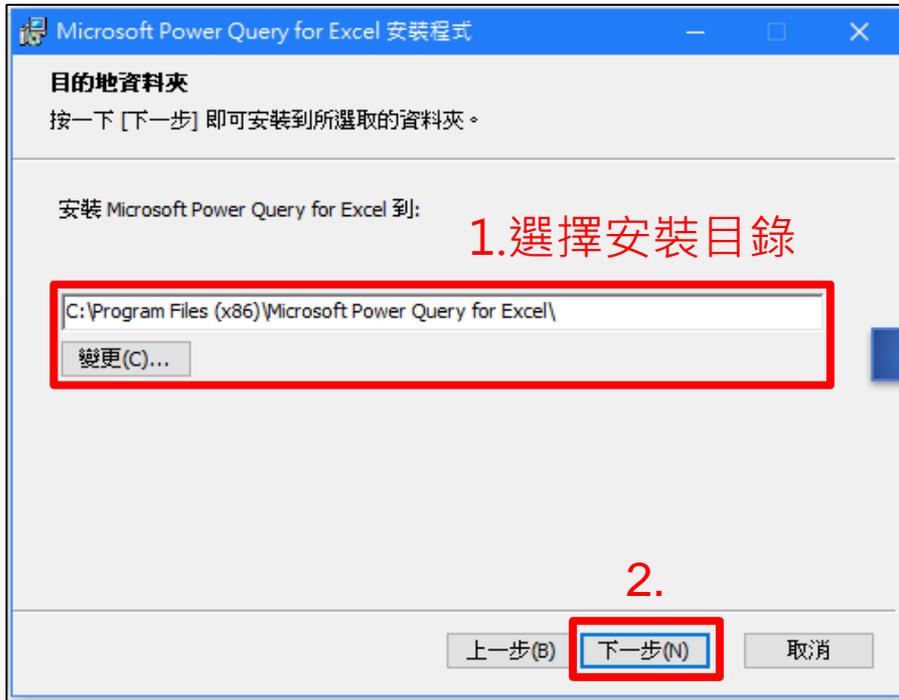
安裝Microsoft Power Query for Excel(1/3)

- Power Query內建於Excel 2016、2019中，功能名稱為「**取得及轉換**」，不需額外安裝Microsoft Power Query for Excel
- 若為Excel 2010或2013，需至微軟官網下載Microsoft Power Query for Excel，並進行安裝
 - <https://www.microsoft.com/zh-TW/download/details.aspx?id=39379>



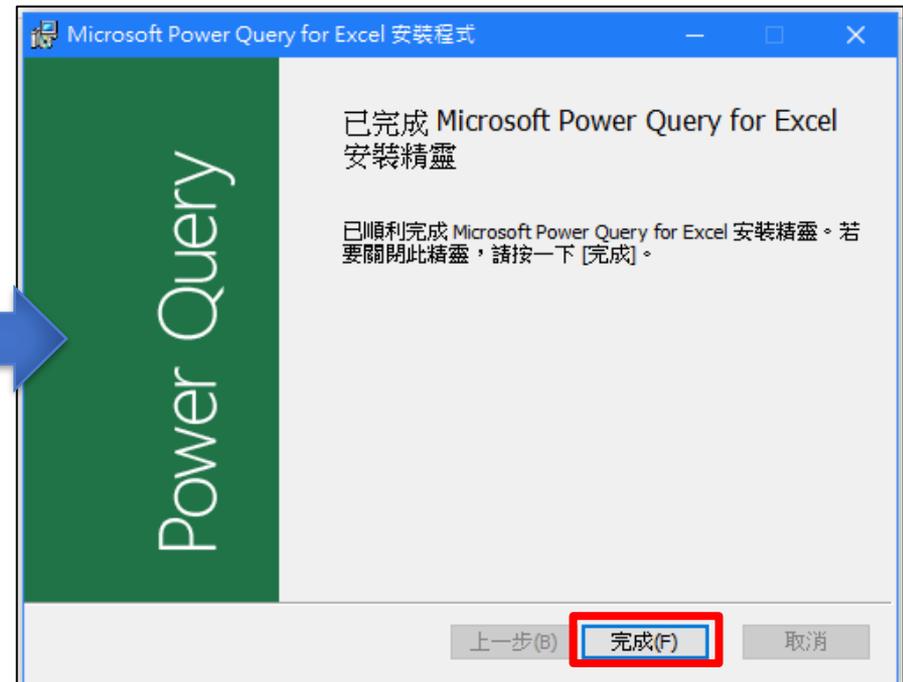
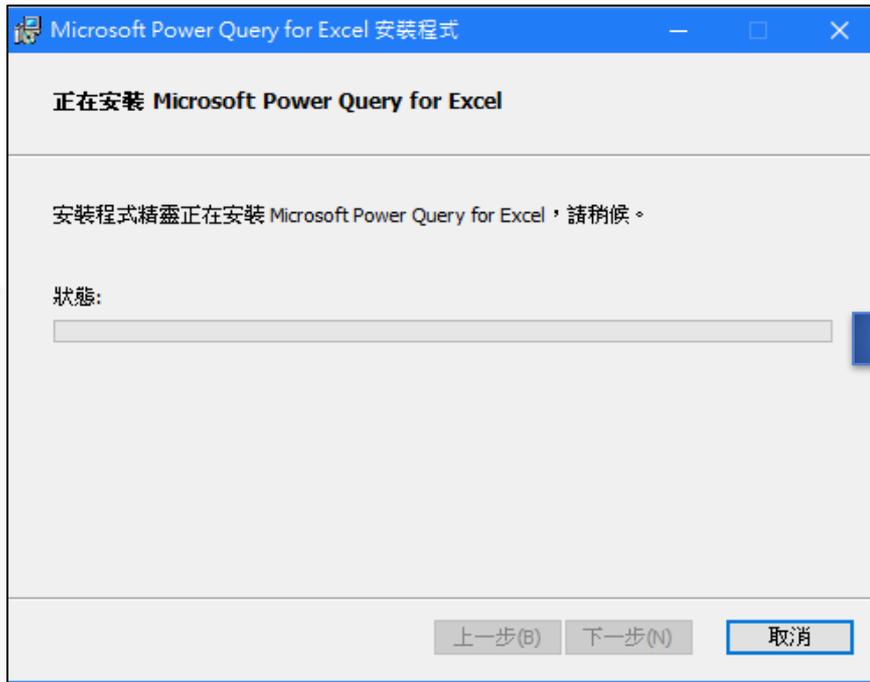
安裝Microsoft Power Query for Excel(2/3)

- 選擇安裝目錄，準備安裝



安裝 Microsoft Power Query for Excel (3/3)

- 進行安裝



附件4

Postman操作方式

NCCST

下載與安裝Postman工具

- 至Postman官方網站下載與安裝工具
– <https://www.postman.com/downloads/>



The screenshot shows the Postman website's navigation bar with the logo and links for Product, How Collaboration Works, Use Cases, Pricing, Enterprise, and Explore. On the right, there are links for Learning Center and Sign In. The main content area features the heading "Get Postman for Windows" and a sub-headline "Join 10 million developers and download the **ONLY** complete API Development Environment." Below this is a prominent orange "Download" button with a Windows logo icon. At the bottom, there are links for "Version 7.18.0", "RELEASE NOTES", and "PRODUCT ROADMAP".

POSTMAN Product ▾ How Collaboration Works Use Cases ▾ Pricing Enterprise Explore Learning Center Sign In

Get Postman for Windows

Join 10 million developers and download the **ONLY** complete API Development Environment.

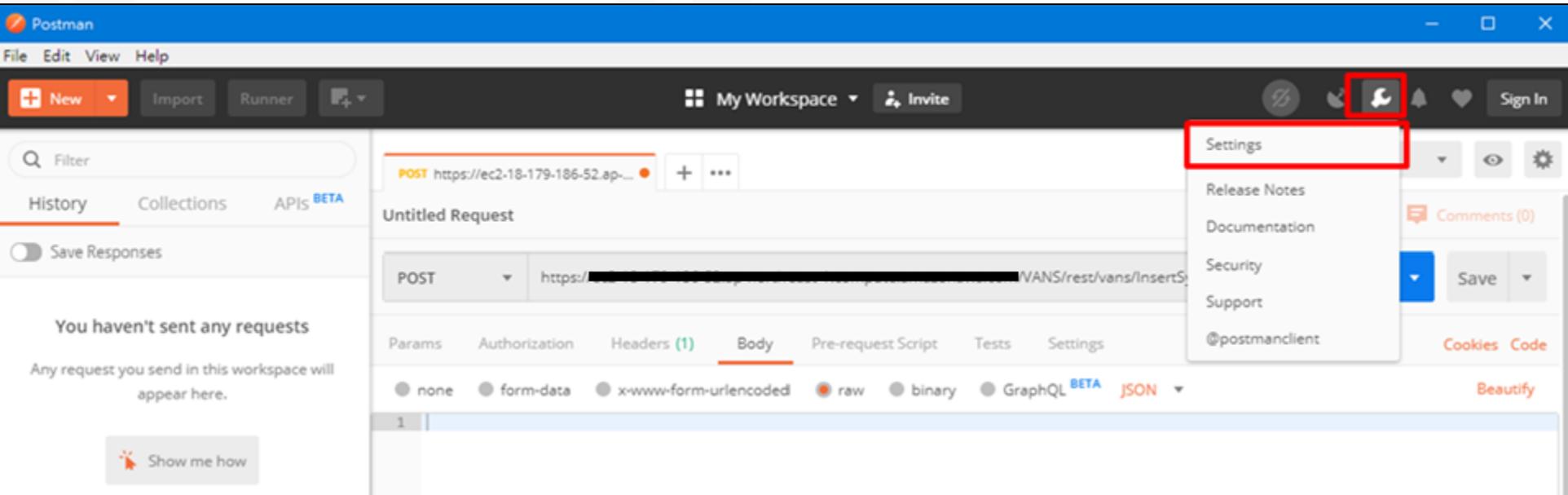
Download ▾

Version 7.18.0 | [RELEASE NOTES](#) | [PRODUCT ROADMAP](#)

Postman設定(1/4)

- 關閉SSL憑證驗證

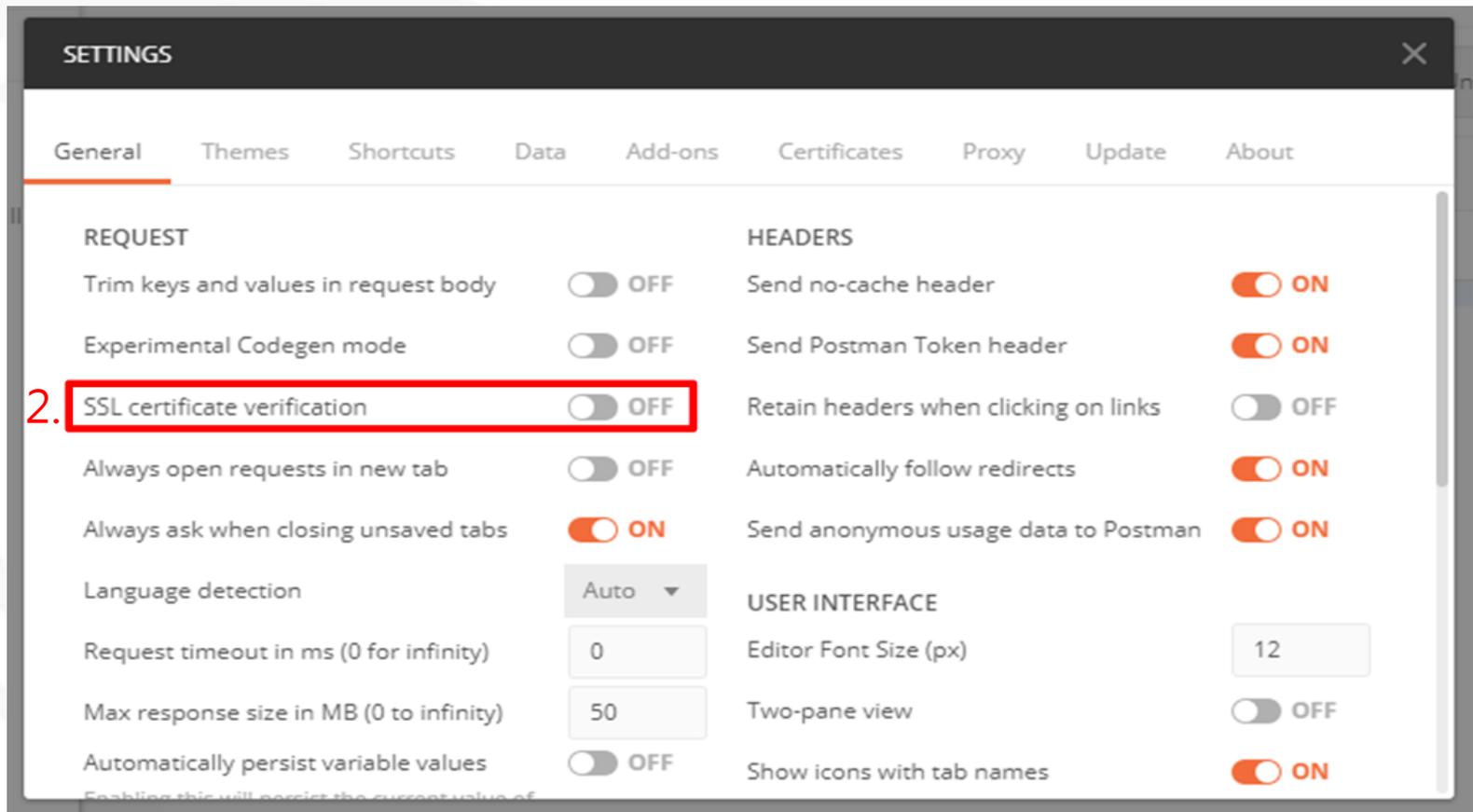
– 因VANS API測試站會有憑證錯誤的問題，故須關閉SSL憑證驗證



Postman設定(2/4)

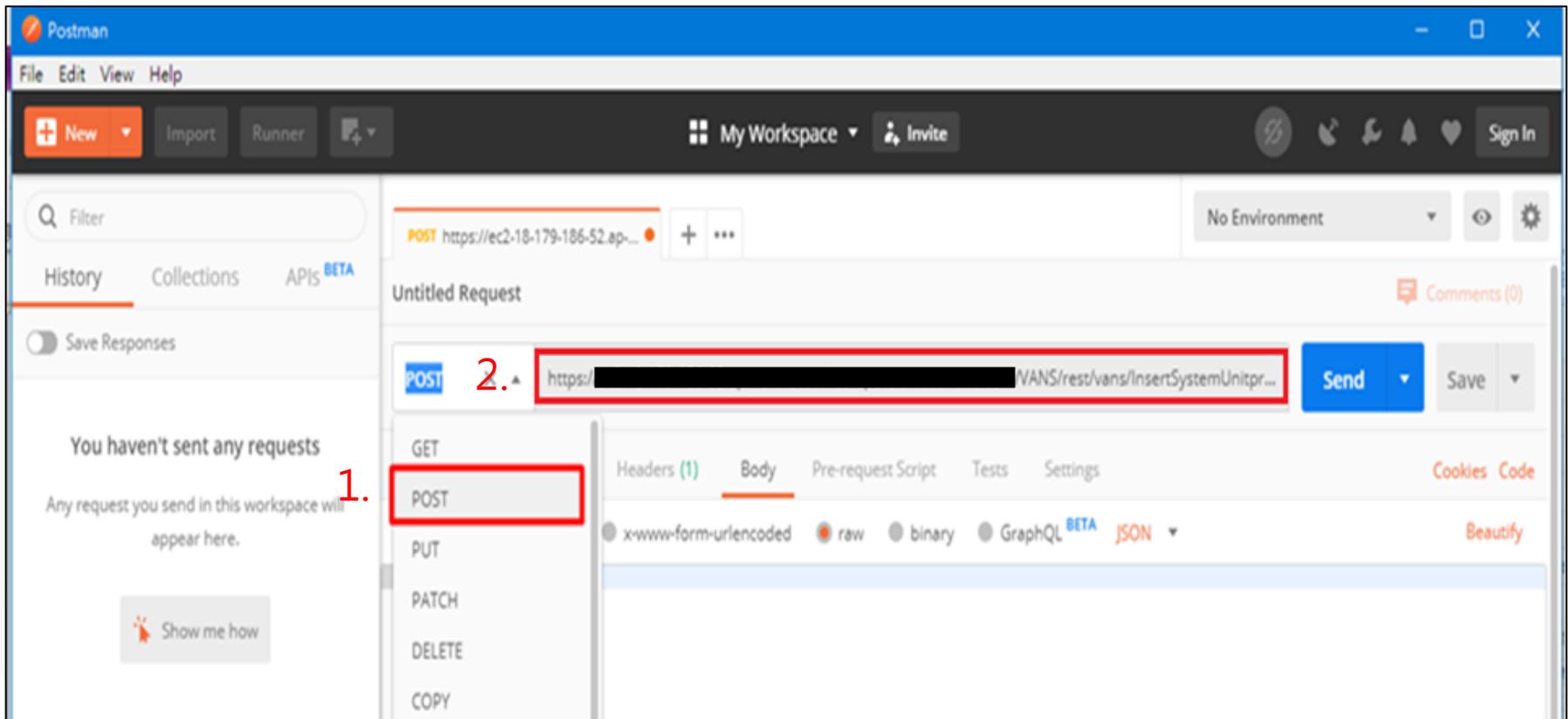
- 關閉SSL憑證驗證

– 因VANS API測試站會有憑證錯誤的問題，故須關閉SSL憑證驗證



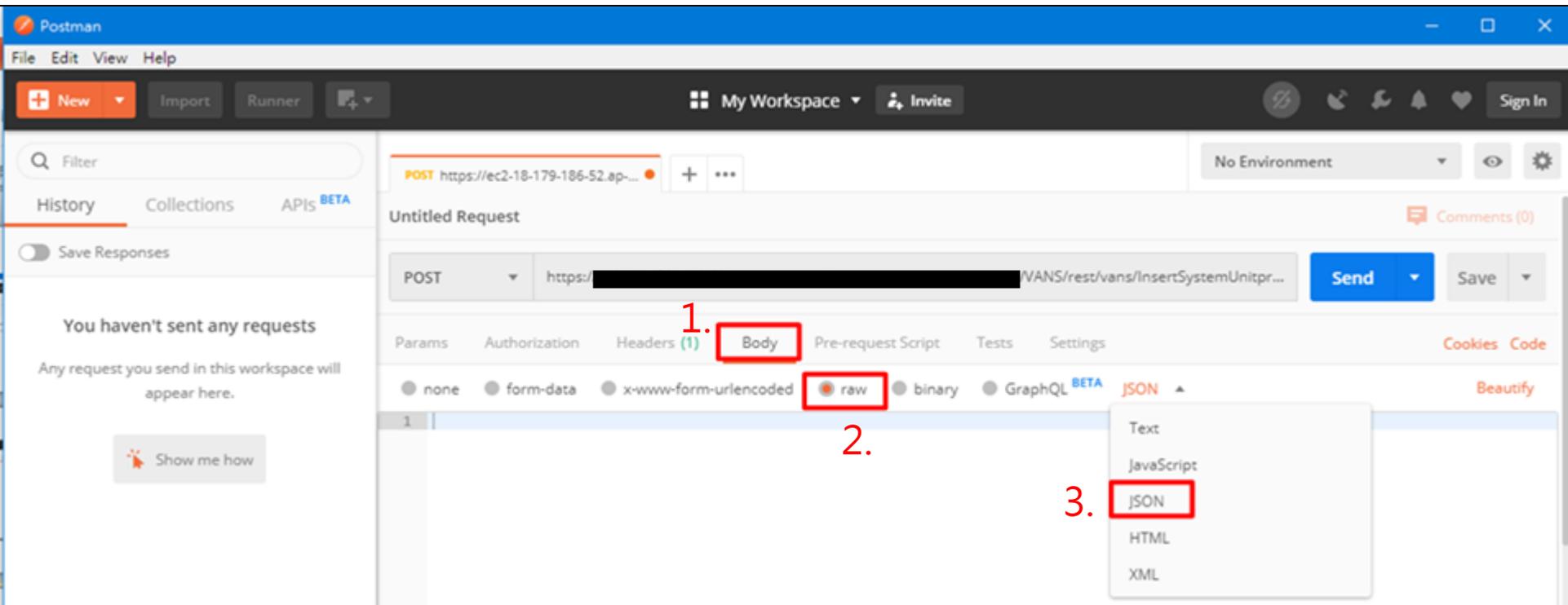
Postman設定(3/4)

- 傳輸方式選擇POST，並貼上實作機API網址



Postman設定(4/4)

- 切換至Body頁籤，選擇raw，右邊格式選擇JSON，即可完成前置設定



執行API登錄(2/2)

- 按下Send，即可於下方看到測試結果

The screenshot shows a REST client interface with a POST request to `https://ec2-18-179-186-52.ap-northeast-1.compute.amazonaws.com/VANS/rest/vans/InsertSystemUnitproduct`. The request body is a JSON array of two objects. The first object represents MariaDB 10.3.9 and the second represents LocalGPO. The response status is 200 OK with a time of 2.59s and size of 242 B. The response body is a JSON object with the following fields:

```
1 {  
2   "Message": "0101",  
3   "Describe": "success"  
4 }
```

The `Send` button is highlighted with a red box, and the response body is highlighted with a green box. The text "API傳輸後回傳之訊息代碼" is overlaid on the response body.