



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**6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檢測之能力
- 課程重點
 - 政府機關資安弱點通報機制說明與實作
 - 安全性更新管理機制說明與實作
- 重要產出
 - 政府機關資安弱點通報機制實作結果
 - 安全性更新管理機制實作結果

課程行政事項

- 上課時間安排
 - 上午：9:30-12:30(3小時)
 - 午休：12:30-13:30
 - 下午：13:30-16:30(3小時)
 - 問題討論：16:30-17:00
- 課程進行中，為確保學習效果請勿使用3C產品
- 上午與下午課程請記得分別簽到
- 上課中有任何需求，請告知行政人員或講師

課程大綱

- 前言
- VANS機制介紹
- VANS系統說明與實作
 - VANS系統說明
 - 資訊資產弱點管理作業流程
 - 實作練習1：資訊資產盤點
 - 實作練習2：資訊資產正規化與登錄
 - 實作練習3：弱點修補與資產更新作業
 - 安全性更新管理機制說明與實作
 - MBSA工具介紹
 - 安全性更新檢測流程
 - 實作練習4：單機環境檢測與報告分析
 - 實作練習5：網域派送檢測

課程大綱

- 前言
- VANS機制介紹
- VANS系統說明與實作
 - VANS系統說明
 - 資訊資產弱點管理作業流程
 - 實作練習1：資訊資產盤點
 - 實作練習2：資訊資產正規化與登錄
 - 實作練習3：弱點修補與資產更新作業
- 安全性更新管理機制說明與實作
 - MBSA工具介紹
 - 安全性更新檢測流程
 - 實作練習4：單機環境檢測與報告分析
 - 實作練習5：網域派送檢測

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

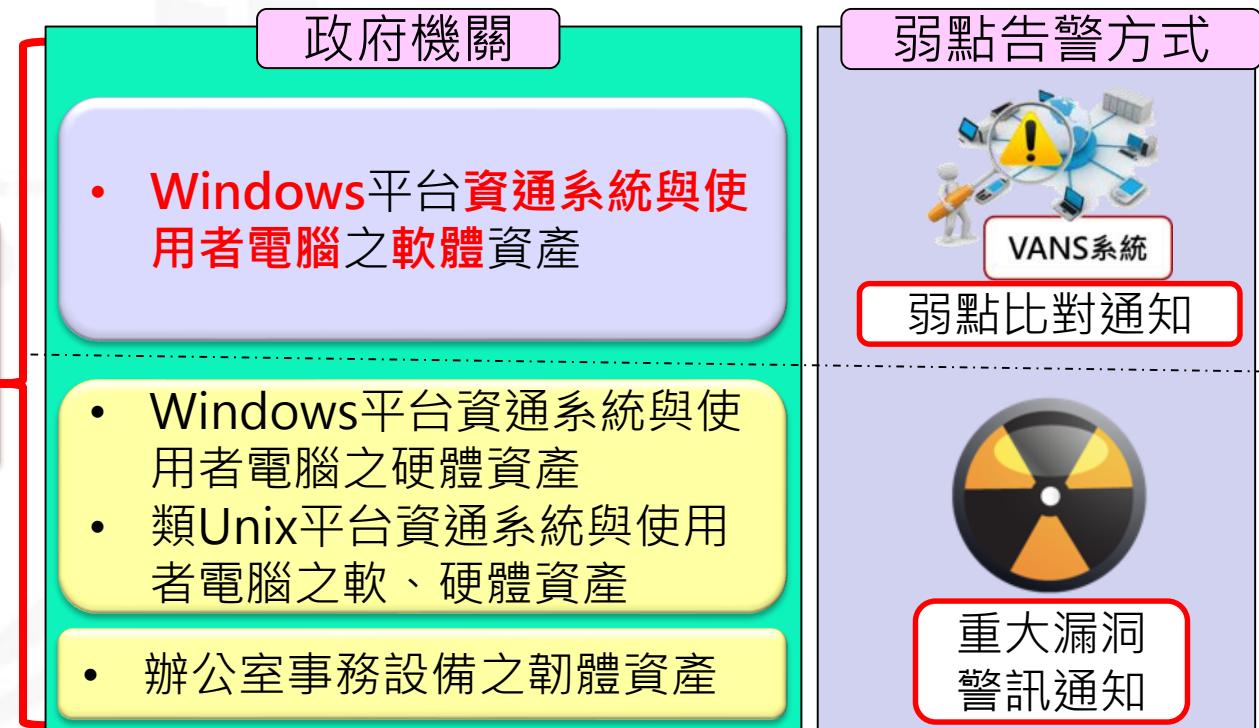
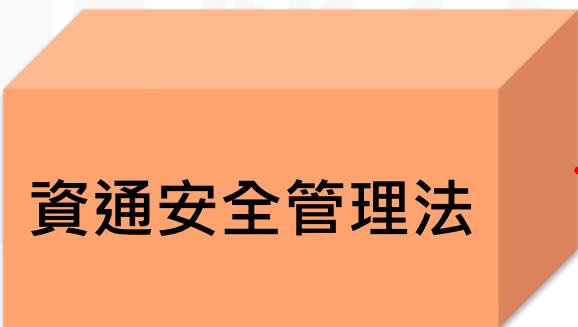
- 如何在應變處理後，持續追蹤弱點修補情形

課程大綱

- 前言
- VANS機制介紹
- VANS系統說明與實作
 - VANS系統說明
 - 資訊資產弱點管理作業流程
 - 實作練習1：資訊資產盤點
 - 實作練習2：資訊資產正規化與登錄
 - 實作練習3：弱點修補與資產更新作業
- 安全性更新管理機制說明與實作
 - MBSA工具介紹
 - 安全性更新檢測流程
 - 實作練習4：單機環境檢測與報告分析
 - 實作練習5：網域派送檢測

資通安全管理法相關規定

- 資通安全管理法第二章第十條
 - 公務機關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



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
 - 定期蒐集資通系統主機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

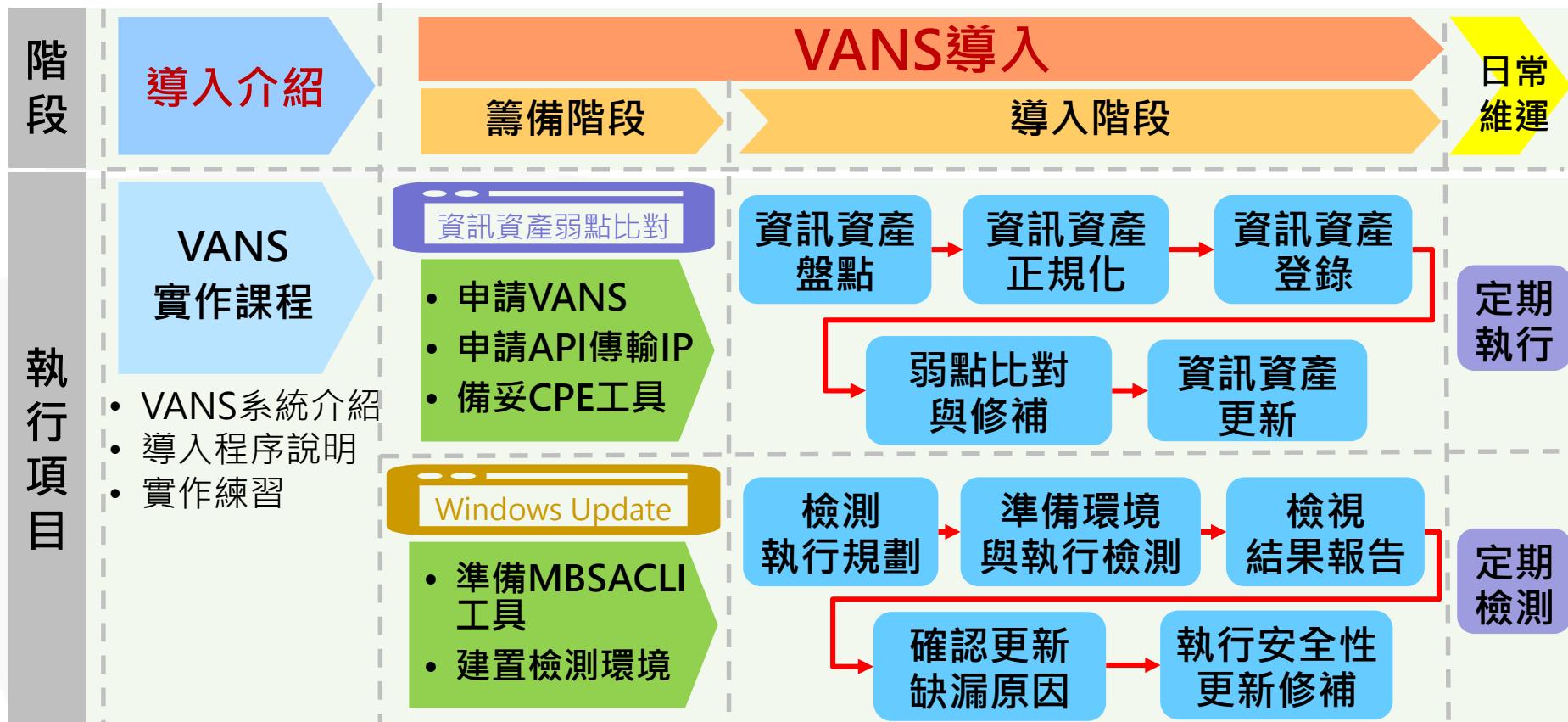


VANS目標

- 確認資訊資產弱點
 - 著集政府機關使用之**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
- 微軟安全性更新檢測報告解析功能
 - 搭配微軟提供之免費**MBSA**檢測工具，協助機關以**自動化方式**檢視安全更新落實程度



VANS導入作業流程



預期效益

- 縮短弱點修補空窗期
 - VANS每日更新弱點資料庫(NVD)資料，以提供最新弱點比對結果，當使用軟體存在重大弱點時，機關得以及早得知與應變處理
- 降低重大弱點管控與追蹤之成本
 - 提供相關弱點資訊與自我檢查機制，以降低重大弱點管控與修補情形追蹤之人力與資源成本
- 追蹤軟體資產弱點修補情形
 - 定時至VANS更新資訊資產項目，完整掌握各項弱點修補情形



課程大綱

- 前言
- VANS機制介紹
- VANS系統說明與實作
 - VANS系統說明
 - 資訊資產弱點管理作業流程
 - 實作練習1：資訊資產盤點
 - 實作練習2：資訊資產正規化與登錄
 - 實作練習3：弱點修補與資產更新作業
 - 安全性更新管理機制說明與實作
 - MBSA工具介紹
 - 安全性更新檢測流程
 - 實作練習4：單機環境檢測與報告分析
 - 實作練習5：網域派送檢測

系統介紹

- VANS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機制 (VANS)

一般權限帳號登入 機關管理者帳號登入

NCCST

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：

電話：(02)6631-6458 陳先生
Email : julianchen@nccst.nat.gov.tw

機關管理員帳號

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
2012 R2



Windows
Server 2016
Datacenter



Windows



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

資訊資產格式

- 資通系統與使用者電腦組成多變，所安裝之軟體套件多樣，難有資產管理系統能提供一體適用之軟體套件蒐集方式
- 不同廠商針對同一軟體資產，可能有不同描述方式



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)

資訊資產呈現方式(2/2)

- CPE條目範例

- Windows Server 2008 R2 Service Pack 1 64位元

廠商名稱	版本	版次
➤cpe:2.3: o :microsoft: windows_server_2008 : r2 sp1 : x64 :*.*.*.*.*		
產品類別	產品名稱	更新

- Oracle JDK 1.8.0 Update 92

廠商名稱	版本	
➤cpe:2.3: a :oracle: jdk 1.8.0 update_92 :*.*.*.*.*		
產品類別	產品名稱	更新

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資安風險之名稱標準化，俾利於各個弱點資料庫與安全工具之間統一漏洞相關資料
- 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**

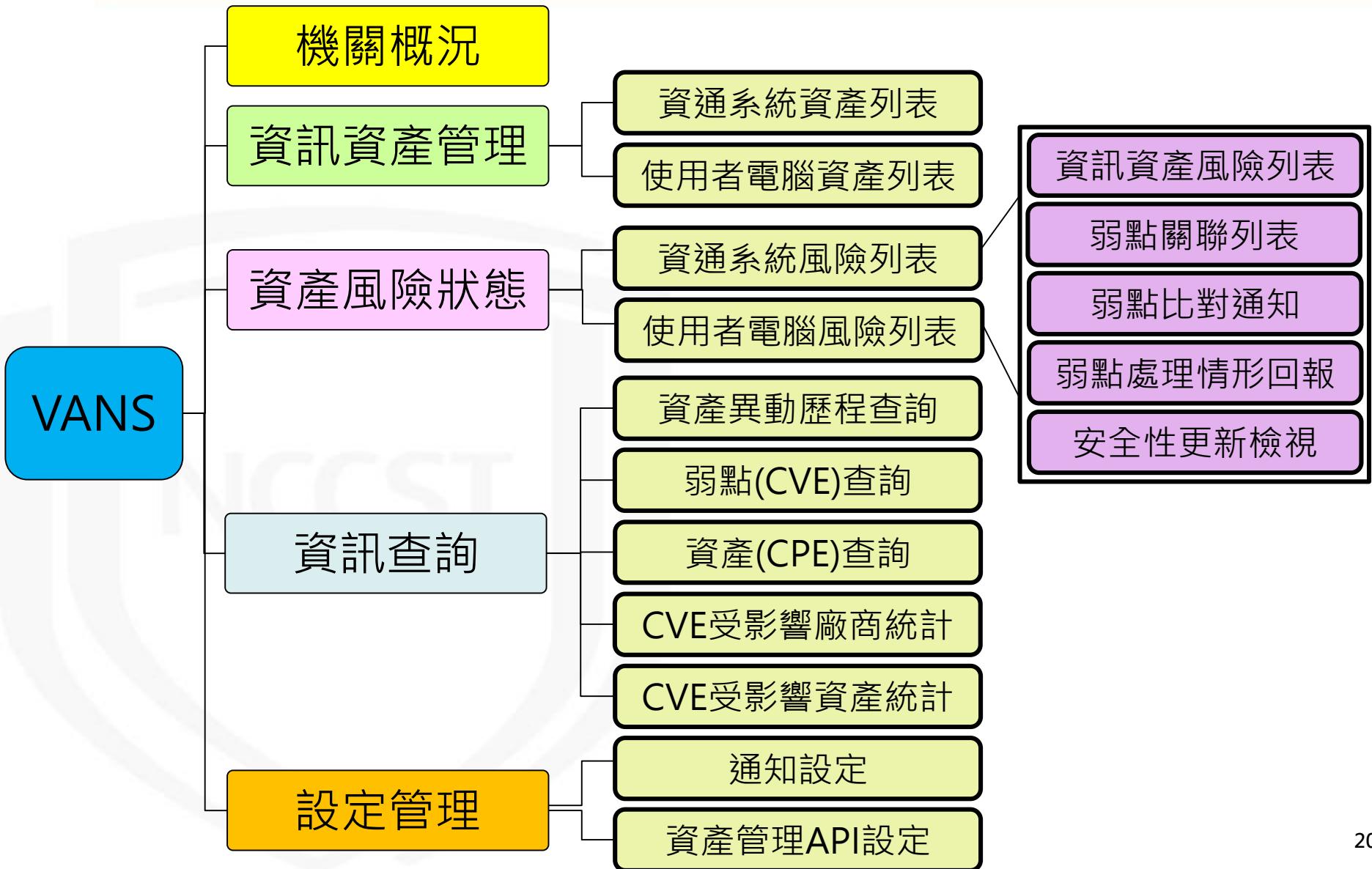
西元紀年 流水號



弱點資料庫

- National Vulnerability Database(簡稱NVD)為NIST所建置，專門用來蒐集各種弱點資訊的資料庫網站
 - 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
 - 目前已有150,148筆弱點數量與396,268筆CPE數量
 - VANS系統每天更新1次弱點資訊

系統功能總覽



系統介面說明

系統名稱

登出



政府機關資安弱點通報機制

測試人員



機關概況

功能路徑

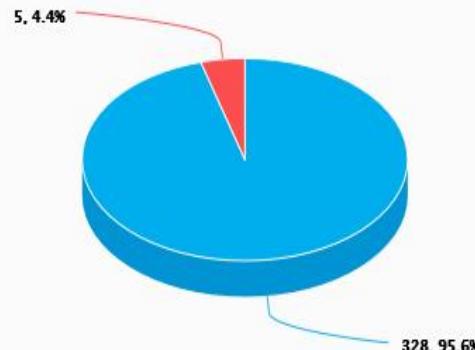
檢視方式

資通系統 使用者電腦

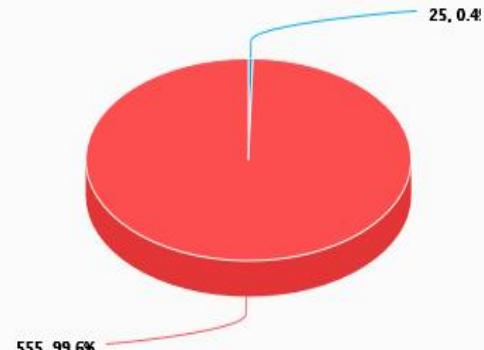
主畫面

功能選單列

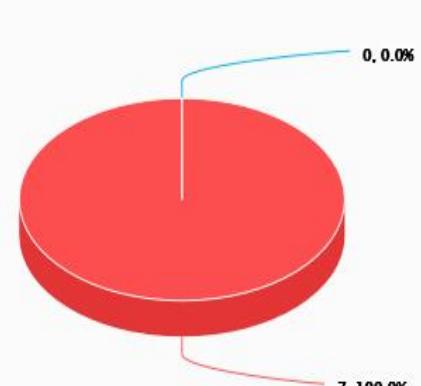
資通系統資產類別統計



資通系統弱點處理情形(CVE)



資通系統安全性更新情形(Windows Update)



服務申請流程



機關提出申請

- 電話申請
- Email申請

提供申請資訊

- 單位資訊
- 聯絡資訊



參閱操作手冊

- 操作諮詢
- 服務說明



開始使用服務

- 資料建立
- 弱點比對

聯絡窗口：陳先生

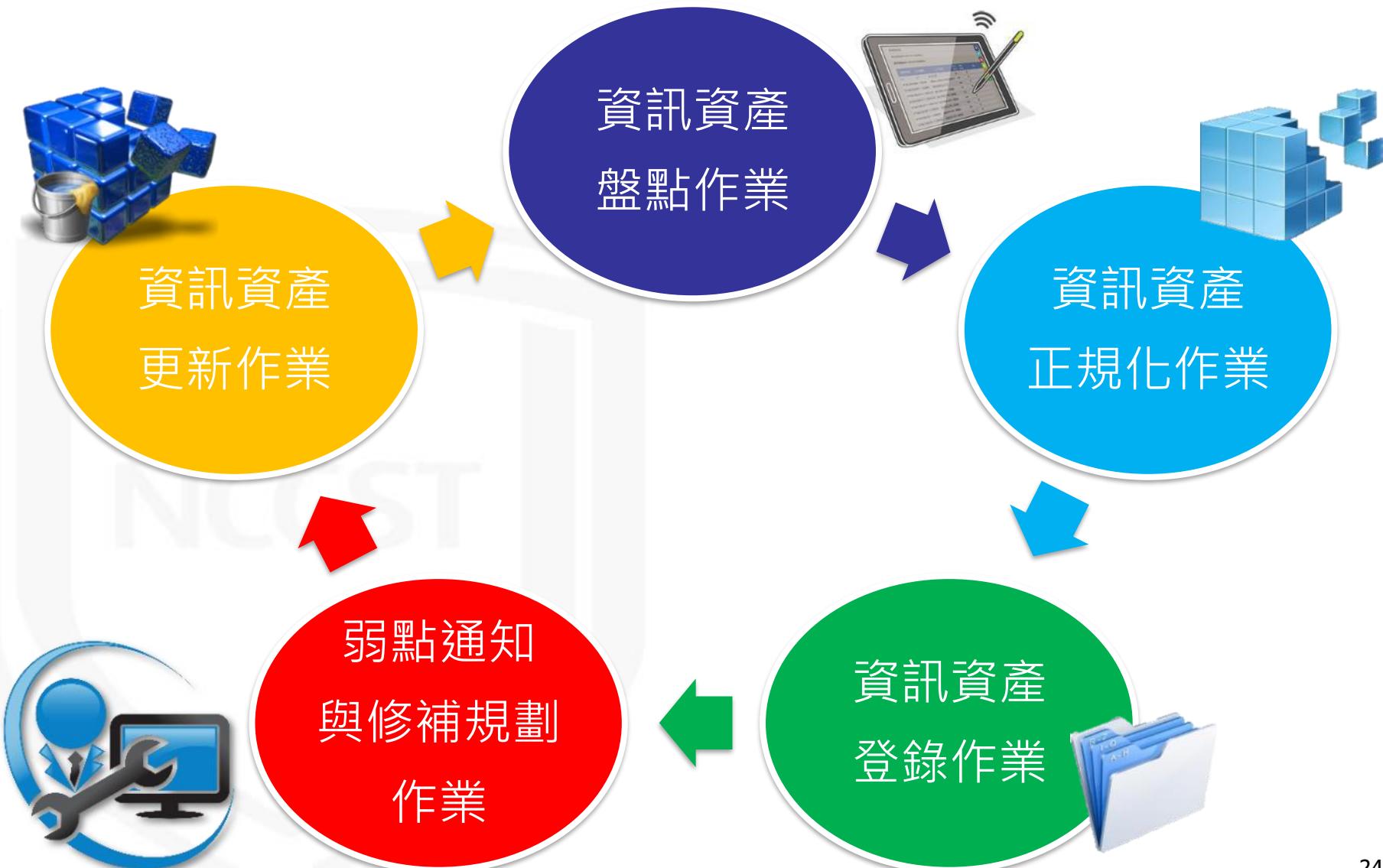
聯絡電話：(02)6631-6458

聯絡信箱：julianchen@nccst.nat.gov.tw

課程大綱

- 前言
- VANS機制介紹
- VANS系統說明與實作
 - VANS系統說明
 - 資訊資產弱點管理作業流程
 - 實作練習1：資訊資產盤點
 - 實作練習2：資訊資產正規化與登錄
 - 實作練習3：弱點修補與資產更新作業
 - 安全性更新管理機制說明與實作
 - MBSA工具介紹
 - 安全性更新檢測流程
 - 實作練習4：單機環境檢測與報告分析
 - 實作練習5：網域派送檢測

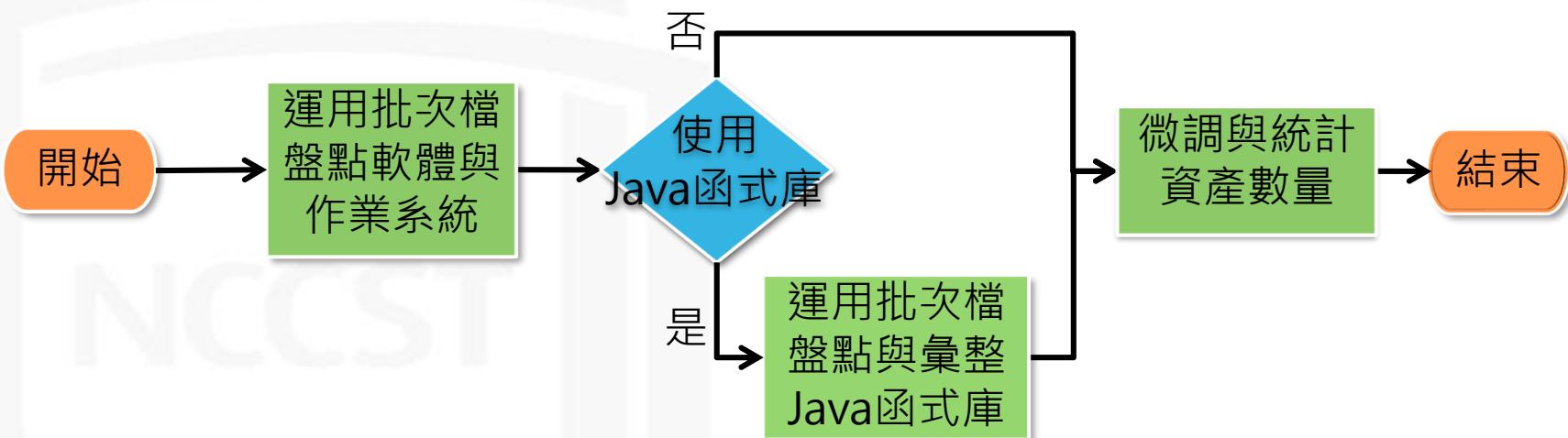
資訊資產弱點管理作業流程



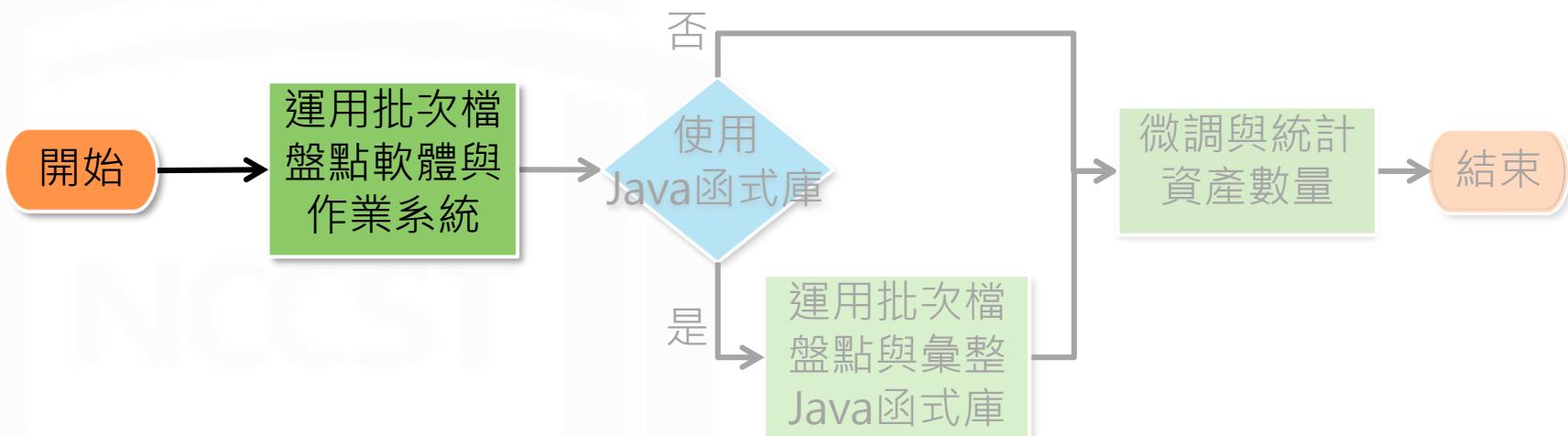
資訊資產弱點管理作業流程



資訊資產盤點作業流程



資訊資產盤點作業流程



批次檔盤點工具介紹

● WMIC

- 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
- WMIC為Windows管理工具之命令列介面，可用以盤點作業系統資訊與已安裝軟體清單

● 登錄機碼值

- 藉由查詢登錄機碼值，可列出已安裝軟體清單



運用批次檔盤點

- STEP1：以系統管理員身分執行**軟體盤點**批次檔
- STEP2：於**公用文件**檢視盤點清單
 - 包含**作業系統資訊**與**軟體盤點**清單

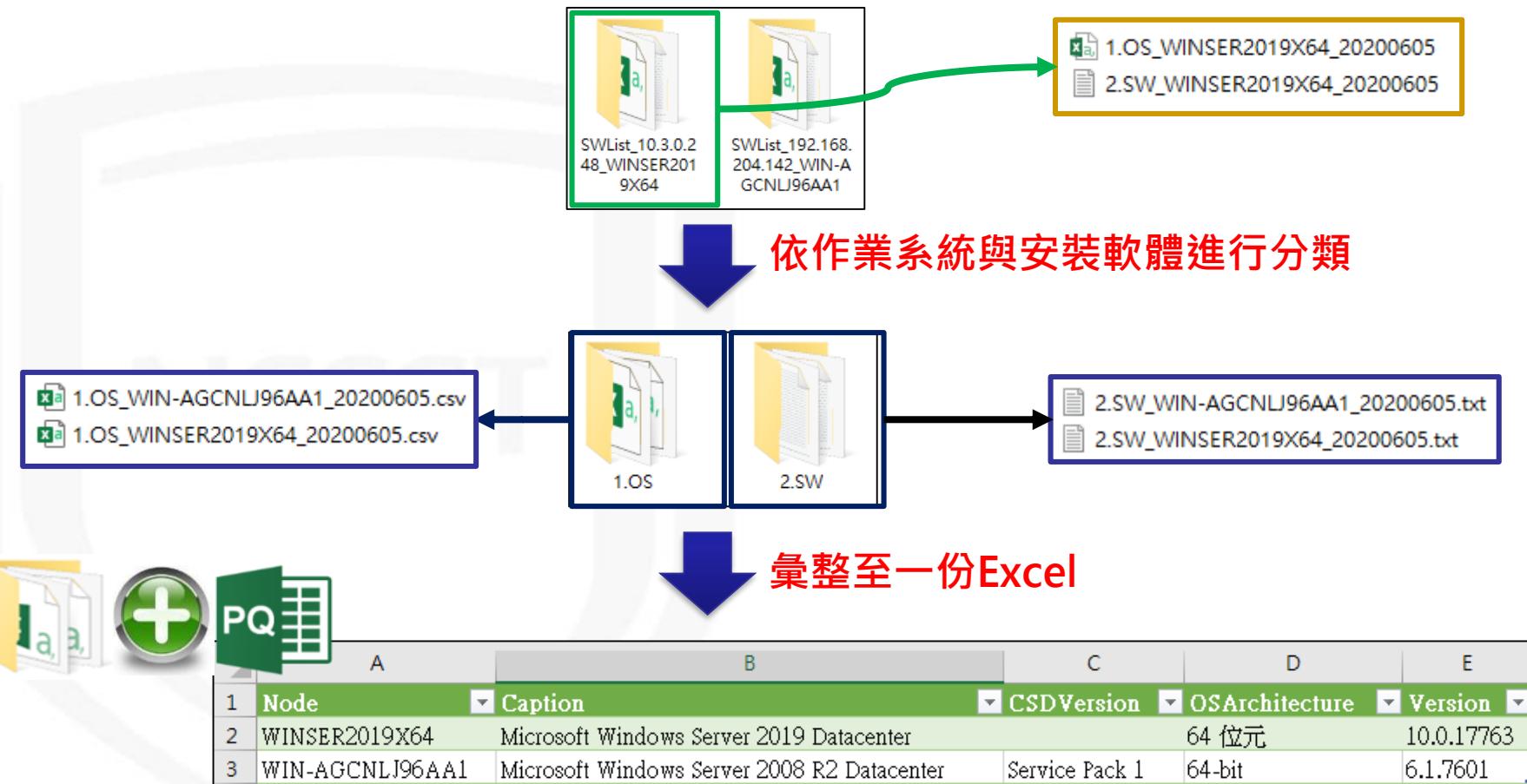


Excel彙整功能介紹

- 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**或更新的版本
- 下載網址：
 - <https://www.microsoft.com/zh-TW/download/details.aspx?id=39379>

彙整資訊資產清單(1/2)

- STEP1：將盤點批次檔產出之作業系統資訊與軟體盤點清單，歸類至個別資料夾



彙整資訊資產清單(2/2)

- STEP2：透過Power Query匯入歸類後之資料夾

- 若為Excel 2010或2013，選擇上方選單列「Power Query」，並選擇從資料夾匯入檔案
- 若為Excel 2016或2019，選擇上方選單列「資料」，並選擇從資料夾匯入檔案

*適用版本



Excel 2010 Excel 2013

1. Power Query

2. 從資料夾

3. 從資料夾
匯入有關資料夾中各檔案的中繼資料和連結。

*適用版本



Excel 2016

1. 資料

2. 新查訉

3. 從檔案(E)

4. 從資料夾(E)

*適用版本



Excel 2019

1. 資料

2. 取得資料

3. 從檔案(E)

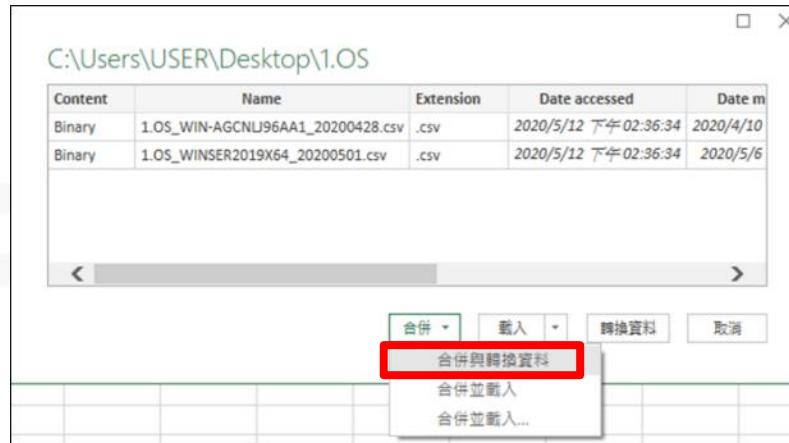
4. 從資料夾(E)

資料夾
資料夾路徑
C:\Users\USER\Desktop\1.OS
確定 取消

32

彙整資訊資產清單_作業系統(1/4)

- STEP1：開啟1.OS資料夾，選擇合併與轉換資料



- STEP2：出現「合併檔案」視窗，直接點選「確定」



彙整資訊資產清單_作業系統(2/4)



- STEP3：於查詢編輯器視窗中，篩選與移除多餘資訊
 - 移除「Source.Name」
 - 篩選「Column1」欄位，過濾空白資料列
 - 點選「使用第一個資料列作為標頭」，以命名欄位名稱
 - 篩選「Node」欄位，過濾多餘表頭列

The screenshot shows the Microsoft Query Editor interface with three main windows:

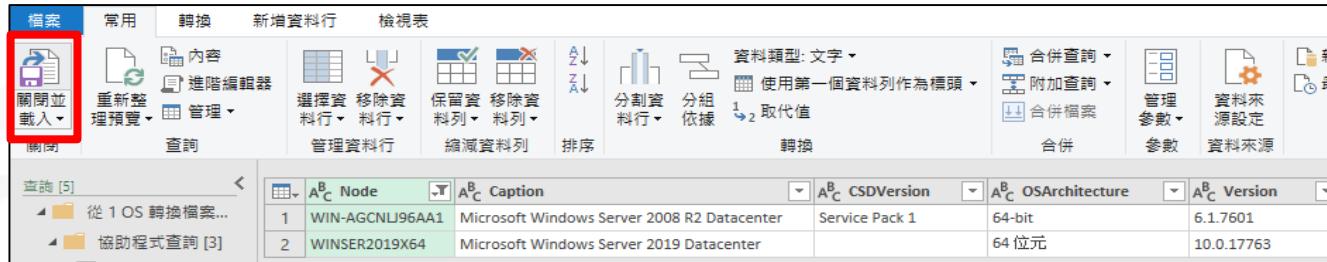
- Left Window (Data View):** Displays a table with columns "Source.Name" and "Column1". The "Column1" column contains values like "Node", "WIN-AGCNLJ96AA", etc. A context menu is open over the first row of "Column1", with the "Delete" option highlighted.
- Middle Window (Query Editor):** Shows the "常用" (Common) tab selected. The "Text Type" dropdown is set to "Text". A red box highlights the "Use the first data row as header" checkbox under the "Transform" tab.
- Right Window (Result View):** Displays a table with columns "Node" and "Caption". The "Caption" column contains values like "Microsoft Windows", "Caption", etc. A context menu is open over the first row of "Node", with the "Delete" option highlighted.

Bottom navigation bar:

- Search bar: (All selected)
- Checkboxes: Node (unchecked), WIN-AGCNLJ96AA (checked), WINSER2019X64 (checked)
- Buttons: 確定 (OK), 取消 (Cancel)

彙整資訊資產清單_作業系統(3/4)

- STEP4：點選「關閉並載入」完成彙整
- STEP5：將彙整結果複製貼上至資訊資產清冊*

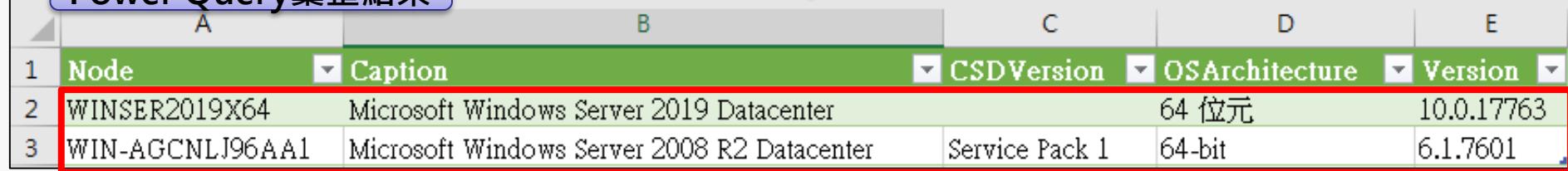


A screenshot of the Microsoft Power Query ribbon. The '常用' (Home) tab is selected. The '转换' (Transform) tab is active. The '关闭并载入' (Close & Load) button is highlighted with a red box. Below the ribbon, a preview pane shows two rows of data from a Windows Server dataset.

	A ^B _Node	A ^B _Caption	A ^B _CSDVersion	A ^B _OSArchitecture	A ^B _Version
1	WIN-AGCNLJ96AA1	Microsoft Windows Server 2008 R2 Datacenter	Service Pack 1	64-bit	6.1.7601
2	WINSER2019X64	Microsoft Windows Server 2019 Datacenter		64 位元	10.0.17763

 完成彙整

Power Query彙整結果

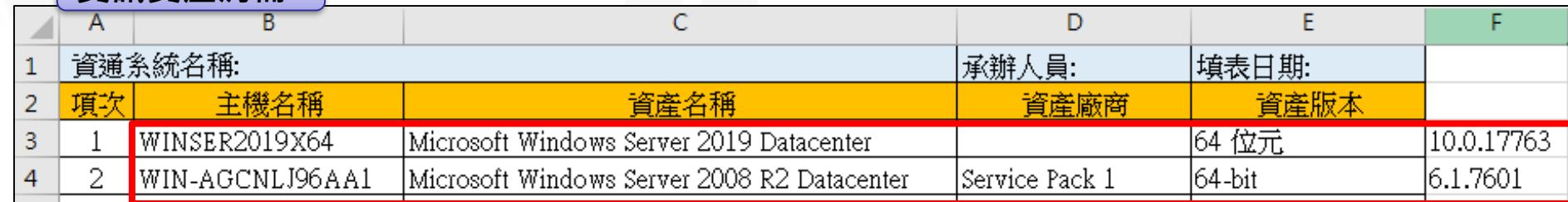


A screenshot of a Microsoft Excel spreadsheet. The title bar says 'Power Query彙整結果'. The table has four columns: 'Node', 'Caption', 'CSDVersion', and 'Version'. Row 1: Node (A1), Caption (B1), CSDVersion (C1), Version (D1). Row 2: WINSER2019X64 (A2), Microsoft Windows Server 2019 Datacenter (B2), 64 位元 (C2), 10.0.17763 (D2). Row 3: WIN-AGCNLJ96AA1 (A3), Microsoft Windows Server 2008 R2 Datacenter (B3), Service Pack 1 (C3), 64-bit (D3).

	Node	Caption	CSDVersion	Version
1	WINSER2019X64	Microsoft Windows Server 2019 Datacenter	64 位元	10.0.17763
2	WIN-AGCNLJ96AA1	Microsoft Windows Server 2008 R2 Datacenter	Service Pack 1	64-bit

 複製貼上

資訊資產清冊



A screenshot of a Microsoft Excel spreadsheet titled '資訊資產清冊'. The table has six columns: 'A', 'B', 'C', 'D', 'E', and 'F'. Row 1: 資通系統名稱: (B1), 承辦人員: (D1), 填表日期: (E1). Row 2: 項次 (A2), 主機名稱 (B2), 資產名稱 (C2), 資產廠商 (D2), 資產版本 (E2). Row 3: 1 (A3), WINSER2019X64 (B3), Microsoft Windows Server 2019 Datacenter (C3), (D3), 64 位元 (E3), 10.0.17763 (F3). Row 4: 2 (A4), WIN-AGCNLJ96AA1 (B4), Microsoft Windows Server 2008 R2 Datacenter (C4), Service Pack 1 (D4), 64-bit (E4), 6.1.7601 (F4).

	A	B	C	D	E	F
1	資通系統名稱:			承辦人員:	填表日期:	
2	項次	主機名稱	資產名稱	資產廠商	資產版本	
3	1	WINSER2019X64	Microsoft Windows Server 2019 Datacenter		64 位元	10.0.17763
4	2	WIN-AGCNLJ96AA1	Microsoft Windows Server 2008 R2 Datacenter	Service Pack 1	64-bit	6.1.7601

*資訊資產清冊：課堂中提供

彙整資訊資產清單_作業系統(4/4)

- STEP6：手動調整資產資訊清冊

– 作業系統資訊需手動調整「資產名稱」與填寫「資產廠商」欄位

	A	B	C	D	E	F
1	資通系統名稱:		承辦人員:	填表日期:		
2	項次	主機名稱	資產名稱	資產廠商	資產版本	
3	1	WINSER2019X64	Microsoft Windows Server 2019 Datacenter		64 位元	10.0.17763
4	2	WIN-AGCNLJ96AA1	Microsoft Windows Server 2008 R2 Datacenter	Service Pack 1	64-bit	6.1.7601

↓ 複製貼上

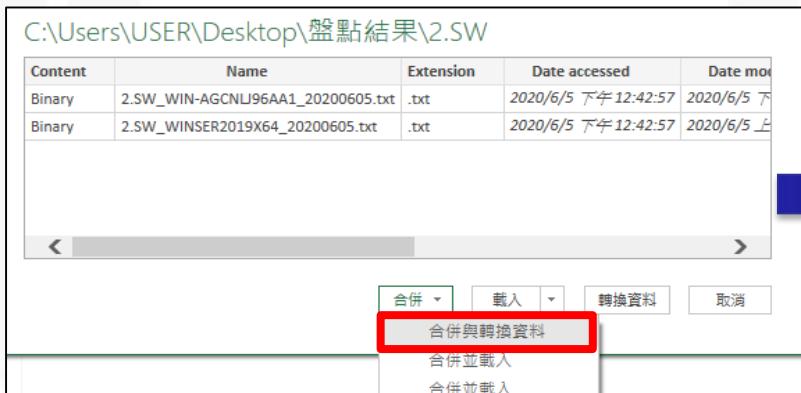
↓ 複製貼上

	A	B	C	D	E
1	資通系統名稱:		承辦人員:	填表日期:	
2	項次	主機名稱	資產名稱	資產廠商	資產版本
3	1	WINSER2019X64	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763
4	2	WIN-AGCNLJ96AA1	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit	Microsoft Corporation	6.1.7601

手動填寫

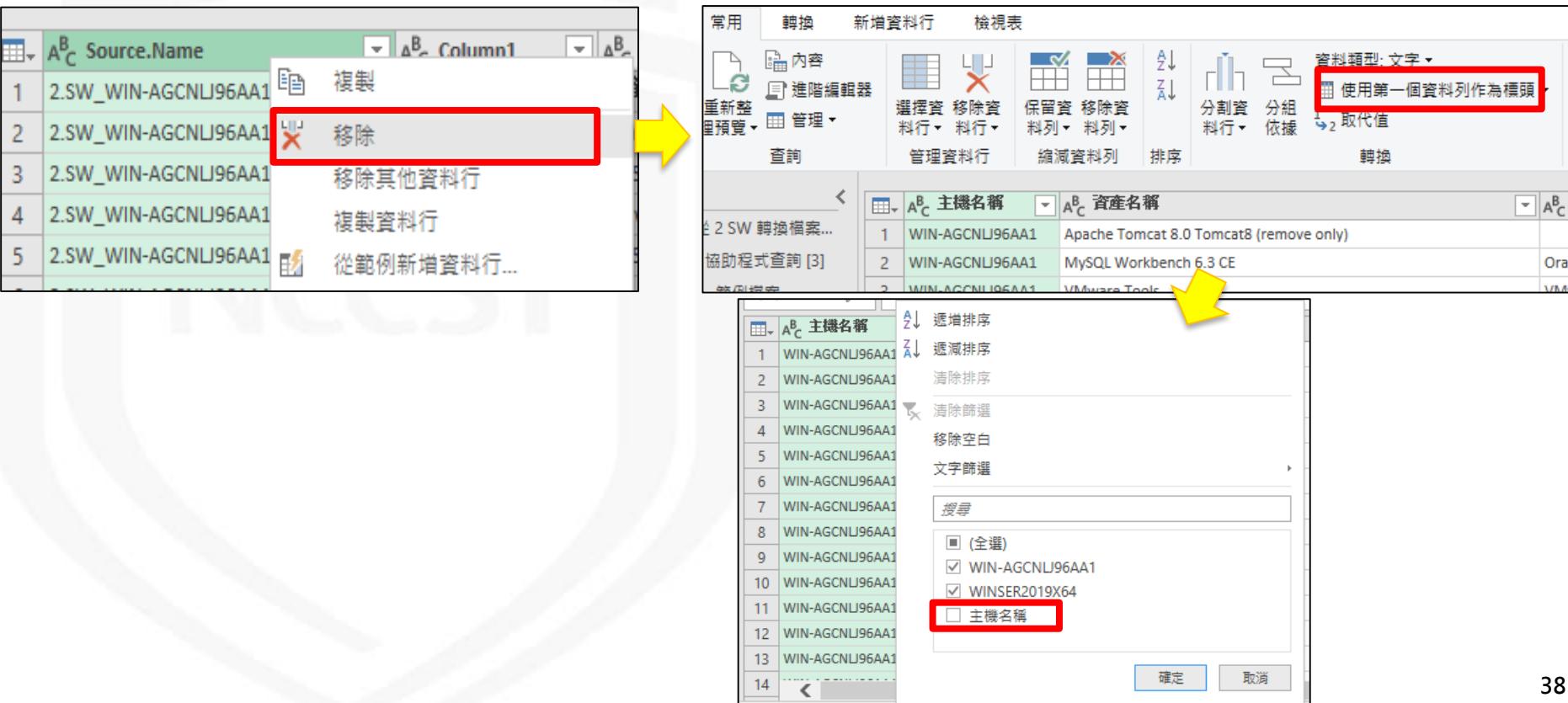
彙整資訊資產清單_應用程式(1/3)

- STEP1：開啟2.SW資料夾，選擇合併與轉換資料
- STEP2：於「合併檔案」視窗，將檔案原點(編碼方式)調整為65001:Unicode(utf-8)
- STEP3：將自訂分隔符號設定為「|」
– 輸入方式：Shift+\



彙整資訊資產清單_應用程式(2/3)

- STEP3：於查詢編輯器視窗中，篩選與移除多餘資訊
 - 移除「Source.Name」
 - 點選「使用第一個資料列作為標頭」，以命名欄位名稱
 - 篩選「主機名稱」欄位，過濾多餘表頭列欄位



The screenshot shows the Microsoft Query Editor interface. On the left, a context menu is open over the 'Source.Name' column header, with the 'Remove' option highlighted by a red box and a yellow arrow pointing to the 'Header' tab in the ribbon.

The 'Header' tab in the ribbon has a red box around the 'Use first column as header' checkbox. Below it, the 'Header' dropdown shows 'Host Name' selected.

The main query results grid shows three rows of data:

	主機名稱	資產名稱
1	WIN-AGCNLU96AA1	Apache Tomcat 8.0 Tomcat8 (remove only)
2	WIN-AGCNLU96AA1	MySQL Workbench 6.3 CE
3	WIN-AGCNLU96AA1	VMware Tools

At the bottom, a detailed filter dialog is open, also with a red box around the 'Host Name' checkbox. It lists several host names in the 'Selected' section, including 'WIN-AGCNLU96AA1' and 'WINSER2019X64'.

彙整資訊資產清單_應用程式(3/3)

- STEP4：點選「關閉並載入」完成彙整
- STEP5：將彙整結果複製貼上至資訊資產清冊*

Screenshot of the Power Query ribbon showing the '閉關並載入' (Close and Load) button highlighted in red.

The Power Query interface displays a query result table:

	A 主機名稱	B 資產名稱	C 資產廠商	D 資產版本
66	WINSER2019X64	Java SE Development Kit 8 Update 202 (64-bit)	Oracle Corporation	8.0.2020.8
67	WINSER2019X64	MySQL Connector Python v8.0.19	Oracle	8.0.19

完成彙整

Power Query彙整結果

Power Query彙整結果 table (highlighted by a red box):

	A 主機名稱	B 資產名稱	C 資產廠商	D 資產版本
1	主機名稱	資產名稱	資產廠商	資產版本
2	WIN-AGCNLJ96AA1	Apache Tomcat 8.0 Tomcat8 (remove only)		8.0.30
3	WIN-AGCNLJ96AA1	MySQL Workbench 6.3 CE	Oracle Corporation	6.3.7

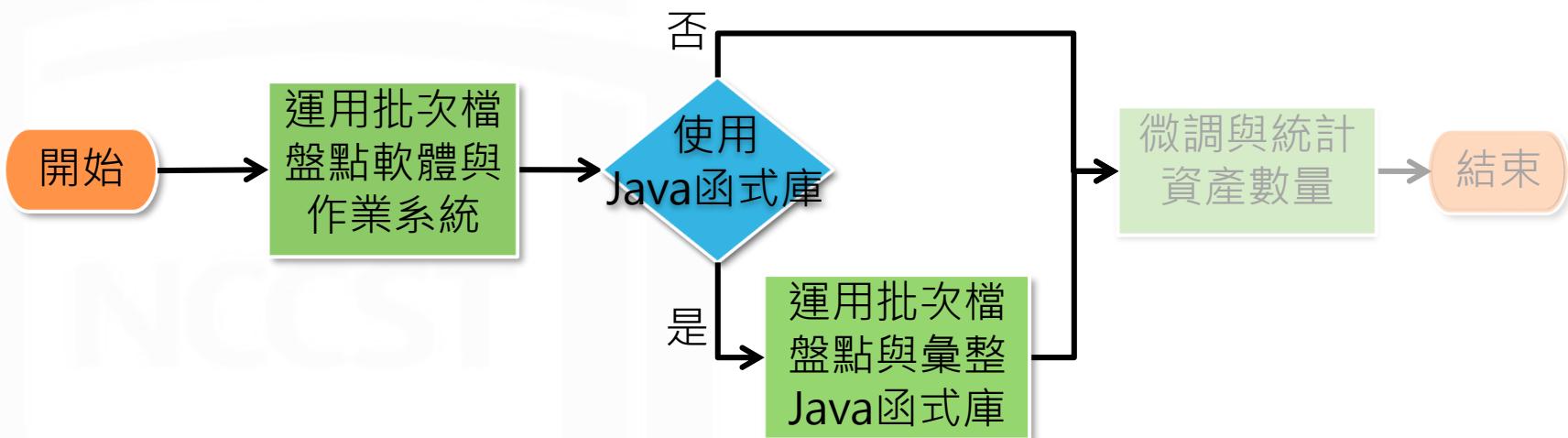
複製貼上

資訊資產清冊

資訊資產清冊 table (highlighted by a red box):

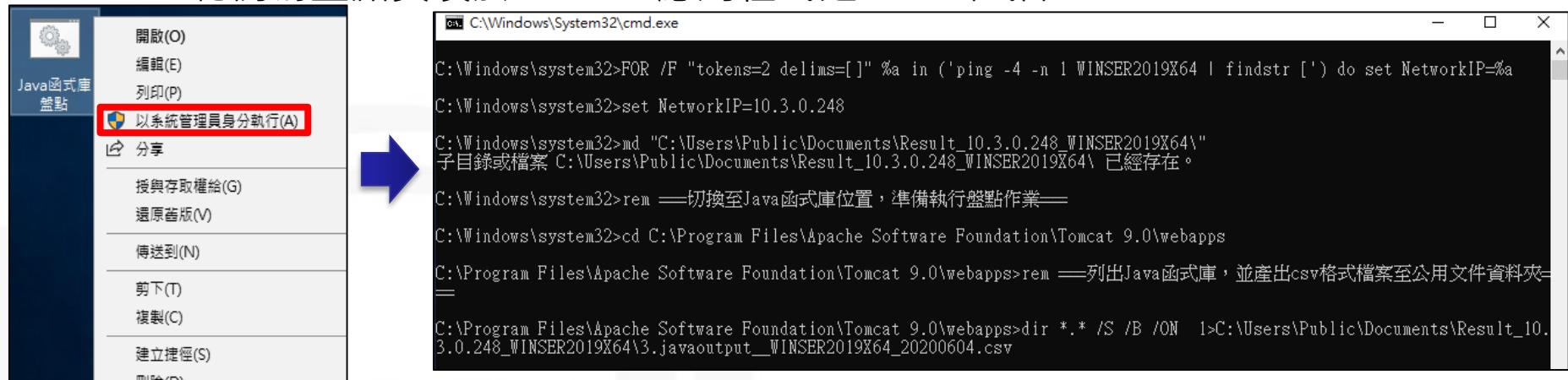
	A 資通系統名稱:	C 資產名稱	D 承辦人員:	E 填表日期:	
1	項	主機名稱	資產廠商	資產版本	
2	3	WIN-AGCNLJ96AA	Apache Tomcat 8.0 Tomcat8 (remove only)	8.0.30	
5	4	WIN-AGCNLJ96AA	MySQL Workbench 6.3 CE	Oracle Corporation	6.3.7

資訊資產盤點作業流程

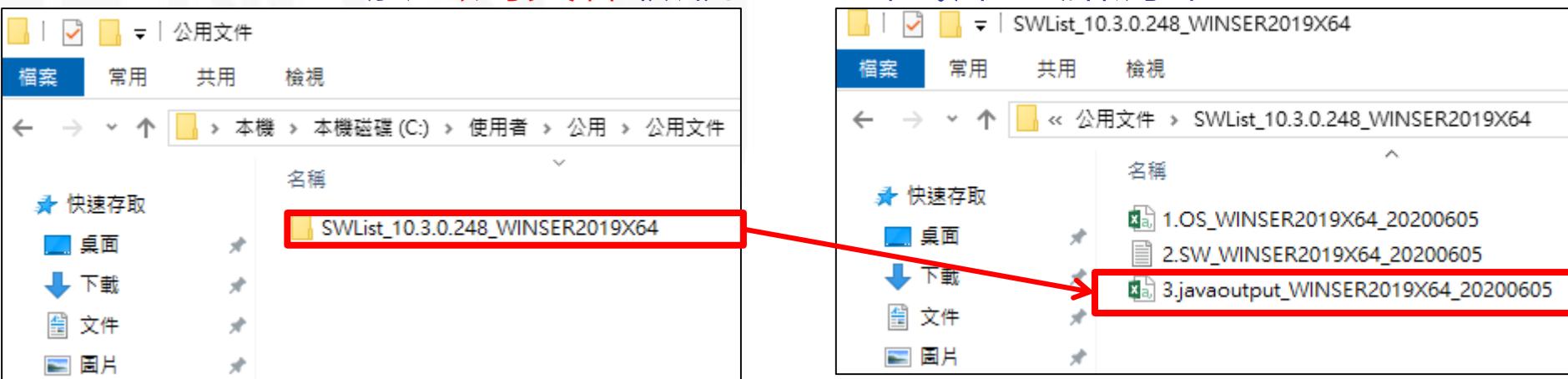


運用批次檔盤點Java函式庫

- STEP1：以系統管理員身分執行「Java函式庫盤點」批次檔
— 範例為盤點安裝於Tomcat應用程式之Java函式庫



- STEP2：於公用文件檢視Java函式庫盤點清單



彙整Java函式庫清單(1/3)

- STEP1：Java函式庫盤點清單彙整至Java函式庫彙整範本*

Java函式庫盤點清單

	A	B
1	C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\docs\WEB-INF\lib\commons-beanutils-1.8.0.jar	
2	C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\docs\WEB-INF\lib\commons-fileupload-1.3.2.jar	
3	C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\docs\WEB-INF\lib\commons-io-2.2.jar	
4	C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\docs\WEB-INF\lib\commons-lang-2.4.jar	
5	C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\docs\WEB-INF\lib\commons-lang3-3.2.jar	
6	C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\docs\WEB-INF\lib\freemarker-2.3.22.jar	

↓ 複製貼上

Java函式庫彙整範本

A	B	C	D	E
原始資料				
1 C:\Program Files\Apache Software	Java函式庫	用取代去除.jar	Java函式庫名稱	Java函式庫版本
2 commons-beanutils-1.8.0.jar	commons-beanutils-1.8.0	commons-beanutils-1.8.0	commons-beanutils	1.8.0
3 commons-fileupload-1.3.2.jar	commons-fileupload-1.3.2	commons-fileupload-1.3.2	commons-fileupload	1.3.2
4 commons-io-2.2.jar	commons-io-2.2	commons-io-2.2	commons-io	2.2
5 commons-lang-2.4.jar	commons-lang-2.4	commons-lang-2.4	commons-lang	2.4
6 commons-lang3-3.2.jar	commons-lang3-3.2	commons-lang3-3.2	commons-lang3	3.2
7 freemarker-2.3.22.jar	freemarker-2.3.22	freemarker-2.3.22	freemarker	2.3.22

彙整Java函式庫清單(2/3)

- STEP2：取得Java函式庫名稱與Java函式庫版本欄位之值並手動調整
 - 複製D、E欄位並至調整後欄位F、G貼上值
 - 若版本包含「-」需於調整後欄位手動調整

Java函式庫彙整範本

D	E	F	G
Java函式庫名稱	Java函式庫版本	Java函式庫名稱(調整後)	Java函式庫版本(調整後)
commons-beanutils	1.8.0	commons-beanutils	1.8.0
commons-fileupload	1.3.2	commons-fileupload	1.3.2
commons-io	2.2	commons-io	2.2
commons-lang	2.4	commons-lang	2.4
commons-lang3	3.2	commons-lang3	3.2
freemarker	2.3.22	freemarker	2.3.22
javassist	3.11.0.GA	javassist	3.11.0.GA
ognl	3.0.19	ognl	3.0.19
struts2-core	2.3.30	struts2-core	2.3.30
xwork-core	2.3.30	xwork-core	2.3.30

複製並貼上「值」

彙整Java函式庫清單(3/3)

- STEP3：將Java函式庫彙整範本彙整至資訊資產清冊中
 - 將Java函式庫名稱(調整後)複製至**資產名稱**
 - 將Java函式庫版本(調整後)複製至**資產版本**

Java函式庫彙整範本

D	E	F	G
Java函式庫名稱	Java函式庫版本	Java函式庫名稱(調整後)	Java函式庫版本(調整後)
commons-beanutils	1.8.0	commons-beanutils	1.8.0
commons-fileupload	1.3.2	commons-fileupload	1.3.2
commons-io	2.2	commons-io	2.2
commons-lang	2.4	commons-lang	2.4
commons-lang3	3.2	commons-lang3	3.2

資訊資產清冊

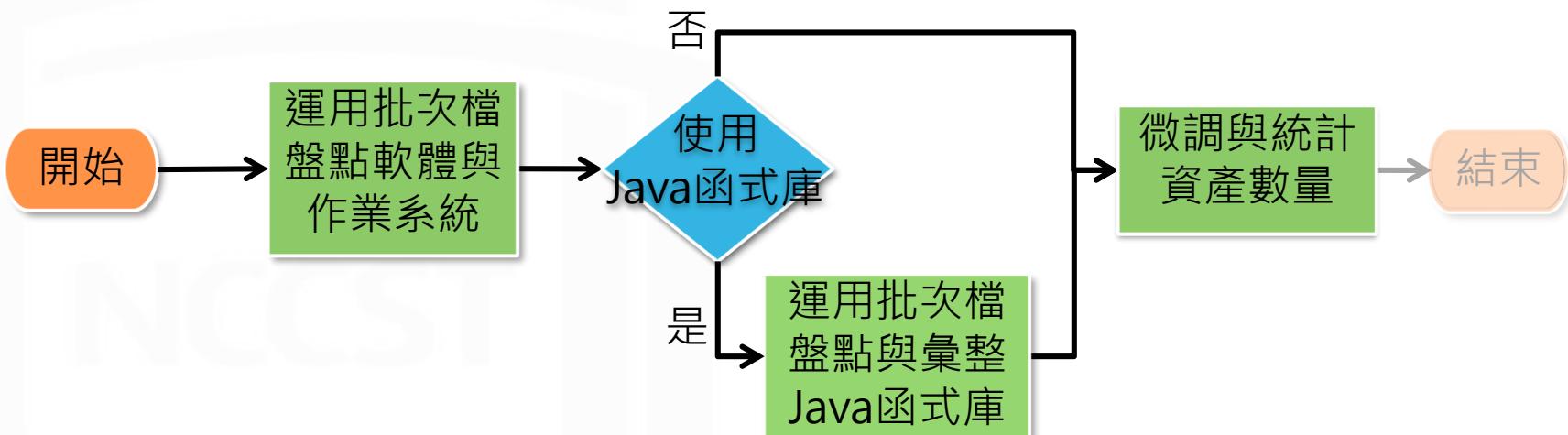
A	B	C	D	E
1	資通系統名稱:	承辦人員:	填表日期:	
2	項	主機名稱	資產廠商	資產版本
110	108	WINSER2019X64	1.8.0	
111	109	WINSER2019X64	1.3.2	
112	110	WINSER2019X64	2.2	
113	111	WINSER2019X64	2.4	
114	112	WINSER2019X64	3.2	

填寫項次與主機名稱

↓ 複製貼上

↓ 複製貼上

資訊資產盤點作業流程



空白欄位填上N/A

- 部分軟體與Java函式庫因無「資產廠商」資訊，需於資產廠商填上N/A

– 於資產廠商篩選「空格」按下確定，並統一補上N/A

A	B	C	D	E	F	G
1 資通系統名稱:			承辦人員:	填表日期:		
2 項:	主機名稱	資產名稱	資產廠商	資產版本		
3 1 WINSER2019X64	Microsoft Windows Server 2019 Datacenter 64 位元		從 A 到 Z 排序(S)	10.0.17763		
4 2 WIN-AGCNLJ96AA	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit		從 Z 到 A 排序(O)	6.1.7601		
5 3 WIN-AGCNLJ96AA	Apache Tomcat 8.0 Tomcat8 (remove only)		依色彩排序(I)	8.0.30		
6 4 WIN-AGCNLJ96AA	MySQL Workbench 6.3 CE		依色彩篩選(I)	6.3.7		
7 5 WIN-AGCNLJ96AA	VMware Tools		文字篩選(E)	10.0.5.3228253		
8 6 WIN-AGCNLJ96AA	MySQL Connector/ODBC 5.3		搜尋	5.3.6		
9 7 WIN-AGCNLJ96AA	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219			10.0.40219		
10 8 WIN-AGCNLJ96AA	Java 8 Update 77 (64-bit)			8.0.770.3		
11 9 WIN-AGCNLJ96AA	MySQL Server 5.7			5.7.14		
12 10 WIN-AGCNLJ96AA	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161			9.0.30729.6161		
13 11 WIN-AGCNLJ96AA	Java SE Development Kit 8 Update 77 (64-bit)			8.0.770.3		
14 12 WIN-AGCNLJ96AA	Microsoft .NET Framework 4.5.1			4.5.50938		
15 13 WIN-AGCNLJ96AA	Microsoft Office IME (Chinese (Traditional)) 2010			14.0.4763.1000		
16 14 WIN-AGCNLJ96AA	Microsoft Office Office 64-bit Components 2010			14.0.4763.1000		
17 15 WIN-AGCNLJ96AA	Microsoft Office Shared 64-bit MUI (Chinese (Traditional)) 2010			14.0.4763.1000		
18 16 WIN-AGCNLJ96AA	MySQL Connector C++ 1.1.7			1.1.7		
19 17 WIN-AGCNLJ96AA	MySQL Connector/C 6.1			6.1.6		

篩選「空格」

填上N/A

統計資訊資產數量(1/3)

- STEP1：切換至資訊資產清冊「資產數量統計」頁籤
- STEP2：複製「資產數量(F)」欄位之值，貼上至「資產數量(A)」欄位，以保留資產數量欄位之值

資訊資產清冊

A	B	C	D	E	F
資產數量	資產名稱	資產廠商	資產版本	TEMP	資產數量
1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763	Microsoft Windows Server 2019 Datacenter 64 位元	1
1	Microsoft Windows Server 2008 R2 Datacenter Serv	Microsoft Corporation	6.1.7601	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bitMic	1
1	Apache Tomcat 8.0 Tomcat8 (remove only)		0.8.0.30	Apache Tomcat 8.0 Tomcat8 (remove only) 0.8.0.30	1
1	MySQL Workbench 6.3 CE	Oracle Corporation	6.3.7	MySQL Workbench 6.3 CE Oracle Corporation 6.3.7	1
1	VMware Tools	VMware, Inc.	10.0.5.322825	VMware Tools VMware, Inc. 10.0.5.3228253	1
1	MySQL Connector/ODBC 5.3	Oracle Corporation	5.3.6	MySQL Connector/ODBC 5.3 Oracle Corporation 5.3.6	1
1	Microsoft Visual C++ 2010 x64 Redistributable - 10	Microsoft Corporation	10.0.40219	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219 Microsoft	1
1	Java 8 Update 77 (64-bit)	Oracle Corporation	8.0.770.3	Java 8 Update 77 (64-bit) Oracle Corporation 8.0.770.3	1
1	MySQL Server 5.7	Oracle Corporation	5.7.14	MySQL Server 5.7 Oracle Corporation 5.7.14	1
1	Microsoft Visual C++ 2008 Redistributable - x64 9.0	Microsoft Corporation	9.0.30729.616	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 Micros	1
1	Java SE Development Kit 8 Update 77 (64-bit)	Oracle Corporation	8.0.770.3	Java SE Development Kit 8 Update 77 (64-bit) Oracle Corporation 8.0.7	1
2	Microsoft .NET Framework 4.5.1	Microsoft Corporation	4.5.50938	Microsoft .NET Framework 4.5.1 Microsoft Corporation 4.5.50938	2

複製並貼上「值」

統計資訊資產數量(2/3)

● STEP3：清除重複出現之資產

- 全選表格，點選功能列的「資料」→「移除重複項」
- 移除重複項中，點選「全選」並「確定」

資訊資產清冊

1 資料

2 移除重複項

3 全選(A)

4 確定

A	B	C	D	E	F
1	資產數量	資產名稱	資產廠商	資產版本	資產數量
2	1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation		Microsoft Windows Server 2019 Datacenter 64 位元
3	1	Microsoft Windows Server 2008 R2 Datacenter Server	Microsoft Corporation		Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit
4	1	Apache Tomcat 8.0 Tomcat8 (remove only)			Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit
5	1	MySQL Workbench 6.3 CE	Oracle Corporation		Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit
6	1	VMware Tools	VMware, Inc.		Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit
7	1	MySQL Connector/ODBC 5.3	Oracle Corporation		Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit
8	1	Microsoft Visual C++ 2010 x64 Redistributable - 10	Microsoft Corporation		Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit
9	1	Java 8 Update 77 (64-bit)	Oracle Corporation		Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit
10	1	MySQL Server 5.7	Oracle Corporation		Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit
11	1	Microsoft Visual C++ 2008 Redistributable - x64 9.0	Microsoft Corporation		Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit
12	1	Java SE Development Kit 8 Update 77 (64-bit)	Oracle Corporation		Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit
13	2	Microsoft .NET Framework 4.5.1	Microsoft Corporation		Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit

統計資訊資產數量(3/3)

- STEP4：點選「確定」即完成資訊資產數量統計

資訊資產清冊

A	B	C	D	E	F
資產數量	資產名稱	資產廠商	資產版本	TEMP	資產數量
1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763	Microsoft Windows Server 2019 Datacenter 64 位元 Microsoft Corporation	1
1	Microsoft Windows Server 2008 R2 Datacenter Serv	Microsoft Corporation	6.1.7601	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit Mic	1
1	Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	0.8.0.30	Apache Tomcat 8.0 Tomcat8 (remove only) N/A8.0.30	1
1	MySQL Workbench 6.3 CE	Microsoft Excel		MySQL Workbench 6.3 CE Oracle Corporation 6.3.7	1
1	VMware Tools	VMware, Inc.		VMware Tools VMware, Inc. 10.0.5.3228253	1
1	MySQL Connector/ODBC 5.3	Oracle Corporation		MySQL Connector/ODBC 5.3 Oracle Corporation 5.3.6	1
1	Microsoft Visual C++ 2010 x64 Redistributable - 10	Microsoft Corporation	10.0.40219	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219 Microsoft C	1
1	Java 8 Update 77 (64-bit)	Oracle Corporation		Java 8 Update 77 (64-bit) Oracle Corporation 8.0.770.3	1
1	MySQL Server 5.7	Oracle Corporation	5.7.14	MySQL Server 5.7 Oracle Corporation 5.7.14	1
1	Microsoft Visual C++ 2008 Redistributable - x64 9.0	Microsoft Corporation	9.0.30729.6161	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 Micros	1
1	Java SE Development Kit 8 Update 77 (64-bit)	Oracle Corporation	8.0.770.3	Java SE Development Kit 8 Update 77 (64-bit) Oracle Corporation 8.0.77	1
2	Microsoft .NET Framework 4.5.1	Microsoft Corporation	4.5.50938	Microsoft .NET Framework 4.5.1 Microsoft Corporation 4.5.50938	2

找到並移除 6 個重複值; 剩 114 個唯一的值。

確定

A	B	C	D	E	F
資產數量	資產名稱	資產廠商	資產版本	TEMP	資產數量
1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763	Microsoft Windows Server 2019 Datacenter 64 位元 Microsoft Corporati	1
1	Microsoft Windows Server 2008 R2 Datacenter Serv	Microsoft Corporation	6.1.7601	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit Mic	1
1	Apache Tomcat 8.0 Tomcat8 (remove only)		0.8.0.30	Apache Tomcat 8.0 Tomcat8 (remove only) 08.0.30	1
1	MySQL Workbench 6.3 CE	Oracle Corporation	6.3.7	MySQL Workbench 6.3 CE Oracle Corporation 6.3.7	1
1	VMware Tools	VMware, Inc.	10.0.5.3228253	VMware Tools VMware, Inc. 10.0.5.3228253	1
1	MySQL Connector/ODBC 5.3	Oracle Corporation	5.3.6	MySQL Connector/ODBC 5.3 Oracle Corporation 5.3.6	1
1	Microsoft Visual C++ 2010 x64 Redistributable - 10	Microsoft Corporation	10.0.40219	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219 Microsoft C	1
1	Java 8 Update 77 (64-bit)	Oracle Corporation	8.0.770.3	Java 8 Update 77 (64-bit) Oracle Corporation 8.0.770.3	1
1	MySQL Server 5.7	Oracle Corporation	5.7.14	MySQL Server 5.7 Oracle Corporation 5.7.14	1
1	Microsoft Visual C++ 2008 Redistributable - x64 9.0	Microsoft Corporation	9.0.30729.6161	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161 Micros	1
1	Java SE Development Kit 8 Update 77 (64-bit)	Oracle Corporation	8.0.770.3	Java SE Development Kit 8 Update 77 (64-bit) Oracle Corporation 8.0.77	1
2	Microsoft .NET Framework 4.5.1	Microsoft Corporation	4.5.50938	Microsoft .NET Framework 4.5.1 Microsoft Corporation 4.5.50938	1



實作練習1

資訊資產盤點

實作練習1：資訊資產盤點(環境說明)

- 環境說明
 - VM名稱：實作練習_Windows Server 2019
 - 帳號：TEST\Administrator
 - 密碼：1qaz@WSX3edc
- 指令範本
 - 位置：桌面\01.政府機關資安弱點通報機制\指令範本
 - 軟體盤點.bat
 - Java函式庫盤點.bat
- 文件範本
 - 位置：桌面\01.政府機關資安弱點通報機制\文件範本
 - 資訊資產清冊(空白).xlsx
 - Java函式庫彙整範本(空白).xlsx
- 盤點資料夾
 - 位置：桌面\01.政府機關資安弱點通報機制\盤點資料夾
 - 內含Windows Server 2008 R2盤點資料



Windows Server 2019

實作練習1：資訊資產盤點

- 於「實作練習_Windows Server 2019」VM執行資訊資產盤點作業
- 本項練習時間**20分鐘**

項次	執行項目	產出項目/執行結果
1	執行軟體盤點批次檔	作業系統資訊與軟體盤點清單
2	執行Java函式庫盤點批次檔	Java函式庫清單
3	盤點結果放入 盤點資料夾 後，彙整作業系統資訊、軟體盤點清單及Java函式庫清單至 資訊資產清冊	資訊資產清冊
4	於 資產數量統計 頁籤統計資訊資產數量	資訊資產清冊

資訊資產弱點管理作業流程



資訊資產正規化作業流程



資訊資產正規化作業流程



彙整資訊資產至上傳清單(1/2)

- STEP1：於VANS系統下載上傳清單

- 資訊資產管理>資通系統資產列表/使用者電腦資產列表
- 上傳清單包含機關資訊、常見資產格式及CPE格式



The screenshot shows the 'Information Asset Management > Asset System Asset List' page. On the left sidebar, 'Information Asset Management' is selected. Under it, 'Asset System Asset List' and 'User Computer Asset List' are highlighted with red boxes. In the center, there are several download buttons: 'Full Software Asset CPE List Download', 'Common Important Software Asset CPE List Download', 'Upload List Format Download' (which is also highlighted with a red box), and 'Asset List Upload'. Below these are buttons for 'Asset System Asset List Download', 'Asset Association Update CPE List Download', and 'Asset System Asset List Export (PDF)'. A large blue arrow points downwards from the 'Upload List Format Download' button towards the Excel file.



The screenshot shows an Excel spreadsheet titled 'Upload_Template.xls'. The top row contains headers: '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', and 'CPE完整名稱'. The first column (A) is labeled '機關資訊', the second column (B) is labeled '常見資產格式', and the third column (C) is labeled 'CPE格式'. A large blue arrow points downwards from the 'Upload List Format Download' button in the previous screenshot towards this Excel file.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	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					
2													
3													
4													
5													
6													

彙整資訊資產至上傳清單(2/2)

- STEP2：彙整資訊資產清冊至上傳清單

- 開啟**資訊資產清冊**「**資產數量統計**」頁籤
- 複製資產數量、資產名稱、資產廠商及資產版本等4個欄位(A~D)之值，貼至**上傳清單**常見資產格式(C~F)欄位

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	資產數量
2	1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763	Microsoft Windows Server 2019 Datacenter 64 位元 Microsoft Corporation
3	1	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1	Microsoft Corporation	6.1.7601	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bit Microsoft Corporation
4	1	Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	8.0.30	Apache Tomcat 8.0 Tomcat8 (remove only) N/A 8.0.30
5	1	MySQL Workbench 6.3 CE	Oracle Corporation	6.3.7	MySQL Workbench 6.3 CE Oracle Corporation 6.3.7
6	1	VMware Tools	VMware, Inc.	10.0.5.3228253	VMware Tools VMware, Inc. 10.0.5.3228253

上傳清單

↓ 複製並貼上「值」

C	D	E	F	G	H	I	J	K	L	M
1	資產數量	資產名稱	資產廠商	資產版本	CPE 2.3	CPE完整名稱				
2	1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763						
3	1	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1	Microsoft Corporation	6.1.7601						
4	1	Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	8.0.30						
5	1	MySQL Workbench 6.3 CE	Oracle Corporation	6.3.7						
6	1	VMware Tools	VMware, Inc.	10.0.5.3228253						

資訊資產正規化作業流程



進行CPE轉換(1/3)

- STEP1：下載並開啟完整軟體資產CPE清單或常見重要軟體資產CPE清單
 - 資訊資產管理 > 資通系統資產列表/使用者電腦資產列表



The screenshot shows the 'Information Asset Management' module. On the left sidebar, 'Information Asset Management' and 'Communication System Asset List' are highlighted with red boxes. In the main content area, there are several download buttons: 'Download Complete Software Asset CPE List' (highlighted with a red box), 'Download Common Important Software Asset CPE List', 'Upload List Format Download', and 'Asset List Upload'. Below these are buttons for 'Download Communication System Asset List', 'Download Asset Association Update CPE List', and 'Download Communication System Asset List (PDF)'. A large blue arrow points downwards from the highlighted 'Download Complete Software Asset CPE List' button towards the table below.

下載

A	B	C	D	E	F	G
	CPE Full Name	Vendor	Product	Version	Update	Version
1 CPE 2.3						
3078 cpe:2.3:o:microsoft:windows_server_2016:-*:****:*	Microsoft Windows Server 2016	microsoft	windows_s-	*	*	
3079 cpe:2.3:o:microsoft:windows_server_2016:1709:*****	Microsoft Windows Server 2016 1709	microsoft	windows_s1709	*	*	
3080 cpe:2.3:o:microsoft:windows_server_2016:1803:*****	Microsoft Windows Server 2016 1803	microsoft	windows_s1803	*	*	
3081 cpe:2.3:o:microsoft:windows_server_2016:1909:*****	Microsoft Windows Server 2016 1909	microsoft	windows_s1909	*	*	
3082 cpe:2.3:o:microsoft:windows_server_2019:-*:***:datacenter:*.x86:*	Microsoft Windows Server 2019 Datacenter Edition on x86	microsoft	windows_s-	*	*	
3083 cpe:2.3:o:microsoft:windows_server_2019:-*:***:standard:*.x64:*	Microsoft Windows Server 2019 Standard Edition on x64	microsoft	windows_s-	*	*	
3084 cpe:2.3:o:microsoft:windows_server_2019:-*:***:datacenter:*.x64:*	Microsoft Windows Server 2019 Datacenter Edition on x64	microsoft	windows_s-	*	*	
3085 cpe:2.3:o:microsoft:windows_server_2019:-*:*****	Microsoft Windows Server 2019	microsoft	windows_s-	*	*	
3086 cpe:2.3:o:microsoft:windows_server_2019:-*:***:standard:*.x86:*	Microsoft Windows Server 2019 Standard Edition on x86	microsoft	windows_s-	*	*	
3087 cpe:2.3:o:microsoft:windows_small_business_server_2011:***:essential:*.x64:*	Microsoft Windows Small Business Server 2011 Essentials Edition on x64	microsoft	windows_s	*	*	

進行CPE轉換(2/3)

- STEP2：針對上傳清單中的資訊資產，於軟體資產CPE清單進行搜尋

– 情境1：若已知該資訊資產對應之類別，可切換至相對應資訊資產類別頁籤，透過「篩選」關鍵字搜尋

– 情境2：若不確定該資訊資產之類別，可透過Excel「尋找及取代」功能，將搜尋範圍設定為活頁簿，對整份Excel的內容進行關鍵字搜尋

上傳清單

C	D	E	F	G	H	I	J	K	L	M
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
1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763							
2	1 Microsoft Windows Server 2008 R2 Datacenter Service Pack 1	Microsoft Corporation	6.1.7601							
3	1 Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	8.0.30							
4	1 MySQL Workbench 6.3 CE	Oracle Corporation	6.3.7							

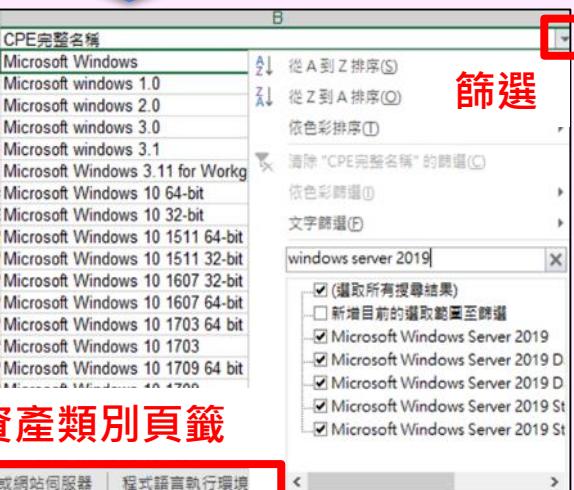
情境1

情境2

軟體資產CPE清單

資訊資產類別頁籤

篩選



1

2

3

全部尋找(B) 挑下一個(E) 關閉

尋找及取代

尋找(D) 取代(B)

尋找目標(N): windows server 2019

大小寫須相符(C) 儲存格內容須完全相符(D) 全半形須相符(B)

搜尋範圍(S): 活頁簿

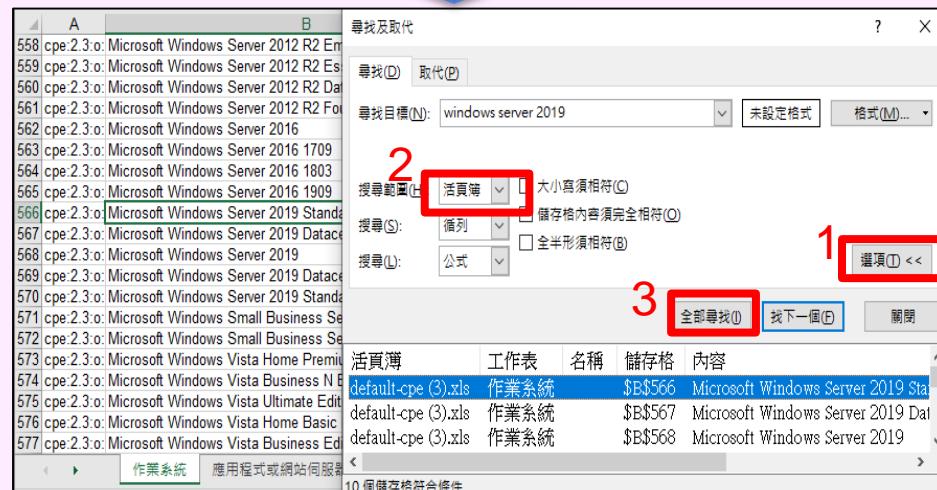
搜尋(S): 順列

搜尋(U): 公式

活頁簿 工作表 名稱 儲存格 內容

default-cpe (3).xls	作業系統	\$B\$566	Microsoft Windows Server 2019 Sta
default-cpe (3).xls	作業系統	\$B\$567	Microsoft Windows Server 2019 Da
default-cpe (3).xls	作業系統	\$B\$568	Microsoft Windows Server 2019

10 個儲存格符合條件



進行CPE轉換(3/3)

- STEP3：填寫上傳清單CPE格式欄位

- 於軟體資產CPE清單找到對應CPE格式後，複製CPE2.3與CPE完整名稱貼至上傳清單之G與H欄位
- 若於完整軟體資產CPE清單無找到相符CPE，則於CPE格式中，填入N/A
- 無相符CPE條目：包含無相符產品、無相同版本及自行開發軟體

軟體資產CPE清單

	A	B	C	D	E	F	G
1	CPE 2.3	CPE完整名稱	廠商	產品	版本	更新	版次
3082	cpe:2.3:o:microsoft:windows_server_2019:-***:datacenter:*:x86:*	Microsoft Windows Server 2019 Datacenter Edition on x86	microsoft	windows_s-	*	*	
3083	cpe:2.3:o:microsoft:windows_server_2019:-***:standard:*:x64:*	Microsoft Windows Server 2019 Standard Edition on x64	microsoft	windows_s-	*	*	
3084	cpe:2.3:o:microsoft:windows_server_2019:-***:datacenter:*:x64:*	Microsoft Windows Server 2019 Datacenter Edition on x64	microsoft	windows_s-	*	*	
3085	cpe:2.3:o:microsoft:windows_server_2019:-***:*	Microsoft Windows Server 2019	microsoft	windows_s-	*	*	
3086	cpe:2.3:o:microsoft:windows_server_2019:-***:standard:*:x86:*	Microsoft Windows Server 2019 Standard Edition on x86	microsoft	windows_s-	*	*	
3087	cpe:2.3:o:microsoft:windows_small_business_server_2011:-***:es	Microsoft Windows Small Business Server 2011 Essentials Edition on x64	microsoft	windows_s-	*	*	

上傳清單

↓ 複製貼上

D	E	F	G	H	I	J	K	L	M
1 資產名稱	資產廠商	資產版本	CPE 2.3	CPE完整名稱					
2 Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763	cpe:2.3:o:microsoft:windows_server_2019:-***:datacenter:x64:*	Microsoft Windows Server 2019 Datacenter Edition on x64					
3 Microsoft Windows Server 2008 R2 Datacenter Service Pack 1	Microsoft Corporation	6.1.7601	cpe:2.3:o:microsoft:windows_server_2008:-***:datacenter:sp1:x64:*	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 Edition on x64					
4 Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	8.0.30	cpe:2.3:a:apache:tomcat:8.0.30:*	Apache Tomcat 8.0 Tomcat8 (remove only)					
5 MySQL Workbench 6.3 CE	Oracle Corporation	6.3.7	N/A	N/A					

填上N/A

資訊資產正規化作業流程



完成上傳清單

- 填寫上傳清單之機關資訊(A與B)欄位

- 填寫欲上傳資產之機關OID與機關名稱
- 選取A、B欄位並雙擊右下角的方形，自動填滿機關OID與機關名稱

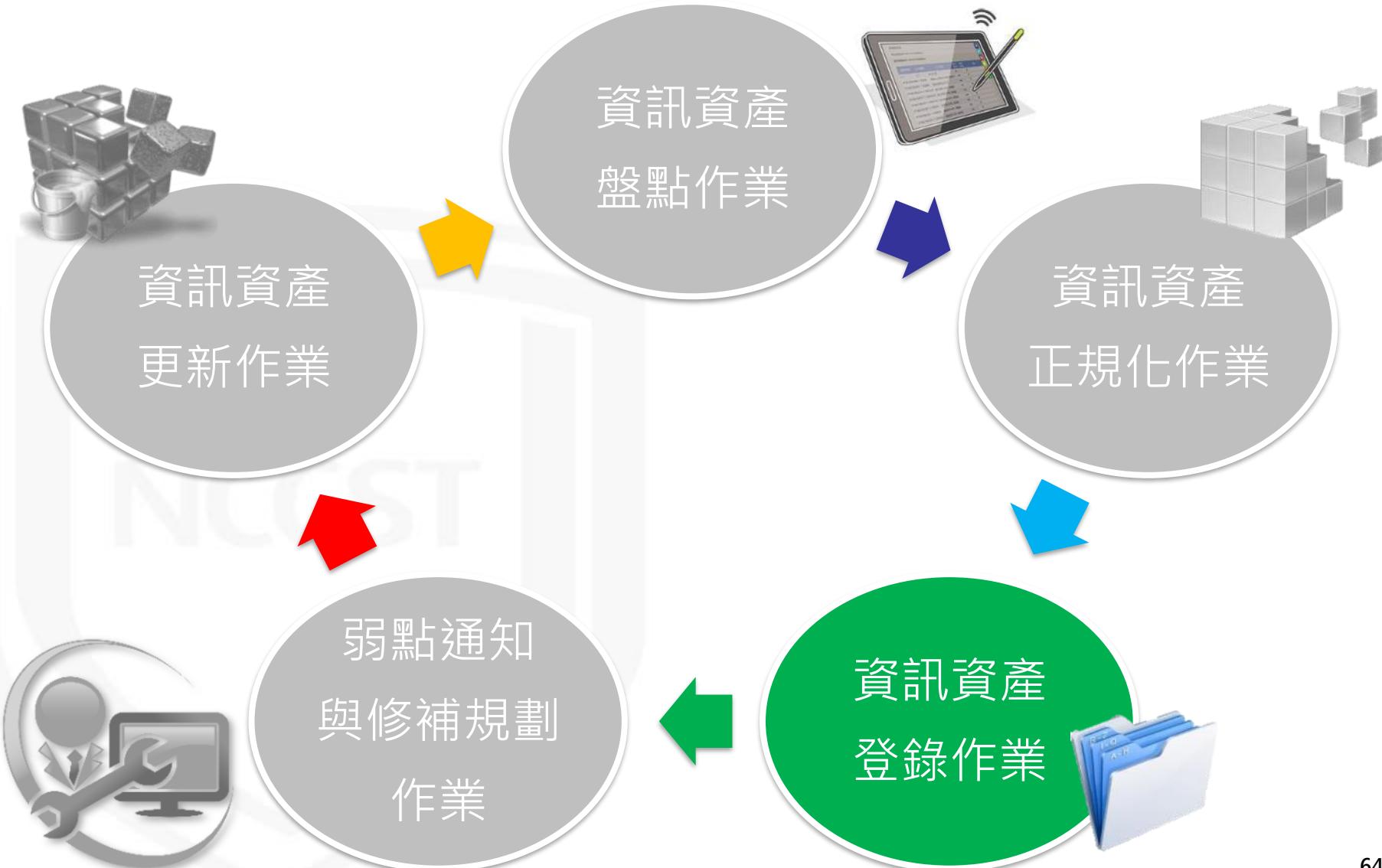
A	B	C	D	E	F	G
1 機關OID	機關名稱	資產數量	資產名稱	資產廠商	資產版本	CPE 2.3
2 NCCST	技服中心	1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763	cpe:2.3:o:micr
3		1	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1	Microsoft Corporation	6.1.7601	cpe:2.3:o:micr
4		1	Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	8.0.30	cpe:2.3:a:apac
5		1	MySQL Workbench 6.3 CE	Oracle Corporation	6.3.7	N/A
6		1	VMware Tools	VMware, Inc.	10.0.5.322825	N/A



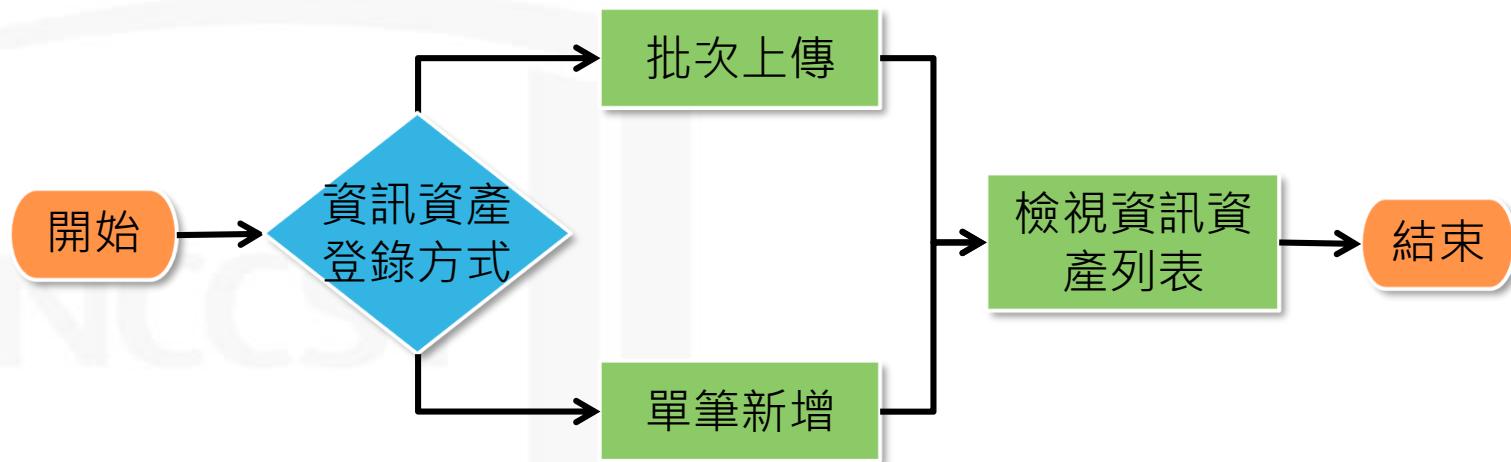
自動填滿

A	B	C	D	E	F	G
1 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
2 NCCST	技服中心	1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763	cpe:2.3:o:micr
3 NCCST	技服中心	1	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1	Microsoft Corporation	6.1.7601	cpe:2.3:o:micr
4 NCCST	技服中心	1	Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	8.0.30	cpe:2.3:a:apac
5 NCCST	技服中心	1	MySQL Workbench 6.3 CE	Oracle Corporation	6.3.7	N/A
6 NCCST	技服中心	1	VMware Tools	VMware, Inc.	10.0.5.322825	N/A

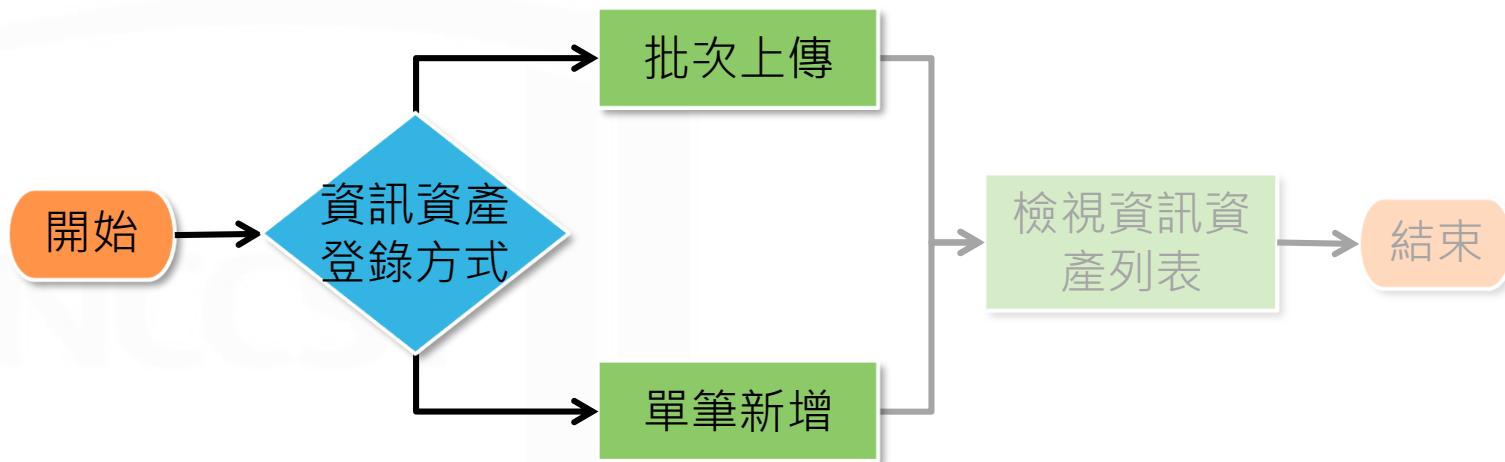
資訊資產弱點管理作業流程



資訊資產登錄作業流程



資訊資產登錄作業流程



批次上傳

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



單筆新增(1/2)

- STEP1：於VANS系統進行新增資產
 - 資訊資產管理>資通系統資產列表/使用者電腦資產列表
- STEP2：點選新增資產，開啟新增資產彈出式視窗



The screenshot shows the 'Information Asset Management > Asset List' page. On the left, there is a sidebar with the following menu items:

- 機關概況
- 資訊資產管理
- 資通系統資產列表 (highlighted with a red box)
- 使用者電腦資產列表
- 資產風險狀態
- 資訊查詢
- 設定管理

The main content area has the following sections:

- 常見重要資產CPE清單，供機關快速選取資訊系統之重要軟體資產
- 操作按钮：完整軟體資產CPE清單下載、常見重要軟體資產CPE清單下載、上傳清單格式下載、資產清單上傳
- 子菜单：資通系統資產清單下載、資產關聯更新CPE清單下載、資通系統資產清單匯出(PDF)
- 搜索框：以廠商名稱搜尋 (廠商:)、以產品名稱搜尋 (產品: ex.tomcat)、無CPE資訊的資產 (資產廠商: ex.microsoft)
- 筛选框：版本: , 更新: , 版次: , 資產數量: ex.2
- 操作按钮：新增資產 (highlighted with a red box and a blue arrow pointing to the right panel)
- 右侧弹窗：新增資產 (highlighted with a red box)
- 右侧弹窗操作按钮：取消

單筆新增(2/2)

- STEP3：填寫相關欄位後點選「新增資產」即可完成新增
 - 可透過輸入廠商名稱或產品名稱搜尋資產
 - 透過下拉選單搜尋對應之產品、廠商、版本、更新及版次，填寫完即可新增CPE格式資產
 - 搜尋不到時，則於右方無CPE資訊之欄位進行資產新增

新增資產

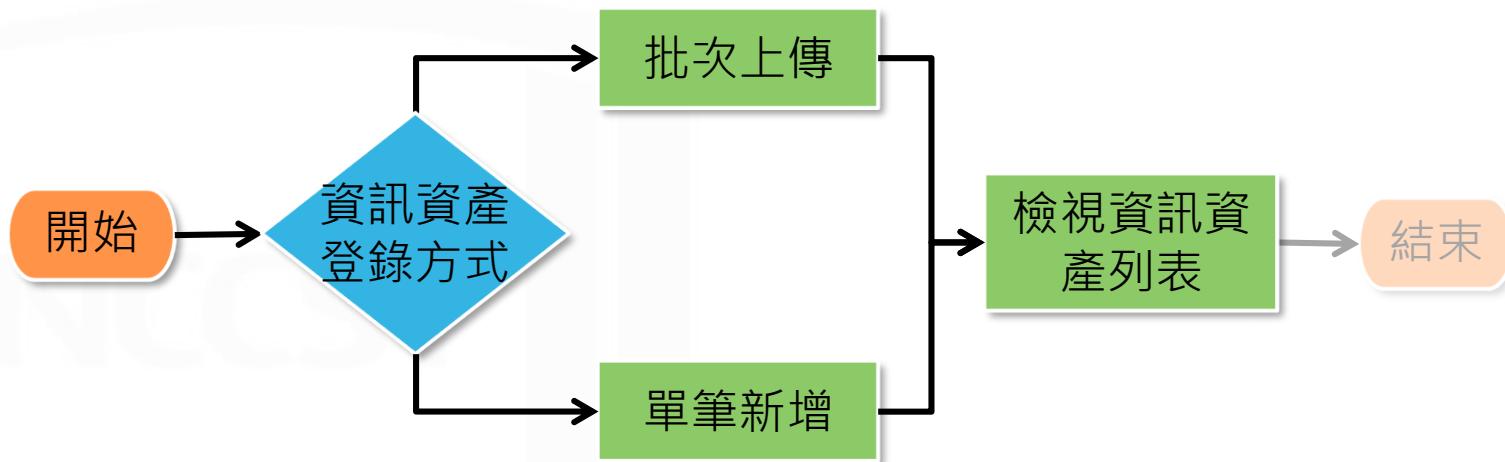
新增CPE格式資產

新增無CPE格式資產

取消

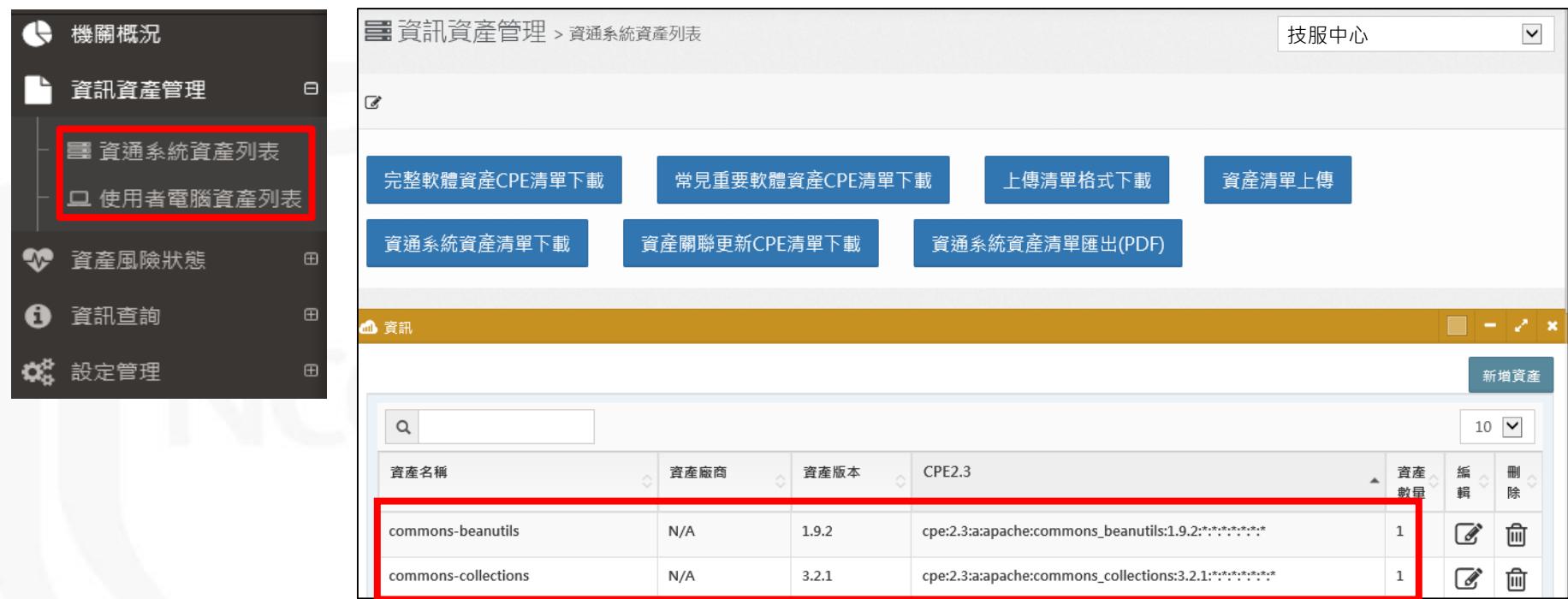
以廠商名稱搜尋 廠商: <input type="text" value="microsoft"/> 產品: <input type="text" value="windows_server"/> <ul style="list-style-type: none">.net_windows_serverwindows_server_2003windows_server_2008windows_server_2012windows_server_2016windows_server_2019 ex.2 <input type="button" value="新增資產"/>	以產品名稱搜尋 產品: <input type="text" value="ex.tomcat"/> 廠商: <input type="text"/> 版本: <input type="text"/> 更新: <input type="text"/> 版次: <input type="text"/> 資產數量: <input type="text" value="ex.2"/> <input type="button" value="新增資產"/>	無CPE資訊的資產 資產廠商: <input type="text" value="ex.microsoft"/> 資產名稱: <input type="text" value="ex.sqlserver"/> 資產版本: <input type="text" value="ex.2008"/> 更新: <input type="text" value="ex.*"/> 版次: <input type="text" value="ex.*"/> 資產數量: <input type="text" value="ex.2"/> <input type="button" value="新增資產"/>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

資訊資產登錄作業流程



檢視資訊資產列表

- 可於資訊資產管理功能查看已登錄至VANS系統之資產項目
 - 資訊資產管理>資通系統資產列表/使用者電腦資產列表



機關概況

資訊資產管理

資訊資產管理 > 資通系統資產列表

技服中心

完整軟體資產CPE清單下載

常見重要軟體資產CPE清單下載

上傳清單格式下載

資產清單上傳

資產風險狀態

資訊查詢

設定管理

新增資產

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	編輯	刪除
commons-beanutils	N/A	1.9.2	cpe:2.3:a:apache:commons_beansutils:1.9.2:*,*,*,*,*	1		
commons-collections	N/A	3.2.1	cpe:2.3:a:apache:commons_collections:3.2.1:*,*,*,*,*	1		



實作練習2

資訊資產正規化與登錄

實作練習2：資訊資產正規化與登錄(環境說明)

● VANS系統_實工作站

– 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



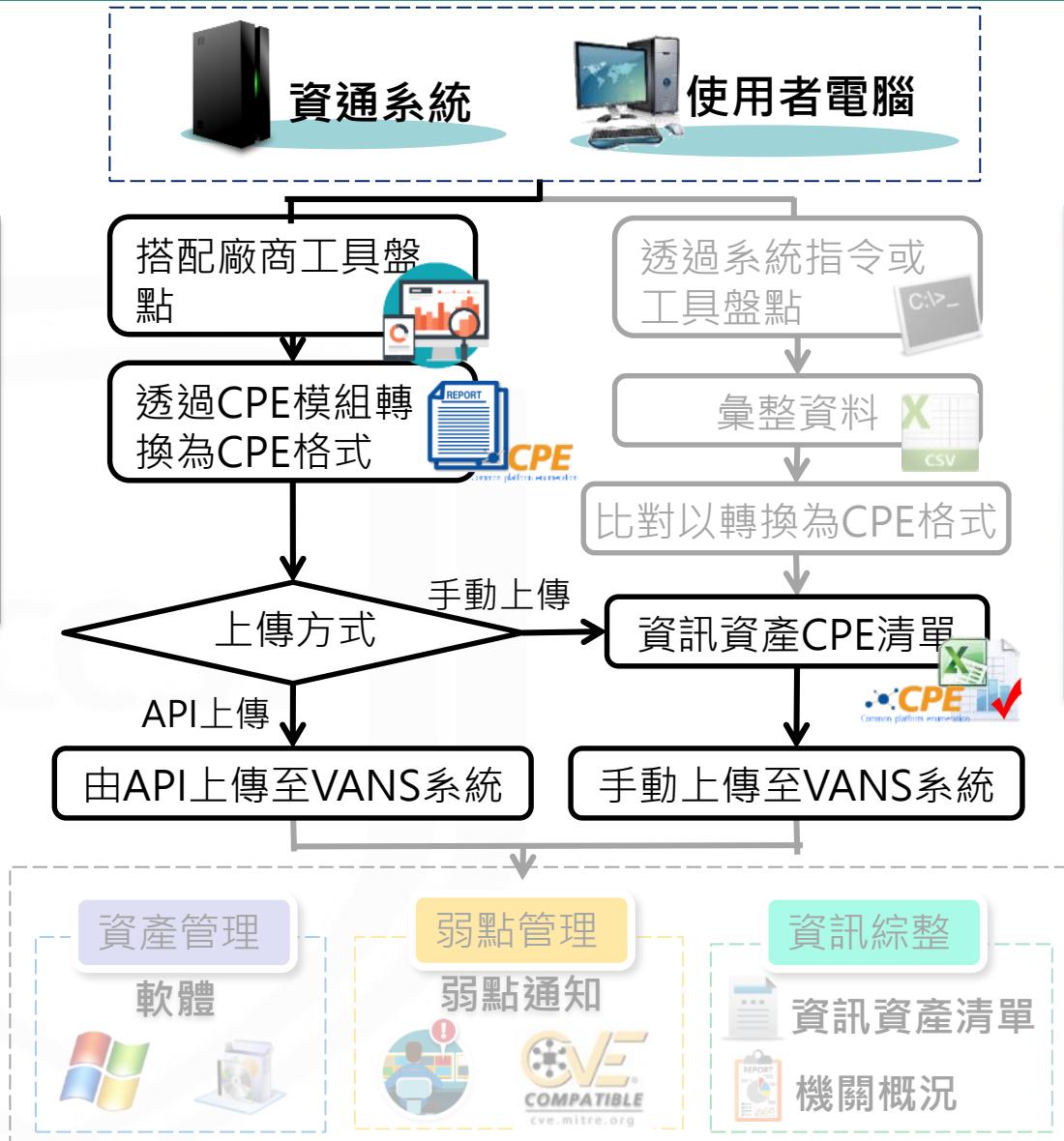


實作練習2：資訊資產正規化與登錄

- 請將「實作練習1」建立之資訊資產清冊執行正規化與登錄作業，並於VANS系統上新增1筆資產
- 本項練習時間**30分鐘**

項次	執行項目	產出項目/執行結果
1	登入VANS系統下載 完整資產CPE清單 與 上傳清單	下載 完整資產CPE清單 與 上傳清單
2	彙整資訊資產清冊至 上傳清單	
3	<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	上傳清單
4	將其餘CPE格式欄位填上 N/A	
5	登錄上傳清單至VANS系統	於資產列表檢視登錄資產
6	於VANS系統之資產列表頁面上 新增資產 <ul style="list-style-type: none">WinRAR 5.50版	於資產列表檢視新增之資產

資訊資產弱點管理流程



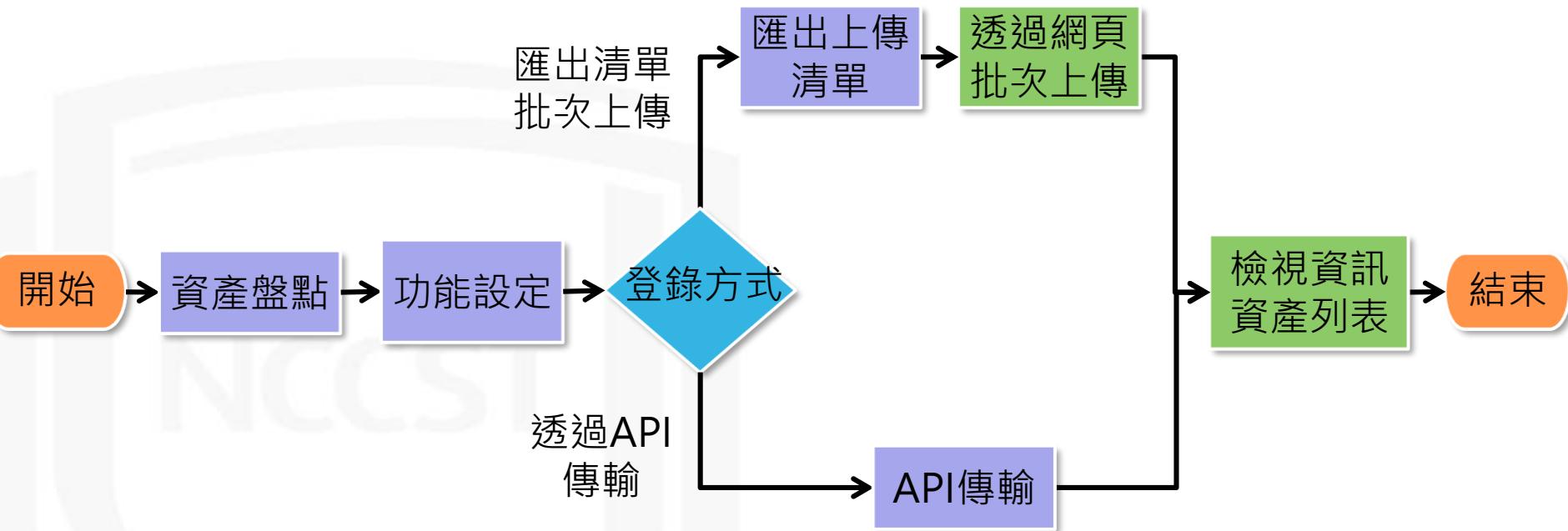
透過AD派送批次檔方式盤點軟體資產資訊，再以PowerQuery擴充套件彙整



資訊資產弱點管理作業流程



廠商工具作業流程

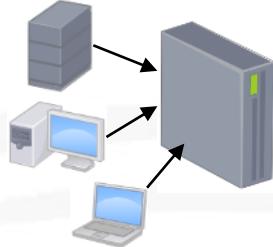


於廠商工具執行

於VANS系統執行

範例-合作廠商A作業流程

透過Console蒐集Agent
回傳之資訊資產



設定機關OID與機關名稱
等資訊

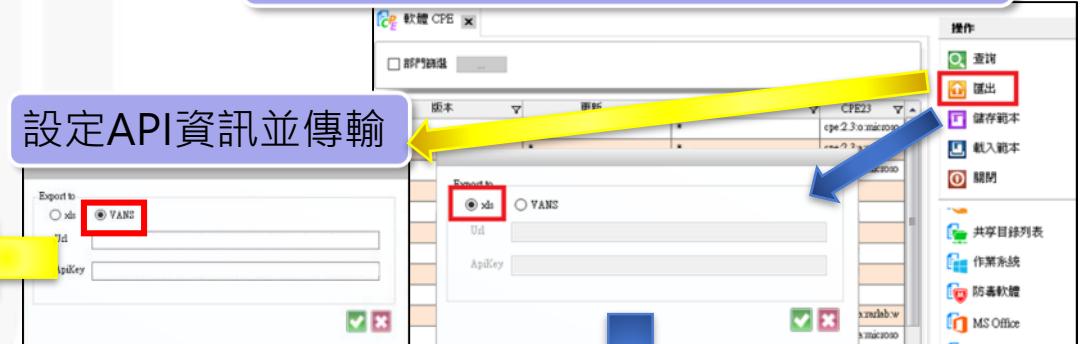


選擇匯出CPE清單或透過API傳輸

完成登錄



設定API資訊並傳輸



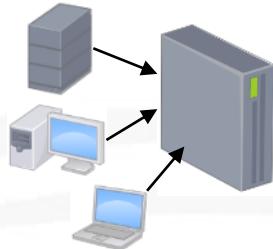
匯出CPE清單

於VANS系統上傳CPE清單

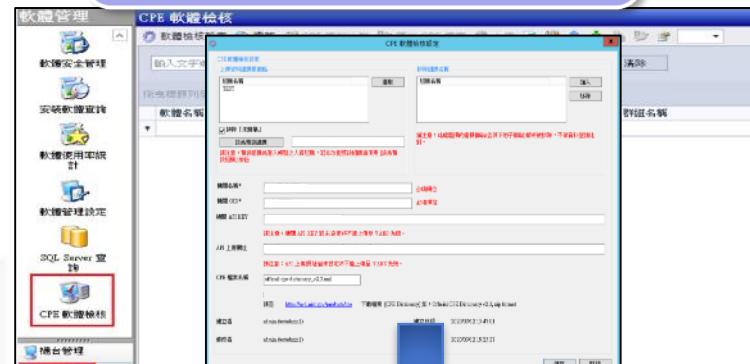


範例-合作廠商B作業流程

透過Console蒐集Agent
回傳之資訊資產



填入機關OID、機關名稱
及API Key等設定



完成登錄

API傳輸

選擇匯出清單或透過API傳輸

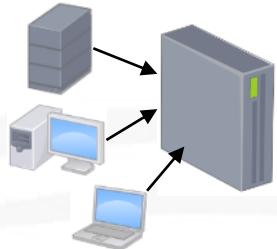


匯出CPE清單
於VANS系統上傳CPE清單



範例-合作廠商C作業流程

透過Console蒐集Agent
回傳之資訊資產



設定機關OID與機關名稱等資訊

資料名稱	機位名稱	對應機位	預設值
asset_manager	oid	--選擇--	N/A
	unit_name	--選擇--	N/A
	asset_number	CPE 完整名稱	N/A
	product_name	CPE 產品	N/A



挑選傳輸API方式

完成登錄

選擇匯出清單或透過API傳輸

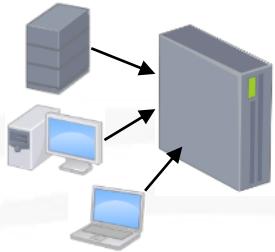
動作	名稱	報表範本類型	報表範本名稱	建立者全名
	CPE電路比對結果	Report	CPE電路比對結果	[REDACTED]
	編輯	Report	CPE電路比對結果	[REDACTED]
	刪除	Report	CPE電路比對結果	[REDACTED]
	匯出報表	Report	Default_資產管理 - C...	[REDACTED]
	傳送至 Api 伺服器	Report	CPE 與軟體	[REDACTED]

匯出CPE清單

於VANS系統上傳CPE清單

範例-合作廠商D作業流程

透過Console蒐集Agent
回傳之資訊資產



選擇匯出CPE清單或透過API傳輸

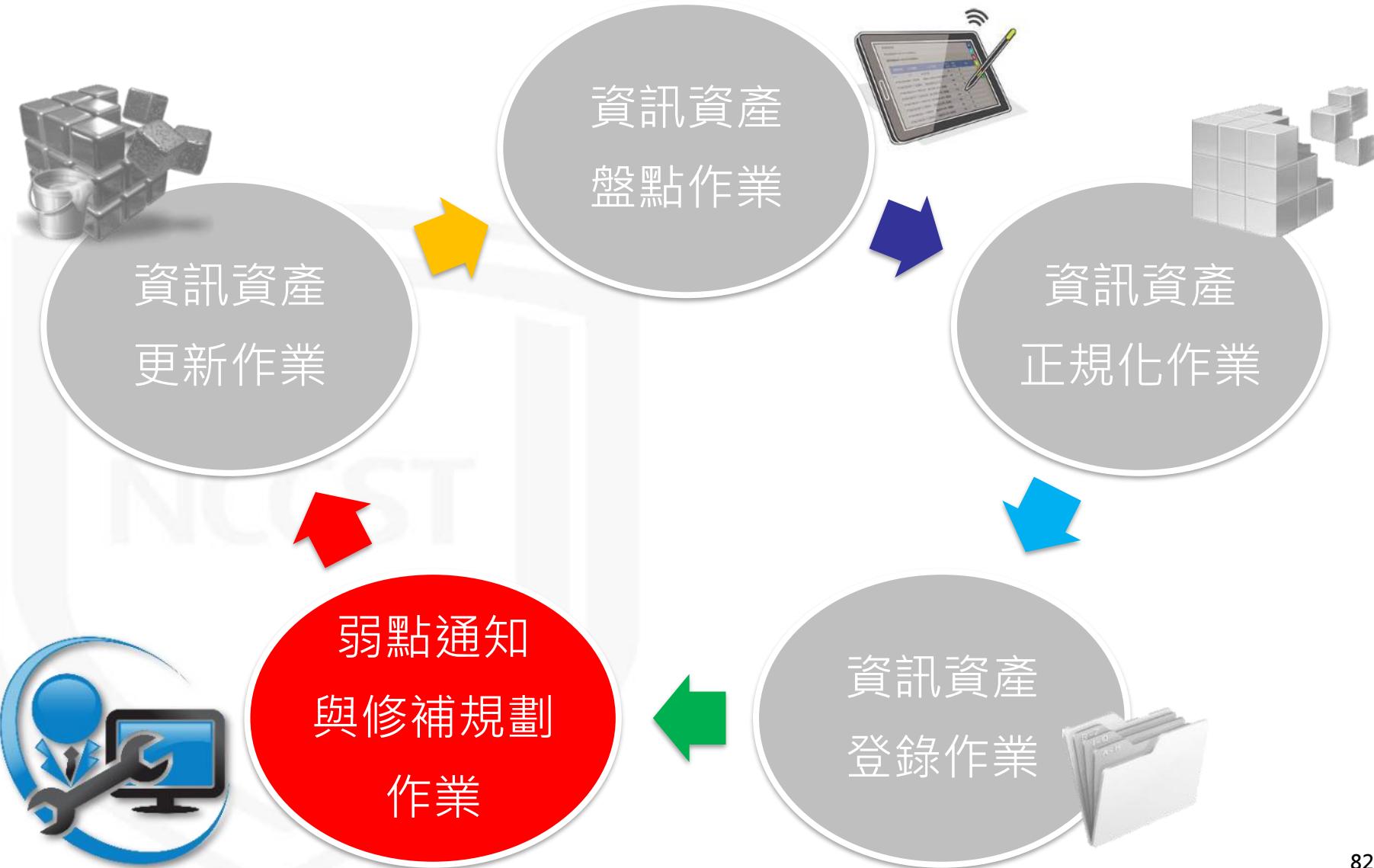
匯出CPE清單

完成登錄

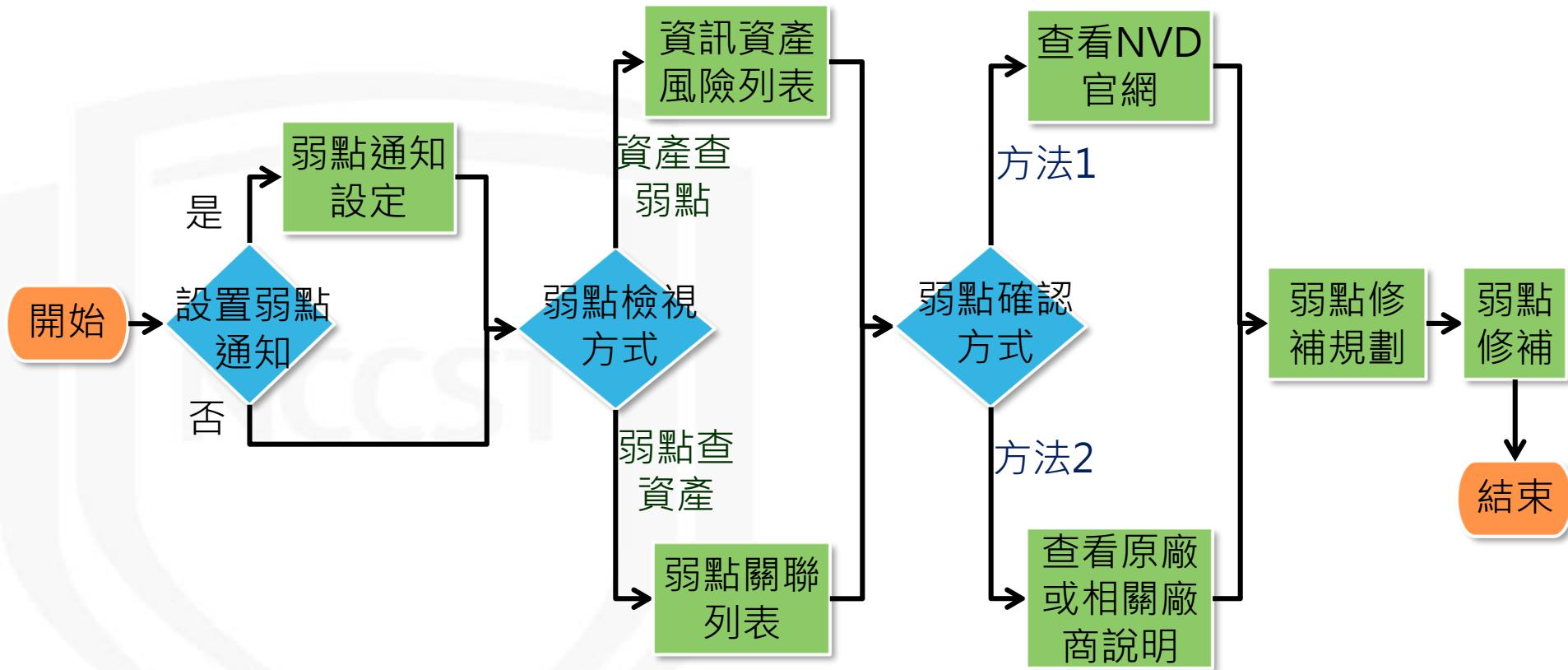
於VANS系統上傳CPE清單

API資訊設定

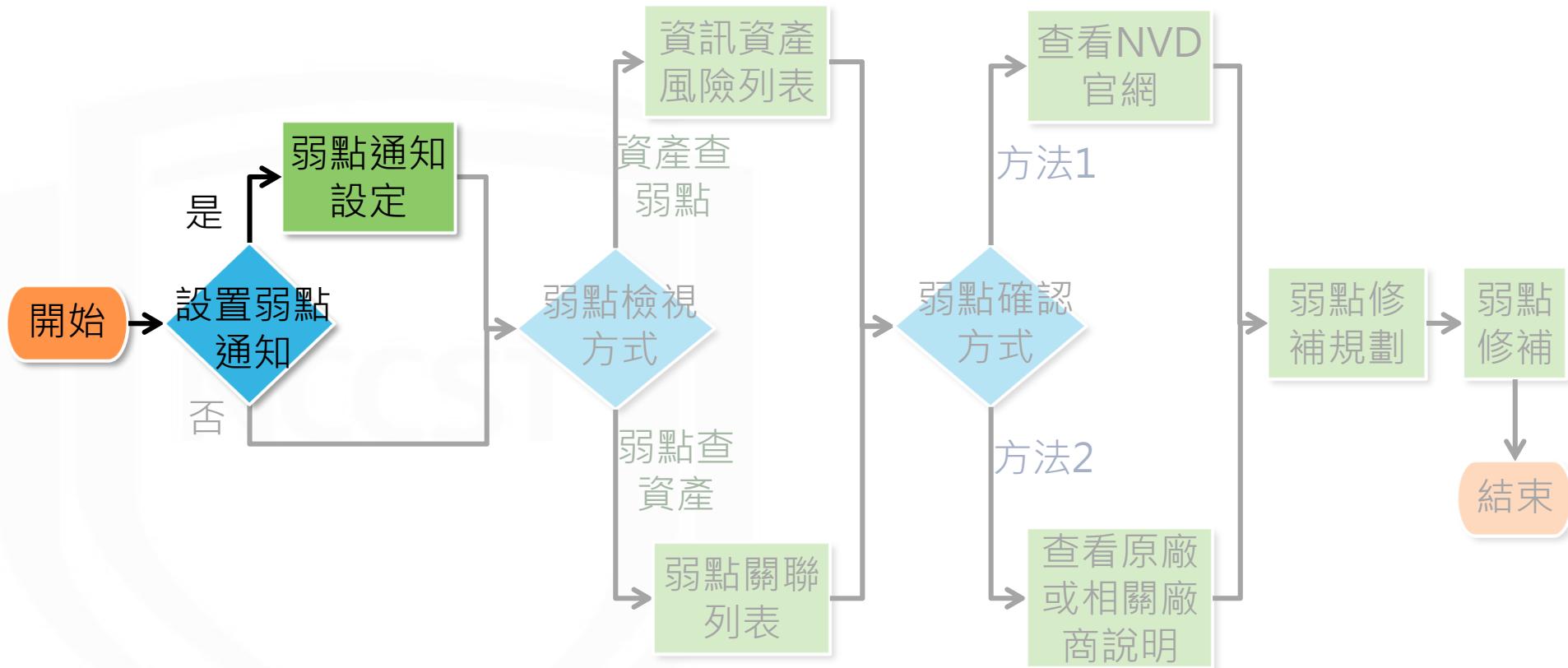
資訊資產弱點管理作業流程



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機制

student2

設定 > 弱點通知設定

弱點通知設定

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。

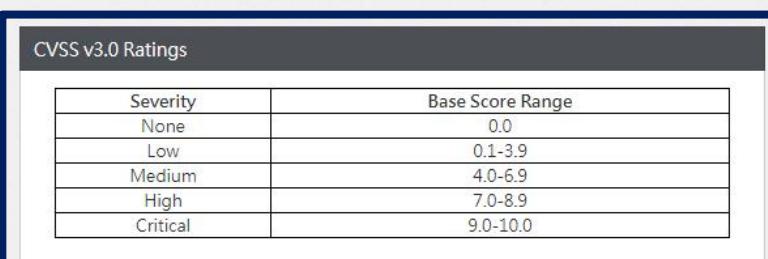
OFF **通知開關**

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)

0.0 - 10 **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。

email@address.com **設定接收通知Email**

 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



The screenshot shows the 'Setting Management > Notification Settings' page. On the left, a sidebar lists various management functions, with 'Notification Settings' highlighted by a red box. The main area contains two configuration sections:

- Weak Point Notification Score Setting:** A text input field displays '4.0'. Below it is a red box containing the text 'Adjust the CVSS score threshold setting'.
- Weak Point Notification Email Setting:** An email input field contains 'test@nccst.nat.gov.tw'. Below it is a red box containing the text 'Set up receiving notification Email'.

To the right, there is a reference table for 'CVSS v3.0 Ratings' and a note about using the ISMS weak point repair baseline to set the CVSS score threshold. At the bottom, there is a section for enabling notifications with a red box around the 'ON' switch.

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

CVSS v3.0 Ratings

可參考ISMS弱點修復基準
設置CVSS分數門檻

通知設定

請選擇是否接收弱點通知

ON

通知開關

設定

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系統若比對出高於CVSS分數門檻之弱點，則發送通知
 - 發送通知信予接收通知Email
 - 於VANS系統上顯示弱點比對通知
- 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

【VANS】資訊資產風險項目通知

收件者
郵件名 vans@nccst.nat.gov.tw

尊敬者 您好：

此為「政府機關資安弱點通報機制」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，以避免資產修補作業完成後，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，請聯絡客服中心陳耕硯先生，謝謝。

聯絡電話：(02)6631-6458



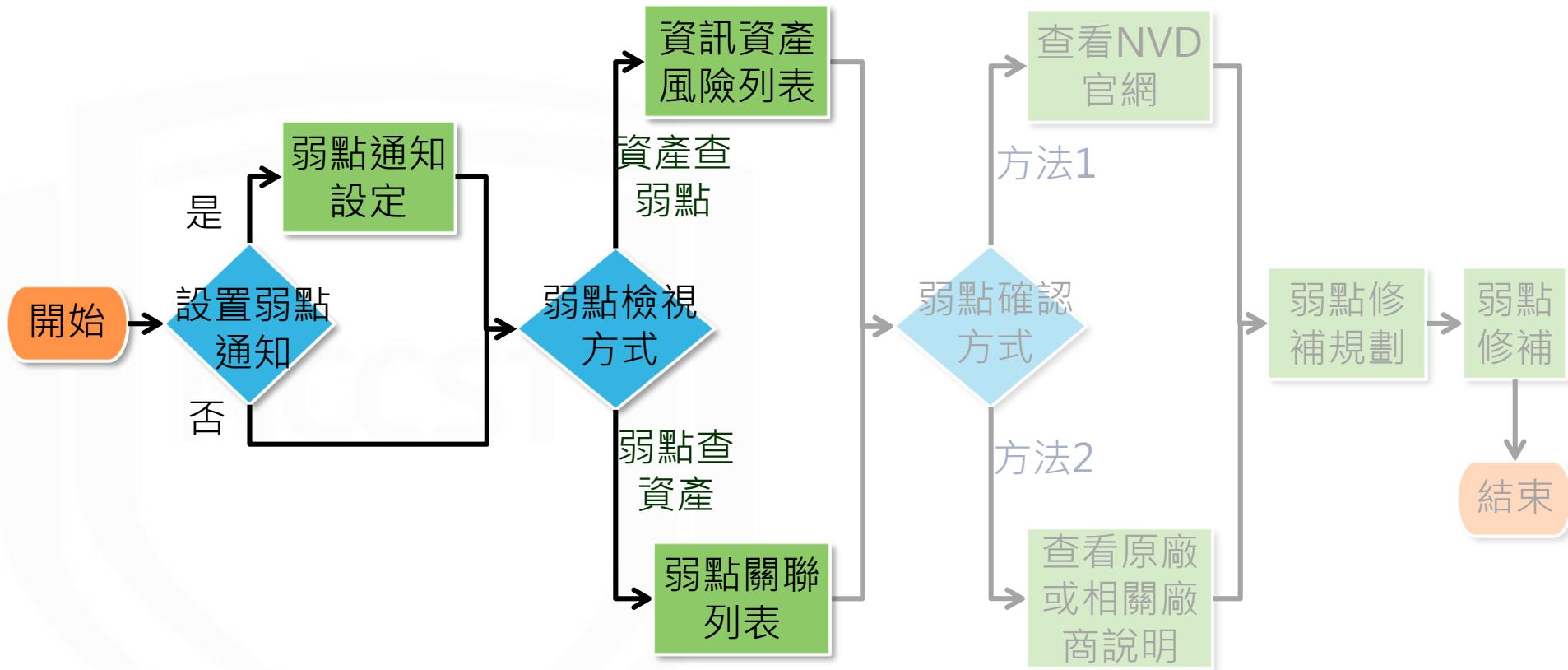
資產風險狀態 > 資通系統資產風險狀態> 弱點比對通知

弱點通知列表

通知時間	資產數量	弱點數量	詳細資訊	通知顯示	匯出勾選擬弱點通知
2019-11-17 00:37:17	1	171	<input type="button" value="開啟"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2019-11-08 16:39:21	28	456	<input type="button" value="開啟"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Showing 1 to 2 of 2 entries

弱點通知與修補規劃作業流程



弱點檢視方式-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

機關概況

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** (Selected)
- 弱點關聯列表**
- 弱點比對通知**
- 弱點處理情形回報**
- 安全性更新檢視**

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
上傳弱點清單
技服中心

資產名稱	資產廠商	資產版本	CPE2.3	風險指數	弱點數量	處理情形	弱點資訊
Apache Tomcat 9.0 Tomcat9 (remove only)	The Apache Software Foundation	9.0.16	cpe:2.3:a:apache:tomcat:9.0.16:*****	5.96	9	0/9	詳細資訊
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beansutils:1.8.0:*****	7.50	2	0/2	詳細資訊

詳細資訊

CVE編號	CVSS	發布時間	更新時間	改善措施	填寫勾選擬改善措施	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"/>	<input checked="" type="checkbox"/>
CVE-2014-0432	9.3	2014-04-16 08:55:00	2018-01-05 10:29:00	填寫改善措施	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CVE-2014-0446	7.5	2014-04-16 08:55:00	2018-01-05 10:29:00	填寫改善措施	<input type="checkbox"/>	<input checked="" type="checkbox"/>

弱點檢視方式-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

機關概況

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 (Red Box)

弱點比對通知

弱點處理情形回報

安全性更新檢視

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 > 弱點關聯列表

技服中心

請輸入CVE編號

起始時間 2020-04-08 結束時間 2020-05-08

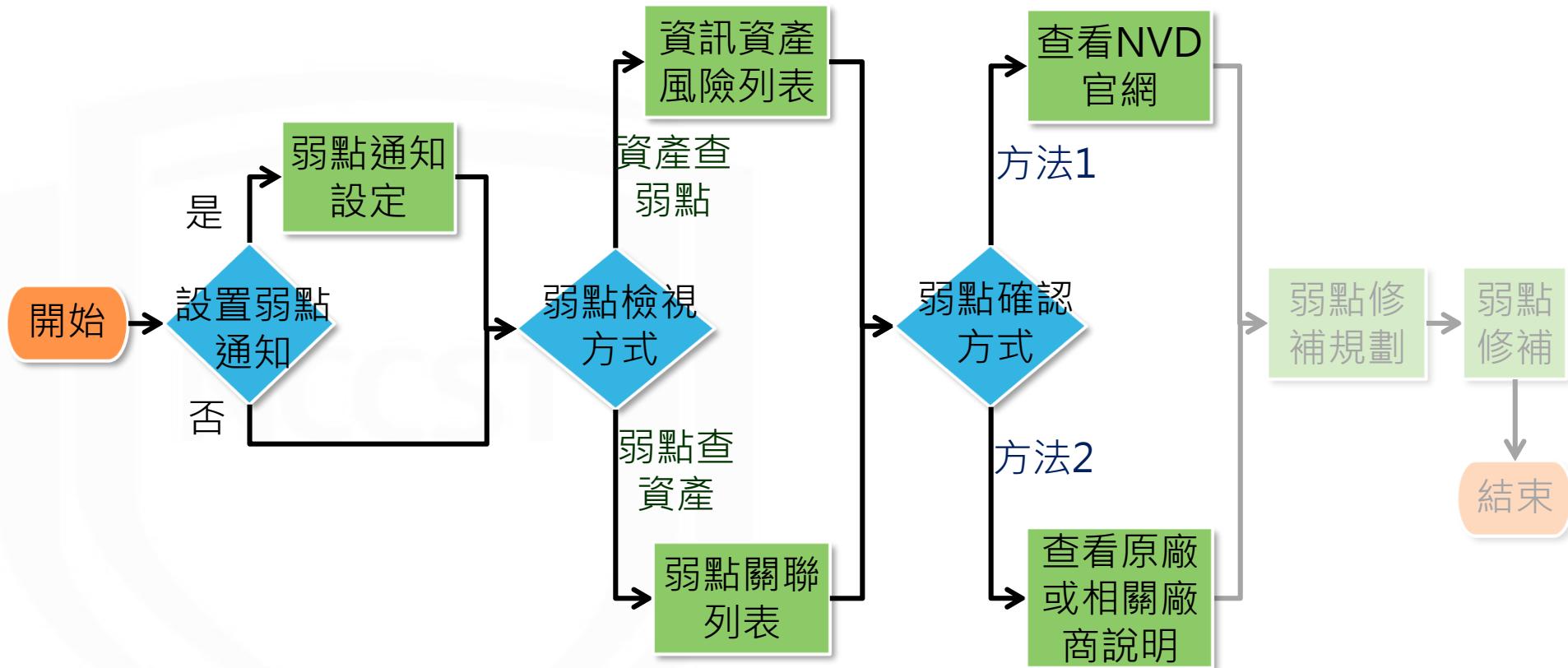
查詢

資訊

CVE-2020-7067		CVSS Score: 5	發布時間: 2020-04-28 05:15:00	更新時間: 2020-05-06 12:05:00
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
common_php	common_php	common_7.2.0	cpe:2.3:a:php:php:7.2.0:rc6:*****	2020-05-06 08:28:11

CVE-2020-1745		CVSS Score: 5	發布時間: 2020-04-28 11:15:00	更新時間: 2020-05-06 04:05:00
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
common_tomcat	common_apache	common_8.5.0	cpe:2.3:a:apache:tomcat:8.5.0:*****	2020-05-07 05:28:13
Apache Tomcat 9.0 Tomcat9 (remove only)	The Apache Software Foundation	9.0.16	cpe:2.3:a:apache:tomcat:9.0.16:*****	2020-05-08 07:28:34

弱點通知與修補規劃作業流程



弱點確認方式(1/4)

- 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 技服中心

下載弱點清單 上傳弱點清單

資訊

資產名稱	資產廠商	資產版本	CPE2.3	風險指數	弱點數量	處理情形	弱點資訊
Apache Tomcat 9.0 Tomcat9 (remove only)	The Apache Software Foundation	9.0.16	cpe:2.3:a:apache:tomcat:9.0.16:*****	5.96	9	0/9	詳細資訊
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beansutils:1.8.0:*****	7.50	2	0/2	詳細資訊
commons-fileupload	N/A	1.3.2	cpe:2.3:a:apache:commons_fileupload:1.3.2:*****	7.50	1	0/1	詳細資訊
Java 8 Update 202 (64-bit)	Oracle Corporation	8.0.2020.8	cpe:2.3:a:oracle:jre:1.8.0:update_202:*****	7.07	37	0/37	詳細資訊

弱點確認方式(2/4)

- 點選弱點編號，可查看弱點描述與相關連結

詳細資訊

詳
細
資
訊

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

CVE資訊

查看弱點描述

NVD官網弱點說明連結

https://nvd.nist.gov/vuln/detail/CVE-2014-0429

CVSS Score: 10

Access Vector

AccessComplexity: LOW

AccessVector: NETWORK

Authentication: NONE

關閉

93

弱點確認方式(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	

弱點確認方式(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

Ask "Does Oracle have chatbots?"

View Accounts Try Oracle Cloud Free Tier

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.

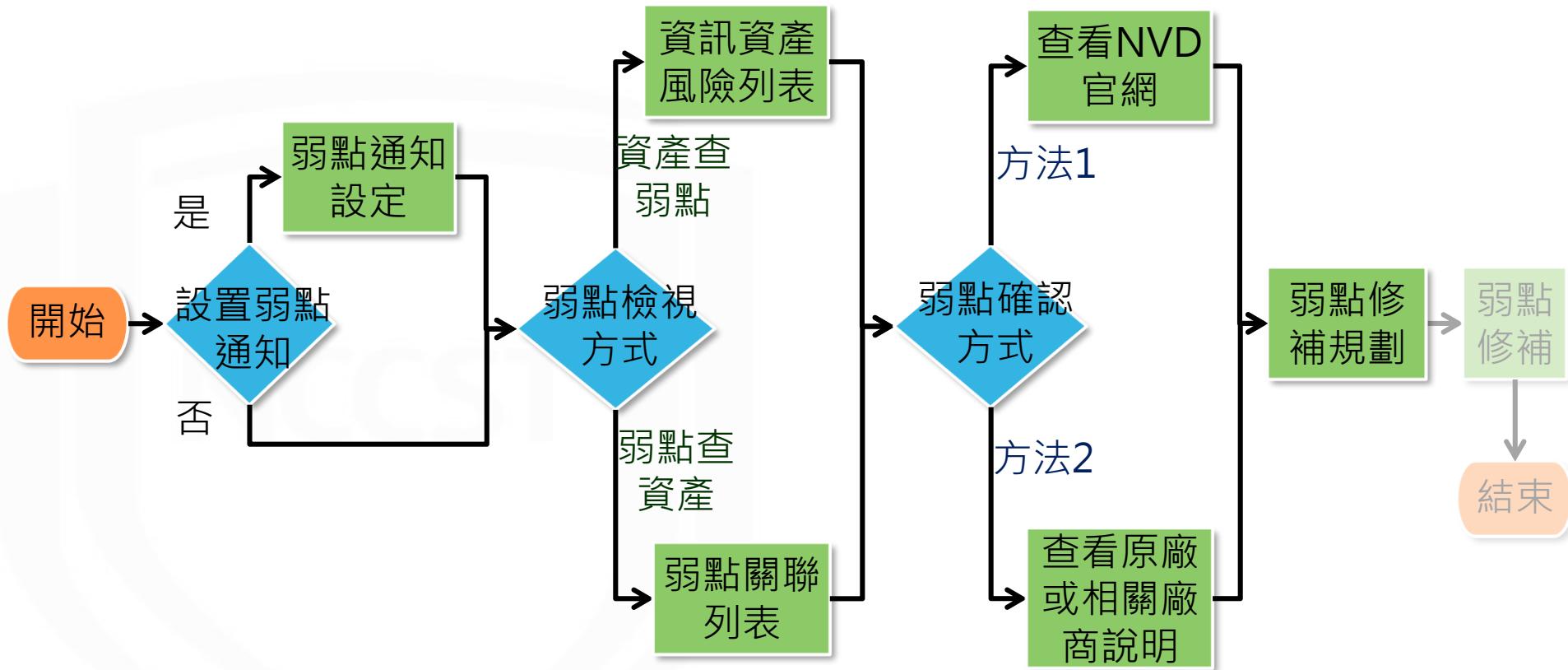
Skipped Critical Patch Updates

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

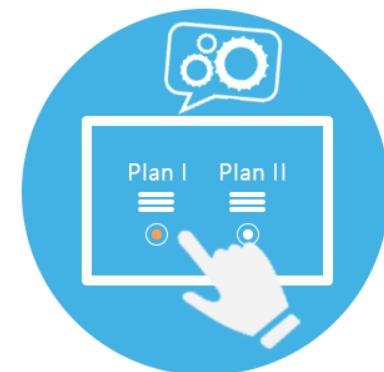
Oracle products may have dependencies on other Oracle products. Hence security vulnerability fixes announced in this Critical Patch Update may affect one or more dependent Oracle products. For details regarding these dependencies and how to apply patches to dependent products, please refer to [Patch Set Update and Critical Patch Update April 2014 Availability Document](#), [My Oracle Support Note 16182131](#).

弱點通知與修補規劃作業流程



弱點修補規劃(1/6)

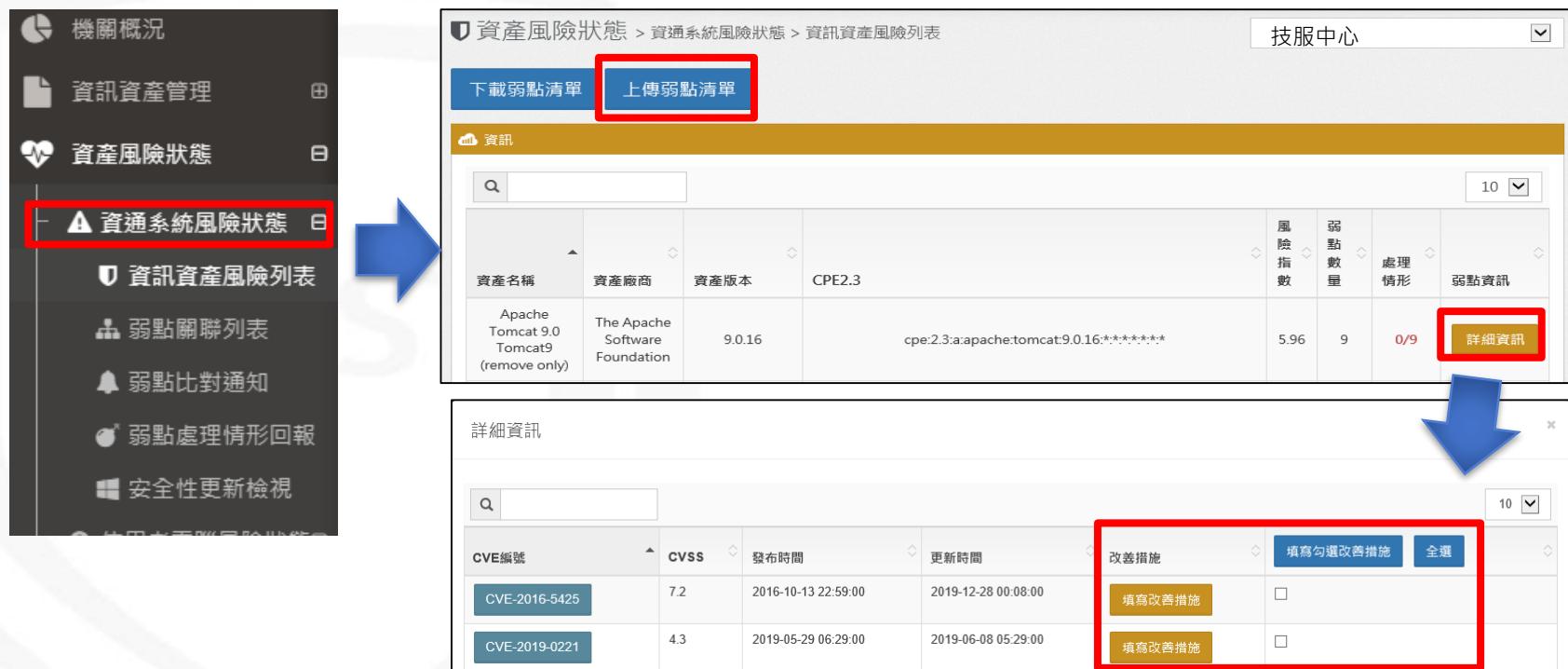
- 依據機關ISMS政策訂定弱點修復基準與修復時程，若無法立即修補或須接受風險之弱點，可針對該風險填寫改善措施
- 針對達到弱點修復基準之弱點進行修補規劃
 - 確認是否可透過更新方式修補弱點？
 - 是否有其他替代修補措施？
 - 預計修補時程



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 figure illustrates the workflow for managing asset vulnerabilities. It starts with a screenshot of the main navigation bar on the left, which includes links for Agency Overview, Asset Management, Asset Risk Status, and several sub-links under Asset Risk Status (including System Risk Status, Asset Risk List, Vulnerability Association List, Vulnerability Comparison Alert, Vulnerability Handling Report, and Security Update Review). A red box highlights the '資通系統風險狀態' link. A blue arrow points from this link to a larger screenshot on the right.

The right-hand screenshot shows the '資產風險狀態 > 資通系統風險狀態 > 資訊資產風險列表' page. At the top, there are two buttons: '下載弱點清單' (Download Vulnerability List) and '上傳弱點清單' (Upload Vulnerability List), with the latter being highlighted by a red box. Below this is a search bar and a table with the following columns: 資產名稱 (Asset Name), 資產廠商 (Asset Vendor), 資產版本 (Asset Version), CPE2.3, 風險指數 (Risk Score), 弱點數量 (Number of Vulnerabilities), 處理情形 (Handling Status), and 弱點資訊 (Vulnerability Information). A specific row for 'Apache Tomcat 9.0 Tomcat9 (remove only)' is shown with a risk score of 5.96, 9 vulnerabilities, and a handling status of '0/9'. A red box highlights the '詳細資訊' (Detailed Information) button in the bottom right corner of this row.

A large blue arrow points down to a third screenshot at the bottom, titled '詳細資訊' (Detailed Information). This screenshot shows a table with columns: CVE編號 (CVE Number), CVSS, 發布時間 (Release Time), 更新時間 (Update Time), 改善措施 (Improvement Measures), 填寫勾選擬改善措施 (Checklist for Filling in Improvement Measures), and 全選 (Select All). Two rows are listed: one for CVE-2016-5425 (CVSS 7.2) and another for CVE-2019-0221 (CVSS 4.3). Each row has a '填寫改善措施' (Fill in Improvement Measures) button and a checkbox. A red box highlights the '填寫改善措施' button in the first row.

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

CVE編號	CVSS	發布時間	更新時間	改善措施	填寫勾選擬改善措施	全選
CVE-2005-4838	4.3	2005-12-31 13:00:00	2019-03-25 19:29:00	填寫改善措施	<input type="checkbox"/>	
CVE-2006-7196	4.3			填寫改善措施	<input type="checkbox"/>	

填寫改善措施

請勿使用 >、<、&、" 或 ' 字元填寫改善措施

送出



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**填寫勾選擬改善措施**，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

CVE編號	CVSS	發佈時間	更新時間	改善措施	
CVE-2005-4838	4.			<input checked="" type="checkbox"/> 填寫改善措施	<input type="checkbox"/>
CVE-2006-7196	4.			<input checked="" type="checkbox"/> 填寫改善措施	<input type="checkbox"/>
CVE-2007-2449	4.			<input checked="" type="checkbox"/> 填寫改善措施	<input type="checkbox"/>
CVE-2008-0128	5			<input checked="" type="checkbox"/> 填寫改善措施	<input type="checkbox"/>

請勿使用 >、<、 &、 "或'等特殊字元填寫改善措施

送出

填寫勾選擬改善措施

10



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

技服中心

	B	C	D	E	F	G	H	I	J	K
1	資產廠商	資產版本	CPE2.0	資產數量	CVE編號	CVS	發布時間	更新時間	弱點說明	NVD弱點說明連結
2	Microsoft Co	4.5.50938	cpe:2.3:an 1		CVE-2014-10.0	2014/10/15 18	2018/10/13 06	Microsoft .NET	https://web.nvd.nist.gov	
3	Microsoft Co	4.5.50938	cpe:2.3:an 1		CVE-2014-10.0	2014/10/15 18	2018/10/13 06	Microsoft .NET	https://web.nvd.nist.gov	
4	Microsoft Co	4.5.50938	cpe:2.3:an 1		CVE-2014-10.0	2014/05/14 19	2018/10/13 06	The .NET Re	https://web.nvd.nist.gov	

改善措施

檢視WSUS主機後，確認後未勾選此類型產品，已安排駐點廠商協助測試，確認安裝後不影響系統運作時，即立刻以手動方式更新完成修補，預計3天內完成。

檢視WSUS主機後，確認後未勾選此類型產品，已安排駐點廠商協助測試，確認安裝後不影響系統運作時，即立刻以手動方式更新完成修補，預計3天內完成。

檢視WSUS主機後，確認後未勾選此類型產品，已安排駐點廠商協助測試，確認安裝後不影響系統運作時，即立刻以手動方式更新完成修補，預計3天內完成。

指 數 處理

A	B	C	D	E	F	G	H	I	J	K	L	
1	資產名稱	資產廠商	資產版本	CPE2.0	資產數量	CVE編號	CVS	發布時間	更新時間	弱點說明	NVD弱點說明連結	改善措施
2	Microsoft .NET	Microsoft Co	4.5.50938	cpe:2.3:an 1				2014/10/15 18	2018/10/13 06	Microsoft .NET	https://web.nvd.nist.gov	尚未填寫
3	Microsoft .NET	Microsoft Co	4.5.50938	cpe:2.3:an 1				2014/10/15 18	2018/10/13 06	Microsoft .NET	https://web.nvd.nist.gov	尚未填寫
4	Microsoft .NET	Microsoft Co	4.5.50938	cpe:2.3:an 1				2014/05/14 19	2018/10/13 06	The .NET Re	https://web.nvd.nist.gov	尚未填寫
5	Microsoft .NET	Microsoft Co	4.5.50938	cpe:2.3:an 1				2015/12/09 19	2019/05/15 21	The Windows	https://web.nvd.nist.gov	尚未填寫
6	Microsoft .NET	Microsoft Co	4.5.50938	cpe:2.3:an 1				2015/09/09 08	2018/10/13 06	Microsoft .NET	https://web.nvd.nist.gov	尚未填寫
7	Microsoft .NET	Microsoft Co	4.5.50938	cpe:2.3:an 1				2015/08/15 08	2019/05/15 21	Microsoft Wi	https://web.nvd.nist.gov	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處理與已填寫改善措施之弱點數量
 - 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

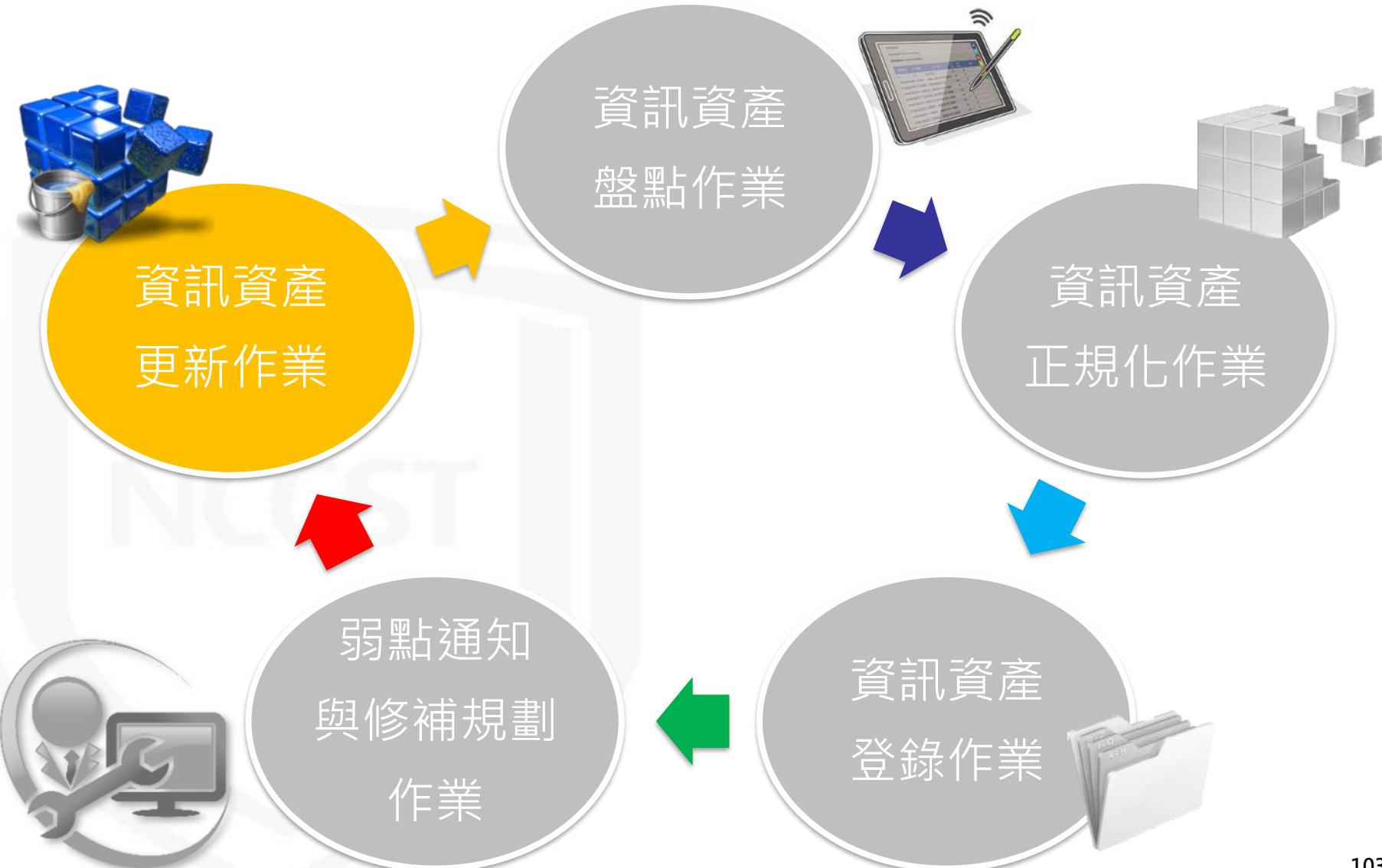
資產風險狀態 > 資通系統風險狀態 > 資訊資產風險列表 技服中心

下載弱點清單 上傳弱點清單

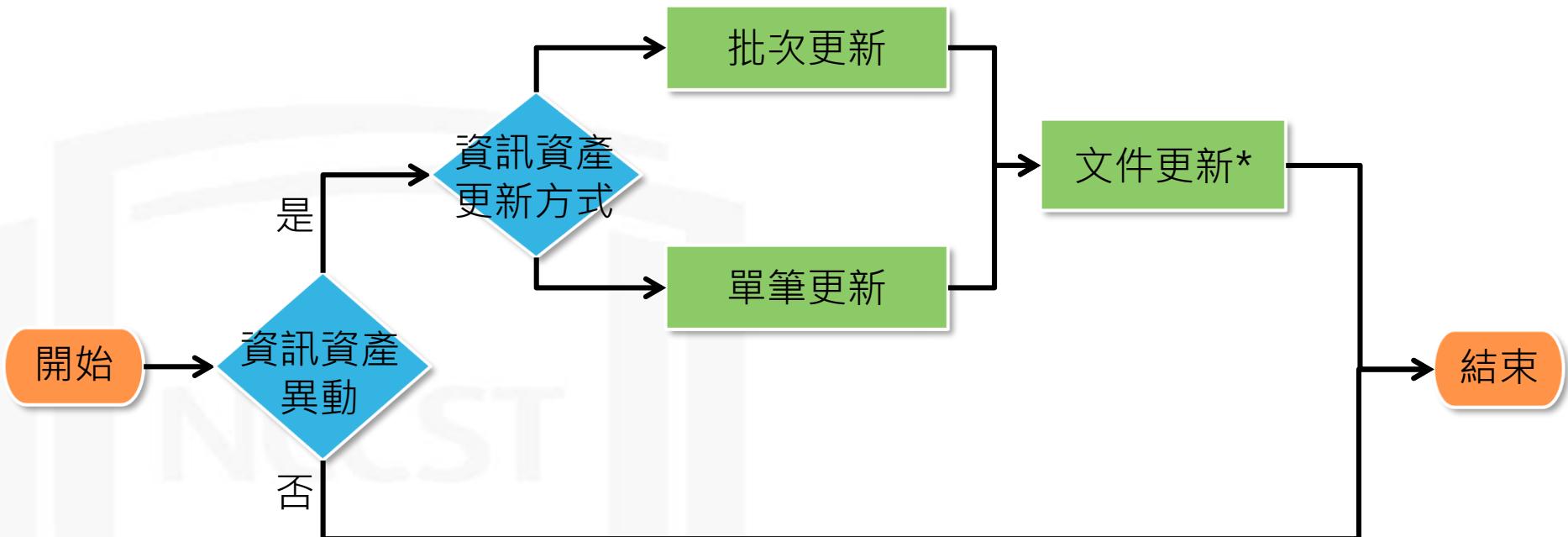
資訊

資產名稱	資產廠商	資產版本	CPE2.3	風險指數	弱點數量	處理情形	弱點資訊
Apache Tomcat 9.0 Tomcat9 (remove only)	The Apache Software Foundation	9.0.16	cpe:2.3:a:apache:tomcat:9.0.16:*****:*	5.96	9	0/9	詳細資訊
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beans:1.8.0:*****:*	7.50	2	0/2	詳細資訊
commons-fileupload	N/A	1.3.2	cpe:2.3:a:apache:commons_fileupload:1.3.2:*****:*	7.50	1	0/1	詳細資訊
Java 8 Update 202 (64-bit)	Oracle Corporation	8.0.2020.8	cpe:2.3:a:oracle:jre:1.8.0:update_202:*****:*	7.07	37	0/37	詳細資訊

資訊資產弱點管理作業流程



資訊資產更新作業流程



*文件更新：

1. 更新資訊資產清冊
2. 重新匯出弱點清單

資訊資產更新-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

技服中心

完整軟體資產CPE清單下載 常見重要軟體資產CPE清單下載 上傳清單格式下載 資產清單上傳

資通系統資產清單下載 (選項)

資產關聯更新CPE清單下載 資通系統資產清單匯出(PDF)

default-cpe-NCCST-ServerAsset-download.xls [相容模式] - Excel (產品啟動失敗)

Administrator@test.com

資料

資產名稱

S108

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	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	廠商	產品	版本	更新	版次	
2	NCCST	技服中心	1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft	(10.0.17761:cpe:2.3:or: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:or:Microsoft\microsoft	windows_sr2	*	*	*	*	*	*	
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:or: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	

軟體資產清單-1

就緒

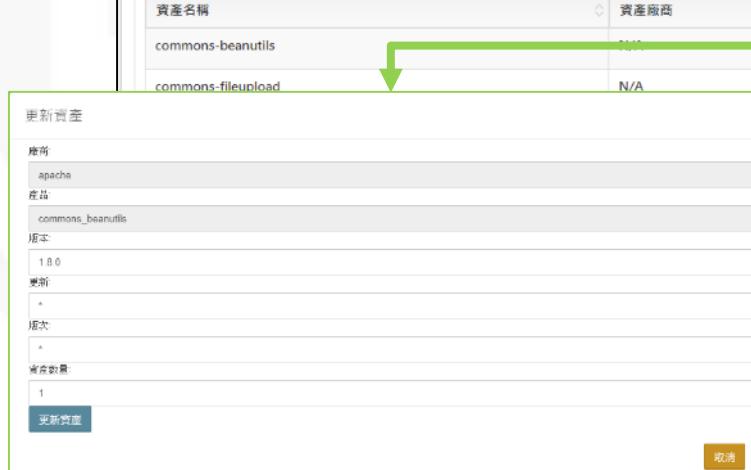
100%

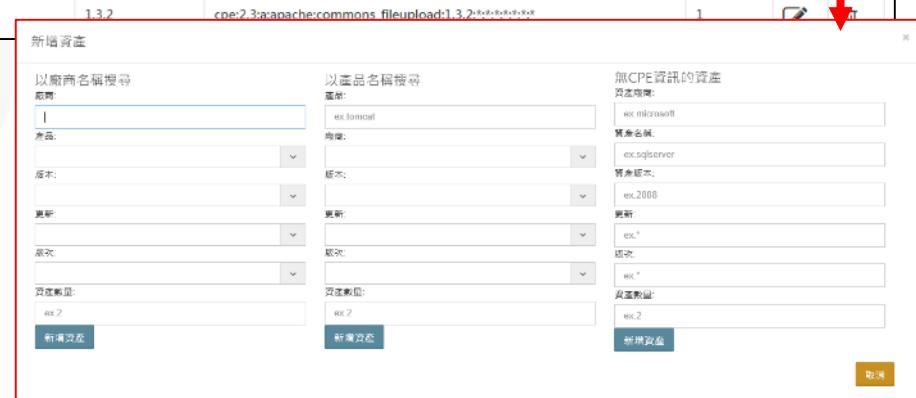
資訊資產更新-單筆更新

● 編輯資訊資產

- 除透過CPE清單批次更新資產外，亦可透過網頁頁面進行單筆資訊資產新增、修改及刪除等作業







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

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
 - 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
資產數量	資產名稱	資產廠商	資產版本	TEMP	資產數量
1	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation	10.0.17763	Microsoft Windows Server 2019 Datacenter 64 位元	Microsoft Corporation
1	Microsoft Windows Server 2008 R2 Datacenter Serv	Microsoft Corporation	6.1.7601	Microsoft Windows Server 2008 R2 Datacenter Service Pack 1 64-bitMic	1
2	Microsoft DCF MUI (Chinese (Traditional)) 2016	Microsoft Corporation	16.0.4266.100	Microsoft DCF MUI (Chinese (Traditional)) 2016	Microsoft Corporation
2	Microsoft Office Professional Plus 2016	Microsoft Corporation	16.0.4266.100	Microsoft Office Professional Plus 2016	Microsoft Corporation
2	Microsoft OneNote MUI (Chinese (Traditional)) 201	Microsoft Corporation	16.0.4266.100	Microsoft OneNote MUI (Chinese (Traditional)) 2016	Microsoft Corporati
2	Microsoft Office 32-bit Components 2016	Microsoft Corporation	16.0.4266.100	Microsoft Office 32-bit Components 2016	Microsoft Corporation
2	Microsoft Office Shared 32-bit MUI (Chinese (Tradi	Microsoft Corporation	16.0.4266.100	Microsoft Office Shared 32-bit MUI (Chinese (Traditional)) 2016Microso	1

弱點清單

B	C	D	E	F	G	H	I	J	K	L
資產廠商	資產版本	CPE2.1	資產數量	CVE編號	CVS	發布時間	更新時間	弱點說明	NVD弱點說明連結	改善措施
Microsoft Co	4.5.50938	cpe:2.3:ari	1	CVE-2014-10.0	2014/10/15 18	2018/10/13 00	Microsoft .NET Re	https://web.nvd.nist.gov/		檢視WSUS主機後，確認後未勾選此類型產品，已安排駐點廠商協助測試，確認安裝後不影響系統運作時，即立刻以手動方式更新完成修補，預計3天內完成
Microsoft Co	4.5.50938	cpe:2.3:ari	1	CVE-2014-10.0	2014/10/15 18	2018/10/13 00	Microsoft .NET Re	https://web.nvd.nist.gov/		檢視WSUS主機後，確認後未勾選此類型產品，已安排駐點廠商協助測試，確認安裝後不影響系統運作時，即立刻以手動方式更新完成修補，預計3天內完成
Microsoft Co	4.5.50938	cpe:2.3:ari	1	CVE-2014-10.0	2014/05/14 19	2018/10/13 00	The .NET Re	https://web.nvd.nist.gov/		檢視WSUS主機後，確認後未勾選此類型產品，已安排駐點廠商協助測試，確認安裝後不影響系統運作時，即立刻以手動方式更新完成修補，預計3天內完成
Microsoft Co	4.5.50938	cpe:2.3:ari	1	CVE-2015-9.3	2015/12/09 19	2019/05/15 22	The Window	https://web.nvd.nist.gov/		檢視WSUS主機後，確認後未勾選此類型產品，已安排駐點廠商協助測試，確認安裝後不影響系統運作時，即立刻以手動方式更新完成修補，預計3天內完成
Microsoft Co	4.5.50938	cpe:2.3:ari	1	CVE-2015-9.3	2015/09/09 08	2018/10/13 00	Microsoft .NET	https://web.nvd.nist.gov/		檢視WSUS主機後，確認後未勾選此類型產品，已安排駐點廠商協助測試，確認安裝後不影響系統運作時，即立刻以手動方式更新完成修補，預計3天內完成



實作練習3

弱點修補與資產更新作業

實作練習3：弱點修補與資產更新作業

- 請於VANS系統上進行弱點通知設定，並針對弱點進行修補規劃作業
- 本項練習時間**20分鐘**

項次	執行項目	產出項目/執行結果
1	修改弱點通知CVSS分數門檻為8.5分	於弱點通知檢視設定值
2	於 資產風險狀態 檢視比對後的WinRAR 5.50之弱點，並以版更方式進行修補；更新版為WinRAR 5.90	完成WinRAR版本更新後，重新上傳資產清單，待弱點比對完成後再次檢視WinRAR弱點是否已修補
3	於 資產風險狀態 檢視比對後的Apache Tomcat 8.0.30之弱點，透過查詢建議修補方式填寫改善措施，並下載弱點清單	<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

常見問答(1/2)

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	每10分鐘比對1次	定期執行掃描

常見問答(2/2)

Q2

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

Q3

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

Q4

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

Q

&

A

課程大綱

- 前言
- VANS機制介紹
- VANS系統說明與實作
 - VANS系統說明
 - 資訊資產弱點管理作業流程
 - 實作練習1：資訊資產盤點
 - 實作練習2：資訊資產正規化與登錄
 - 實作練習3：弱點修補與資產更新作業
- 安全性更新管理機制說明與實作
 - MBSA工具介紹
 - 安全性更新檢測流程
 - 實作練習4：單機環境檢測與報告分析
 - 實作練習5：網域派送檢測

緣起

- 由於安全性更新頻繁，且Windows作業系統除非大型更新，否則不會改變軟體資訊，因此僅採用資產管理軟體所取得之軟體版本資訊無法有效判斷是否已安裝安全性更新修補程式
- 藉由安全性更新管理機制，可了解伺服器主機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與原因，以強化安全性更新落實情形



預期效益

- 提升微軟系列產品安全性更新掌握能力
- 提高微軟系列產品更新落實程度
- 重大弱點爆發時，可快速確認未安裝安全性更新之伺服器主機與使用者電腦數量與範圍，並進行應變處理



檢測方式評估(1/3)

- 微軟修補弱點之方式為透過Windows Update，許多機關採用WSUS進行安全性更新派送，但WSUS可能因漏派安全性更新而造成缺漏情形
- 微軟提供免費的**MBSA**(Microsoft Baseline Security Analyzer)掃描工具，該工具有執行單純與快速之特點，且可檢查更新檔安裝情形，以掌握微軟系列產品更新情況



檢測方式評估(2/3)

- 微軟於2018年10月公告停止支援MBSA，未來不會進行程式更新，並已刪除最新的MBSA 2.3版下載連結
 - <https://docs.microsoft.com/zh-tw/windows/security/threat-protection/mbsa-removal-and-guidance>

什麼是 Microsoft 基準安全分析分析器及其用途？

2018/10/05 · 🎉

Microsoft 基準安全分析工具（MBSA）可用來驗證修補程式合規性。MBSA 也會執行數個其他 Windows、IIS 和 SQL Server 安全檢查。遺憾的是，從 Windows XP 和 Windows Server 2003 起，這些額外檢查所留下的邏輯尚未積極維護。在產品中所做的變更，因為這些安全性檢查已過時，且有一些建議 counterproductive。

MBSA 在 Microsoft Update 或 local WSUS 或 Configuration Manager 伺服器都無法使用的情況中，或作為相容性工具，以確保所有安全更新都已部署到受管理的環境中，是很大的。雖然 MBSA 版本2.3 推出了 Windows Server 2012 R2 和 Windows 8.1 的支援，但它已被棄用，且不再開發。MBSA 2.3 沒有更新成完全支援 Windows 10 和 Windows Server 2016。

- 微軟仍持續維護與更新WSUS 離線掃描檔案(wsusscn2.cab)，因此仍可使用MBSA檢測電腦的安全性更新情形

檢測方式評估(3/3)

- MBSA執行方式分為圖形化(MBSA.exe)與Command Line(mbsacli.exe)等兩種，建議以**MBSACLI**進行檢測，因其具有下列特點：
 - 可以產出**XML**格式之安全性更新檢測報告
 - 受測電腦可透過**免安裝方式**進行安全性更新檢測



```
C:\ 系統管理員: 命令提示字元 - mbsacli /xmlout /catalog wsusscn2.cab /unicode /nvc
Microsoft Windows [版本 10.0.18363.720]
(c) 2019 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\WINDOWS\system32>E:
E:\>cd MBSA
E:\MBSA>mbsacli /xmlout /catalog wsusscn2.cab /unicode /nvc >> results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2%%DATE:~8,2%.xml
Microsoft Baseline Security Analyzer
Version 2.3 (2.3.2211.0)
(C) Copyright 2002-2013 Microsoft Corporation. All rights reserved.
```

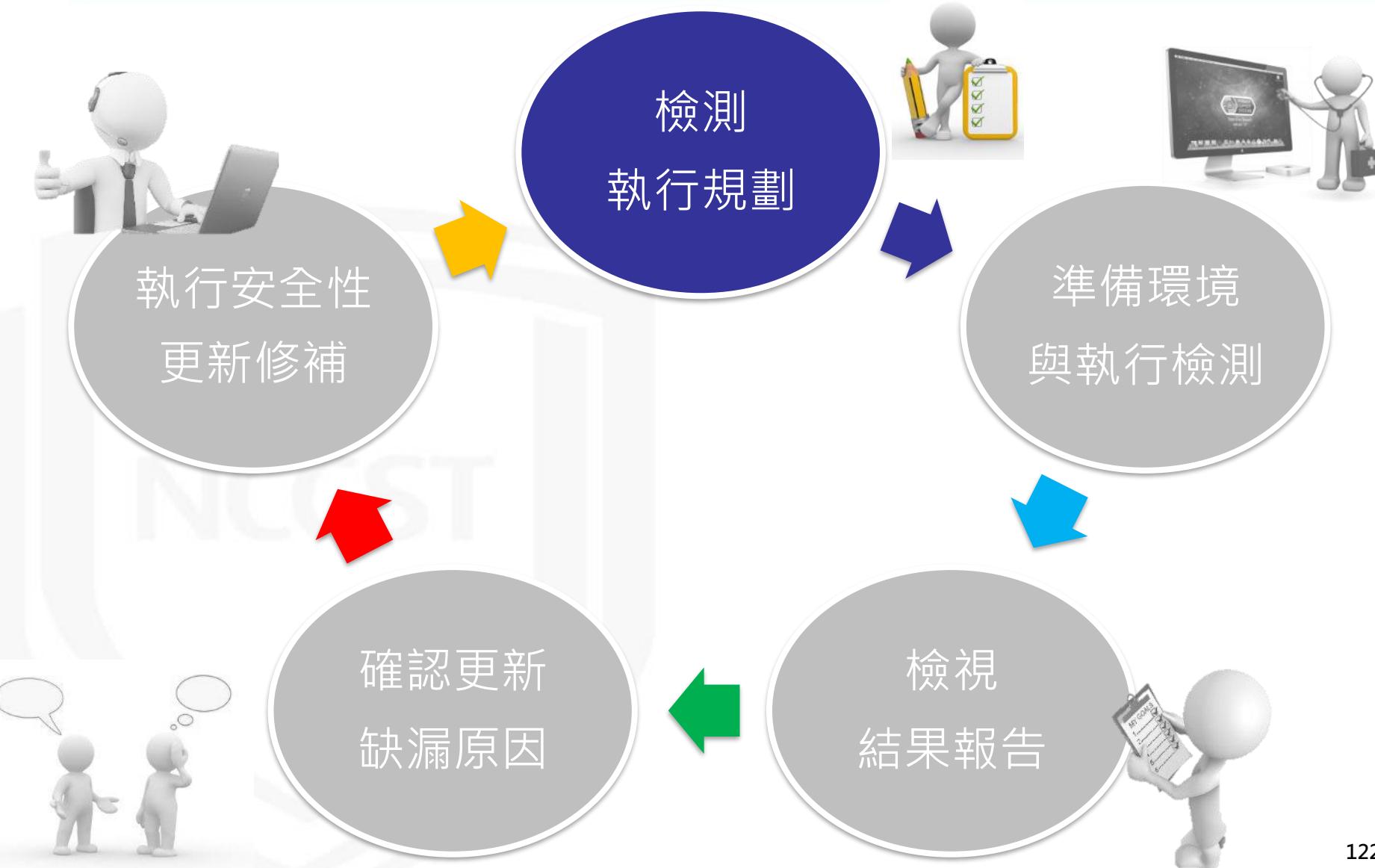
課程大綱

- 前言
- VANS機制介紹
- VANS系統說明與實作
 - VANS系統說明
 - 資訊資產弱點管理作業流程
 - 實作練習1：資訊資產盤點
 - 實作練習2：資訊資產正規化與登錄
 - 實作練習3：弱點修補與資產更新作業
- 安全性更新管理機制說明與實作
 - MBSA工具介紹
 - 安全性更新檢測流程
 - 實作練習4：單機環境檢測與報告分析
 - 實作練習5：網域派送檢測

安全性更新管理機制作業流程



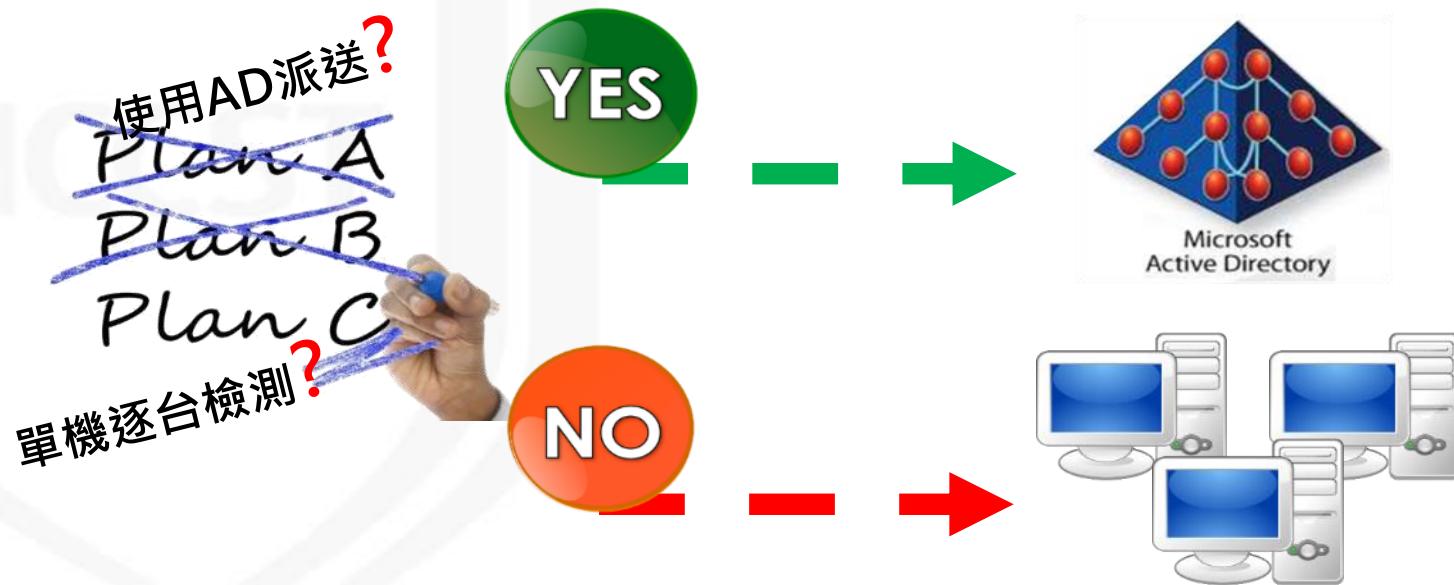
安全性更新管理機制作業流程



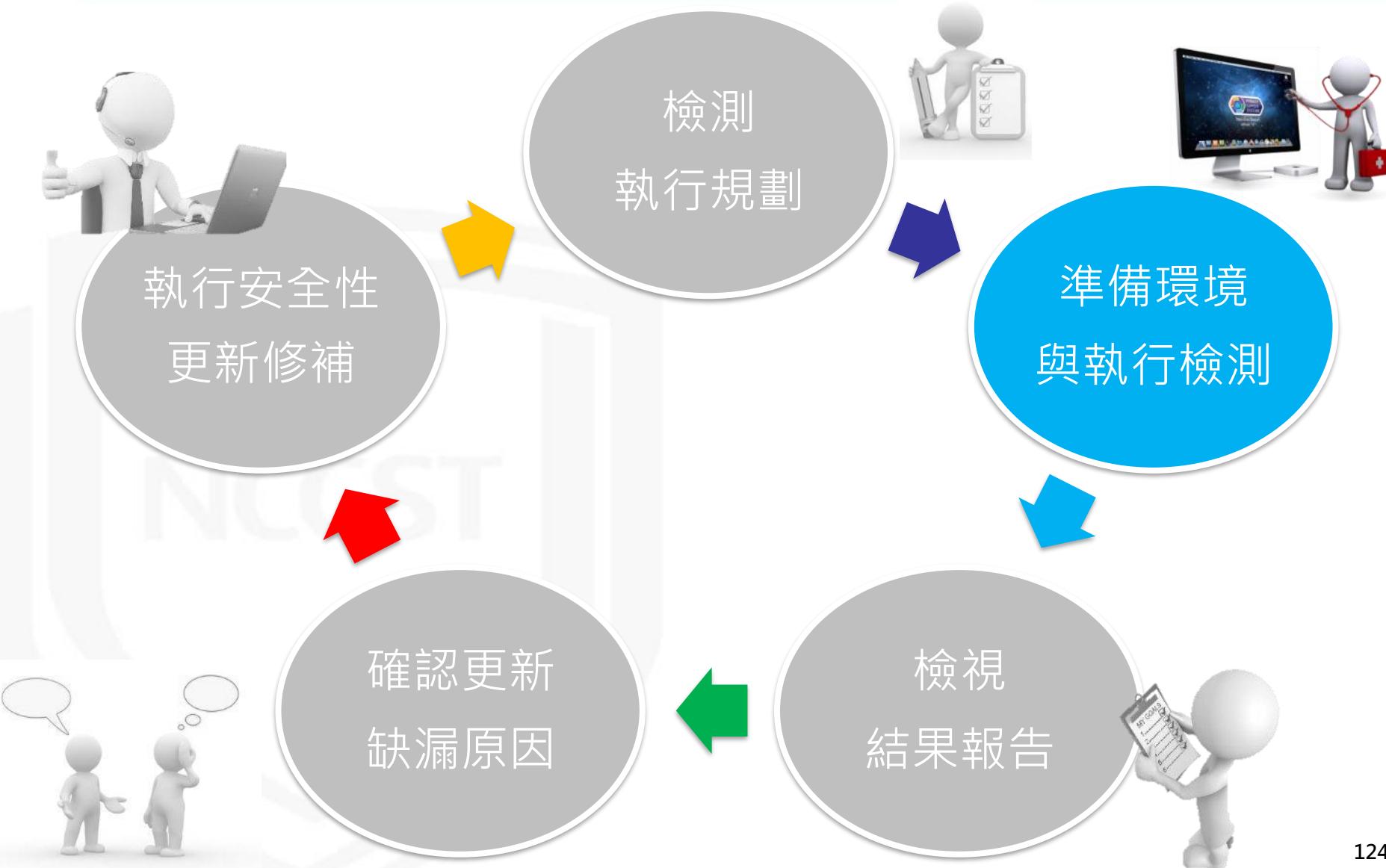
檢測執行規劃

- 依據機關環境擬定檢測執行規劃

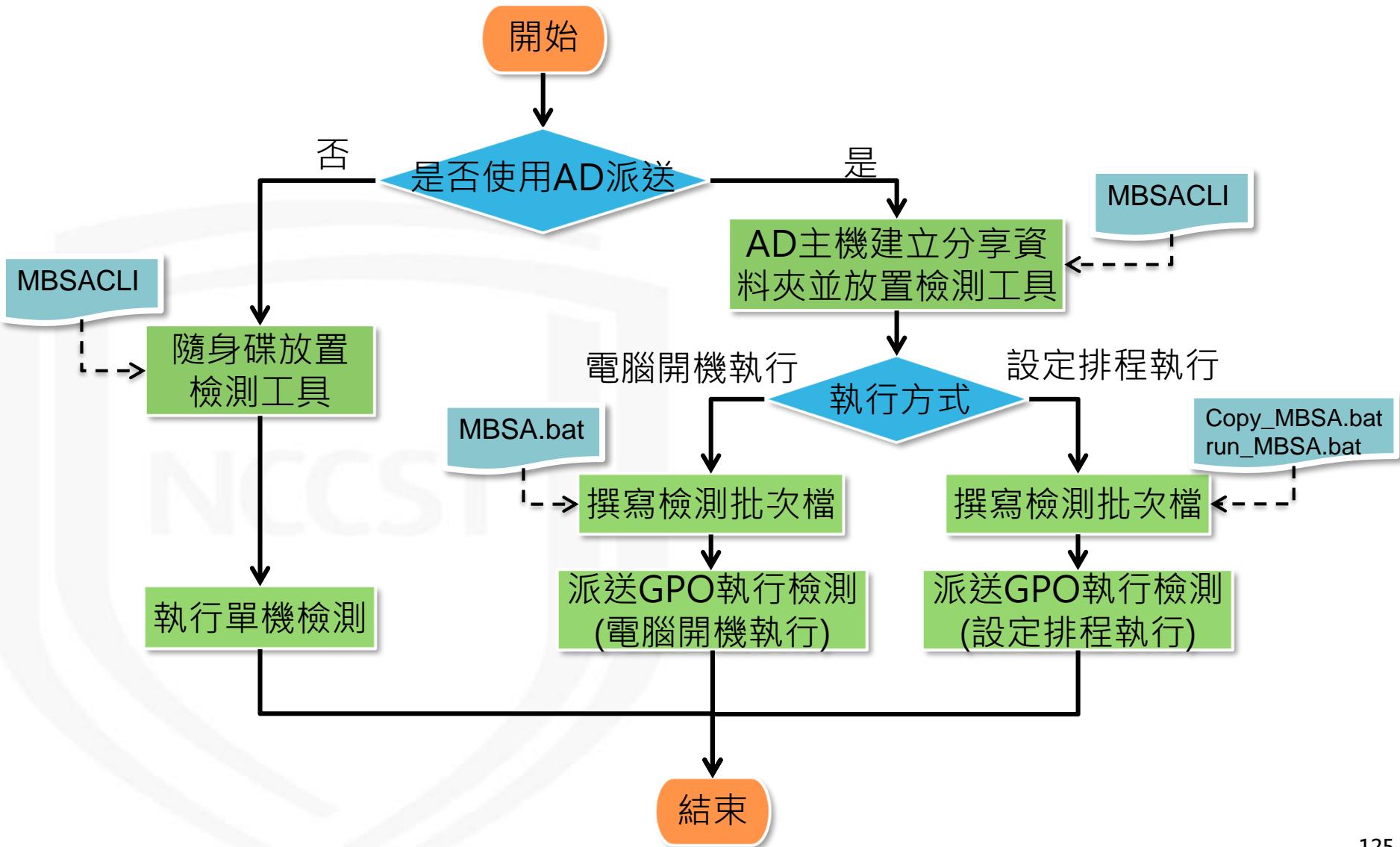
- 執行範圍：本部/本部與所屬、伺服器主機/使用者電腦
- 執行時程：人力評估、導入測試起訖時間、實際導入起訖時間
- 執行方式：單機逐台檢測/AD派送GPO執行多台檢測



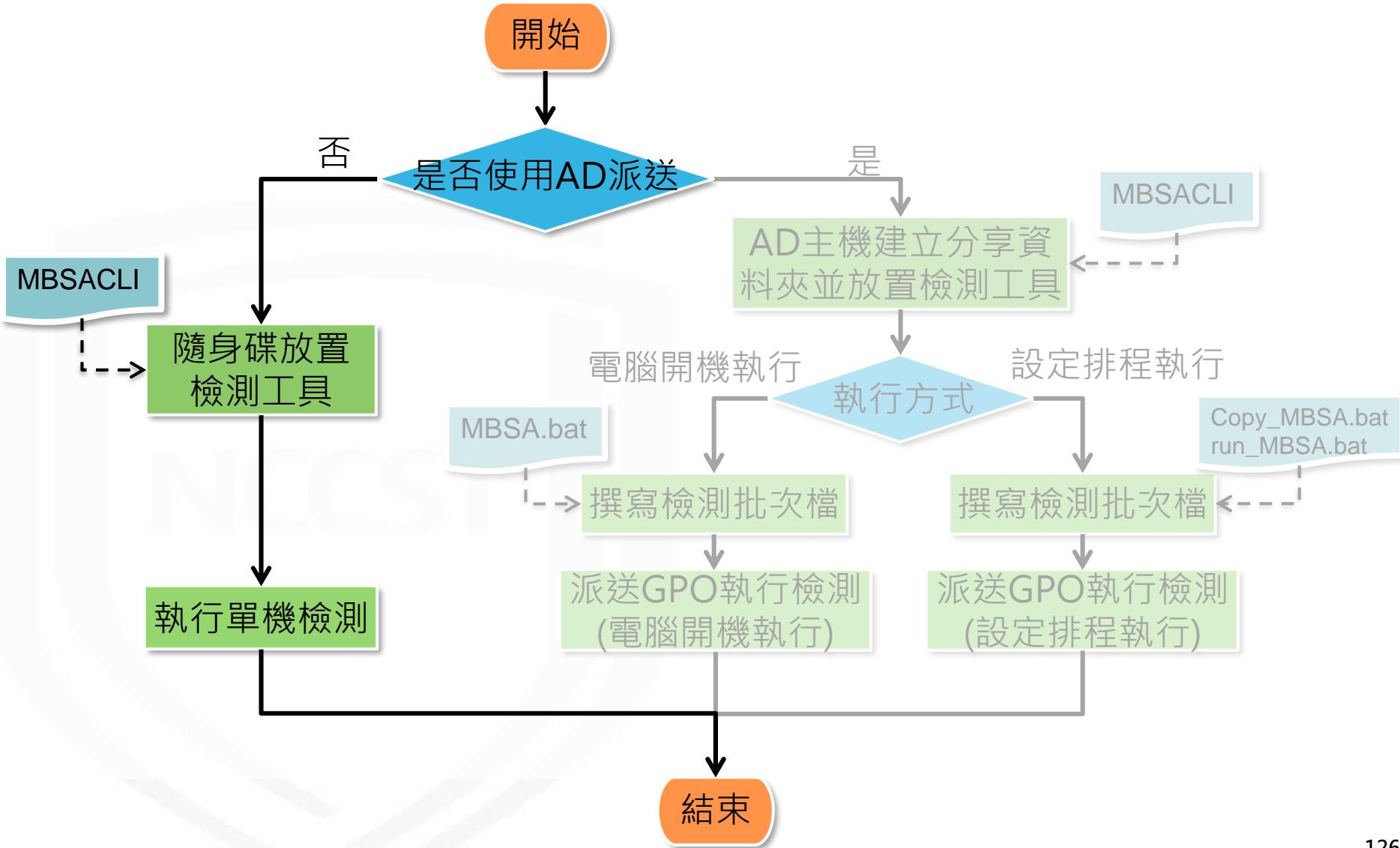
安全性更新管理機制作業流程



安全性更新檢測流程

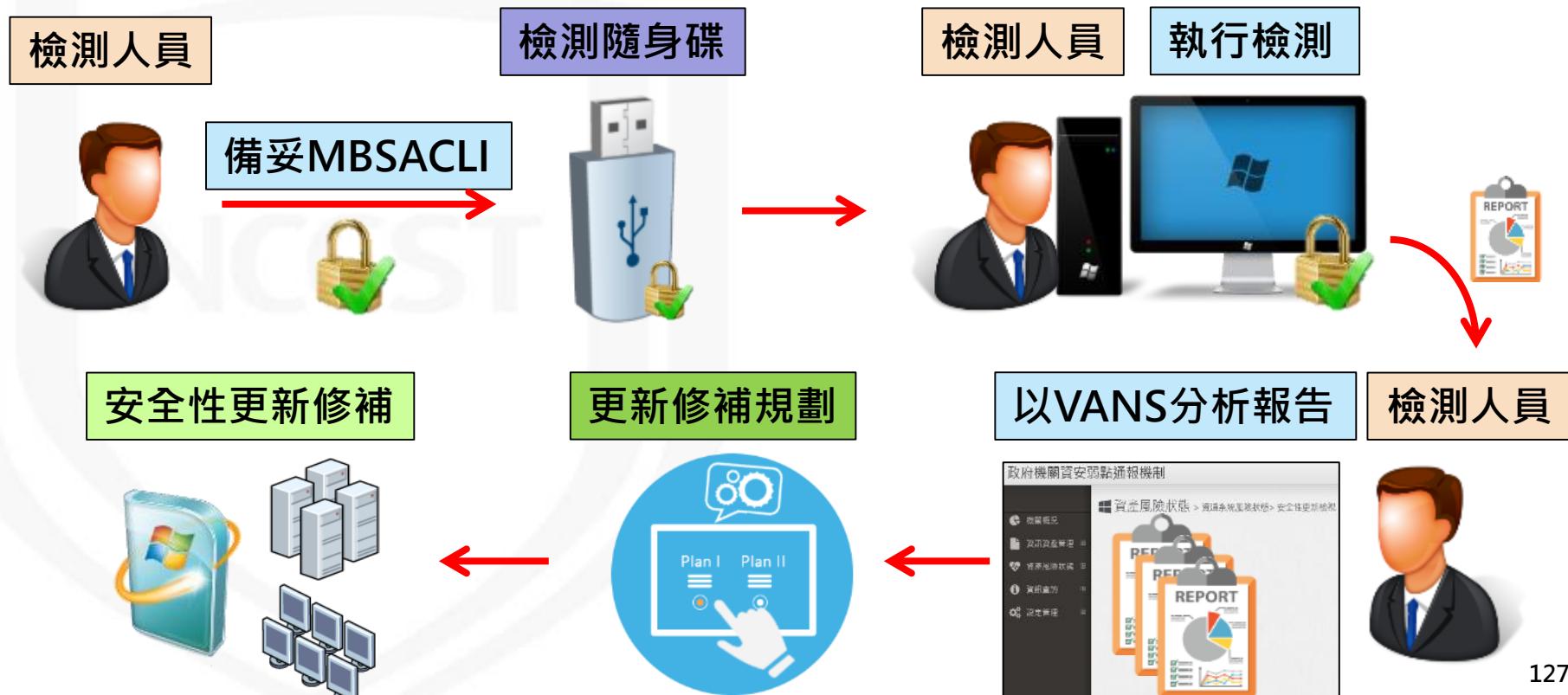


安全性更新檢測流程



單機環境檢測作業流程

- 檢測人員於檢測隨身碟中放置MBSACLI，使用Command Line進行檢測。檢測完成後，進行報告彙整並透過VANS系統分析檢測結果，依據機關安全性更新管理政策進行更新修補規劃與執行



隨身碟放置檢測工具

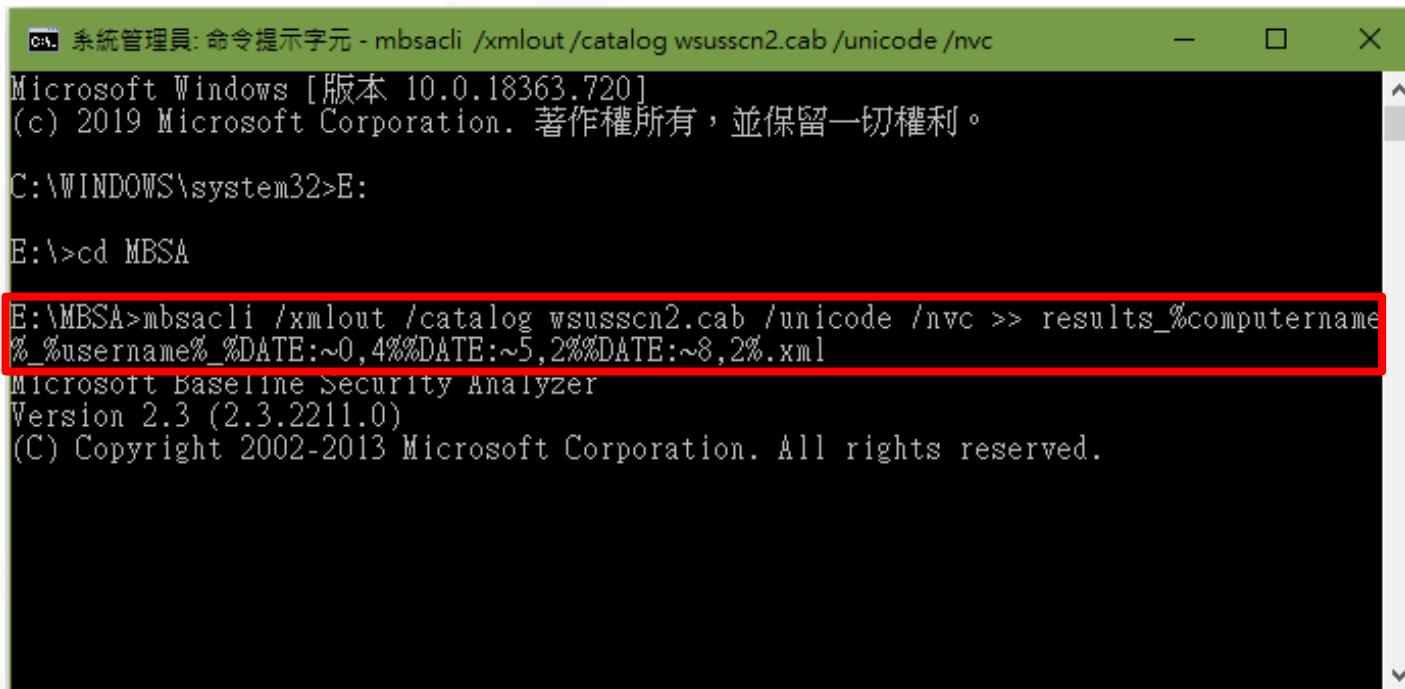
- MBSA安裝資料夾中，包含MBSACLI檔案
 - 預設路徑：%SystemDrive%\Program Files\Microsoft Baseline Security Analyzer 2
 - 受測電腦須使用對應之32位元或64位元的MBSA安裝檔

 - 於隨身碟建立資料夾放置MBSACLI檔案
 - mbsacli.exe : MBSACLI執行檔
 - wusscan.dll : MBSACLI工具必要檔案
 - wsusscn2.cab : 檢測時，將以此微軟更新離線資料庫做為檢測基準
- 下載網址：<http://go.microsoft.com/fwlink/?LinkId=74689>



執行單機檢測(1/2)

- 於受測電腦**以系統管理員身分執行**開啟命令提示字元，切換至隨身碟的MBSA CLI 資料夾，並以下列指令執行檢測
 - mbsacli /xmlout /catalog wsusscn2.cab /unicode /nvc >> results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2% %DATE:~8,2%.xml

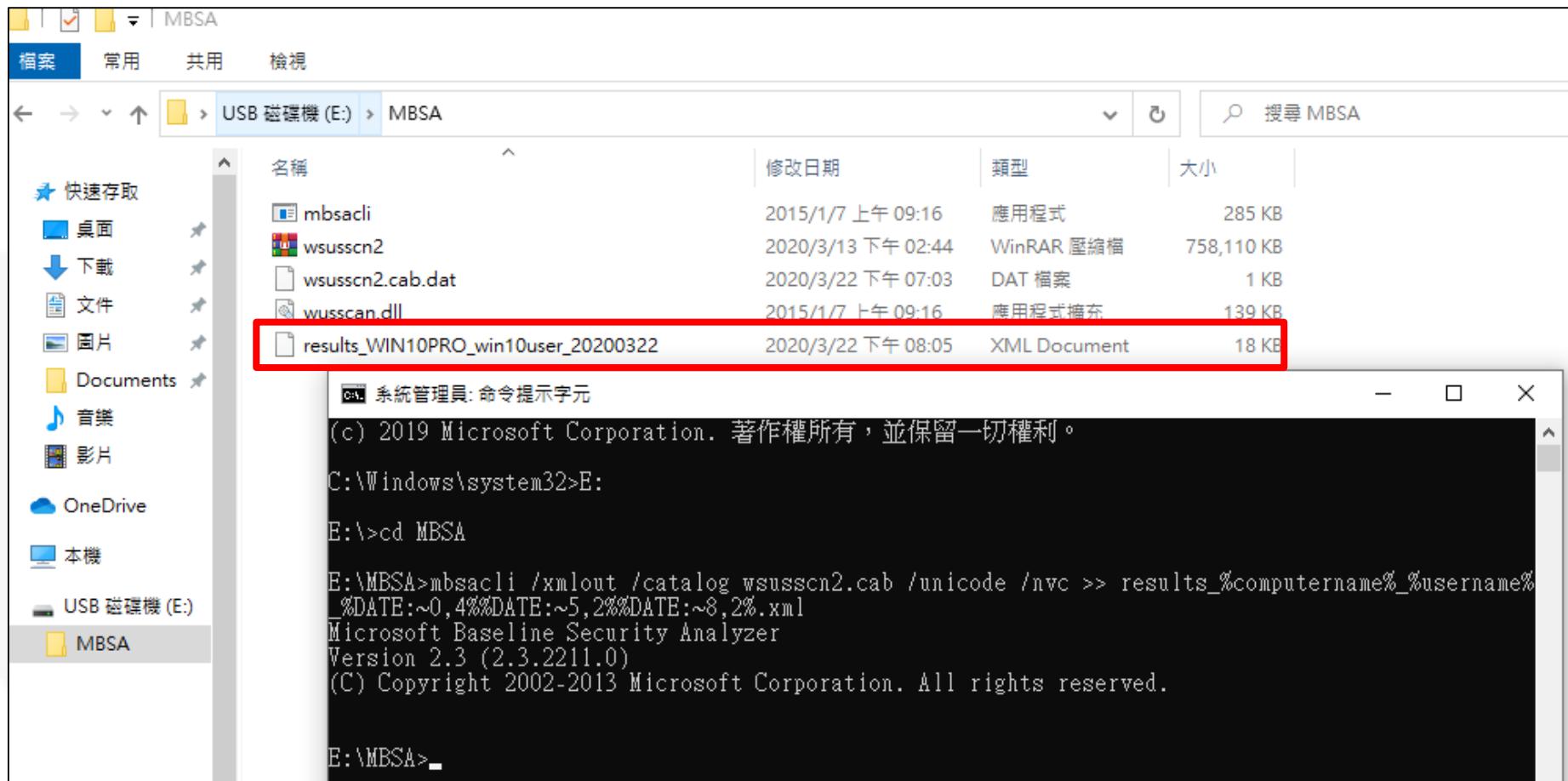


The screenshot shows a Windows Command Prompt window titled "系統管理員: 命令提示字元 - mbsacli /xmlout /catalog wsusscn2.cab /unicode /nvc". The window displays the following text:
Microsoft Windows [版本 10.0.18363.720]
(c) 2019 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\WINDOWS\system32>E:
E:\>cd MBSA
E:\MBSA>mbsacli /xmlout /catalog wsusscn2.cab /unicode /nvc >> results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2% %DATE:~8,2%.xml

The command `mbsacli /xmlout /catalog wsusscn2.cab /unicode /nvc >> results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2% %DATE:~8,2%.xml` is highlighted with a red rectangle.

執行單機檢測(2/2)

- 檢測完成後將產出XML格式之檢測報告





實作練習4

單機環境檢測與報告分析

實作練習4：單機環境檢測與報告分析(環境說明)

● 環境說明

– VM名稱：實作練習_Windows 10 x64

➤ 帳號：TEST\win10user

➤ 密碼：1qaz@WSX3edc



● 指令範本

– 位置：桌面\02.安全性更新管理機制\指令範本

➤ MBSA_單機檢測.bat

● 檢測報告範本

– 位置：桌面\02.安全性更新管理機制\檢測報告範本

實作練習4：單機環境檢測與報告分析

- 於「實作練習_Windows 10 x64」VM執行資訊資產盤點作業
- 透過VANS系統，上傳檢測報告壓縮檔，以查看檢測結果
- 本項練習時間**10分鐘**

項次	執行項目	產出項目/執行結果
1	執行桌面MBSA內的MBSA_單機檢測	安全性更新檢測報告
2	將檢測報告範例加入壓縮檔，上傳到VANS系統(請參考P.175、176)	於VANS系統檢視解析結果

網域環境檢測作業流程(1/2)

- 檢測人員準備**MBSACLI**檢測所需檔案
- AD管理員於AD主機建置分享資料夾並將**MBSACLI**檢測所需檔案放置於分享資料夾
- AD主機派送GPO至網域伺服器主機與使用者電腦，設定電腦開機或設定排程執行自動化腳本
- 網域伺服器主機與使用者電腦更新並套用GPO原則

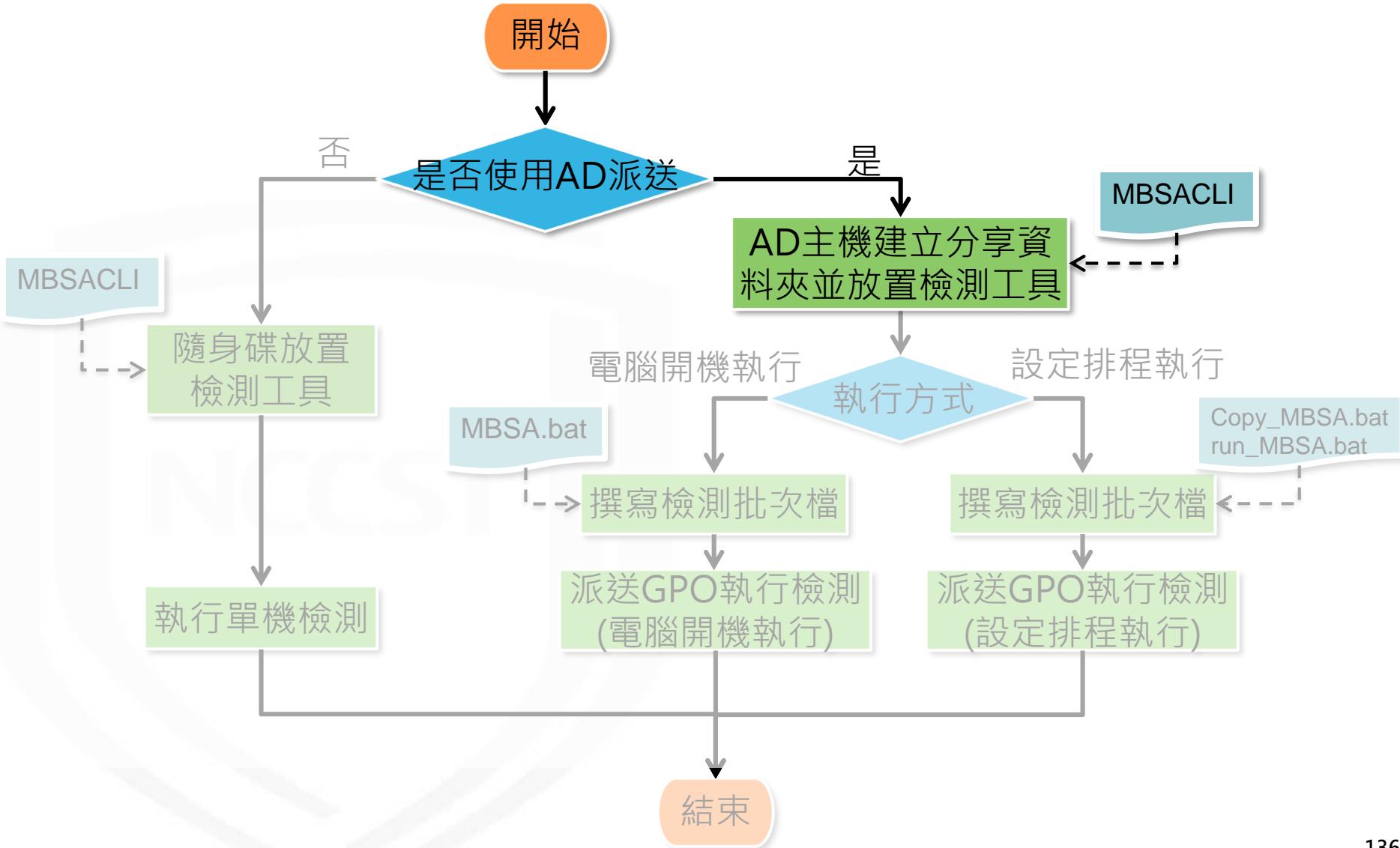


網域環境檢測作業流程(2/2)

- 電腦開機或排程時間到時，將自動執行檢測並回傳檢測報告至AD主機分享資料夾。承辦人進行報告彙整並透過VANS系統分析檢測結果，依據機關安全性更新管理政策進行更新修補規劃與更新作業



安全性更新檢測流程



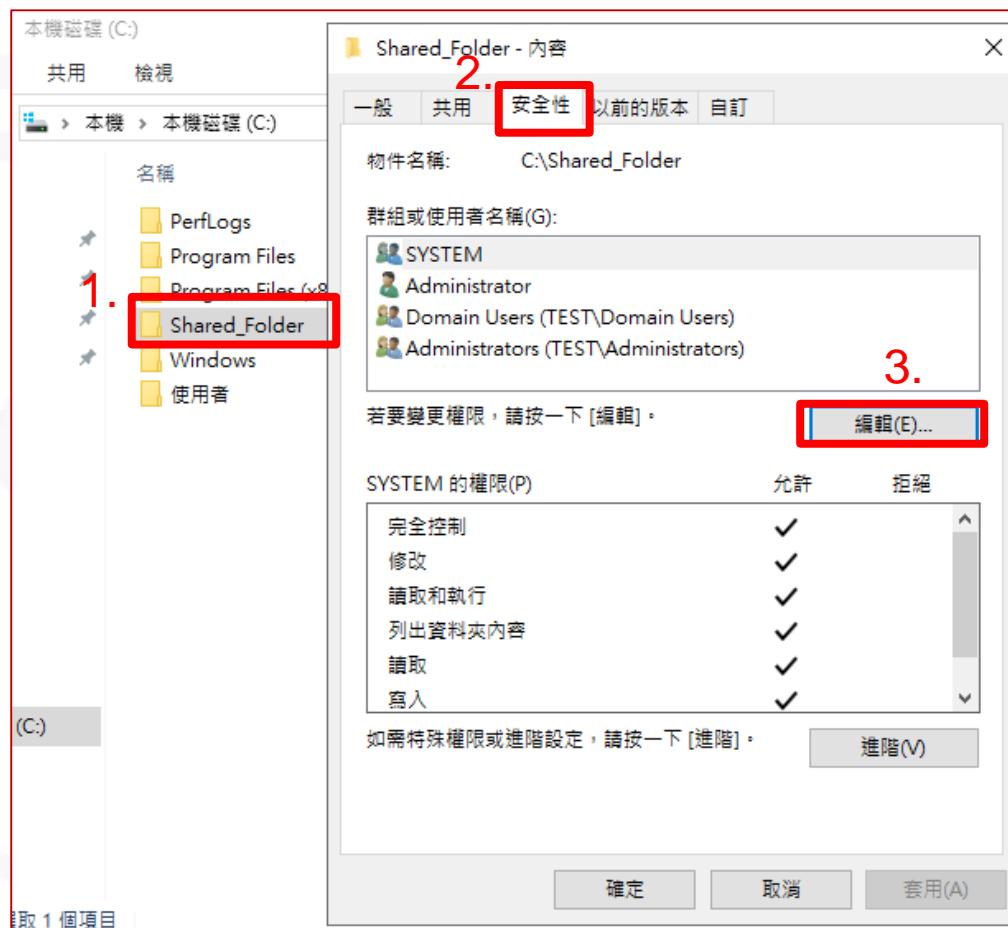
AD主機建立分享資料夾(1/3)

- 於AD主機建立分享資料夾(Shared_Folder)，並按右鍵選擇內容，接著點選共用頁籤，設定 Domain Users 可「讀取/寫入」此資料夾



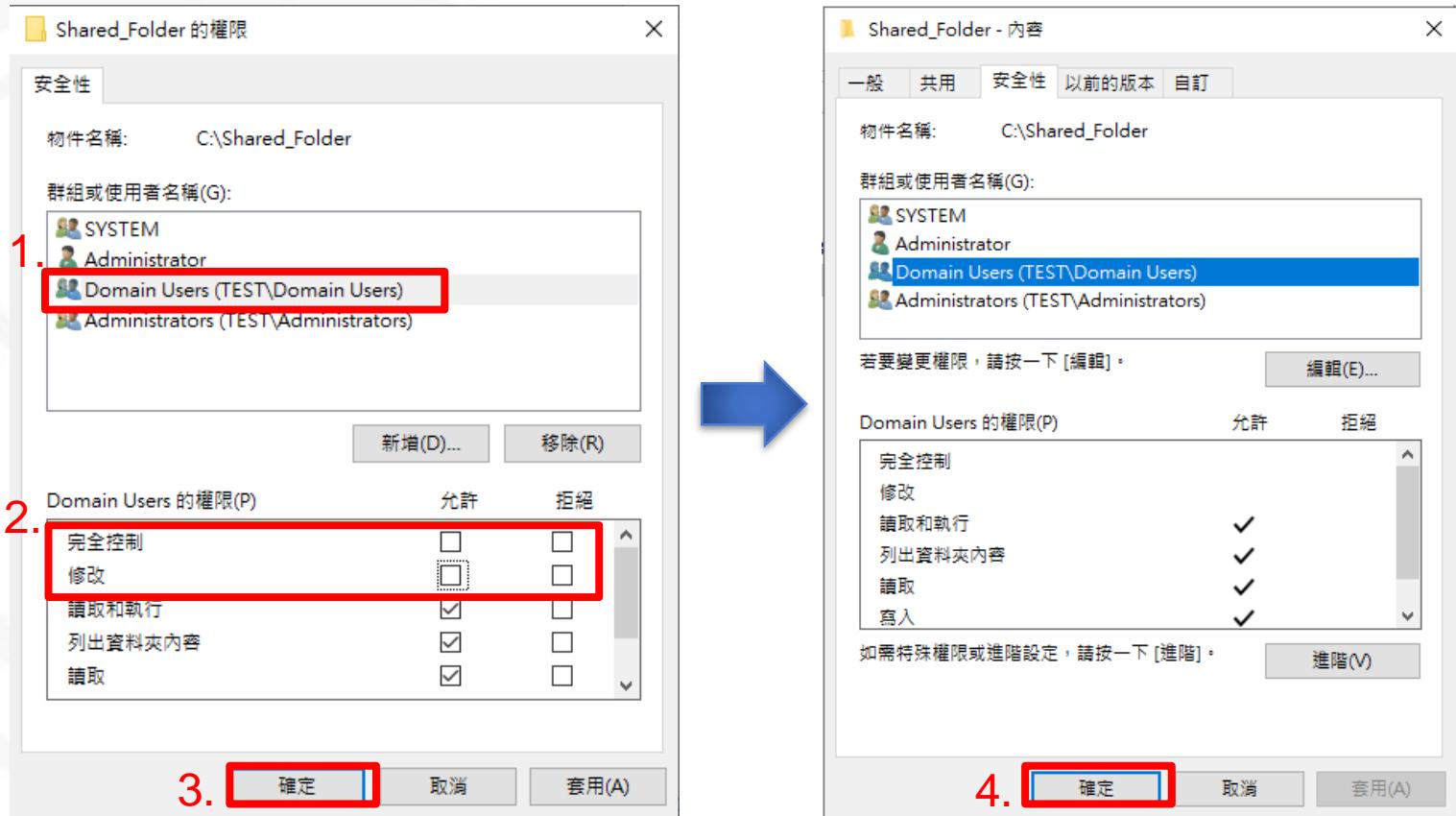
AD主機建立分享資料夾(2/3)

- 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



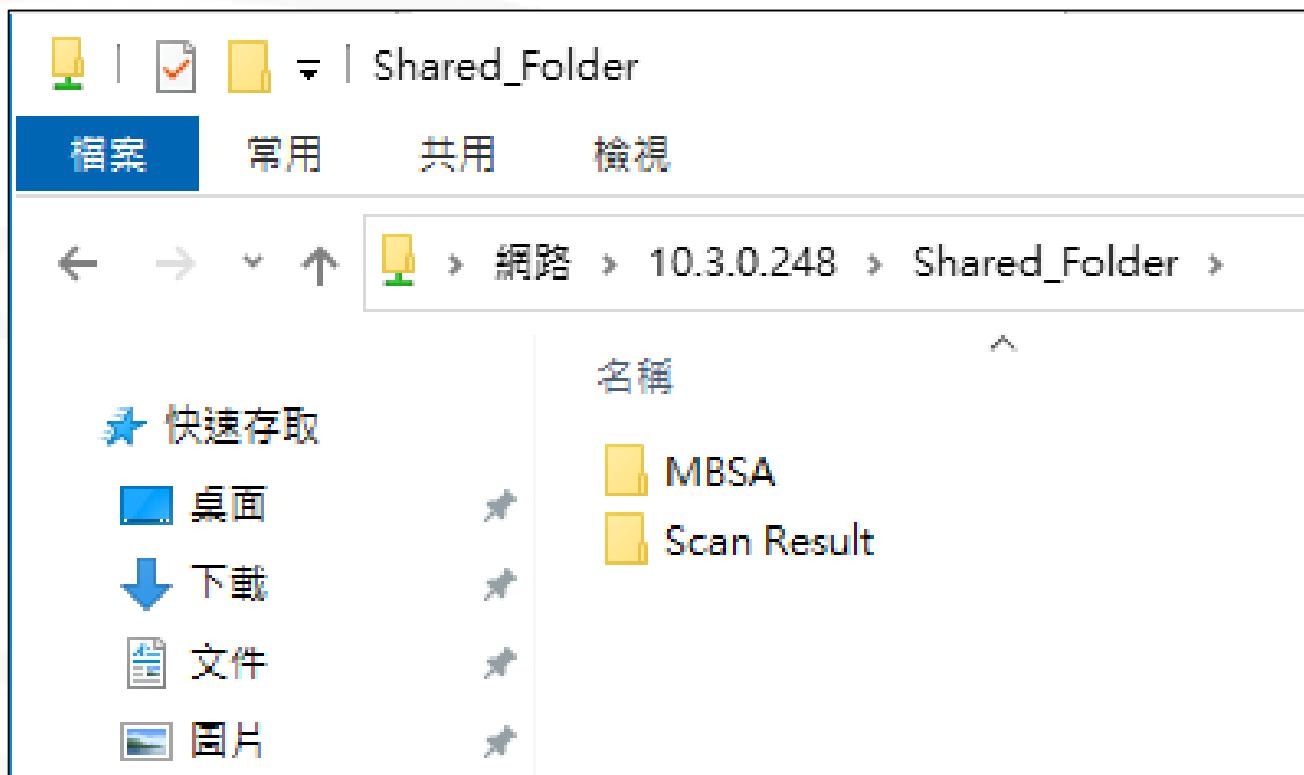
AD主機建立分享資料夾(3/3)

- 接著選取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



放置檢測工具(1/2)

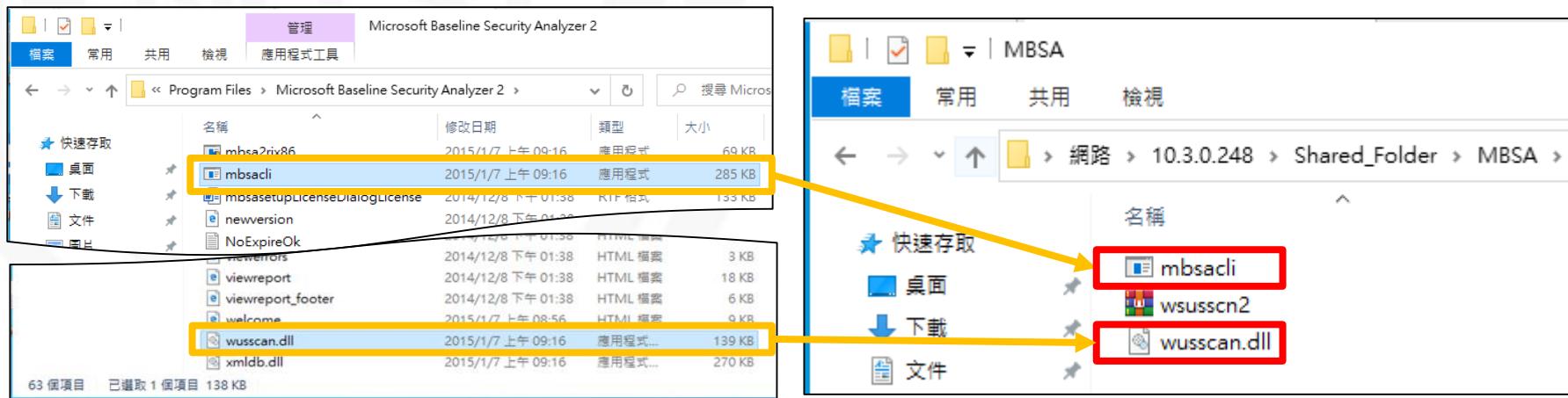
- 於AD主機分享資料夾(Shared_Folder)放置檢測所需相關檔案，並確認Domain User可正常存取檔案
 - MBSA資料夾：存放MBSACLI所需的3個檔案
 - Scan Result資料夾：做為存放MBSACLI檢測報告XML檔之資料夾



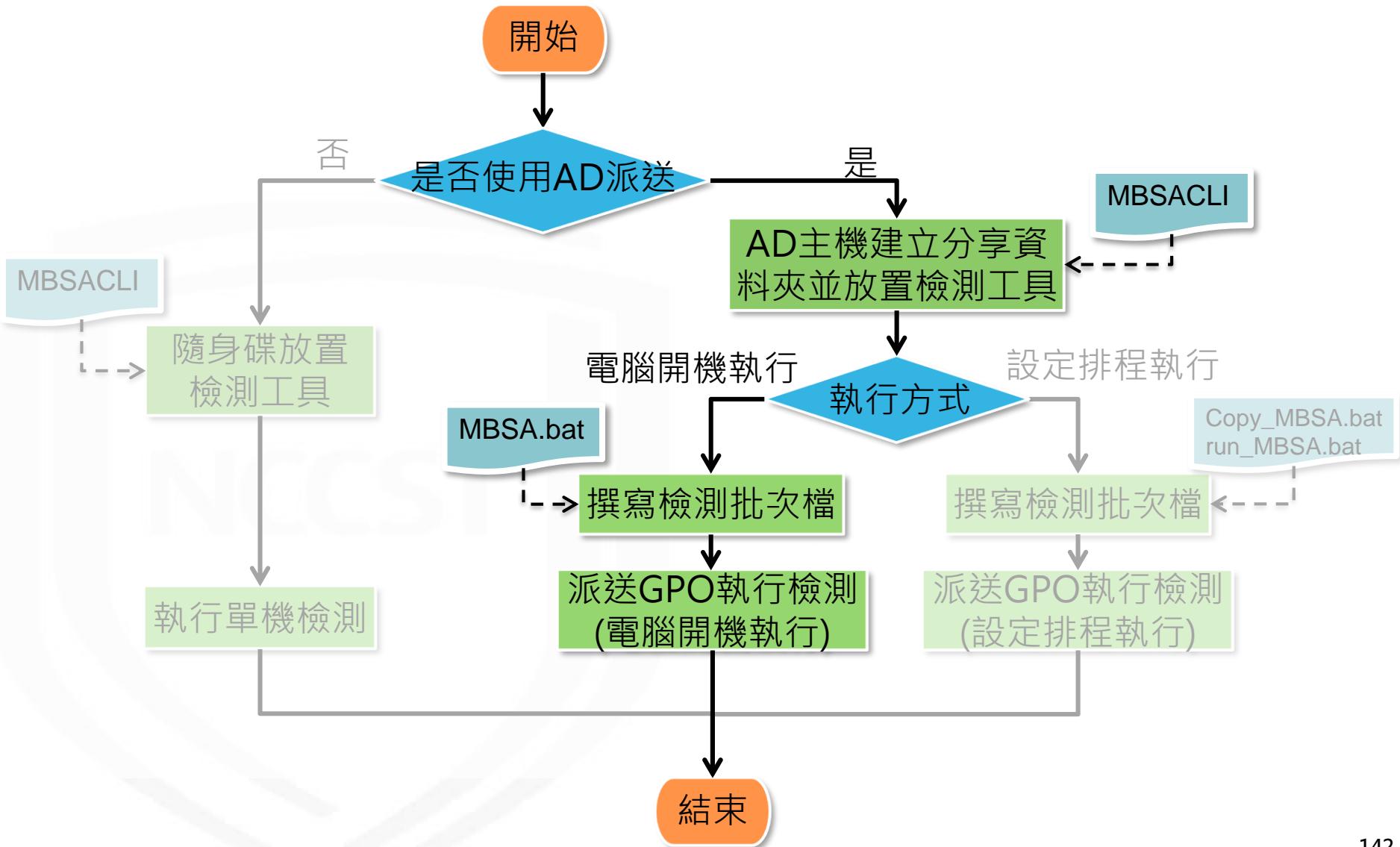
放置檢測工具(2/2)

- MBSA安裝資料夾中，包含MBSACLI檔案
 - 預設路徑：%SystemDrive%\Program Files\Microsoft Baseline Security Analyzer 2
 - 受測電腦須使用對應之32位元或64位元的MBSA安裝檔
- 於AD主機分享資料夾放置MBSACLI檔案
 - mbsacli.exe : MBSACLI執行檔
 - wusscan.dll : MBSACLI工具必要檔案
 - wsusscn2.cab : 檢測時，將以此微軟更新離線資料庫做為檢測基準

➤ 下載網址：<http://go.microsoft.com/fwlink/?LinkId=74689>



安全性更新檢測流程



電腦開機執行檢測方式(1/6)

● 撰寫MBSA CLI 檢測作業指令批次檔(MBSA.bat)

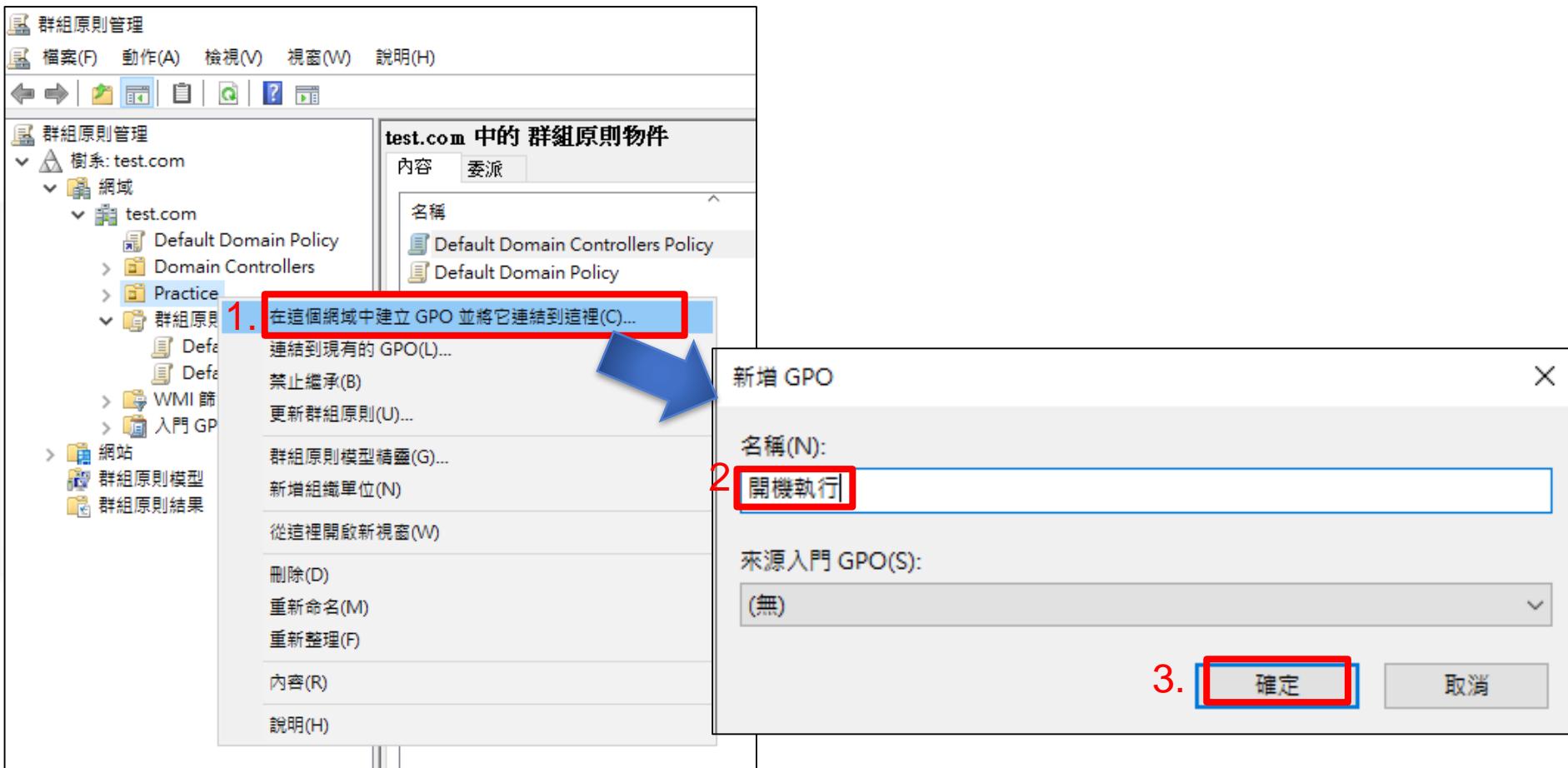
```
MBSA.bat
1 if exist "C:\Users\Public\Documents\MBSA_Result\results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2%%DATE:~8,2%.xml" goto P
2 net use X: "\\\\"10.3.0.248\Shared_Folder" /user:WIN10User "1qaz@WSX3edc"
3 md "C:\Users\Public\Documents\MBSA"
4 md "C:\Users\Public\Documents\MBSA_Result"
5 xcopy /y "X:\MBSA" "C:\Users\Public\Documents\MBSA"
6 cd "C:\Users\Public\Documents\MBSA"
7 mbsacli /xmlout /catalog wsusscn2.cab /unicode /nvc >> results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2%%DATE:~8,2%.xml
8 xcopy /y "C:\Users\Public\Documents\MBSA\*.xml" "C:\Users\Public\Documents\MBSA_Result\"%
9 xcopy /y "C:\Users\Public\Documents\MBSA\*.xml" "X:\Scan Result"
10 cd \
11 rd /Q /S "C:\Users\Public\Documents\MBSA"
12 net use /delete X:
13 :P
```

- | | |
|-------|-----------------------------------------------------------|
| 1 | 判斷使用者電腦的「公用文件」中是否已存在檢測報告，若已有報告則不執行檢測 |
| 2 | 將Shared_Folder掛載為代號X之網路磁碟機，並設定可存取Shared_Folder之帳號密碼 |
| 3~4 | 於「公用文件」建立「MBSA」與「MBSA_Result」兩個資料夾 |
| 5 | 將Shared_Folder的MBSA資料夾內之檔案複製至「公用文件」中的「MBSA」資料夾 |
| 6~7 | 切換至「公用文件」中的「MBSA」資料夾並執行檢測，檢測報告以 電腦名稱、使用者名稱及檢測日期 命名 |
| 8~9 | 複製檢測報告XML檔至使用者電腦的「公用文件」中的「MBSA_Result」與「Scan Result」資料夾 |
| 10 | 切換至根目錄，離開MBSA資料夾 |
| 11~12 | 刪除「公用文件」中的MBSA資料夾並中斷網路磁碟機(X) |

電腦開機執行檢測方式(2/6)

- 在目標OU建立GPO

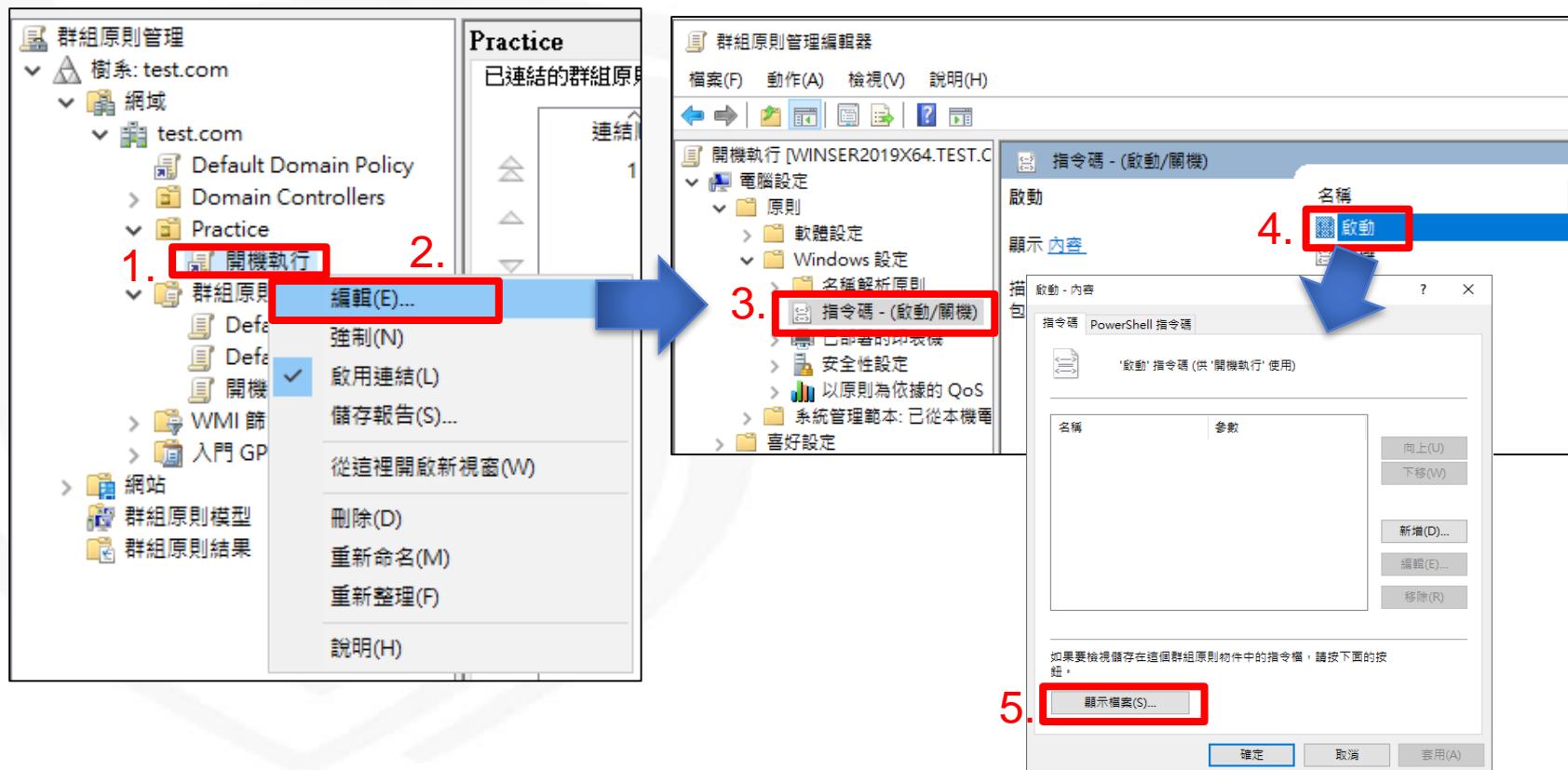
- 新增「開機執行」GPO



電腦開機執行檢測方式(3/6)

● 編輯GPO，於電腦開機時執行檢測批次檔

- 點選剛建立的「開機執行」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)\啟動
- 點選「顯示檔案」，準備放入檢測批次檔



電腦開機執行檢測方式(4/6)

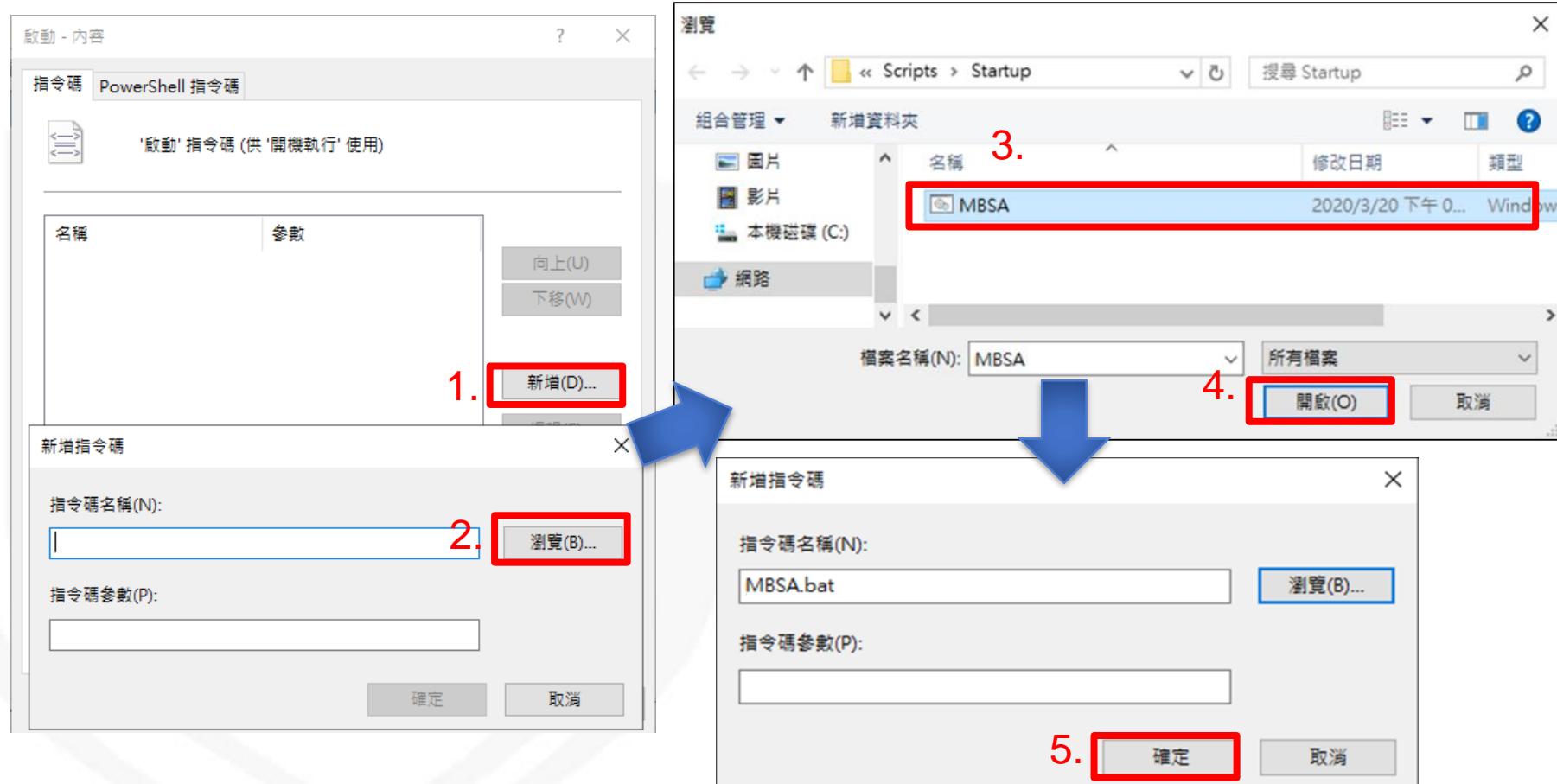
- 因作業系統預設不允許直接複製檔案至網路位置，故須將資料夾路徑改為本機路徑後，即可放入檢測批次檔
 - 由「\\[網域名稱]\\SysVol\[網域名稱]\\Policies\\{開機執行 GPO_GUID }\\Machine\\Scripts\\Startup」
 - 改成「C:\\Windows\\SYSVOL\\domain\\Policies\\{開機執行 GPO_GUID }\\Machine\\Scripts\\Startup」



電腦開機執行檢測方式(5/6)

- 選擇開機執行的檔案

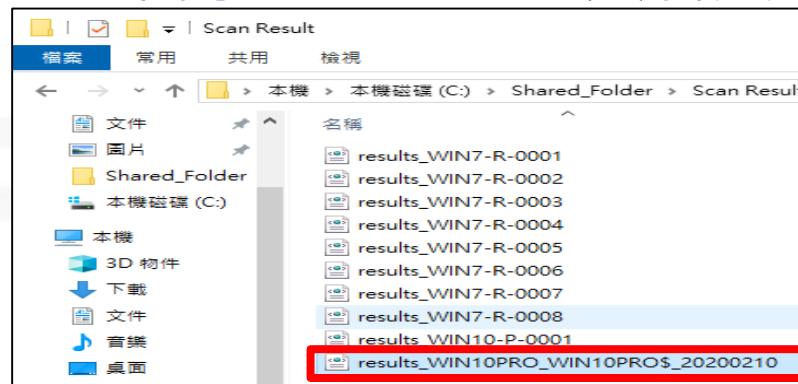
– 選擇「新增」後，點選「瀏覽」並選取前一步驟放入的檢測批次檔



- 電腦開機後，將自動執行檢測

電腦開機執行檢測方式(6/6)

- 檢測完成後，檢測報告將自動回存至AD主機 Shared_Folder 中的 Scan Result 資料夾

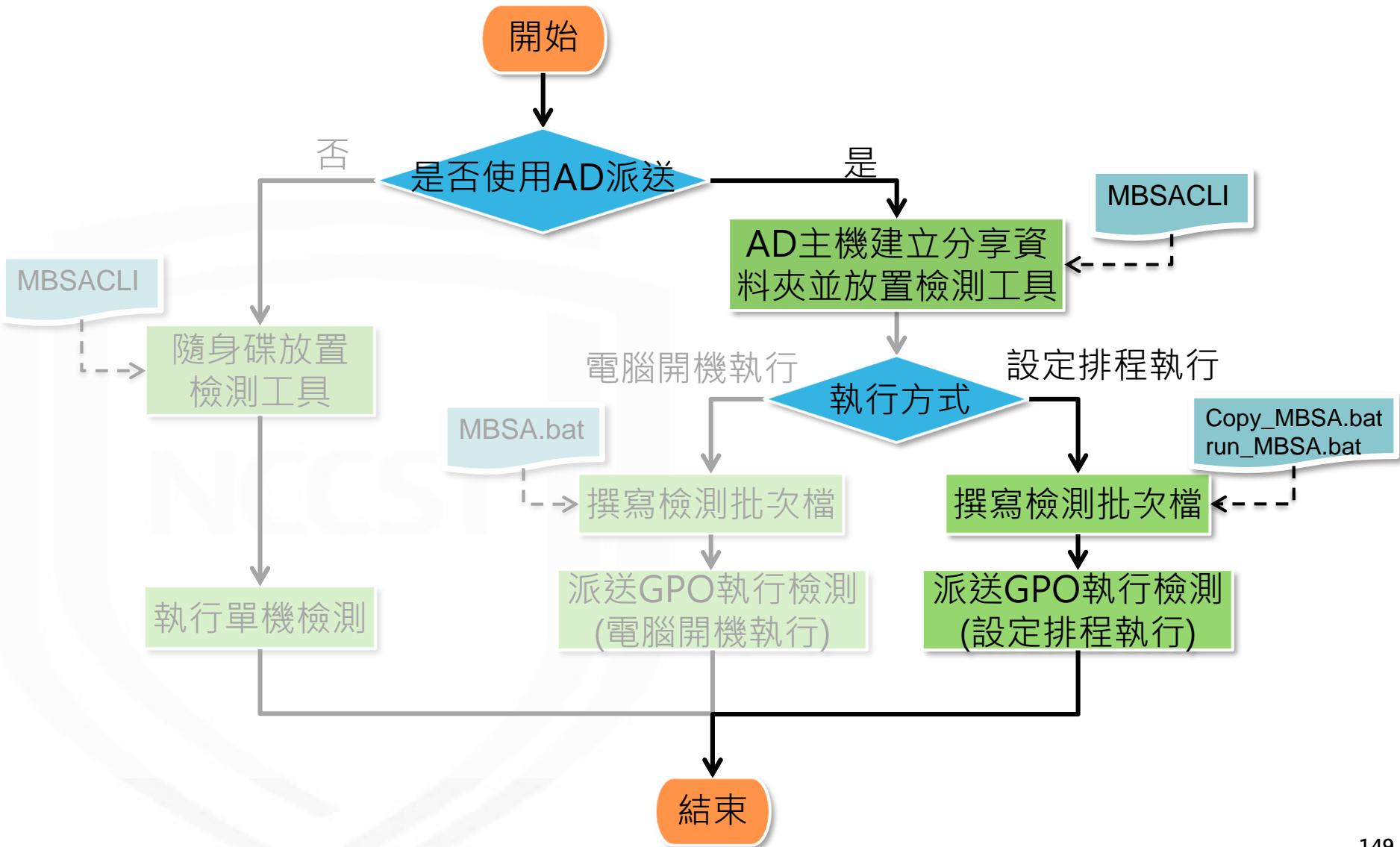


- 執行後，受測電腦中僅保留 MBSA_Result 資料夾與檢測報告，其餘檢測檔案將自動刪除



- 後續可將檢測報告上傳至 VANS 系統進行解析

安全性更新檢測流程



設定排程執行檢測方式(1/17)

● 撰寫複製檔案批次檔(copy_MBSA.bat)

```
copy_MBSA.bat
1 net use X: "\\\\"10.3.0.248\\Shared_Folder" /user:Win10User "lqaz@WSX3edc"
2
3 if exist "C:\\Users\\Public\\Documents\\MBSA\\results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2%%DATE:~8,2%.xml" (
4     xcopy /y "C:\\Users\\Public\\Documents\\MBSA\\results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2%%DATE:~8,2%.xml" "X:\\Scan Result"
5     goto end
6 ) else (
7     md "C:\\Users\\Public\\Documents\\MBSA"
8 )
9
10 if not exist "C:\\Users\\Public\\Documents\\run_MBSA.bat" (
11     xcopy /y "X:\\run_MBSA.bat" "C:\\Users\\Public\\Documents\\"
12 )
13
14 if not exist "C:\\Users\\Public\\Documents\\MBSA\\wsusscn2.cab" (
15     xcopy /y "X:\\MBSA\\wsusscn2.cab" "C:\\Users\\Public\\Documents\\MBSA"
16 )
17
18 if not exist "C:\\Users\\Public\\Documents\\MBSA\\mbsacli.exe" (
19     xcopy /y "X:\\MBSA\\mbsacli.exe" "C:\\Users\\Public\\Documents\\MBSA"
20 )
21
22 if not exist "C:\\Users\\Public\\Documents\\MBSA\\wusscan.dll" (
23     xcopy /y "X:\\MBSA\\wusscan.dll" "C:\\Users\\Public\\Documents\\MBSA"
24 )
25
26 :end
27 net use /delete X:
```

1	將Shared_Folder掛載為代號X之網路磁碟機，並設定可存取Shared_Folder之帳號密碼
3~8	判斷受測電腦的「公用文件」中是否已存在檢測報告 <ul style="list-style-type: none"> 若已有報告，則複製檢測報告XML檔至AD主機與Shared_Folder的「Scan Result」資料夾 若無報告，則於受測電腦「公用文件」建立「MBSA」資料夾
10~12	判斷受測電腦的「公用文件」中，是否包含run_MBSA批次檔。若無，則複製該批次檔至受測電腦的「公用文件」
14~24	判斷受測電腦的「公用文件」中的「MBSA」資料夾中，是否包含MBSACLI檢測所需的3個檔案。若無，則複製缺少的檔案至受測電腦的「公用文件」中的「MBSA」資料夾
27	中斷網路磁碟機(X)

設定排程執行檢測方式(2/17)

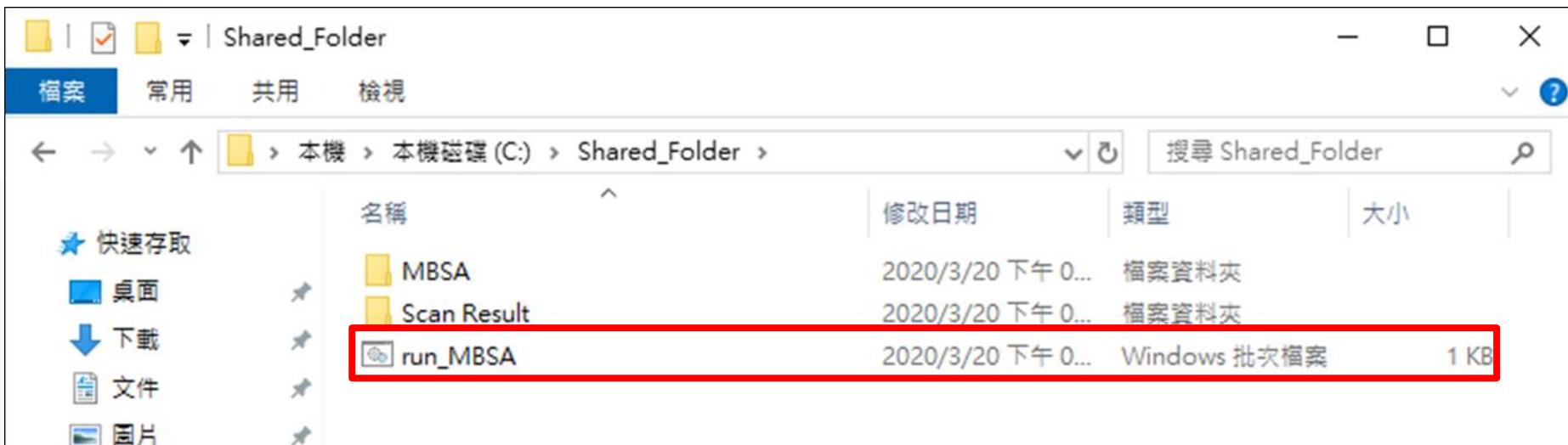
● 撰寫執行檢測作業批次檔(run MBSA.bat)

```
run_MBSA.bat [x]
1 if exist "C:\Users\Public\Documents\MBSA\results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2%%DATE:~8,2%.xml" (
2     rem ----測試MBSA檢測結果報告是否小於1KB----
3     FOR %%F IN (C:\Users\Public\Documents\MBSA\results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2%%DATE:~8,2%.xml) DO (
4         if %%~zF LSS 1024 (
5             DEL %%F
6             goto runMBSA
7         ) ELSE (
8             goto end
9         )
10    )
11 )
12
13 :runMBSA
14 md "C:\Users\Public\Documents\MBSA_Result"
15 cd "C:\Users\Public\Documents\MBSA"
16 del /Q "C:\Users\Public\Documents\MBSA\results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2%%DATE:~8,2%.xml"
17 del /Q "C:\Users\Public\Documents\MBSA\wsusscn2.cab.dat"
18 mbsacli /xmlout /catalog wsusscn2.cab /unicode /nvc >> results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2%%DATE:~8,2%.xml
19
20 xcopy /y "C:\Users\Public\Documents\MBSA\results_%computername%_%username%_%DATE:~0,4%%DATE:~5,2%%DATE:~8,2%.xml"
"C:\Users\Public\Documents\MBSA_Result\" 
21 cd \
22 :end
```

- | | |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 1~13 | 判斷受測電腦的「公用文件」中是否存在檢測報告，若已有報告或報告檔案大小大於1KB，則不執行檢測 |
| 14 | 於「公用文件」建立「MBSA_Result」資料夾 |
| 15~18 | <ul style="list-style-type: none">切換至「公用文件」中的「MBSA」資料夾並執行檢測，檢測報告以<u>電腦名稱、使用者名稱及檢測日期</u>命名檢測前，移除前次檢測報告與檢測過程中產生之dat檔 |
| 20 | 複製檢測報告XML檔至使用者電腦的「公用文件」中的「MBSA_Result」資料夾 |
| 21 | 切換至根目錄，離開MBSA資料夾 |

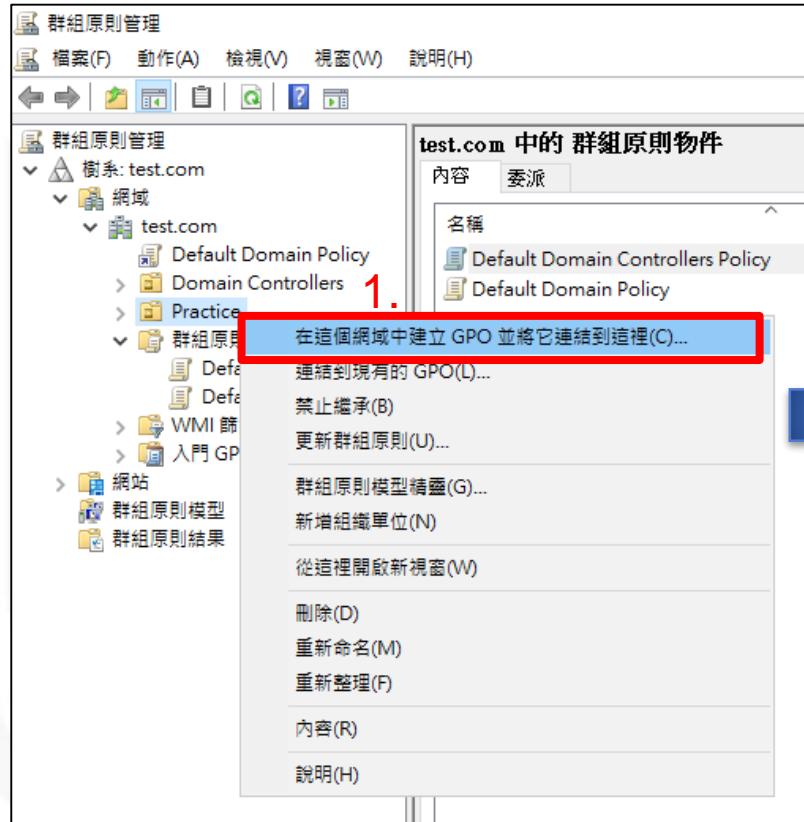
設定排程執行檢測方式(3/17)

- 於Shared_Folder放置run_MBSA批次檔，並確認Domain Users可正常存取檔案



設定排程執行檢測方式(4/17)

- 在目標網域或OU建立GPO
 - 新增「設定排程執行」GPO



設定排程執行檢測方式(5/17)

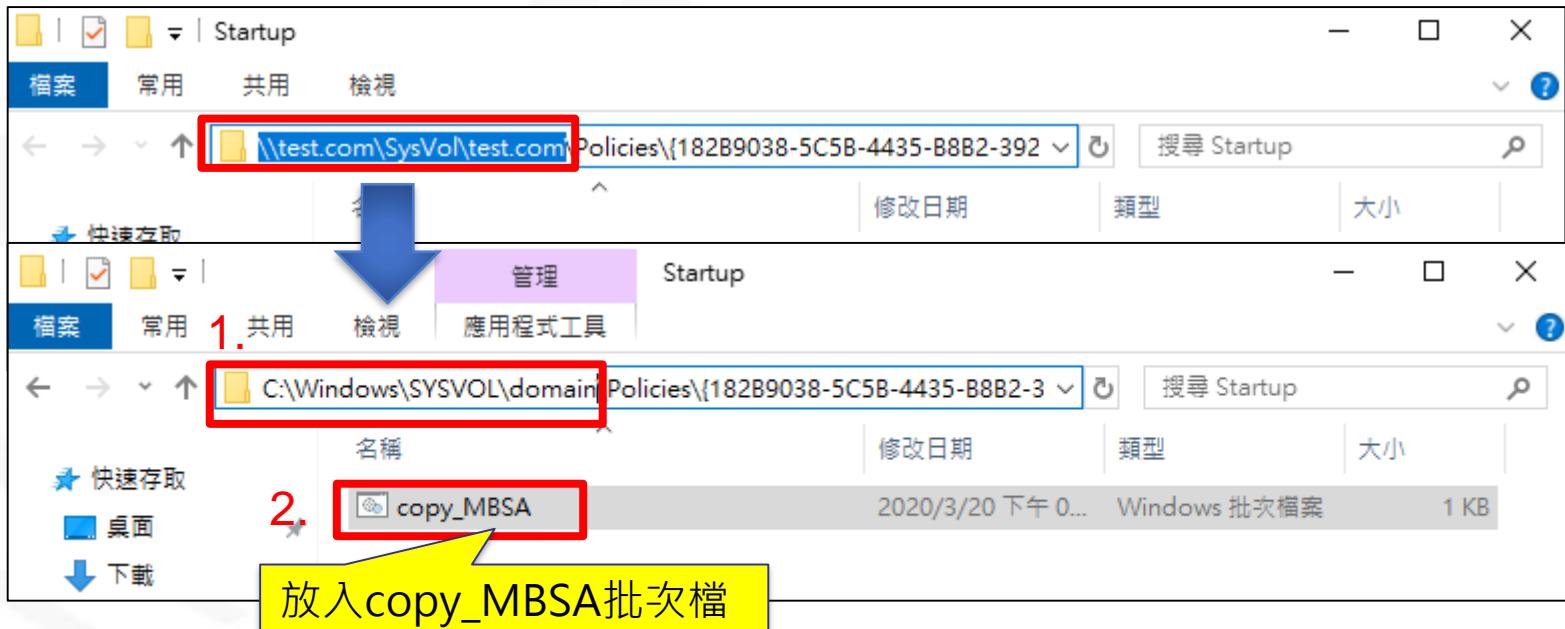
- 編輯GPO，透過排定的工作於指定時段執行MBSACLI檢測執行檔

- 點選剛建立的「排程執行」GPO，按右鍵選擇編輯
- GPO路徑為「電腦設定\原則\Windows設定\指令碼 - (啟動/關機)\啟動」
- 點選「顯示檔案」，準備放入檢測批次檔



設定排程執行檢測方式(6/17)

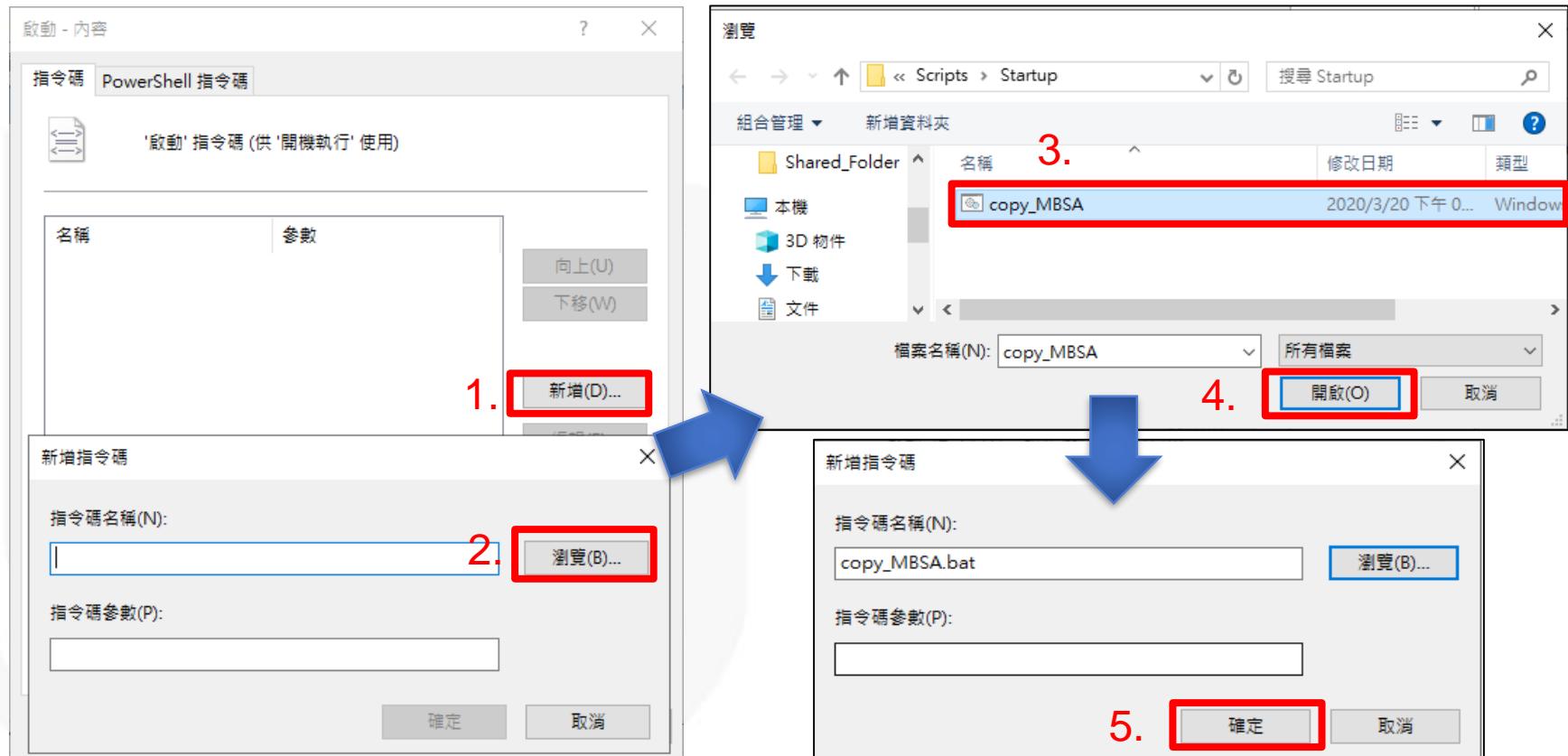
- 因作業系統預設不允許直接複製檔案至網路位置，故須將資料夾路徑改為本機路徑，即可放入批次檔
 - 由「\\[網域名稱]\\SysVol\[網域名稱]\\Policies\\{開機執行 GPO_GUID }\\Machine\\Scripts\\Startup」
 - 改成「C:\\Windows\\SYSVOL\\domain\\Policies\\{開機執行 GPO_GUID }\\Machine\\Scripts\\Startup」



設定排程執行檢測方式(7/17)

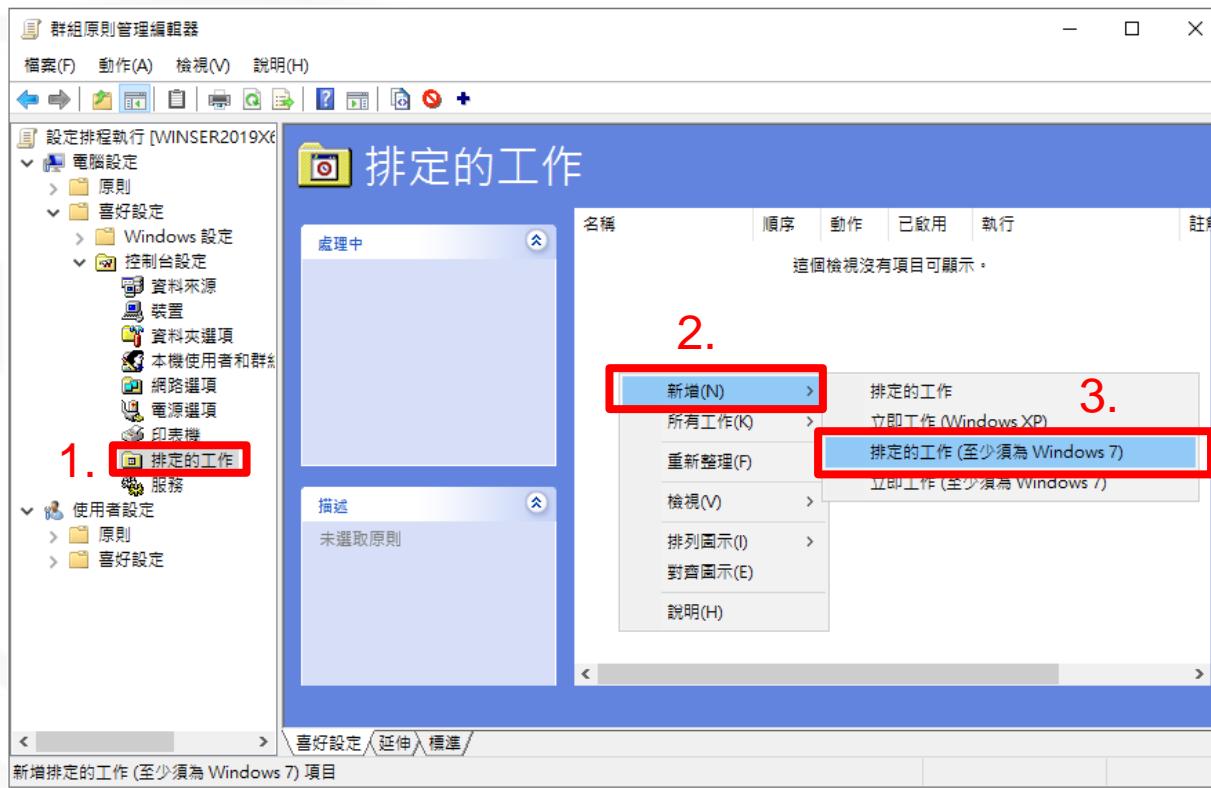
- 選擇開機執行的批次檔(copy_MBSA.bat)

– 選擇「新增」後，點選「瀏覽」並選取前一步驟放入的批次檔



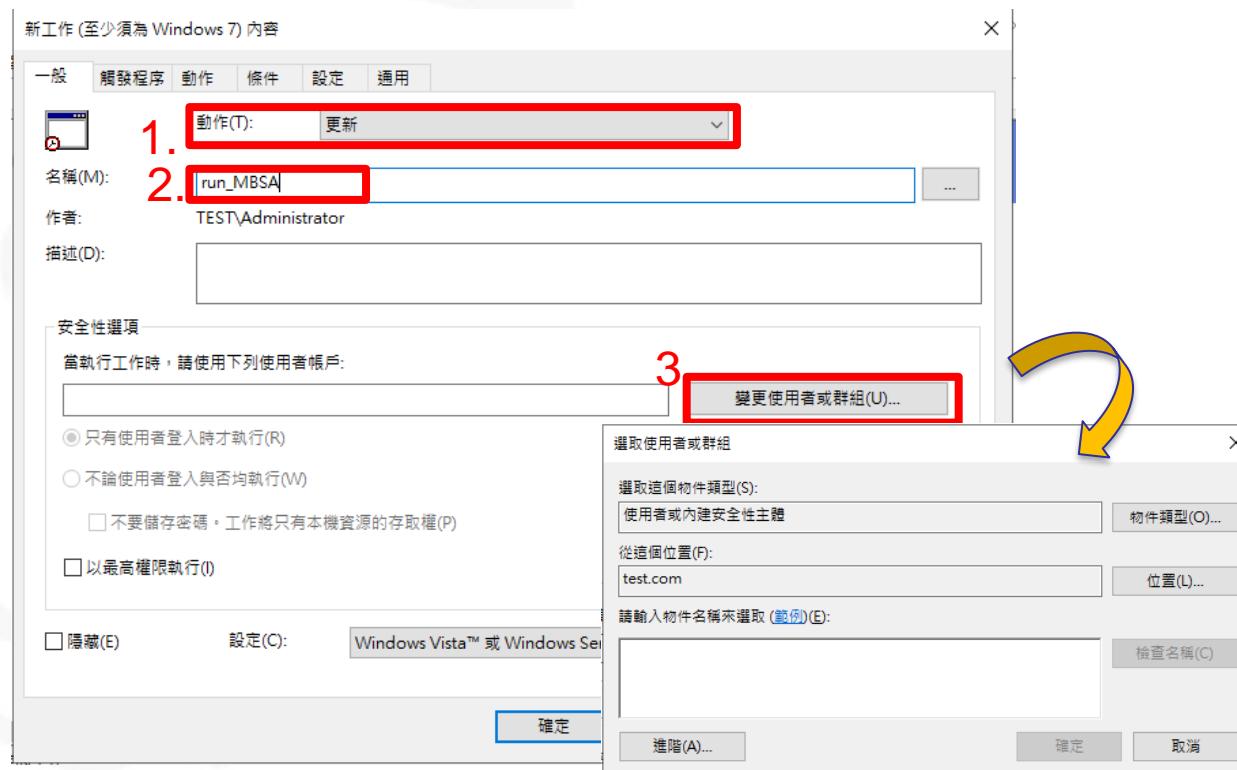
設定排程執行檢測方式(8/17)

- 編輯GPO，透過排定的工作於指定時段執行MBSACLI檢測之批次檔(run_MBSA.bat)
 - GPO路徑為「電腦設定\喜好設定\控制台設定\排定的工作」
 - 於右側視窗按右鍵選擇「新增 → 排定的工作(至少須為Windows 7)」



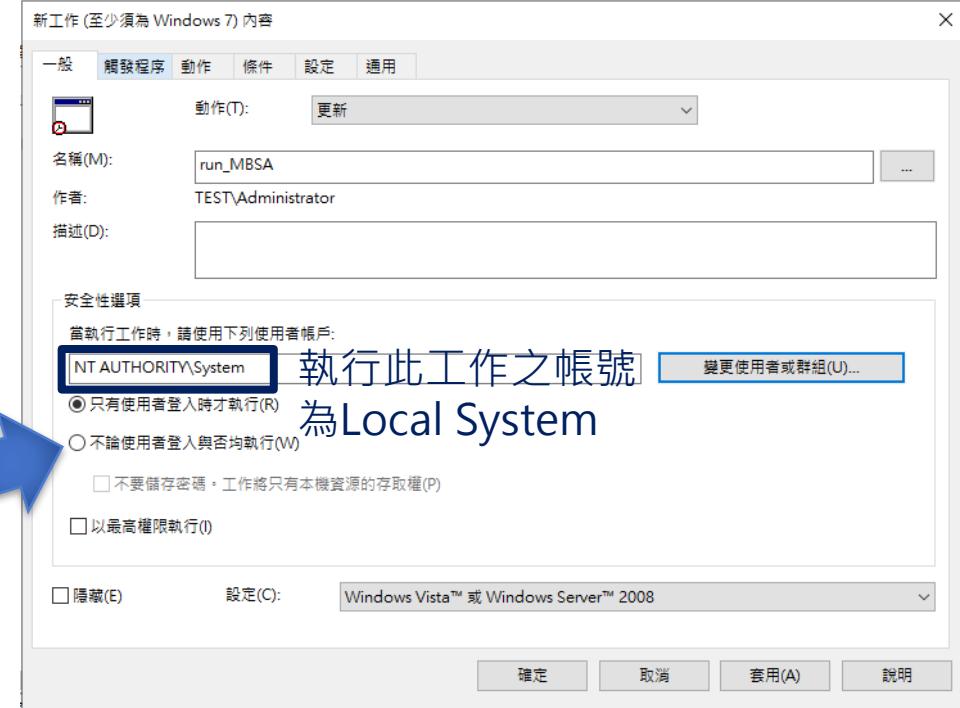
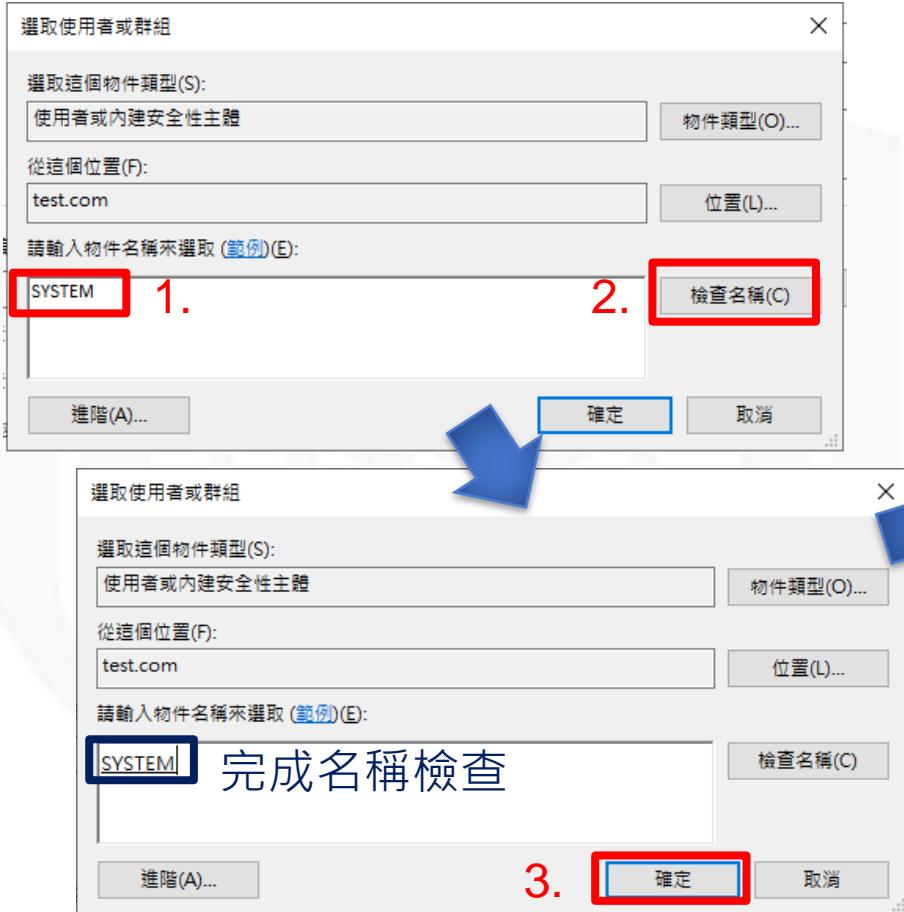
設定排程執行檢測方式(9/17)

- 於「新工作(至少須為Windows 7)內容」視窗中，進行下列設定：
 - 「動作」選擇「更新」
 - 於「名稱」欄位鍵入任務排程之名稱(例如：run_MBSA)
 - 由於MBSA需要至少管理者權限方可成功執行檢測，故選取「變更使用者或群組」按鈕



設定排程執行檢測方式(10/17)

- 於「選取使用者或群組」視窗，輸入「SYSTEM」並點選「檢查名稱」按鈕進行名稱檢查後按下確定，即可指定以Local System帳號執行此排程工作



執行此工作之帳號

為Local System

設定排程執行檢測方式(11/17)

- 為使一般使用者可於未登入之狀態下，仍可執行排程工作，勾選「**不論使用者登入與否均執行**」
- 勾選「**以最高權限執行**」，使指定的程式以最高權限啟動
- 調整設定工作的作業系統為**Windows 7、Windows Server 2008R2**



設定排程執行檢測方式(12/17)

- 切換至「觸發程序」頁籤，並點選「新增」
- 於「新增觸發程序」視窗，設定工作開始時間

1.



設定排程執行檢測方式(13/17)

- 切換至「動作」頁籤，並點選「新增」
- 於「新增動作」視窗，鍵入「程式或指令碼位置」與「啟動位置」
 - 透過工作排程器呼叫bat檔之預設路徑在「C:\Windows\SYSTEM32」，因此需鍵入放置批次檔之本機公用文件資料夾位置(例如：
C:\Users\Public\Documents\run_MBSA.bat)



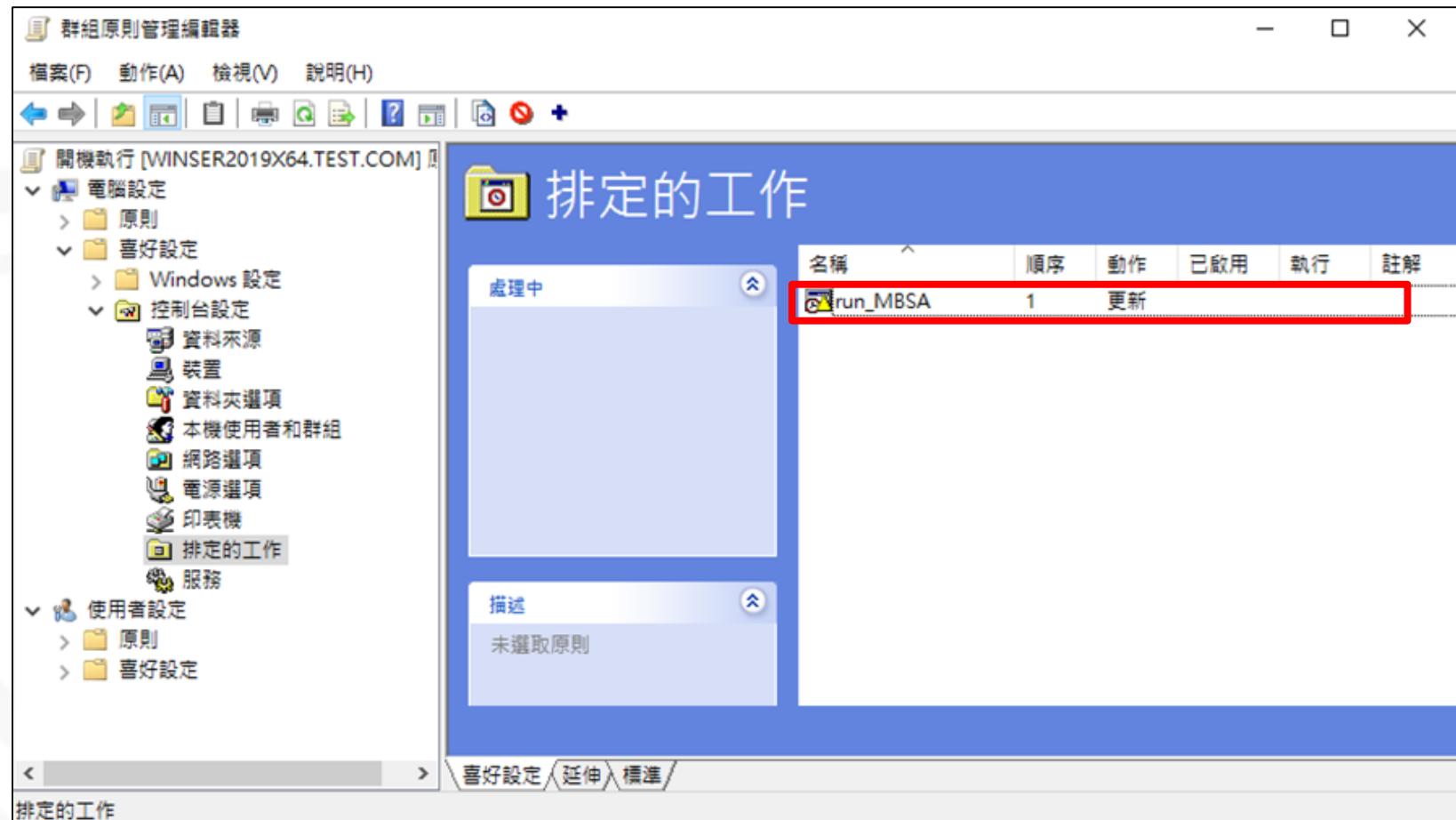
設定排程執行檢測方式(14/17)

- 切換至「設定」頁籤，勾選「在錯過排定的啟動後盡快執行工作」
 - 當因電腦關閉或工作排程器服務忙碌而無法啟動工作時，工作排程器服務預設將等待10分鐘後再次啟動工作
- 設定完成後，按下確定



設定排程執行檢測方式(15/17)

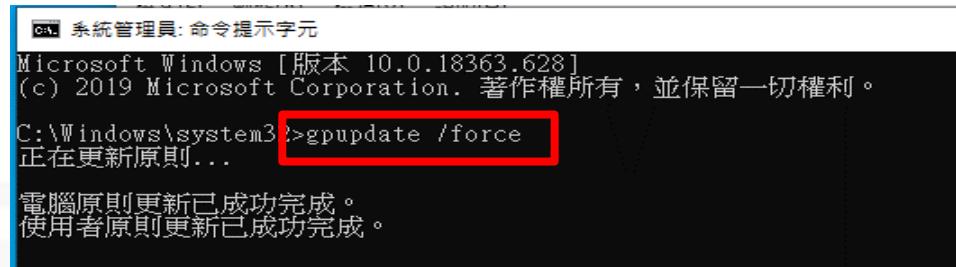
● 完成排程工作設定



設定排程執行檢測方式(16/17)

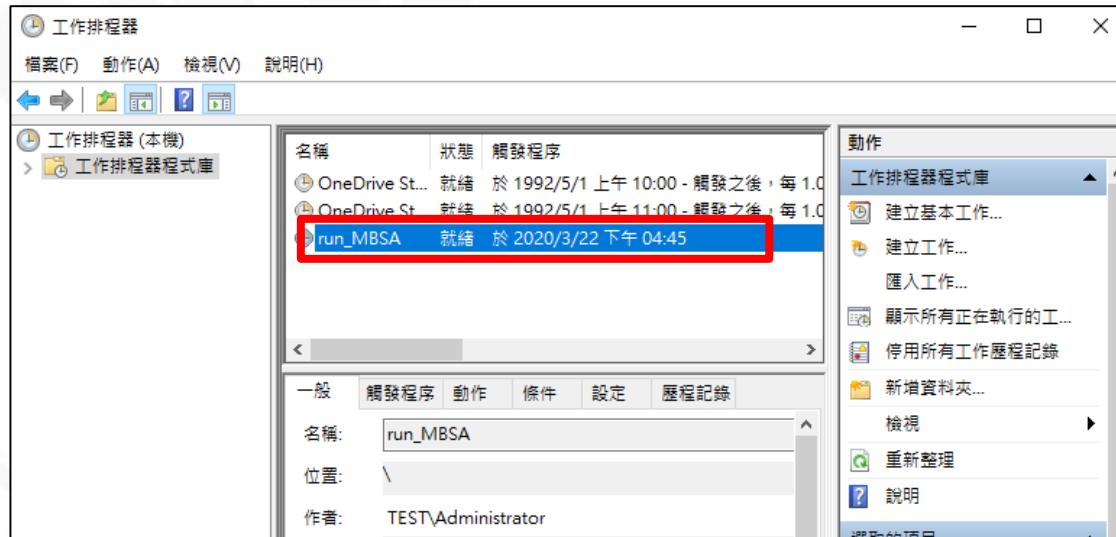
- 受測電腦端更新群組原則

- gpupdate /force



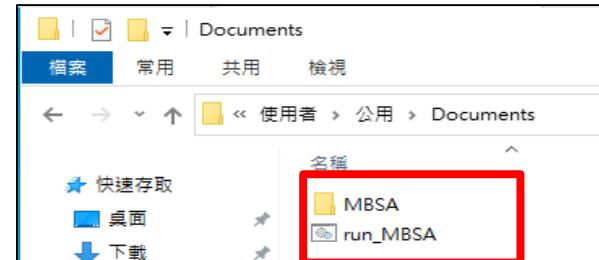
```
系統管理員: 命令提示字元
Microsoft Windows [版本 10.0.18363.628]
(c) 2019 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\Windows\system32>gpupdate /force
正在更新原則...
電腦原則更新已成功完成。
使用者原則更新已成功完成。
```

- 群組原則更新完畢後，可於受測電腦開啟工作排程器檢視排程狀態

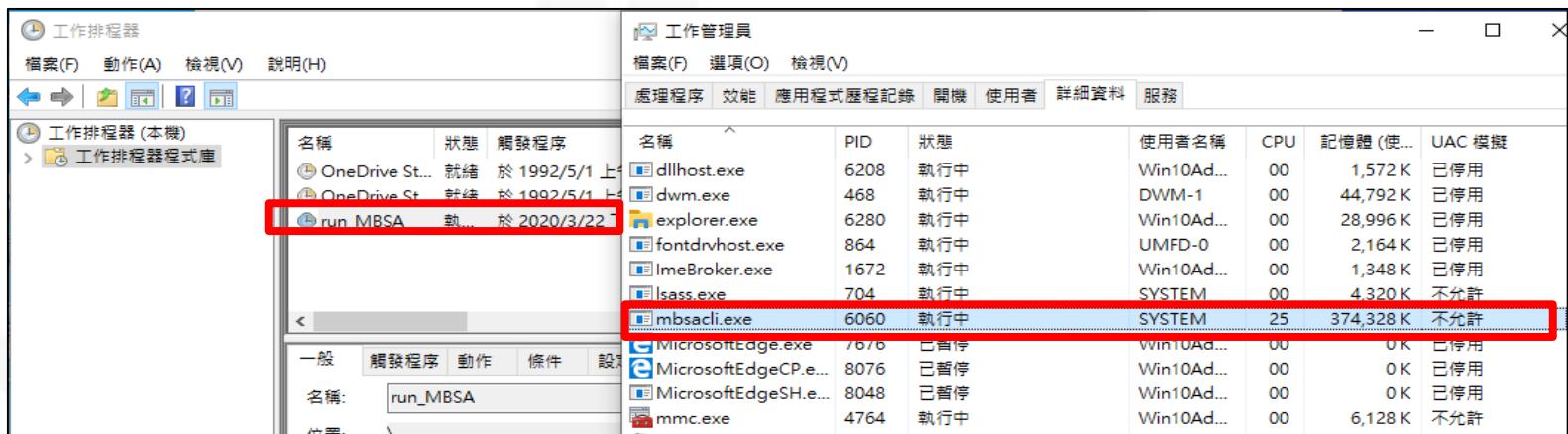


設定排程執行檢測方式(17/17)

- 受測電腦下次開機時，將自動複製MBSA資料夾與 run_MBSA.bat至公用文件資料夾中



- MBSACLI檢測作業將於指定排程時間執行，並於下次開機時自動將報告回傳至AD主機Shared_Folder中的Scan Result資料夾



名稱	PID	狀態	使用者名稱	CPU	記憶體 (使...)	UAC 模擬
dllhost.exe	6208	執行中	Win10Ad...	00	1,572 K	已停用
dwm.exe	468	執行中	DWM-1	00	44,792 K	已停用
explorer.exe	6280	執行中	Win10Ad...	00	28,996 K	已停用
fontdrvhost.exe	864	執行中	UMFD-0	00	2,164 K	已停用
ImeBroker.exe	1672	執行中	Win10Ad...	00	1,348 K	已停用
lsass.exe	704	執行中	SYSTEM	00	4,320 K	不分許
mbsaci.exe	6060	執行中	SYSTEM	25	374,328 K	不允許
MicrosoftEdge.exe	7676	已暫停	Win10Ad...	00	0 K	已停用
MicrosoftEdgeCP.e...	8076	已暫停	Win10Ad...	00	0 K	已停用
MicrosoftEdgeSH.e...	8048	已暫停	Win10Ad...	00	0 K	已停用
mmc.exe	4764	執行中	Win10Ad...	00	6,128 K	不允許

- 後續可將檢測報告上傳至VANS系統進行解析



實作練習5

網域派送檢測

實作練習5：網域派送檢測(環境說明)

● 環境說明

- VM名稱：實作練習_Windows Server 2019(AD主機，進行網域派送)
 - 帳號：TEST\Administrator
 - 密碼：1qaz@WSX3edc
- VM名稱：實作練習_Windows 10 x64(網域內電腦)
 - 帳號：TEST\win10user
 - 密碼：1qaz@WSX3edc

● 指令範本

- 位置：桌面\02.安全性更新管理機制\指令範本
 - 網域派送檢測



實作練習5：網域派送檢測

- 於「實作練習_Windows Server 2019」，進行網域派送**排程執行檢測**
- 本項練習時間：**45分鐘**

項次	執行項目
1	於Shared_Folder資料夾確認資料夾權限，並放置檢測相關檔案(請參考P.137~P.141)
2	請依 設定排程執行檢測方式 教學步驟進行相關設定(請參考P.149~P.166)
3	請於受測電腦「實作練習_Windows 10 x64」更新群組原則，並確認任務排程器中新增MBSA的排程工作
4	請重啟受測電腦並確認於指定排程時間會自動進行MBSACLI檢測
5	完成檢測後，請重啟受測電腦並確認報告是否回傳至AD主機分享資料夾

實作練習5：常見問答(1/4)

Q1

已確認受測電腦皆成功套用GPO，但為何有些受測電腦開機時仍不會執行檢測？

- 以電腦開機方式檢測時，當電腦開機完畢即執行GPO派送之批次檔，若有下列情形可能導致受測電腦無法如期進行檢測：
 - 受測電腦之網路環境較慢，無法於開機完成後立即連線至AD主機之分享資料夾
 - 受測電腦使用外接式網卡連線至網路，無法於開機完成後立即連線至AD主機的分享資料夾
- 參考解決方案：
 - 方法一：改以排程方式執行檢測
 - 方法二：將批次檔分為兩個
 - 批次檔A：複製MBSACLI檔案至受測電腦
 - 批次檔B：受測電腦呼叫其電腦中的MBSACLI執行檢測並回傳報告

電腦關機時執行

電腦開機時執行

實作練習5：常見問答(2/4)

Q2

wsusscn2.cab更新資料庫高達842MB左右，若同時執行檢測，恐造成網路壅塞之情況

- 參考解決方案：

- 建議可分批執行檢測，例如依照網域組織單位(OU)進行劃分與派送

Q3

透過電腦開機方式派送後，每次電腦開機後都會執行檢測，可否每台電腦僅檢測一次？

- 參考解決方案：

- 可於受測電腦留存檢測報告，並於批次檔增加判斷式，當受測電腦有檢測報告時略過檢測

- if exist

- "C:\Users\Public\Documents\MBSA_Result\results_%computername%.xml"

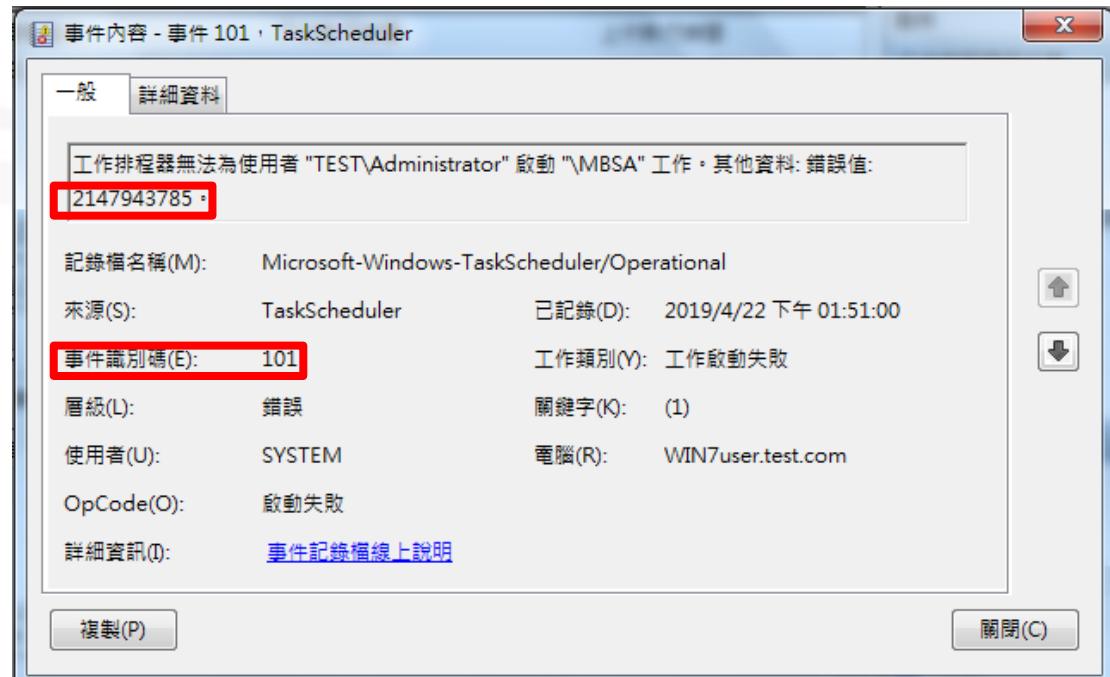
- goto P

- 此方法須留意當MBSA檢測異常中斷或檢測失敗時，該受測電腦將不會再次執行檢測

實作練習5：常見問答(3/4)

Q4

執行排程工作時出現如下圖之工作啟動失敗錯誤，事件識別碼為101，錯誤值為2147943785



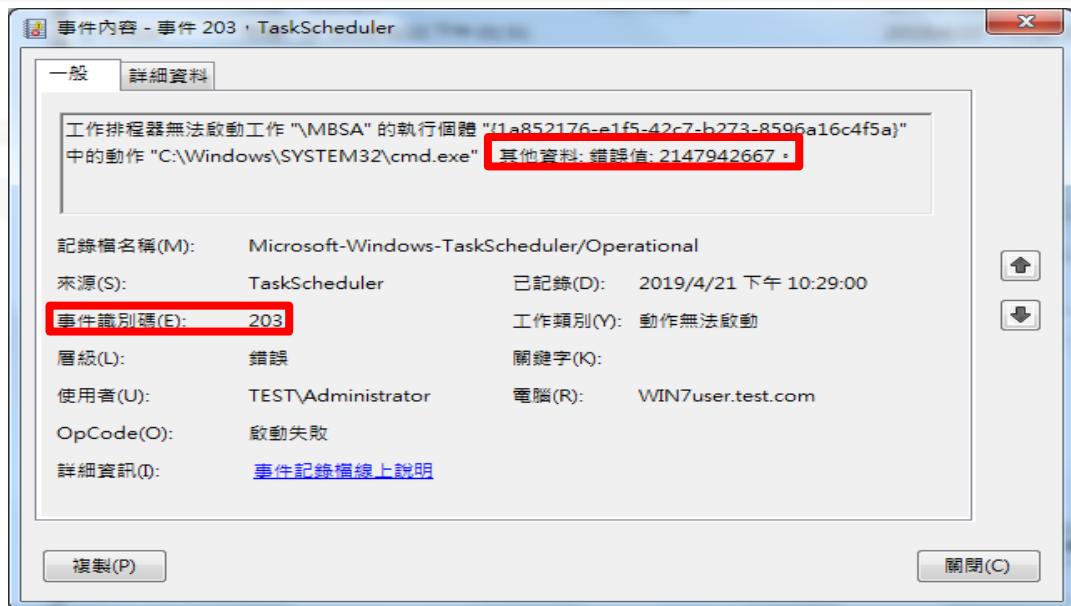
● 參考解決方案：

- 若套用下列組態設定可能導致工作啟動失敗，應視需求調整其設定值。
 - 電腦設定\Windows設定\安全性設定\本機原則\使用者權限指派\以批次工作登入

實作練習5：常見問答(4/4)

Q5

執行排程工作時出現如下圖之工作啟動失敗錯誤，事件識別碼為203，錯誤值為2147942667

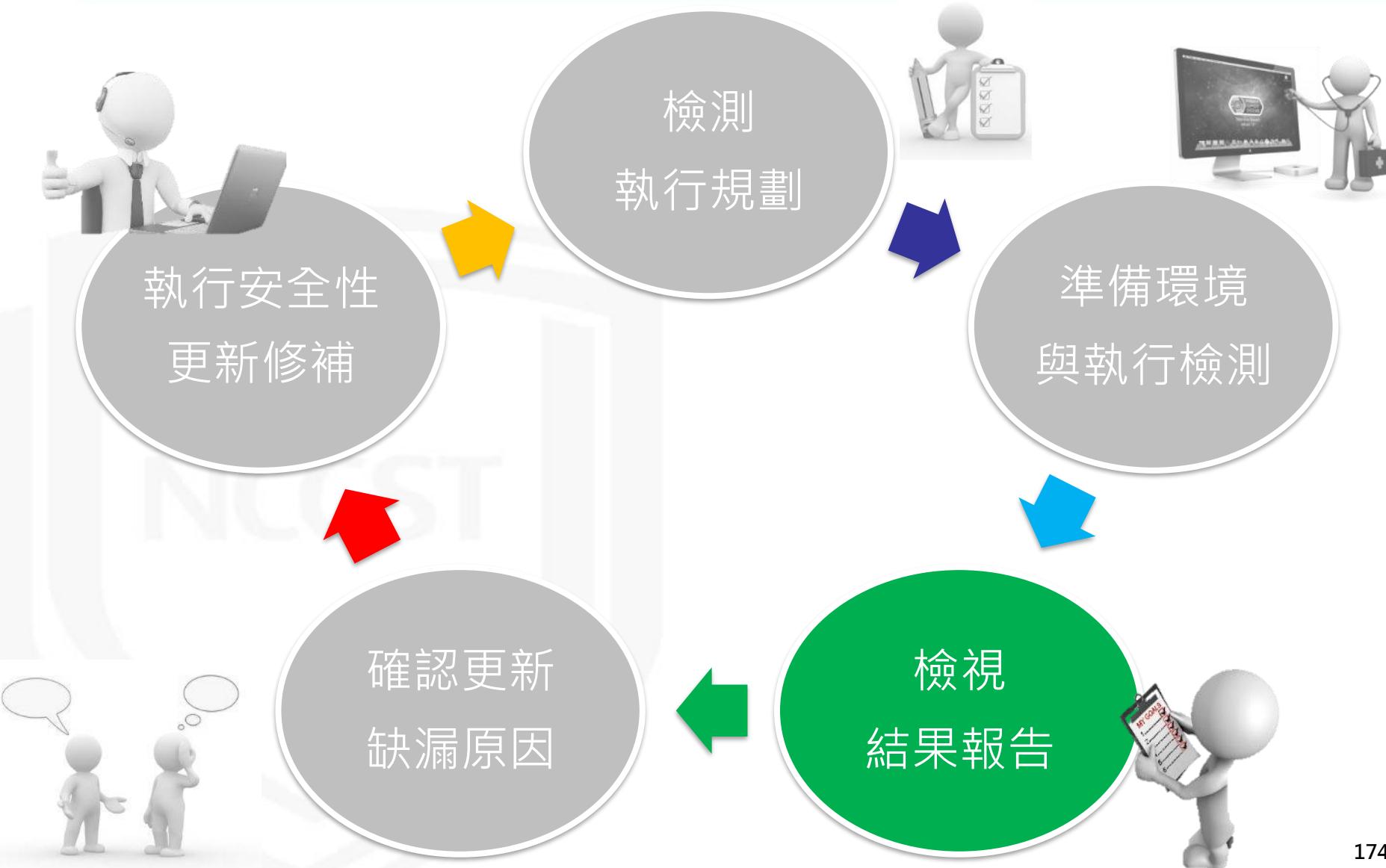


● 參考解決方案：

- 請於「一般」頁籤確認未勾選「不要儲存密碼」。工作將只有本機資源存取權」選項
- 請於「動作」頁籤確認下指定之批次檔路徑是否正確

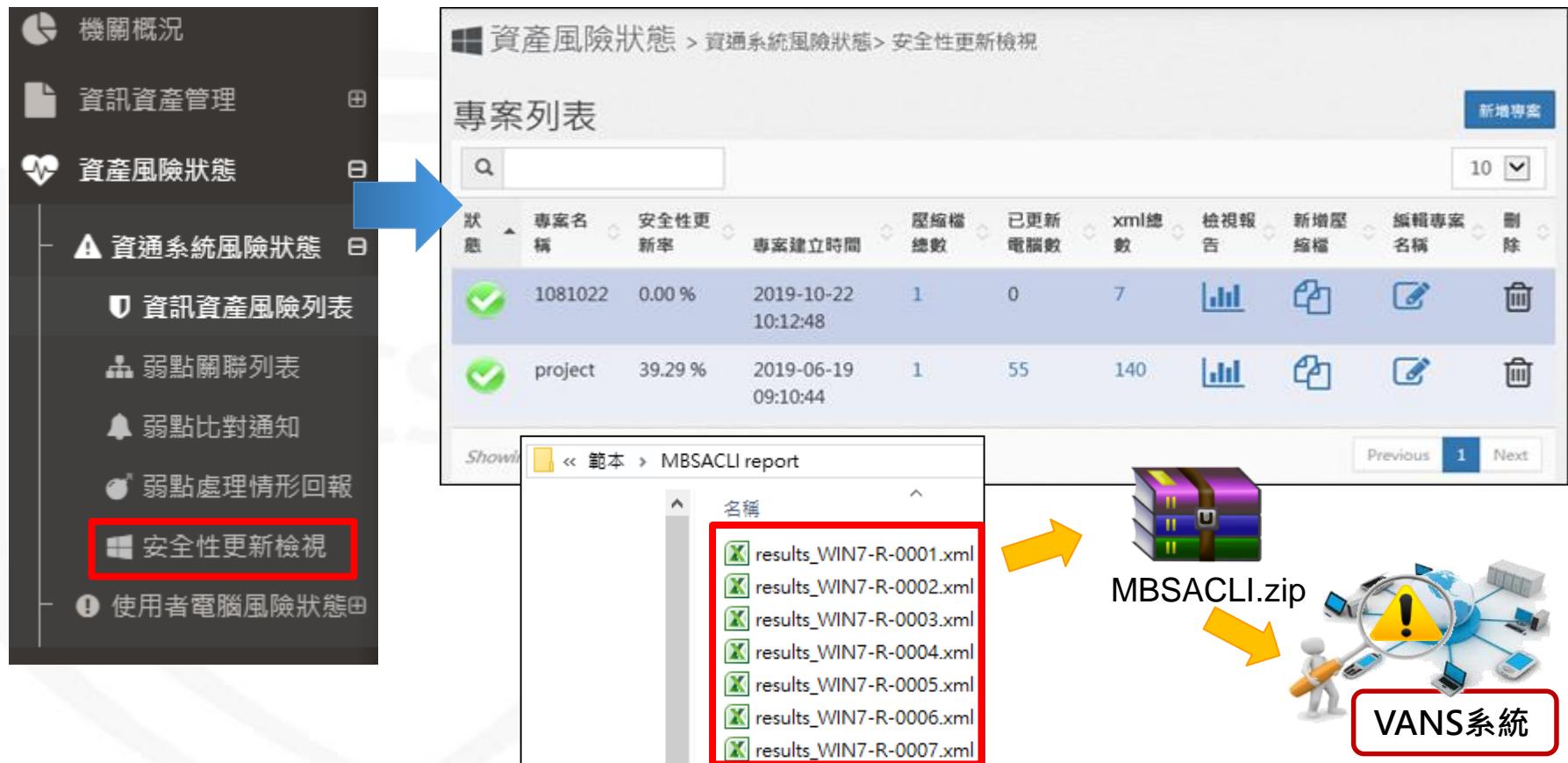


安全性更新管理機制作業流程



以VANS分析檢測報告(1/8)

- VANS系統提供「安全性更新檢視」功能，可將多份MBSACLI檢測報告打包為壓縮檔後上傳，並檢視解析結果



The screenshot illustrates the VANS system's 'Security Update Review' feature. On the left, a navigation sidebar lists various modules: 機關概況, 資訊資產管理, 資產風險狀態, 資通系統風險狀態 (highlighted with a red box), 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, 安全性更新檢視 (highlighted with a red box), and 使用者電腦風險狀態。A blue arrow points from the 'Security Update Review' item in the sidebar to the main content area.

The main content area shows the 'Asset Risk Status > Communication System Risk Status > Security Update Review' page. It displays a 'Case List' grid with columns: 狀態, 專案名稱, 安全性更新率, 專案建立時間, 壓縮檔總數, 已更新電腦數, XML總數, 檢視報告, 新增壓縮檔, 編輯專案名稱, and 刪除. Two cases are listed:

狀態	專案名稱	安全性更新率	專案建立時間	壓縮檔總數	已更新電腦數	XML總數	檢視報告	新增壓縮檔	編輯專案名稱	刪除
✓	1081022	0.00 %	2019-10-22 10:12:48	1	0	7				
✓	project	39.29 %	2019-06-19 09:10:44	1	55	140				

A modal window titled 'Show' (範本) displays a list of XML files under the heading 'MBSACLI report': results_WIN7-R-0001.xml, results_WIN7-R-0002.xml, results_WIN7-R-0003.xml, results_WIN7-R-0004.xml, results_WIN7-R-0005.xml, results_WIN7-R-0006.xml, and results_WIN7-R-0007.xml. These files are highlighted with a red box.

To the right, there is a graphic illustrating the process: a stack of three colored boxes labeled 'MBSACLI.zip' is connected by arrows to a magnifying glass over a network of devices, symbolizing the analysis of the compressed report. A small figure holding a magnifying glass is also shown. The entire graphic is enclosed in a red box with the text 'VANS系統'.

以VANS分析檢測報告(2/8)

- 透過新增專案，鍵入專案名稱與專案描述，將多份 MBSACLI 檢測報告壓縮後上傳



The screenshot shows two pages of the VANS system:

- Top Page (Project List):** Shows a search bar and a 'New Project' button (highlighted with a red box). A large blue arrow points down from this page to the second page.
- Bottom Page (Add Project):**
 - Step 1:** Shows the 'New Project' button highlighted with a red box.
 - Step 2:** Shows the 'Project Name' field highlighted with a red box.
 - Step 3:** Shows the 'Browse...' button highlighted with a red box.
 - Step 4:** Shows the 'Add Project' button highlighted with a red box.

注意事項:

- 請將多份MBSACLI(MBSA的Command Line模式)檢測結果報告(XML檔)壓縮後上傳。
- 單次上傳壓縮檔大小限制為**20MB** 以內，若檔案太大請分次上傳。
- 同一專案內，不可重複上傳同檔名之**MBSACLI**檢測結果報告。

以VANS分析檢測報告(3/8)

- 專案列表頁面列出所有專案項目，可於此頁面檢視專案狀態、專案名稱、安全性更新率、專案建立時間、壓縮檔總數、已更新電腦數、XML總數...等欄位

專案列表											新增專案
狀態	專案名稱	安全性 更新率	專案建立時間	壓縮檔 總數	已更新 電腦數	xml 總數	檢視 報告	新增壓 縮檔	編輯專 案名稱	刪除	
	Project01	0.00 %	2019-01-28 02:47:33	2	0	2					
	fileload zip	0.00 %	2019-01-15 09:42:57	1	0	15					
	test111	6.67 %	2019-01-15 09:42:22	2	1	15					
	testMBSAGUI	0.00 %	2019-01-07 09:27:10	2	0	5					

以VANS分析檢測報告(4/8)

- 專案列表頁面之「狀態」欄位，可檢視各專案最近一次上傳的壓縮檔解析進度與壓縮檔是否符合規範

資產風險狀態 > 資通系統風險狀態> 安全性更新檢視

狀態	說明
	正在解析MBSACLI檢測結果
	解析完成，檔案無誤
	解析完成，檔案有誤：有重複檔名的XML報告
	解析完成，檔案有誤：請確認「壓縮檔總數」與「xml總數」內的錯誤訊息

新增專案 10 編輯專案名稱 刪除 專案名稱 Project test11 testMBSAGUI 0.00 % 2019-01-07 09:27:10 2 0 5

以VANS分析檢測報告(5/8)

- 「安全性更新率」為本專案中的電腦更新比例

資產風險狀態 > 資通系統風險狀態 > 安全性更新檢視

專案列表

新增專案

狀態	專案名稱	安全性更新率	專案建立時間	壓縮檔總數	已更新電腦數	xml總數	檢視報告	新增壓縮檔	編輯專案名稱	刪除
	1080807test	38.10 %	2019-08-07 05:29:59	2	56	147				



$$\text{安全性更新率} = \frac{\text{已更新電腦數}}{\text{XML總數}} \times 100\%$$

以VANS分析檢測報告(6/8)

- 「已更新電腦數」為已完整安裝安全性更新的電腦數，並可點選檢視已更新電腦列表

資產風險狀態 > 資通系統風險狀態> 安全性更新檢視

專案列表

新增專案

10

狀態	專案名稱	安全性更新率	專案建立時間	壓縮檔總數	已更新電腦數	xml總數	檢視報告	新增壓縮檔	編輯專案名稱	刪除
	1080807test	38.10 %	2019-08-07 05:29:59	2	56	147				

已更新電腦列表

編號	電腦名稱
1	4.MBSA_120813-PC-CTTI_20190121.xml
2	4.MBSA_120821-PC-CTTI_20190121.xml
3	4.MBSA_120823-VM-CTTI_20190120.xml

以VANS分析檢測報告(7/8)

- 「檢視報告」呈現各電腦的MBSACLI檢測結果
 - 點選後跳轉至「電腦更新情形列表」，顯示各電腦缺漏安全性更新列表
 - 點選「安全性更新說明連結」將開啟該安全性更新之Microsoft官方說明網頁

資產風險狀態 > 資通系統風險狀態> 安全性更新檢視

專案列表

狀態	專案名稱	安全性更新率	專案建立時間	壓縮檔總數	已更新電腦數	xml總數	檢視報告	新增壓縮檔	編輯專案名稱	刪除
	1080807test	38.10 %	2019-08-07 05:29:59	2	56	147				

資產風險狀態 > 資通系統風險狀態> 安全性更新檢視> 同服器主機更新情形列表

專案名稱: 1080807test
4.MBSA_120204-PC-CTTI_20190121

KBID	安全性更新類別	安全性更新名稱
2289078	Office	Security Update for Microsoft Office 2010 Bit Edition
2345000	Office	Security Update for Microsoft Word 2010 Edition

MS10-105 : 說明 Microsoft Office 2010 安全性更新 : 2010 年 12 月 14 日

Severity: [Safety Update for Microsoft Office 2010 Bit Edition](http://support.microsoft.com/kb/2289078)

Severity: [Security Update for Microsoft Word 2010 Edition](http://support.microsoft.com/kb/2345000)

以VANS分析檢測報告(8/8)

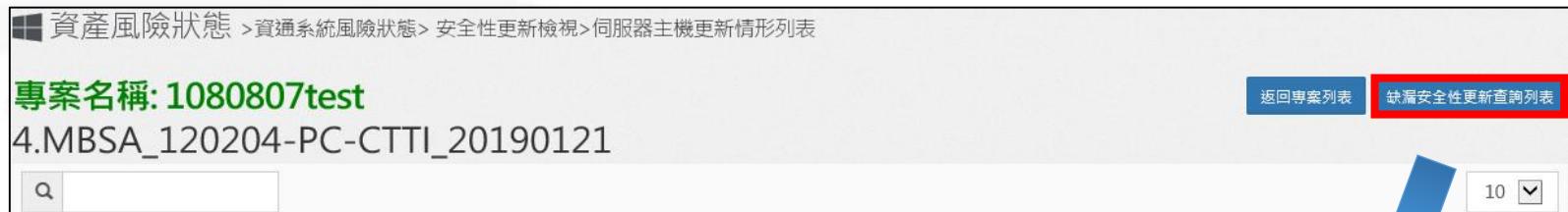
- 於電腦更新情形列表點選「**缺漏安全性更新查詢列表**」按鈕，可檢視各安全性更新分別有哪些電腦有缺漏更新
 - 點選「**安全性更新說明連結**」將連至Microsoft針對該安全性更新的說明網頁

資產風險狀態 > 資通系統風險狀態 > 安全性更新檢視 > 電腦主機更新情形列表

專案名稱: 1080807test

4.MBSA_120204-PC-CTTI_20190121

[返回專案列表](#) [缺漏安全性更新查詢列表](#)



資產風險狀態 > 資通系統風險狀態 > 安全性更新檢視 > 缺漏安全性更新查詢列表

專案名稱: 1080807test

KBID	安全性更新類別	安全性更新
4486458	Windows	2019-01 Servicing Stack Update 1703 for x64-based Sys

缺漏本更新之報告名稱 :

4.MBSA_171040-NB-CTTI_20190119 4.MBSA_171040

KBID	安全性更新類別	安全性更新
4481481	Windows	2019-01 Security Only Update 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1

[Microsoft](#)

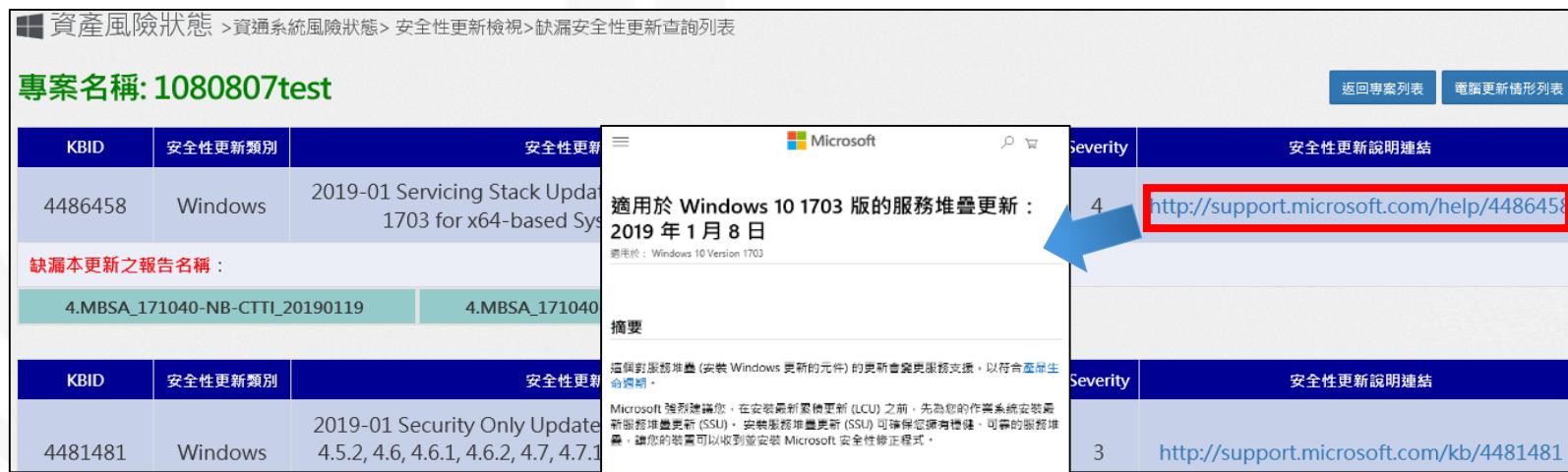
適用於 Windows 10 1703 版的服務堆疊更新 : 2019 年 1 月 8 日
適用於 : Windows 10 Version 1703

摘要

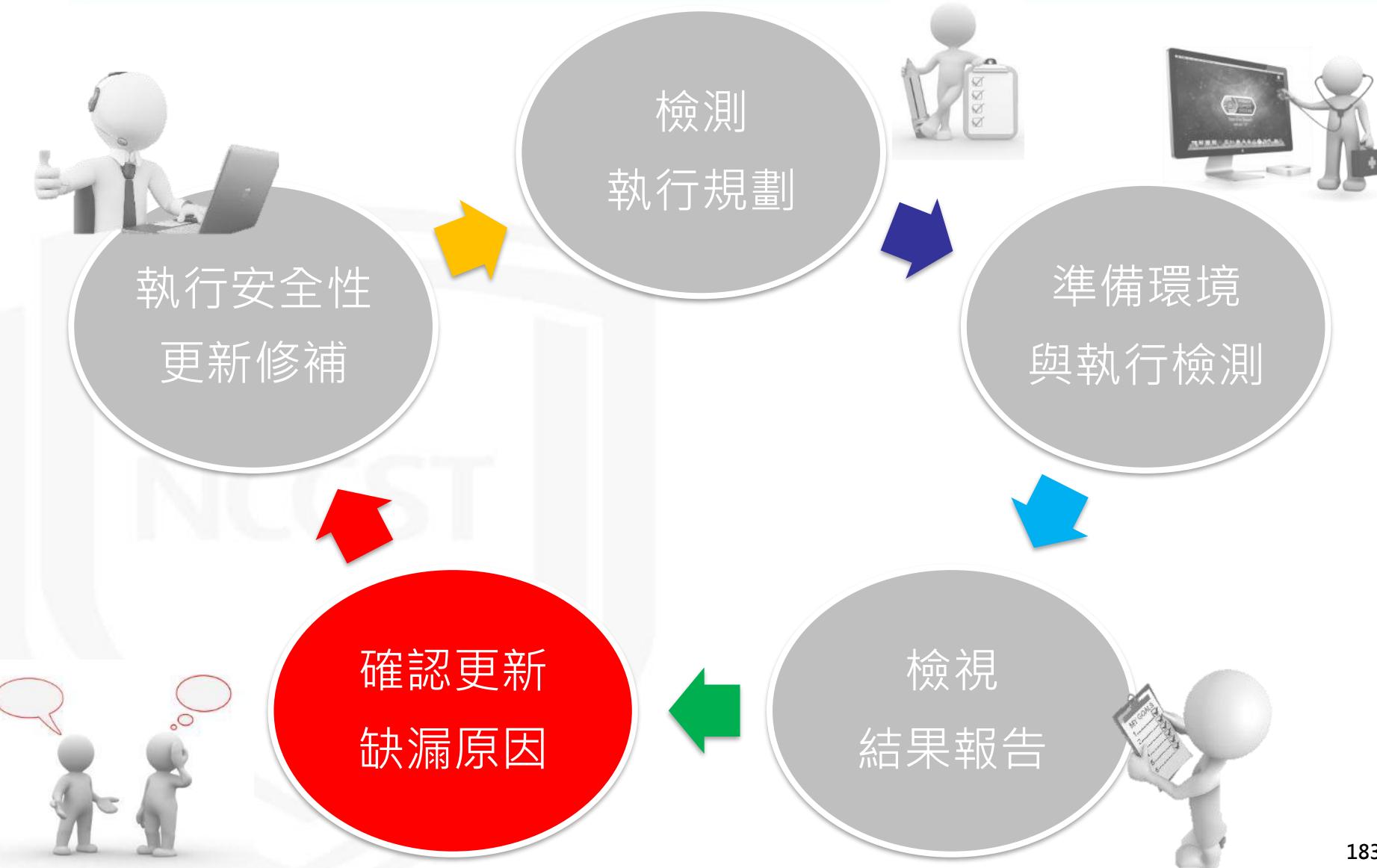
這個對服務堆疊 (安裝 Windows 更新的元件) 的更新會變更服務支援，以符合**藍色生命周期**。

Microsoft 強烈建議您，在安裝最新累積更新 (LCU) 之前，先為您的作業系統安裝最新服務堆疊更新 (SSU)。安裝服務堆疊更新 (SSU) 可確保您擁有穩健、可靠的服務堆疊，讓您的裝置可以收到並安裝 Microsoft 安全性修正程式。

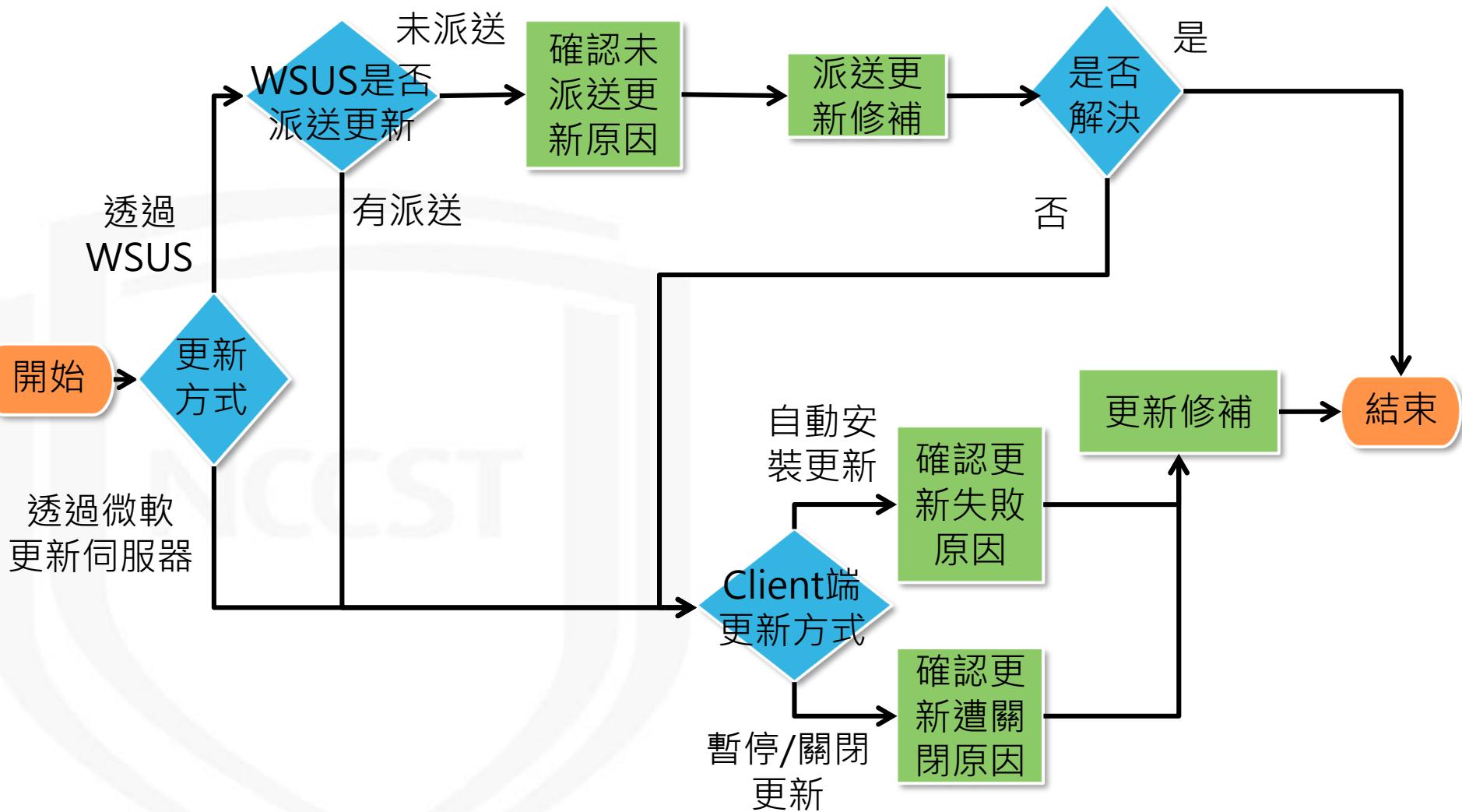
Severity	安全性更新說明連結
4	http://support.microsoft.com/help/4486458
3	http://support.microsoft.com/kb/4481481



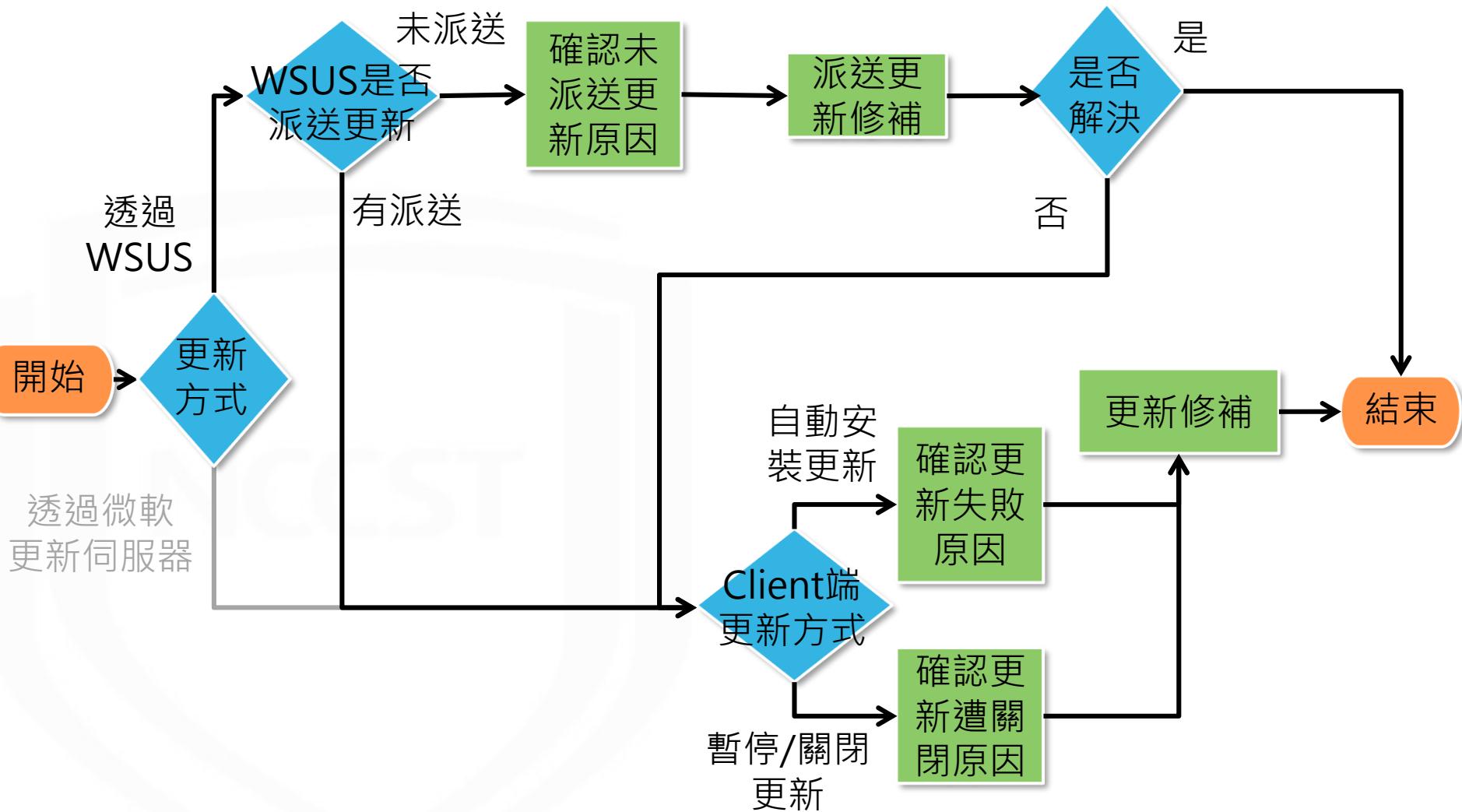
安全性更新管理機制作業流程



確認更新缺漏原因

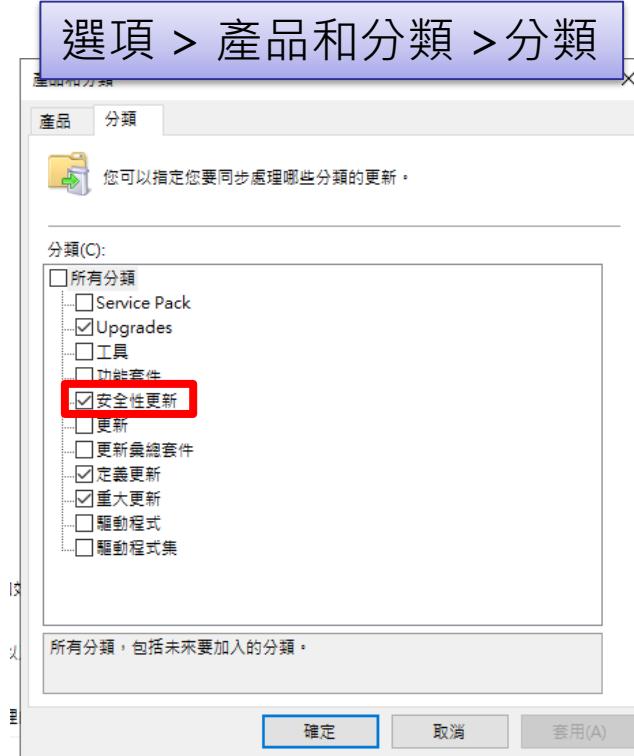
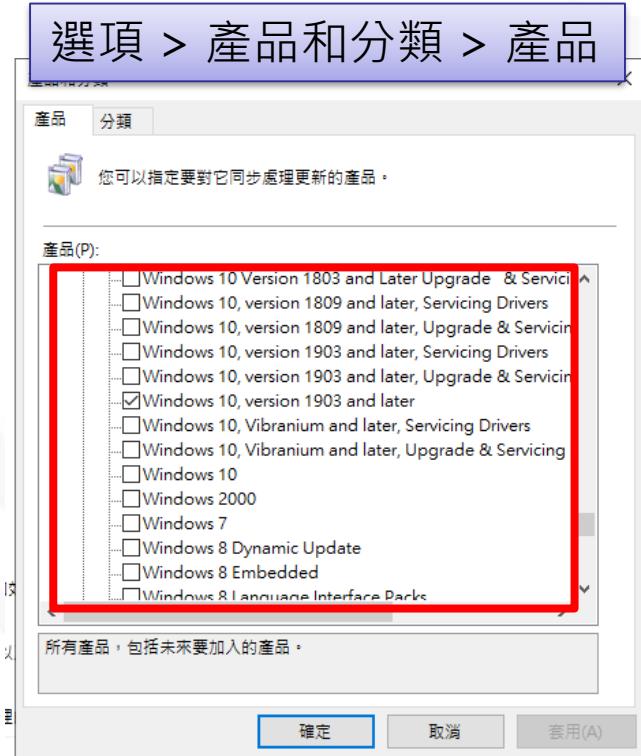


確認更新缺漏原因



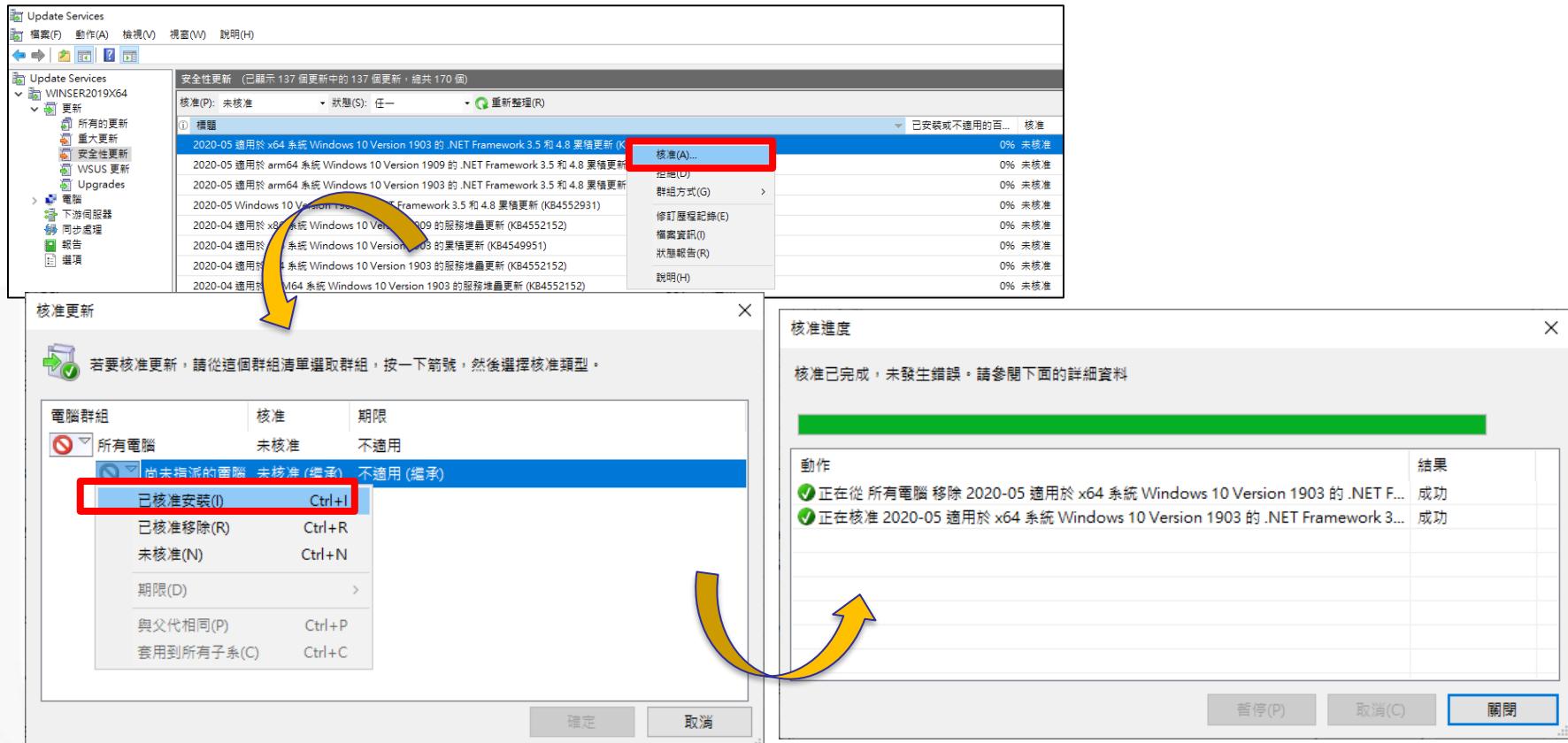
確認WSUS更新派送狀態(1/2)

- 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



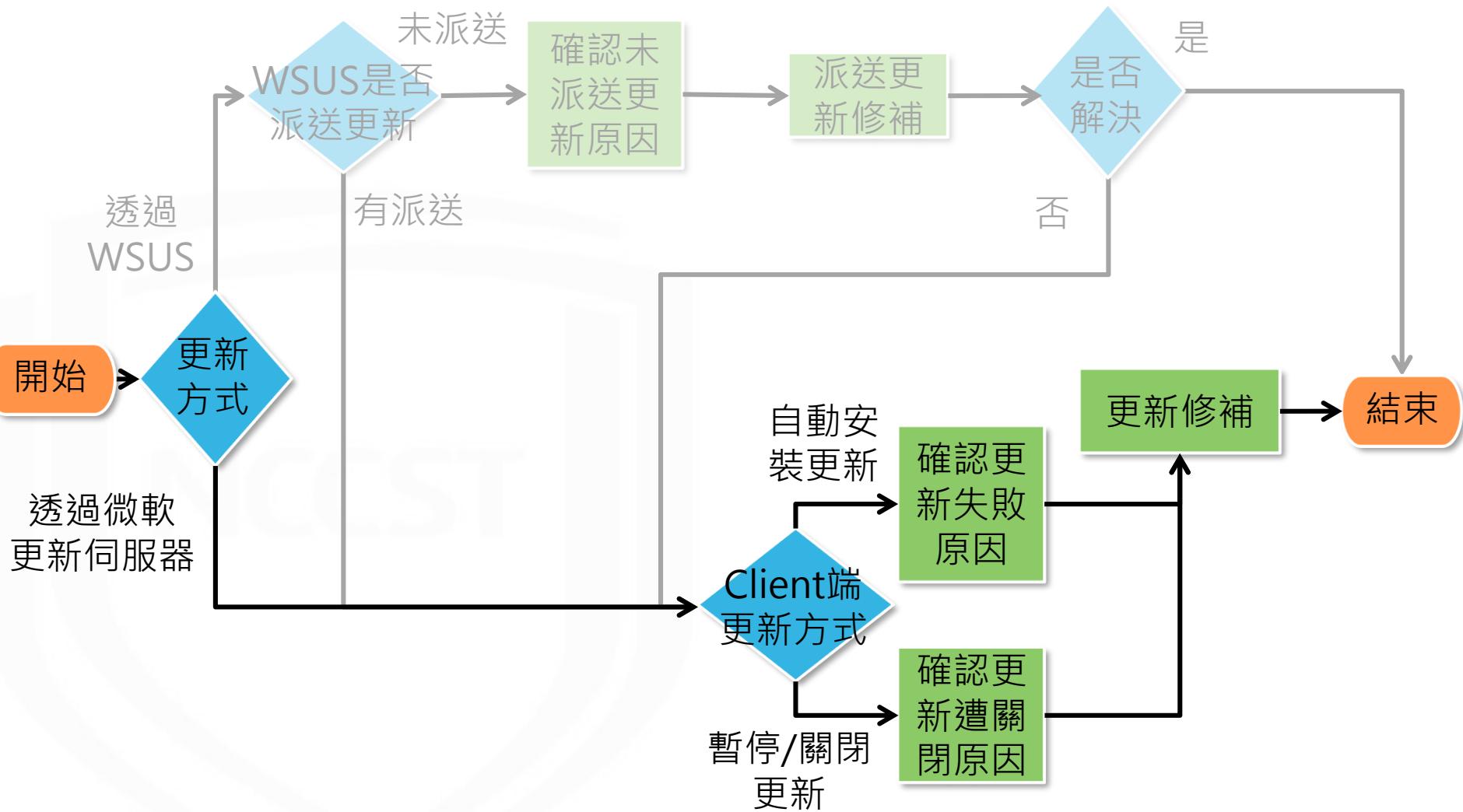
確認WSUS更新派送狀態(2/2)

- 確認缺漏更新是否已於WSUS核准派送



- 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



The screenshot shows a Microsoft Docs page titled "依元件的 Windows 更新錯誤代碼" (Windows Update Error Codes by Component). The page was last updated on 2018/09/18. A callout box highlights the text "透過Ctrl+F搜尋錯誤代碼" (Search for error codes using Ctrl+F). Another callout box highlights the "自動更新錯誤" (Automatic Updates Errors) section, which contains a table of error codes and their descriptions. The table is framed with a red border.

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。

On the right side of the page, there are sections for "此頁面有所助益嗎？" (Was this page helpful?) with "Yes" and "No" buttons, and a sidebar with links to "自動更新錯誤" (Automatic Updates Errors), "Windows Update UI 錯誤", "庫存錯誤", "運算式計算機錯誤", "報告錯誤", and "重新導向程式錯誤".

安全性更新管理機制作業流程



執行安全性更新修補

- 派送更新前，建議進行測試以確認更新檔安裝後，日常作業與服務仍可正常運作
- 修補完成後，執行複測確保缺漏更新確實完成修補







參考資料

參考資料(1/2)

- Windows Management Instrumentation
 - <https://docs.microsoft.com/zh-tw/windows/desktop/wmisdk/wmi-start-page>
- 用wmic建立已安裝軟體清單
 - <http://jdev.tw/blog2/2487/wmic-product>
- Find windows OS version from command line
 - <https://www.windows-commandline.com/find-windows-os-version-from-command/>
- 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>

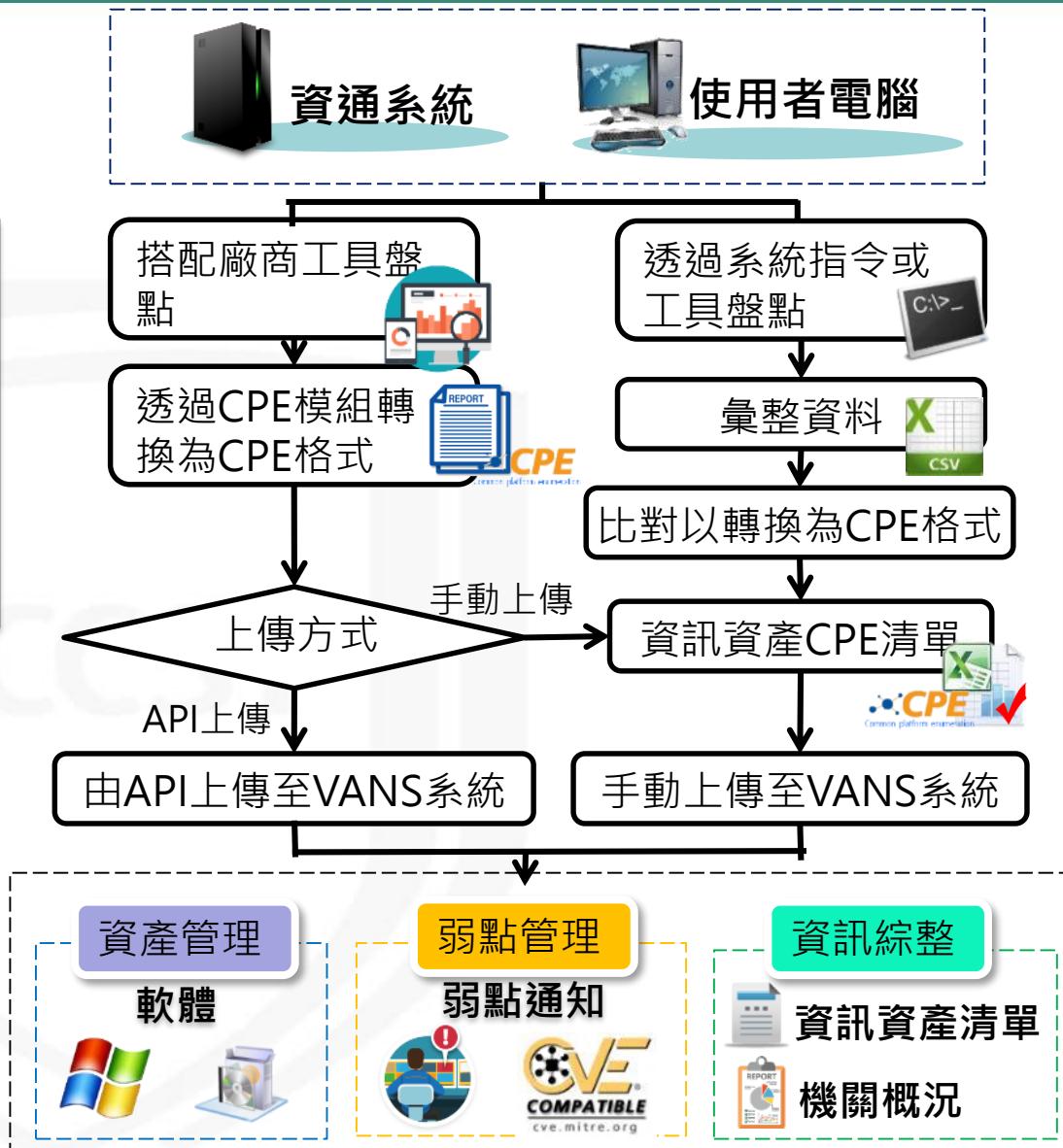
參考資料(2/2)

- 什麼是 Microsoft 基準安全分析分析器及其用途 ?
 - <https://docs.microsoft.com/zh-tw/windows/security/threat-protection/msa-removal-and-guidance>
- 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>
- Power Query 快速入門
 - <https://support.office.com/zh-tw/article/Power-Query-%E5%BF%AB%E9%80%9F%E5%85%A5%E9%96%80-7104fbea-9e62-4cb9-a02e-5fbf1a6c536a>
- 合併多個資料來源的資料 (Power Query)
 - <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-70cf661-5a2a-4d9d-a4fe-586cc7878c7d>
- 工作排程器概觀
 - <https://forsenergy.com/zh-tw/taskscheduler/html/61e2eb14-d71d-4a60-9eab-ba7bdd422b94.htm>



附件

附件1.資訊資產弱點管理總覽



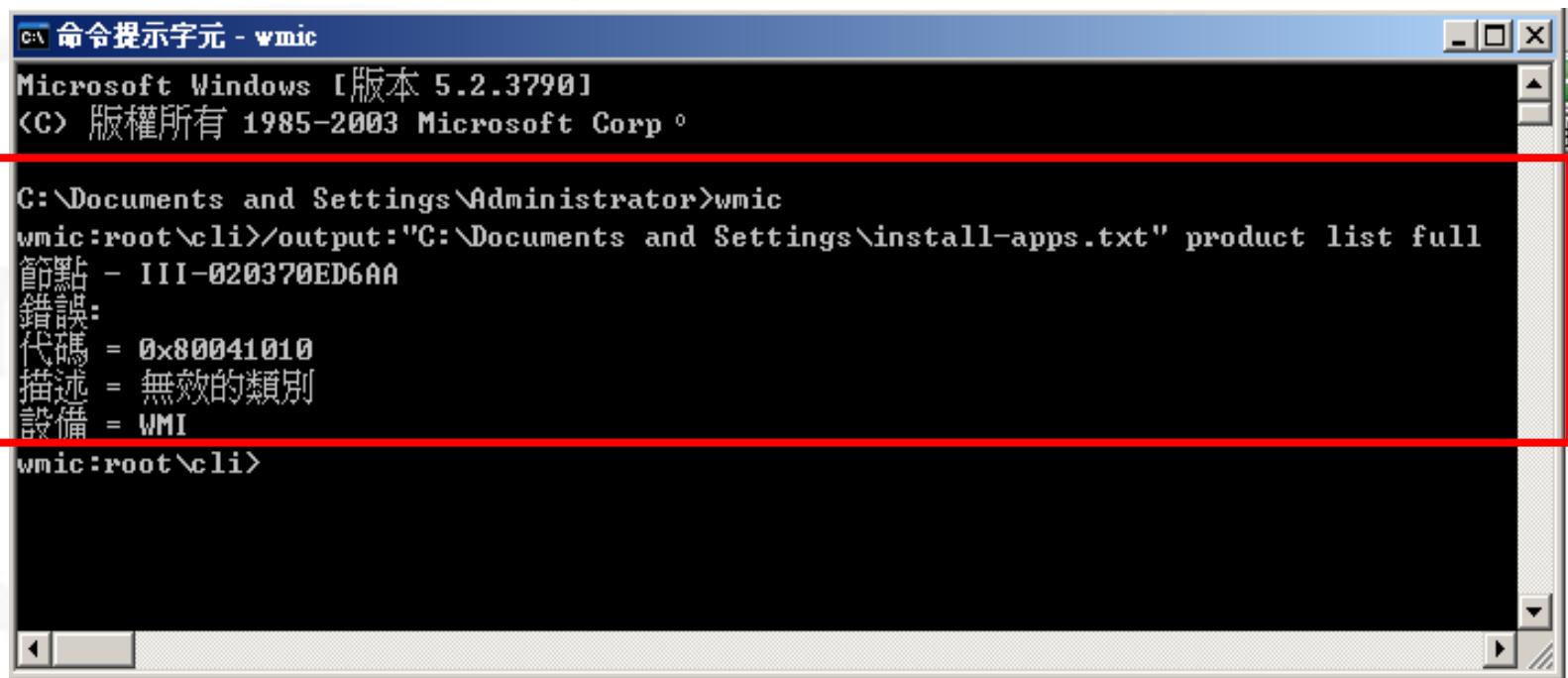


附件2

WMI Windows Installer提供者 安裝步驟

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



```
命令提示字元 - wmic
Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

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

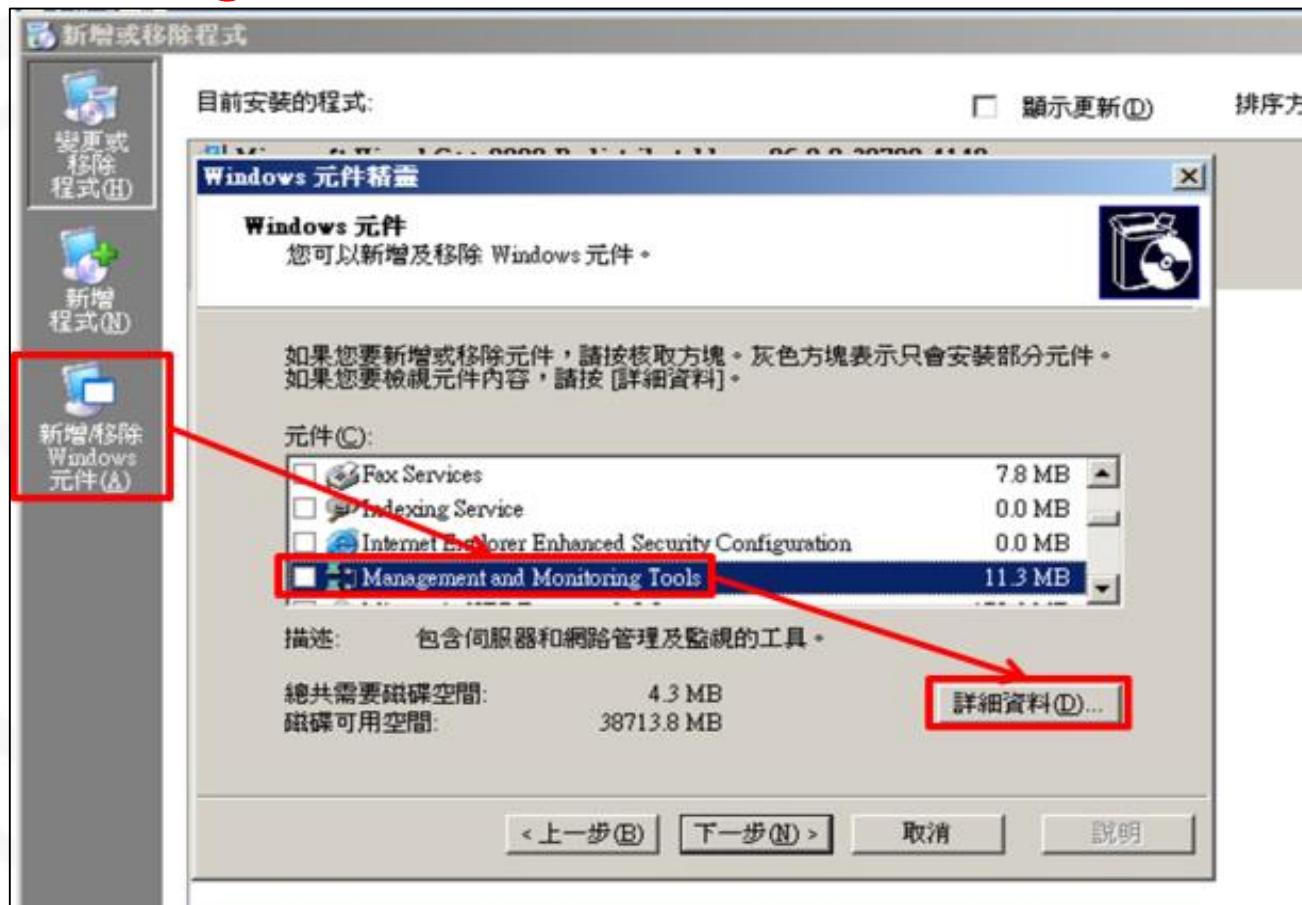
安裝WMI Windows Installer(2/7)

- 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」



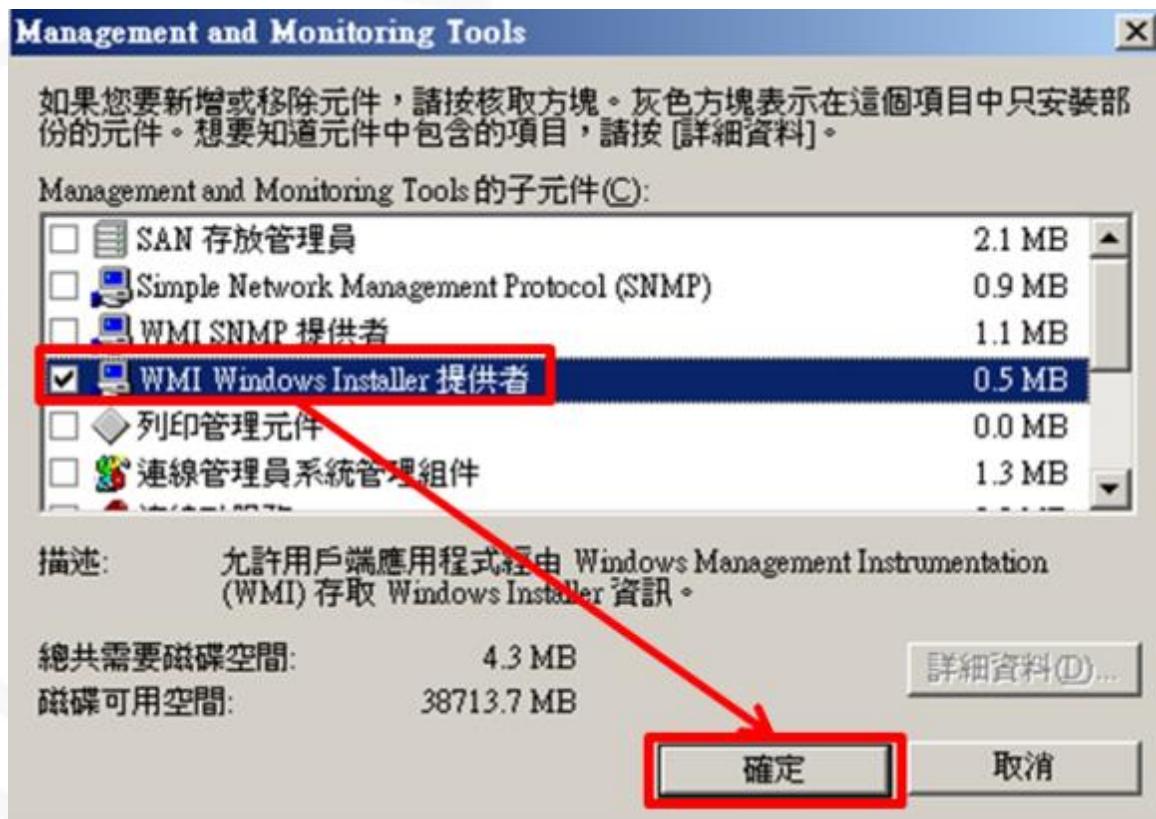
安裝WMI Windows Installer(3/7)

- 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)

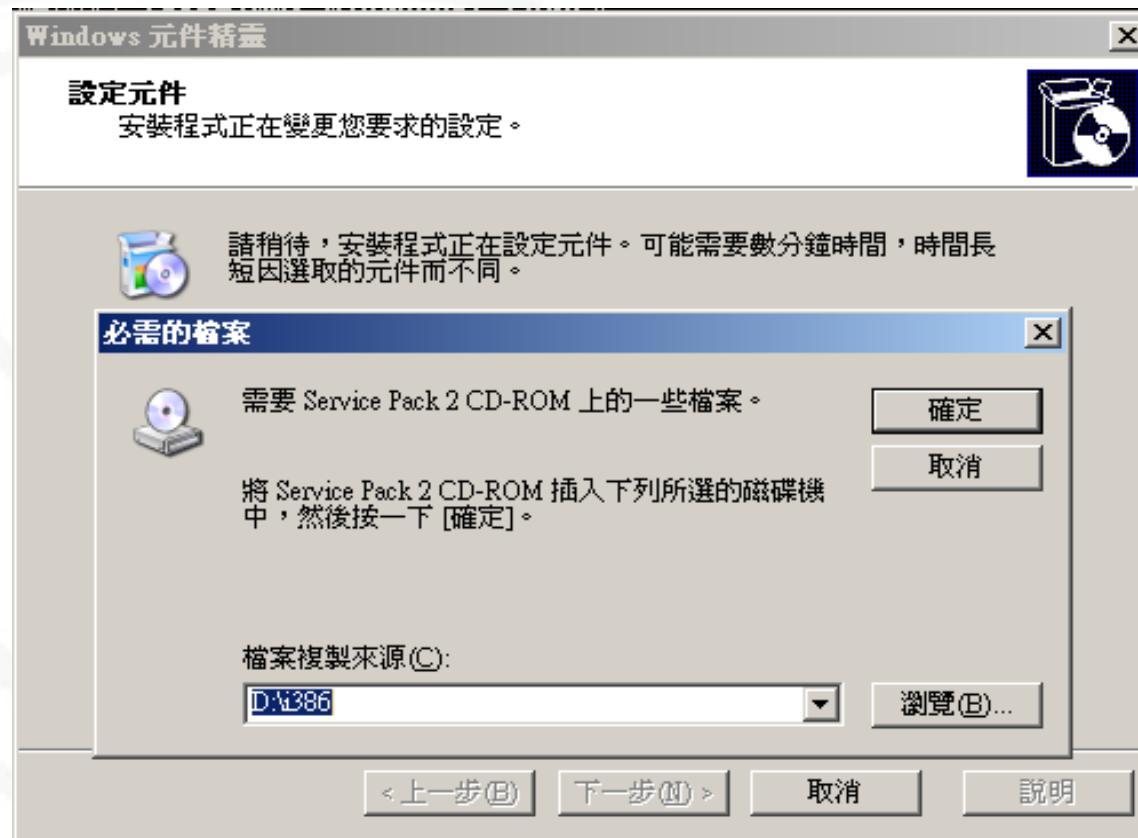
- 步驟三：於「Management and Monitoring Tools」對話方塊中，勾選「WMI Windows Installer提供者」，並點選「確定」



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



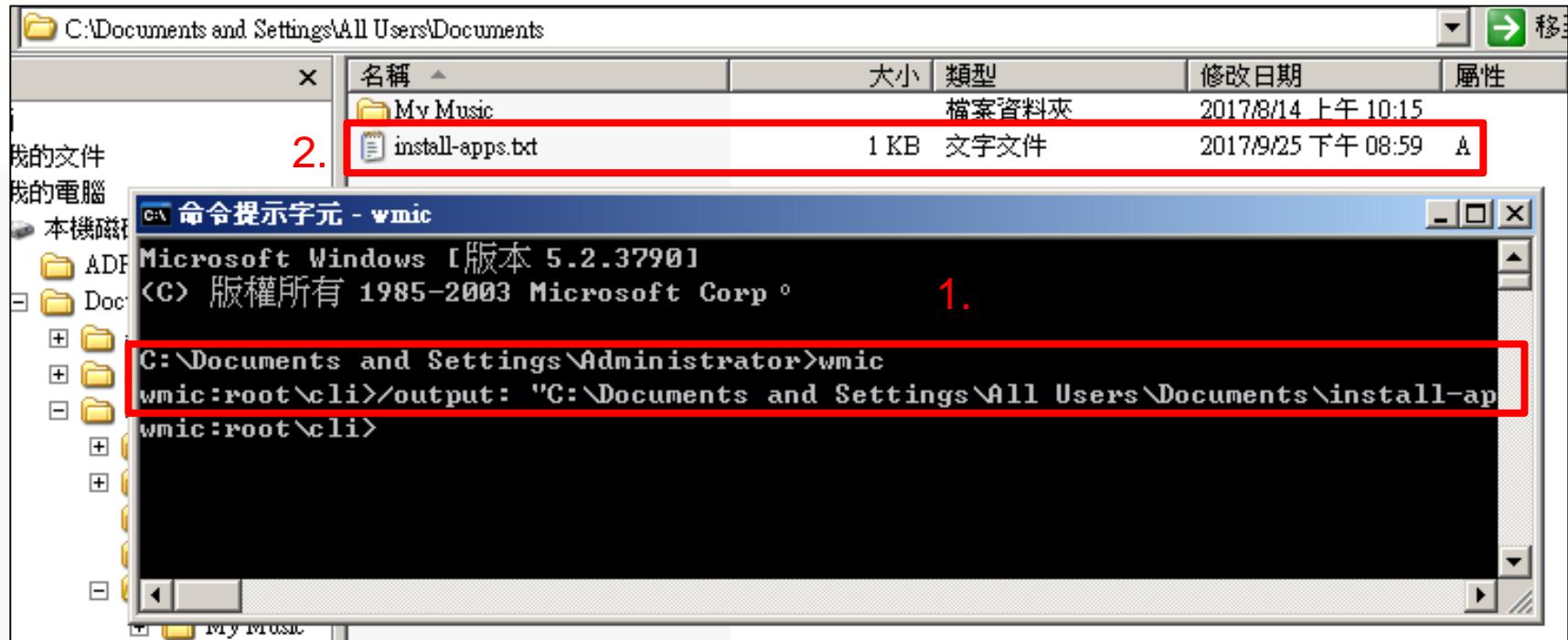
安裝WMI Windows Installer(6/7)

● 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



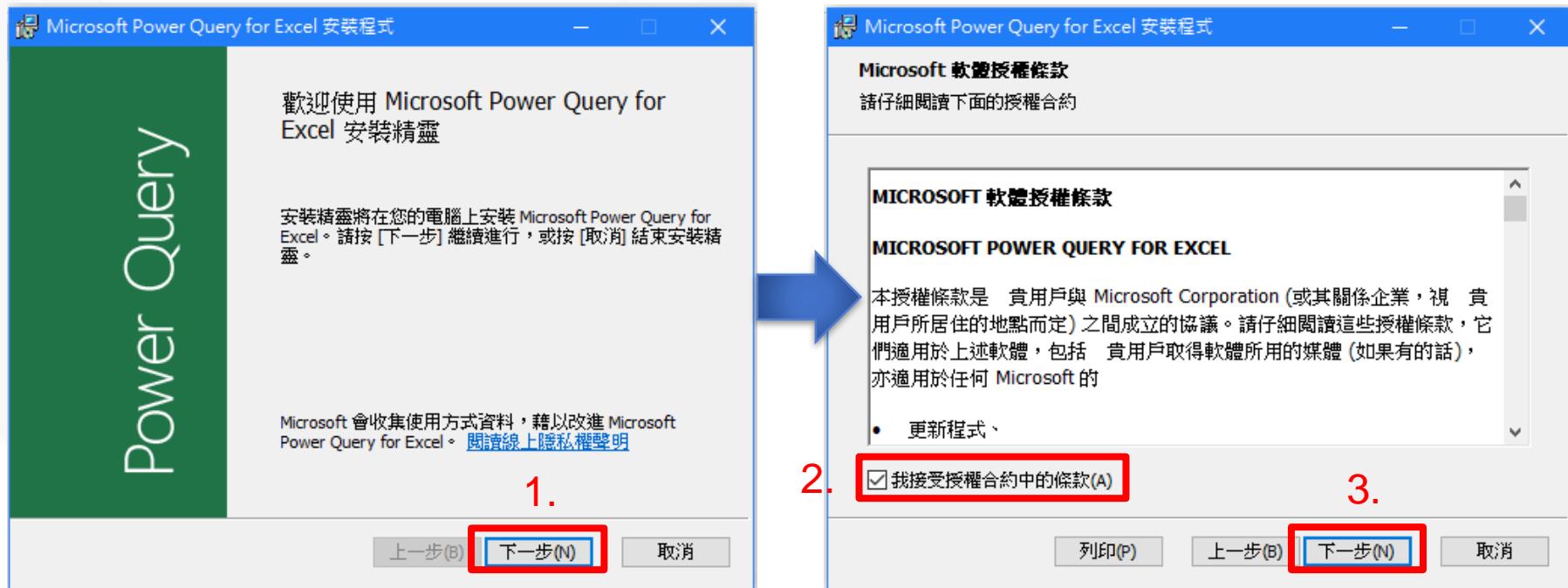


附件3

Microsoft Power Query for Excel 安裝步驟

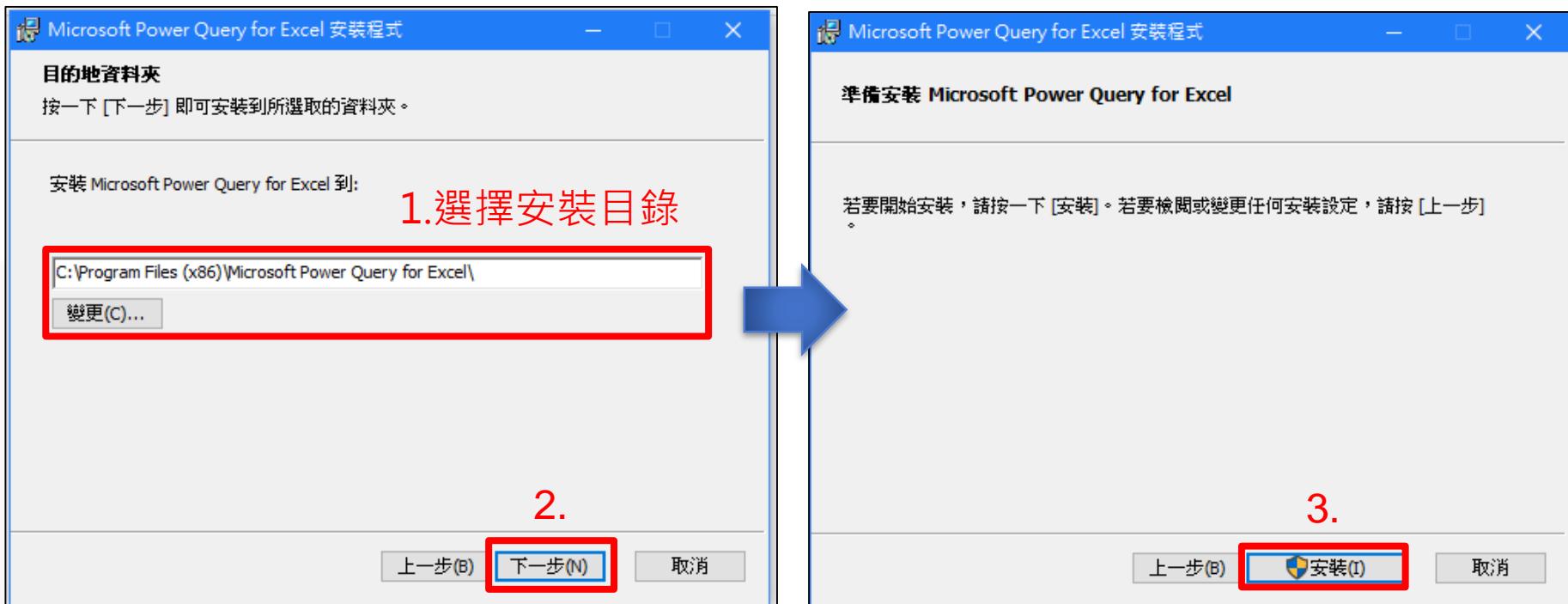
安裝Microsoft Power Query for Excel(1/3)

- 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

