國家資通安全研究院
National Institute of Cyber Security

新版資通安全弱點通報系統(VANS 2.0)推廣教材

檢測防禦中心

113年11月18日

【普通】

課程簡介

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

課程大綱

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

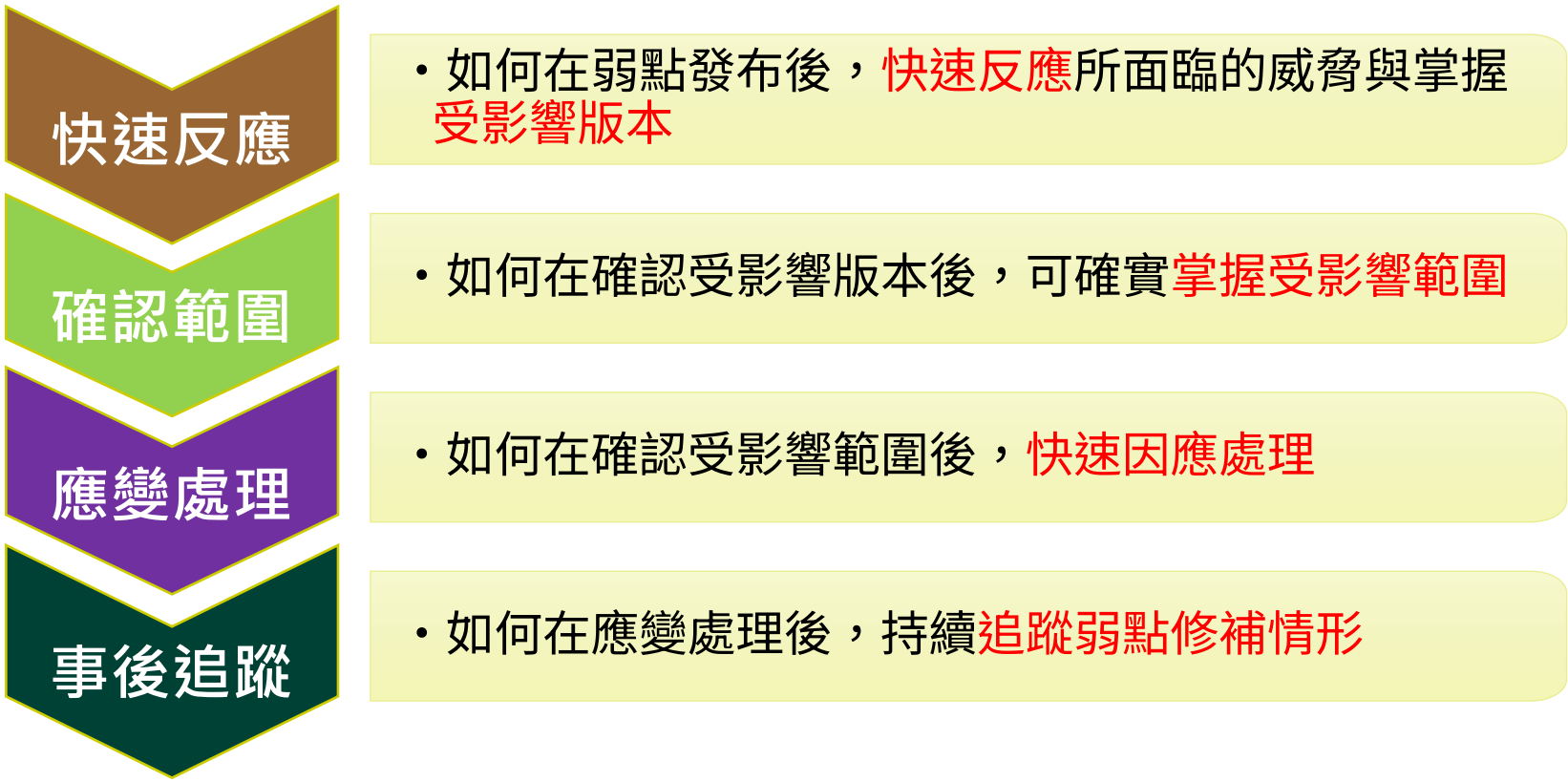
課程大綱

國家資通安全研究院
National Institute of Cyber Security

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

前言

- 不定期爆發之重大弱點，若未能即時反應與修補，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訊資產情況，即可快速因應，將損害降至最低



資通安全管理法應辦事項規定(1/2)

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

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

資通安全管理法應辦事項規定(2/2)

國家資通安全研究院
National Institute of Cyber Security

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

課程大綱

國家資通安全研究院
National Institute of Cyber Security

- 前言與法規政策說明
- **資通安全弱點通報系統說明**
- 資通安全弱點通報系統實作
  - 資訊資產與已安裝KBID盤點作業
  - 資訊資產與已安裝KBID正規化作業
  - 資訊資產與已安裝KBID登錄作業
  - 弱點通知與修補作業
    - 實作練習1
    - 實作練習2
  - 資訊資產與已安裝KBID更新作業
    - 實作練習3

資通安全弱點通報機制

國家資通安全研究院
National Institute of Cyber Security

- 資通安全弱點通報機制(Vulnerability Analysis and Notice System)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訊資產盤點與風險評估應辦事項
  - 定期蒐集資通系統、使用者電腦及工業控制系統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

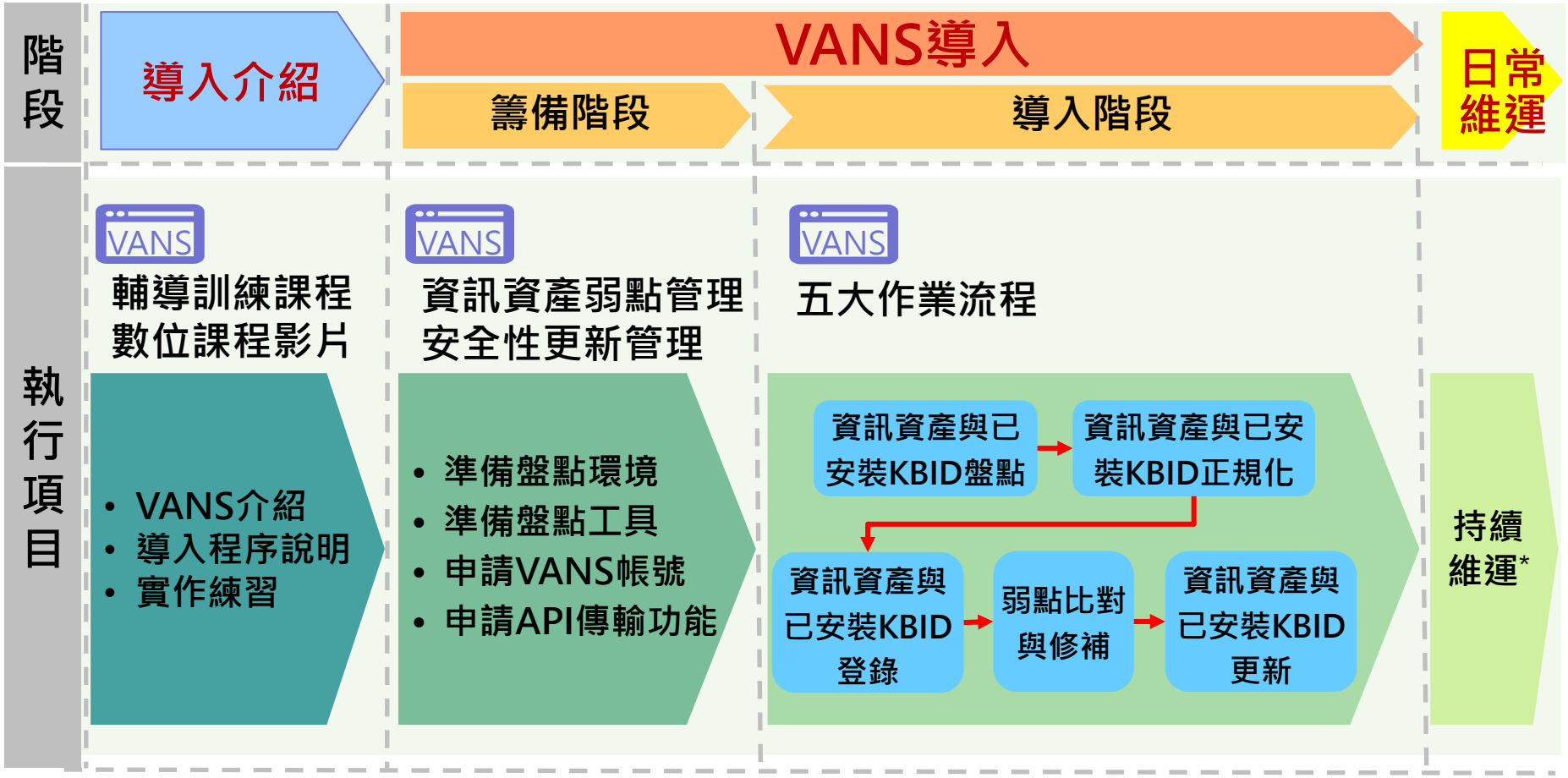
VANS目標

國家資通安全研究院
National Institute of Cyber Security

- 確認資訊資產弱點
  - 蒐集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，提供機關相關弱點資訊與自我檢查機制
- 追蹤資訊資產弱點修補情形
  - 依照機關訂定之風險值門檻，及時提醒資訊資產風險情形，並進行弱點評估與修補作業
- 強化安全性更新落實情形
  - 搭配上傳微軟系列軟體已安裝安全性更新，以協助機關確認微軟資訊資產之安全性更新缺漏項目，更精準呈現微軟弱點修補情形

VANS機制導入作業流程

國家資通安全研究院
National Institute of Cyber Security



*持續維運：包含定期執行及不定期執行(例如資訊資產異動時)

系統介紹

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

資訊資產盤點標的(1/3)

國家資通安全研究院
National Institute of Cyber Security

- 蒐集範圍：資通系統、工業控制系統及使用者電腦之軟體資產

資訊資產盤點標的(2/3)

國家資通安全研究院
National Institute of Cyber Security

- 增加資產識別碼
  - 為利機關識別須修補的主機，提升資訊資產管理效率，規劃在機關上傳資訊資產與已安裝KBID資產清單內新增「資產識別碼」欄位
  - 適用於採用VANS新系統制定之新版資訊資產與已安裝KBID資料格式資訊資產
- 產生資產識別碼的方法
  - 取得資訊資產主機的MAC Address(例如：XXX90FFE0001)
  - 將MAC Address經由雜湊函式(hash)，輸出雜湊值(例如：7602f215e57ff39e787f058576ac8ae3)
  - 此雜湊值即為此資訊資產主機之資產識別碼
- 採用VANS舊系統制定的舊版資訊資產與已安裝KBID格式的資料上傳時，系統會在資產識別碼欄位內，填入共用資產識別碼，即「VANSONECOMMAID」

資訊資產盤點標的(3/3)

- 增加資產群組
  - 為便於不同資訊資產管理者，可於系統掌握其管理之資訊資產弱點與處理情形，規劃在機關上傳資訊資產與已安裝KBID資產清單內，新增「資產群組」欄位
  - 適用於採用VANS新版資訊資產與KBID資料規格上之資訊資產
- 產生資產群組的方法
  - 由機關依照資訊資產隸屬單位、系統別或管理人員等進行分群，自行定義資產群組分類方式
  - 機關可利用本系統提供之「系統管理>資產分群管理」功能，建立機關資產群組
- 資訊資產與已安裝KBID資料格式上傳時，本系統會自動為機關建立「預設資產群組」，其代碼與名稱分別為「DEFAULT」與「預設資產群組」

資訊資產呈現方式(1/3)

- 資通系統、使用者電腦及工業控制系統組成多變，所安裝之軟體套件多樣，難有資訊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訊資產，可能有不同描述方式

資訊資產呈現方式(2/3)

- 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)

CPE common platform enumeration

資訊資產呈現方式(3/3)

- CPE條目範例
  - Microsoft Windows Server 2003 R2 Service Pack 1 on X64

廠商名稱　　版本　　版次

➢cpe:2.3:o:microsoft:windows_server_2003:r2:sp1:*:*:datacenter:*: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:update92:*:*:*:*:*:*

產品類別　　產品名稱　　更新

CPE common platform enumeration

弱點呈現方式

- Common Vulnerabilities and Exposures(簡稱CVE)羅列各種資安弱點，並給予編號以便查閱
- CVE目標為將所有已知弱點與相關風險資訊標準化，俾利於各個弱點資料庫與安全工具之間統一弱點相關資料
- 現由美國非營利組織MITRE所屬之National Cybersecurity FFRDC負責營運維護
- 每一個資安弱點皆賦予一個CVE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之資料庫網站
  - 自MITRE取得CVE列表，並增加修補建議連結、嚴重性評分(CVSS分數)及影響等級等資訊
  - 建立CPE與CVE對應關係，以解決弱點與資訊資產之對應關係
  - VANS系統每天更新1次資訊資產與弱點資訊

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

微軟安全性更新(1/2)

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

微軟安全性更新(2/2)

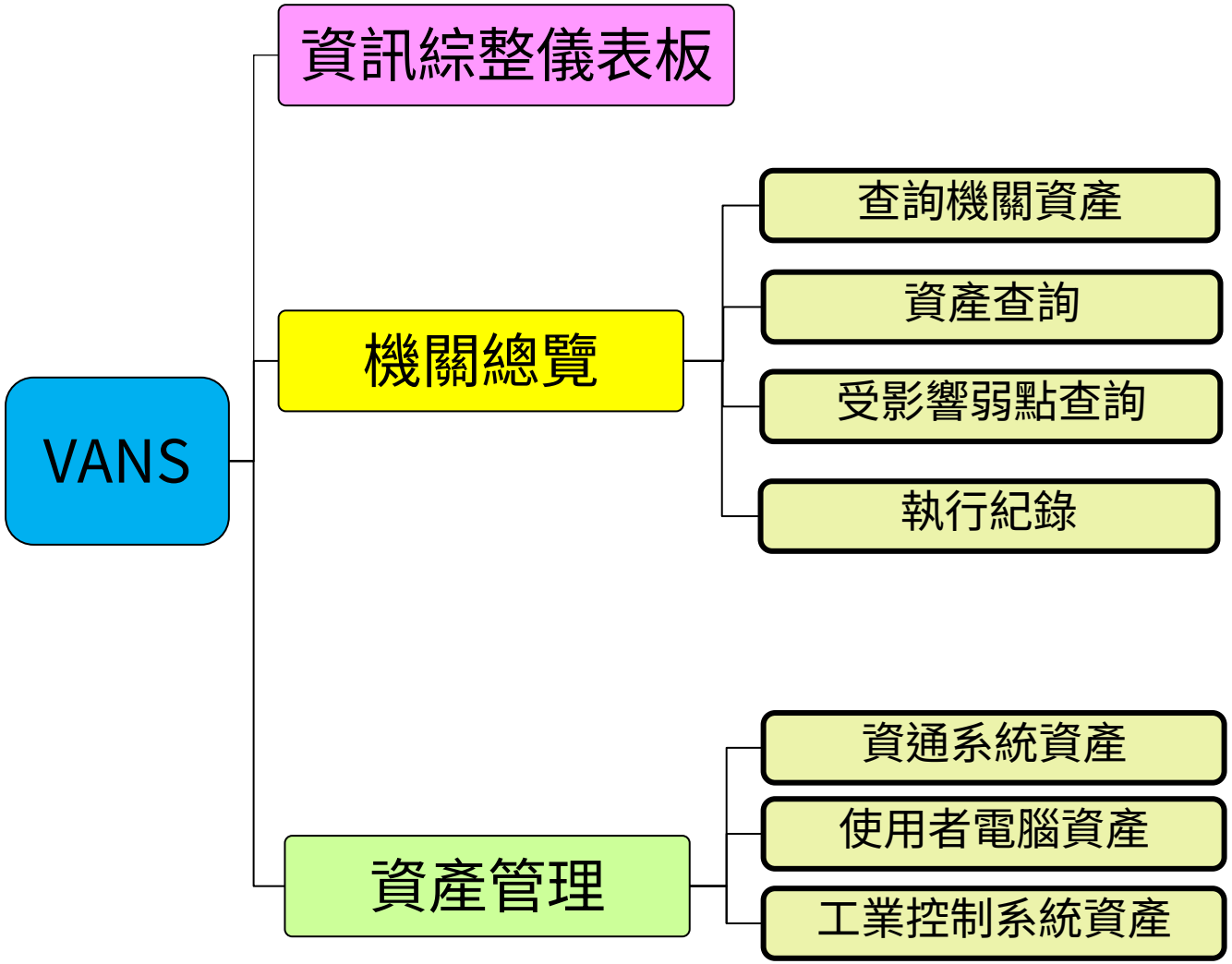
- 以Microsoft Windows 10作業系統而言，因CPE僅會列出大版本(如22h2)，透過Windows Update進行安全性更新作業不會異動大版本資訊(22h2)，導致難以透過CPE判斷Windows Update更新情形
- VANS系統可透過機關上傳之已安裝KBID，判斷弱點修補狀態

cpe:2.3:o:microsoft:windows_10_22h2:-:*:*:*:*:*:x64:*

Microsoft Windows 10 22h2

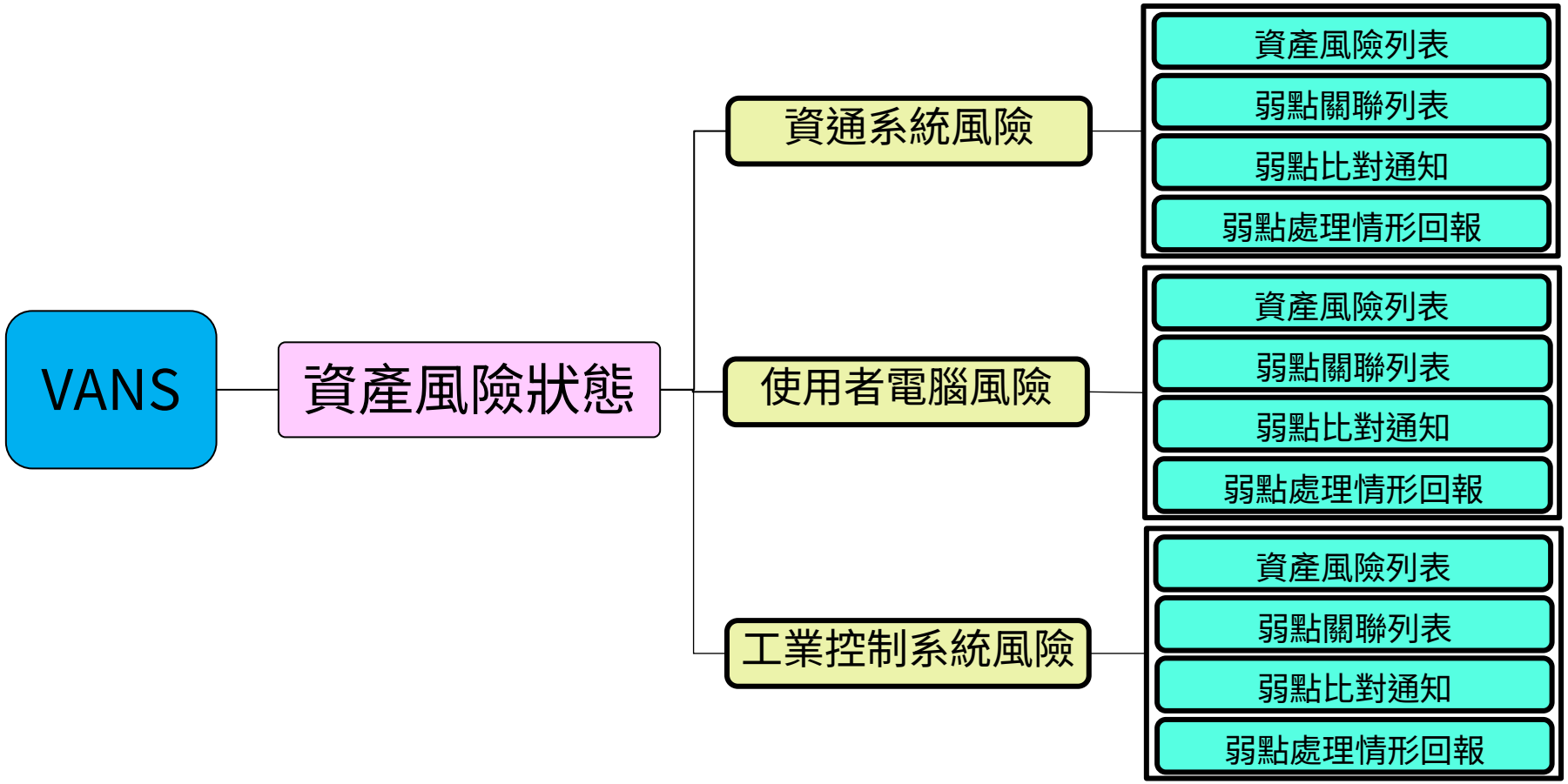
系統功能總覽(1/3)

國家資通安全研究院
National Institute of Cyber Security



系統功能總覽(2/3)

國家資通安全研究院
National Institute of Cyber Security



系統功能總覽(3/3)

國家資通安全研究院
National Institute of Cyber Security

系統介面說明

國家資通安全研究院
National Institute of Cyber Security

服務申請流程

國家資通安全研究院
National Institute of Cyber Security

聯絡資訊
服務電話：(02)6631-6423
服務信箱：VansService@nics.nat.gov.tw

申請個人帳號

・於iAuth平台申請個人帳號

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

機關提出申請

・於iAuth平台提出VANS帳號申請

・於VANS專區下載並填寫機關管理者帳號申請(異動)單，完成後Email予資安署

資安院VANS專區
https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/VANS/

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

VANS系統
https://vans.nat.gov.tw/

VANS帳號管理(1/2)

國家資通安全研究院
National Institute of Cyber Security

- 機關管理者帳號權限異動
  - 單一機關至多2個機關管理者帳號
  - 有異動需求時，請填寫機關管理者帳號申請(異動)單，完成後Email予資安署，審核通過後，資安院將協助進行後續處理
- 閒置帳號鎖定
  - 若iAuth帳號長達180天未有登入行為，則將進入鎖定狀態，無法登入系統進行操作
  - 可透過iAuth平台重新啟用帳號

VANS帳號管理(2/2)

國家資通安全研究院
National Institute of Cyber Security

- 機關登入VANS系統分為下列兩種帳號

機關管理者帳號

- ✓ 檢視機關總覽
- ✓ 資產與已安裝KBID管理
- ✓ 資產風險檢視與回報弱點
- ✓ **資產分群管理**
- ✓ 檢視機關各帳號操作紀錄
- ✓ **申請API介接IP**並**重新產生**API Key

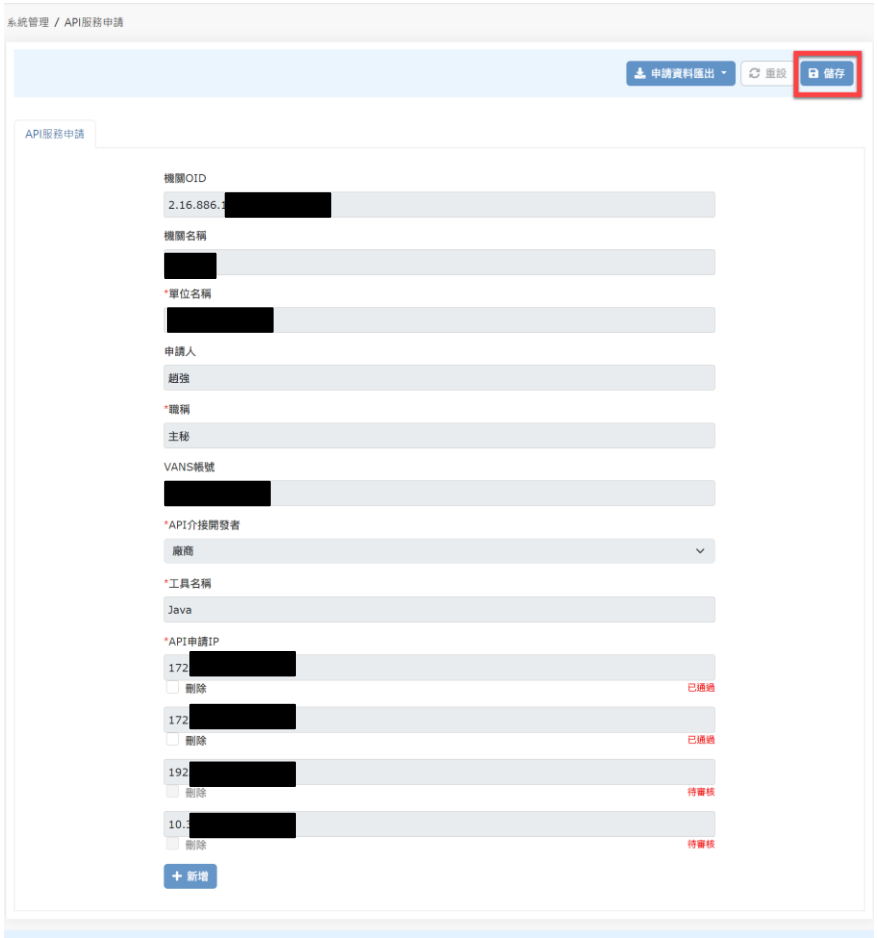
一般權限帳號

- ✓ 檢視機關總覽
- ✓ 資產與已安裝KBID管理
- ✓ 資產風險檢視與回報弱點
- ✓ 檢視自己帳號操作紀錄
- ✓ **檢視及複製**API Key

系統管理-API服務申請(1/2)

國家資通安全研究院
National Institute of Cyber Security

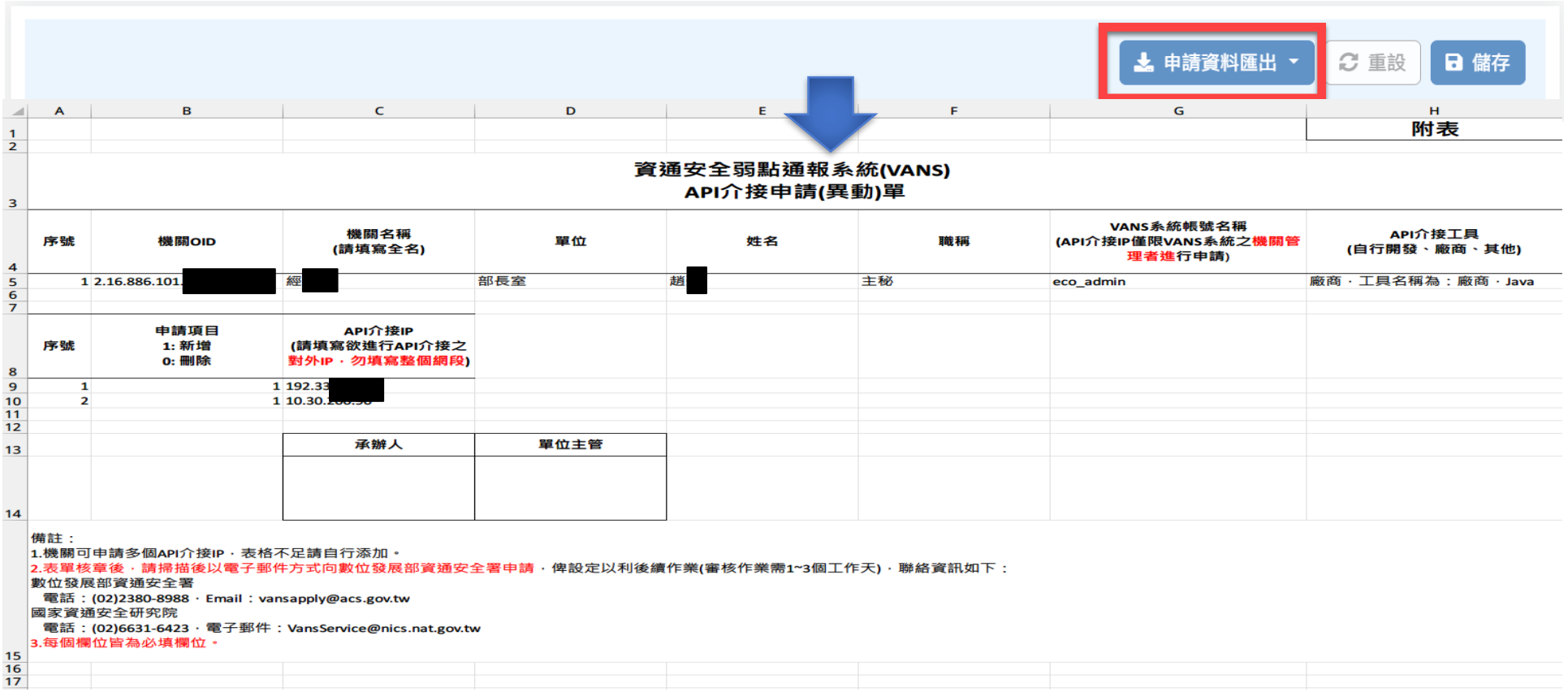
- API服務申請
  - ➢使用者進入此功能可以填完資料後，按「儲存」鈕送出申請



系統管理-API服務申請(2/2)

國家資通安全研究院
National Institute of Cyber Security

- API申請資料匯出
  - ➢使用者送出API申請資料後，可按「申請資料匯出」鈕將資料匯出後，再列印紙本送審



附表

資通安全弱點通報系統(VANS)
API介接申請(異動)單

序號	機關OID	機關名稱 (請填寫全名)	單位	姓名	職稱	VANS系統帳號名稱 (API介接IP僅限VANS系統之機關管理者進行申請)	API介接工具 (自行開發、廠商、其他)
1	2.16.886.101[redacted]	經[redacted]	部長室	趙[redacted]	主秘	eco_admin	廠商，工具名稱為：廠商，Java

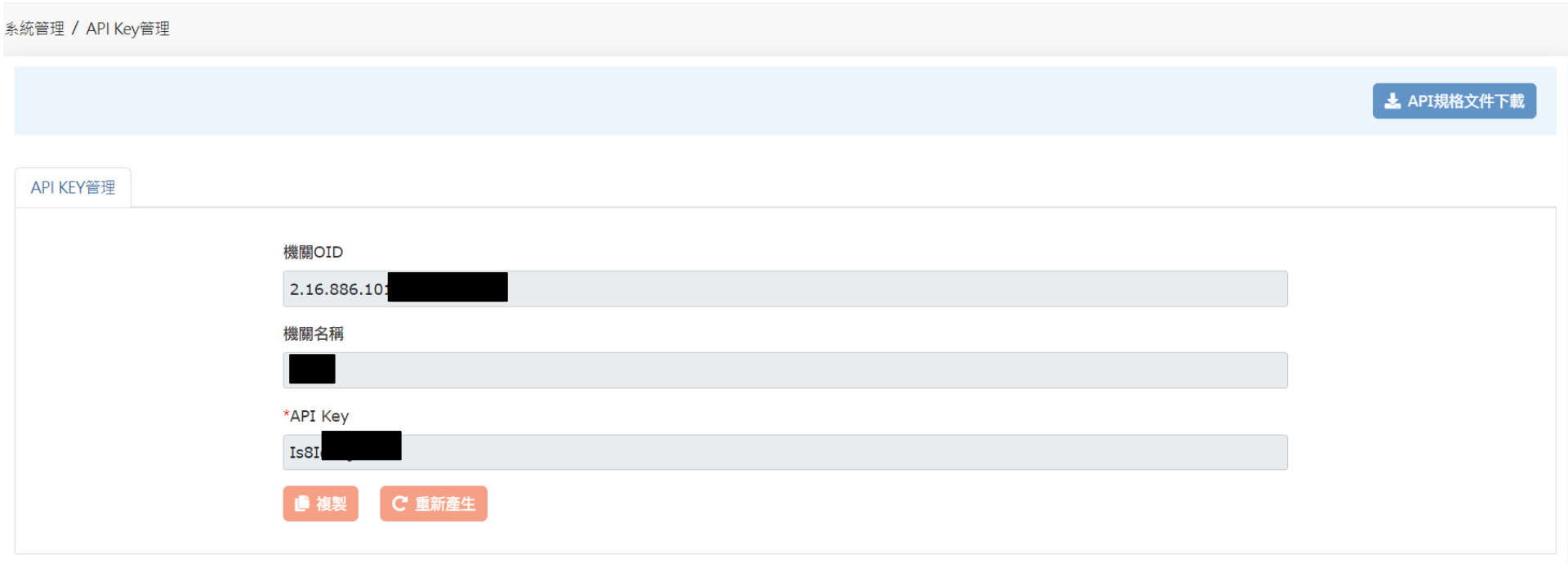
序號	申請項目 1: 新增 0: 刪除	API介接IP (請填寫欲進行API介接之對外IP，勿填寫整個網段)
1	1	192.33[redacted]
2	1	10.30.[redacted]

承辦人	單位主管

備註：
1.機關可申請多個API介接IP，表格不足請自行添加。
2.表單核章後，請掃描後以電子郵件方式向數位發展部資通安全署申請，俾設定以利後續作業(審核作業需1~3個工作天)，聯絡資訊如下：
數位發展部資通安全署
電話：(02)2380-8988，Email：vansapply@acs.gov.tw
國家資通安全研究院
電話：(02)6631-6423，電子郵件：VansService@nics.nat.gov.tw
3.每個欄位皆為必填欄位。

系統管理-API KEY管理(1/3)

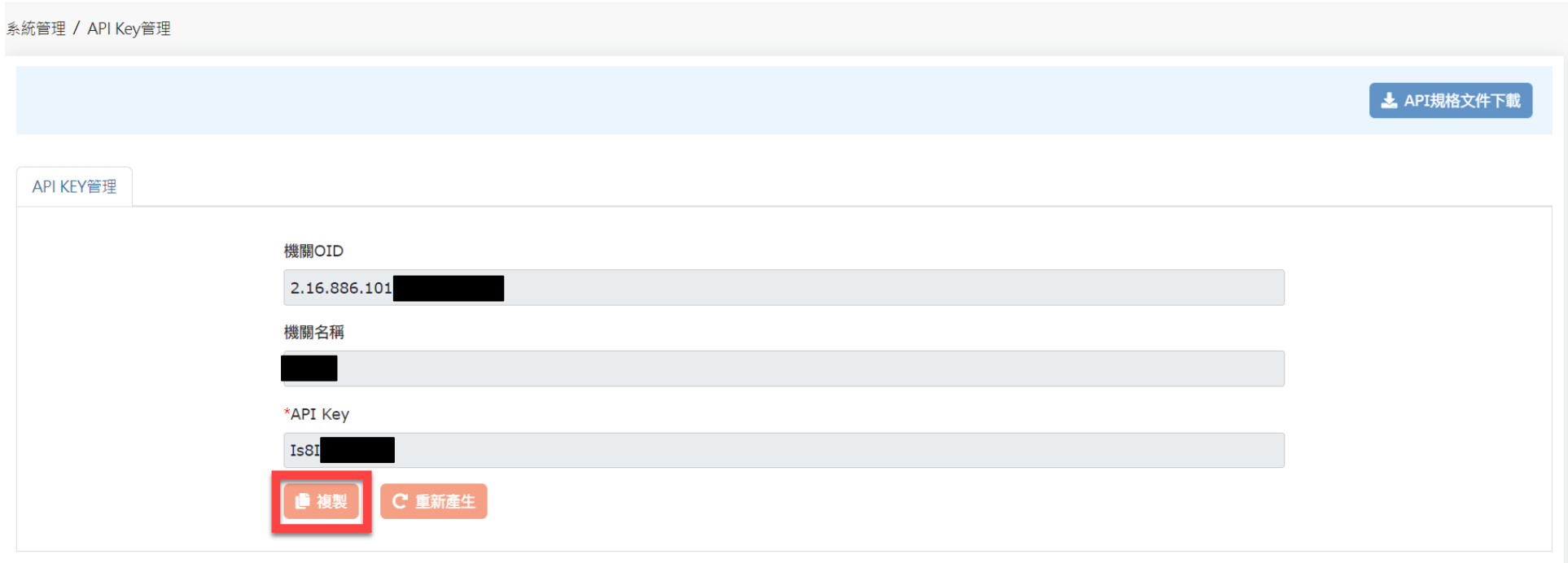
- 查詢API KEY
  - ➢使用者申請完API服務後，系統會產生一組API KEY，進入此功能，系統顯示已產生的API KEY



系統管理-API KEY管理(2/3)

國家資通安全研究院
National Institute of Cyber Security

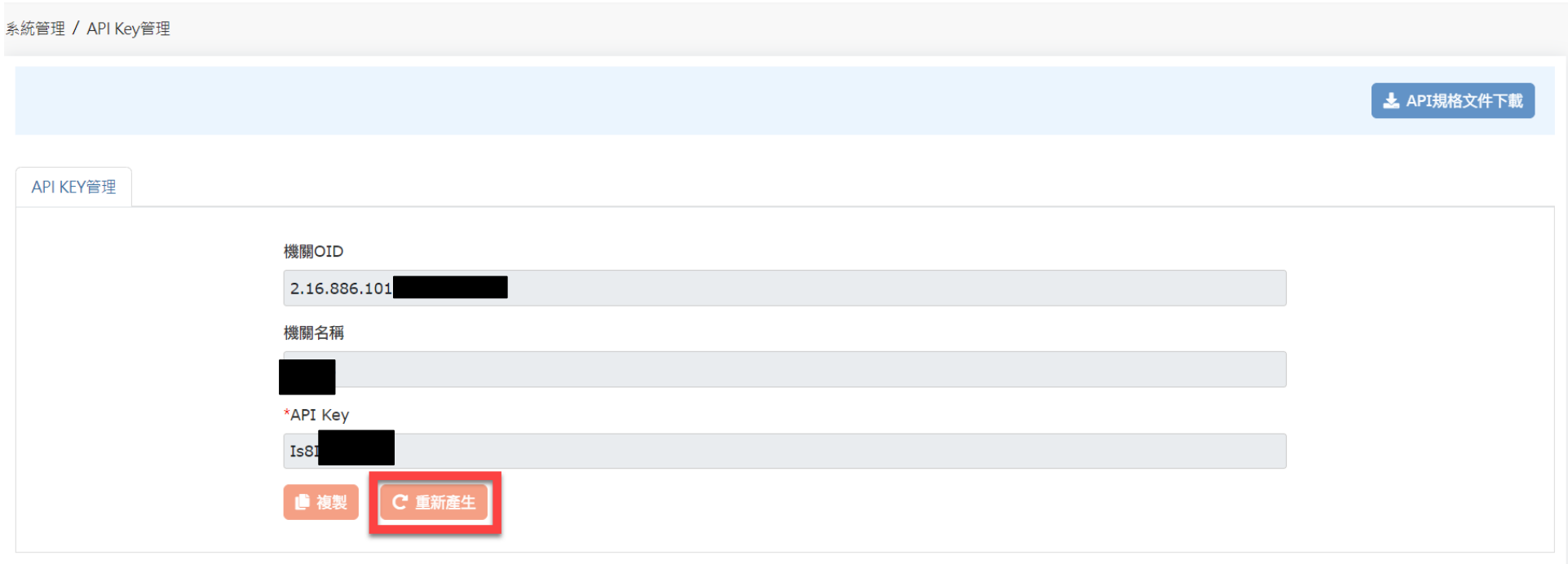
- 複製API KEY
  - ➢使用者進入此功能，點擊「複製」鈕，可將目前的API KEY複製至剪貼簿



系統管理-API KEY管理(3/3)

國家資通安全研究院
National Institute of Cyber Security

- 重新產生 API KEY(限機關管理者)
  - ➢機關管理者進入此功能，點擊「重新產生」鈕，可產生新的API KEY

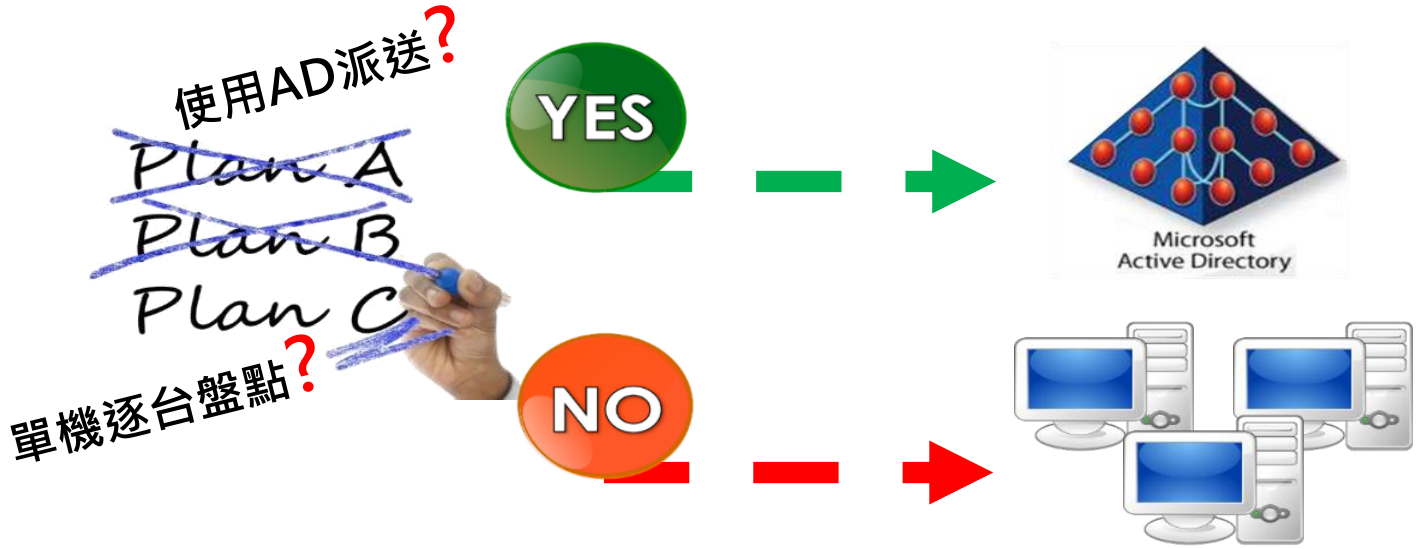


課程大綱

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

執行規劃

- 依據機關環境擬定導入執行規劃
  - 執行範圍：本部/本部與所屬、資通系統/使用者電腦/工業控制系統
  - 執行時程：人力評估、導入測試起訖時間、正式導入起訖時間
  - 執行方式：單機/AD派送GPO執行、第三方工具執行

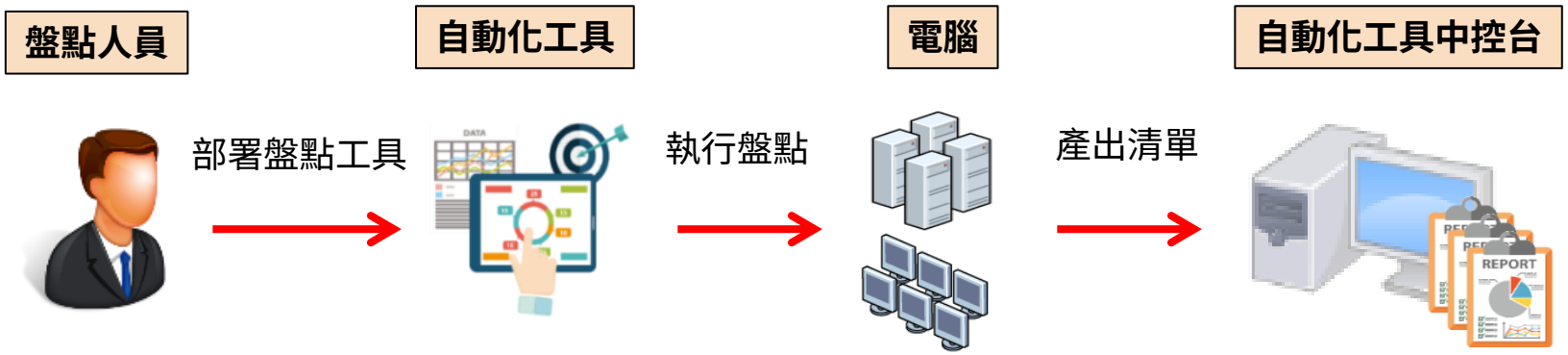


情境說明(1/3)

國家資通安全研究院
National Institute of Cyber Security

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

1 透過自動化工具盤點



情境說明(2/3)

國家資通安全研究院
National Institute of Cyber Security

2 透過系統指令批次盤點

情境說明(3/3)

國家資通安全研究院
National Institute of Cyber Security

3 透過系統指令單機盤點

導入作業流程

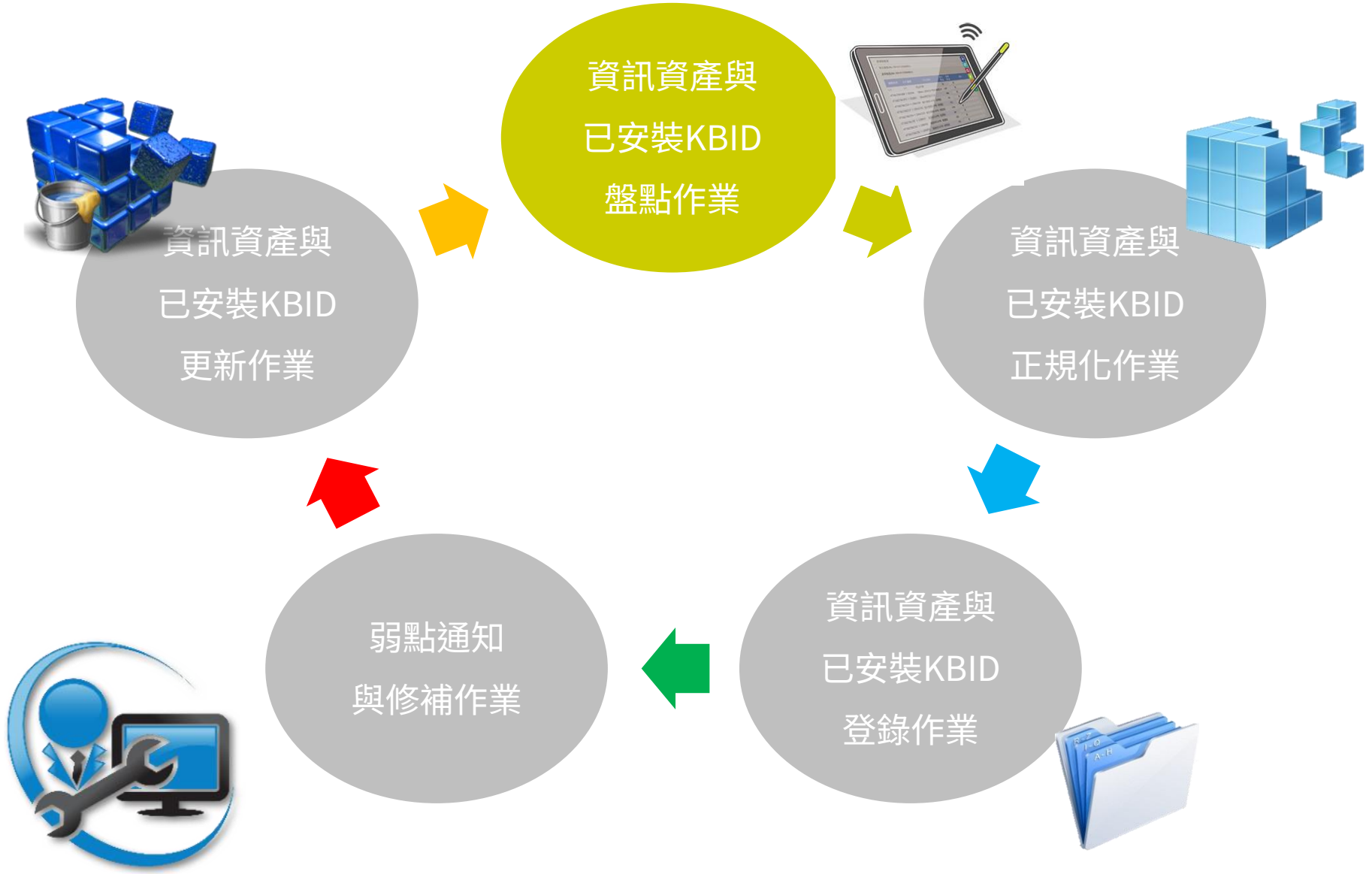
國家資通安全研究院
National Institute of Cyber Security

資訊資產弱點管理總覽

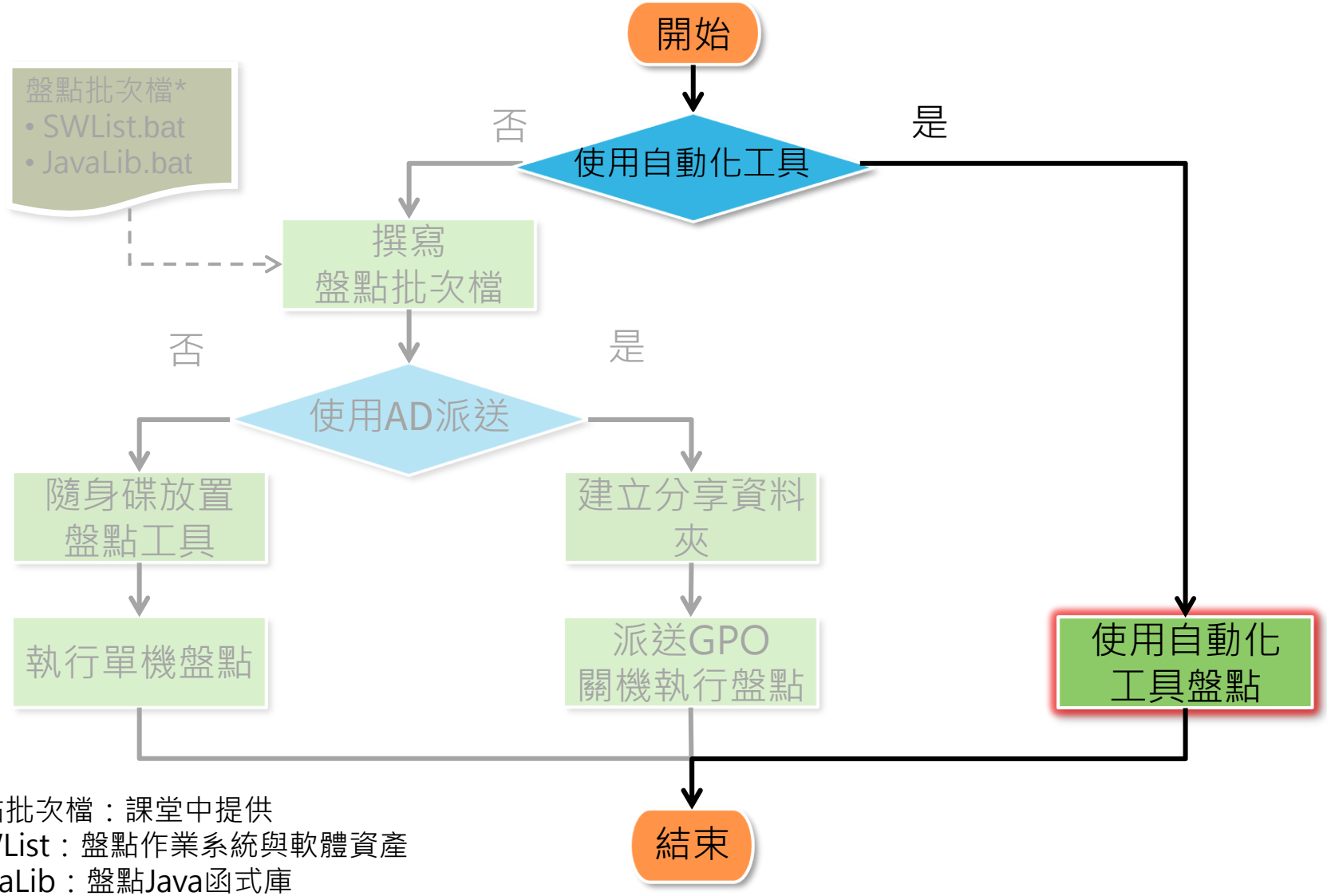
國家資通安全研究院
National Institute of Cyber Security

導入作業流程

國家資通安全研究院
National Institute of Cyber Security



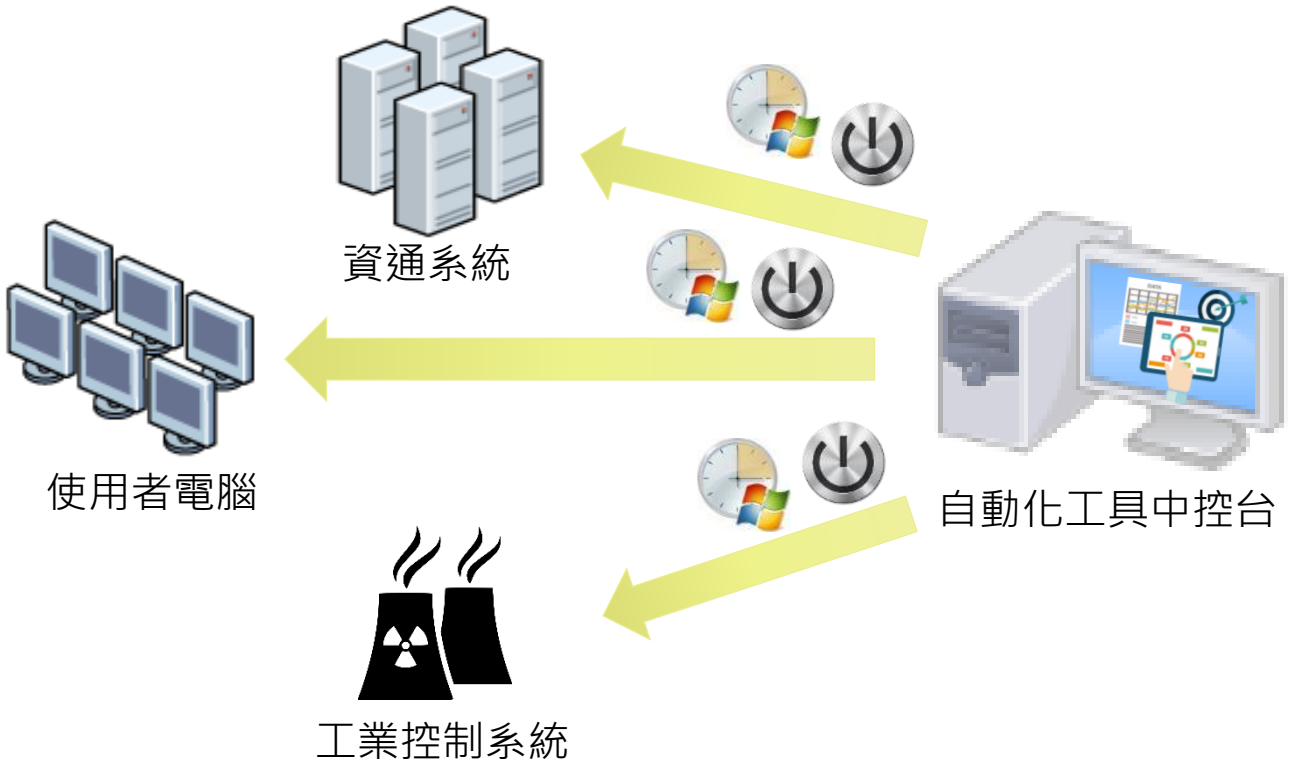
盤點作業流程



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

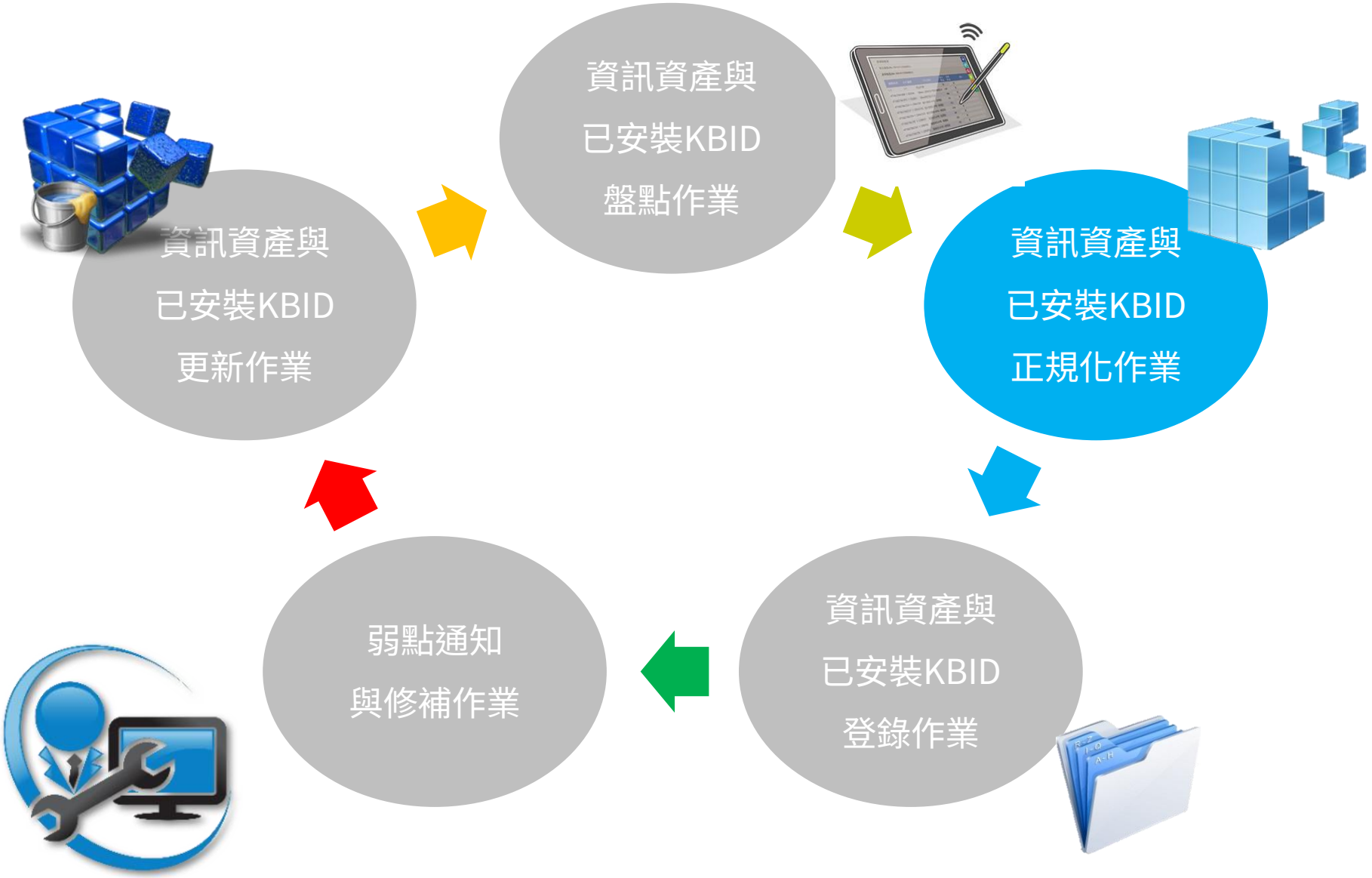
運用自動化工具盤點

- 於資通系統、使用者電腦、工業控制系統部署自動化工具
- 透過設定排程或指定條件觸發時，進行資訊資產與已安裝KBID盤點



導入作業流程

國家資通安全研究院
National Institute of Cyber Security



國家資通安全研究院
National Institute of Cyber Security

資訊資產正規化作業流程

資產群組欄位

國家資通安全研究院
National Institute of Cyber Security

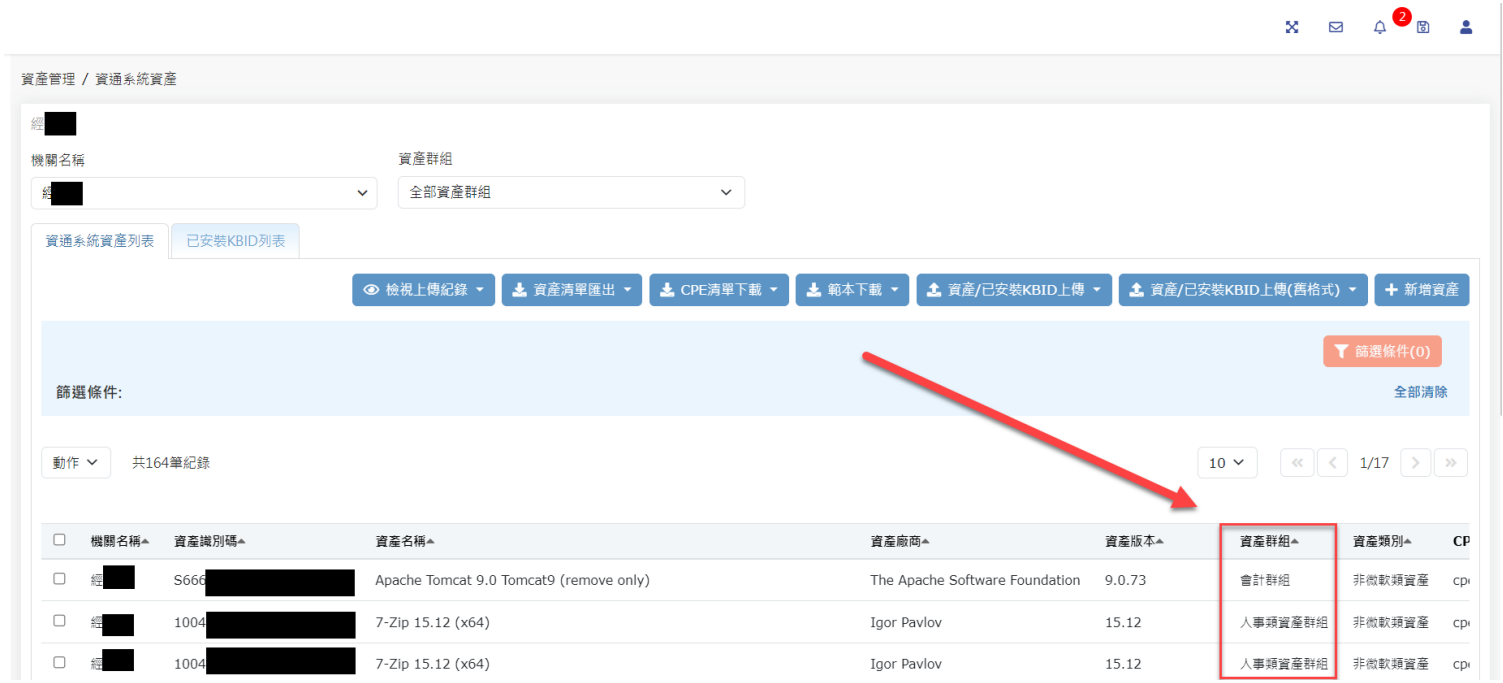
- 各機關須自行建立其所屬的資訊資產群組
- 建立資產群組
  - 登入VANS
  - 點選「系統管理>資產分群管理」
  - 新增「資產群組」與「指定資產群組使用者」
- 範例
  - HR

機關名稱	資產群組代碼	資產群組名稱	資產群組使用者	建立時間	最後修改時間	動作
經[redacted]	VANSONECOMMAG...	vans 1.0 common asset group...		2024-02-06 16:55		
經[redacted]	PROCUREMENT	採購類資產群組		2024-01-22 13:45	2024-03-20 11:28	
經[redacted]	GOVDOC	公文類資產群組		2024-01-22 13:44		
經[redacted]	Accounting	會計群組	Harry, 張[redacted]	2024-01-11 17:53	2024-01-11 18:52	
經[redacted]	MARKETING	行銷類資產群組	Sophia, Harry	2024-01-11 15:36	2024-01-11 18:50	
經[redacted]	CYBER_SECURITY	資訊安全類資訊資產	Sophia, 趙[redacted]	2024-01-11 15:36	2024-01-11 18:51	
經[redacted]	Admin	行政類資產群組	趙[redacted]	2024-01-11 15:34	2024-01-11 18:36	
經[redacted]	HR	人事類資產群組	Sophia, 張[redacted]	2024-01-11 15:34	2024-01-17 11:48	

查詢資產群組資訊

國家資通安全研究院
National Institute of Cyber Security

- 登入VANS
- 點選「資產管理>資通系統資產」或「資產管理>使用者電腦資產」
- 執行查詢資訊資產後，在資訊資產列表內可查看資產群組，如下：

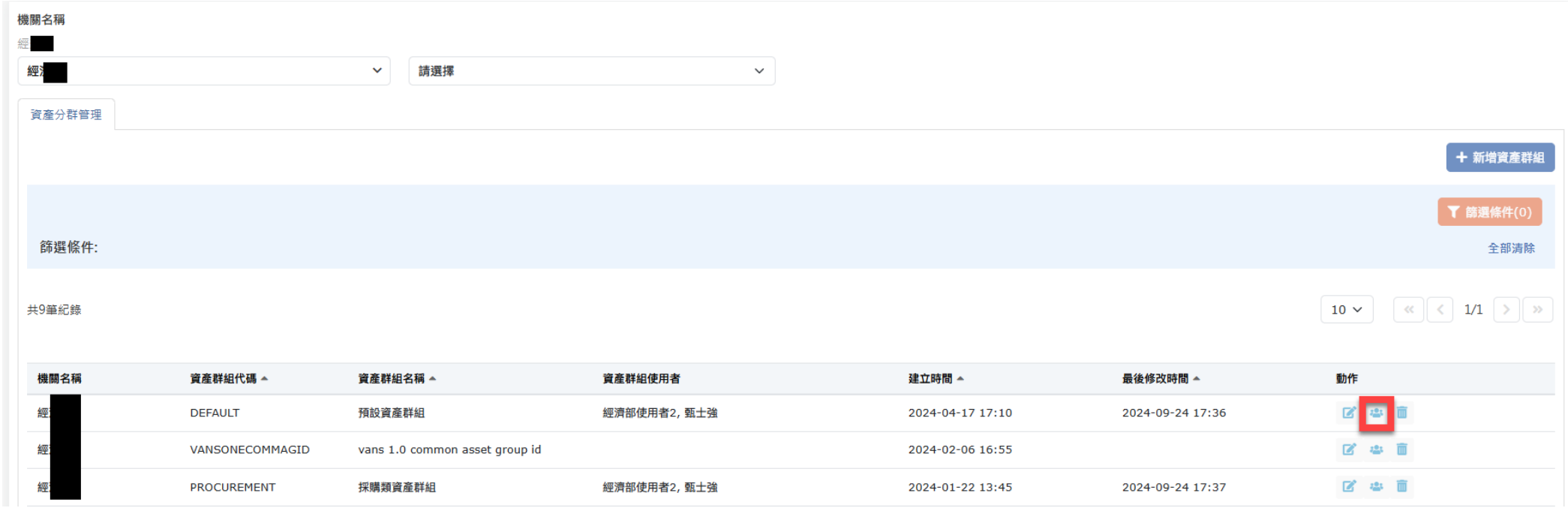


資產群組更新成員(1/2)

國家資通安全研究院
National Institute of Cyber Security

- 預設情況下只有機關管理者可檢視資產與弱點內容。故機關內其他人員在上傳資產後卻無法看到自己上傳的該資產亦無法查詢弱點比對結果，表示該員不屬於上傳該資產群組(如：DEFAULT)成員，解法如下：

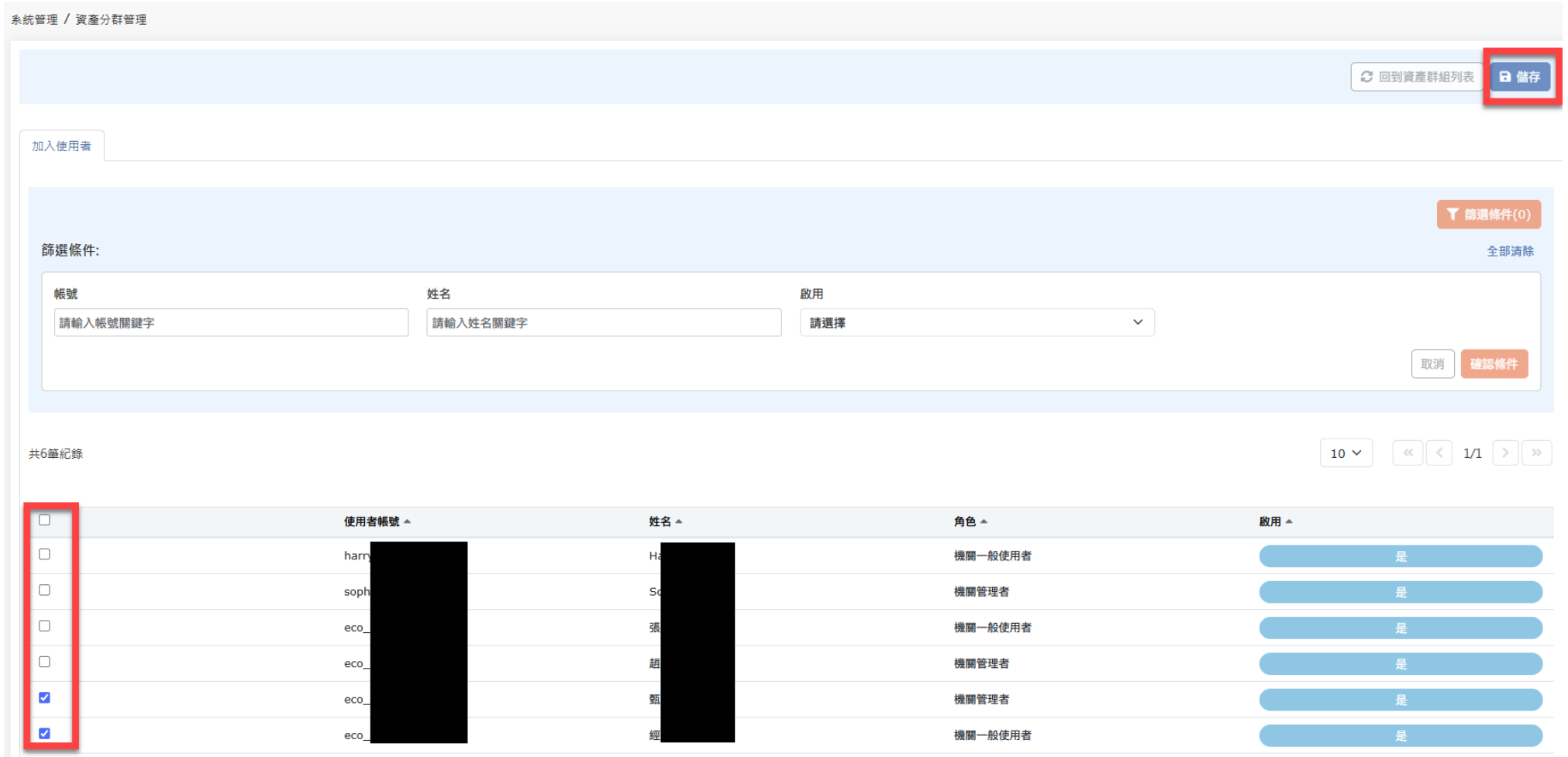
1. 由機關管理者登入VANS後，點選「系統管理>資產分群管理」
2. 點選資產群組右方人形圖示，進入「加入使用者頁面」



資產群組更新成員(2/2)

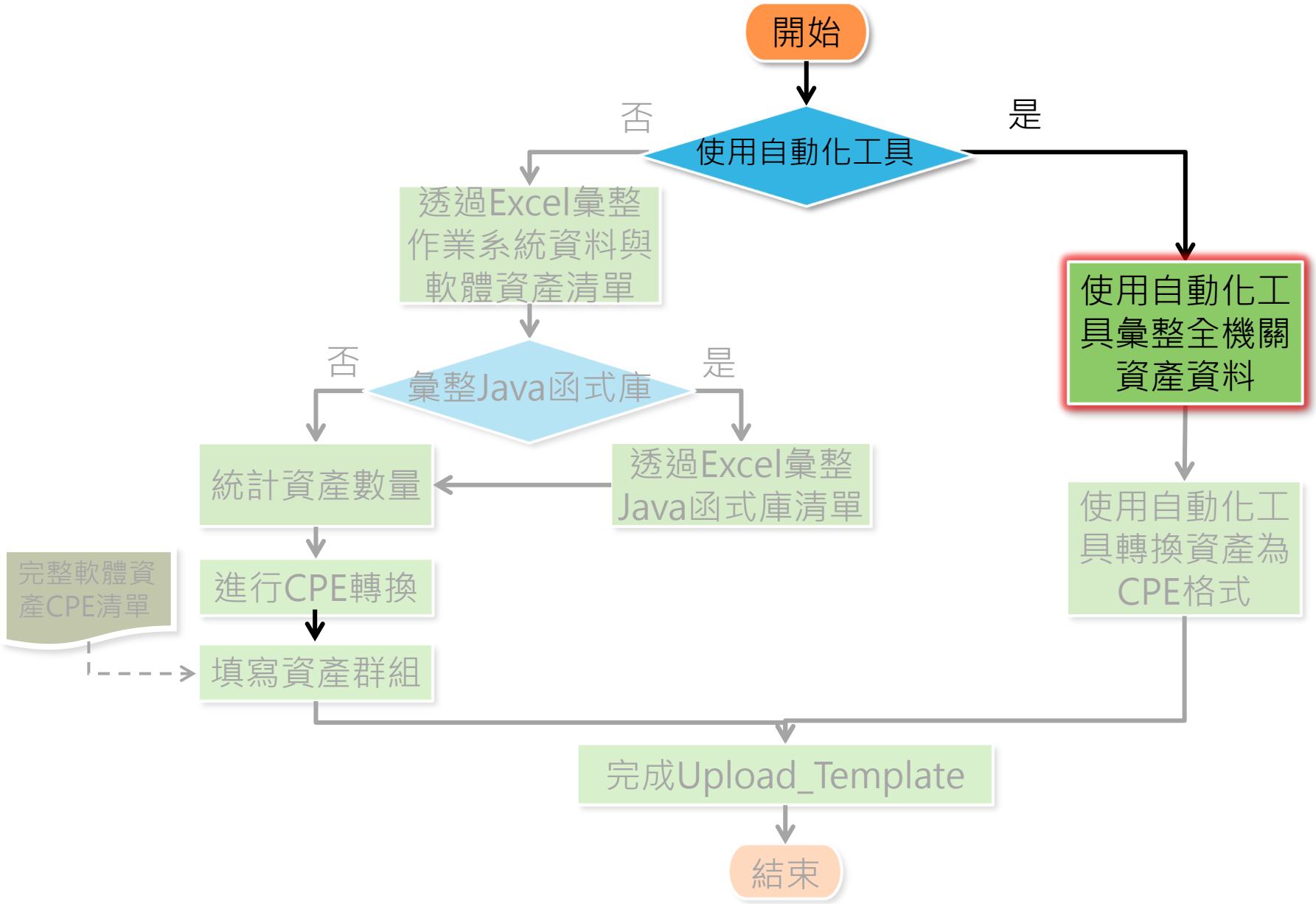
國家資通安全研究院
National Institute of Cyber Security

3. 利用翻頁或搜尋找到該人員帳號後，勾選其前面方框，並按「儲存」鈕
4. 該員即加入此資產群組，並可於資產管理功能中檢視資產與弱點



資訊資產正規化作業流程

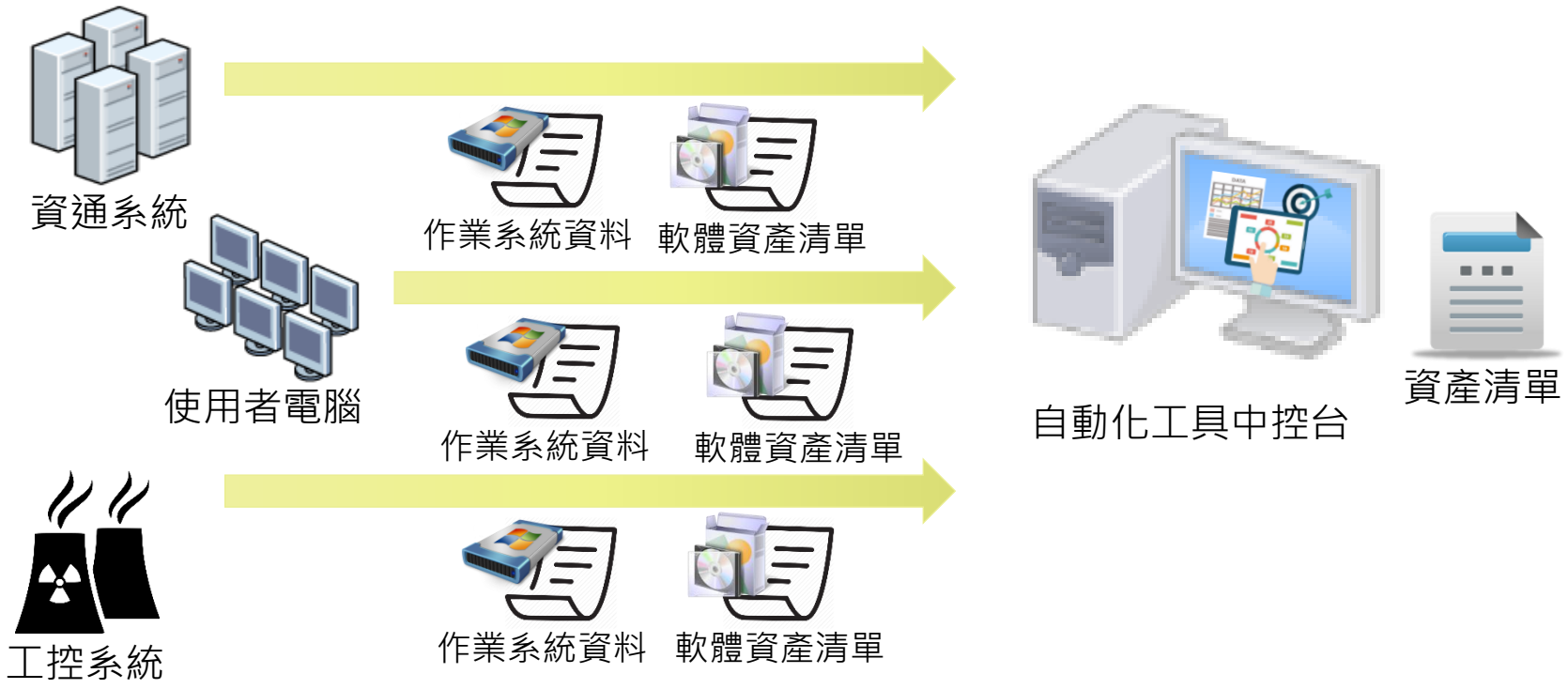
國家資通安全研究院
National Institute of Cyber Security



使用自動化工具彙整資產

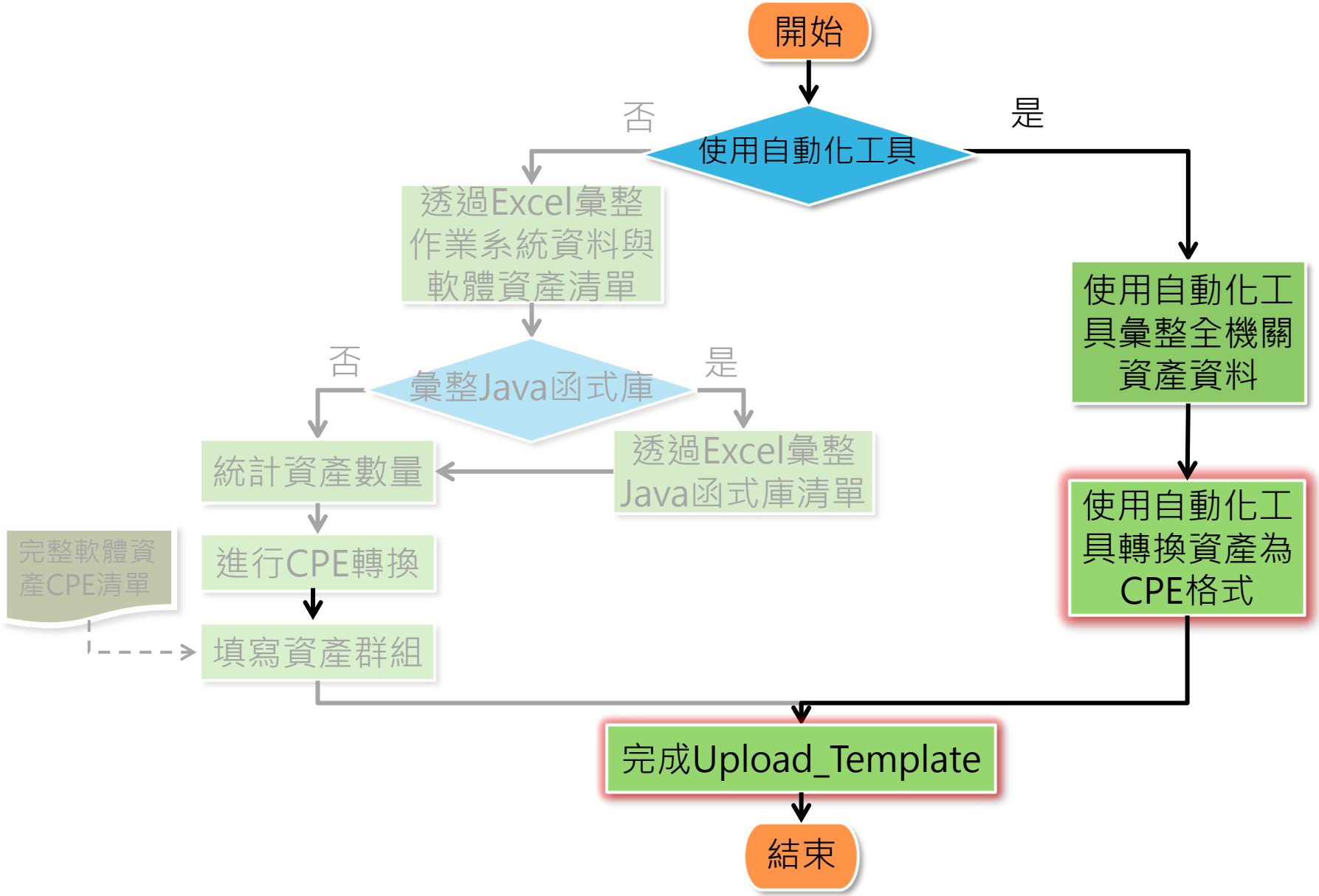
國家資通安全研究院
National Institute of Cyber Security

- 自動蒐集與彙整資通系統、使用者電腦及工業控制系統的作業系統、韌體資產(NVD歸類在軟體類別)、硬體資產及已安裝KBID等內容
- 自動去識別化整併為全機關資產清單，並提供反查對照功能，便於機關管理資產清單
- 透過排程定時回傳盤點結果予自動化工具中控台



資產正規化作業流程

國家資通安全研究院
National Institute of Cyber Security



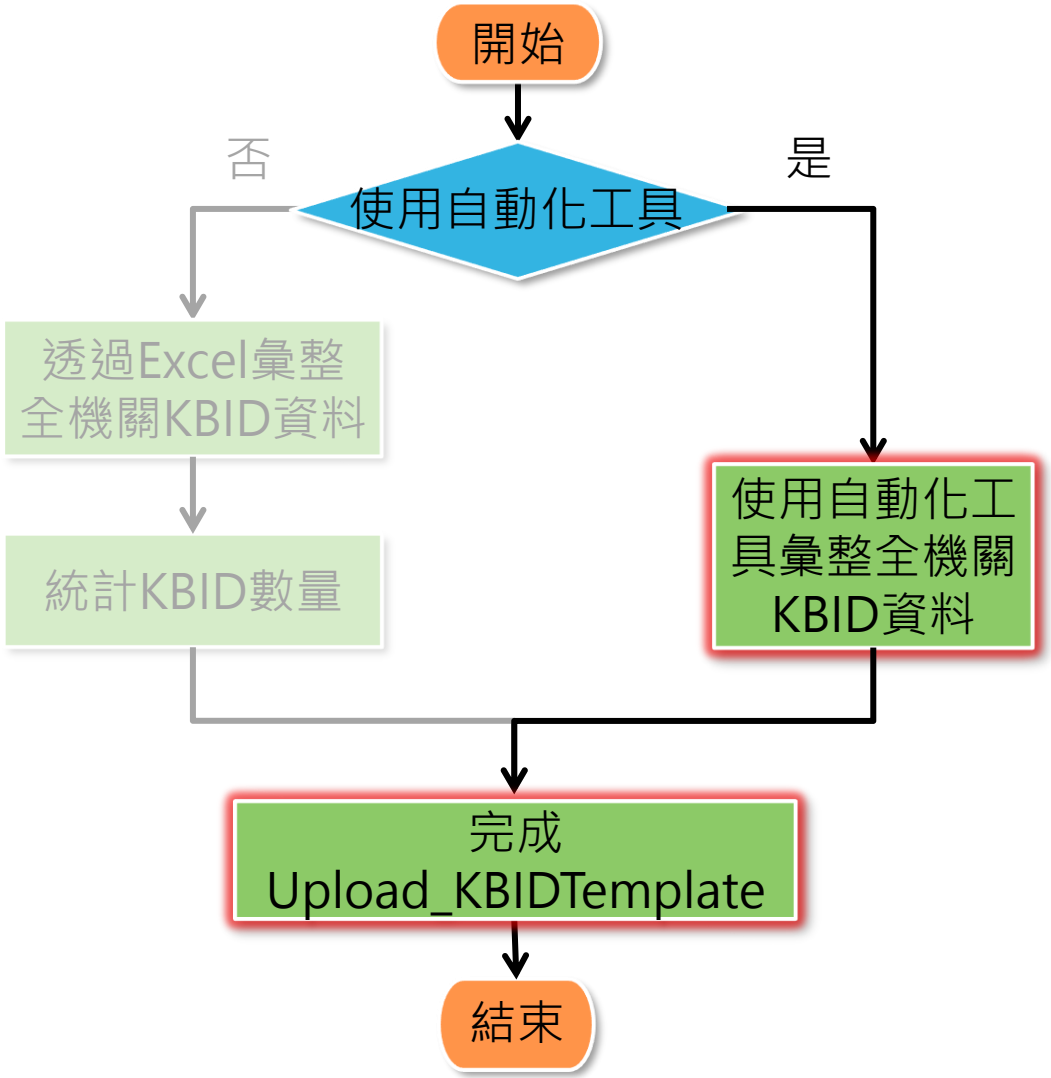
使用自動化工具轉換資產格式

國家資通安全研究院
National Institute of Cyber Security

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

已安裝KBID正規化作業

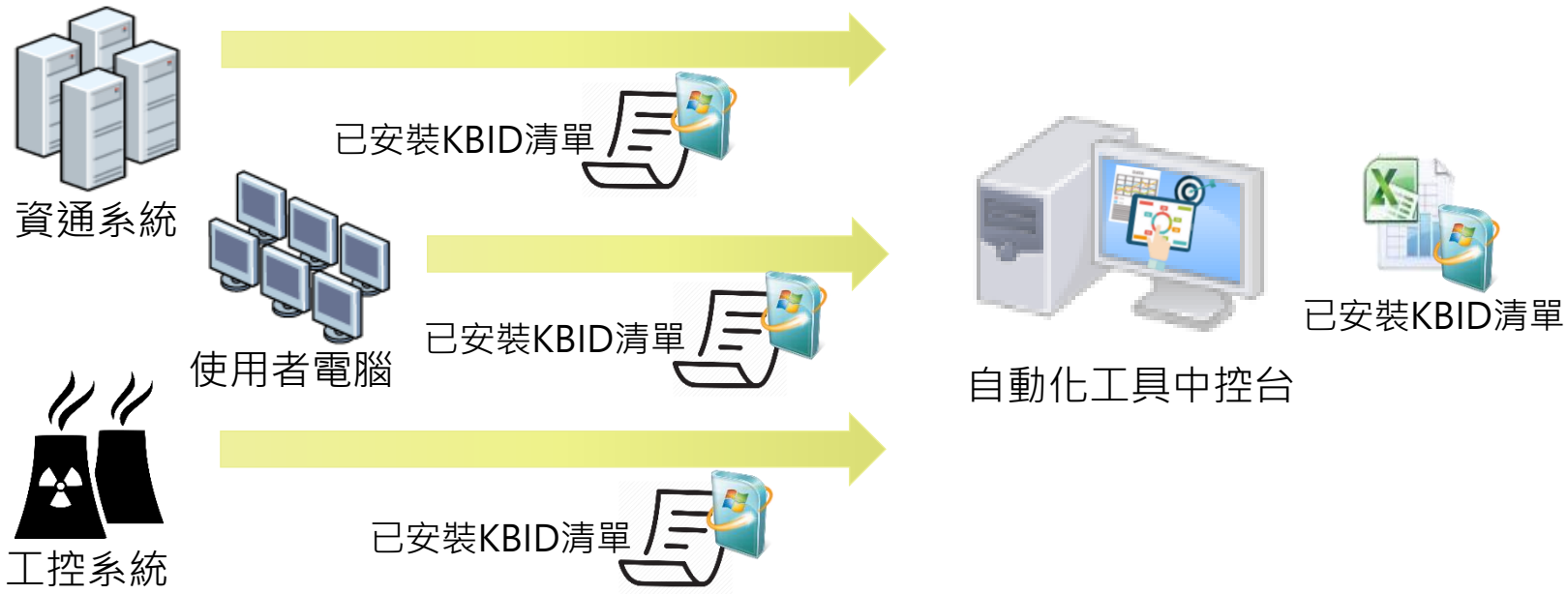
已安裝KBID正規化作業流程



使用自動化工具彙整已安裝KBID

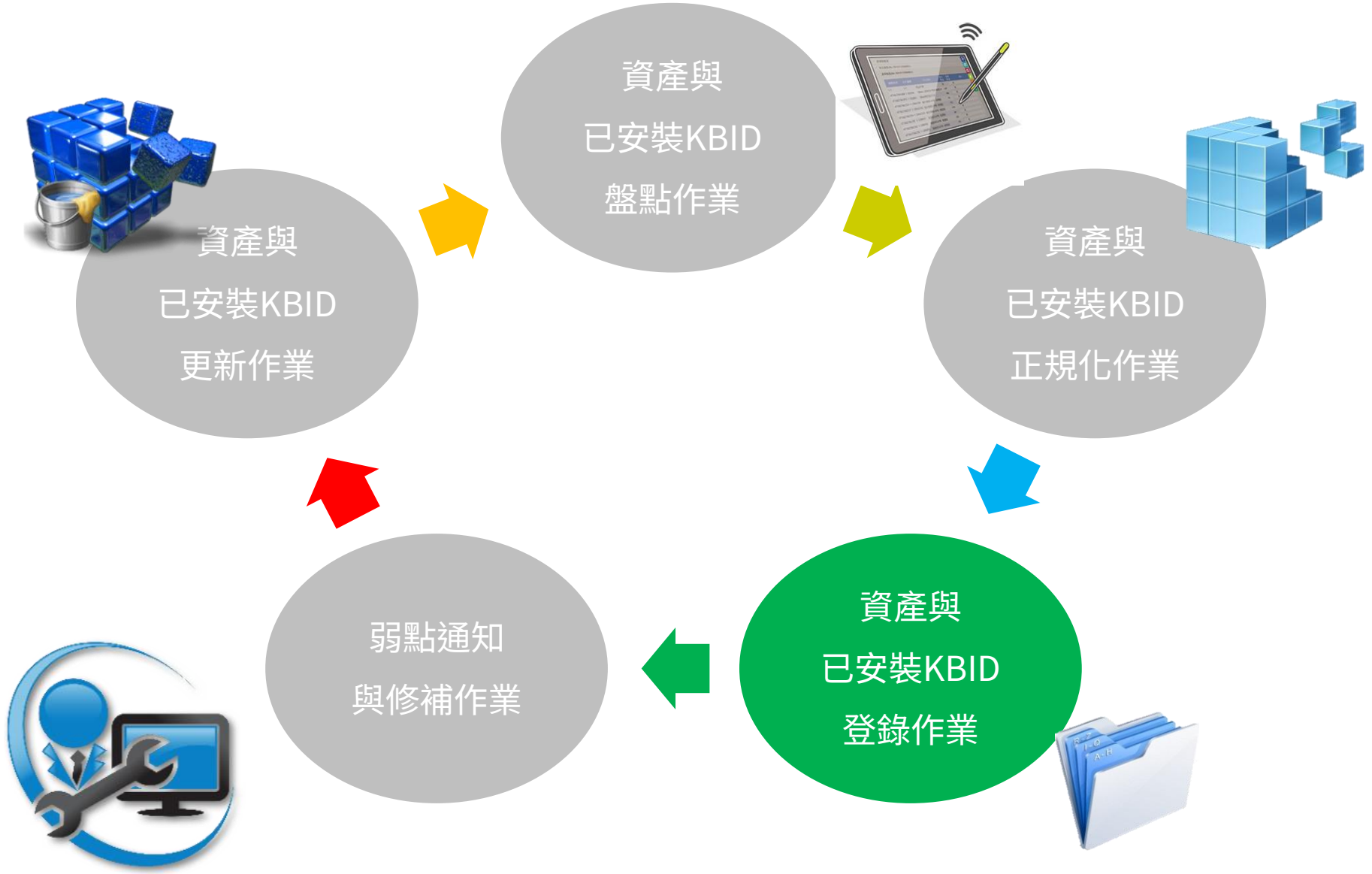
國家資通安全研究院
National Institute of Cyber Security

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

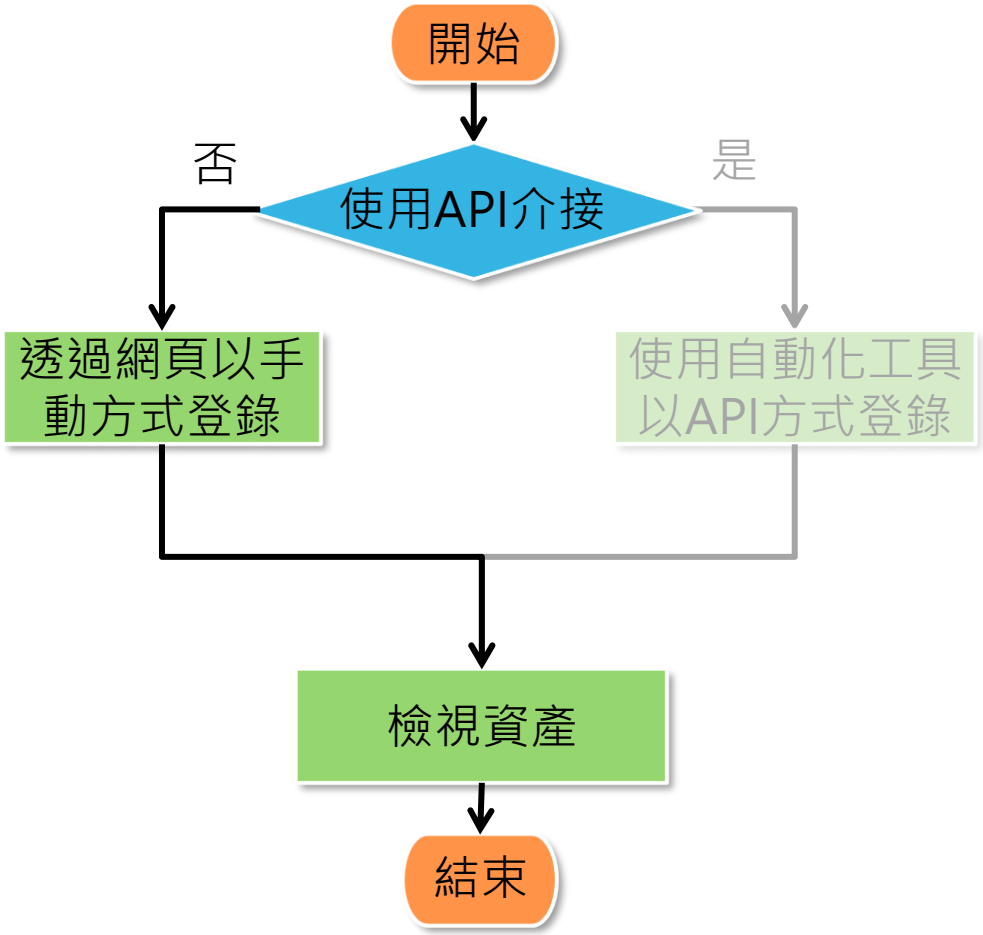


導入作業流程

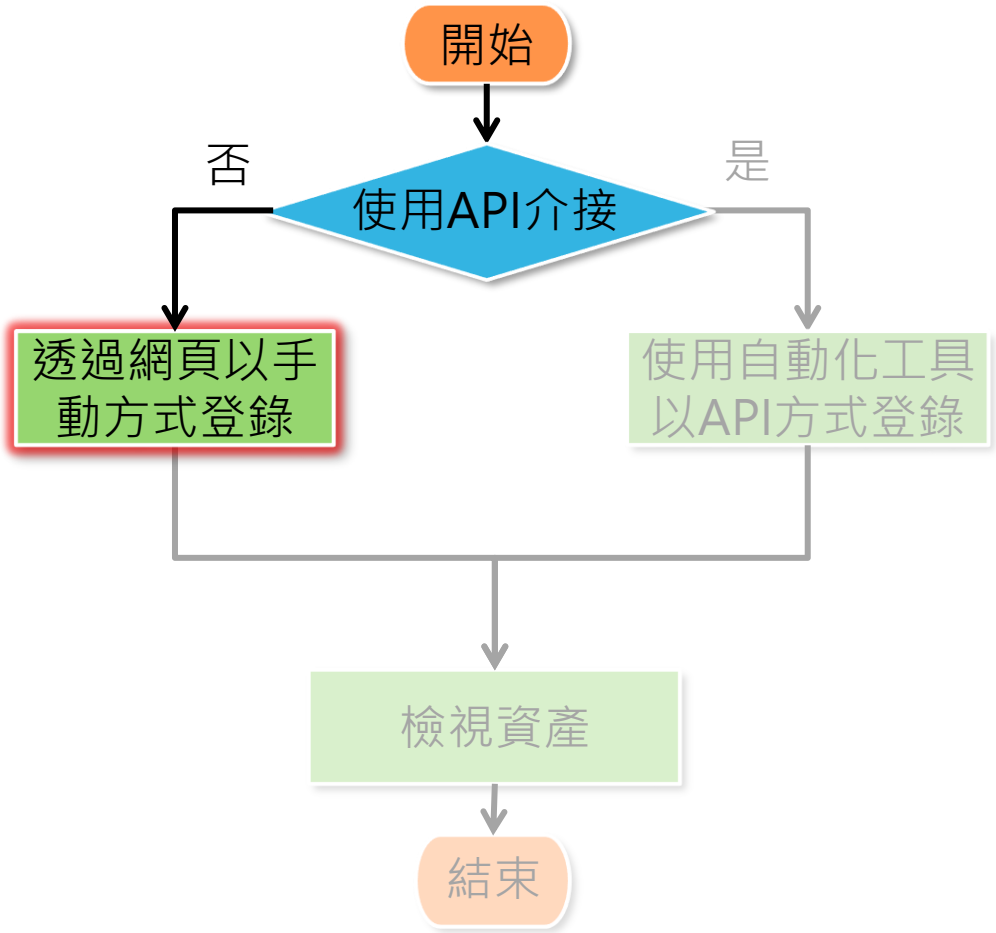
國家資通安全研究院
National Institute of Cyber Security



登錄作業流程



登錄作業流程



網頁登錄-資產(1/5)

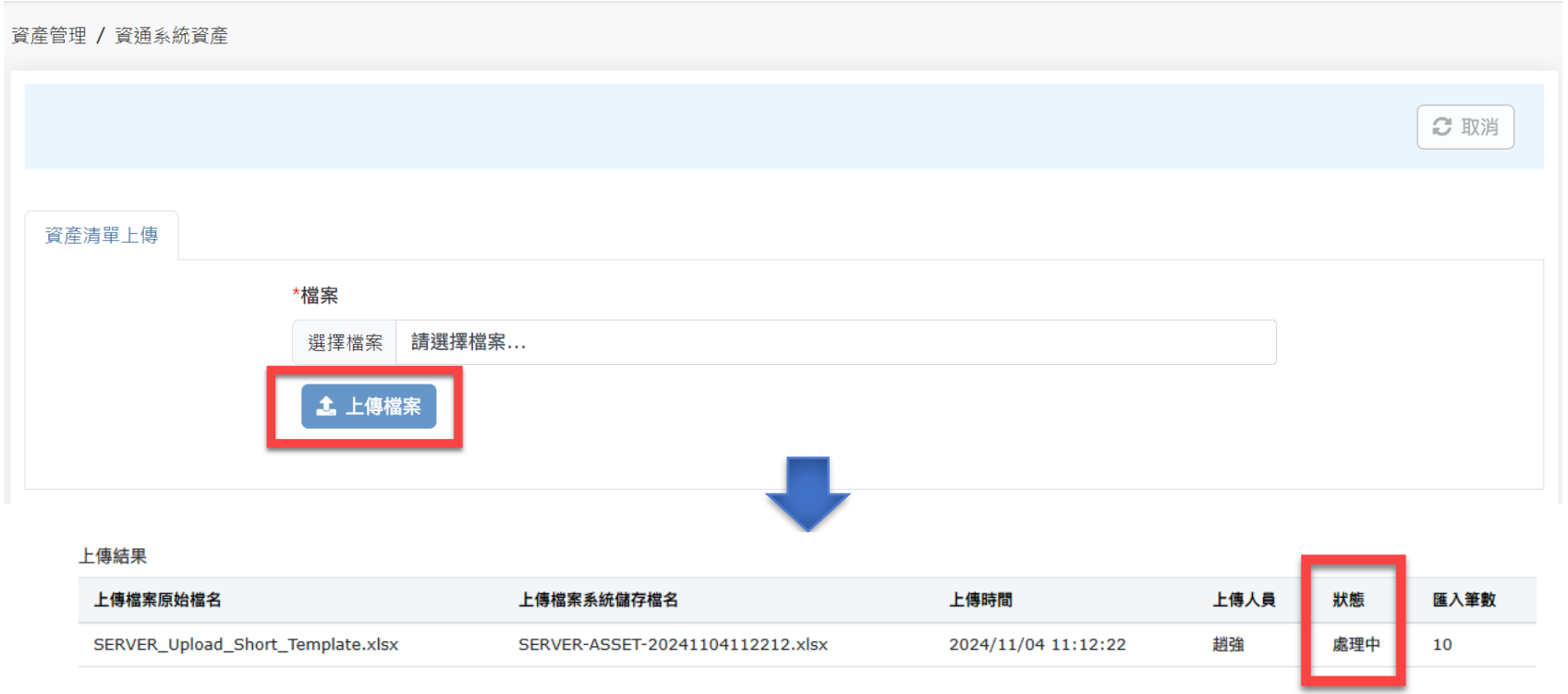
國家資通安全研究院
National Institute of Cyber Security

- STEP1：於VANS系統點選資產清單上傳
  - 資產管理>資通系統資產/使用者電腦資產/工業控制系統資產
- STEP2：選取已完成之上傳清單

網頁登錄-資產(2/5)

國家資通安全研究院
National Institute of Cyber Security

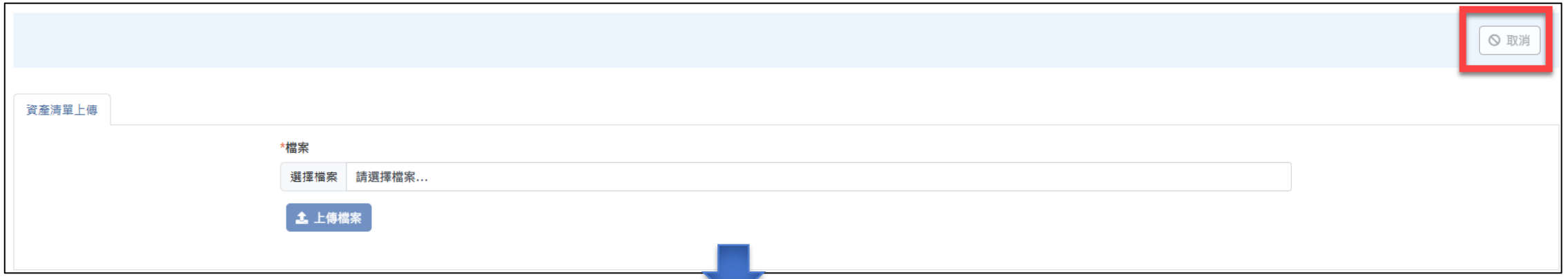
- STEP3：點選「上傳檔案」，由系統初步判讀檔案
- STEP4：系統顯示上傳完成，狀態為「處理中」，檔案進入系統解析階段，待解析完收到成功結果通知信後，方可檢視剛上傳之資產



網頁登錄-資產(3/5)

國家資通安全研究院
National Institute of Cyber Security

- STEP5：按「取消鈕」，回到列表頁



網頁登錄-資產(4/5)

國家資通安全研究院
National Institute of Cyber Security

- STEP6：按「檢視上傳紀錄」鈕，選「檢視資產清單上傳紀錄」查看解析結果
  - –顯示「處理中」表示系統仍在解析資產
  - –顯示「成功」表示資產上傳完成
  - –顯示「失敗」則要看郵件通知訊息查看原因

網頁登錄-資產(5/5)

國家資通安全研究院
National Institute of Cyber Security

- STEP7：按右上方的「郵件」圖示，檢視系統所發出的解析結果訊息，依錯誤訊息進行對應處理
- 若訊息為「須待資產弱點比對完成後才可再上傳資產」，表示前一次上傳之資產尚未完成弱點比對，請在收到弱點比對通知信後再進行下一次上傳

網頁登錄-已安裝KBID(1/2)

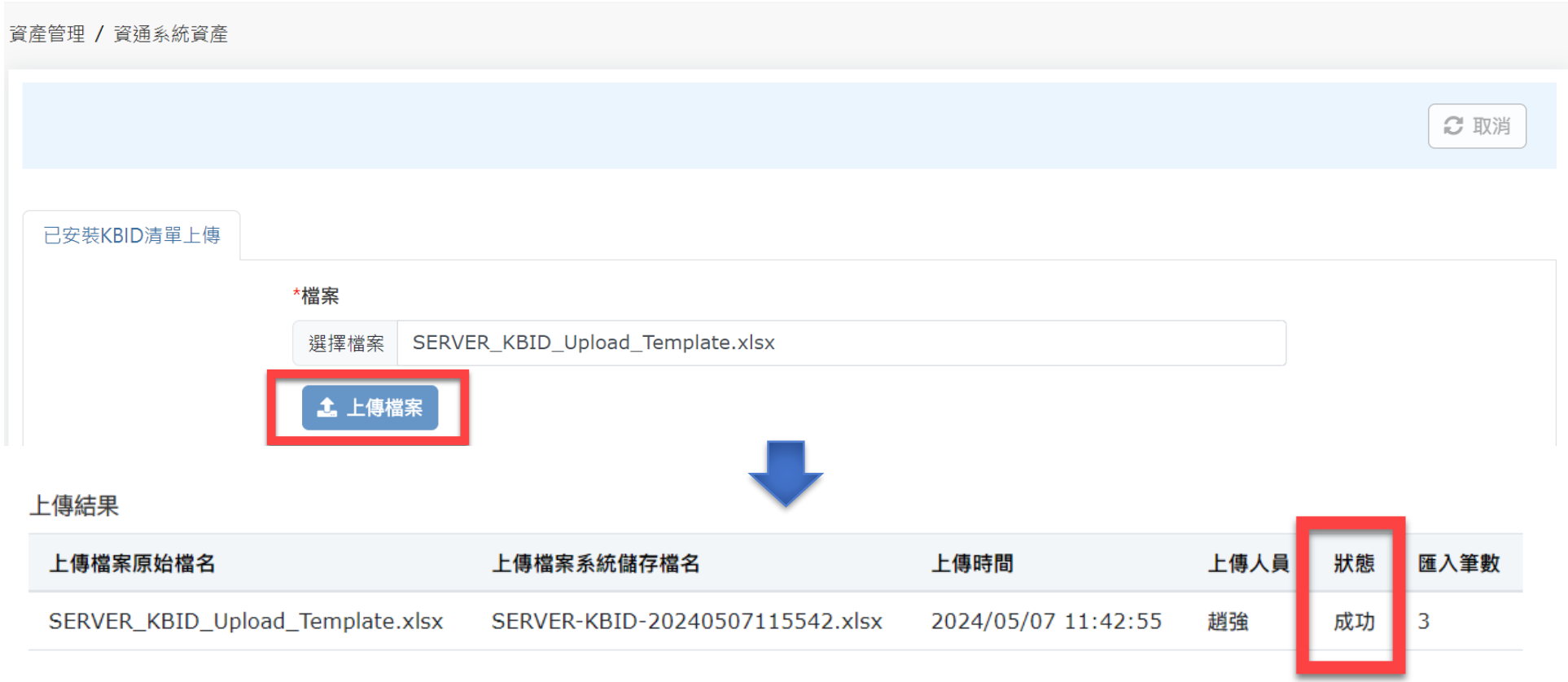
國家資通安全研究院
National Institute of Cyber Security

- STEP1：於VANS系統進行已安裝KBID清單上傳
  - 資產管理>資通系統資產/使用者電腦資產/工業控制系統資產
- STEP2：瀏覽並上傳已完成之上傳清單

網頁登錄-已安裝KBID(2/2)

國家資通安全研究院
National Institute of Cyber Security

- STEP3：點選「上傳檔案」，等待系統解析清單
- STEP4：系統顯示解析成功，即完成登錄



WSUS解析-已安裝KBID(1/4)

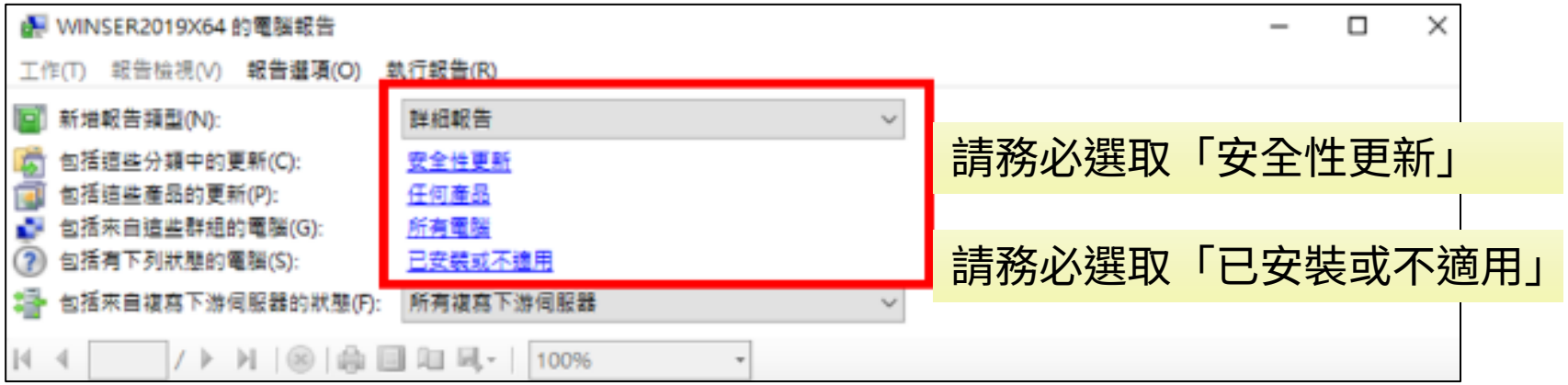
國家資通安全研究院
National Institute of Cyber Security

- 透過解析從WSUS匯出之電腦報告，產出已安裝KBID清單，供使用者上傳至資通系統、使用者電腦及工業控制系統資產列表
- STEP1：請點選「報告」→選擇「電腦詳細狀態」

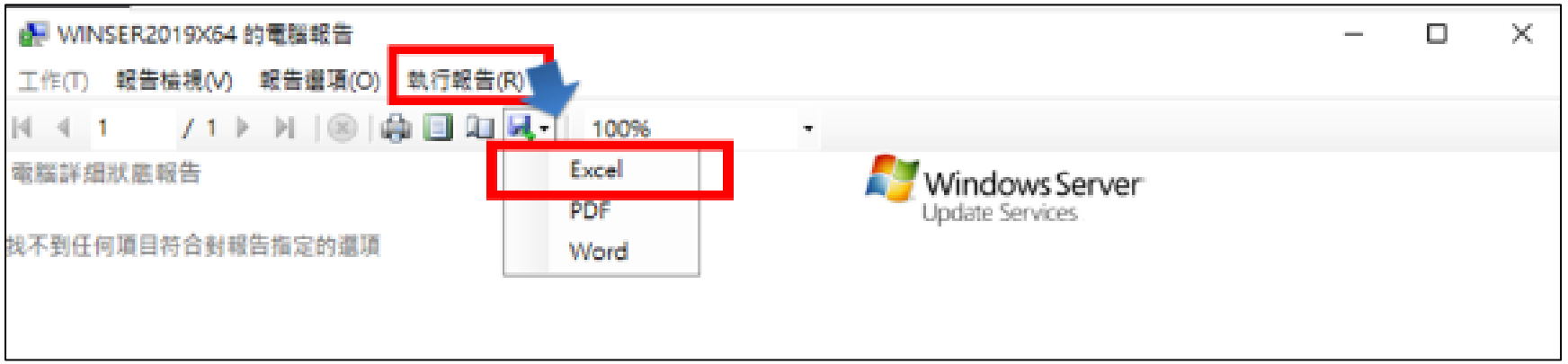
WSUS解析-已安裝KBID(2/4)

國家資通安全研究院
National Institute of Cyber Security

- STEP2：WSUS報告-選擇「報告選項」→「詳細報告」，選擇欲上傳解析的產品種類與已安裝的KBID



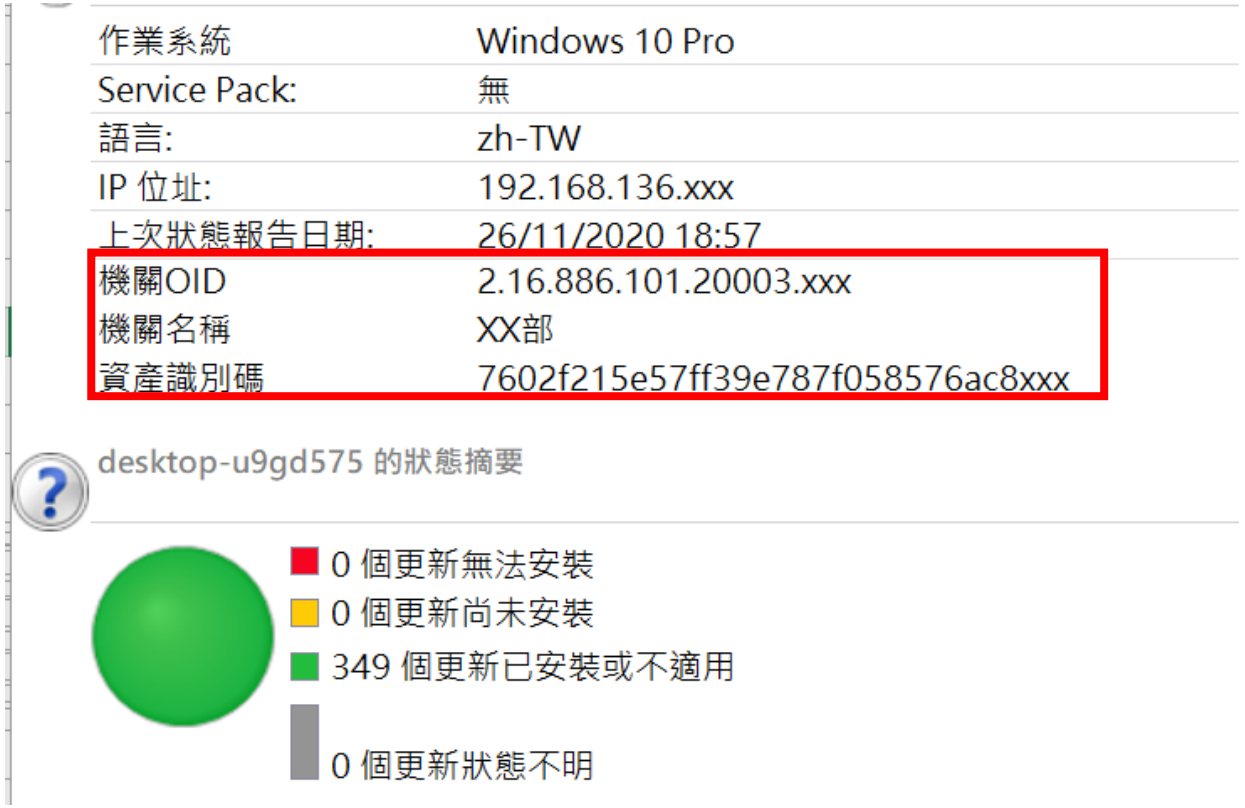
- STEP3：WSUS報告-選擇「執行報告」→選擇「Excel」



WSUS解析-已安裝KBID(3/4)

國家資通安全研究院
National Institute of Cyber Security

- STEP4：開啟WSUS報告-進到每一個「電腦詳細報告」頁籤內→在「機關名稱」資料列下，新增1列，並填上固定字串「資產識別碼」與此電腦之資產識別碼資料值

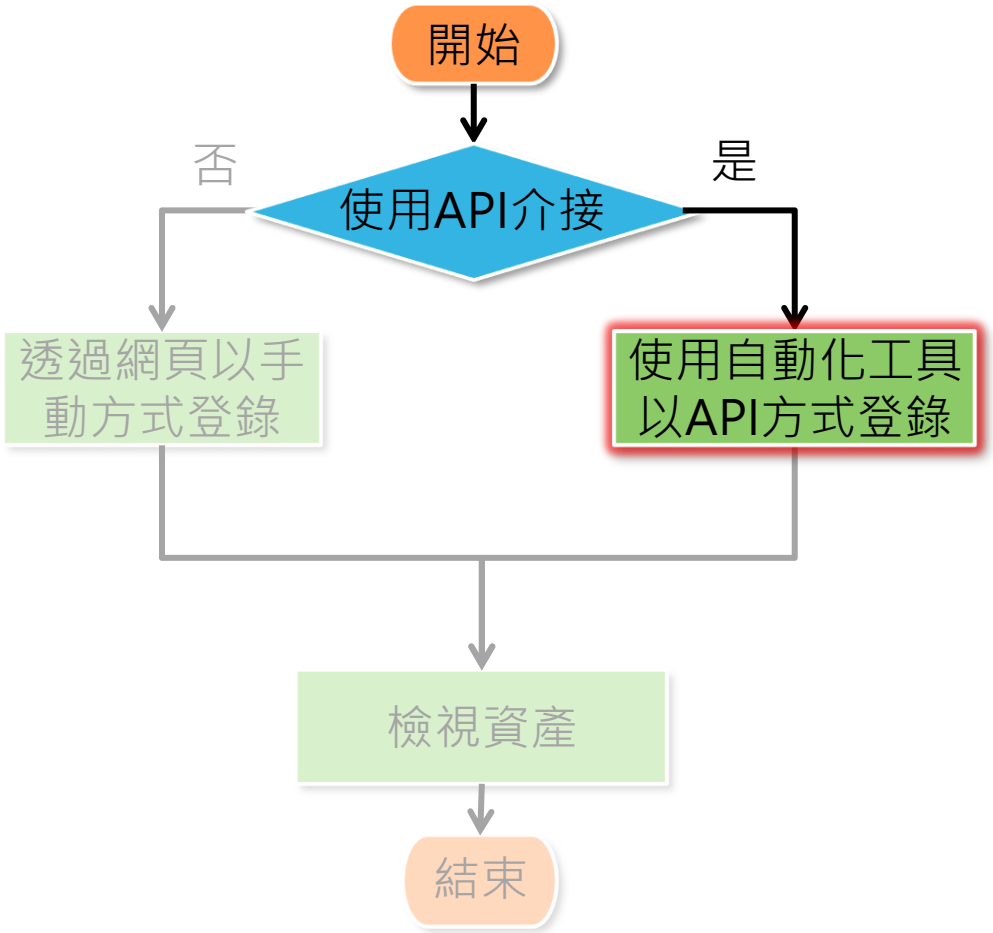


網頁登錄-WSUS報告上傳(4/4)

國家資通安全研究院
National Institute of Cyber Security

- STEP5：可運用「WSUS報告解析」功能產出已安裝KBID清單，以降低人工作業時間成本
- 於VANS系統進行WSUS報告上傳
  - 資產管理>資通系統資產/使用者電腦資產/工業控制系統
  - 瀏覽並上傳已完成之上傳清單

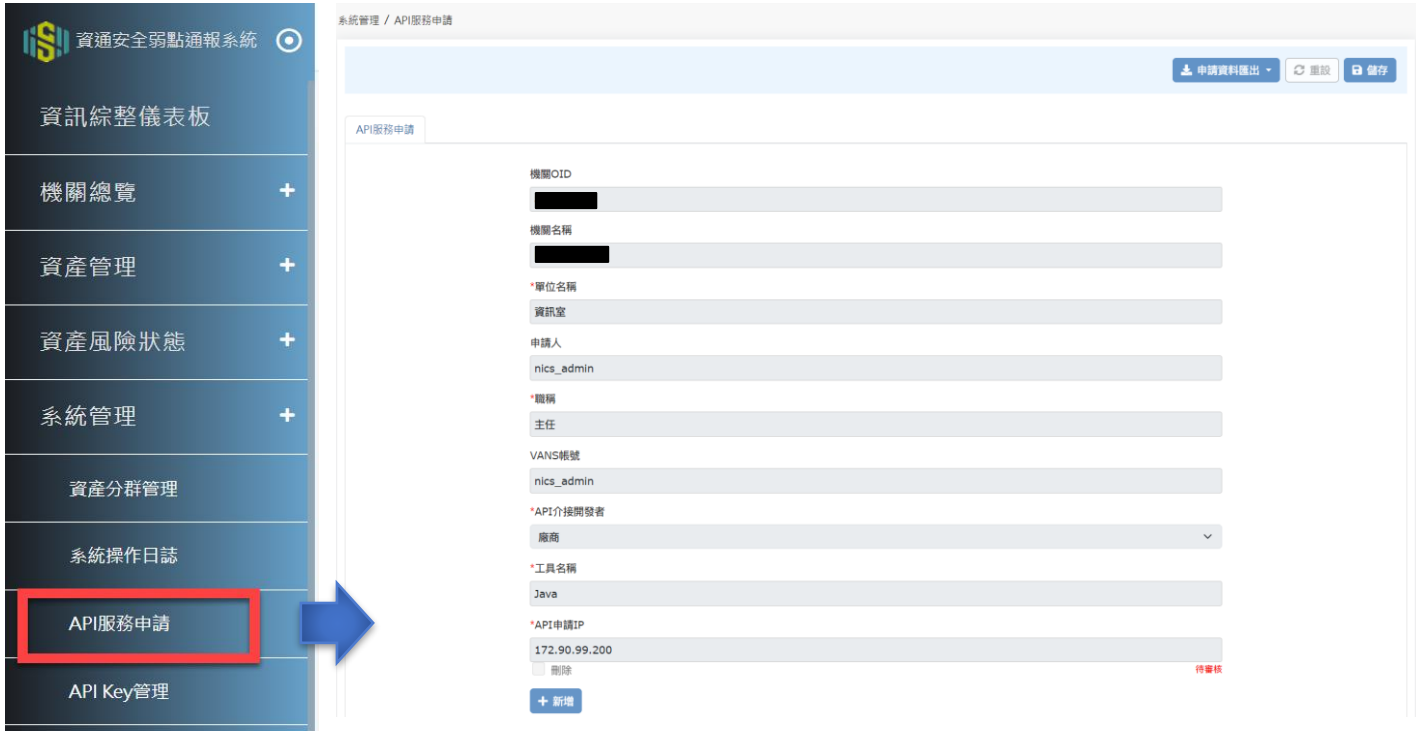
登錄作業流程



使用自動化工具以API方式登錄(1/3)

國家資通安全研究院
National Institute of Cyber Security

- 前置作業申請-填寫API介接IP申請單
  - STEP1：以機關管理者帳號登入VANS系統
  - STEP2：點選系統管理->API服務申請
  - STEP3：輸入欲申請之資料與IP，並儲存
  - STEP4：點選「申請資料匯出」鈕，將文件列印核章後，提交資安署審核



使用自動化工具以API方式登錄(2/3)

國家資通安全研究院
National Institute of Cyber Security

- 前置作業申請-於VANS系統更換API Key
  - STEP1：以機關管理者帳號登入VANS系統
  - STEP2：點選系統管理->API Key管理
  - STEP3：點選「重新產生」鈕以更換API Key

使用自動化工具以API方式登錄(3/3)

國家資通安全研究院
National Institute of Cyber Security

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

VANS_API_KBID_Sample.json .json 檔案 | VANS_API_Sample.json .json 檔案 | VANS系統API功能說明v0.8_1120204.pdf .pdf 檔案

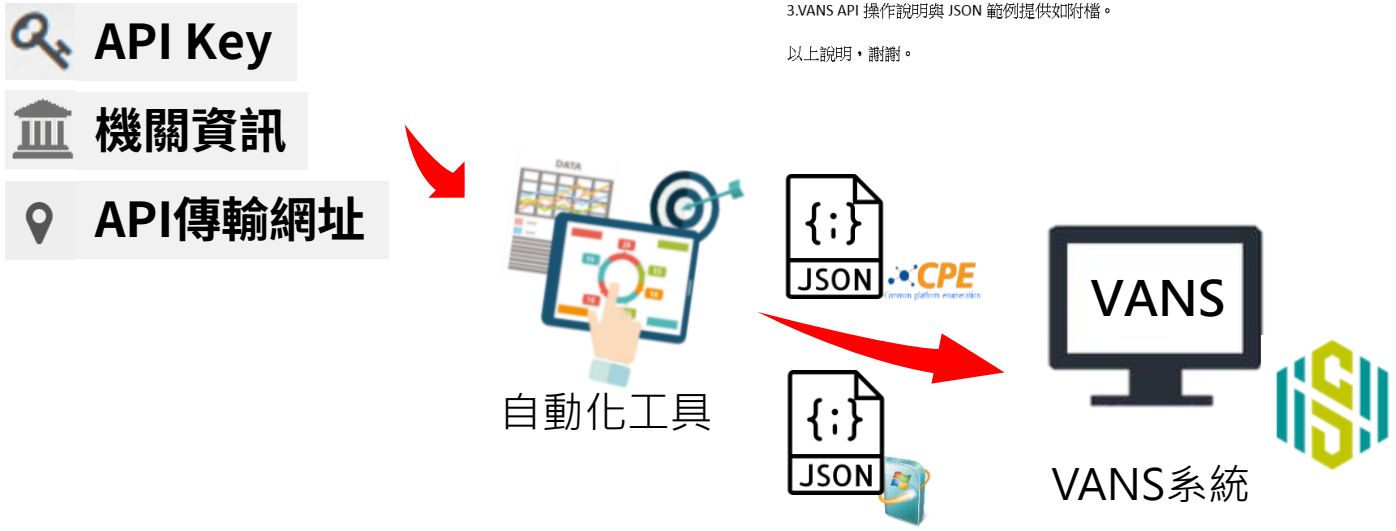
您好:

1.貴單位的 VANS API 介接 IP 已完成開通，可透過 API 方式傳輸資訊資產至 VANS 系統。

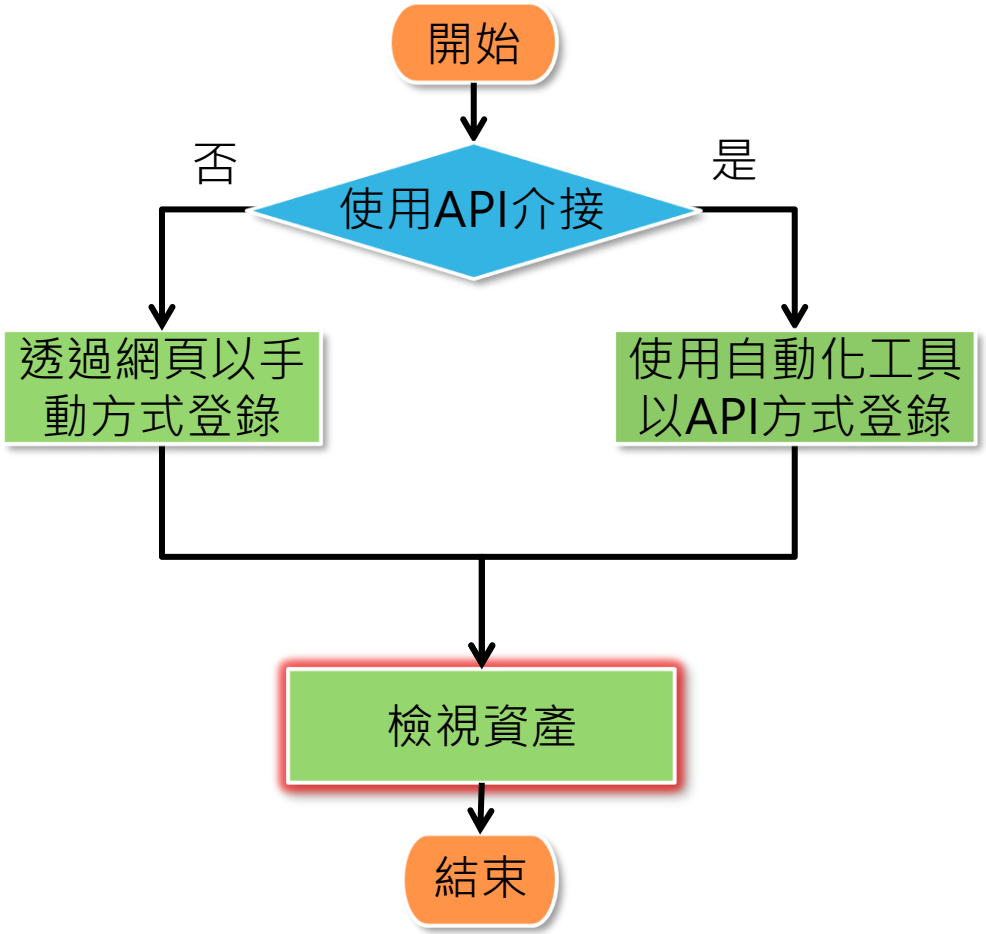
2.VANS 系統對外 IP：[redacted]
VANS API 傳輸使用 port：[redacted]
VANS API 傳輸網址如下：
a.資訊資產
資通系統(System)：
https://vans.nat.gov.tw[redacted]
使用者電腦(Computer)：
https://vans.nat.gov.tw[redacted]
b.已安裝 KBID
資通系統(System)：
https://vans.nat.gov.tw[redacted]
使用者電腦(Computer)：
https://vans.nat.gov.tw[redacted]

3.VANS API 操作說明與 JSON 範例提供如附檔。

以上說明，謝謝。



登錄作業流程



檢視資產

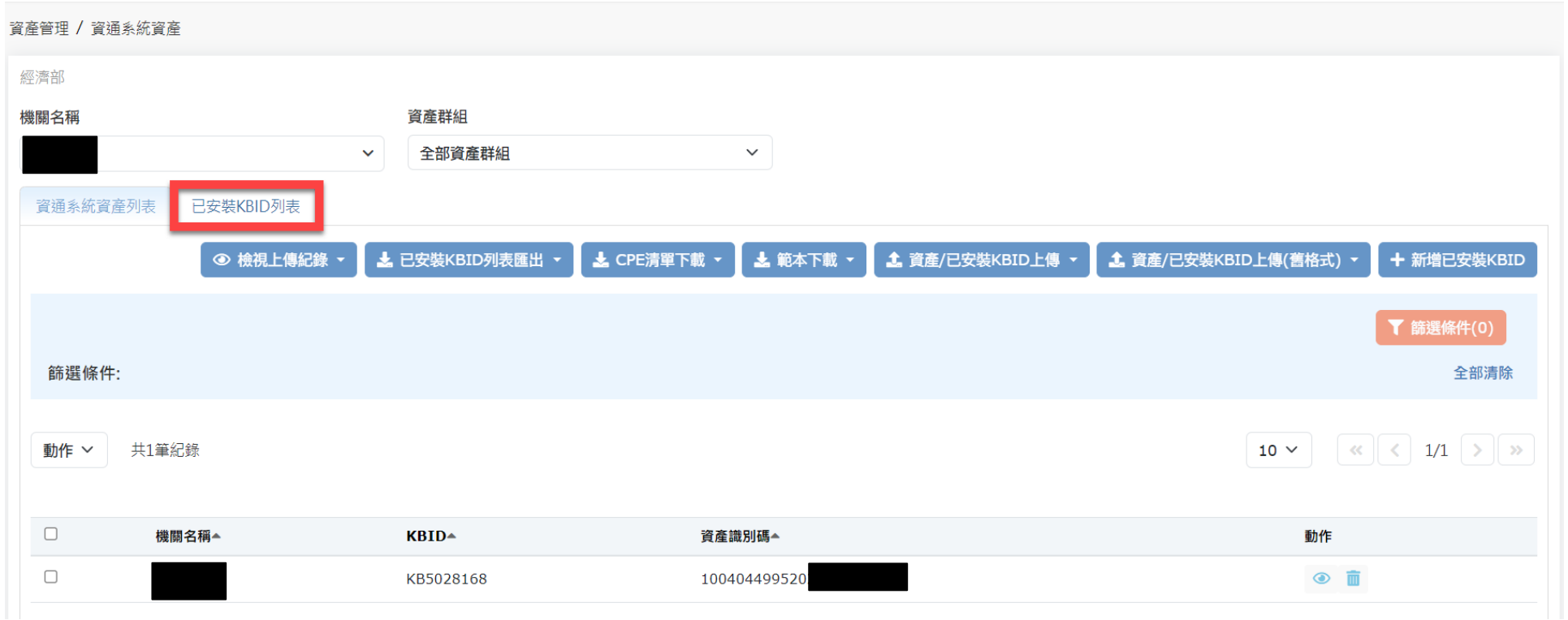
國家資通安全研究院
National Institute of Cyber Security

- 可於資產管理查看已登錄之資產項目
  - 資產管理->資通系統資產/使用者電腦資產/工業控制系統資產

檢視已安裝KBID列表

國家資通安全研究院
National Institute of Cyber Security

- 點選「已安裝KBID列表」頁籤可檢視已安裝KBID項目



檢視資產上傳紀錄

國家資通安全研究院
National Institute of Cyber Security

- 上傳資產或已安裝KBID後，若資產列表或已安裝KBID列表仍無資料，可點選「資產上傳紀錄」檢視過往的上傳紀錄

上傳失敗案例與解決方式(1/5)

國家資通安全研究院
National Institute of Cyber Security

- 若遭遇VANS系統使用上之問題，建議以下列格式來信(VansService@nics.nat.gov.tw)信箱詢問，以加快處理速度
- 格式如下

  1.機關名稱：

  2.上傳方式：

  3.上傳使用檔案：

  4.上傳時間：

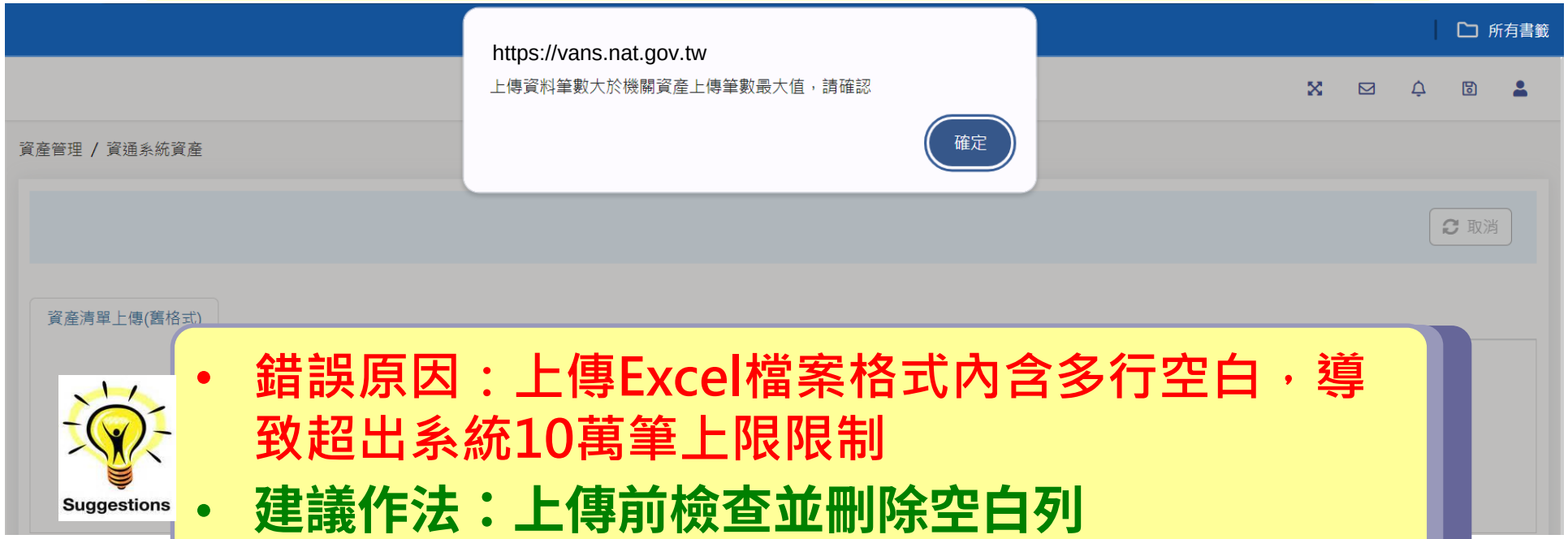
  5.錯誤訊息截圖：

  6.補充說明：

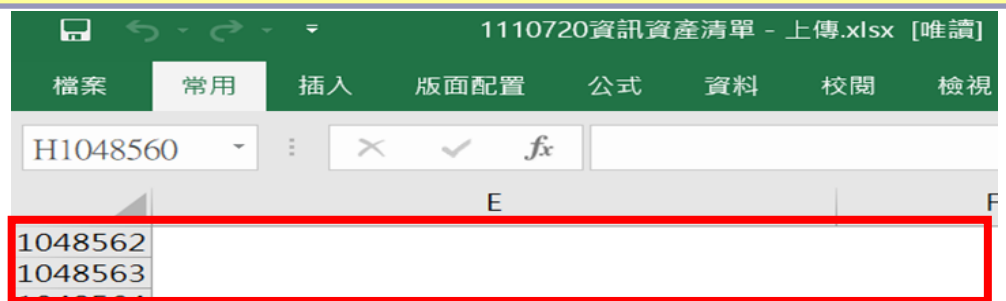
上傳失敗案例與解決方式(2/5)

國家資通安全研究院
National Institute of Cyber Security

案例1.透過網頁登錄資產時，出現「上傳資料筆數大於機關資產上傳筆數最大值」錯誤訊息，該如何處理？



- **錯誤原因：上傳Excel檔案格式內含多行空白，導致超出系統10萬筆上限限制**
- **建議作法：上傳前檢查並刪除空白列**



上傳失敗案例與解決方式(3/5)

國家資通安全研究院
National Institute of Cyber Security

案例2.透過網頁上傳資產，系統顯示『資產群組未驗證通過，不存在本系統』時，該如何處理？

錯誤資料

錯誤訊息	機關OID	機關名稱	資產識別碼
機關OID+資產群組，未驗證通過，不存在本系統	2.16.886.[redacted]	[redacted]	7602f215e57ff39e7[redacted]

Suggestions

- **上傳前請檢查資產群組是否存在資產群組清單中**

機關OID	機關名稱	資產識別碼	資產群組
2.16.886.101.90010.xxxxx	XXX政府	7602f215e57ff39e787f058576ac8xxx	HR
2.16.886.101.90010.xxxxx	XXX政府	7602f215e57ff39e787f058576ac8xxx	GOVDOC
2.16.886.101.90010.xxxxx	XXX政府	7602f215e57ff39e787f058576ac8xxx	GOVDOC
2.16.886.101.90010.xxxxx	XXX政府	7602f215e57ff39e787f058576ac8xxx	GOVDOC
2.16.886.101.90010.xxxxx	XXX政府	7602f215e57ff39e787f058576ac8xxx	GOVDOC
2.16.886.101.90010.xxxxx	XXX政府	7602f215e57ff39e787f058576ac8xxx	GOVDOC

上傳失敗案例與解決方式(4/5)

國家資通安全研究院
National Institute of Cyber Security

案例3.透過網頁上傳已安裝KBID後，顯示上傳失敗，該如何處理？

錯誤資料

錯誤訊息	機關OID	機關名稱	資產識別碼	已安裝KBID
已安裝KBID資料格式有誤，請確認	2.16.886.101.90027.20002	[redacted]	7602f215e57ff39e787f[redacted]	3121212

Suggestions

- **上傳前請檢查KBID清單是否符合下列格式要求：**
  - **已安裝KBID數量：純數字**
  - **已安裝KBID：KB+純數字**

2.16.886.101.90027.XXXXX	XXX政府	7602f215e57ff39e787f058576ac8111	KB3121918
2.16.886.101.90027.XXXXX	XXX政府	7602f215e57ff39e787f058576ac8111	KB3121212
2.16.886.101.90027.XXXXX	XXX政府	7602f215e57ff39e787f058576ac8444	KB5016679
2.16.886.101.90027.XXXXX	XXX政府	7602f215e57ff39e787f058576ac8444	3121212

上傳失敗案例與解決方式(5/5)

國家資通安全研究院
National Institute of Cyber Security

案例4.使用相同資料來源轉換成不同格式，可成功透過網頁以Excel方式上傳，但透過API方式上傳出現「0301」錯誤訊息，該如何解決？

```
{
    "status": false,
    "code": "AST-PC-0301",
    "message": "JSON檔案資料格式錯誤"
}
```

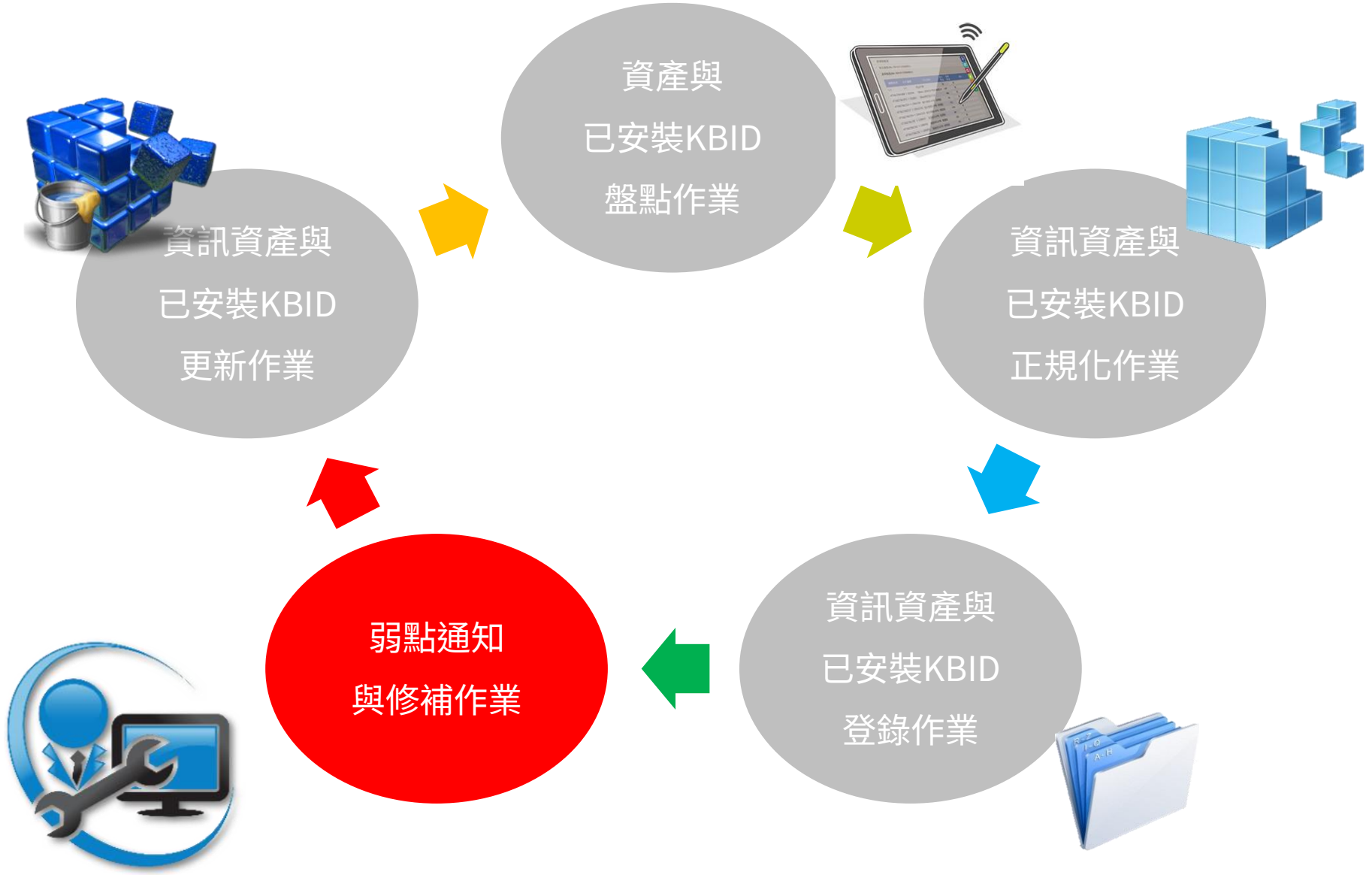
- **上傳前可檢查有無跳脫字元，若有，請於跳脫字元前額外增加一個反斜線，以利系統識別與解析**

錯誤寫法："brand" : "Google\Chrome"
正確寫法： "brand" : "Google \\ Chrome"

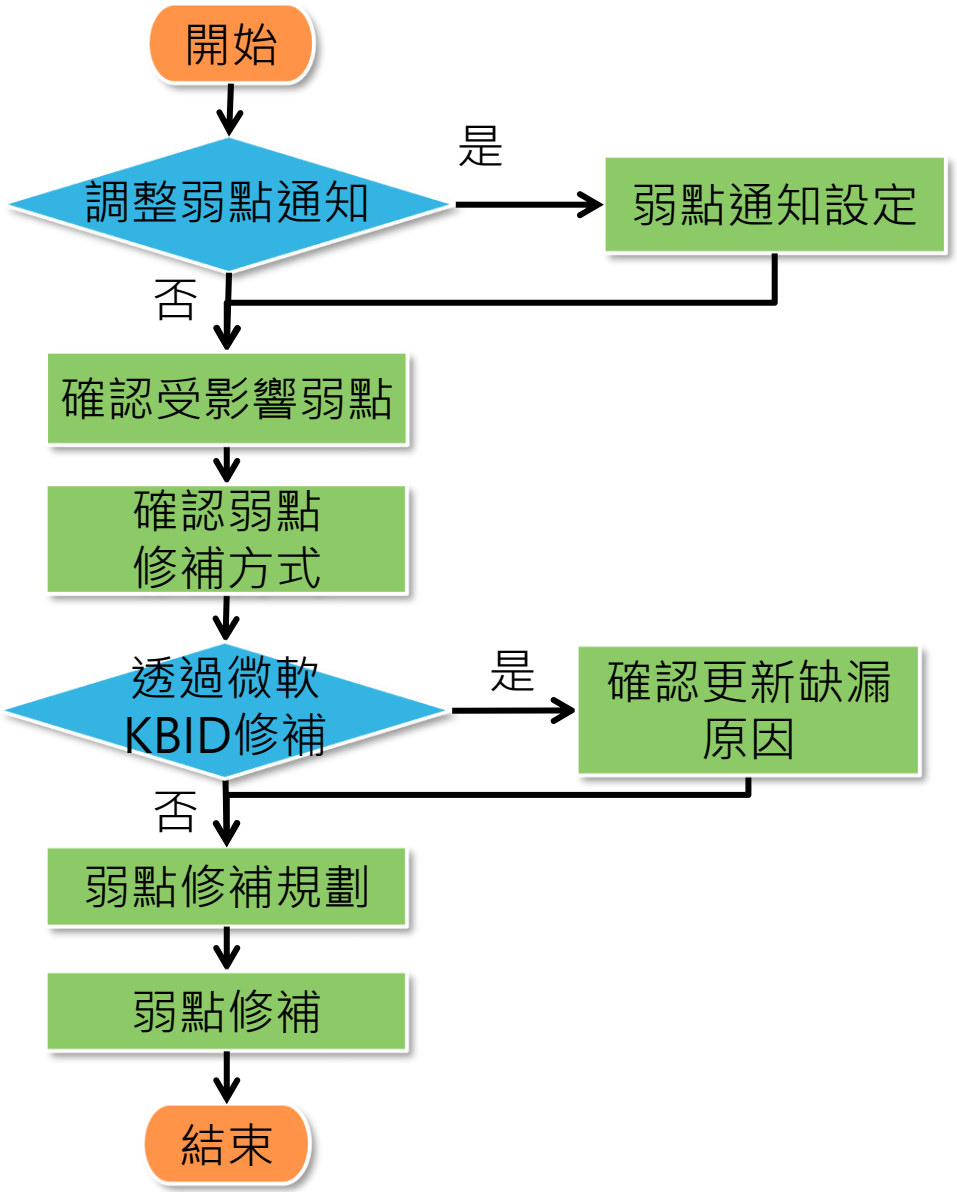
```
    "orgName": "[redacted]政府",
    "identifier": "ntpc[redacted]",
    "assetGroupCode": "[redacted]",
    "assetName": "Chrome 遠端桌面",
    "brand": "Google\Chrome",
    "version": "1.0",
    "cpe": "N/A",
    "cpeName": "N/A"
}
```

導入作業流程

國家資通安全研究院
National Institute of Cyber Security

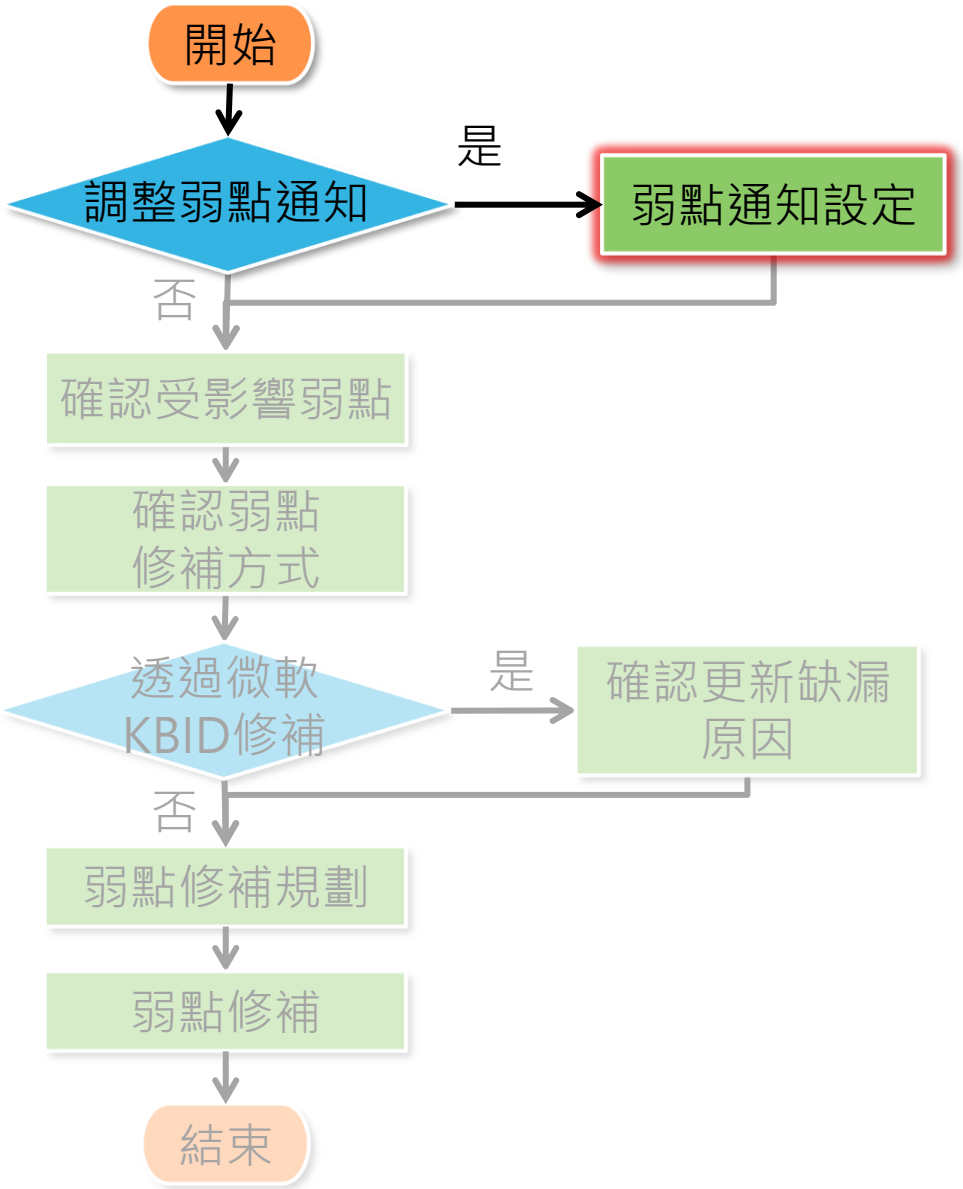


弱點通知與修補規劃作業流程



弱點通知與修補規劃作業流程

國家資通安全研究院
National Institute of Cyber Security



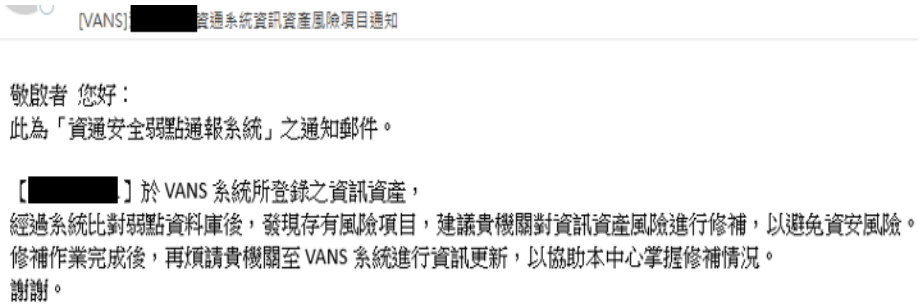
弱點通知設定(1/2)

- 首次登入VANS系統時，系統自動設定弱點通知如以下資訊，無須人工設定
- 可至「CVSS通知設定」功能檢視與調整設定：
  - 請選擇是否接收弱點通知：ON
  - 請輸入欲接收弱點通知：7
  - 請輸入欲接收弱點通知的電子郵件：登入者的電子郵件

弱點通知設定(2/2)

國家資通安全研究院
National Institute of Cyber Security

- 資訊資產與NVD弱點資料庫自動比對後，若有開啟弱點通知功能，VANS系統將於比對出高於CVSS分數門檻之弱點時寄送通知信
  - 寄送通知信予接收通知Email
  - 於VANS系統上顯示弱點比對通知


[VANS][redacted]資通系統資訊資產風險項目通知

敬啟者 您好：
此為「資通安全弱點通報系統」之通知郵件。

【[redacted]】於 VANS 系統所登錄之資訊資產，
經過系統比對弱點資料庫後，發現存有風險項目，建議貴機關對資訊資產風險進行修補，以避免資安風險。
修補作業完成後，再煩請貴機關至 VANS 系統進行資訊更新，以協助本中心掌握修補情況。
謝謝。

實作練習1

實作練習1(環境說明)

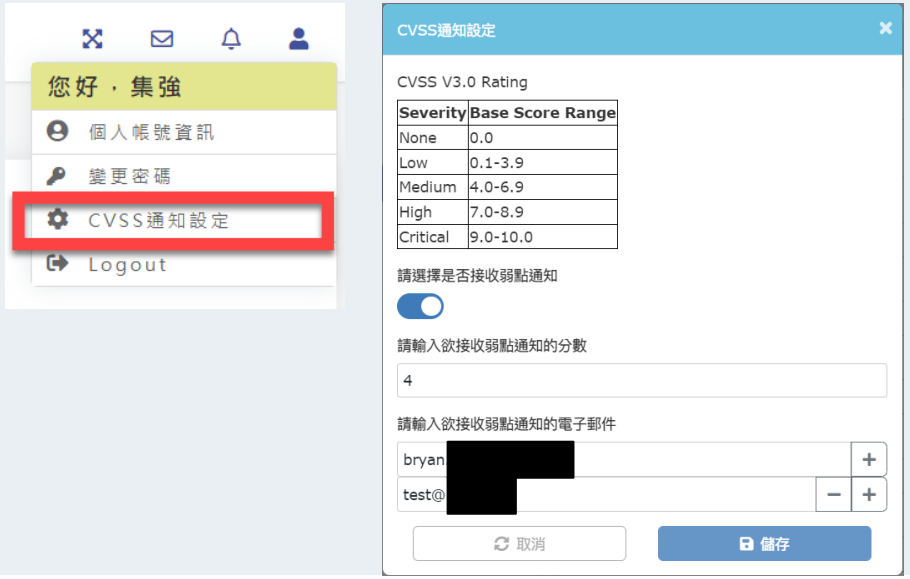
國家資通安全研究院
National Institute of Cyber Security

- VANS系統_實作站
  - **登入資訊**
    - **網址**：已儲存於瀏覽器「書籤列」
    - **帳號**：student01~45
    - **密碼**：1111
  - **機關資訊**
    - **機關OID**：student01~45
    - **機關名稱**：student01~45

實作練習1(1/2)

國家資通安全研究院
National Institute of Cyber Security

- 請以「實作練習1」提供之SERVER_Upload_Template與SERVER_Upload_KBID_Template執行登錄作業
- 本項練習時間10分鐘

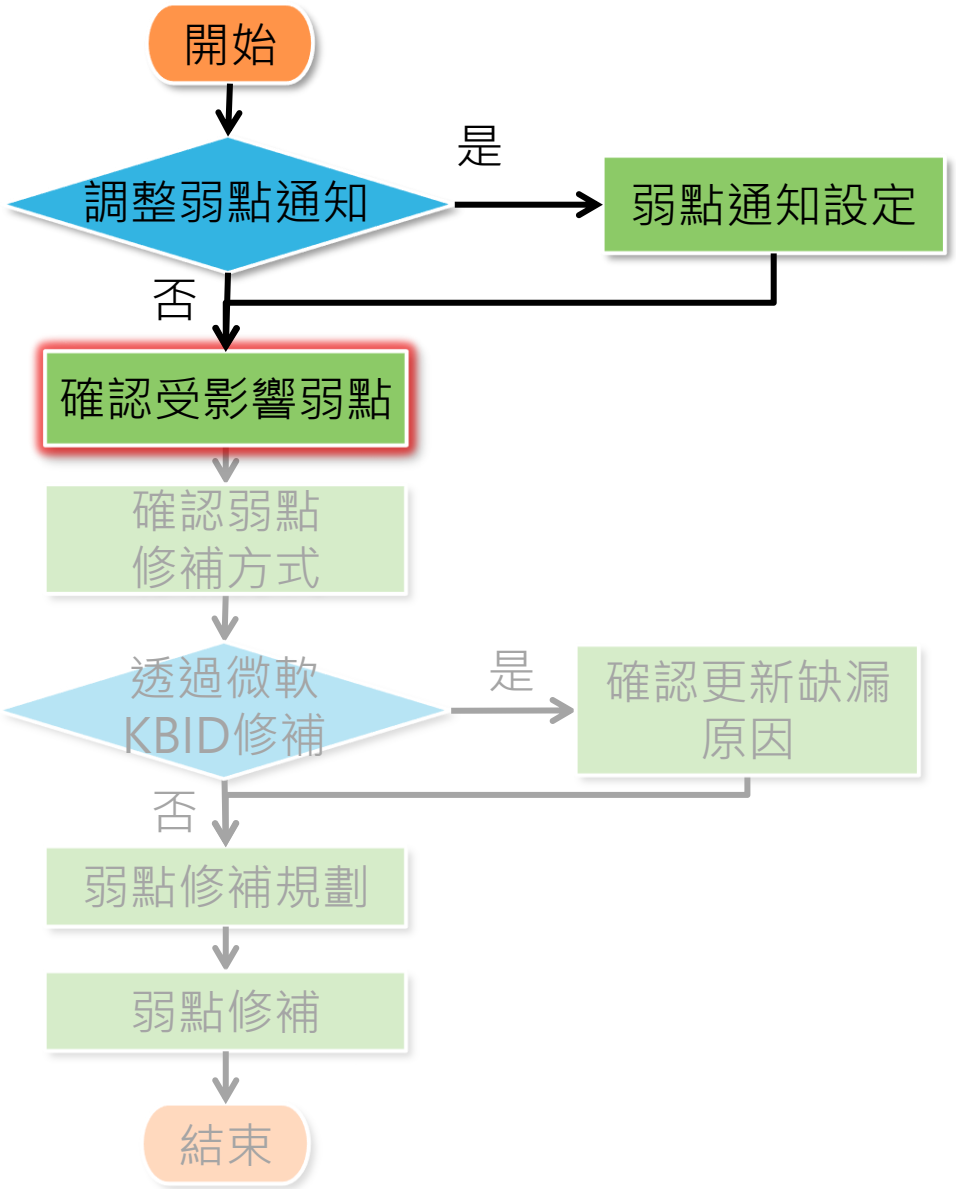
項次	執行項目	產出項目/執行結果
1	進行通知設定 • 是否接收弱點通知：ON • 接收分數設定：4.0 • 接收電子郵件：輸入欲接收的電子郵件	檢視設定接收通知之信箱 

實作練習1(2/2)

國家資通安全研究院
National Institute of Cyber Security

項次	執行項目	產出項目/執行結果
2	開啟Upload_Template (路徑：學員資料夾\01.實作練習\實作練習1\SERVER_Upload_Template.xlsx) • 填寫機關OID與機關名稱 • 完成Upload_Template	SERVER_Upload_Template.xlsx
3	開啟KBID上傳清單 (路徑：學員資料夾\01.實作練習\實作練習1\SERVER_Upload_KBID_Template.xlsx) • 填寫機關OID與機關名稱 • 完成KBID上傳清單	SERVER_Upload_KBID_Template.xlsx
4	上傳SERVER_Upload_Template至VANS系統	於資產列表檢視登錄結果
5	上傳SERVER_Upload_KBID_Template至VANS系統	於已安裝KBID列表檢視登錄結果

弱點通知與修補規劃作業流程



確認受影響弱點–資訊資產風險列表

國家資通安全研究院
National Institute of Cyber Security

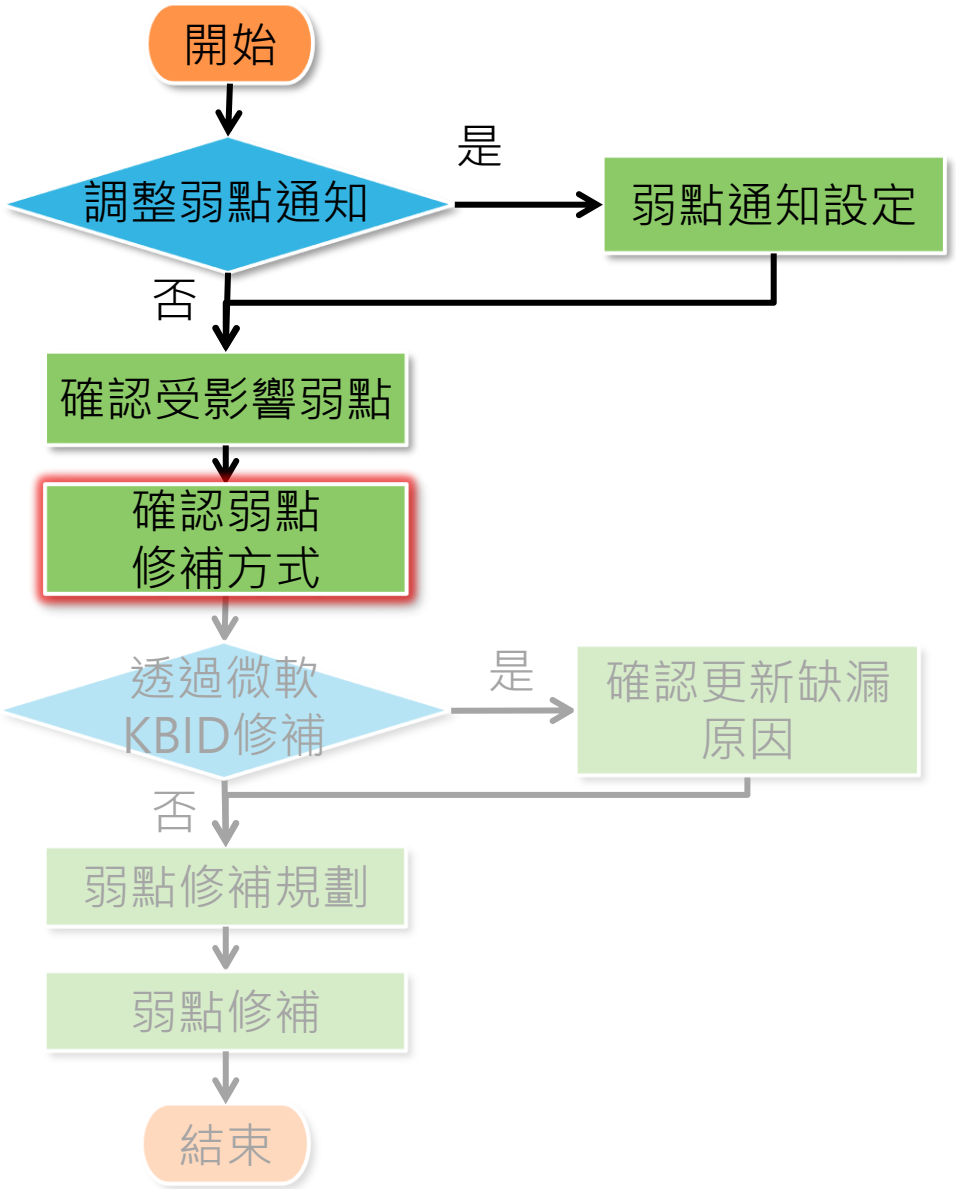
- 於資訊資產風險列表，檢視各資訊資產存在之弱點
  - 資產風險狀態>資通系統風險/使用者電腦風險/工業控制系統風險>資訊資產風險列表

確認受影響弱點–弱點關聯列表

國家資通安全研究院
National Institute of Cyber Security

- 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/使用者電腦風險/工業控制系統風險>弱點關聯列表

弱點通知與修補規劃作業流程



確認弱點修補方式(1/4)

國家資通安全研究院
National Institute of Cyber Security

- 可至NVD官網確認弱點修補方式
- 以資訊資產風險列表為例，點選「詳細資訊」檢視Windows Server 2008 R2 Standard Edition之弱點資訊

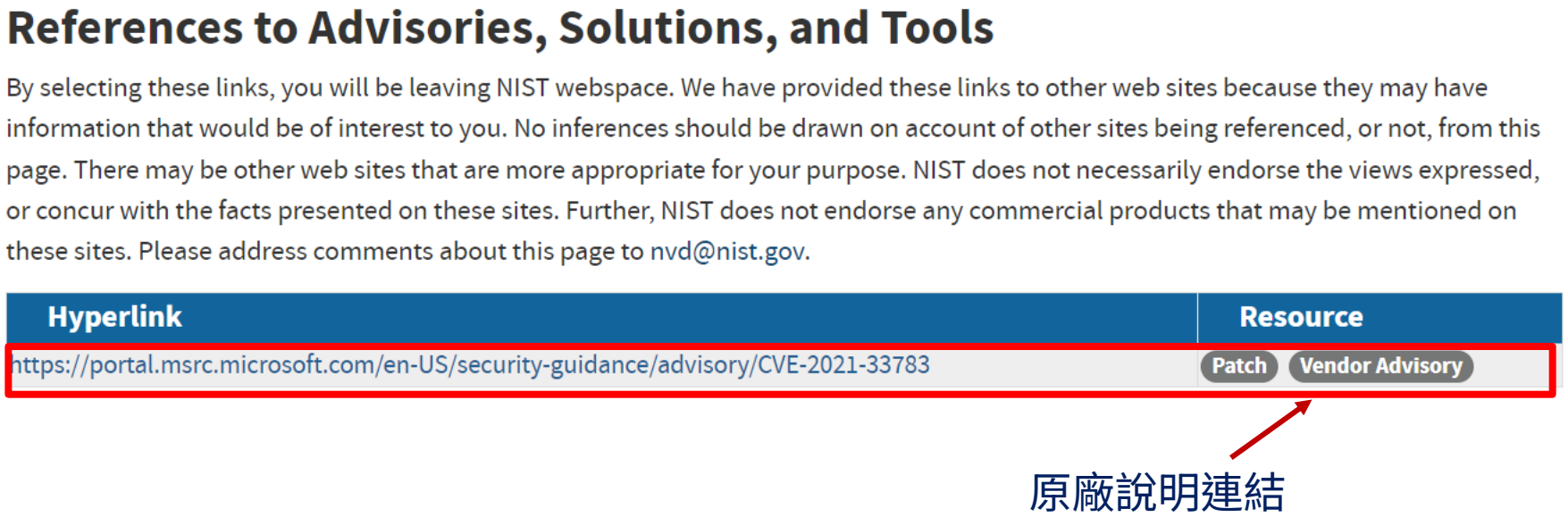
確認弱點修補方式(2/4)

國家資通安全研究院
National Institute of Cyber Security

- 點選弱點編號，可查看弱點描述與相關連結

確認弱點修補方式(3/4)

- 參閱NVD官網建議弱點修補方式



References to Advisories, Solutions, and Tools

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

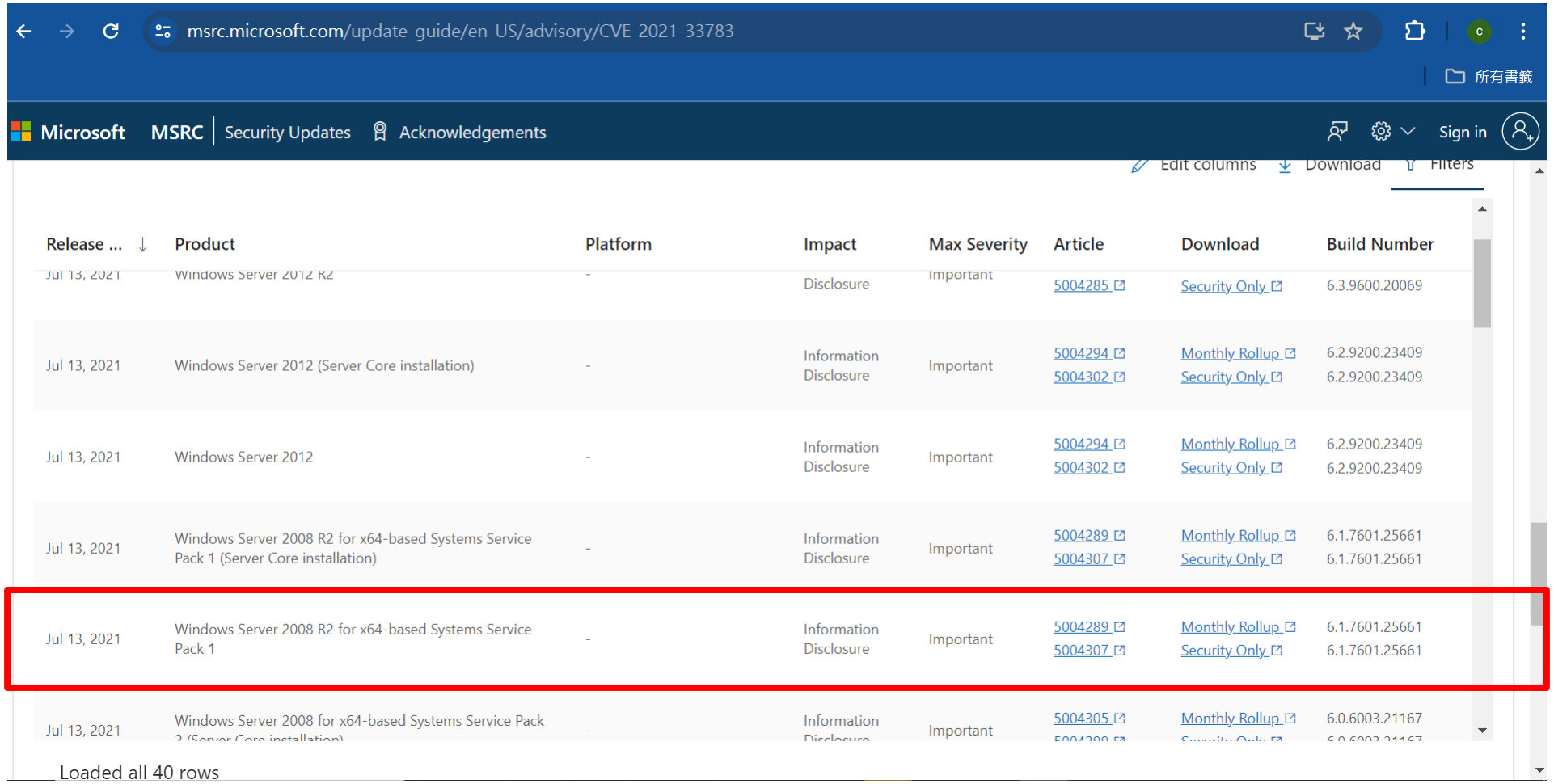
Hyperlink	Resource
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33783	Patch Vendor Advisory

原廠說明連結

確認弱點修補方式(4/4)

國家資通安全研究院
National Institute of Cyber Security

- 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



Release ...	Product	Platform	Impact	Max Severity	Article	Download	Build Number
Jul 13, 2021	Windows Server 2012 R2	-	Disclosure	Important	5004285	Security Only	6.3.9600.20069
Jul 13, 2021	Windows Server 2012 (Server Core installation)	-	Information Disclosure	Important	5004294 5004302	Monthly Rollup Security Only	6.2.9200.23409 6.2.9200.23409
Jul 13, 2021	Windows Server 2012	-	Information Disclosure	Important	5004294 5004302	Monthly Rollup Security Only	6.2.9200.23409 6.2.9200.23409
Jul 13, 2021	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	-	Information Disclosure	Important	5004289 5004307	Monthly Rollup Security Only	6.1.7601.25661 6.1.7601.25661
Jul 13, 2021	Windows Server 2008 R2 for x64-based Systems Service Pack 1	-	Information Disclosure	Important	5004289 5004307	Monthly Rollup Security Only	6.1.7601.25661 6.1.7601.25661
Jul 13, 2021	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	-	Information Disclosure	Important	5004305	Monthly Rollup	6.0.6003.21167

Loaded all 40 rows

確認弱點修補方式-微軟類

國家資通安全研究院
National Institute of Cyber Security

- 微軟類之CVE，可透過詳細資訊中的「可修補KBID」與「已安裝KBID」欄位進行檢視
  - 可從「已安裝KBID」欄位檢視此資訊資產已安裝的KBID
  - 點選「可修補KBID」欄位內的檢視按鈕，查詢可修補此弱點的KBID清單及KBID的受影響產品清單

發佈時間	更新時間	資產編號	資產建立時間	資產更新時間	可修補KBID	已安裝KBID	弱點狀態	動作
2022-08-09 20:15:10	2023-05-31 19:15:14	7602f215e57ff39e787f058576ac8444	2024-04-15 17:37:04	2024-04-19 18:30:42		KB5016679	已安裝KBID修補	檢視
2022-08-09 20:15:10	2023-05-31 19:15:14	7602f215e57ff39e787f058576ac8444	2024-04-15 17:37:04	2024-04-19 18:30:42		KB5016679	已安裝KBID修補	檢視
2022-08-09 20:15:10	2023-05-31 19:15:14	7602f215e57ff39e787f058576ac8444	2024-04-15 17:37:04	2024-04-19 18:30:42		KB5016679	已安裝KBID修補	檢視

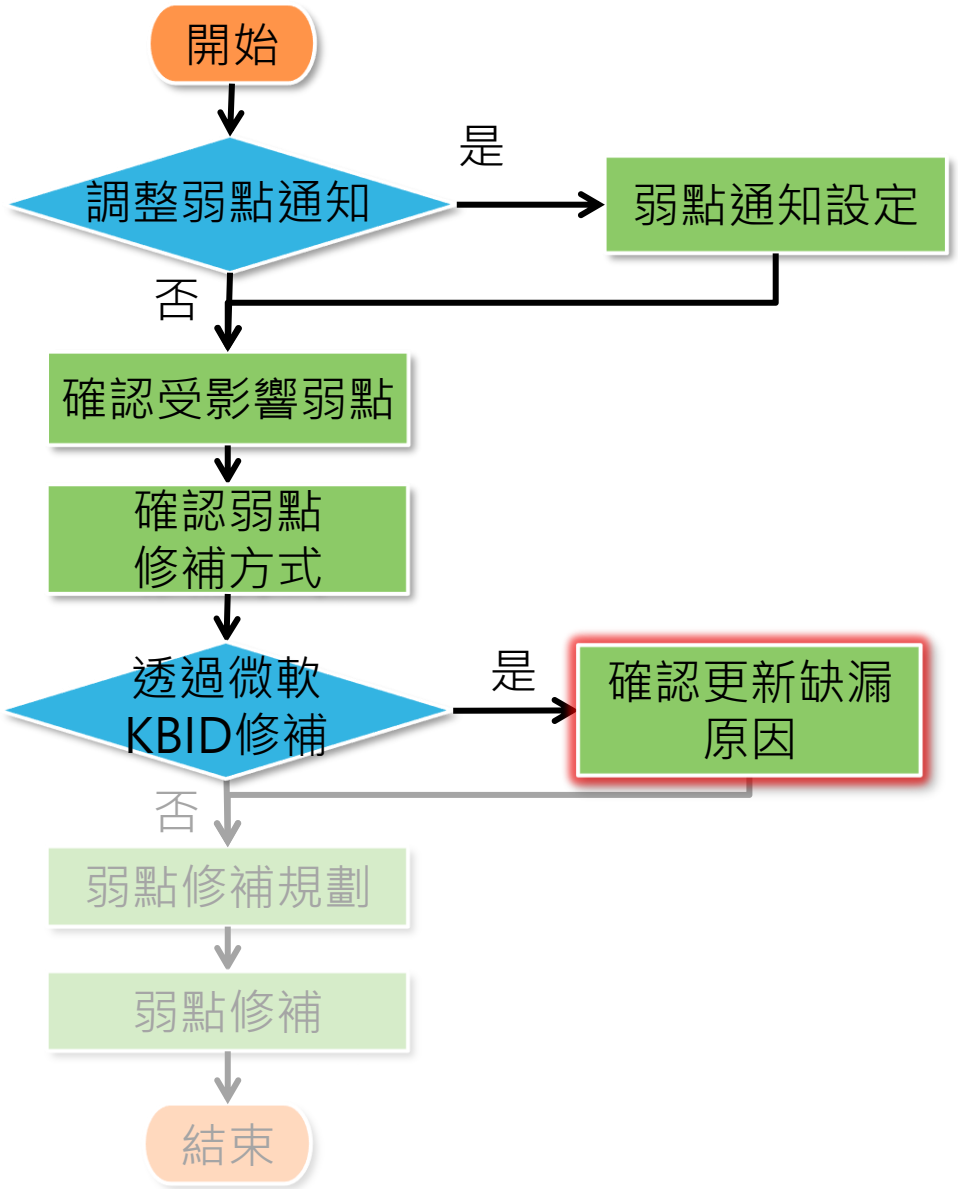
可修補KBID清單

共2筆紀錄 10 1/1

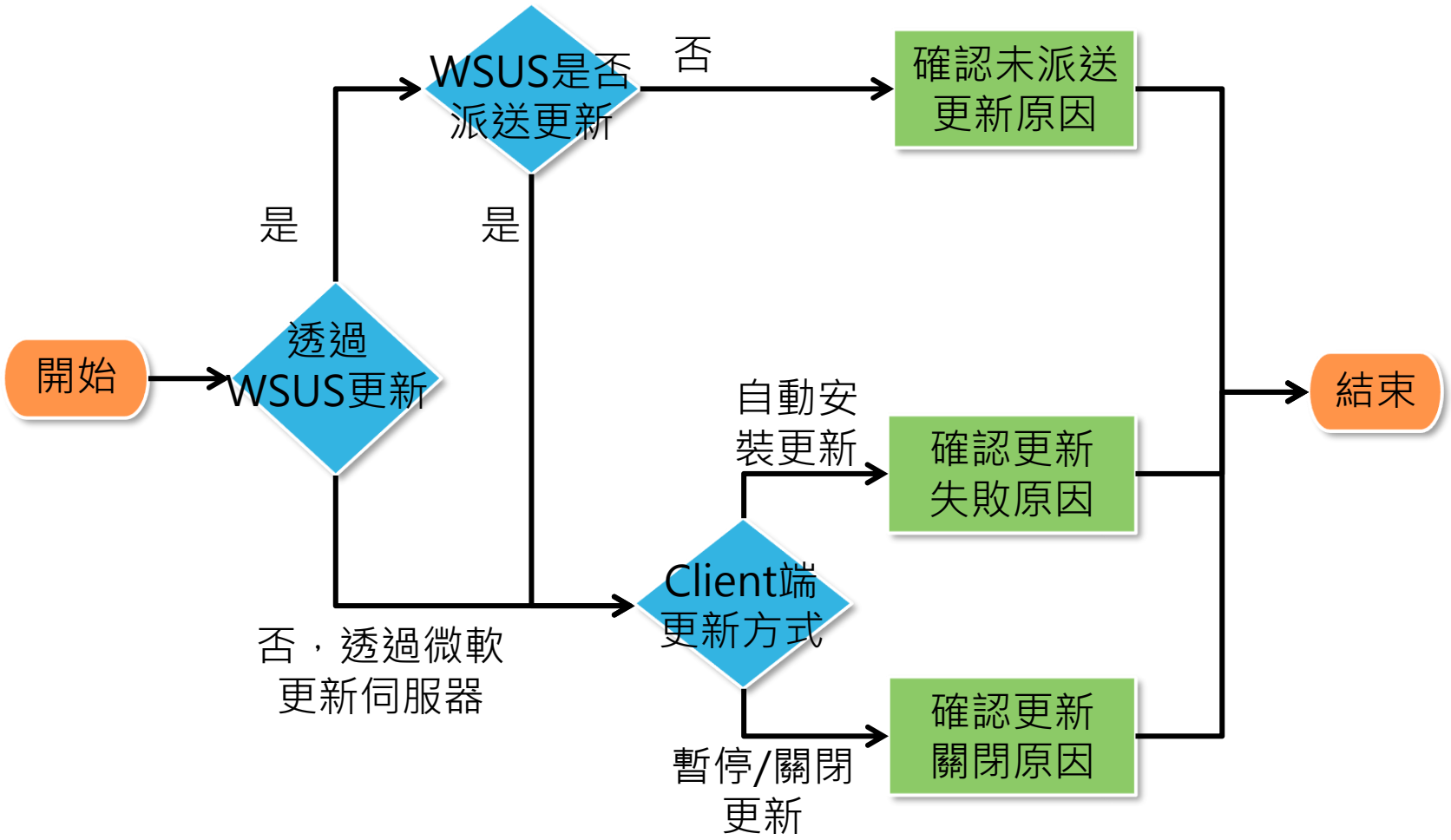
KBID	產品名稱
5016679	Windows Server 2008 R2 for x64-based Systems Service Windows Server 2008 R2 for x64-based Systems Service
5016676	Windows Server 2008 R2 for x64-based Systems Service Windows Server 2008 R2 for x64-based Systems Service

弱點通知與修補規劃作業流程

國家資通安全研究院
National Institute of Cyber Security

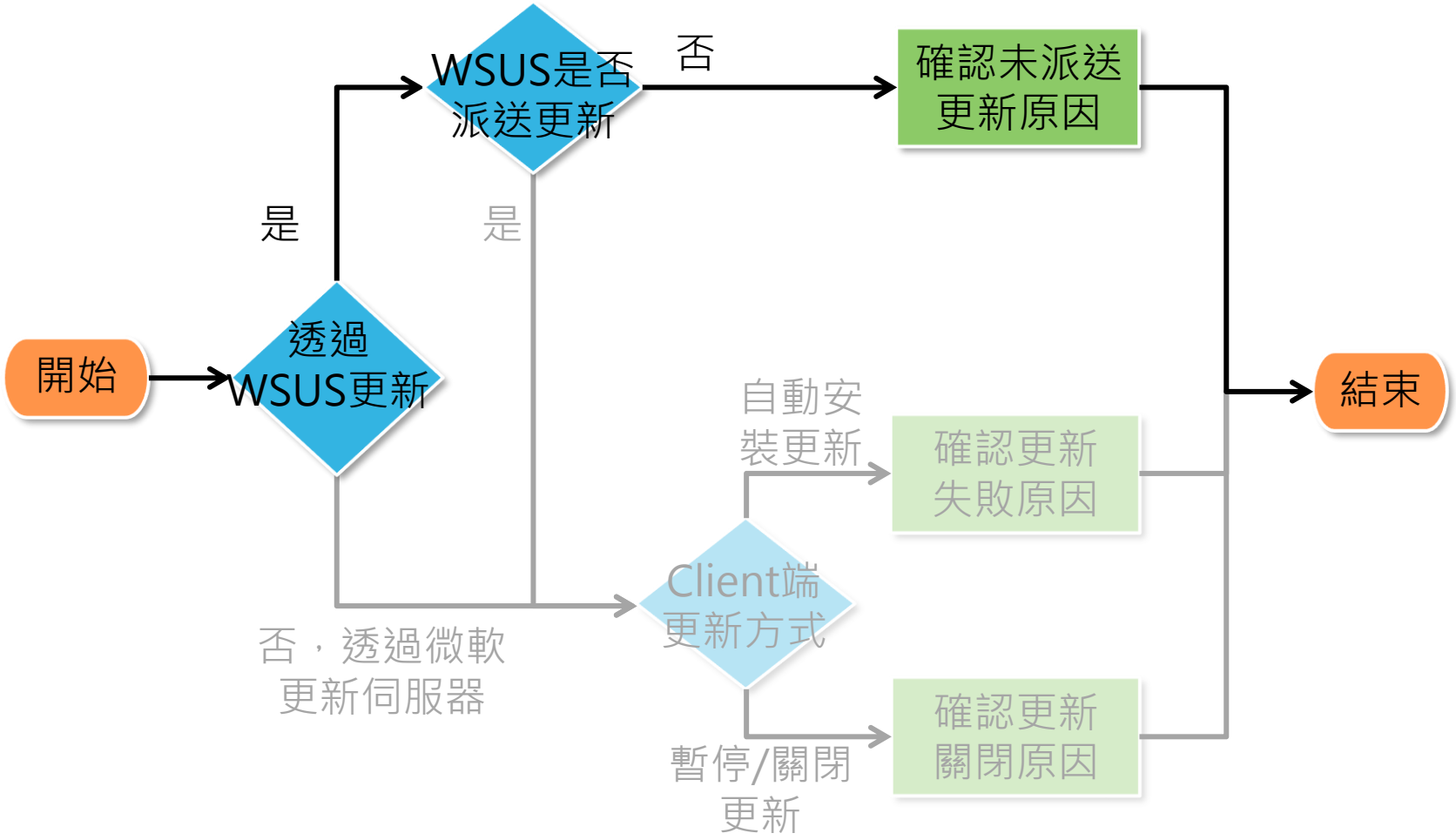


確認更新缺漏原因


開始
透過WSUS更新
是
WSUS是否派送更新
否
確認未派送更新原因
是
否，透過微軟更新伺服器
Client端更新方式
自動安裝更新
確認更新失敗原因
暫停/關閉更新
確認更新關閉原因
結束

確認更新缺漏原因

國家資通安全研究院
National Institute of Cyber Security

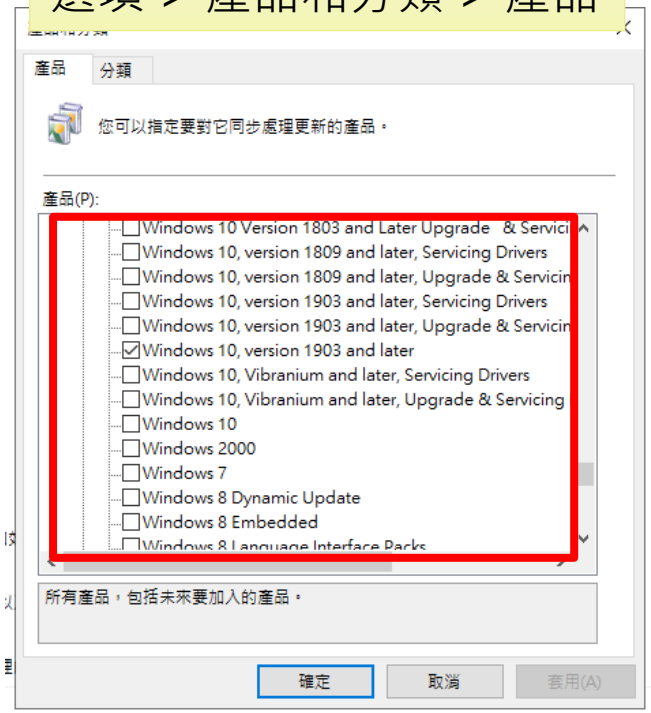


確認WSUS更新派送狀態(1/2)

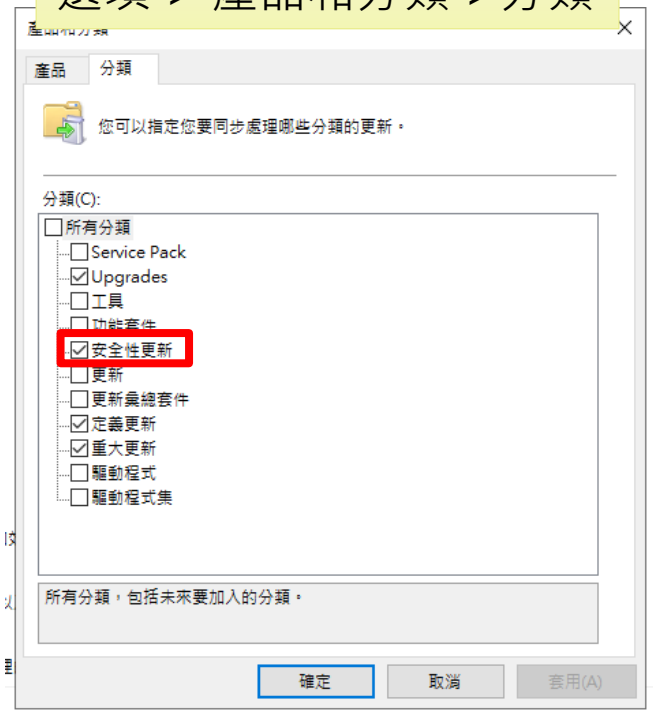
國家資通安全研究院
National Institute of Cyber Security

- 若透過WSUS派送更新，需至WSUS伺服器確認下列設定
  - 可搭配資訊資產清單或資產管理系統，確認機關內所有微軟系列品項，確保完整勾選所需之產品
  - 確認有勾選「安全性更新」類別

選項 > 產品和分類 > 產品



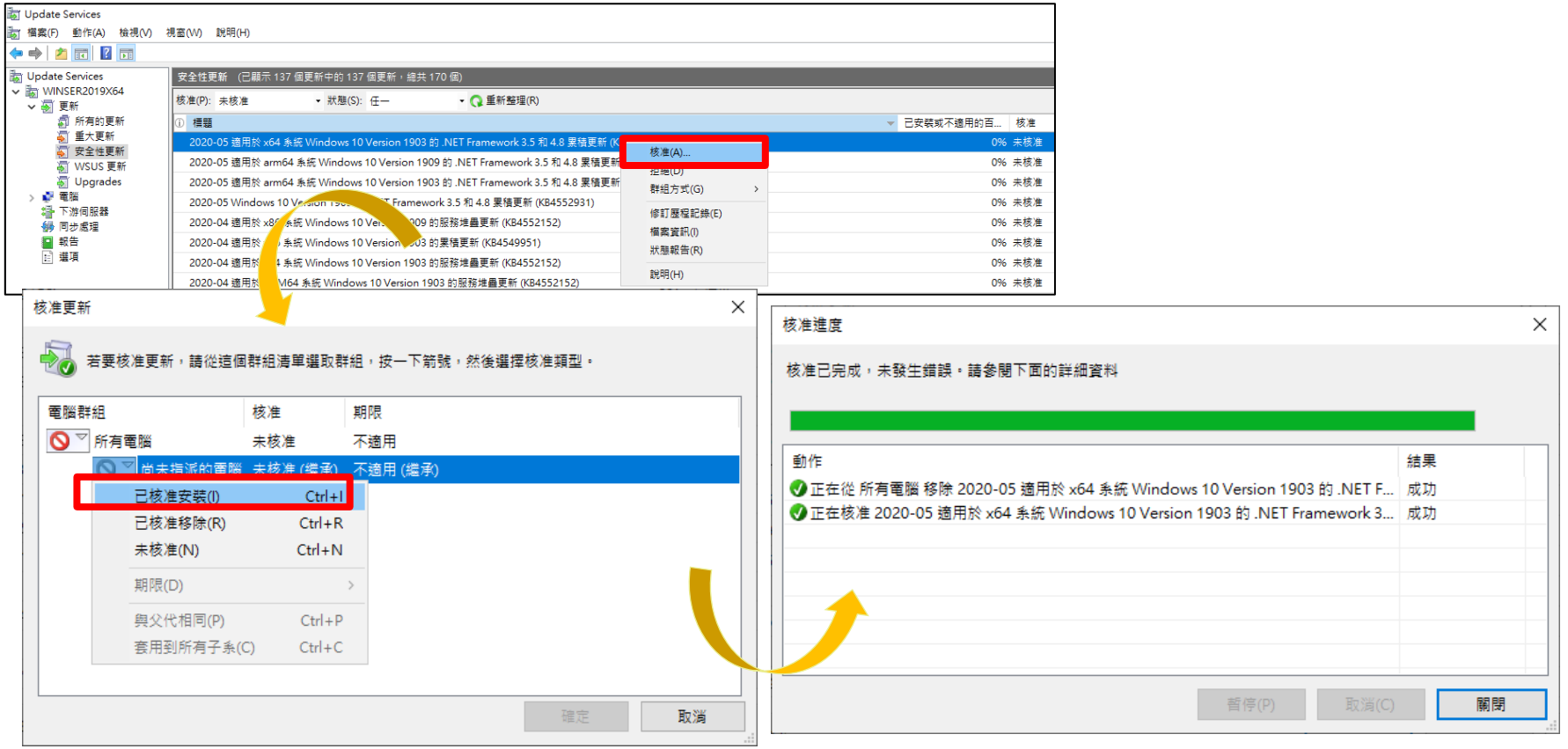
選項 > 產品和分類 >分類



確認WSUS更新派送狀態(2/2)

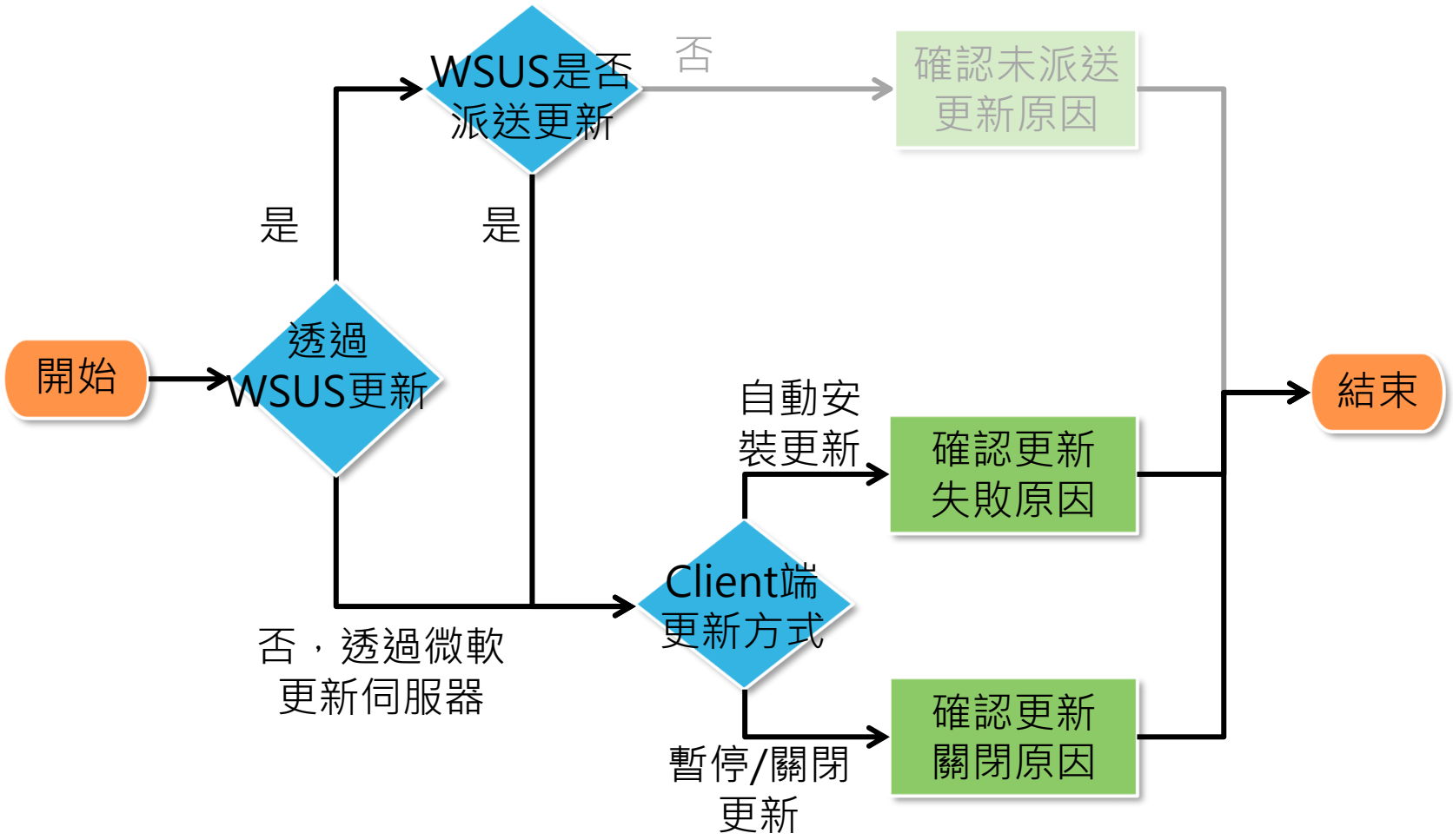
國家資通安全研究院
National Institute of Cyber Security

- 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

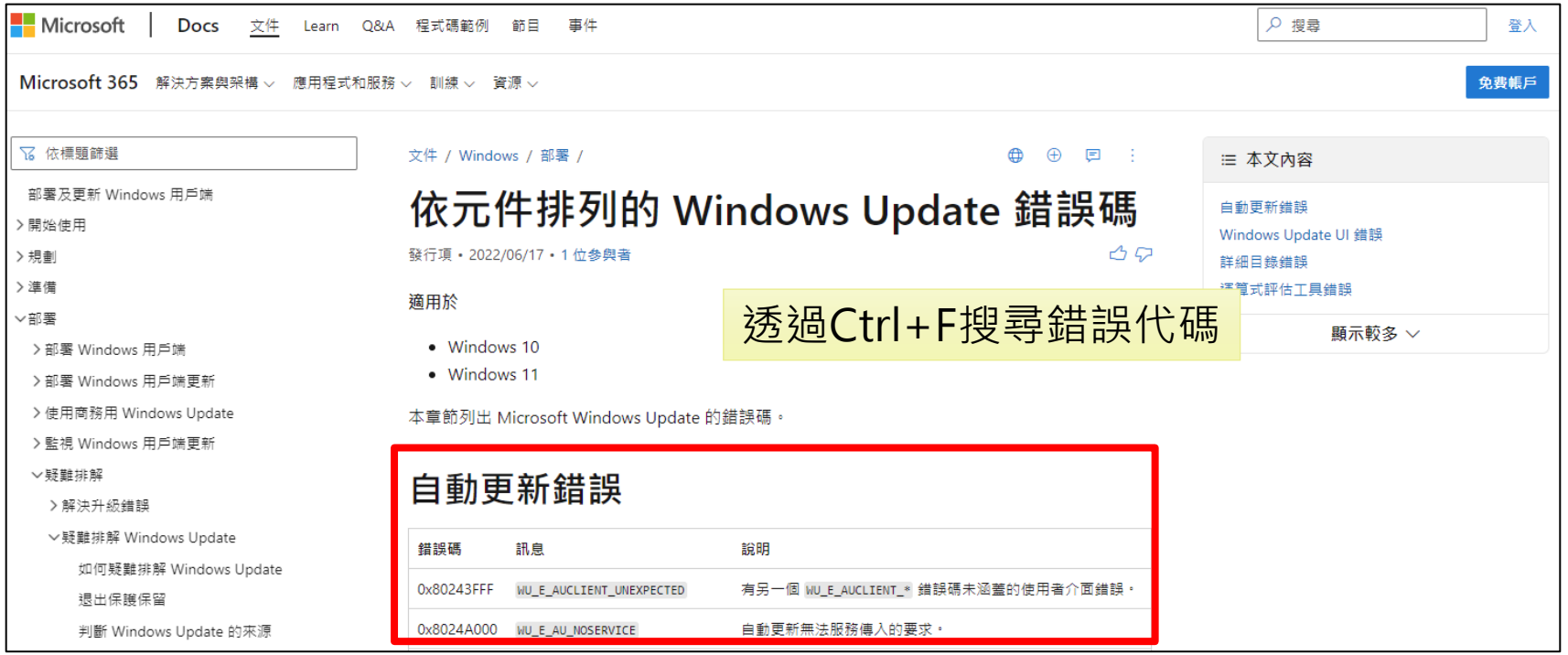
確認更新缺漏原因


開始
透過WSUS更新
是
WSUS是否派送更新
否
確認未派送更新原因
是
否，透過微軟更新伺服器
Client端更新方式
自動安裝更新
確認更新失敗原因
暫停/關閉更新
確認更新關閉原因
結束

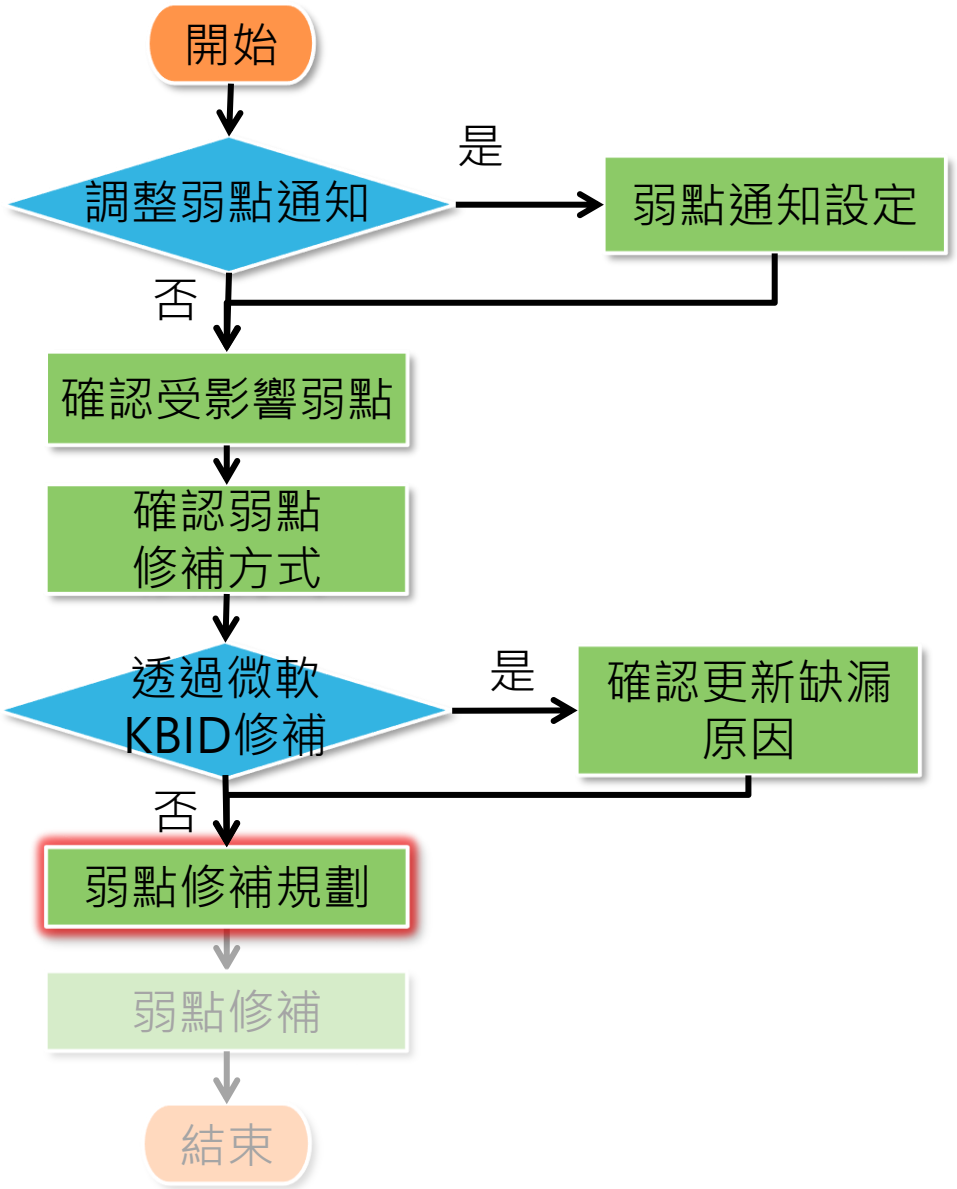
確認Client端更新狀態

國家資通安全研究院
National Institute of Cyber Security

- 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涵義，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



弱點通知與修補規劃作業流程



弱點修補規劃(1/7)

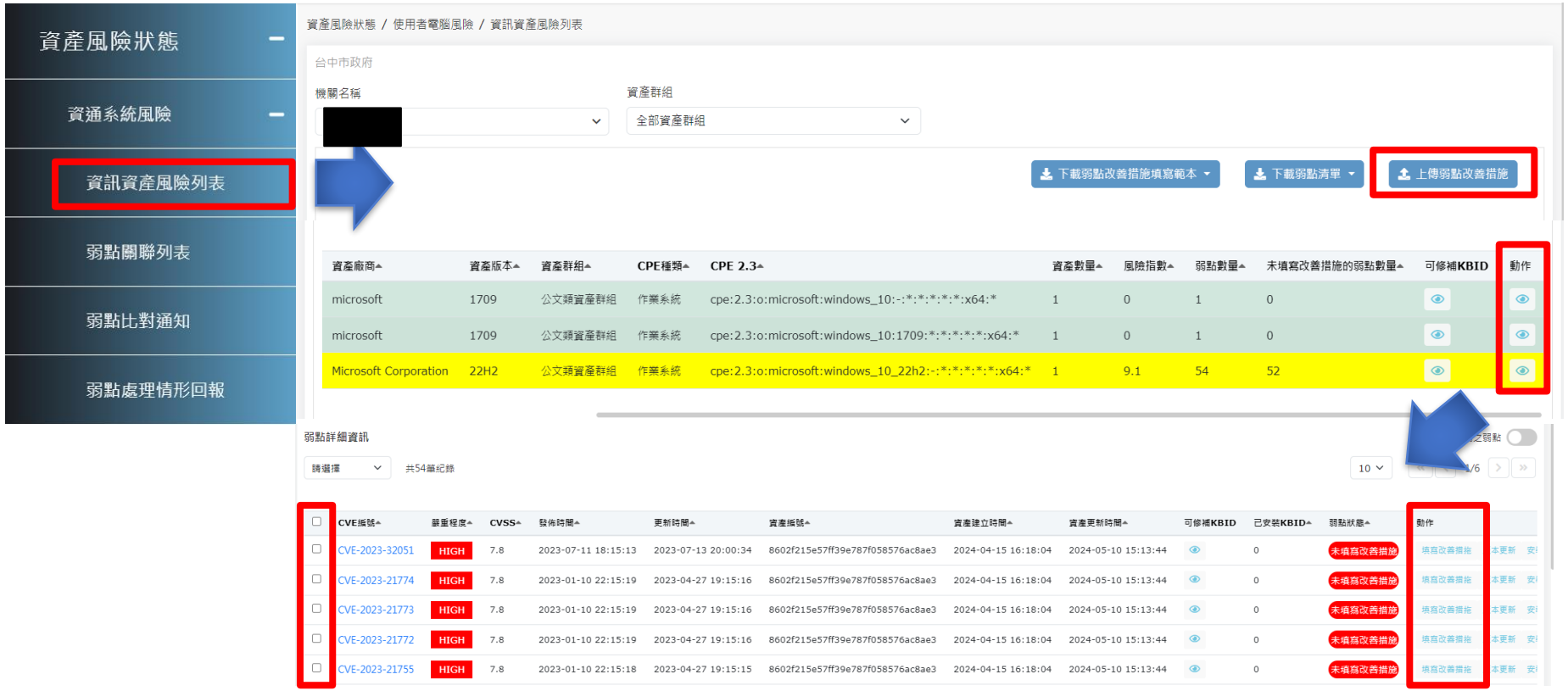
國家資通安全研究院
National Institute of Cyber Security

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

弱點修補規劃(2/7)

國家資通安全研究院
National Institute of Cyber Security

- 改善措施填寫方式分為單筆填寫、批次填寫及上傳更新
- 可依據弱點修補規劃，選擇適合的改善措施範本，填寫改善措施
  - 資產風險狀態>資通系統風險/使用者電腦風險/工業控制系統風險>資訊資產風險列表



弱點修補規劃(3/7)

國家資通安全研究院
National Institute of Cyber Security

- 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「選取範本」，填寫改善措施
  - STEP3：點選「儲存」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

弱點修補規劃(4/7)

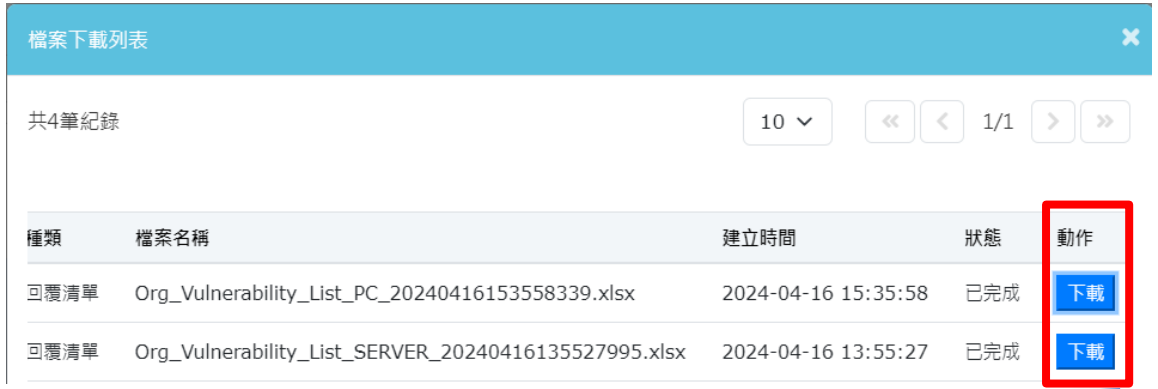
國家資通安全研究院
National Institute of Cyber Security

- 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，勾選左方的方格並點選填寫勾選改善措施，以進行多筆CVE之弱點修補規劃
  - STEP2：點選「選取範本」，填寫改善措施
  - STEP3：點選「儲存」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)

弱點修補規劃(5/7)

國家資通安全研究院
National Institute of Cyber Security

- 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
  - STEP1：點擊「下載弱點清單」，系統開始進行產製弱點清單
  - STEP2：可至檔案下載區查看弱點清單
    - 點擊「下載」按鈕，匯出弱點比對結果。若改善措施為「未填寫改善措施」則表示尚未對該弱點進行修補規劃
    - 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

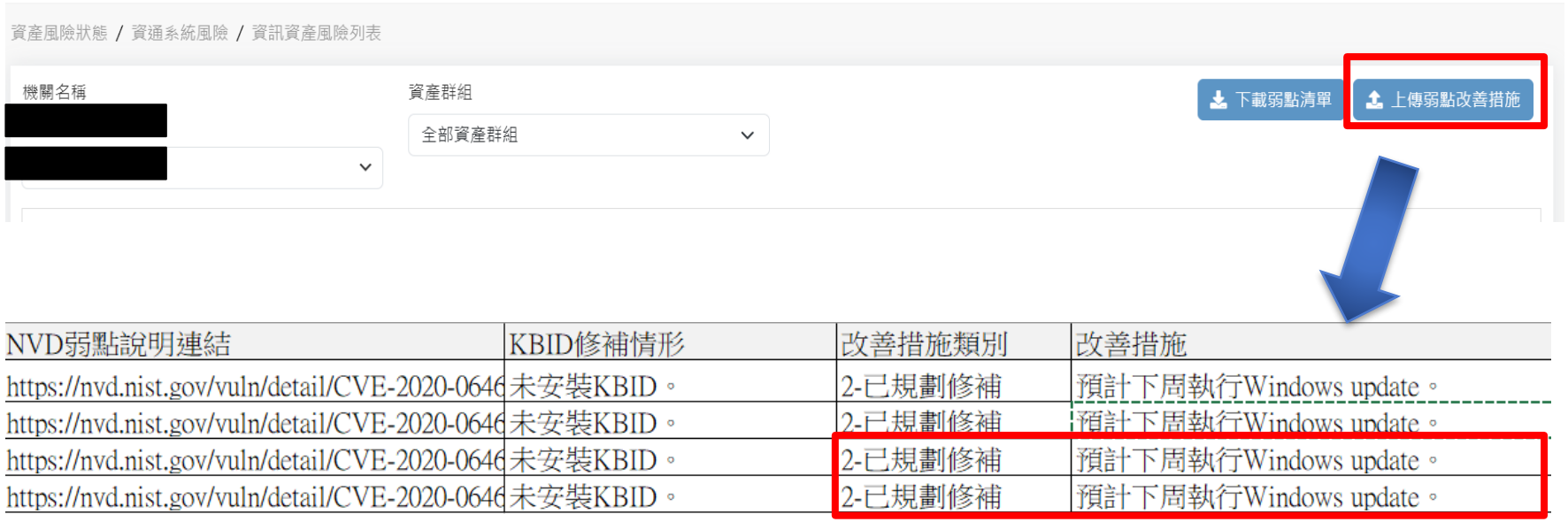


CVSS	發布時間	更新時間	弱點說明	NVD弱點說明連結	KBID修補情形	改善措施類別	改善措施
7.80	2023-01-10 22:15:18	2023-04-27 19:15:15	Windows Kernel Elevation of Privilege Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-202	未安裝KBID	未填寫改善措施	未填寫改善措施
7.50	2023-01-10 22:15:16	2023-04-27 19:15:13	Windows Internet Key Exchange (IKE) Extension Denial of S	https://nvd.nist.gov/vuln/detail/CVE-202	未安裝KBID	未填寫改善措施	未填寫改善措施
7.50	2023-01-10 22:15:17	2023-04-27 19:15:13	Windows Netlogon Denial of Service Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-202	未安裝KBID	未填寫改善措施	未填寫改善措施

弱點修補規劃(6/7)

國家資通安全研究院
National Institute of Cyber Security

- 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
  - 點選「上傳弱點改善措施」按鈕，上傳以登錄弱點修補規劃



NVD弱點說明連結	KBID修補情形	改善措施類別	改善措施
https://nvd.nist.gov/vuln/detail/CVE-2020-0646	未安裝KBID。	2-已規劃修補	預計下周執行Windows update。
https://nvd.nist.gov/vuln/detail/CVE-2020-0646	未安裝KBID。	2-已規劃修補	預計下周執行Windows update。
https://nvd.nist.gov/vuln/detail/CVE-2020-0646	未安裝KBID。	2-已規劃修補	預計下周執行Windows update。
https://nvd.nist.gov/vuln/detail/CVE-2020-0646	未安裝KBID。	2-已規劃修補	預計下周執行Windows update。

弱點修補規劃(7/7)

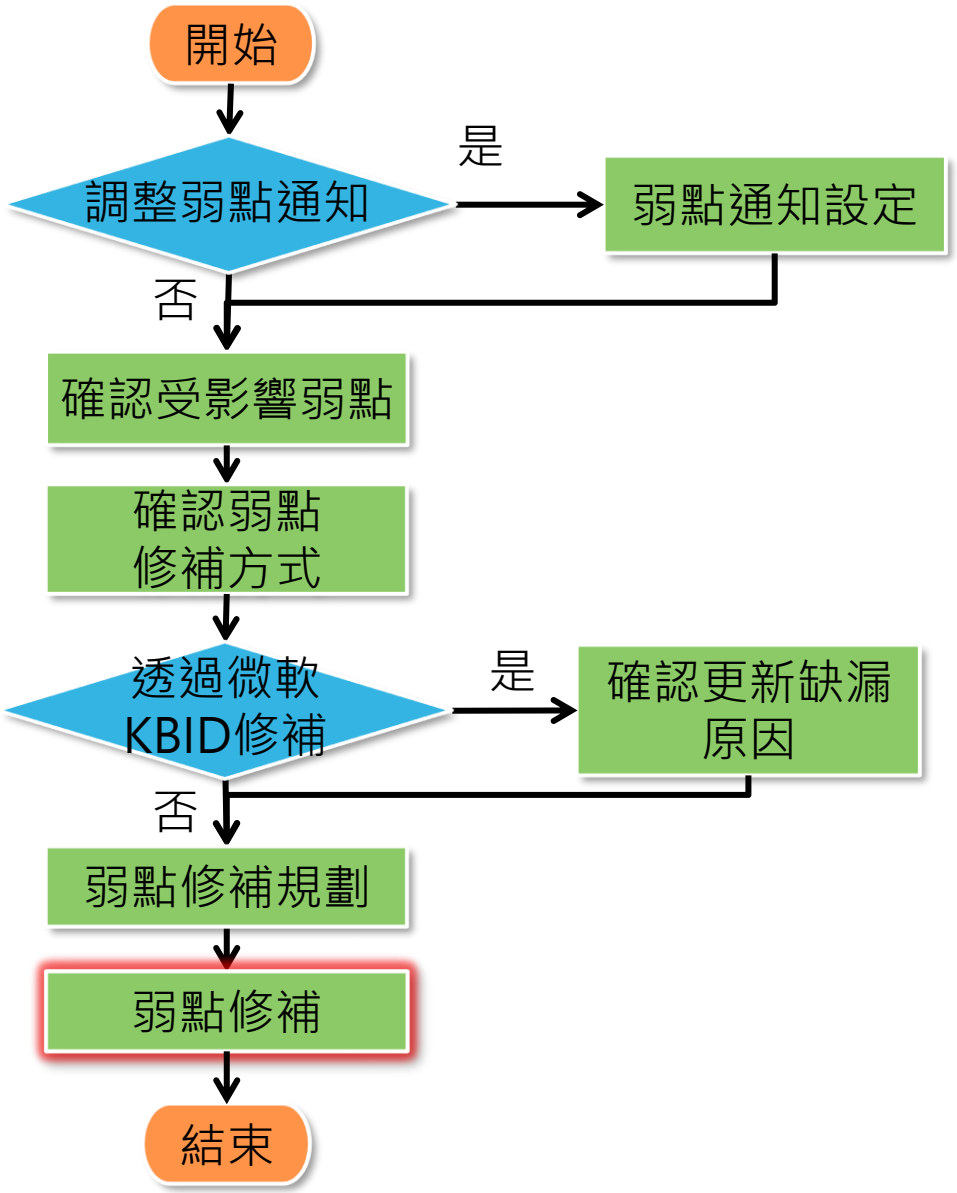
國家資通安全研究院
National Institute of Cyber Security

- 自「未填寫改善措施數量」檢視各軟體資產尚未填寫改善措施之弱點數量
  - 資產風險狀態>資通系統風險/使用者電腦風險/工業控制系統風險>資訊資產風險列表

資產廠商	資產版本	資產群組	CPE種類	CPE 2.3	資產數量	風險指數	弱點數量	未填寫改善措施的弱點數量	可修補KBID	動作
microsoft	1709	公文類資產群組	作業系統	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:x64:*	1	0	1	0		
microsoft	1709	公文類資產群組	作業系統	cpe:2.3:o:microsoft:windows_10:1709:*:*:*:*:*:x64:*	1	0	1	0		
Microsoft Corporation	22H2	公文類資產群組	作業系統	cpe:2.3:o:microsoft:windows_10_22h2:-:*:*:*:*:*:x64:*	1	9.1	54	52		

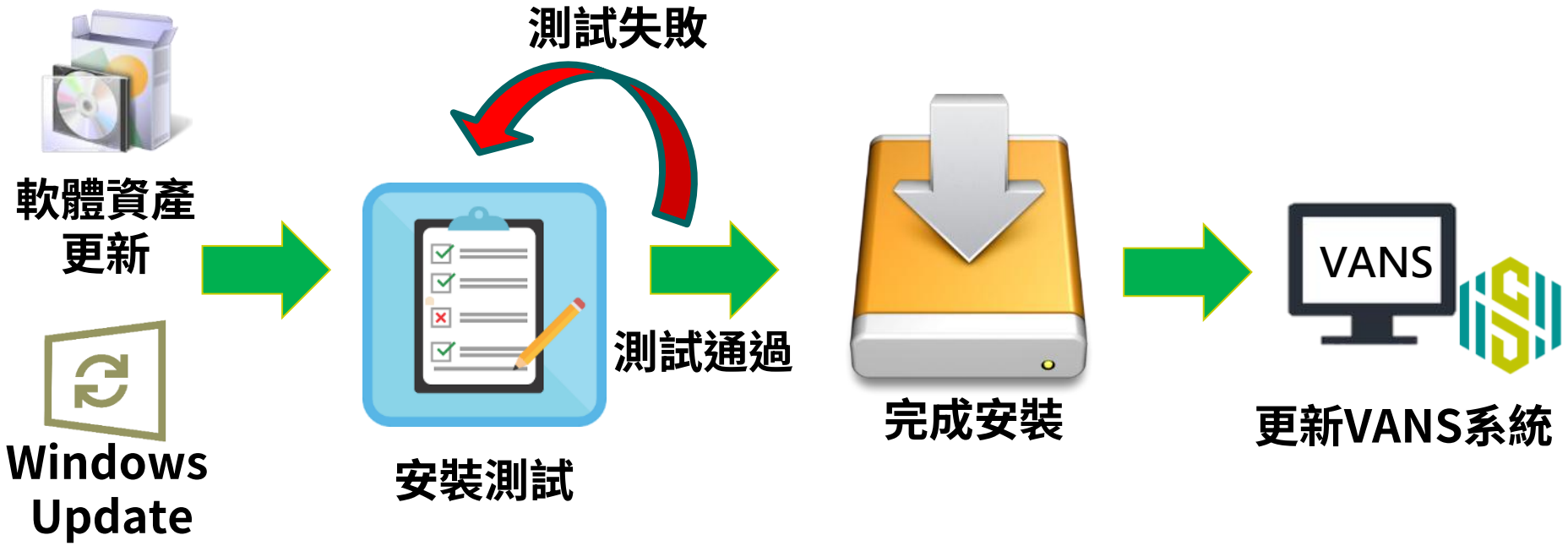
弱點通知與修補規劃作業流程

國家資通安全研究院
National Institute of Cyber Security



弱點修補

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



實作練習2

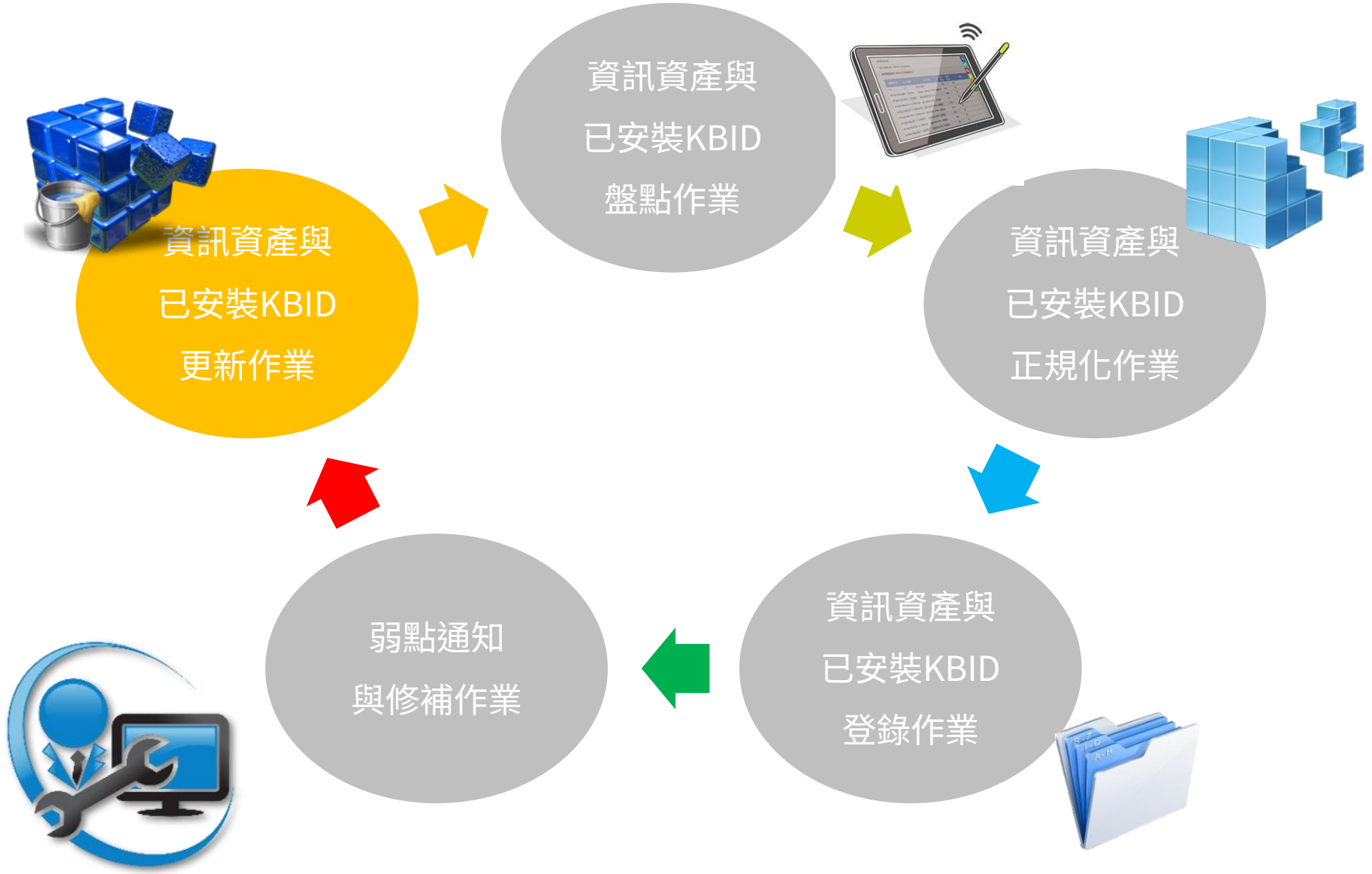
實作練習2

- 檢視弱點通知，並進行弱點修補規劃
- 本項練習時間20分鐘

項次	執行項目	產出項目/執行結果
1	於資訊資產風險列表檢視Apache Tomcat 9.0之弱點，透過查詢建議修補方式填寫改善措施	• 填寫弱點清單中的改善措施 • 改善措施範例： ✓ 選擇「經評估無法修補」的改善措施範本 ✓ 改善措施為「已採行之風險處理措施:已加強防護與異常偵測」
2	於資訊資產風險列表檢視Windows Server 2012 R2之弱點，查詢CVE-2021-34448，透過查詢建議修補方式填寫改善措施	• 填寫弱點清單中的改善措施 • 改善措施範例： ✓ 選擇「已完成修補、修補方式為」的改善措施範本 ✓ 改善措施為「已透過Windows Update修補」

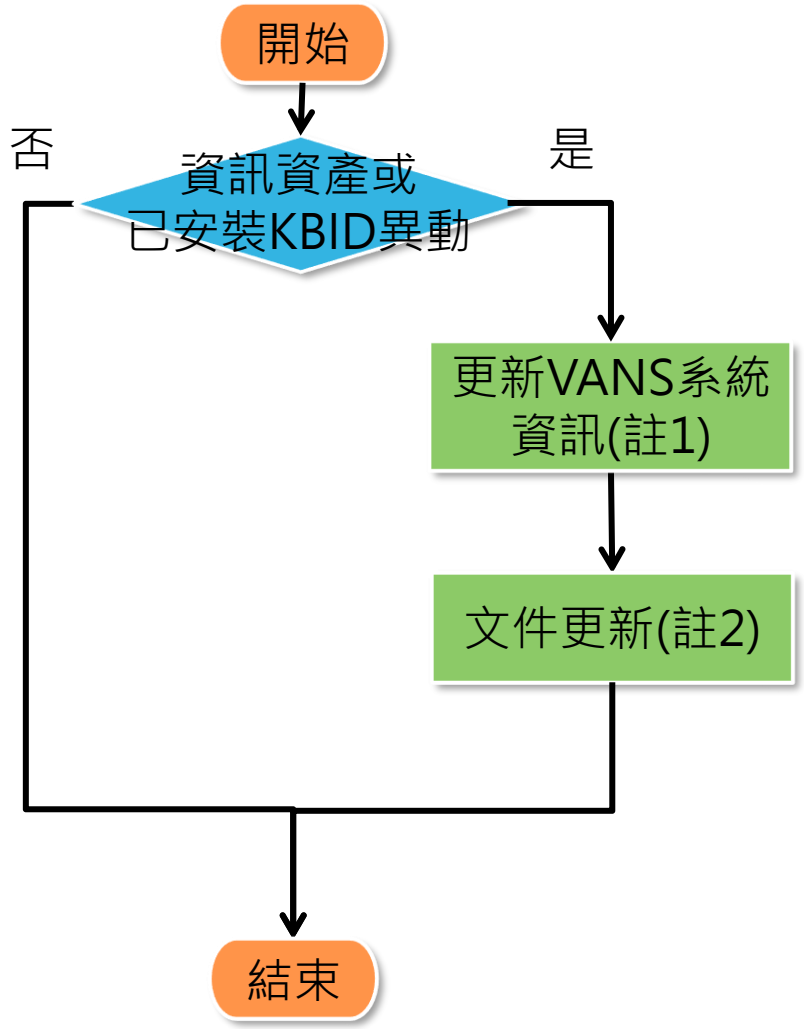
導入作業流程

國家資通安全研究院
National Institute of Cyber Security



資訊資產與已安裝KBID更新作業流程

國家資通安全研究院
National Institute of Cyber Security

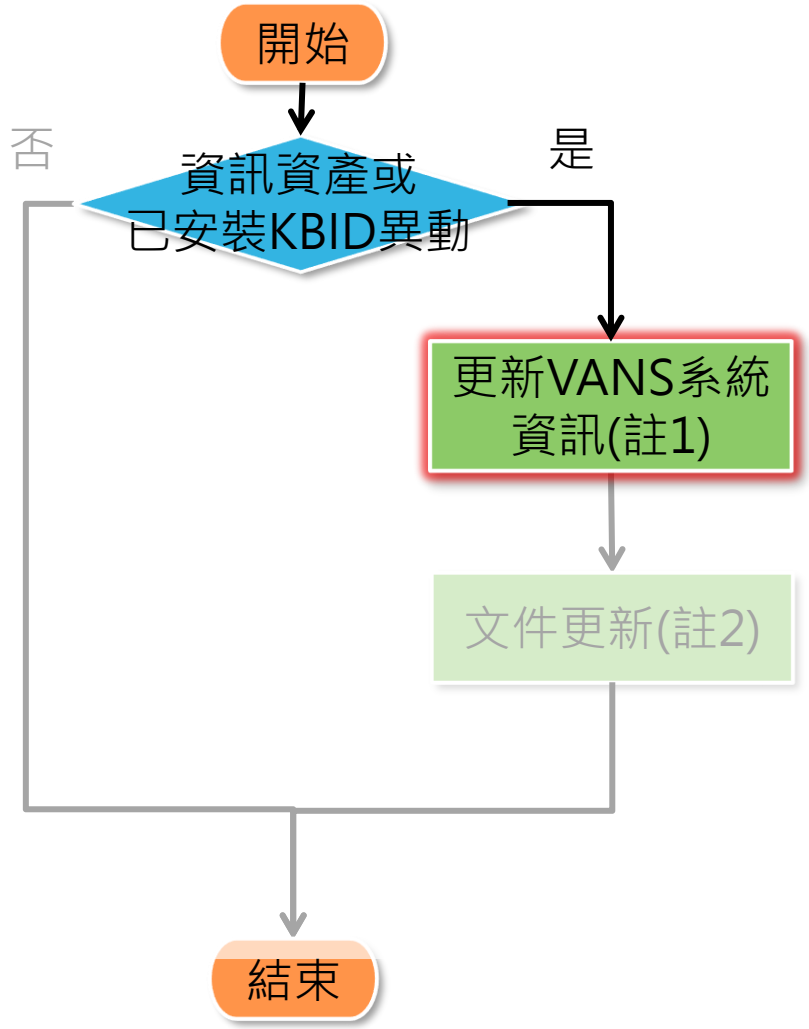


註1：更新VANS系統資訊：
新增、修改及刪除VANS
系統資訊

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

資訊資產與已安裝KBID更新作業流程

國家資通安全研究院
National Institute of Cyber Security



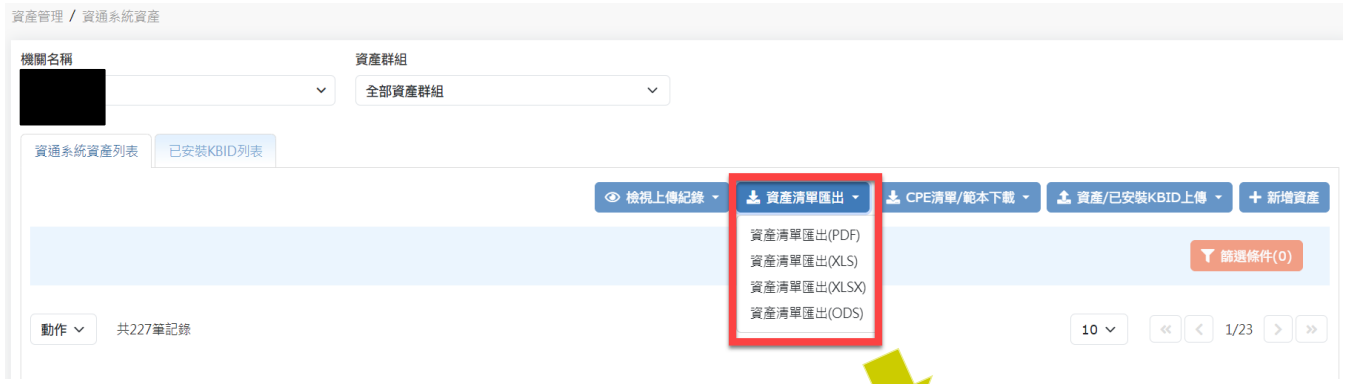
註1：更新VANS系統資訊：
新增、修改及刪除VANS
系統資訊

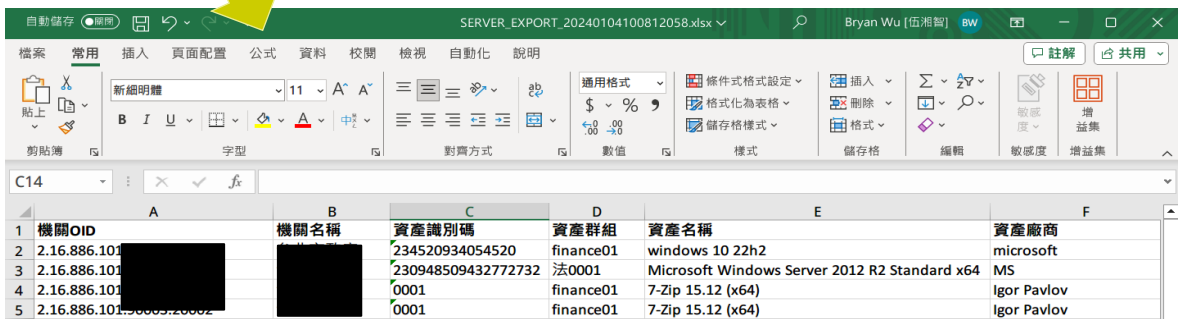
註2：文件更新：
1.更新資訊資產清冊
2.更新已安裝KBID清單
3.重新匯出資訊資產清單
4.重新匯出弱點清單

更新VANS系統資訊-批次更新

國家資通安全研究院
National Institute of Cyber Security

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

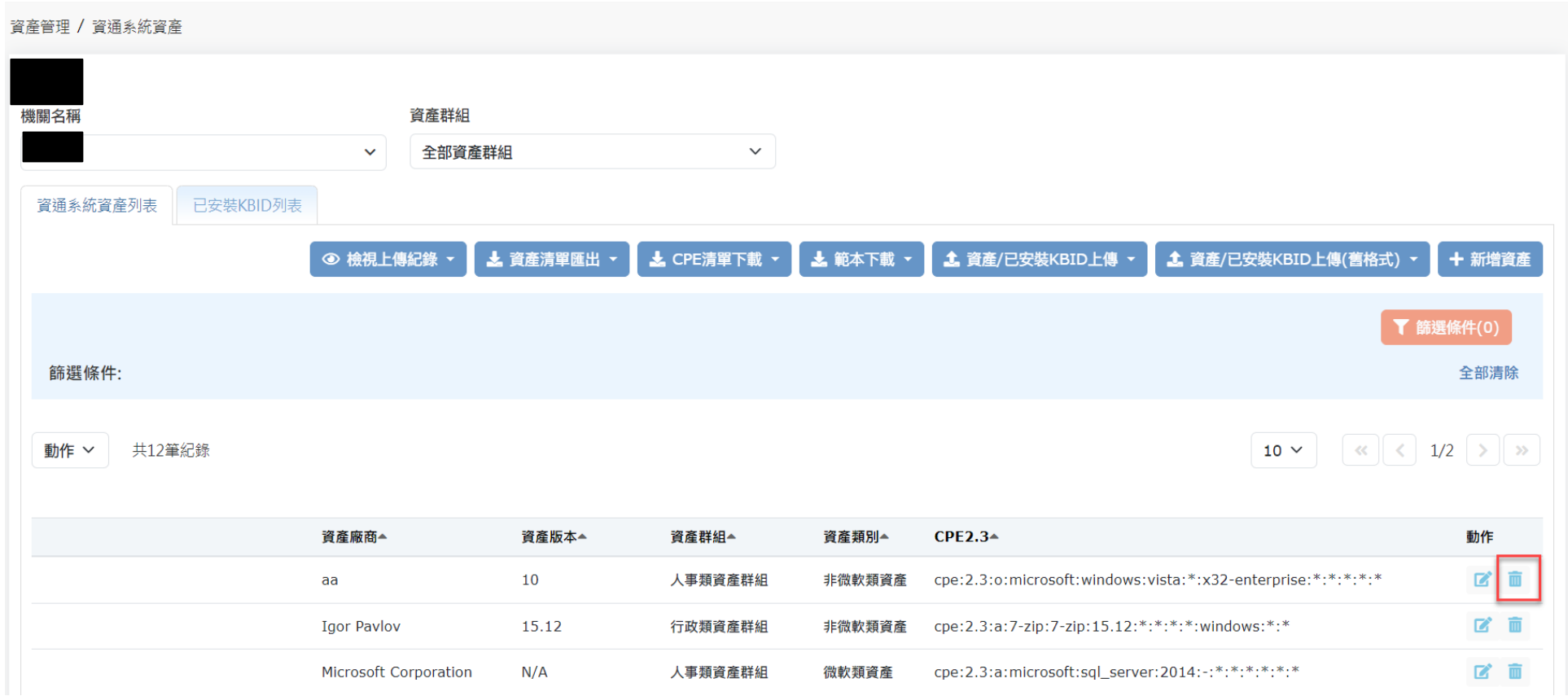




更新VANS系統資訊-單筆更新(1/6)

國家資通安全研究院
National Institute of Cyber Security

- 刪除資產
  - 進入網頁點選「刪除」鈕，進行單筆資產刪除



更新VANS系統資訊-單筆更新(2/6)

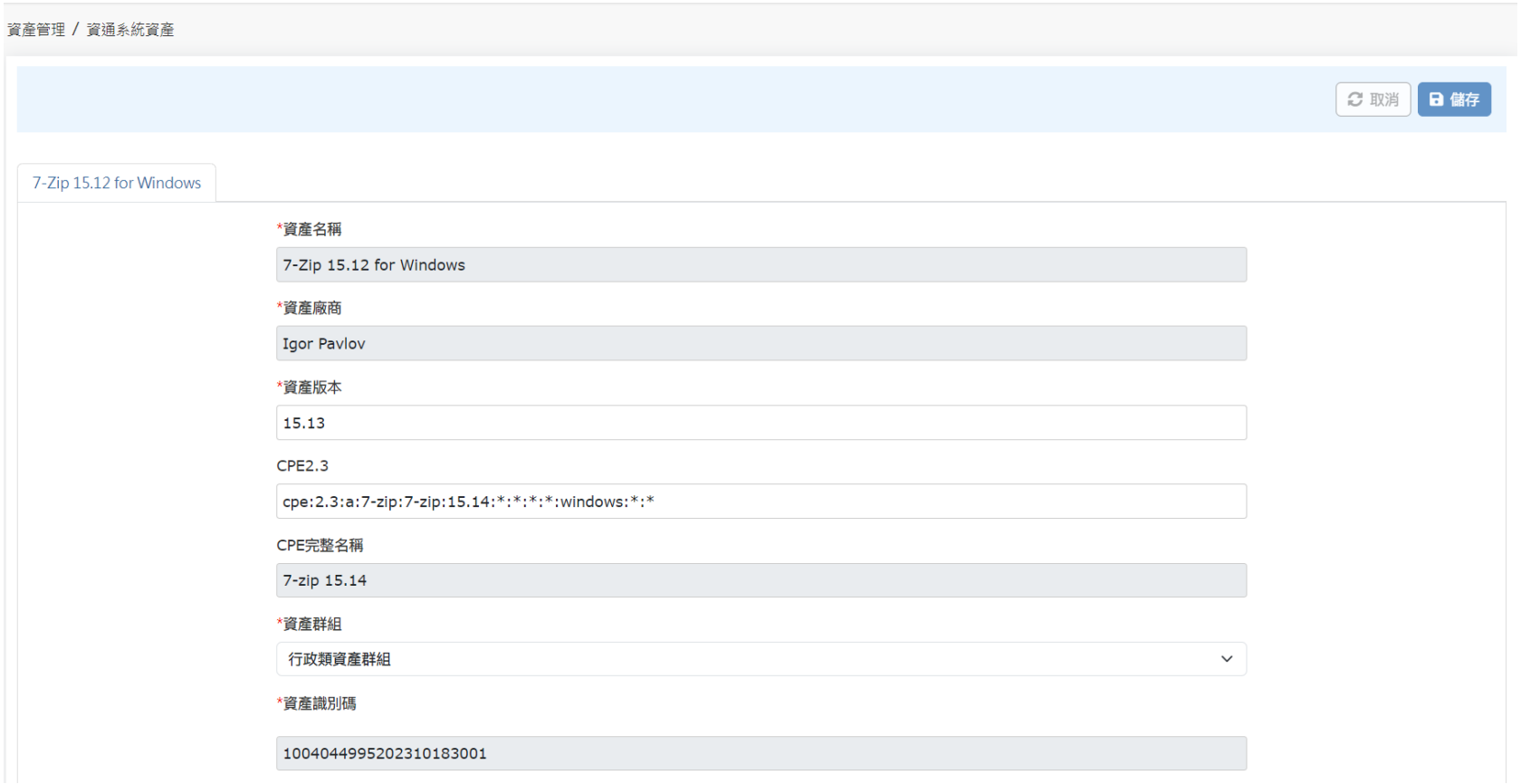
國家資通安全研究院
National Institute of Cyber Security

- 編輯資產
  - Step1 ：進入網頁點選「編輯」鈕

更新VANS系統資訊-單筆更新(3/6)

國家資通安全研究院
National Institute of Cyber Security

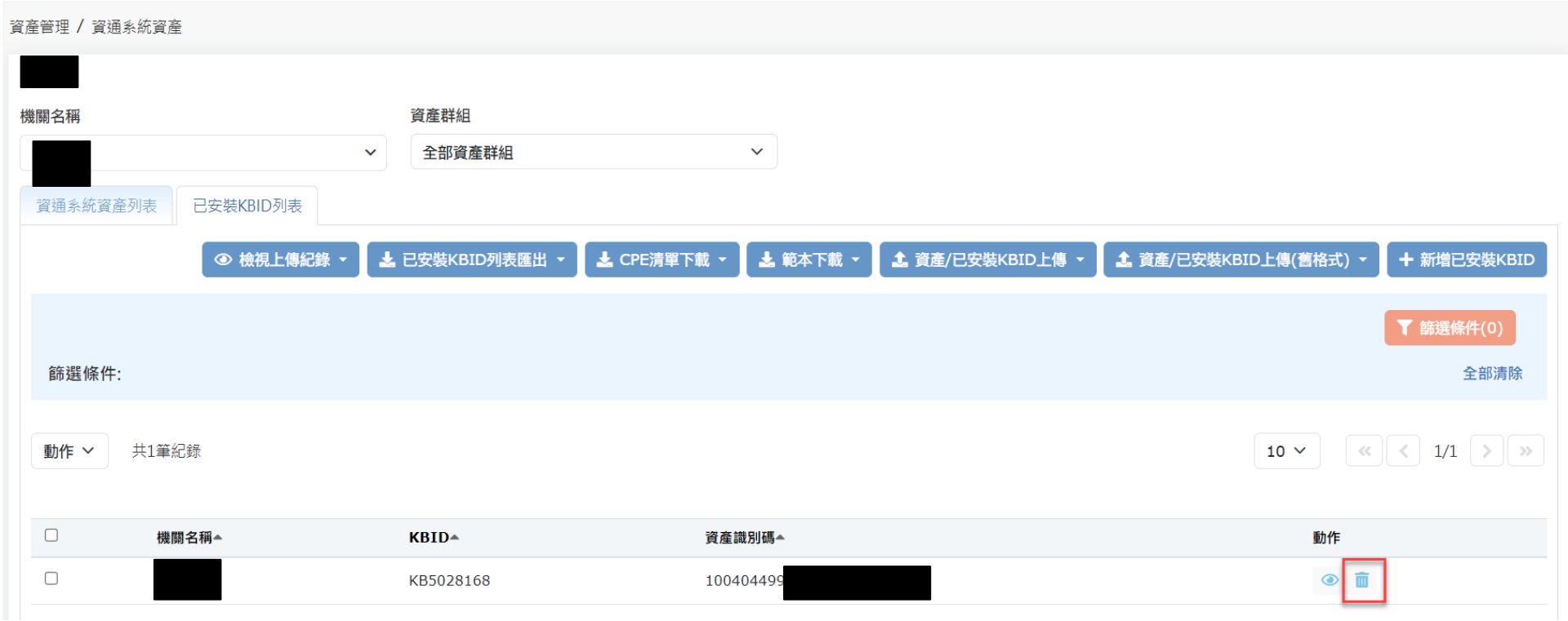
- 編輯資產
  - Step2：對資產的版本、CPE、資產群組欄位進行編輯，完成後按「儲存」鈕



更新VANS系統資訊-單筆更新(4/6)

國家資通安全研究院
National Institute of Cyber Security

- 編輯已安裝KBID
  - Step1：將欲更改的已安裝KBID點選「刪除」鈕



更新VANS系統資訊-單筆更新(5/6)

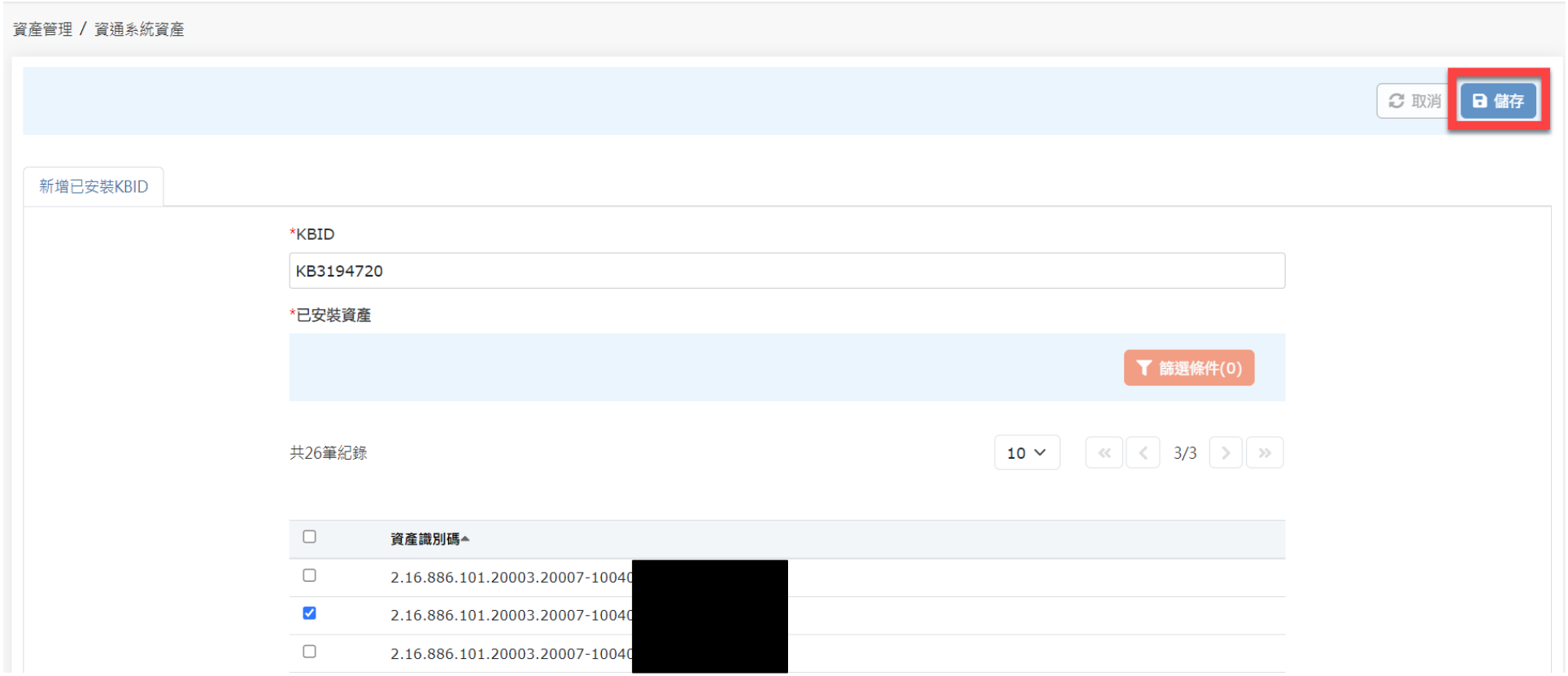
國家資通安全研究院
National Institute of Cyber Security

- 編輯已安裝KBID
  - Step2：點選「新增已安裝KBID」鈕，進入新增KBID頁

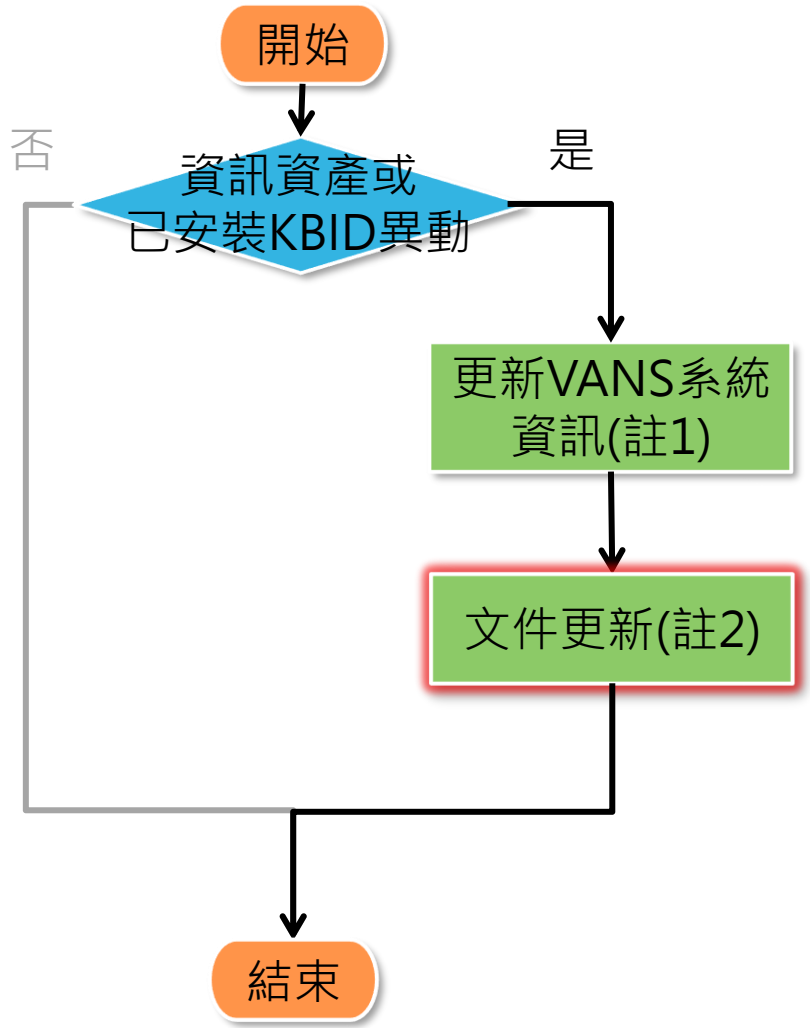
更新VANS系統資訊-單筆更新(6/6)

國家資通安全研究院
National Institute of Cyber Security

- 編輯已安裝KBID
  - Step3：進入此頁後輸入KBID與選取安裝的資產識別碼，按「儲存」鈕



資產與已安裝KBID更新作業流程



註1：更新VANS系統資訊：
新增、修改及刪除VANS
系統資訊

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

文件更新-資產清單匯出

國家資通安全研究院
National Institute of Cyber Security

- 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系統之資產

機關OID	機關名稱	資產識別碼	資產群組	資產名稱	資產廠商	資產版本	CPE 2.3	CPE完整名稱
2.16.886.101.[redacted]	[redacted]	1004044995202310183001	Admin	7-Zip 15.12 for Windows	Igor Pavlov	15.12	cpe:2.3:a:7-zip:7-zip:15.12:*:*:*:*:windows:*:*	7-Zip 15.12 for Windows
2.16.886.101.[redacted]	[redacted]	1004044995202310181012	HR	Microsoft SQL Server 2014 (64 位元)	Microsoft Corporation	N/A	cpe:2.3:a:microsoft:sql_server:2014:-:*:*:*:*:*:*	Microsoft SQL Server 2014
2.16.886.101.[redacted]	[redacted]	1004044995202310181011	Admin	Microsoft Windows Server 2016 Standard STANDARD SERVER 64 位元	Microsoft Corporation	10.0.14393.6351	cpe:2.3:o:microsoft:windows_server_2016:-:-:*:*:standard:*:x64:*	Microsoft Windows Server 2016 Standard Edition on X64

文件更新

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

資訊資產清冊

資產識別碼	資產群組	資產名稱	資產廠商	資產版本	CPE 2.3
7735988686955724972	1	Microsoft Windows Server 2012 R2 Standard x64	Microsoft Corporation	R2	cpe:2.3:o:microsoft:windows_server_2012:r2:sp1:*:*:*:*:x64:*
8735988686955724972	2	Microsoft Windows Server 2019 Datacenter x64	Microsoft	1809	cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:datacenter:*:x64:*
9735988686955724972	3	commons-beanutils	apache	1.8.0	cpe:2.3:a:apache:commons_beanutils:1.8.0:*:*:*:*:*:*:*
6735988686955724972	4	commons-fileupload	apache	1.3.2	cpe:2.3:a:apache:commons_fileupload:1.3.2:*:*:*:*:*:*:*
5735988686955724972	5	commons-io	apache	2.2	cpe:2.3:a:apache:commons_io:2.2:-:*:*:*:*:*:*

弱點清單

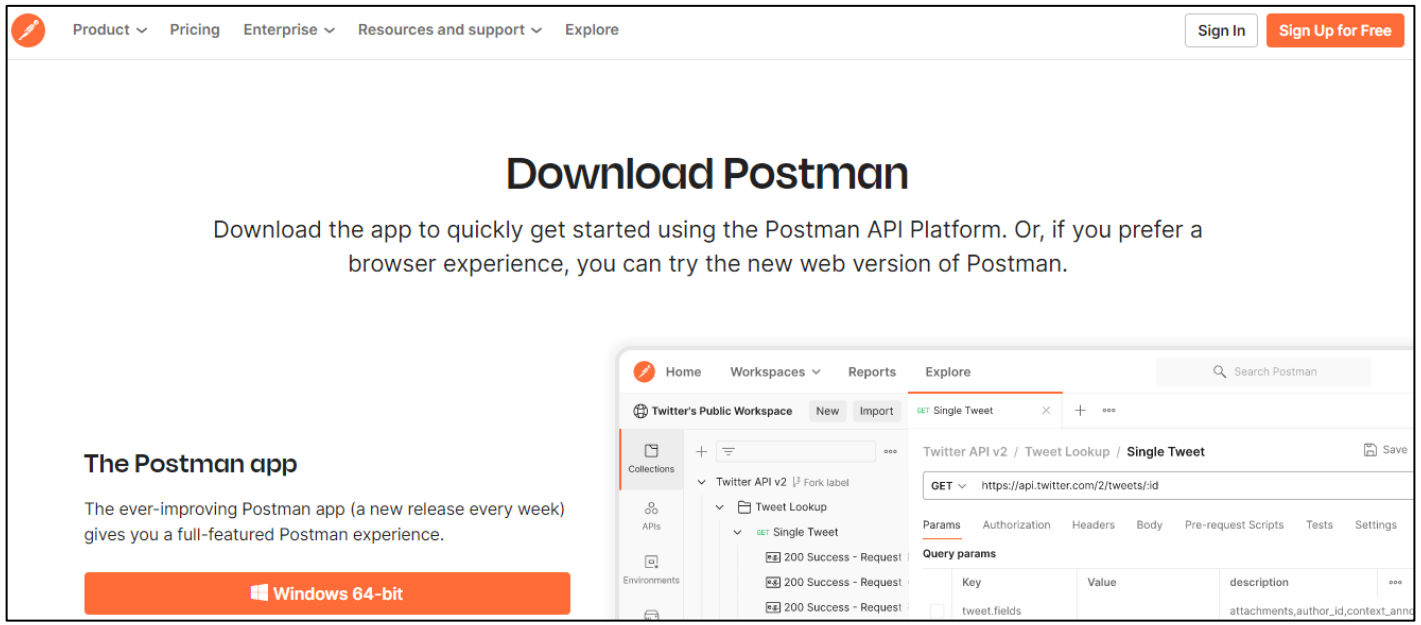
CVSS	發布時間	更新時間	弱點說明	NVD弱點說明連結	KBID修補情形	改善措施類別	改善措施
9.8	2020-01-14 23:15:33	2022-07-12 17:42:04	A remote code execution	https://nvd.nist.gov/vuln/detail/CVE-2020-0646	未安裝KBID。	2-已規劃修補	預計下周執行Windows update。
9.8	2020-01-14 23:15:33	2022-07-12 17:42:04	A remote code execution	https://nvd.nist.gov/vuln/detail/CVE-2020-0646	未安裝KBID。	2-已規劃修補	預計下周執行Windows update。
9.8	2020-01-14 23:15:33	2022-07-12 17:42:04	A remote code execution	https://nvd.nist.gov/vuln/detail/CVE-2020-0646	未安裝KBID。	未填寫改善措施	未填寫改善措施
9.8	2020-01-14 23:15:33	2022-07-12 17:42:04	A remote code execution	https://nvd.nist.gov/vuln/detail/CVE-2020-0646	未安裝KBID。	未填寫改善措施	未填寫改善措施

實作練習3

實作練習3(工具說明)(1/5)

國家資通安全研究院
National Institute of Cyber Security

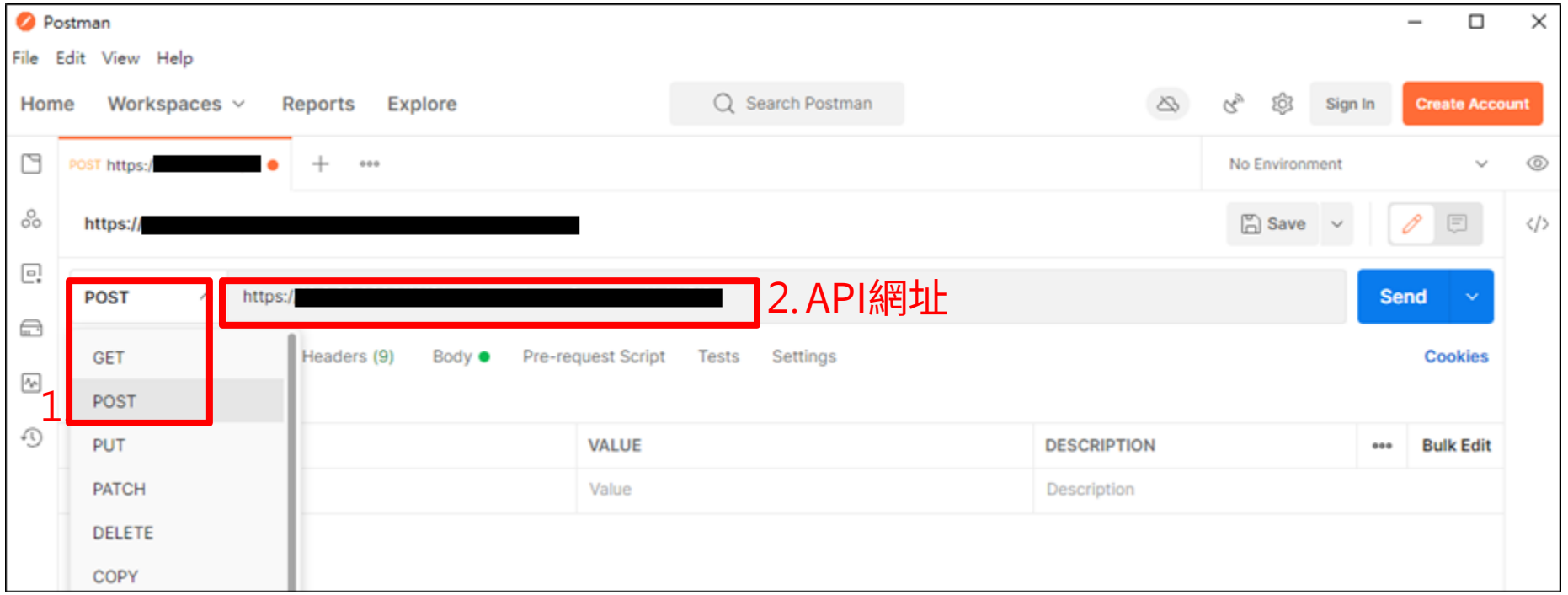
- Postman為API平台，可用來測試HTTP各種請求之工具，藉由回傳之訊息代碼即可得知測試結果
  - 下載網址：https://www.postman.com/downloads/
- API用以將不同服務進行串接，如VANS系統可透過API接收資產管理工具傳送之資訊資產



實作練習3(工具說明)(2/5)

國家資通安全研究院
National Institute of Cyber Security

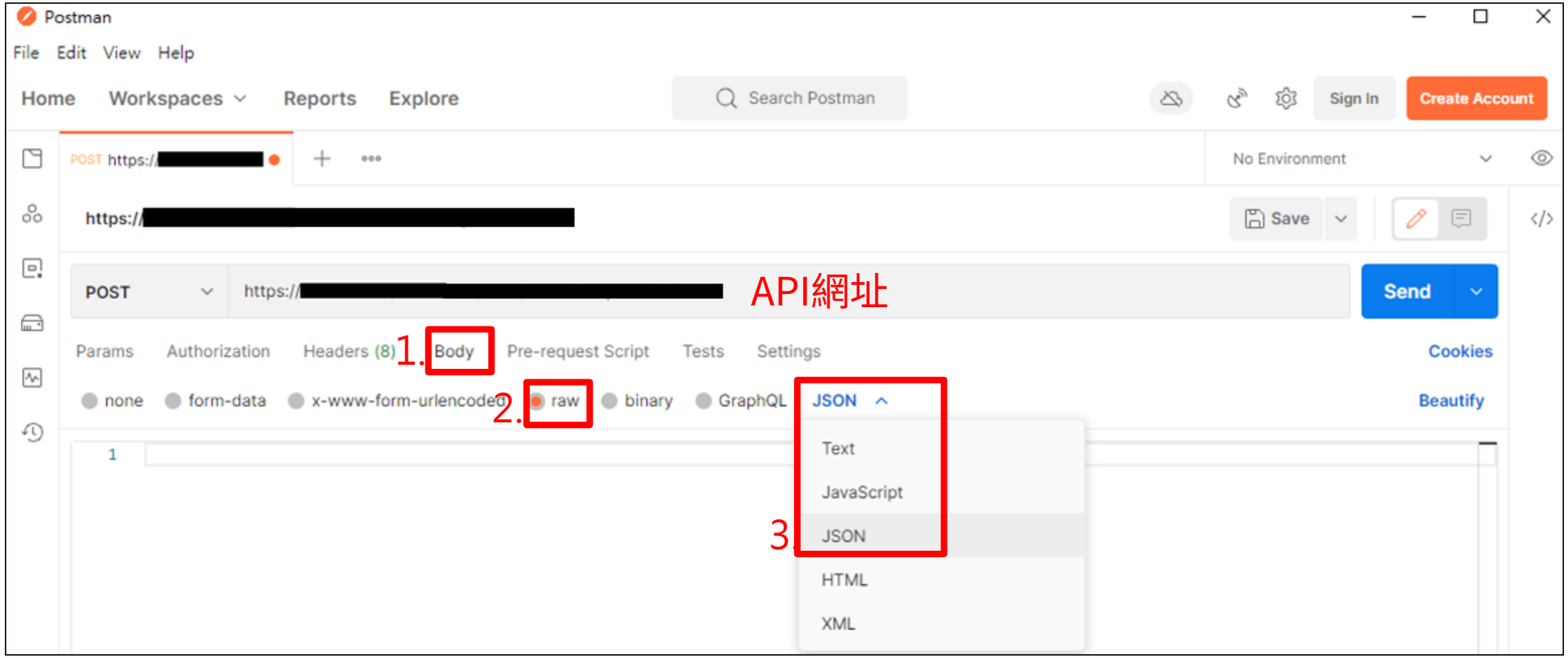
- API傳輸方式為POST
- 設定API網址
  - API IP申請完成通知信中將提供API網址



實作練習3(工具說明)(3/5)

國家資通安全研究院
National Institute of Cyber Security

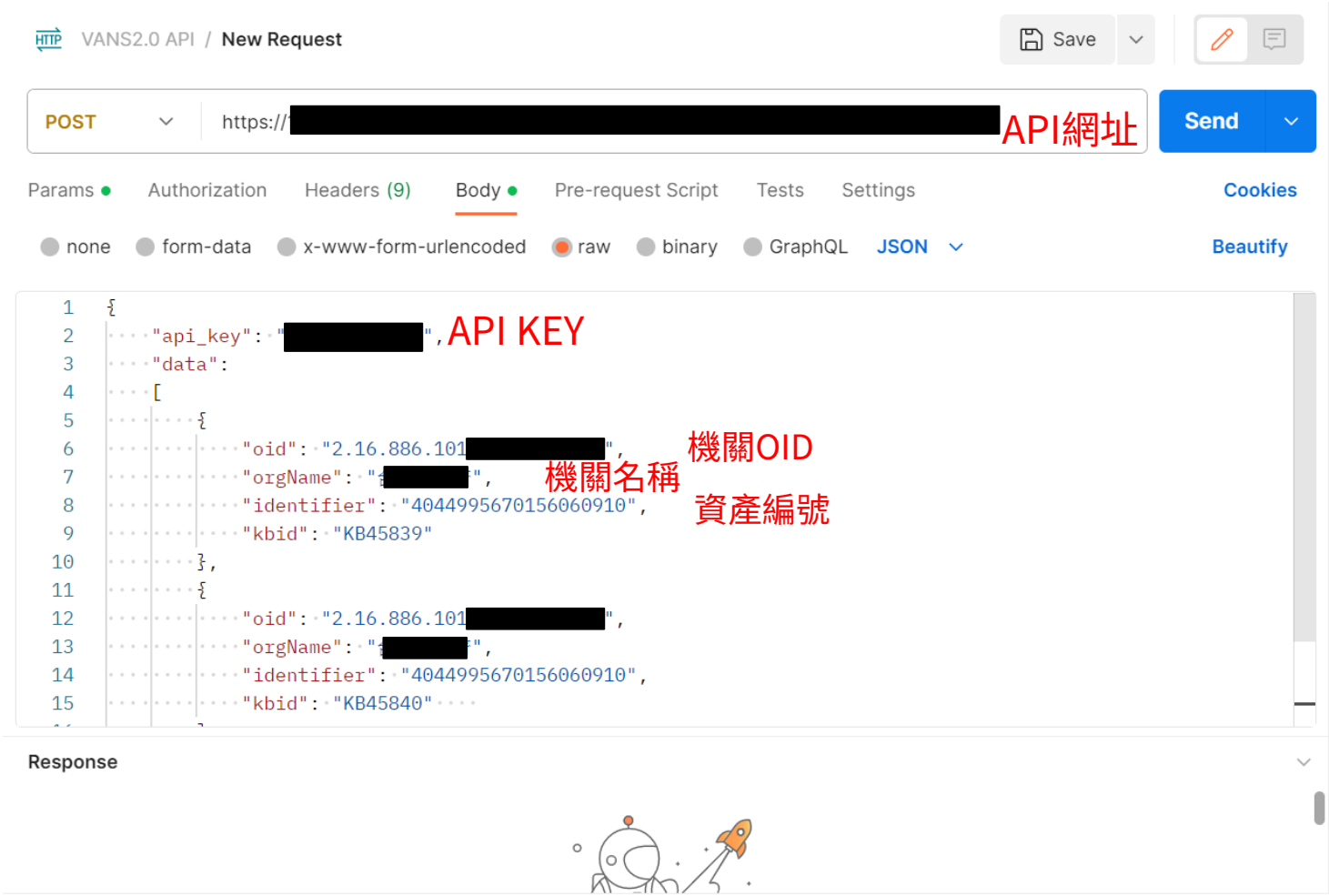
- API傳輸格式為JSON
  - Postman調整格式之步驟如下圖



實作練習3(工具說明)(4/5)

國家資通安全研究院
National Institute of Cyber Security

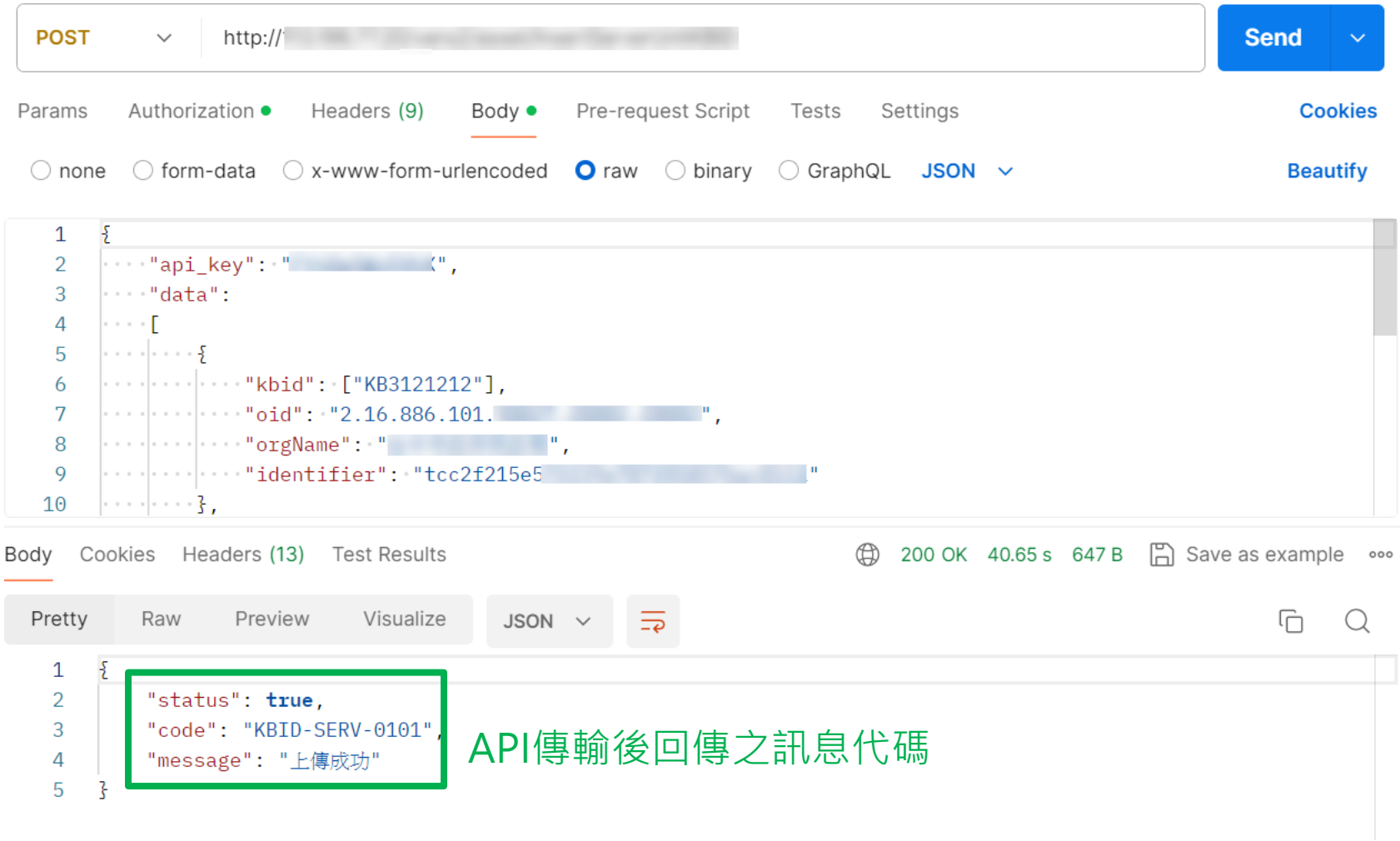
- 設定API KEY、OID、機關名稱(unit_name)及資產識別碼



實作練習3(工具說明)(5/5)

國家資通安全研究院
National Institute of Cyber Security

- 按下Send，即可於下方看到測試結果



實作練習3

國家資通安全研究院
National Institute of Cyber Security

- 登錄已安裝KBID，並確認弱點修補情形
- 本項練習時間15分鐘

項次	執行項目	產出項目/執行結果
1	透過API方式，上傳已安裝KBID • 開啟Postman (路徑：學員資料夾\01.實作練習\實作練習3\postman-portable.exe) • 設定API Key、機關OID、機關名稱、機關識別碼 • 送出	API回傳狀態 = ‘true’ API回傳代碼 = ‘KBID-SERV-0101’ API回傳訊息 = ‘上傳成功’
2	• 於資訊資產風險列表匯出弱點清單，搜尋並檢視CVE-2021-34448是否完成修補 • 安全性更新請參考KBID修補情形欄位	弱點清單

N	O	P	Q	R
弱點說明	NVD弱點說明連結	KBID修補情形	改善措施類別	改善措施
Windows Kernel Elevation of Privilege Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-202	未安裝KBID	未填寫改善措施	未填寫改善措施
Windows Internet Key Exchange (IKE) Extension Denial of S	https://nvd.nist.gov/vuln/detail/CVE-202	未安裝KBID	未填寫改善措施	未填寫改善措施
Windows Netlogon Denial of Service Vulnerability	https://nvd.nist.gov/vuln/detail/CVE-202	未安裝KBID	未填寫改善措施	未填寫改善措施

VANS常見問答(1/11)

國家資通安全研究院
National Institute of Cyber Security

政策規範

1. **應辦事項列表中資通安全弱點通報機制(VANS)應導入範圍為何?是否有建議之上傳頻率？**
   - 公務機關VANS導入範圍以全機關之資訊資產為原則，有關支持核心業務持續運作相關之資通系統主機與電腦應於規定時限內完成導入；關鍵基礎設施提供者VANS之導入範圍至少應涵蓋關鍵資訊基礎設施及營運持續運作必要相關資通系統。
   - 有關資訊資產上傳頻率，除重大弱點通報或大量資產異動外，建議每個月至少定期上傳1次，機關如採系統化介接方式，可增加上傳頻率；並應針對發現弱點設定修補期限，未修補前應加強防護及異常偵測，以確保弱點管理之即時性及有效性。

2. **限於經費無法導入伺服器該如何處理?可否例外?**
   - VANS導入範圍以全機關之資訊資產為原則，機關如囿於經費，可考量與核心業務之關聯性、資安風險程度及資訊資產重要性等，優先導入支持核心業務持續運作相關之資通系統主機與電腦。

3. **針對高風險以上弱點，是否訂定相關修補時間?**
   - 目前尚未訂定修補時間，惟建議發現高風險以上之弱點時，如無法及時完成修補，應於１週內決定弱點處置方式並於VANS系統填寫改善措施。

4. **填寫弱點改善內容後，資安署是否會管考後續改善結果？**
   - VANS機制主要協助機關進行自我弱點管理，惟若爆發重大弱點時，將參考填復內容以了解機關處理方式與進度。

VANS常見問答(2/11)

國家資通安全研究院
National Institute of Cyber Security

作業程序

1. **系統所比對出之弱點，如何得知弱點存在於哪些主機呢？**
   - 執行資訊資產盤點作業後所產出之資訊資產清冊中，內容包含各軟體資產對應之資產識別碼資訊，可藉由弱點詳細資訊中的資產識別碼，得知該弱點之主機。

2. **VANS系統弱點比對結果中，有許多微軟產品弱點，若平時已有定期安裝安全性更新(KBID)，該如何判斷哪些弱點尚待修補？**
   - 若機關已完整安裝安全性更新(KBID)，大多數弱點可視為已完成修補，少數非透過安全性更新修復之弱點，建議參考微軟官方所提供之緩解措施進行處理。
   - 可透過VANS系統安全性更新(KBID)與弱點(CVE)關聯分析功能，查看尚待修補之弱點。

3. **弱點若無法修補時，該如何處理？**
   - 若遇到已停止更新支援或無法修補之弱點時，機關可依據自身ISMS政策評估該弱點對機關可能產生之影響，並採取因應之配套措施，並將實際情況填寫至VANS系統改善措施中。

4. **主管機關是否可替所屬機關上傳資訊資產與已安裝KBID？**
   - 可以。主管機關上傳資料時，可於上傳清單中填寫所屬機關OID、機關名稱欄位，即可替所屬機關上傳資訊資產或已安裝KBID。

VANS常見問答(3/11)

國家資通安全研究院
National Institute of Cyber Security

作業程序

5. 若主管機關替所屬機關上傳資訊資產，所屬機關是否需申請API介接IP？

- 因進行API傳輸者為主管機關，故僅需由主管機關申請API介接IP即可。

6. 為何登入VANS系統時顯示個人帳號已被停用，遇到此狀況時該如何解決?

- 基於資安考量，超過180天未登入iAuth系統之帳號將被鎖定，於登入VANS系統時將顯示該帳號已被停用。
- 被停用的帳號可透過iAuth自行解除鎖定，解除後可再至VANS系統登入。

7. 如何刪除VANS系統機關管理者帳號？

- 請填寫「資通安全弱點通報系統(VANS系統)機關管理者帳號申請(異動)單」並核章後，提交資安署審查，審核過後由資安院管理者進行後續處理。

8. 未比對到CPE之資產，是否仍需上傳至VANS系統？

- 公務機關VANS導入範圍以全機關之資訊資產為原則，關鍵基礎設施提供者VANS之導入範圍至少應涵蓋關鍵資訊基礎設施及營運持續運作必要相關資通系統，因此未比對到CPE條目之資產仍需上傳至VANS系統。

VANS常見問答(4/11)

國家資通安全研究院
National Institute of Cyber Security

系統操作

1. 「資通系統資產」、「使用者電腦資產」及「工業控制系統資產」差異為何？

- 功能皆相同，主要依據盤點對象分為「資通系統」、「使用者電腦」及「工業控制系統」類別，以方便機關區分與管理。

2. 如何知道資產是否上傳成功與弱點比對完成?

- VANS系統於資產上傳後，經系統解析後，會在畫面上顯示成功訊息。
- VANS系統於資產弱點比對完成後，會收到「資產風險項目比對完成」通知信件。

VANS常見問答(5/11)

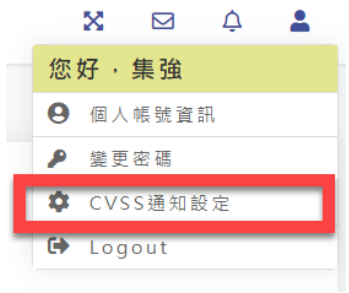
國家資通安全研究院
National Institute of Cyber Security

系統操作

3.

為什麼我收不到VANS系統的通知信?

- 請確認「個人資訊」→「請輸入欲接收弱點通知的電子郵件」是否已經正確設定電子郵件(綠框處是否有您的電子郵件)
- 請確認「設定管理」→「請選擇是否接收弱點通知」是否開啟(紅框處必須為「ON」狀態)



VANS常見問答(6/11)

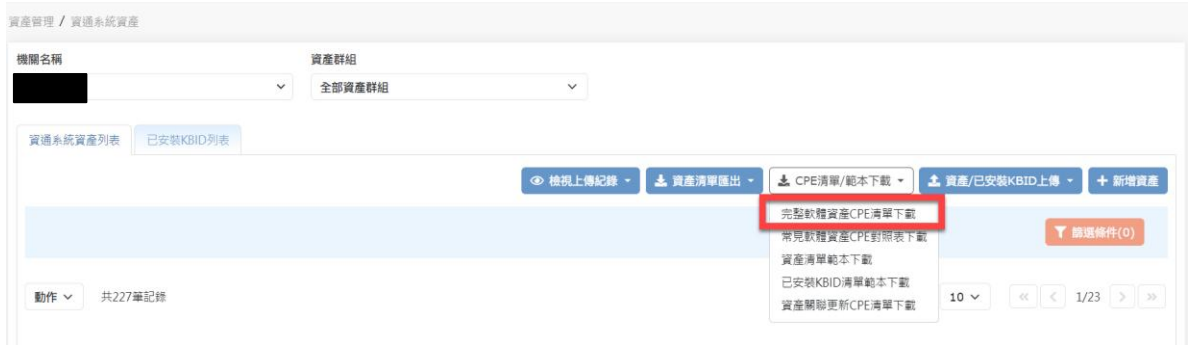
國家資通安全研究院
National Institute of Cyber Security

系統操作

4.

資產上傳出現錯誤該如何排除?

1.自VANS系統下載最新版本「完整軟體資產CPE清單」



2.依據錯誤訊息找到對應之CPE條目，確認是否可於「完整軟體資產CPE清單」找到完全相同之「**CPE2.3**」與「**CPE完整名稱**」

- **有找到相同「CPE2.3」與「CPE完整名稱」**時，應為**正確**之CPE條目。若仍無法上傳請透過VANS服務信箱(VansService@nics.nat.gov.tw)反映
- **未找到相同「CPE2.3」與「CPE完整名稱」**時，應為**錯誤**之CPE條目，無法上傳至VANS系統。請依循步驟3~6至NVD官網進行確認該CPE條目是否已遭取代

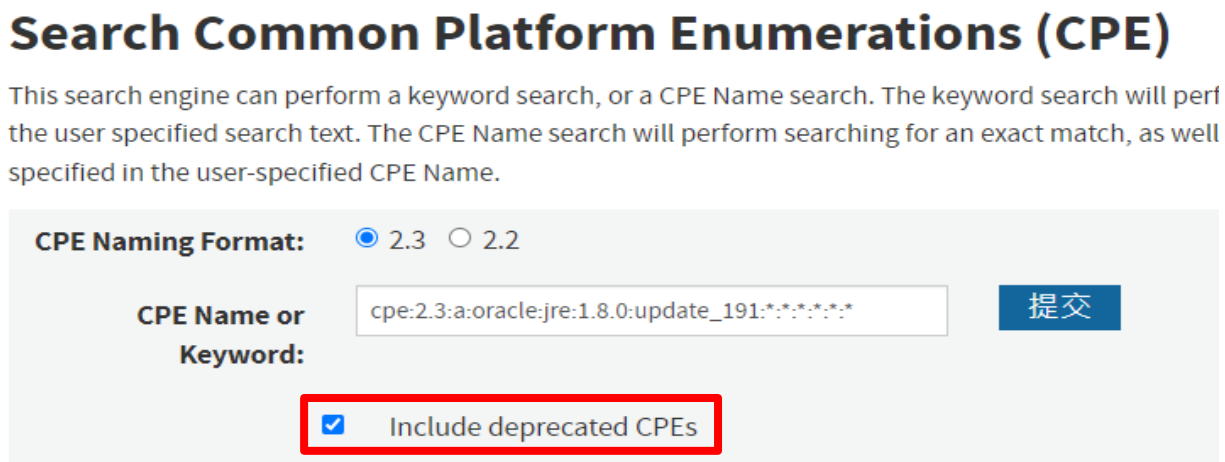
VANS常見問答(7/11)

國家資通安全研究院
National Institute of Cyber Security

系統操作

4.

3.至NVD官網(https://nvd.nist.gov/products/cpe/search)查詢該CPE條目，並確認勾選「Include deprecated CPEs」



4.搜尋後，點選欲查找之CPE條目

VANS常見問答(8/11)

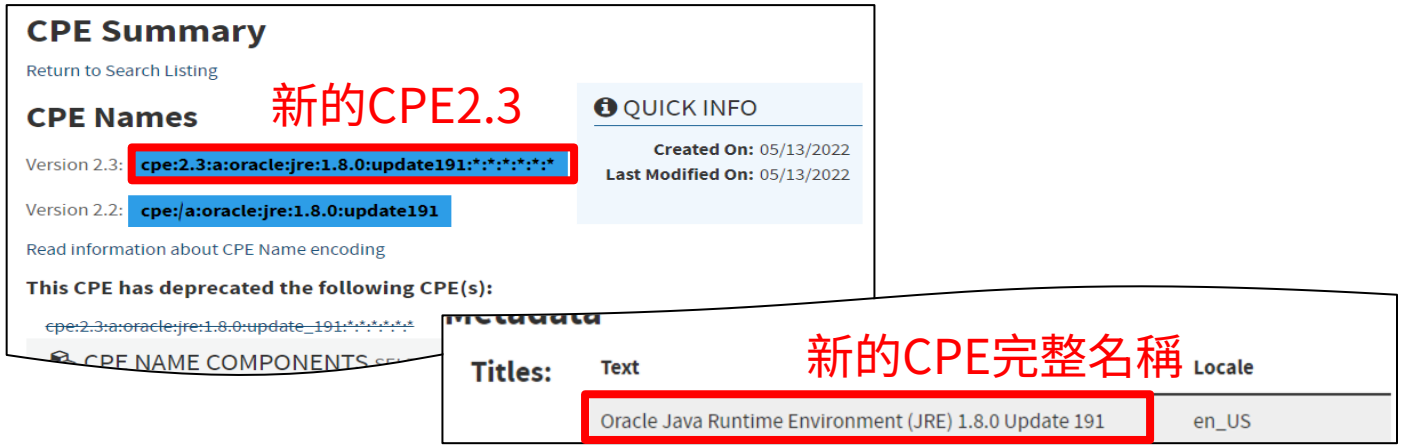
國家資通安全研究院
National Institute of Cyber Security

系統操作

4.

5.依據頁面資訊確認該CPE條目是否已遭取代

6.請點選「新的CPE條目」以查看「新的CPE2.3」與「新的CPE完整名稱」，並更新至上傳清單，即可重新上傳至VANS系統



VANS常見問答(9/11)

國家資通安全研究院
National Institute of Cyber Security

系統操作

5. 曾上傳資產至VANS系統，透過網頁或API再次上傳資產時，系統會如何處理?

- (1)上傳的資產，若不存在系統中，則會新增此資產。
- (2)上傳的資產，若已存在系統中，將以更新的方式更新資產。
- (3)系統現有的資產，若不存在於此次上傳之資產內，將予以刪除。

6. VANS系統之「可修補KBID」功能是否已有考量KB取代關係呢？

- VANS系統已有考量KB取代關係，請點擊CVE弱點之「可修補KBID」欄位，彈出清單內容即顯示可修補此弱點之所有KB編號

7. 上傳已安裝KBID至VANS系統後，要如何查看哪些弱點尚未處置？

- 可至資訊資產風險列表中，查看各資產「弱點詳細資訊」之「弱點狀態」欄位，若欄位值為「**未處置-未填寫改善措施**」，請**儘速進行弱點**修補作業或接受該風險並進行填寫改善措施。

VANS常見問答(10/11)

國家資通安全研究院
National Institute of Cyber Security

系統操作

8. 機關資產、KBID上傳後如何查詢結果？

- (1)上傳完的資產，在各資產管理功能內，點選「檢視上傳紀錄」，選取「檢視資產清單上傳紀錄」，檢視該類別資產的上傳紀錄。
- (2)上傳完的KBID，在各資產管理功能內，點選「檢視上傳紀錄」，選取「檢視已安裝KBID清單上傳紀錄」，檢視該類別資產的KBID上傳紀錄。

9. 機關如何查詢已經完成CVSS 7分以上弱點的改善措施填寫？

- 可使用資產風險狀態的「弱點關聯列表」功能，在「CVSS分數起」查詢欄位輸入7
- 接著在查詢結果中，點選一筆CVE的「受影響資產詳細資訊」按鈕
- 從顯示的弱點詳細資訊中的「弱點狀態」，即可得知。

VANS常見問答(11/11)

國家資通安全研究院
National Institute of Cyber Security

綜合問答

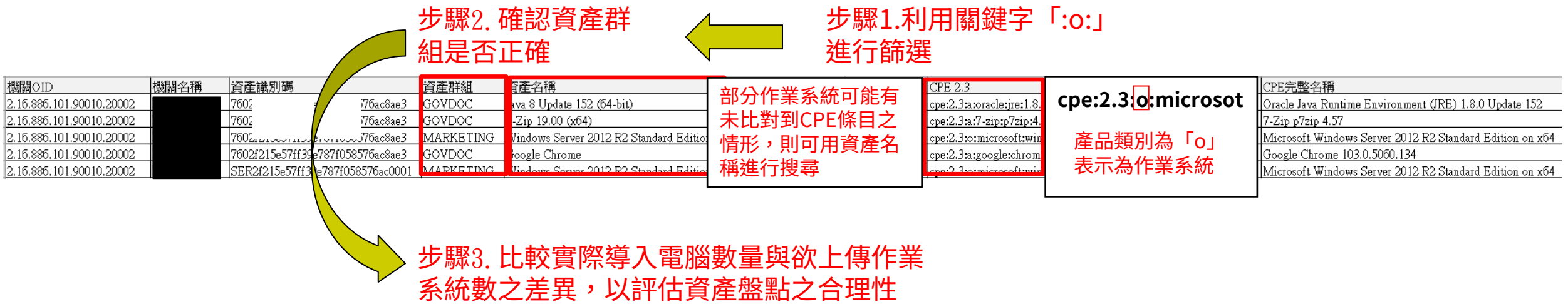
1. VANS與弱點掃描之差異？

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	• 機關資產異動後，會觸發1次弱點比對 • 每日NVD更新後，會觸發1次弱點比對	定期執行掃描

結論(1/2)

國家資通安全研究院
National Institute of Cyber Security

- 導入應特別注意事項
  - ➢上傳資訊資產前：機關應檢視欲上傳資產內容之合理性，如利用CPE條目或資產名稱檢視上傳作業系統數與實際導入電腦數量之差異，以評估資產盤點之合理性



機關OID	機關名稱	資產識別碼	資產群組	資產名稱	CPE 2.3	CPE完整名稱
2.16.886.101.90010.20002	[redacted]	7602 76ac8ae3	GOVDOC	ava 8 Update 152 (64-bit)	cpe:2.3:a:oracle:jre:1.8.	Oracle Java Runtime Environment (JRE) 1.8.0 Update 152
2.16.886.101.90010.20002		7602 76ac8ae3	GOVDOC	-Zip 19.00 (x64)	cpe:2.3:a:7-zip:p7zip:4.	7-Zip p7zip 4.57
2.16.886.101.90010.20002		7602 76ac8ae3	MARKETING	Windows Server 2012 R2 Standard Editio	cpe:2.3:o:microsoft:win	Microsoft Windows Server 2012 R2 Standard Edition on x64
2.16.886.101.90010.20002		7602f215e57ff39e787f058576ac8ae3	GOVDOC	oogle Chrome	cpe:2.3:a:google:chrom	Google Chrome 103.0.5060.134
2.16.886.101.90010.20002		SER2f215e57ff3e787f058576ac0001	MARKETING	Windows Server 2012 R2 Standard Editio	cpe:2.3:o:microsoft:win	Microsoft Windows Server 2012 R2 Standard Edition on x64

結論(2/2)

國家資通安全研究院
National Institute of Cyber Security

- 導入應特別注意事項
  - 上傳資訊資產後：
    - 於上傳資產隔天，應注意資產解析之通知信結果，如解析失敗，可能原因及相關解決方式可參考教材第79~82、145頁
    - 每日：機關應注意VANS弱點通知信(通知分數門檻不應高於7分)，當發現高風險(CVSS 7分)以上之弱點，應儘速決定弱點處置方式並於1週內於VANS系統填寫改善措施
    - 每月：機關應每月更新資訊資產，如接獲重大弱點通報或大量資產異動，亦應即時進行資訊資產更新作業
    - 查詢上傳資訊資產的合理性，步驟如下:


Q
&
A

資產識別碼與資產群組說明

VANS舊資訊格式-共用資產識別碼

- 資產識別碼的來源與用途
  - VANS的資訊資產資訊欄位包含必要的資產識別碼，設計的目的在識別機關的資訊資產所在的資產主機
  - 也可透過資產識別碼，識別KBID安裝的資產主機，可明確的區分出有安裝KBID的資產主機

新/舊格式的功能效用

- 資訊資產、弱點、KBID修補的新/舊格式資訊說明

功能	新格式欄位資訊	舊格式欄位資訊
資訊資產上傳API	資訊資產不可重複	資訊資產可重複
已安裝KBID上傳API	已安裝KBID不可重複	已安裝KBID可重複
新增/修改資訊資產	資訊資產不可重複	資訊資產可重複
弱點	可區分在不同資產上的資訊資產弱點	產生多筆重複的資訊資產的弱點
KBID修補	依據KBID所在資產主機，只修補在此資產主機上的資訊資產的弱點	因所有資產皆在同一台資產主機上，一個KBID即可修補可被其修補的機關內的所有資產的所有弱點

其他功能說明

機關總覽

- 機關總覽包含以下的子功能
  - 查詢機關資產
  - 資產查詢
  - 受影響弱點查詢
  - 執行記錄

機關總覽-查詢機關資產(1/4)

國家資通安全研究院
National Institute of Cyber Security

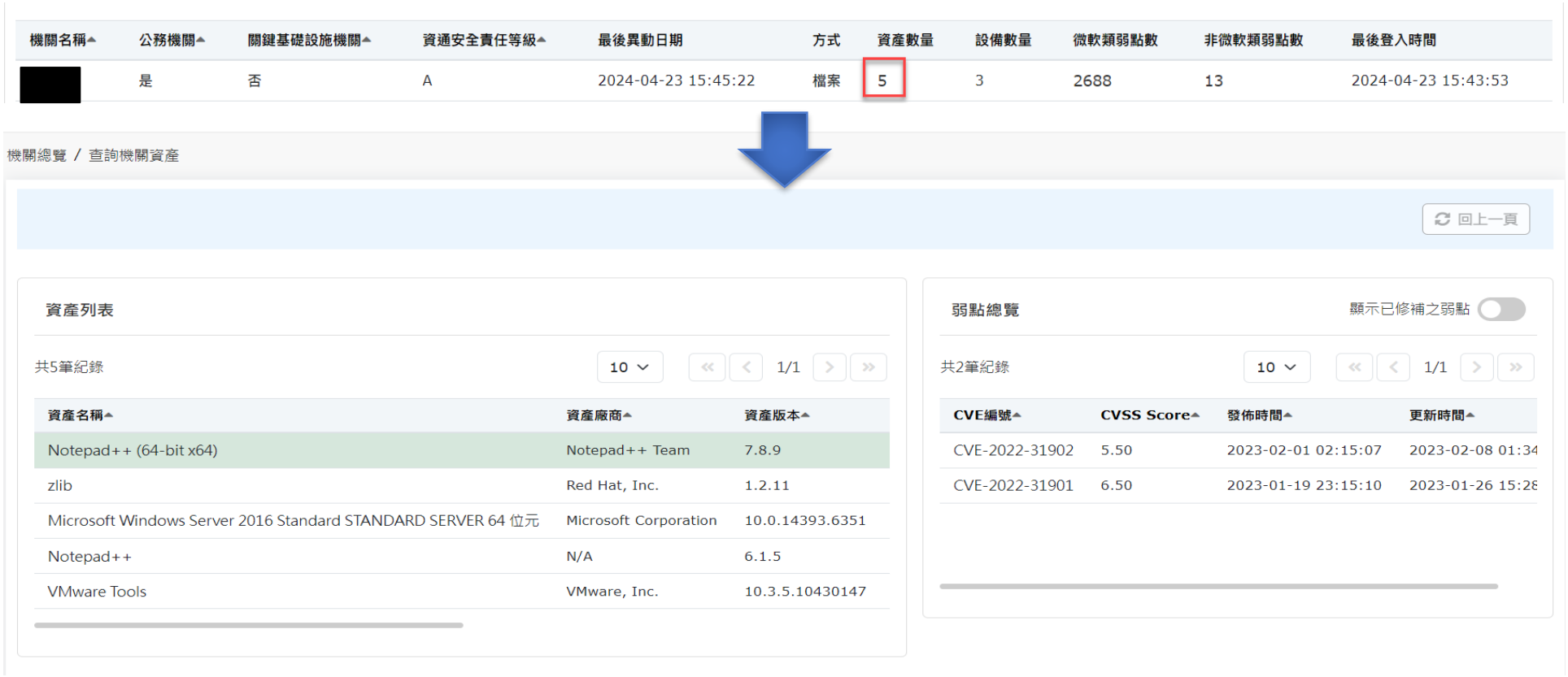
- 查詢機關的資產
  - ➢使用者進入此功能輸入機關名稱與條件，可查詢機關不同類型資產、設備數量及弱點資料

機關名稱	公務機關	關鍵基礎設施機關	資通安全責任等級	最後異動日期	方式	資產數量	設備數量	微軟類弱點數	非微軟類弱點數	最後登入時間
[redacted]	是	否	A	2024-04-23 15:45:22	檔案	5	3	2688	13	2024-04-23 15:43:53
				2024-04-03 17:15:55	API	2	2	0	17	2024-05-09 14:48:49
	是	否	A	2024-04-03 17:15:55	檔案	3	2	0	4	2024-05-09 14:48:49
				2024-04-03 17:15:58	網頁	6	4	2692	19	2024-05-09 14:48:49

機關總覽-查詢機關資產(2/4)

國家資通安全研究院
National Institute of Cyber Security

- 由資產看弱點
  - ➢點擊上頁資產數量的數字，會導到資產列表頁
  - ➢點擊資產列表不同資產，右方會顯示該資產對應的弱點

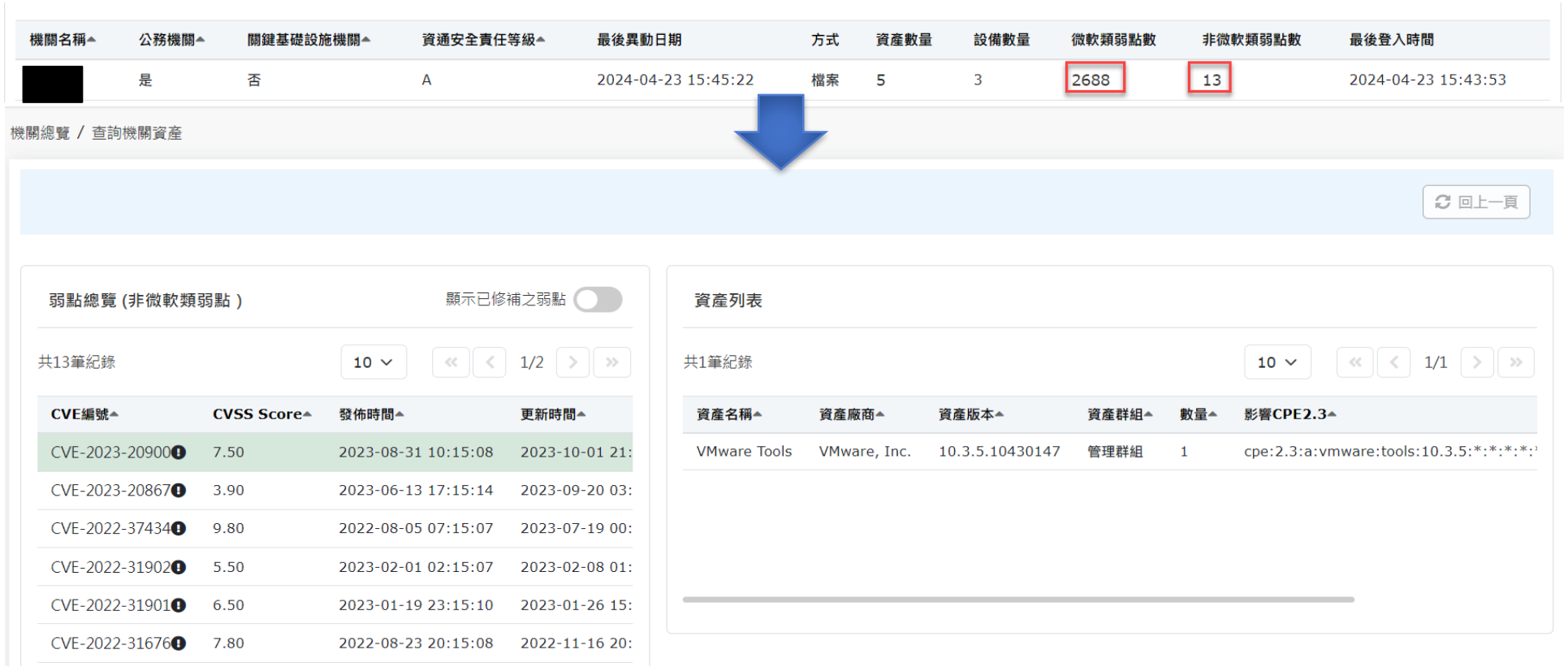


機關名稱	公務機關	關鍵基礎設施機關	資通安全責任等級	最後異動日期	方式	資產數量	設備數量	微軟類弱點數	非微軟類弱點數	最後登入時間
[redacted]	是	否	A	2024-04-23 15:45:22	檔案	5	3	2688	13	2024-04-23 15:43:53

機關總覽-查詢機關資產(3/4)

國家資通安全研究院
National Institute of Cyber Security

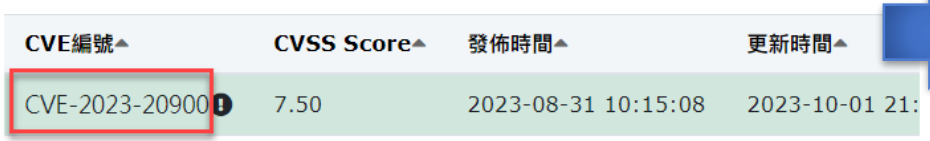
- 由弱點看資產
  - ➢點擊上頁弱點數量的數字，會導到弱點總覽頁
  - ➢點擊❗圖示，右方會顯示該弱點對應的資產



機關總覽-查詢機關資產(4/4)

國家資通安全研究院
National Institute of Cyber Security

- 檢視CVE資訊
  - ➢點擊上頁CVE編號，會彈出CVE資訊的小視窗



機關總覽-資產查詢(1/2)

國家資通安全研究院
National Institute of Cyber Security

- 資產查詢
  - ➢使用者進入此功能輸入機關名稱與條件，可查詢機關各類型資產、設備數量

機關總覽-資產查詢(2/2)

國家資通安全研究院
National Institute of Cyber Security

- 檢視資產詳細資訊
  - ➢點擊上頁資產數量的數字，會彈出資產清單小視窗

機關名稱	公務機關	關鍵基礎設施機關	資通安全責任等級	資通系統數量	資通設備數量	使用者電腦數量	使用者設備數量	工業控制系統數量	工控設備數量	網通設備數量	網通設備數量
[redacted]	是	否	A	5	3	0	0	0	0	0	0

機關總覽-受影響弱點查詢(1/2)

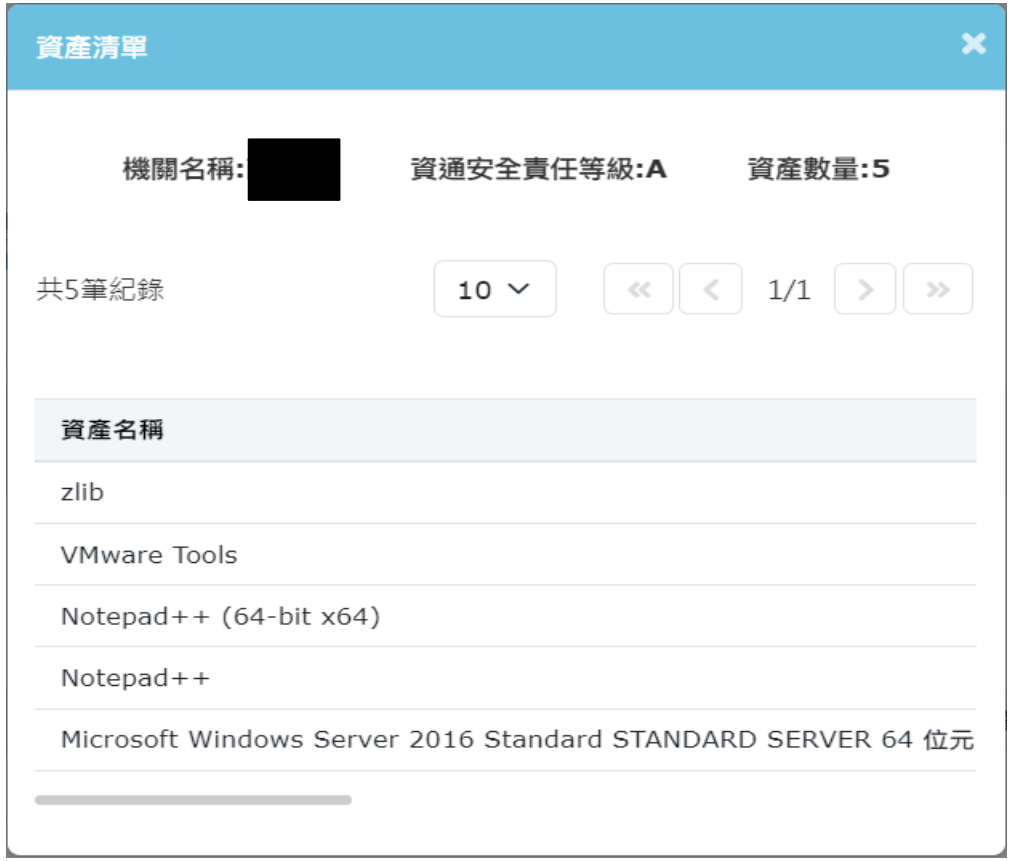
國家資通安全研究院
National Institute of Cyber Security

- 受影響弱點查詢
  - ➢使用者進入此功能輸入機關名稱與CVE編號，可以查詢機關受到弱點影響的各類型資產數量

機關總覽-受影響弱點查詢(2/2)

國家資通安全研究院
National Institute of Cyber Security

- 檢視資產詳細資訊
  - ➢點擊上頁資產數量的數字，會彈出資產清單小視窗如下



機關總覽-執行紀錄(1/2)

國家資通安全研究院
National Institute of Cyber Security

- 提供機關執行紀錄統計、導入情形統計及上傳與弱點處理情形等資訊
- 查詢結果可依照全部、資通系統、使用者電腦或工業控制系統，並分別顯示資料列表與統計圖表

機關總覽-執行紀錄(2/2)

國家資通安全研究院
National Institute of Cyber Security

- 3種執行記錄類別之查詢條件與查詢結果項目

項次	執行記錄類別	查詢條件	查詢結果項目
1	執行紀錄統計	• 最近次數 • 資產異動(上傳)方式	• 資產異動(上傳)次數 • 已安裝KBID異動(上傳)次數 • 資產數量 • 受影響資產數量 • CPE種類弱點數量
2	導入情形統計	• 資產異動(上傳)時間起迄 • 資產異動(上傳)方式	• 資產異動(上傳)次數 • 已安裝KBID異動(上傳)次數 • 資產數量 • 受影響資產數量 • 資產弱點數量 • CPE種類弱點數量 • 弱點修補數量
3	上傳與弱點處理情形	• 作業時間起迄 • 資產異動(上傳)方式	• 弱點修補數量

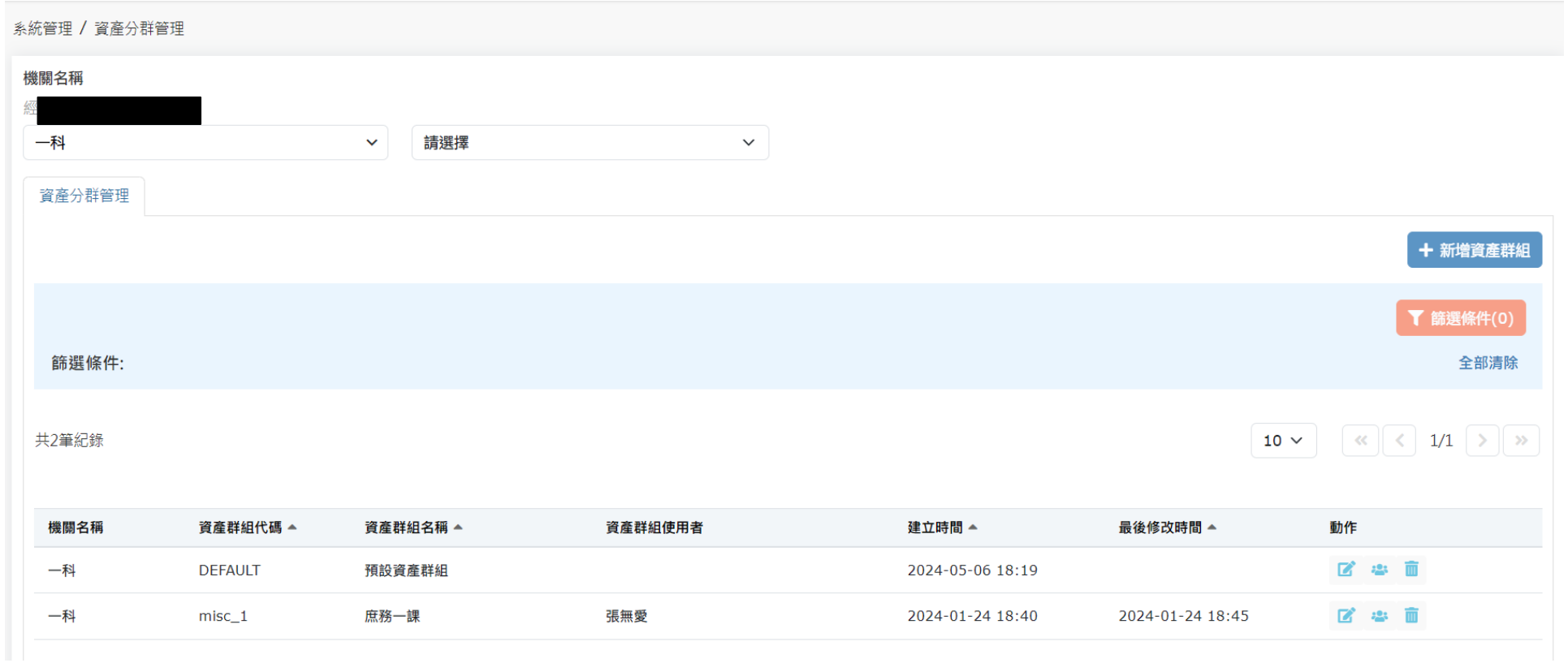
系統管理

- 系統管理包含以下的子功能
  - 資產分群管理(限機關管理者)
  - 系統操作日誌
  - API服務申請(限機關管理者)
  - API KEY管理

系統管理-資產分群管理(1/5)

國家資通安全研究院
National Institute of Cyber Security

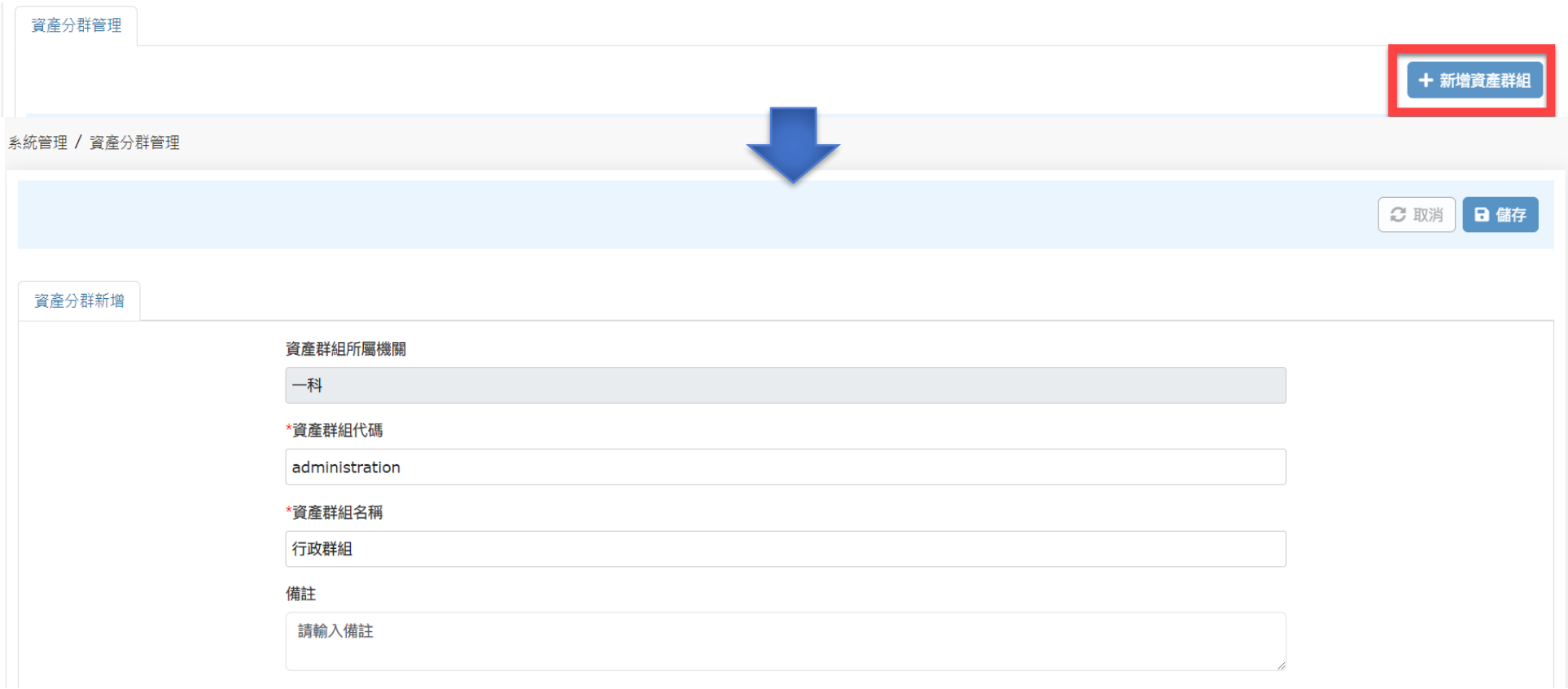
- 查詢資產群組
  - ➢使用者進入此功能選取機關與輸入條件，可以查詢符合條件之資產群組



系統管理-資產分群管理(2/5)

國家資通安全研究院
National Institute of Cyber Security

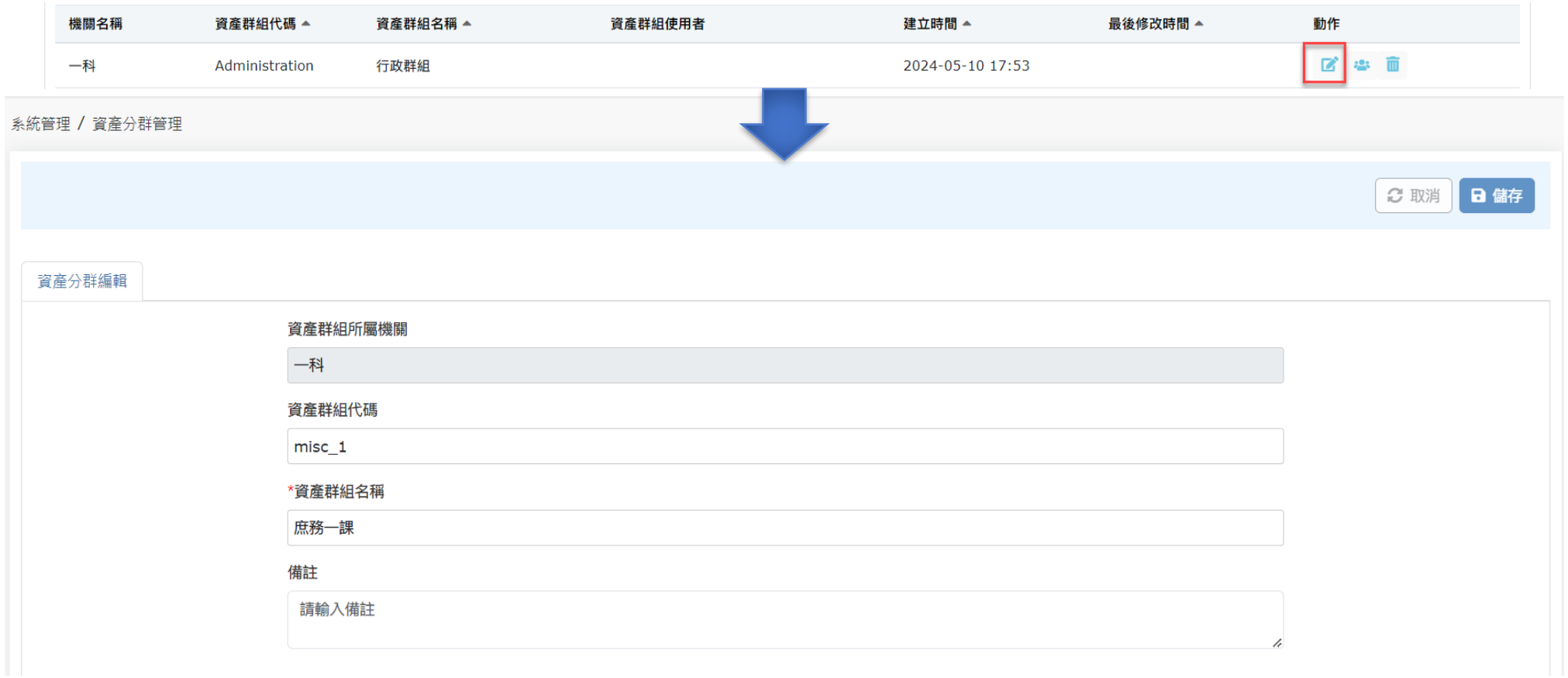
- 新增資產群組
  - ➢點擊上頁的「新增資產群組」鈕，系統導至資產群組新增頁，輸入資料後，按「儲存」鈕



系統管理-資產分群管理(3/5)

國家資通安全研究院
National Institute of Cyber Security

- 編輯資產群組
  - ➢點擊查詢頁的「編輯」鈕，系統導至資產群組編輯頁，修改資料後，按「儲存」鈕



系統管理-資產分群管理(4/5)

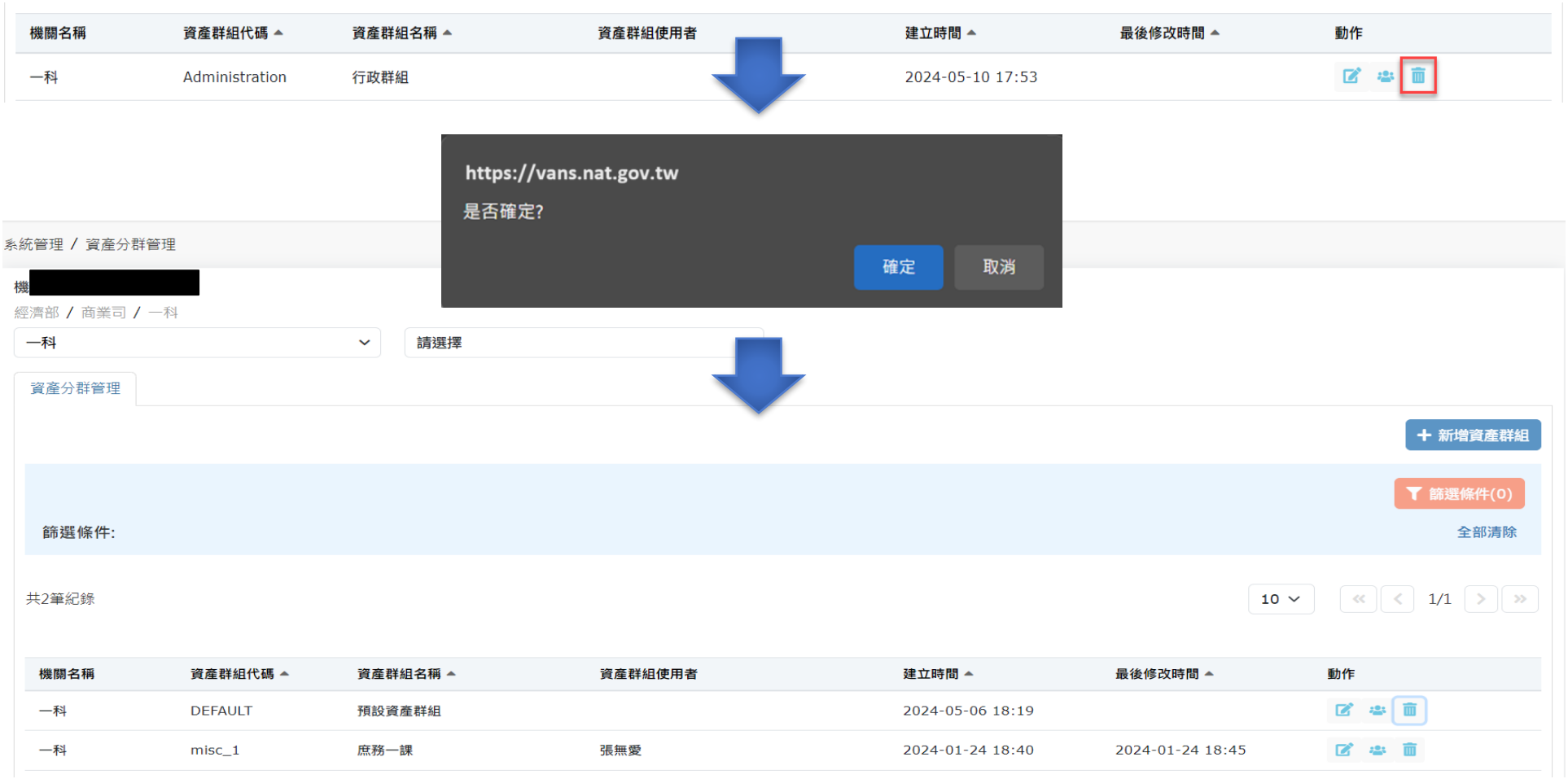
國家資通安全研究院
National Institute of Cyber Security

- 資產群組加入使用者
  - ➢點擊查詢頁的「加入使用者」鈕，系統導至資產群組加入使用者頁，選取使用者後，按「儲存」鈕

系統管理-資產分群管理(5/5)

國家資通安全研究院
National Institute of Cyber Security

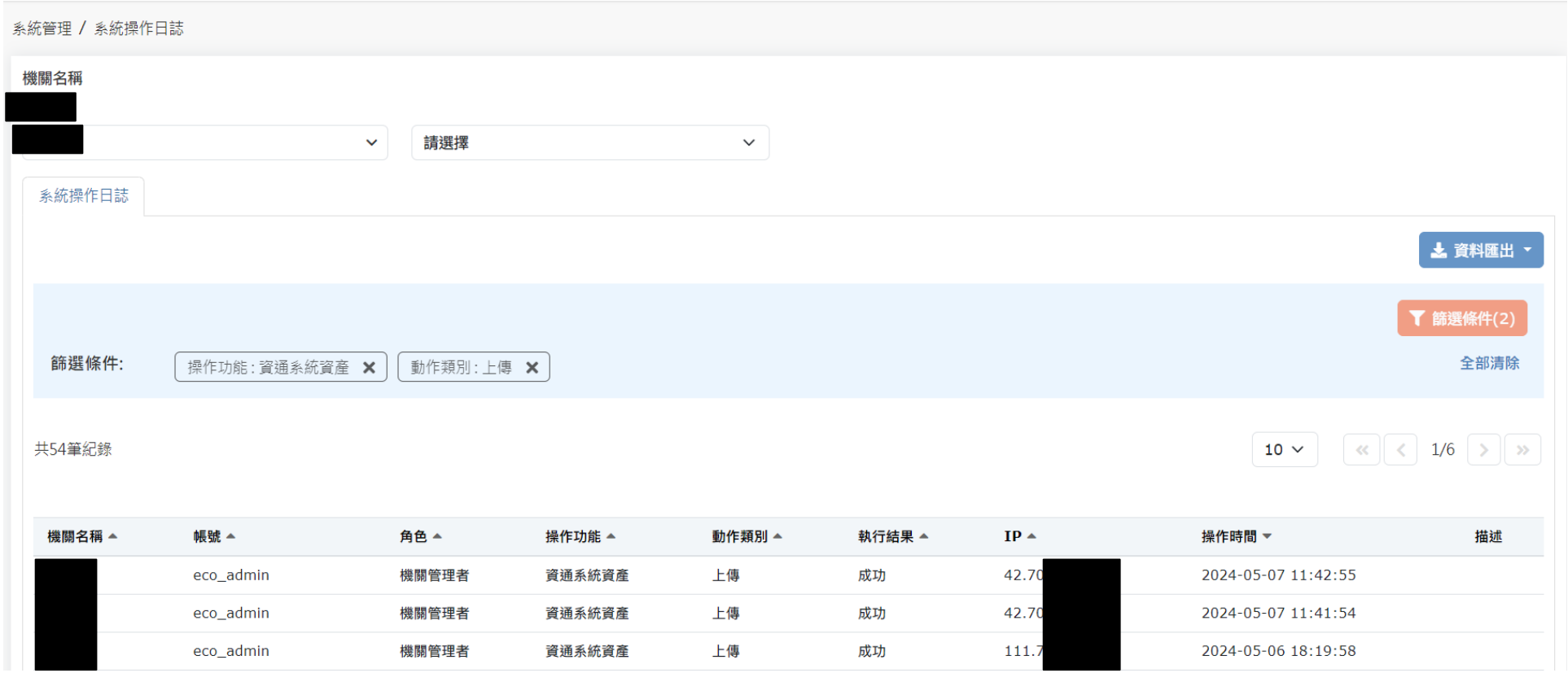
- 刪除資產群組
  - ➢點擊查詢頁的「刪除」鈕，使用者確認後，系統將此資產群組刪除



系統管理-系統操作日誌(1/2)

國家資通安全研究院
National Institute of Cyber Security

- 查詢系統操作日誌
  - ➢使用者進入此功能選取機關與輸入條件，可以查詢符合條件之系統操作日誌



系統管理-系統操作日誌(2/2)

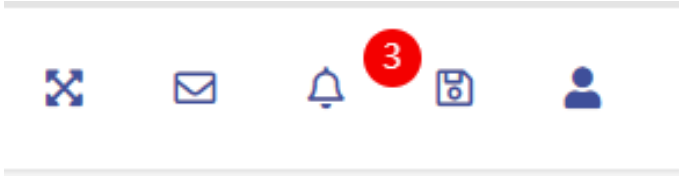
國家資通安全研究院
National Institute of Cyber Security

- 查詢資料匯出
  - ➢使用者查詢出資料後，可按「資料匯出」鈕將資料匯出

	A	B	C	D	E	F	G	H	I
1	機關名稱	帳號	角色	操作功能	動作類別	執行結果	IP	操作時間	描述
2	[redacted]	eco_admin	機關管理者	資通系統資產	上傳	成功	42.70[redacted]	2024-05-07 11:42:55	已安裝KBID清單上傳
3	[redacted]	eco_admin	機關管理者	資通系統資產	上傳	成功	42.70[redacted]	2024-05-07 11:41:54	已安裝KBID清單上傳
4	[redacted]	eco_admin	機關管理者	資通系統資產	上傳	成功	111.7[redacted]	2024-05-06 18:19:58	資產清單上傳
5	[redacted]	eco_admin	機關管理者	資通系統資產	上傳	成功	42.70[redacted]	2024-04-03 17:15:55	資產清單上傳

個人資訊

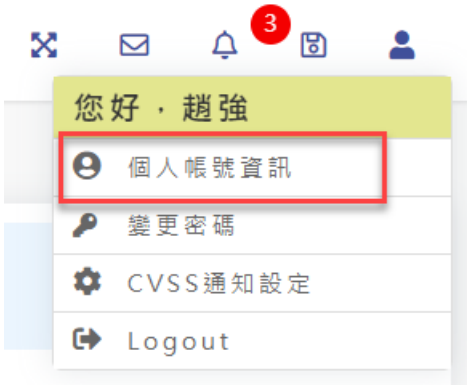
- 個人資訊位在頁面右上方，圖示由右至左功能如下：
  - 個人帳號資訊
  - 檔案下載
  - 通知
  - 訊息
  - 全螢幕



個人資訊-個人帳號資訊

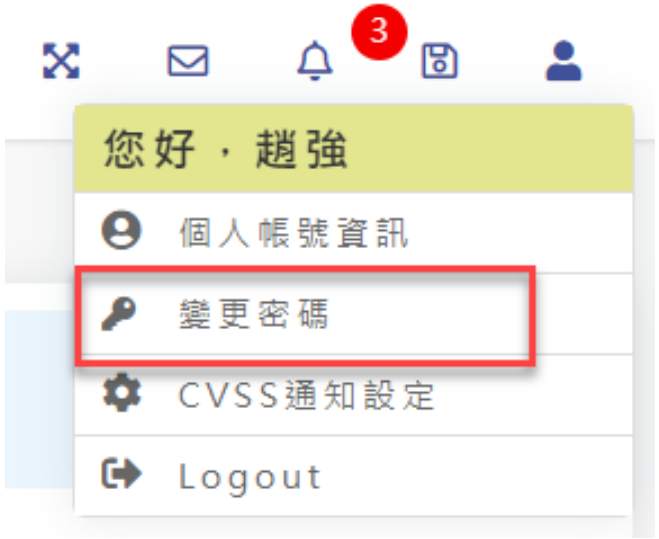
國家資通安全研究院
National Institute of Cyber Security

- 檢視個人帳號資訊
  - ➢使用者進入此功能，可顯示帳號基本資訊，若欲修改資料，可按下「連至iAuth修改」鈕，系統開新視窗連至iAuth系統



個人資訊-變更密碼

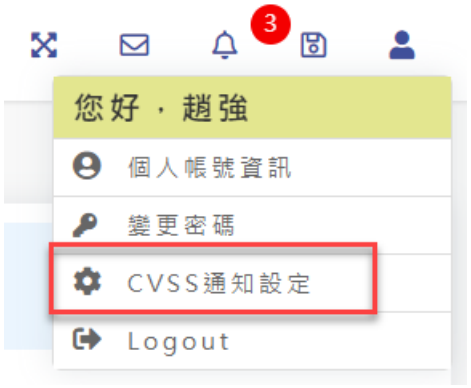
- 變更密碼
  - ➢使用者若欲變更密碼，可按下「變更密碼」，系統開新視窗連至iAuth系統



個人資訊-CVSS通知設定

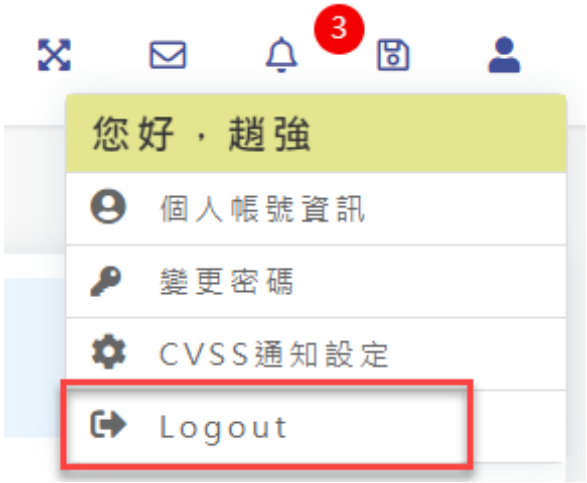
國家資通安全研究院
National Institute of Cyber Security

- CVSS通知設定
  - ➢使用者進入此功能可顯示目前的CVSS通知設定資料，修改資料後，按下「儲存」鈕，即完成資料修改



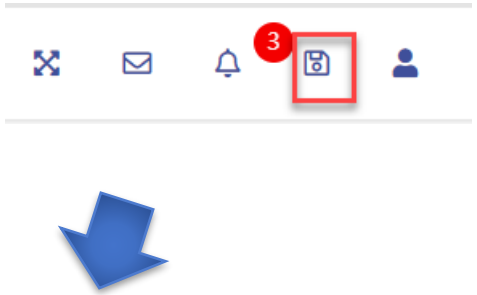
個人資訊-登出

- 登出
  - ➢使用者若欲登出VANS系統，可按下「Logout」，系統會將您登出，導回至登入頁



個人資訊-檔案下載

- 檔案下載
  - ➢使用者進入此功能，可顯示在功能中已匯出的資料，當系統處理完成，會顯示「下載」鈕，點擊後可按將資料下載回本地端電腦



檔案下載列表

共23筆紀錄　10　1/3

項	檔案名稱	建立時間	狀態	動作
	SERVER_EXPORT_20240509152655459.pdf	2024-05-09 15:26:55	已完成	下載
	SERVER_EXPORT_20240325183422119.xls	2024-03-25 18:34:22	已完成	下載
	SERVER_EXPORT_20240320192714775.xlsx	2024-03-20 19:27:14	失敗	
	SERVER_EXPORT_20240320192650099.xls	2024-03-20 19:26:50	失敗	
	SERVER_EXPORT_20240320192629722.xls	2024-03-20 19:26:29	失敗	

個人資訊-通知(1/3)

- CPE異動資產
  - ➢若NVD有更新資產的CPE，使用者登入後會在通知區顯示「CPE-異動資產」，點擊後，系統彈出NVD有異動資產CPE的CPE異動紀錄小視窗，使用者勾選資產後，按「轉換CPE」鈕，可將資產CPE轉換成新的

個人資訊-通知(2/3)

國家資通安全研究院
National Institute of Cyber Security

- 弱點回報(1/2)
  - ➢使用者按下「CVE-XXXX-XXXX弱點回報」，系統導至弱點回報頁

機關名稱	CVE編號	嚴重程度	CVSS
[redacted]	CVE-2023-36792	HIGH	7.80
發佈時間	更新時間		
2023-09-12 17:15:14	2023-09-14 20:21:09		

弱點詳細資訊　　顯示已修補之弱點

請選擇　共3筆紀錄　　10　1/1

資產名稱	資產廠商	資產版本	資產群組	資產CPE
Microsoft Windows Server 2016 Datacenter 8 64 位元	Microsoft Corporation	10.0.14393	行政類資產群組	cpe:2.3:o:microsoft:windows_server_2016:-:-:*:*:datacenter:*:x64:*
Microsoft Windows Server 2016 Standard STANDARD SERVER 64 位元	Microsoft Corporation	10.0.14393.6351	行政類資產群組	cpe:2.3:o:microsoft:windows_server_2016:-:-:*:*:standard:*:x64:*
Microsoft Windows Server 2016 Standard STANDARD SERVER 64 位元	Microsoft Corporation	10.0.14393.6351	行政類資產群組	cpe:2.3:o:microsoft:windows_server_2016:-:-:*:*:standard:*:x64:*

資產編號	資產建立時間	資產更新時間	可修補KBID	已安裝KBID	弱點狀態	動作
400404499520231018100 2	2024-04-17 17:10:43	2024-04-17 17:10:43		0	未填寫改善措施	填寫改善措施 版本更新 安裝KBID修補
400404499520231018100 1	2024-04-16 17:10:43	2024-04-17 17:10:43		0	未填寫改善措施	填寫改善措施 版本更新 安裝KBID修補
100404499520231018101 1	2024-04-03 17:15:58	2024-04-03 17:15:58		0	未填寫改善措施	填寫改善措施 版本更新 安裝KBID修補

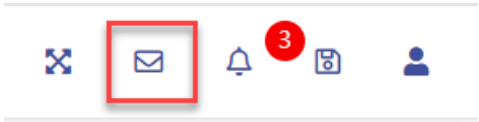
個人資訊-通知(3/3)

- 弱點回報(2/2)
  - ➢使用者可參考「弱點通知與修補作業」章節的作法，對需回報的弱點進行回報作業

個人資訊-訊息

國家資通安全研究院
National Institute of Cyber Security

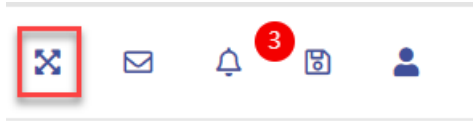
- 查看訊息
  - ➢使用者按下郵件圖示，系統彈出系統寄給使用者通知訊息列表小視窗



個人資訊-全螢幕

國家資通安全研究院
National Institute of Cyber Security

- 查看訊息
  - ➢使用者按下全螢幕圖示，系統會將網頁以全螢幕顯示，按下ESC鍵可回復原來的顯示模式



資訊綜整儀表板(1/13)

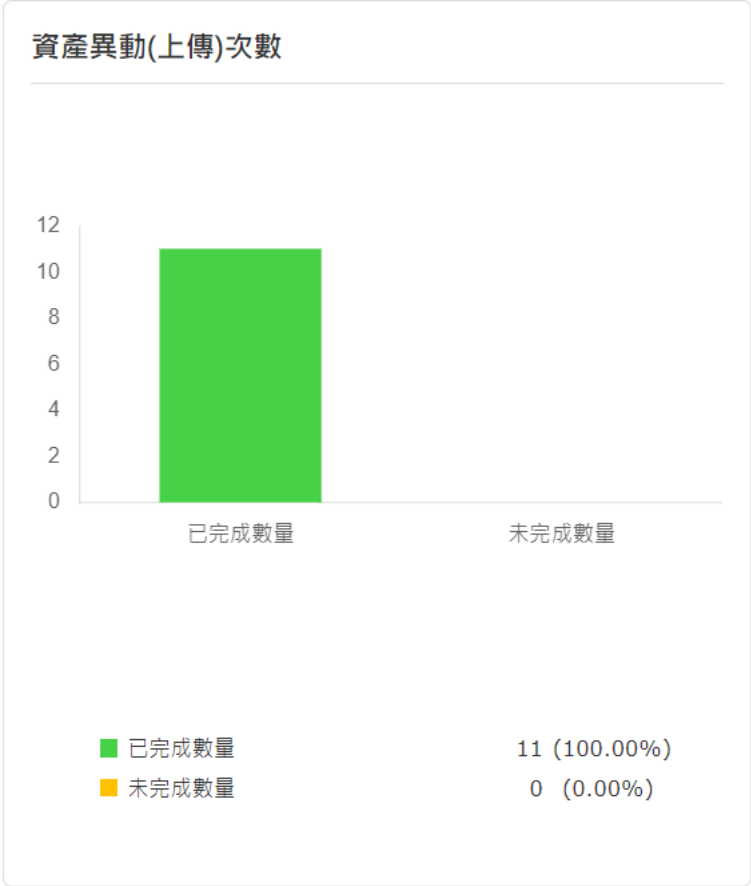
國家資通安全研究院
National Institute of Cyber Security

- 提供機關資產盤點與弱點修補之關鍵資訊
- 查詢結果，可依照全部、資通系統、使用者電腦及工業控制系統，分別顯示各統計圖表
  - 資產類統計圖表
    - 資產異動(上傳)次數、資產數量、CPE資產數量、受影響資產數量
  - 弱點類統計圖表
    - 資產弱點數量、資產CPE種類弱點數量、修補弱點數量、當年度資產弱點與修補累積情形、資產弱點嚴重等級分布情形
  - TOP10類統計圖表
    - 資產數量排名TOP10、資產弱點排名TOP10、資產弱點修補排名TOP10

資訊綜整儀表板(2/13)

國家資通安全研究院
National Institute of Cyber Security

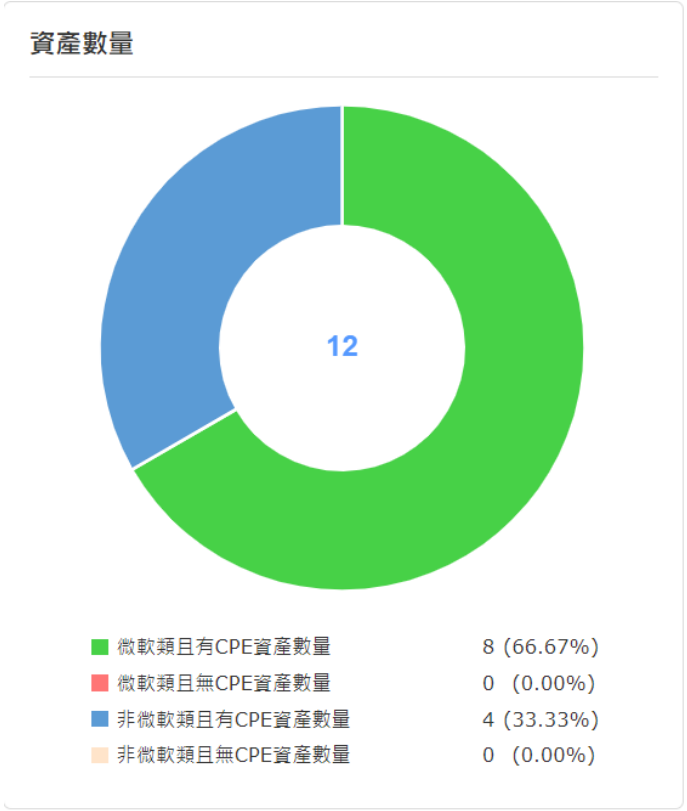
- 資產類統計圖表-資產異動(上傳)次數
  - 顯示已完成與未完成資產異動(上傳)次數與百分比



資訊綜整儀表板(3/13)

國家資通安全研究院
National Institute of Cyber Security

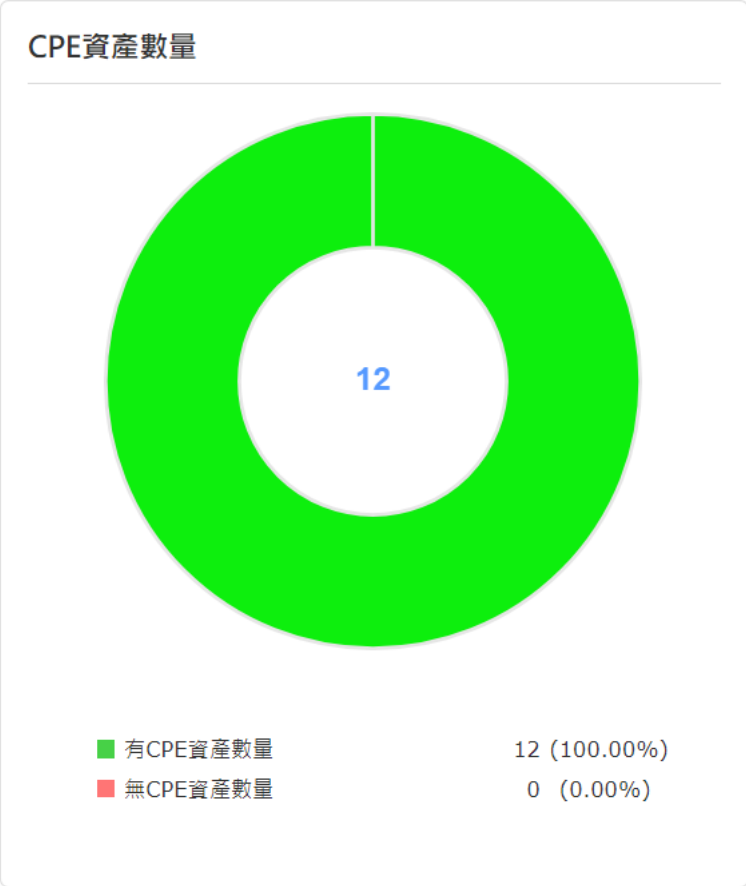
- 資產類統計圖表-資產數量
  - 顯示微軟類且有CPE/微軟類且無CPE資產數量與百分比
  - 顯示非微軟類且有CPE/非微軟類且無CPE資產數量與百分比



資訊綜整儀表板(4/13)

國家資通安全研究院
National Institute of Cyber Security

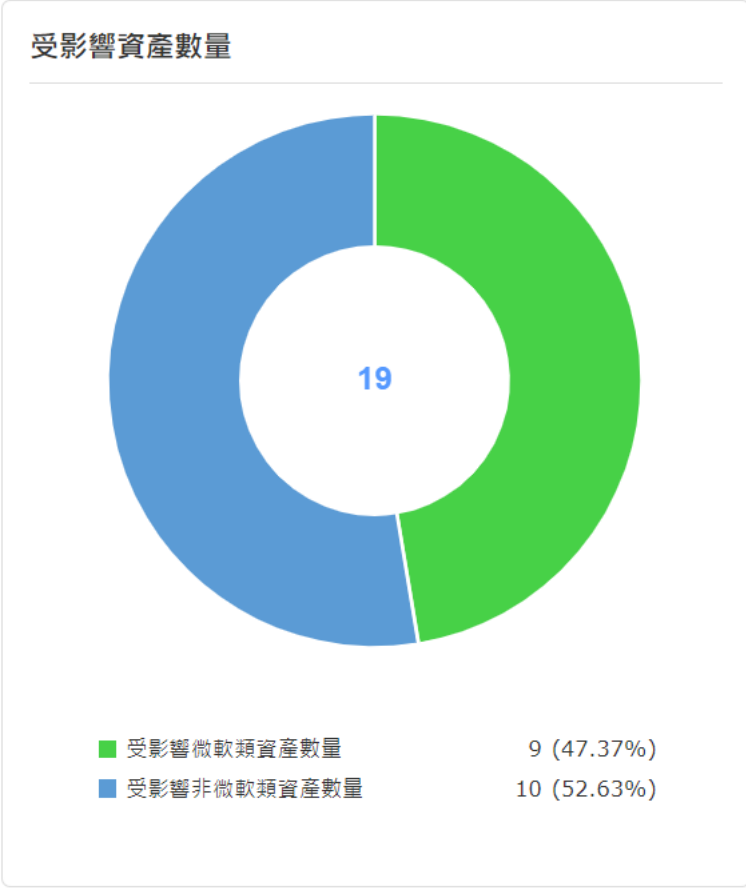
- 資產類統計圖表-CPE資產數量
  - 顯示有CPE資產數量與百分比
  - 顯示無CPE資產數量與百分比



資訊綜整儀表板(5/13)

國家資通安全研究院
National Institute of Cyber Security

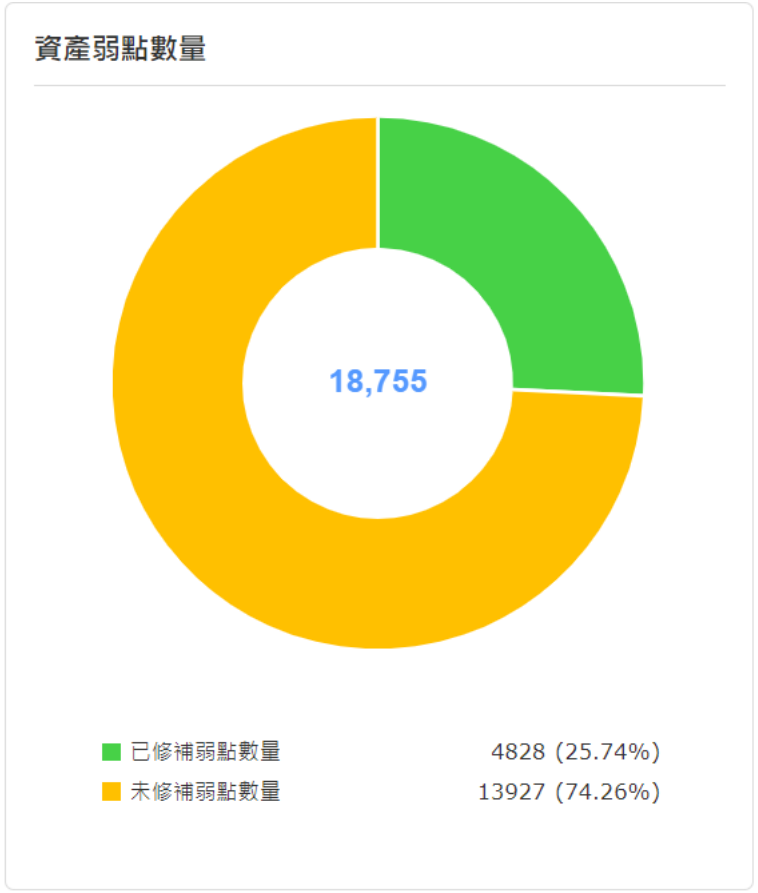
- 資產類統計圖表-受影響資產數量
  - 顯示受影響微軟類資產數量與百分比
  - 顯示受影響非微軟類資產數量與百分比



資訊綜整儀表板(6/13)

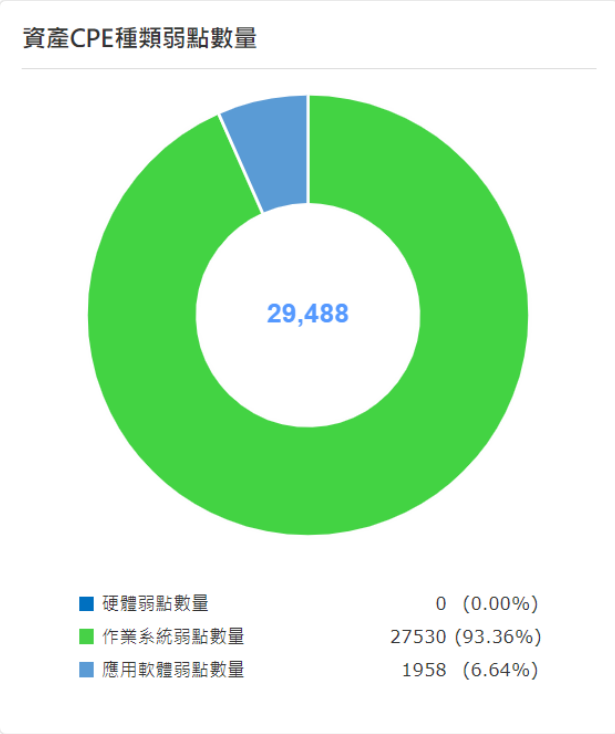
國家資通安全研究院
National Institute of Cyber Security

- 弱點類統計圖表-資產弱點數量
  - 顯示已修補弱點數量與百分比
  - 顯示未修補弱點數量與百分比



資訊綜整儀表板(7/13)

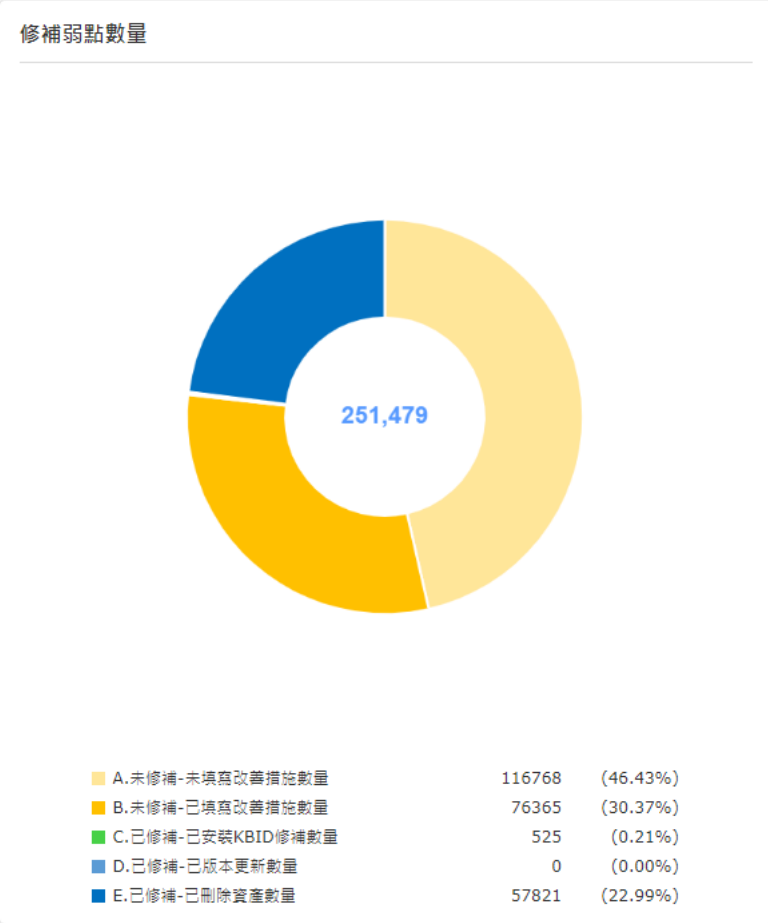
- 弱點類統計圖表-資產CPE種類弱點數量
  - 顯示硬體弱點數量與百分比
  - 顯示作業系統弱點數量與百分比
  - 顯示應用軟體弱點數量與百分比



資訊綜整儀表板(8/13)

國家資通安全研究院
National Institute of Cyber Security

- 弱點類統計圖表-修補弱點數量

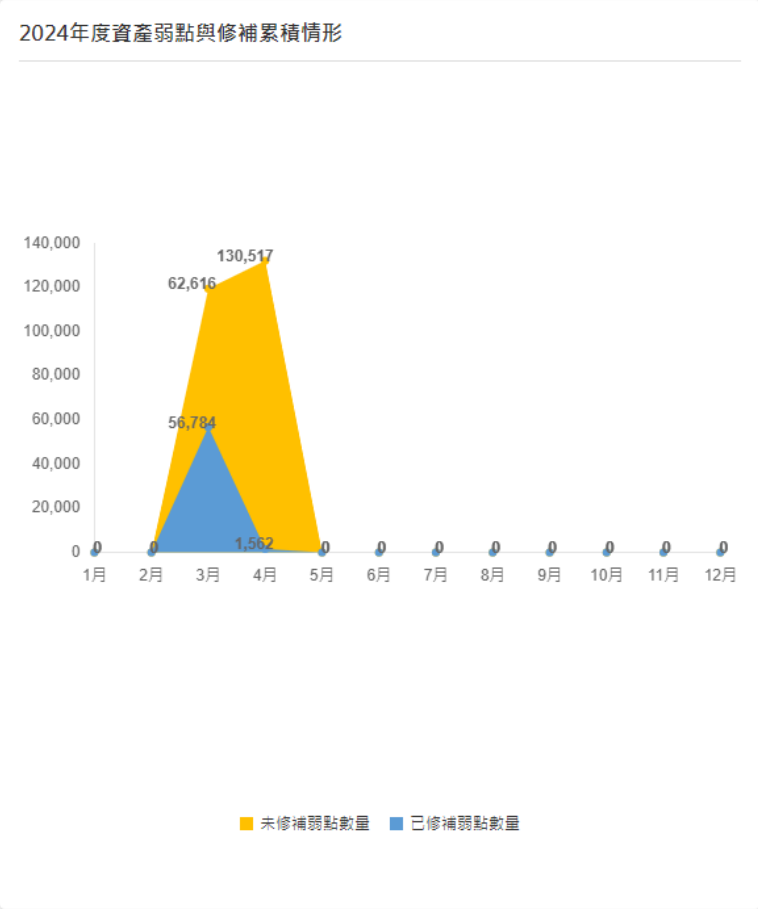


- A.未處置-未填寫改善措施數量與百分比
- B.已處置-已填寫改善措施數量與百分比
- C.已處置-已安裝KBID修補數量與百分比
- D.已處置-已版本更新數量與百分比
- E.已處置-已刪除資產數量與百分比

資訊綜整儀表板(9/13)

國家資通安全研究院
National Institute of Cyber Security

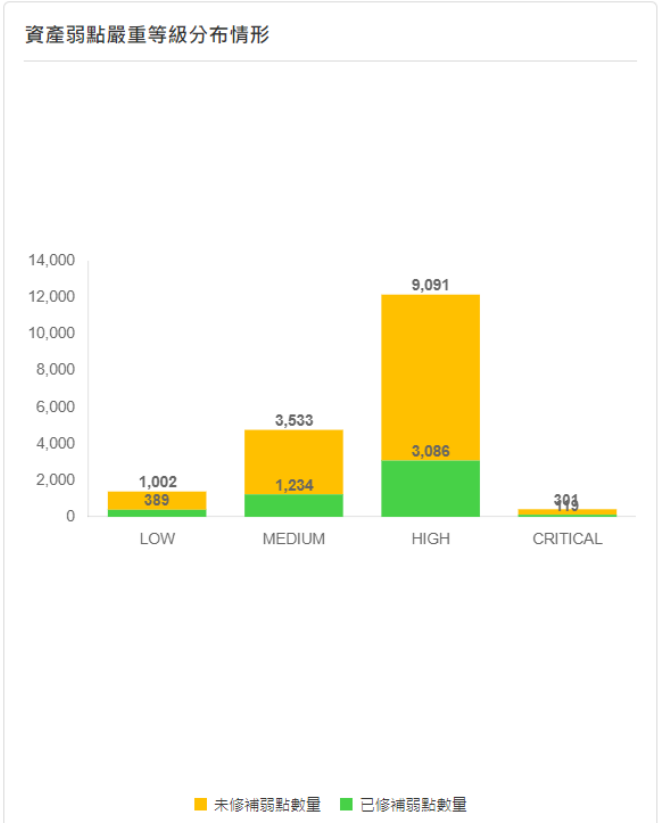
- 弱點類統計圖表-當年度資產弱點與累積修補情形
  - 當年度各月份未修補弱點數量與百分比
  - 當年度各月份已修補弱點數量與百分比



資訊綜整儀表板(10/13)

國家資通安全研究院
National Institute of Cyber Security

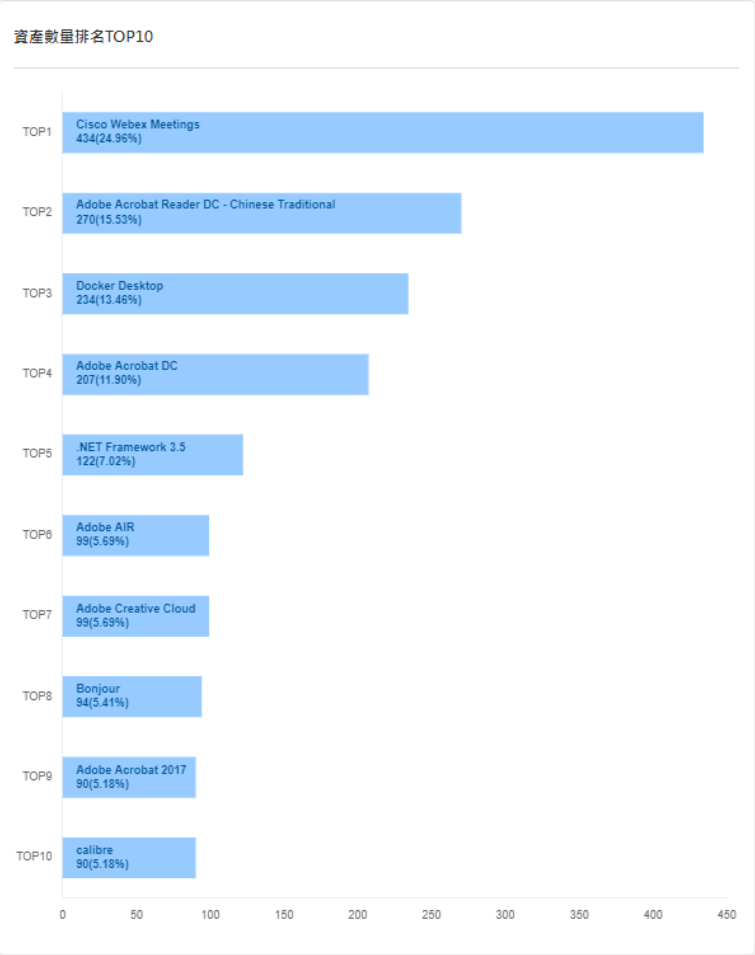
- 弱點類統計圖表-資產弱點嚴重分布情形
  - 各嚴重等級之未修補弱點數量與百分比
  - 各嚴重等級之已修補弱點數量與百分比



資訊綜整儀表板(11/13)

國家資通安全研究院
National Institute of Cyber Security

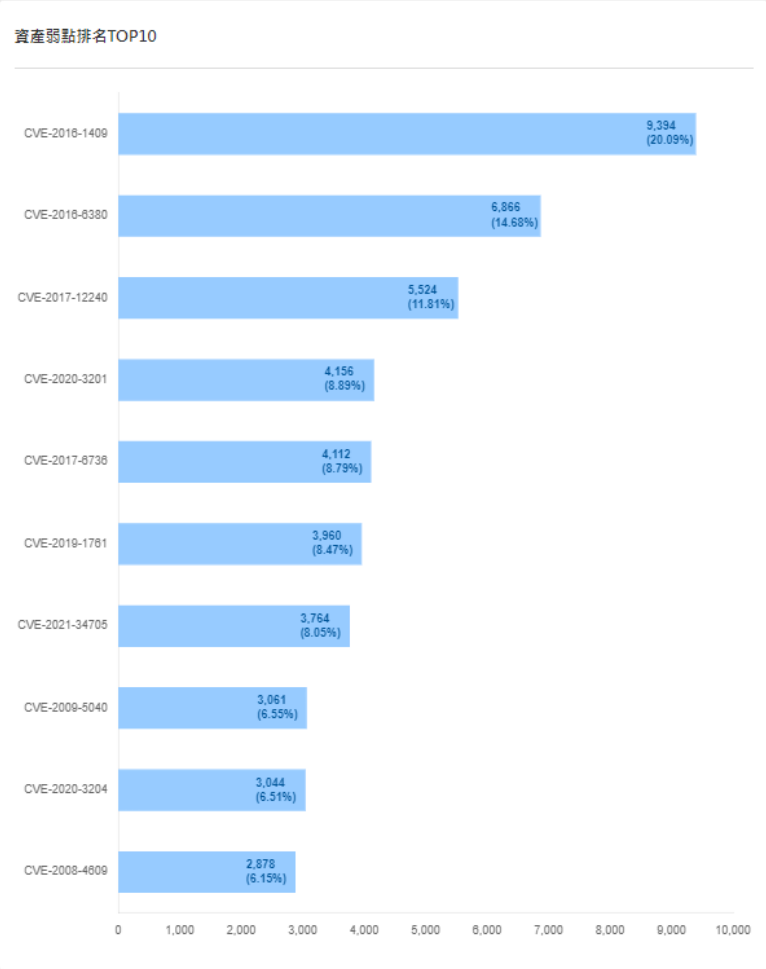
- TOP10類統計圖表-資產數量排名TOP10
  - 資產數量排名前10名之資產列表、資產數量及資產數量百分比



資訊綜整儀表板(12/13)

國家資通安全研究院
National Institute of Cyber Security

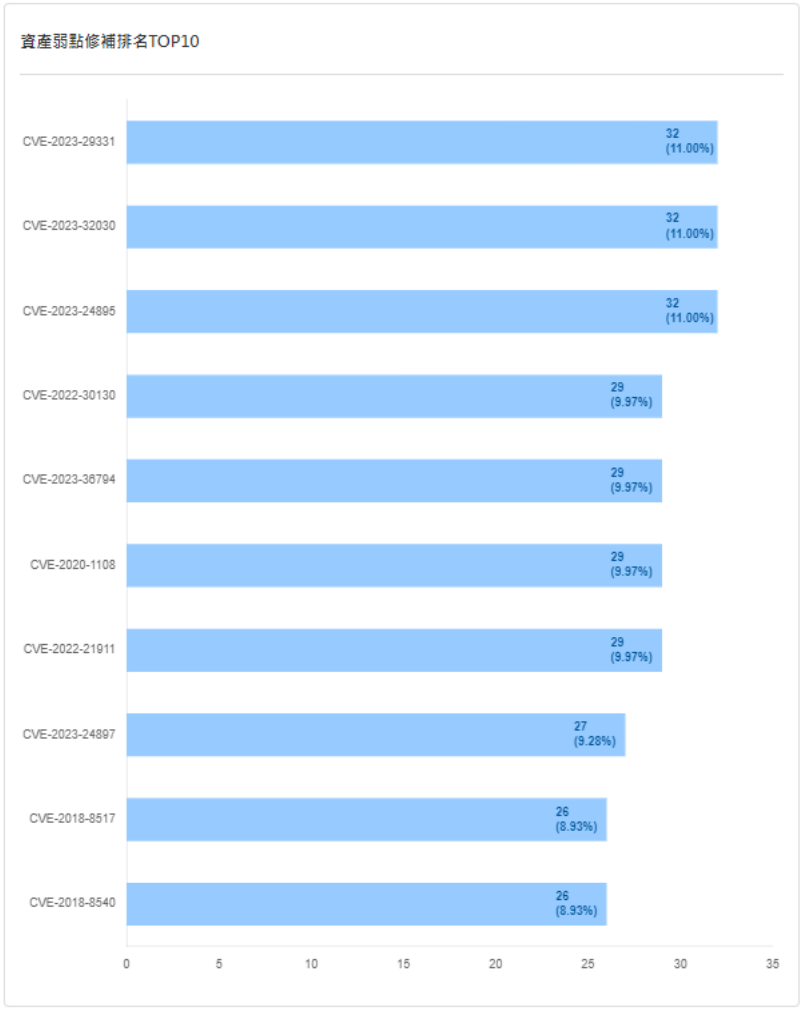
- TOP10類統計圖表-資產弱點排名TOP10
  - 弱點數量排名前10名之弱點列表、弱點數量及弱點數量百分比



資訊綜整儀表板(13/13)

國家資通安全研究院
National Institute of Cyber Security

- TOP10類統計圖表-資產弱點修補排名TOP10
  - 弱點修補數量排名前10名之弱點列表、弱點數量及弱點數量百分比



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

參考資料(2/2)

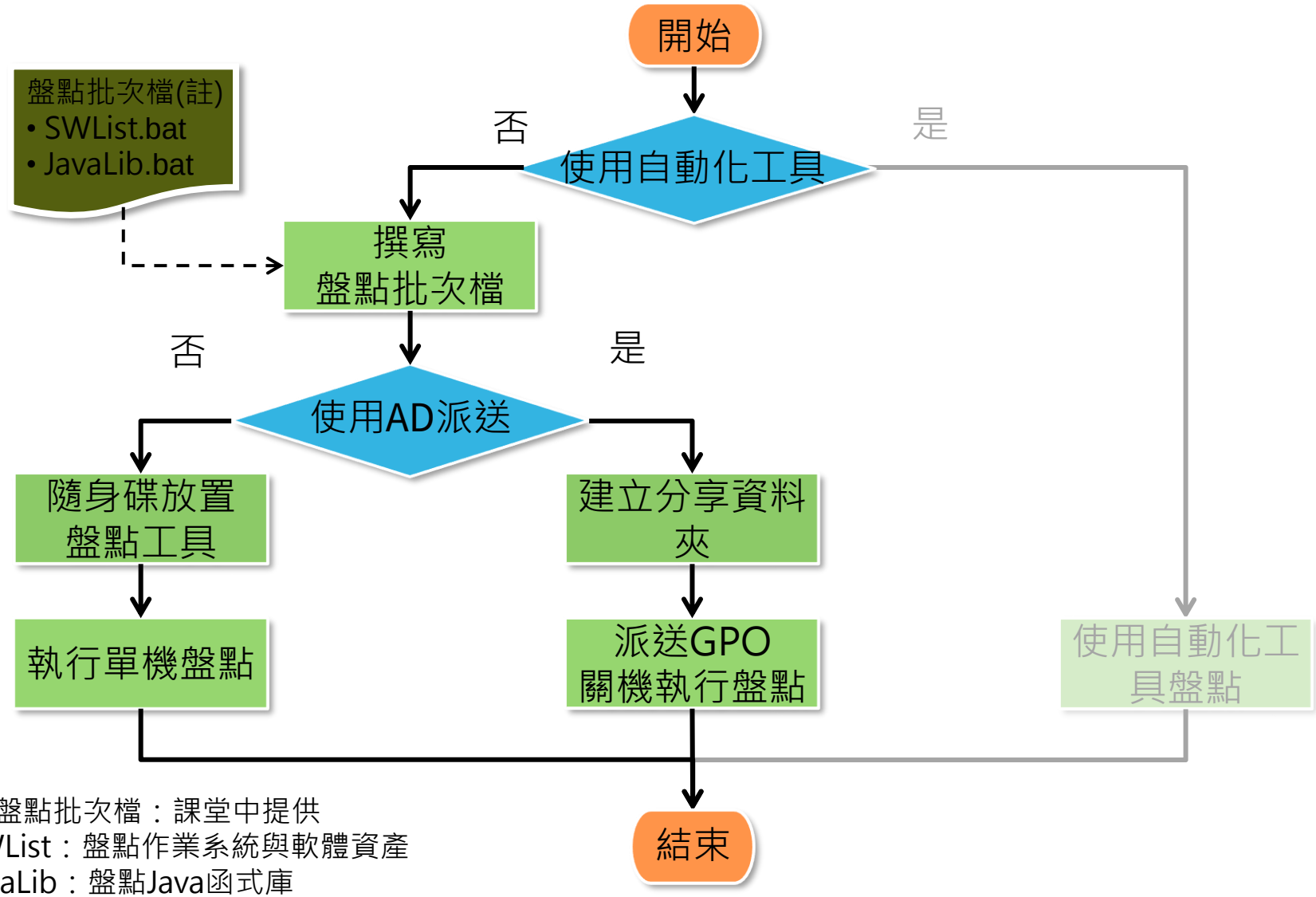
- 用來描述 Microsoft 軟體更新標準術語的說明
  - https://support.microsoft.com/zh-tw/help/824684/description-of-the-standard-terminology-that-is-used-to-describe-micro
- Microsoft Power Query for Excel
  - https://www.microsoft.com/zh-TW/download/details.aspx?id=39379
- 關於 Excel 中的 Power Query
  - https://support.office.com/zh-tw/article/Power-Query-%E5%BF%AB%E9%80%9F%E5%85%A5%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

附件1
手動盤點與正規化作業流程

導入作業流程

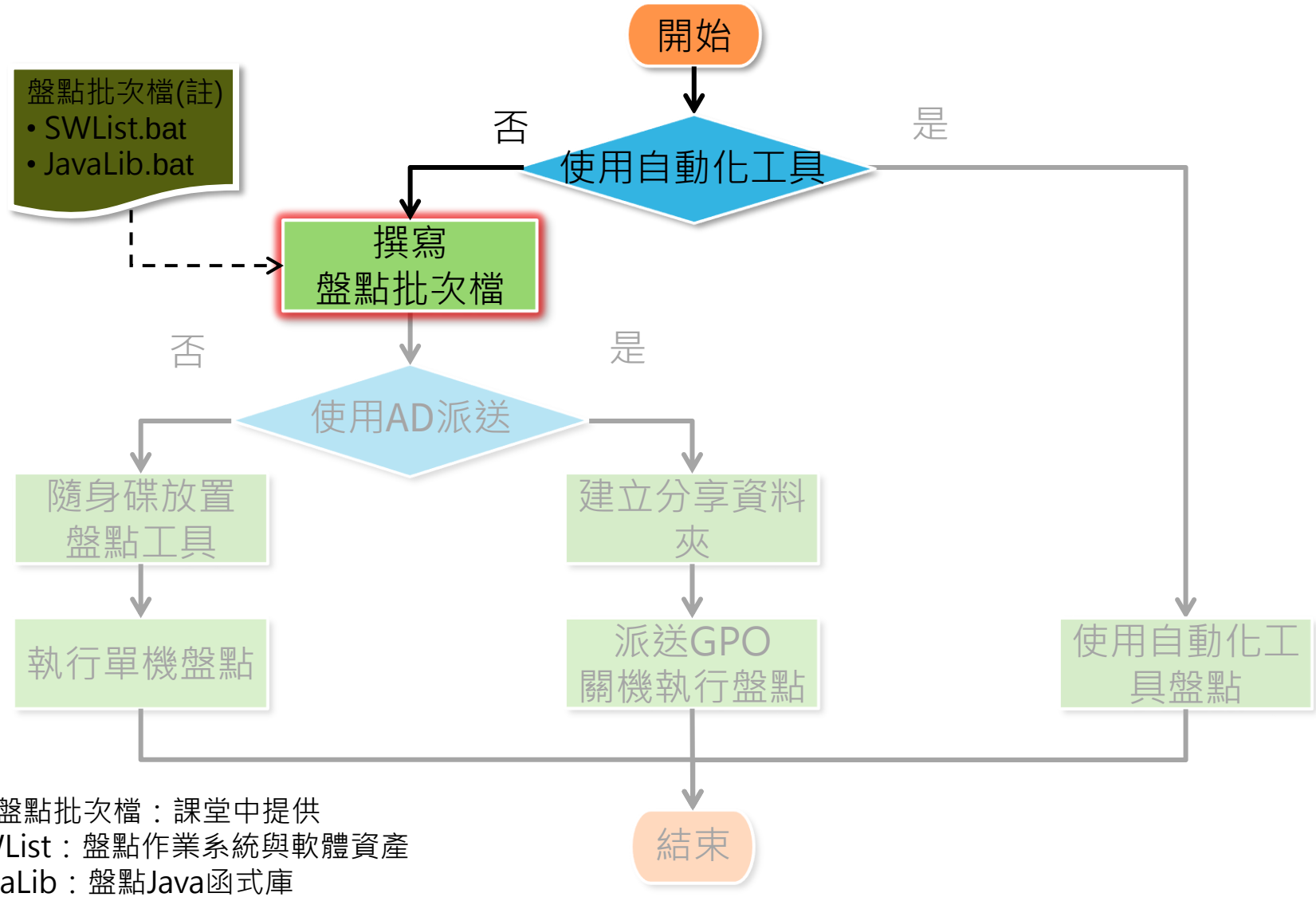
國家資通安全研究院
National Institute of Cyber Security

盤點作業流程



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

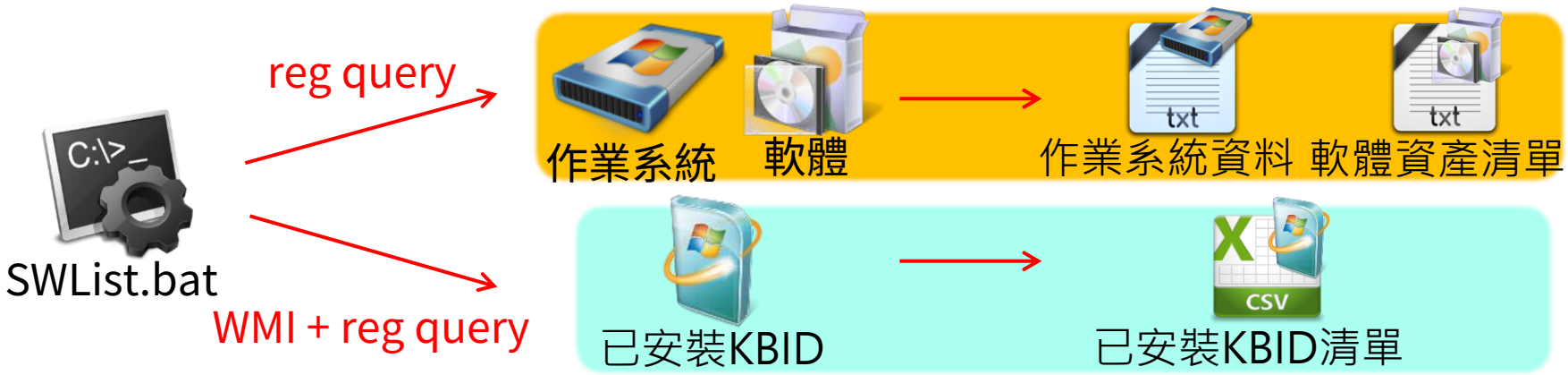
盤點作業流程



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

撰寫盤點批次檔(1/2)

- 登錄機碼值(reg query)
  - 藉由查詢登錄機碼值，可列出作業系統資訊、已安裝軟體清單及Office相關產品之已安裝KBID
- Windows管理工具(簡稱WMI)
  - 運用Windows平台作業系統進行檔案管理與操作之技術，讓使用者可透過WMI管理本機與遠端電腦，可用以盤點已安裝KBID



撰寫盤點批次檔(2/2)

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

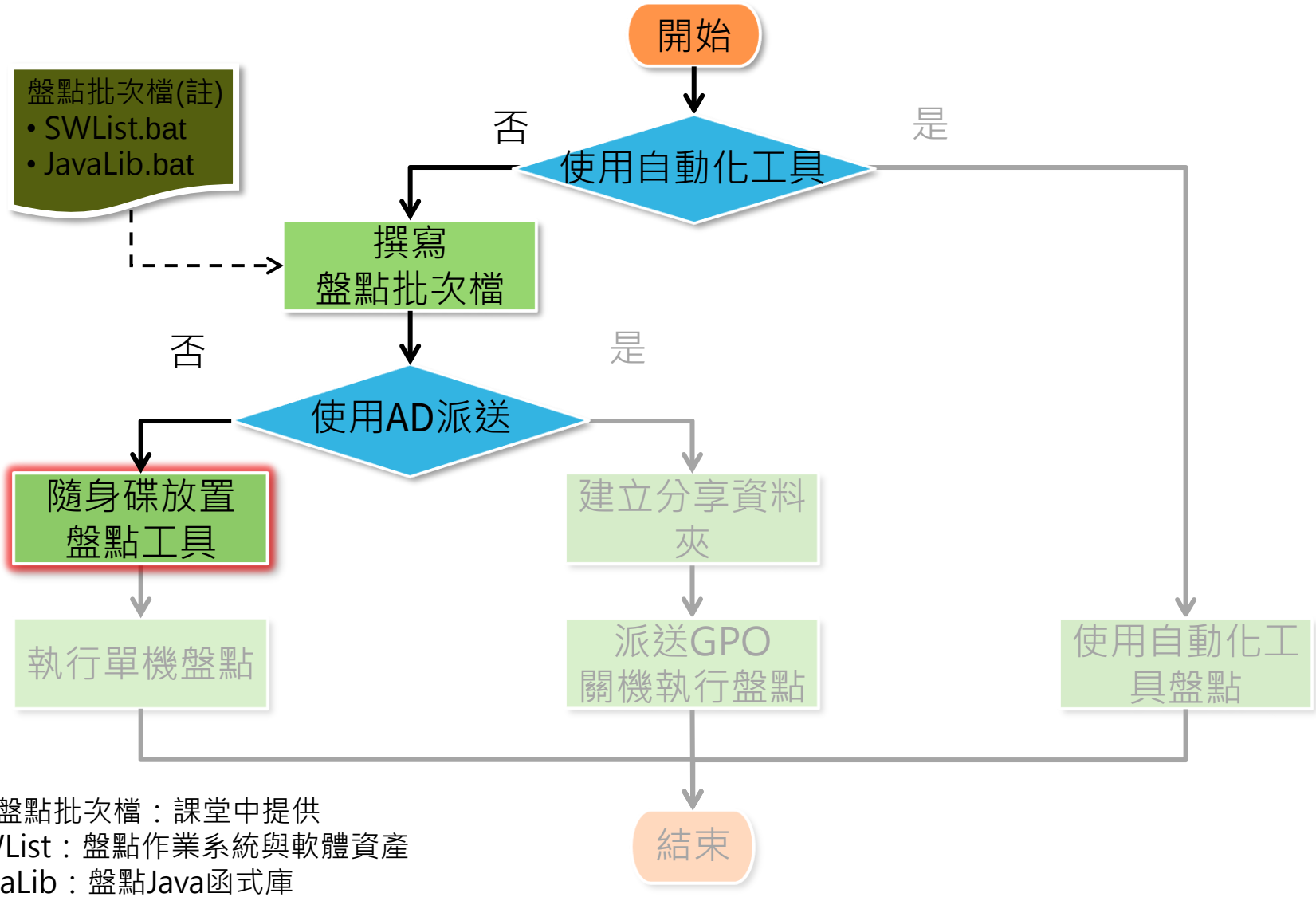
JavaLib_v1.0.bat

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

透過系統指令單機盤點

盤點作業流程

國家資通安全研究院
National Institute of Cyber Security

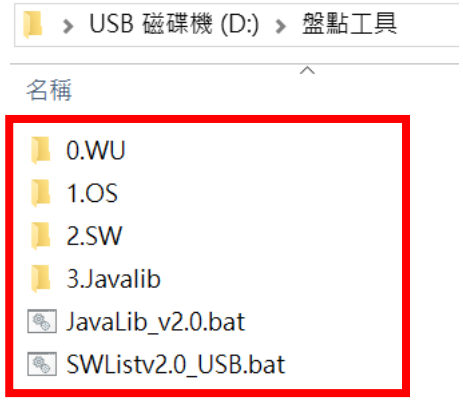


註：盤點批次檔：課堂中提供
1.SWList：盤點作業系統與軟體資產
2.JavaLib：盤點Java函式庫

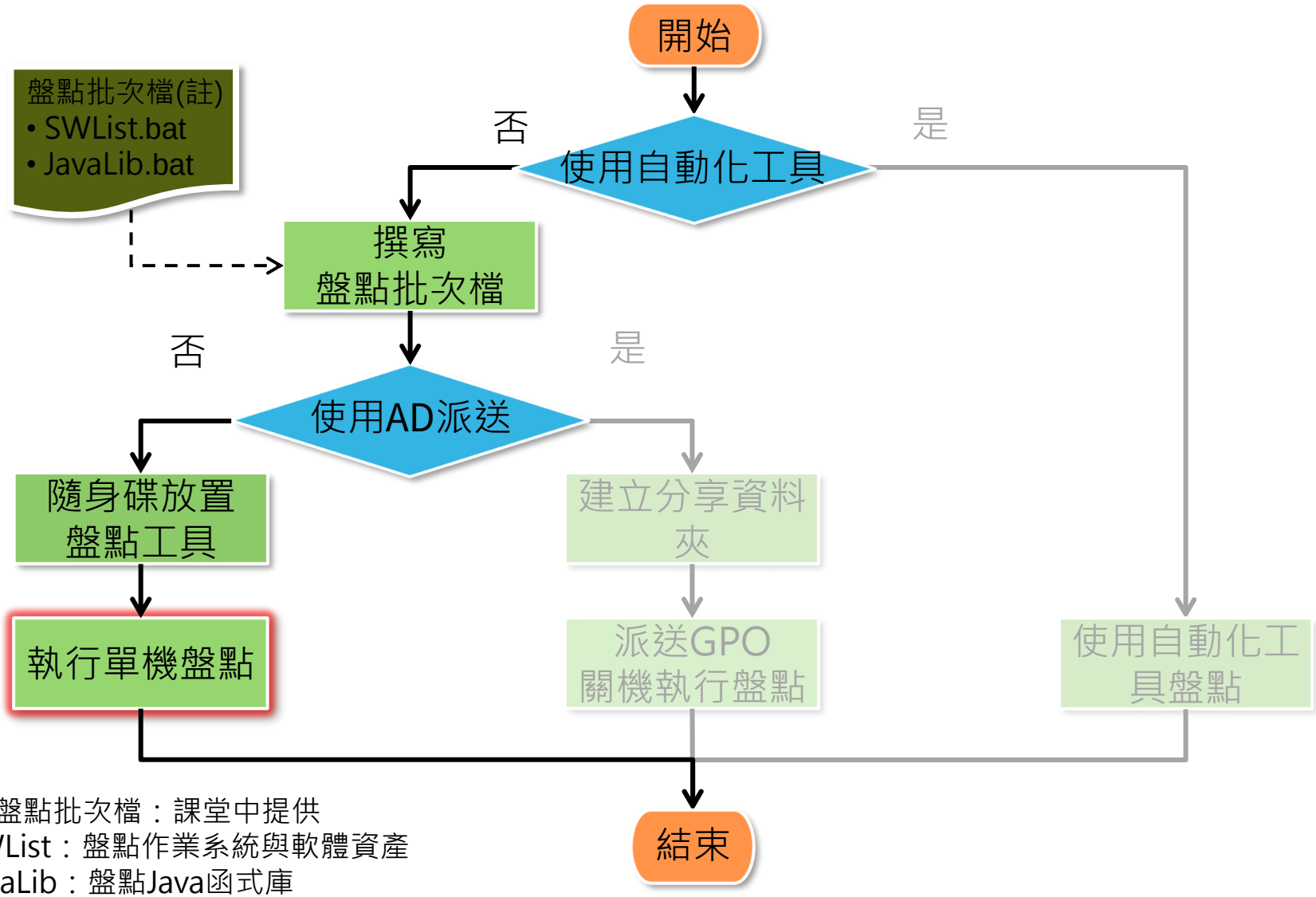
隨身碟放置盤點工具

國家資通安全研究院
National Institute of Cyber Security

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



盤點作業流程

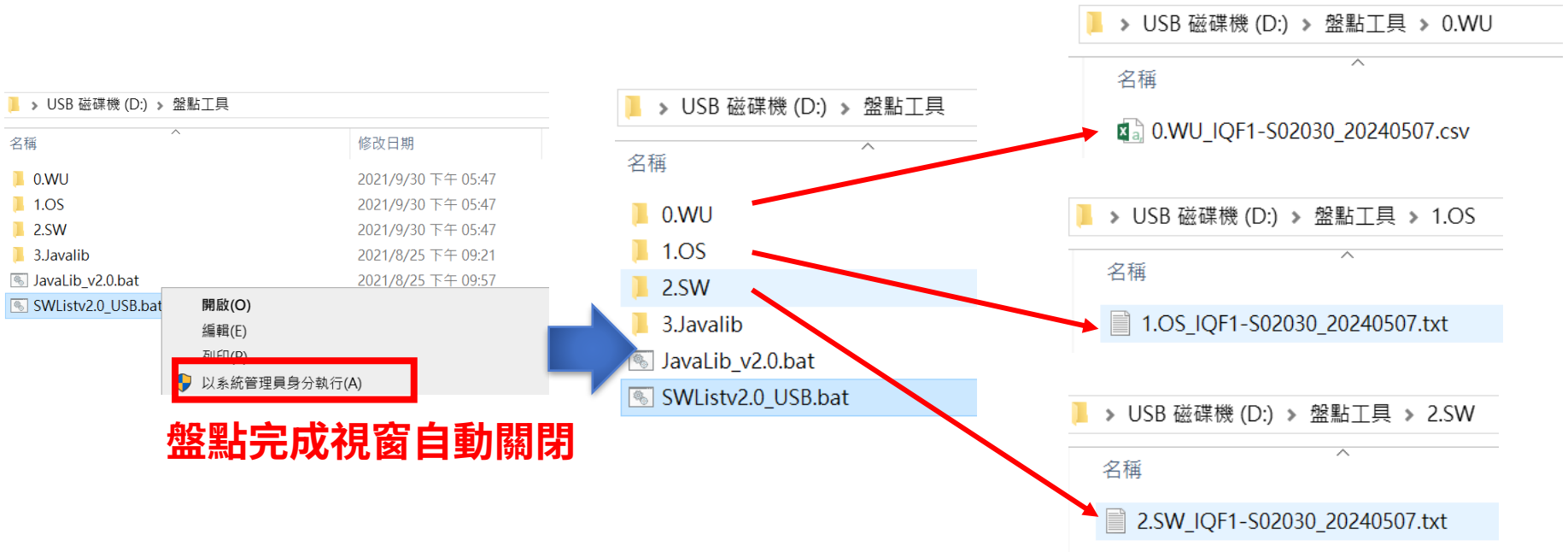


註：盤點批次檔：課堂中提供
1.SWList：盤點作業系統與軟體資產
2.JavaLib：盤點Java函式庫

執行單機盤點(1/2)

國家資通安全研究院
National Institute of Cyber Security

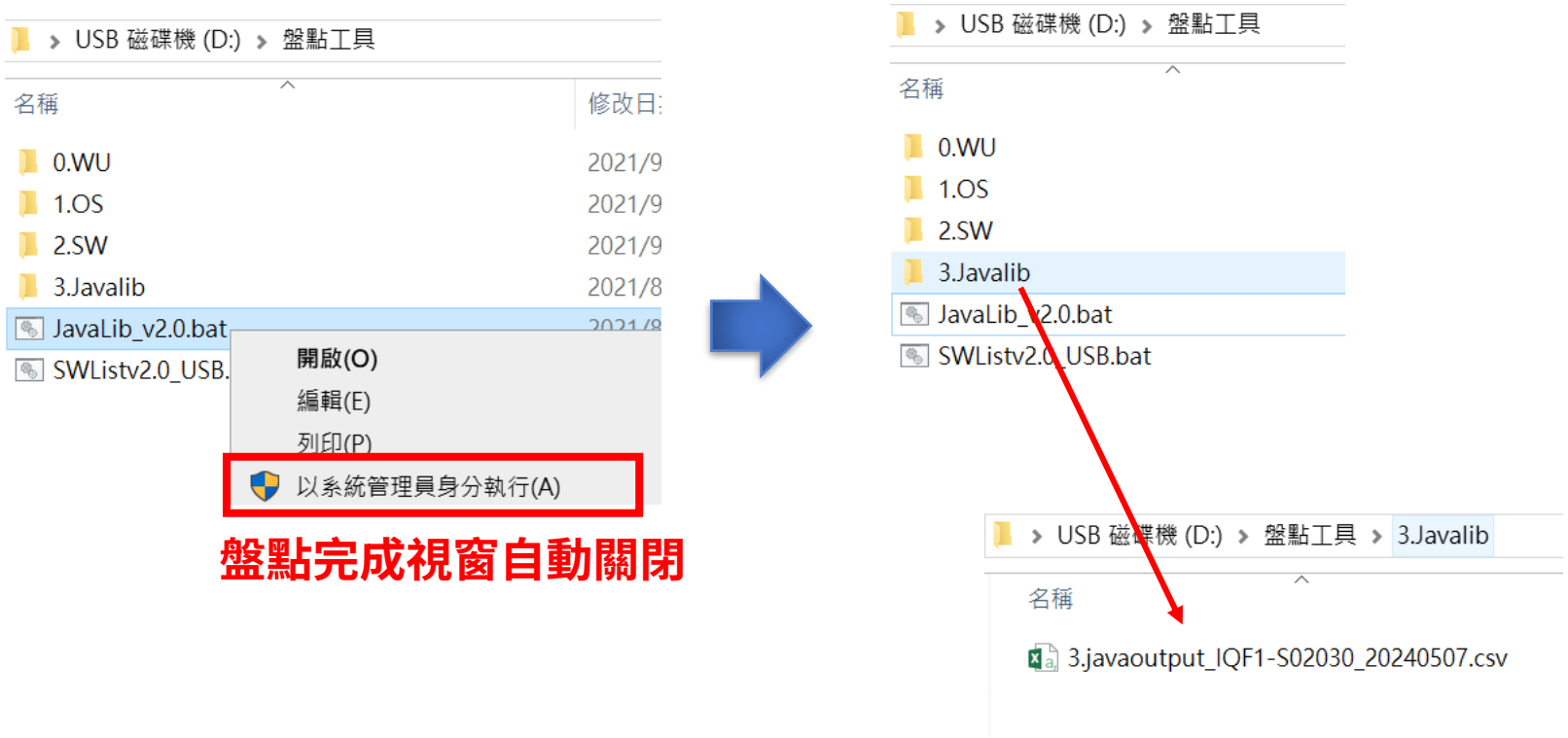
- STEP1：以系統管理員身分執行SWList批次檔
- STEP2：檢視盤點結果資料夾，分別為已安裝KBID清單、作業系統資訊及軟體盤點清單



執行單機盤點(2/2)

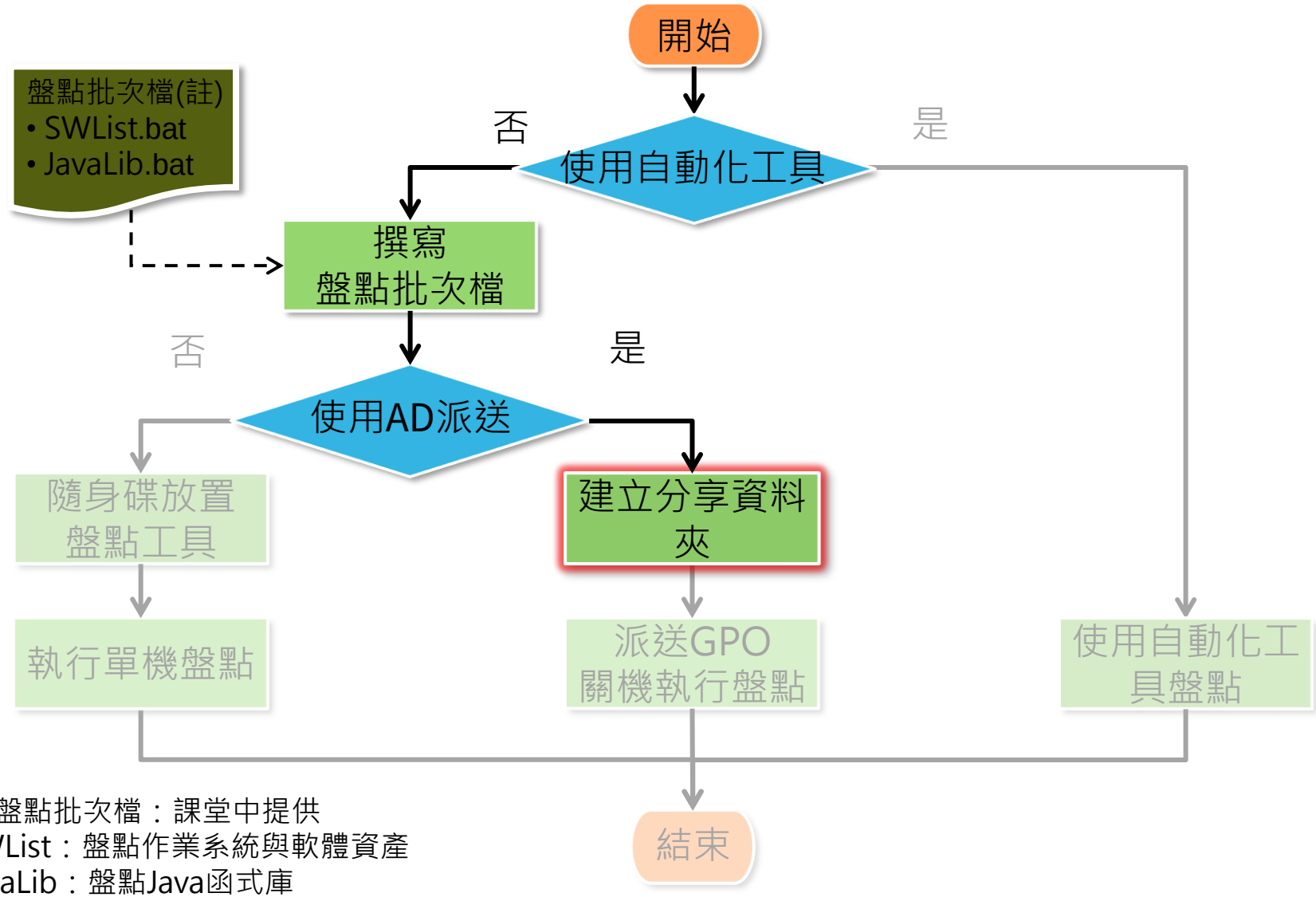
國家資通安全研究院
National Institute of Cyber Security

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



透過系統指令批次盤點

盤點作業流程



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

AD主機建立分享資料夾(1/3)

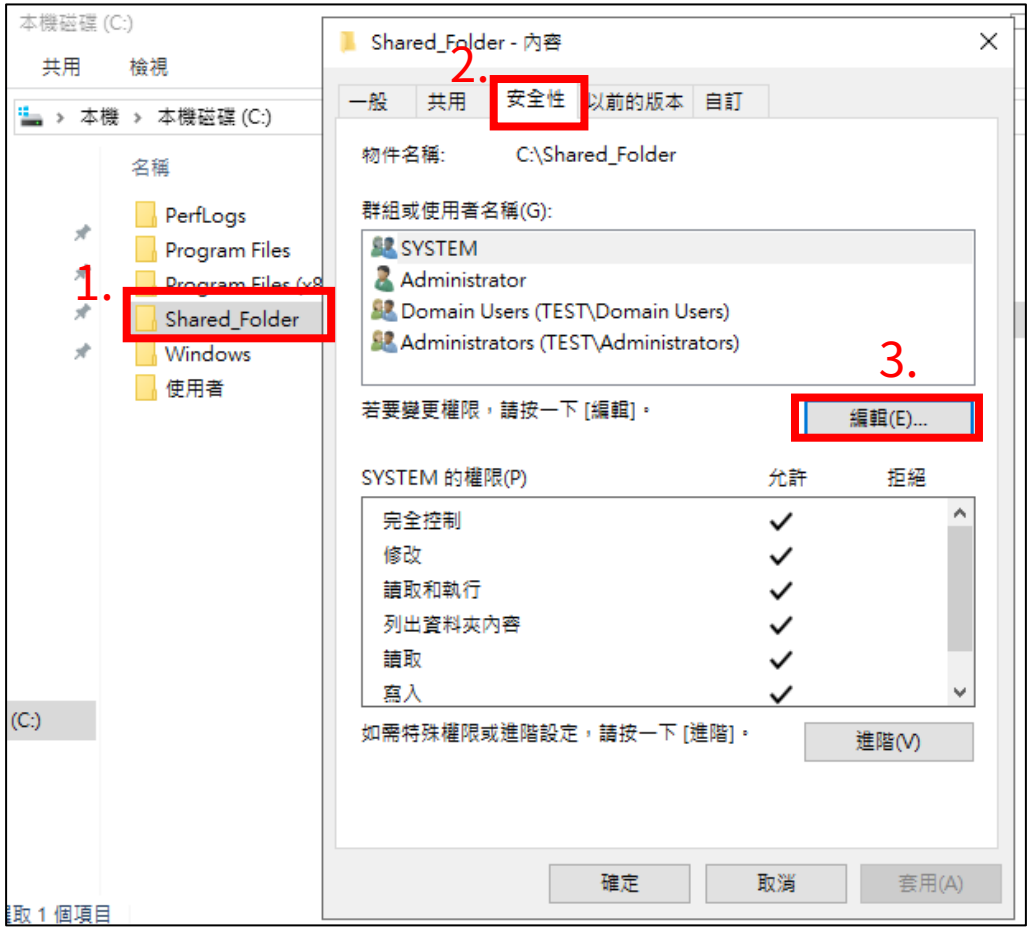
國家資通安全研究院
National Institute of Cyber Security

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

AD主機建立分享資料夾(2/3)

國家資通安全研究院
National Institute of Cyber Security

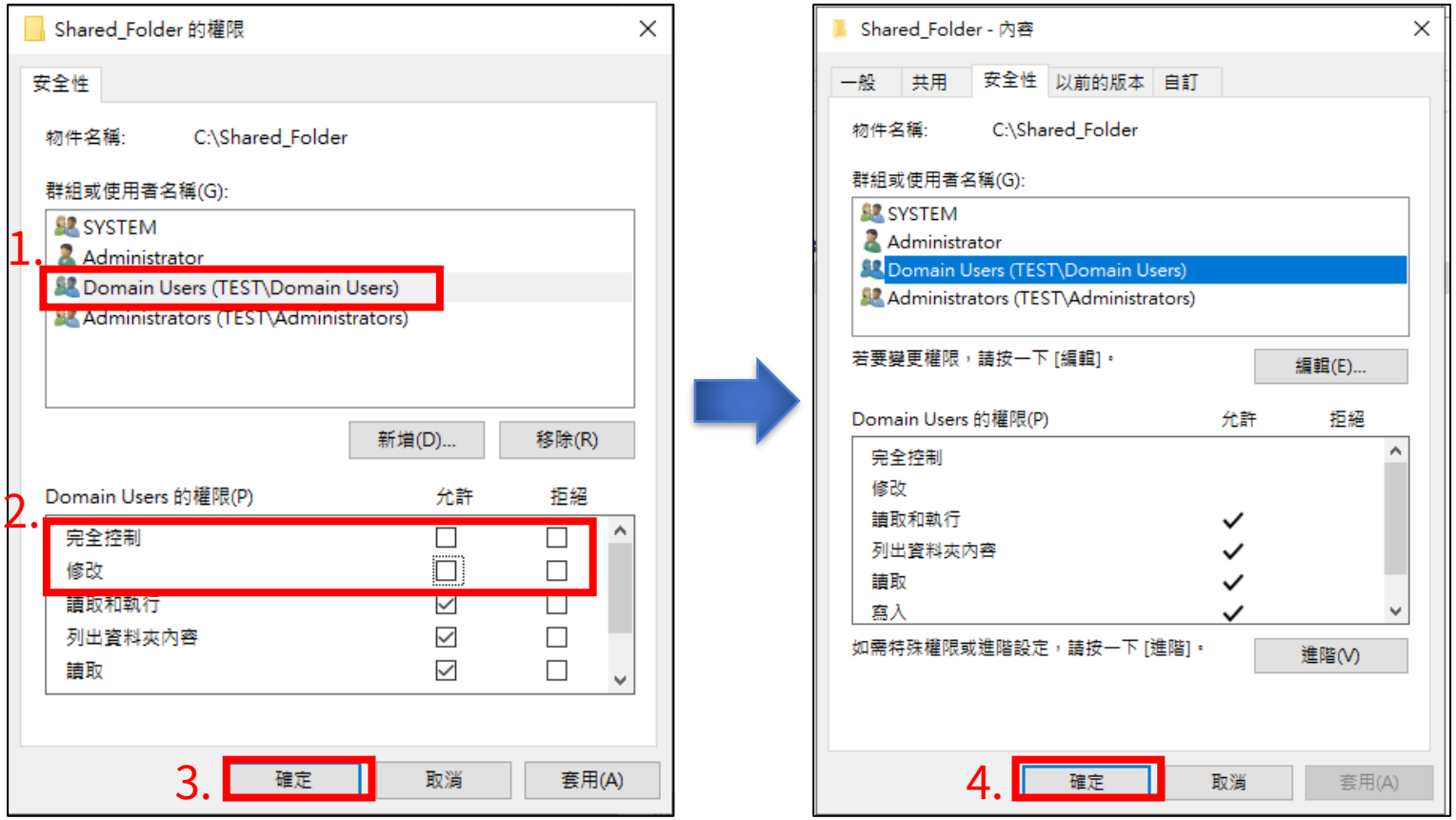
- STEP3：避免網域使用者誤刪檔案，需限縮其存取權限，切換至安全性頁籤，並點選編輯



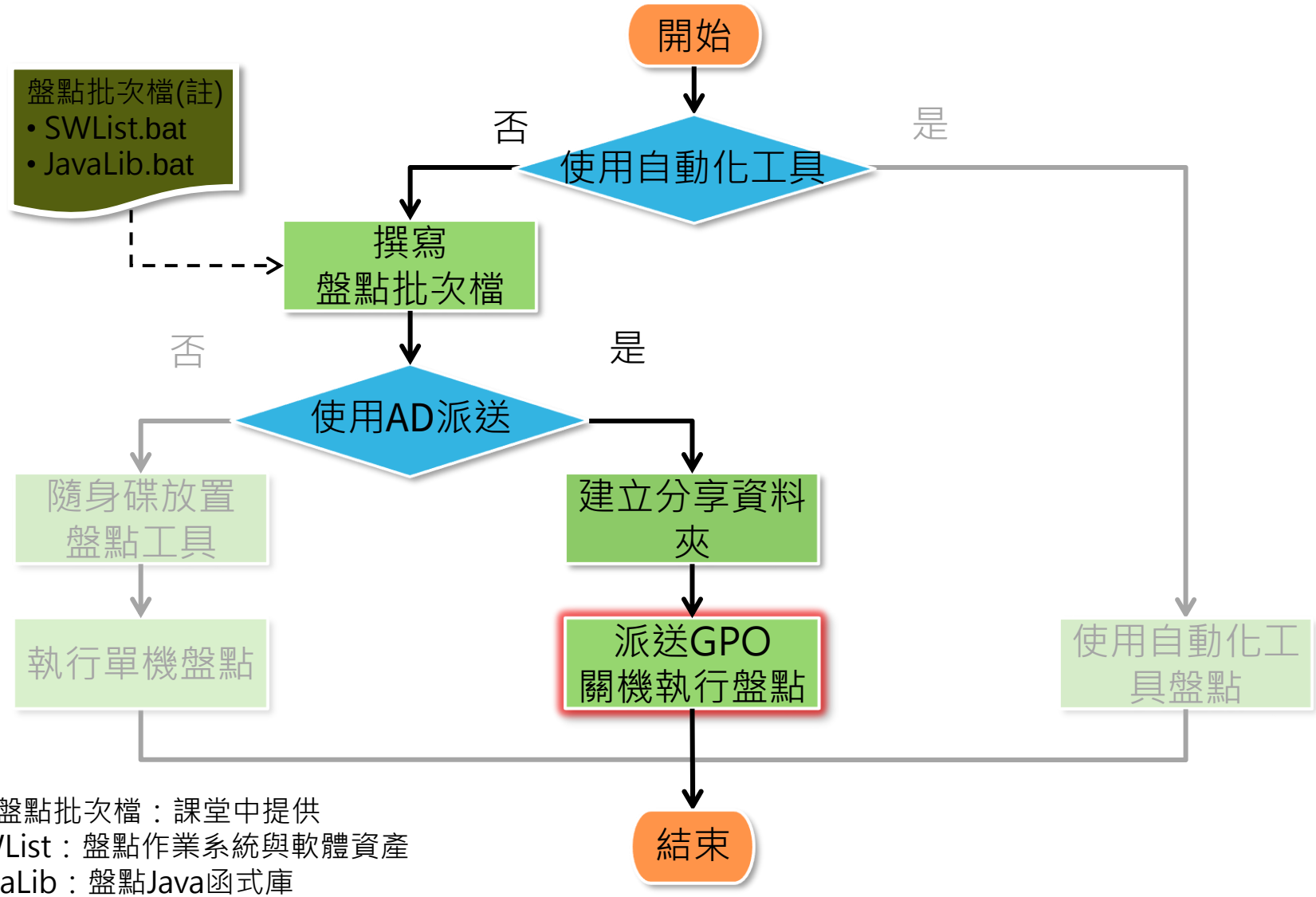
AD主機建立分享資料夾(3/3)

國家資通安全研究院
National Institute of Cyber Security

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



盤點作業流程



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

派送GPO-關機執行(1/5)

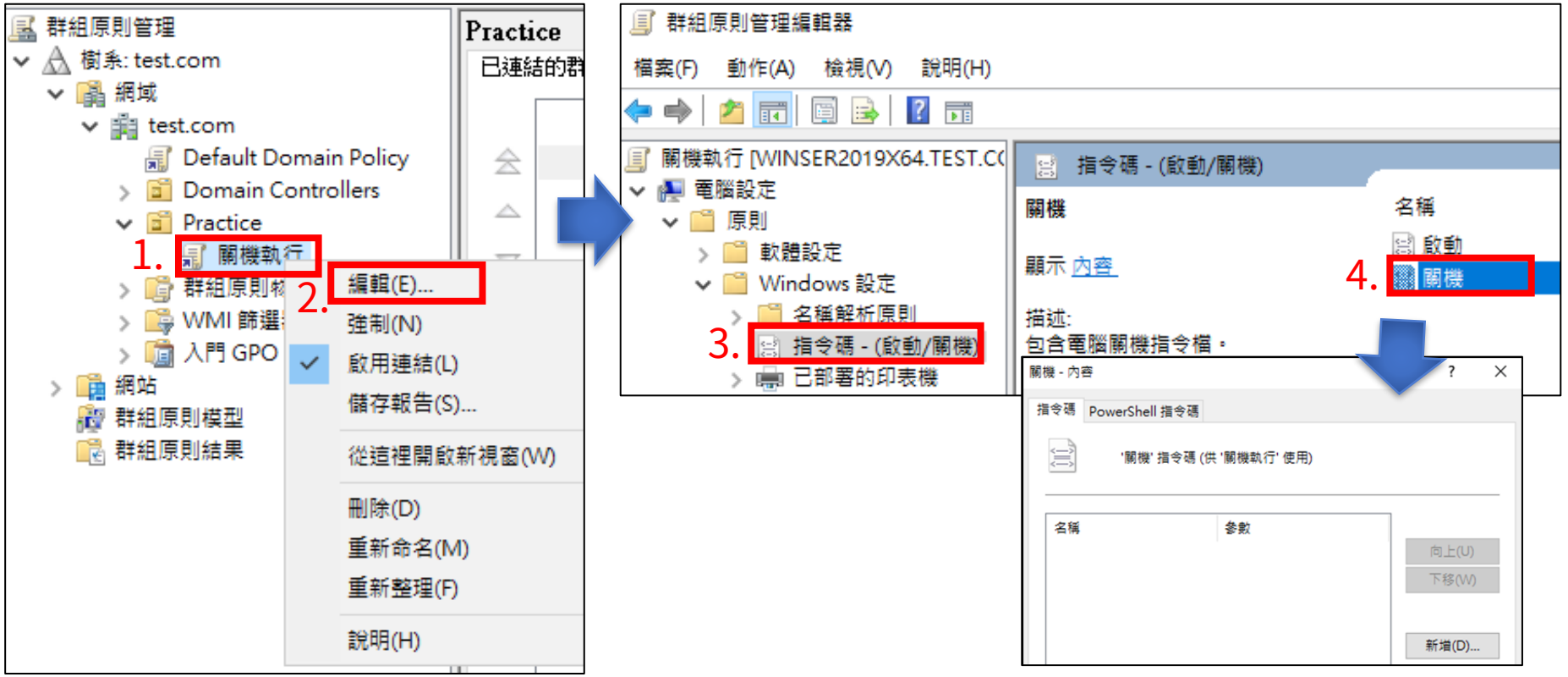
國家資通安全研究院
National Institute of Cyber Security

- 在目標OU點選右鍵並建立GPO
  - 新增「關機執行」GPO

派送GPO-關機執行(2/5)

國家資通安全研究院
National Institute of Cyber Security

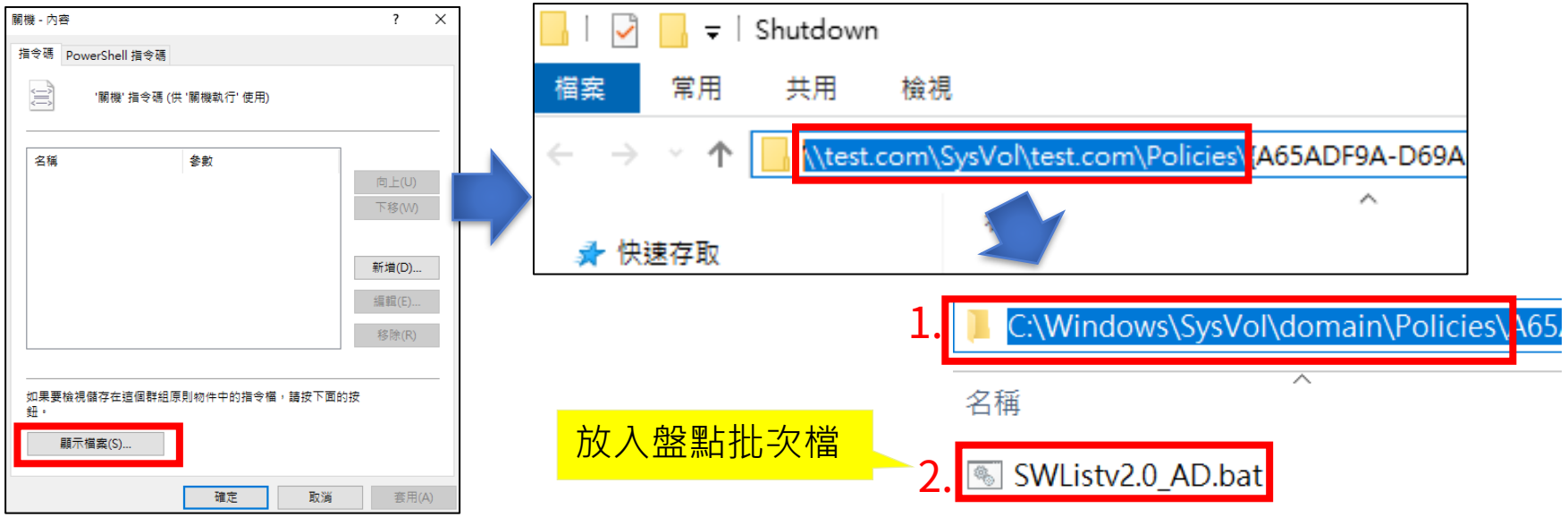
- 編輯GPO，於電腦關機時執行檢測批次檔
  - 點選剛建立的「關機執行」GPO，按右鍵選擇編輯
  - 路徑為：電腦設定\原則\Windows設定\指令碼 - (啟動/關機)\關機
  - 點擊「關機」並編輯「關機-內容」



派送GPO-關機執行(3/5)

國家資通安全研究院
National Institute of Cyber Security

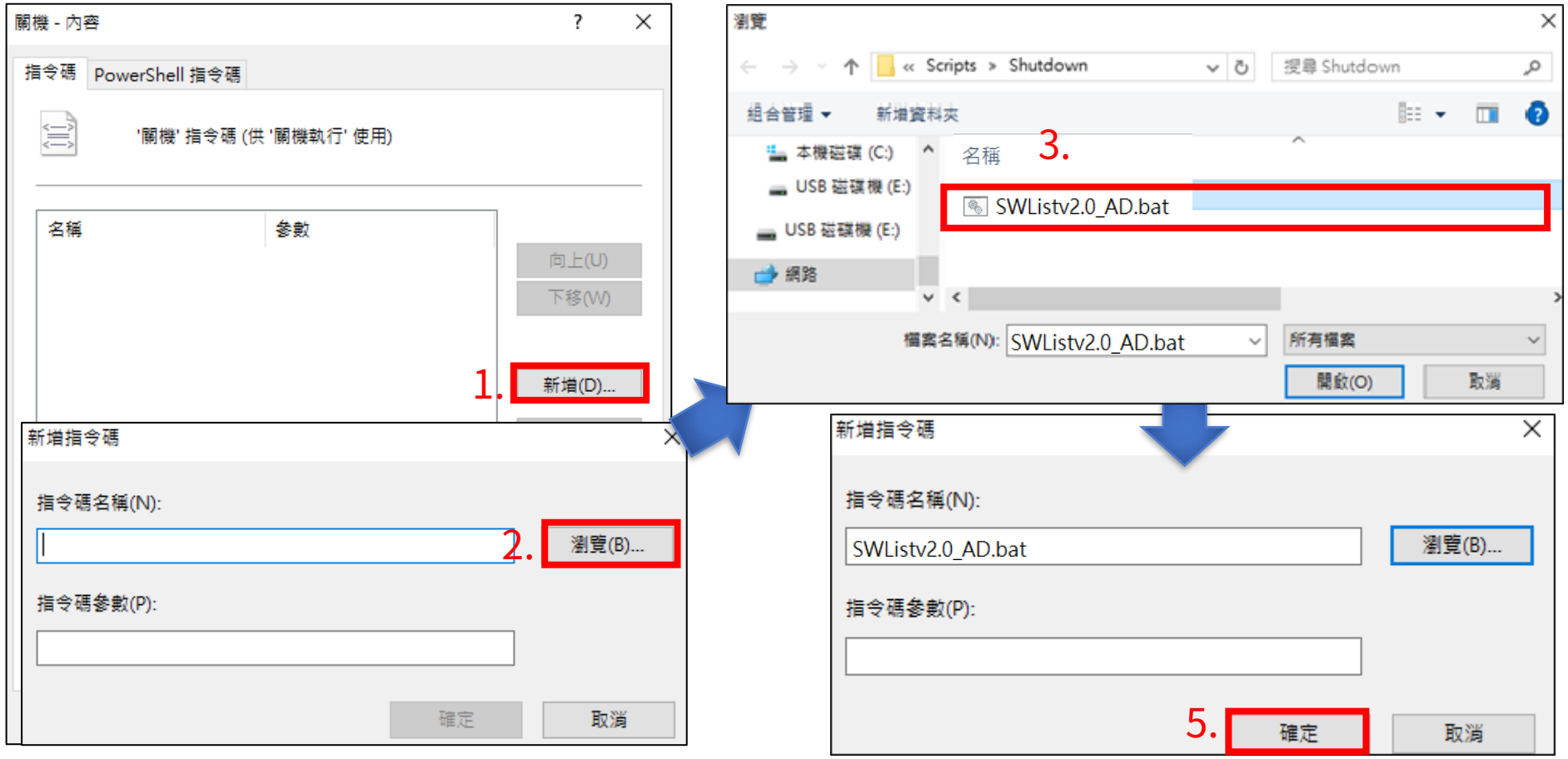
- 點選「顯示檔案」，準備放入檢測批次檔
- 因作業系統預設不允許複製檔案至網路位置，須將資料夾路徑改為本機路徑，放入盤點批次檔後即可關閉
  - 由「**\\[網域名稱]\SysVol\[網域名稱]**\Policies\{關機執行GPO_GUID}\Machine\Scripts\Shutdown」
  - 改成「**C:\Windows\SYSVOL\domain**\Policies\{關機執行GPO_GUID}\Machine\Scripts\Shutdown」



派送GPO-關機執行(4/5)

國家資通安全研究院
National Institute of Cyber Security

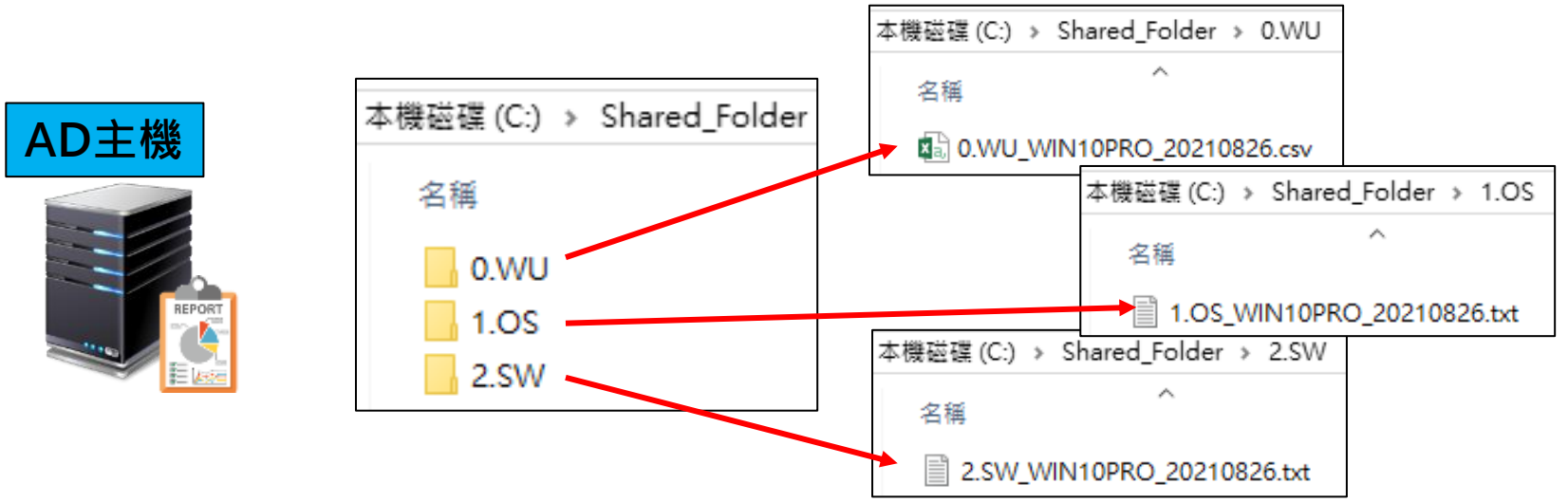
- 選擇關機執行的檔案
  - 選擇「新增」後，點選「瀏覽」並選取前一步驟放入的盤點批次檔



派送GPO-關機執行(5/5)

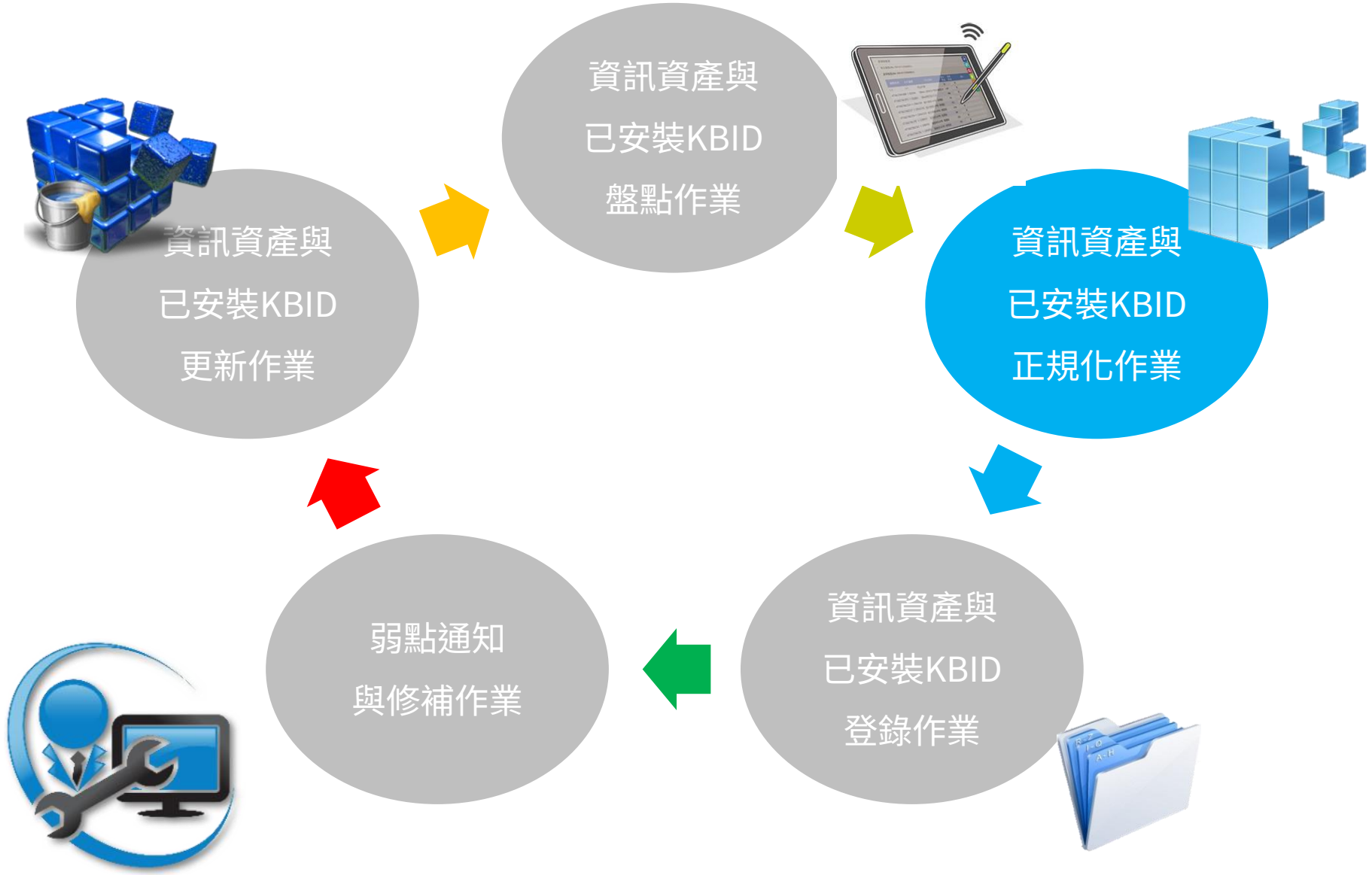
國家資通安全研究院
National Institute of Cyber Security

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



導入作業流程

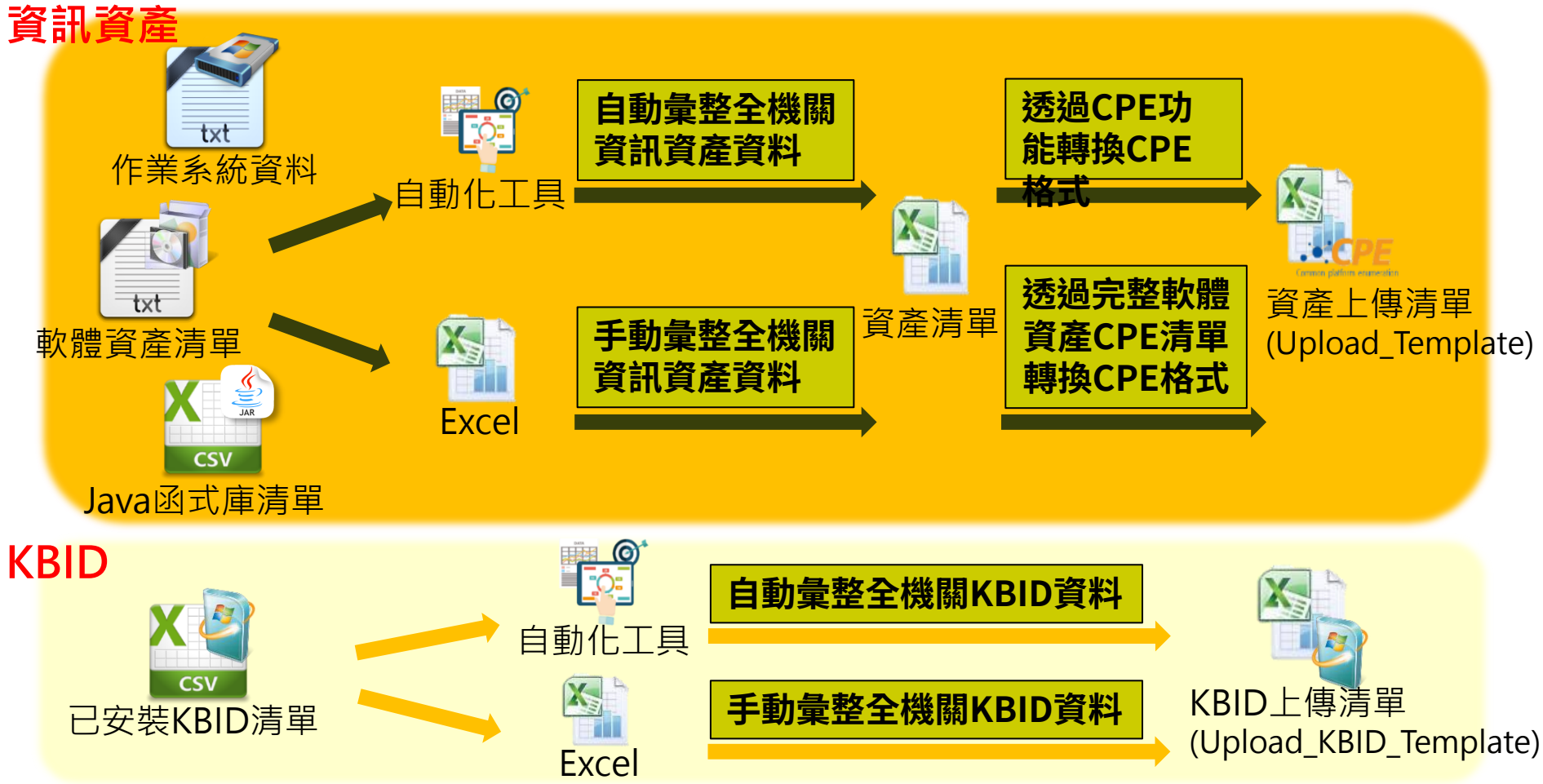
國家資通安全研究院
National Institute of Cyber Security



資訊資產與已安裝KBID正規化

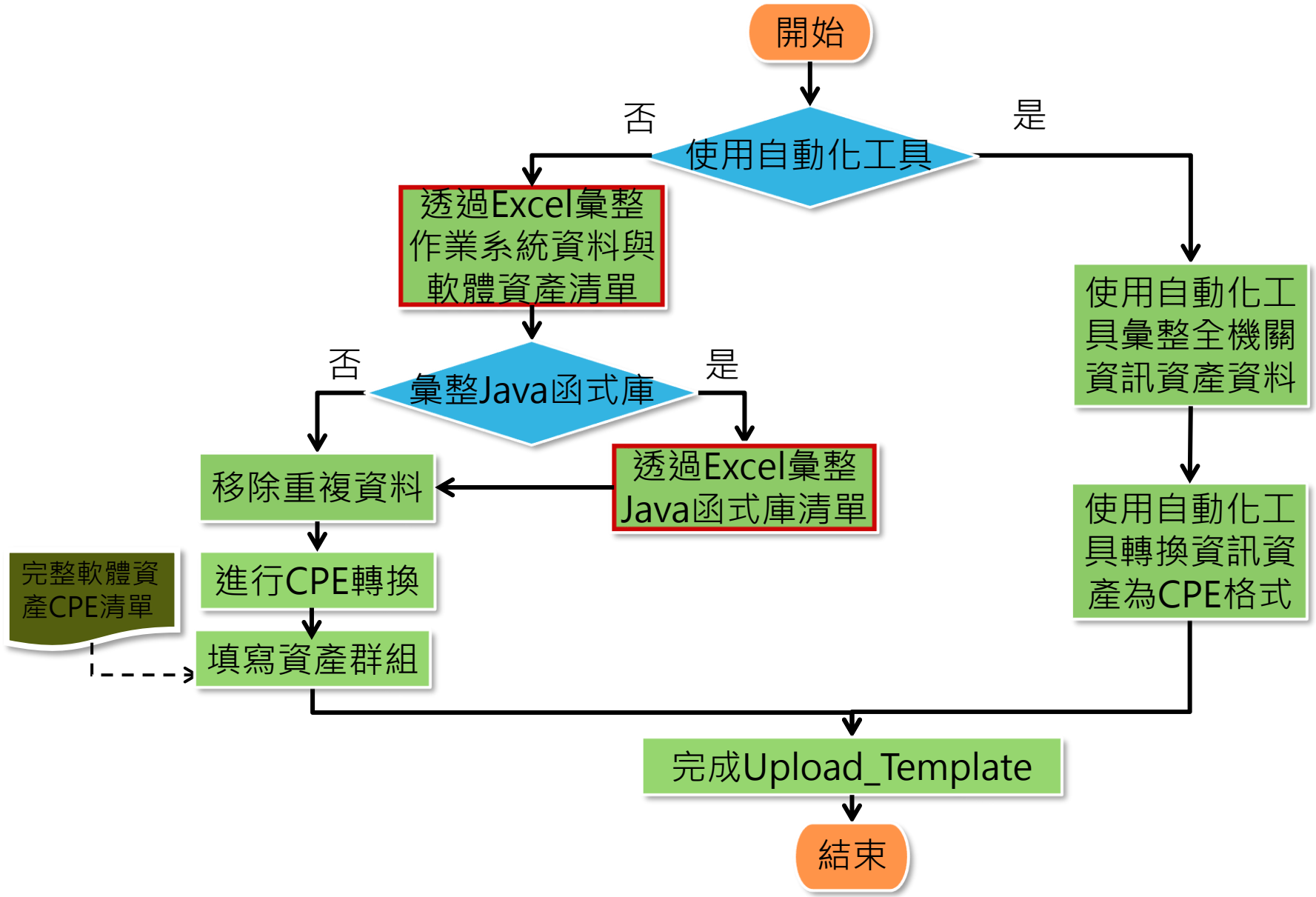
國家資通安全研究院
National Institute of Cyber Security

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



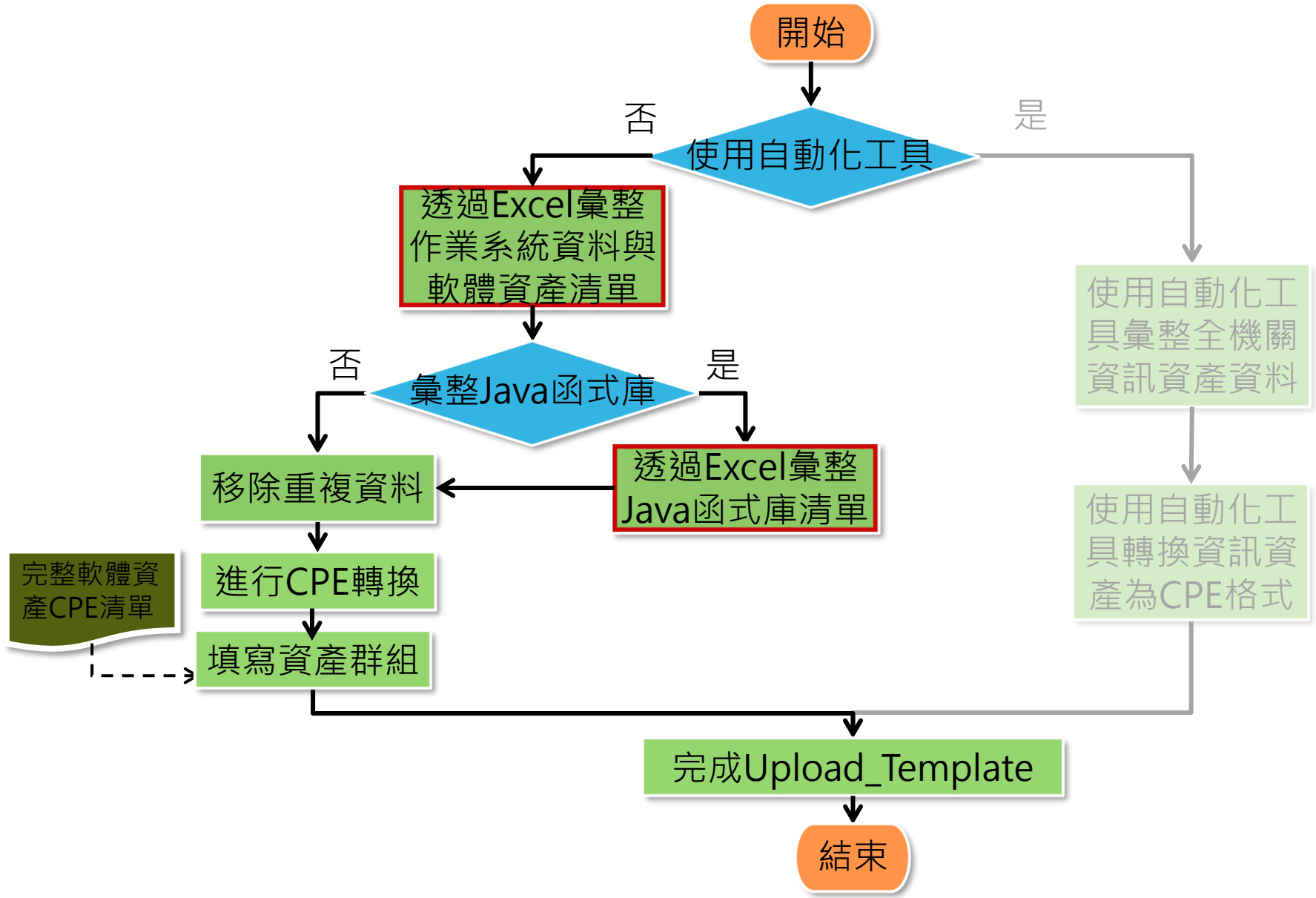
資訊資產正規化作業

資訊資產正規化作業流程



資訊資產正規化作業流程

國家資通安全研究院
National Institute of Cyber Security



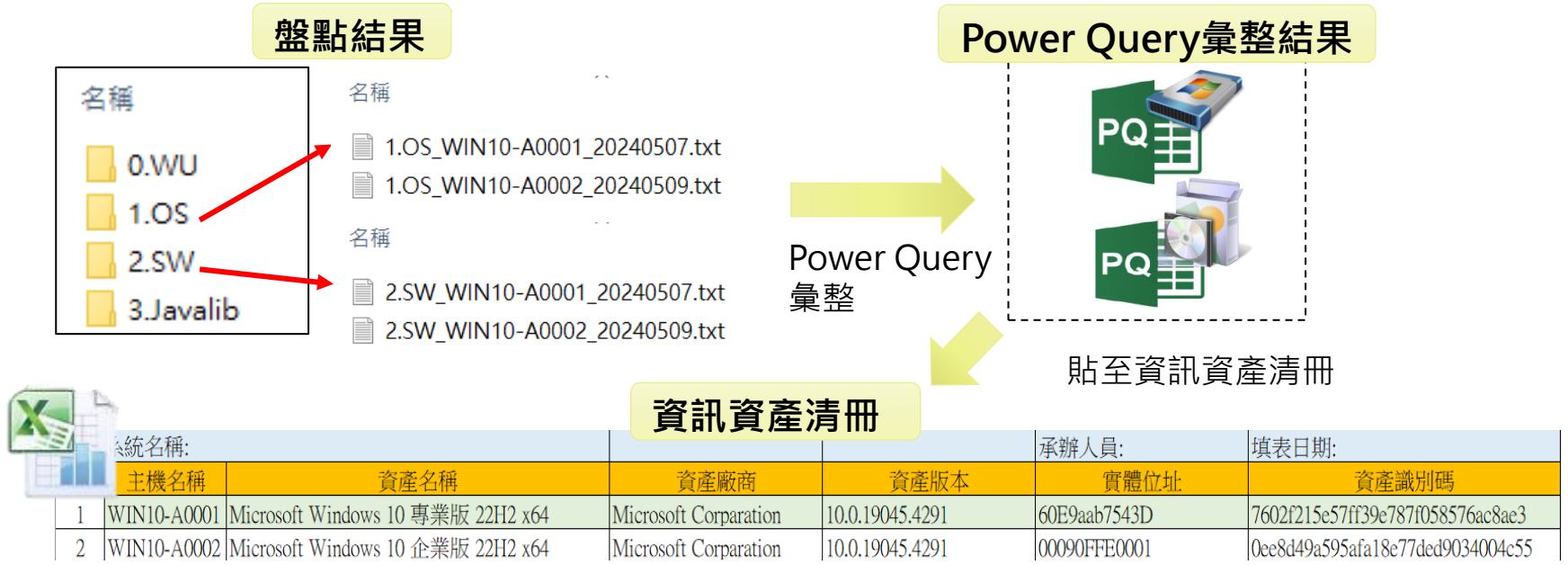
Excel彙整功能介紹

- Microsoft Power Query for Excel可在各種不同的資料來源中合併或精簡資料
  - 適用於32位元與64位元平台
  - 支援作業系統版本
    - Windows 7/8/8.1/10
    - Windows Server 2008 R2/2012
  - 支援Office版本
    - Microsoft Office 2010 Professional Plus(需另行安裝套件)
    - Microsoft Office 2013 (需另行安裝套件)
    - Power Query內建於Excel 2016、2019中，功能名稱為「取得及轉換」
  - 須Internet Explorer 9以上之版本
- 下載網址：
  - https://www.microsoft.com/zh-TW/download/details.aspx?id=39379

彙整資訊資產清單

國家資通安全研究院
National Institute of Cyber Security

- 透過Power Query分別彙整歸類後作業系統與軟體資產之盤點結果
  - 若欲了解彙整步驟，請參閱「資通安全弱點通報系統操作手冊*」v2.0或更新版本
- 將作業系統與軟體資產彙整結果，整合至資訊資產清冊*，以留存查看



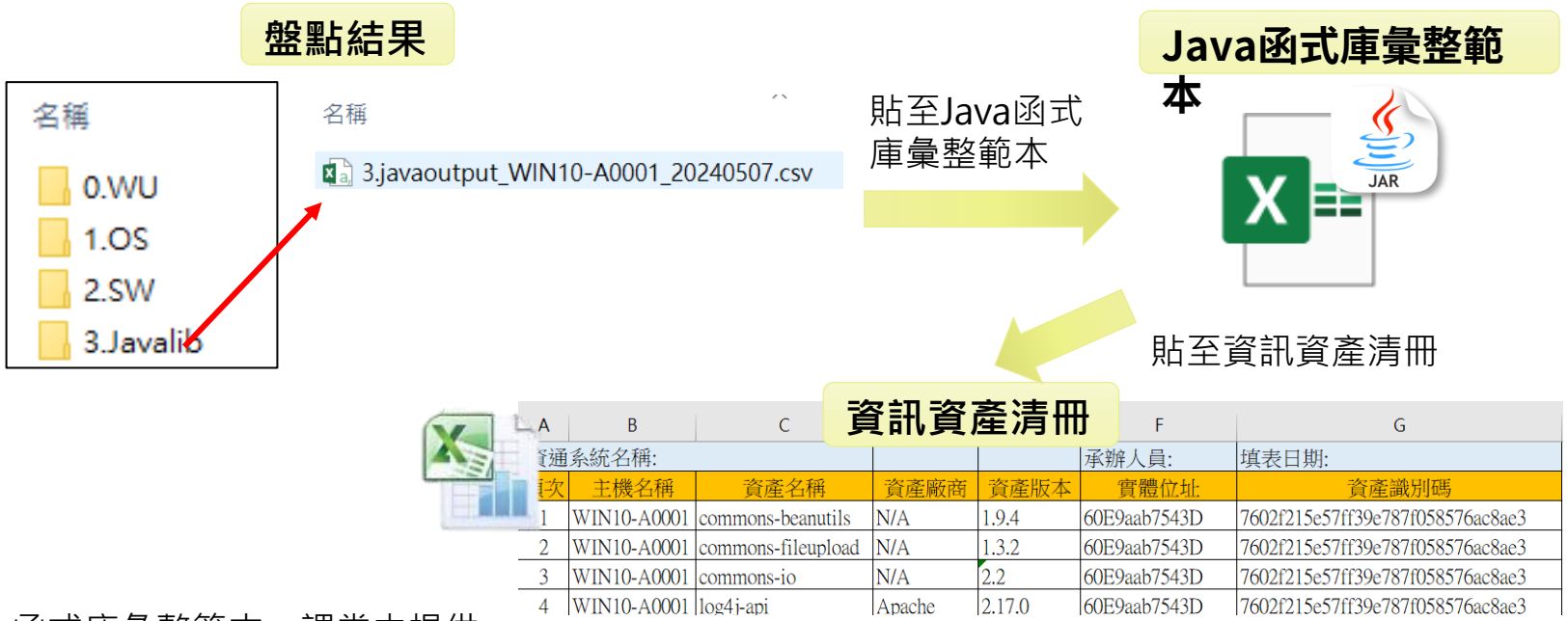
系統名稱:					承辦人員:	填表日期:
	主機名稱	資產名稱	資產廠商	資產版本	實體位址	資產識別碼
1	WIN10-A0001	Microsoft Windows 10 專業版 22H2 x64	Microsoft Corparation	10.0.19045.4291	60E9aab7543D	7602f215e57ff39e787f058576ac8ae3
2	WIN10-A0002	Microsoft Windows 10 企業版 22H2 x64	Microsoft Corparation	10.0.19045.4291	00090FFE0001	0ee8d49a595afa18e77ded9034004c55

註1：操作手冊：機關管理者帳號開通之通知信提供或透過VansService服務信箱索取
註2：資訊資產清冊：課堂中提供

彙整資訊資產清單_Java函式庫

國家資通安全研究院
National Institute of Cyber Security

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

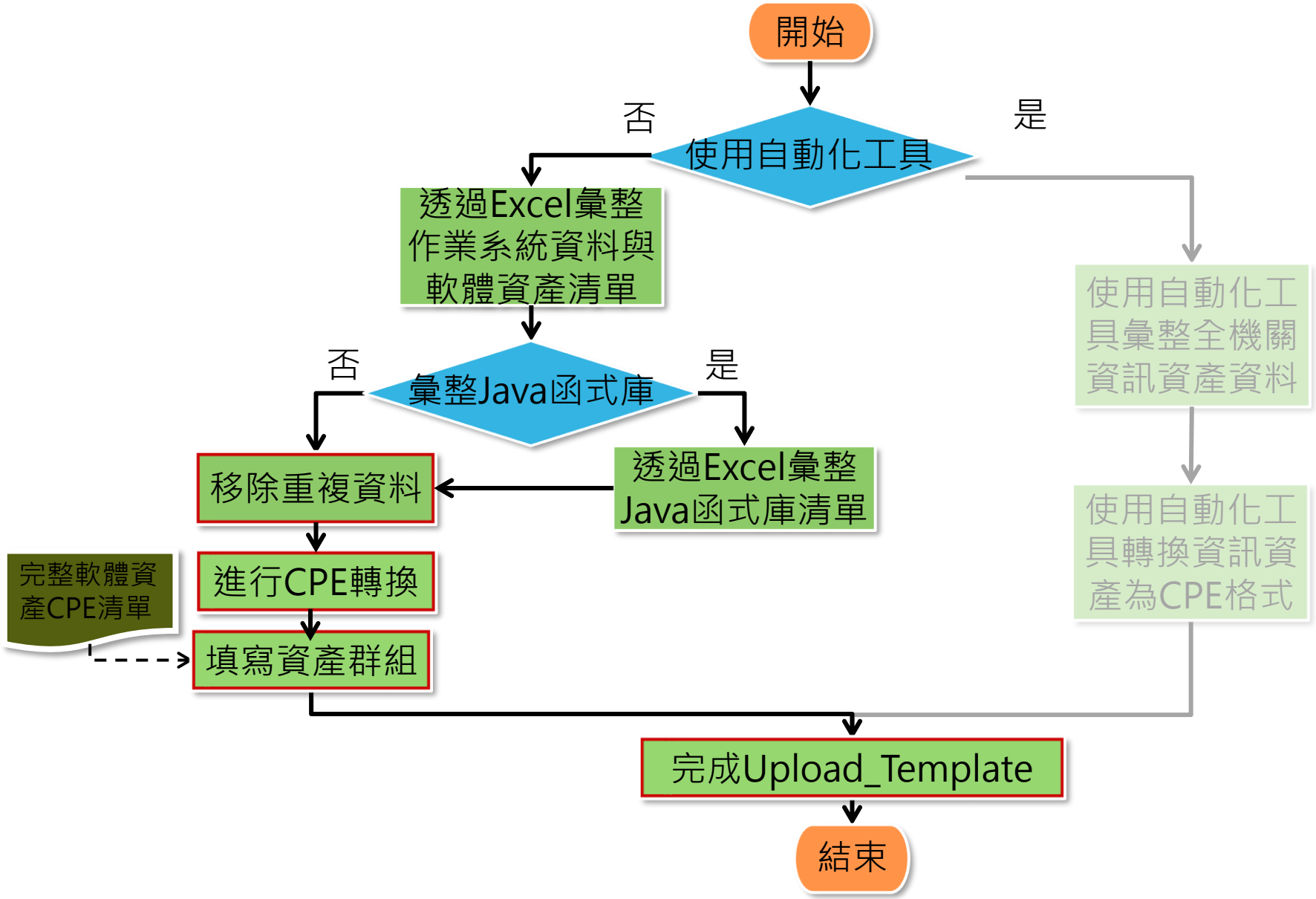


	A	B	C	D	E	F	G
	資通系統名稱:					承辦人員:	填表日期:
	項次	主機名稱	資產名稱	資產廠商	資產版本	實體位址	資產識別碼
	1	WIN10-A0001	commons-beanutils	N/A	1.9.4	60E9aab7543D	7602f215e57ff39e787f058576ac8ae3
	2	WIN10-A0001	commons-fileupload	N/A	1.3.2	60E9aab7543D	7602f215e57ff39e787f058576ac8ae3
	3	WIN10-A0001	commons-io	N/A	2.2	60E9aab7543D	7602f215e57ff39e787f058576ac8ae3
	4	WIN10-A0001	log4j-api	Apache	2.17.0	60E9aab7543D	7602f215e57ff39e787f058576ac8ae3

註： Java函式庫彙整範本：課堂中提供

資訊資產正規化作業流程

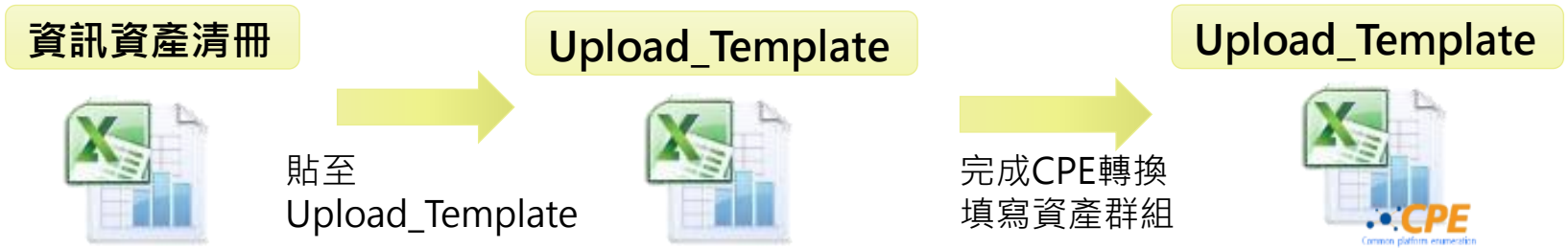
國家資通安全研究院
National Institute of Cyber Security



完成Upload_Template

國家資通安全研究院
National Institute of Cyber Security

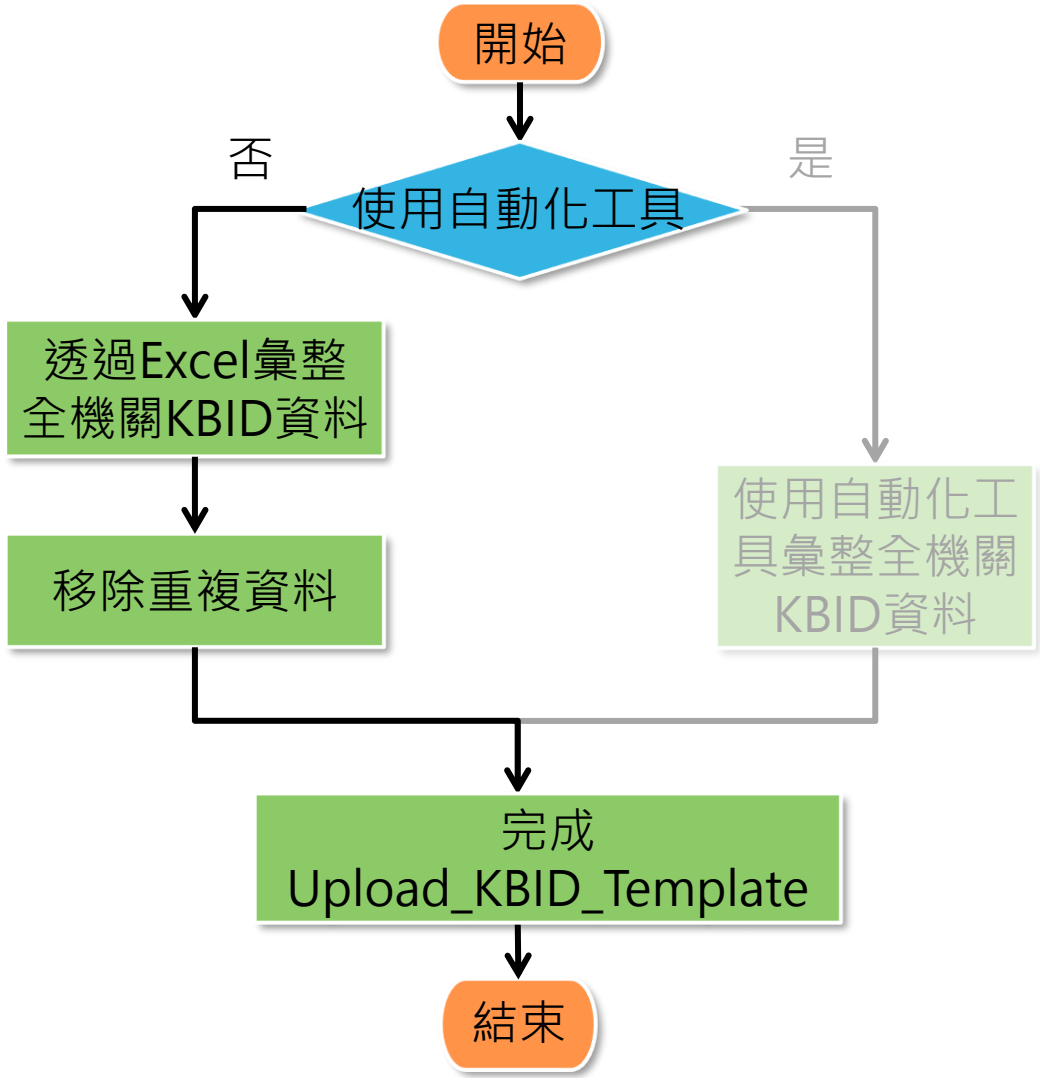
- 移除重複資料
  - 利用移除重複項功能，以避免上傳相同之資訊資產
- 進行CPE轉換
  - 將資訊資產清冊彙整至Upload_Template(註)
  - 於完整軟體資產CPE清單*搜尋，並於Upload_Template填入資訊資產對應之CPE格式，若無則填入N/A
- 填寫資產群組
  - 查詢機關資產群組代碼與資產群組，並將資產群組代碼輸入資產群組欄位。
- 完成Upload_Template
  - 填寫機關OID與機關名稱



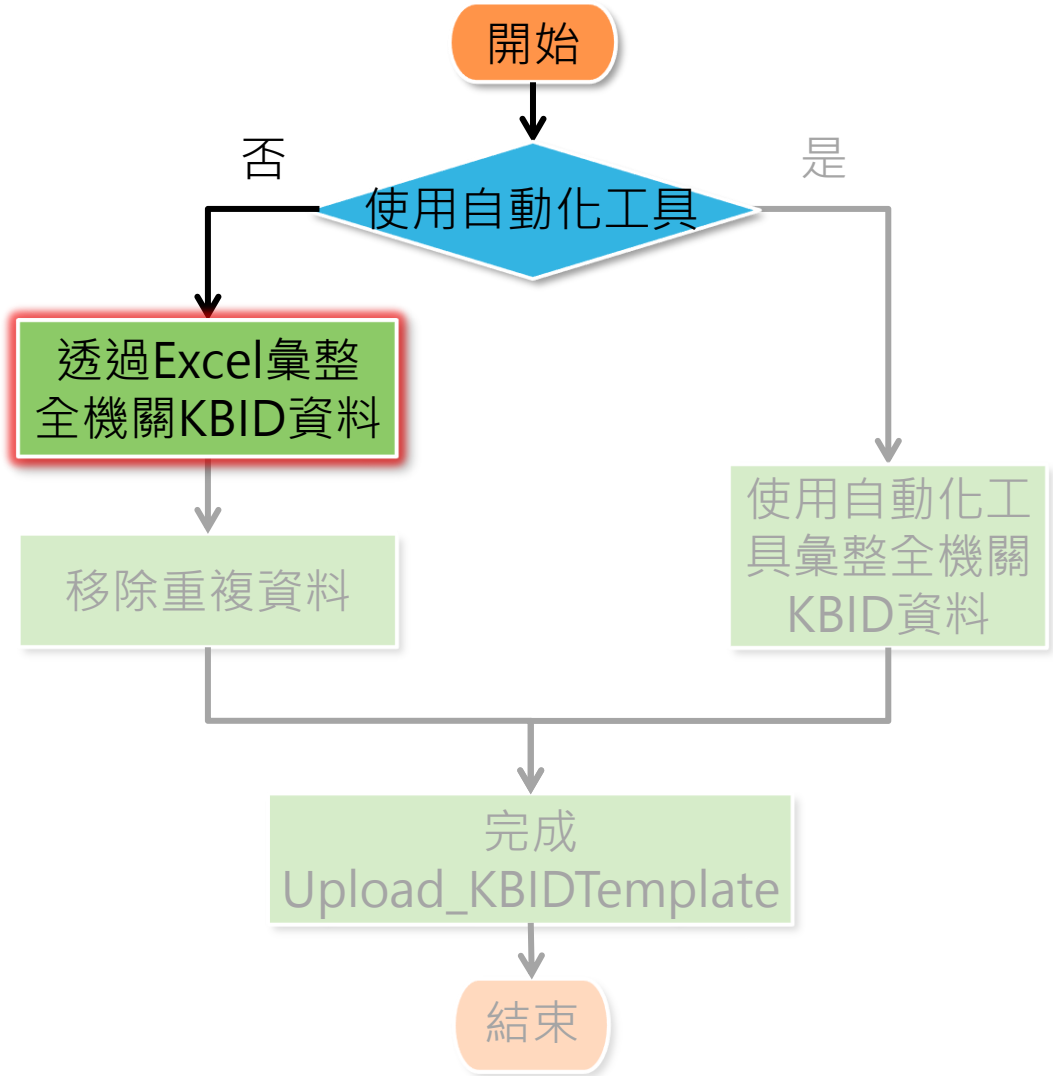
註：於VANS系統下載

已安裝KBID正規化作業

已安裝KBID正規化作業流程



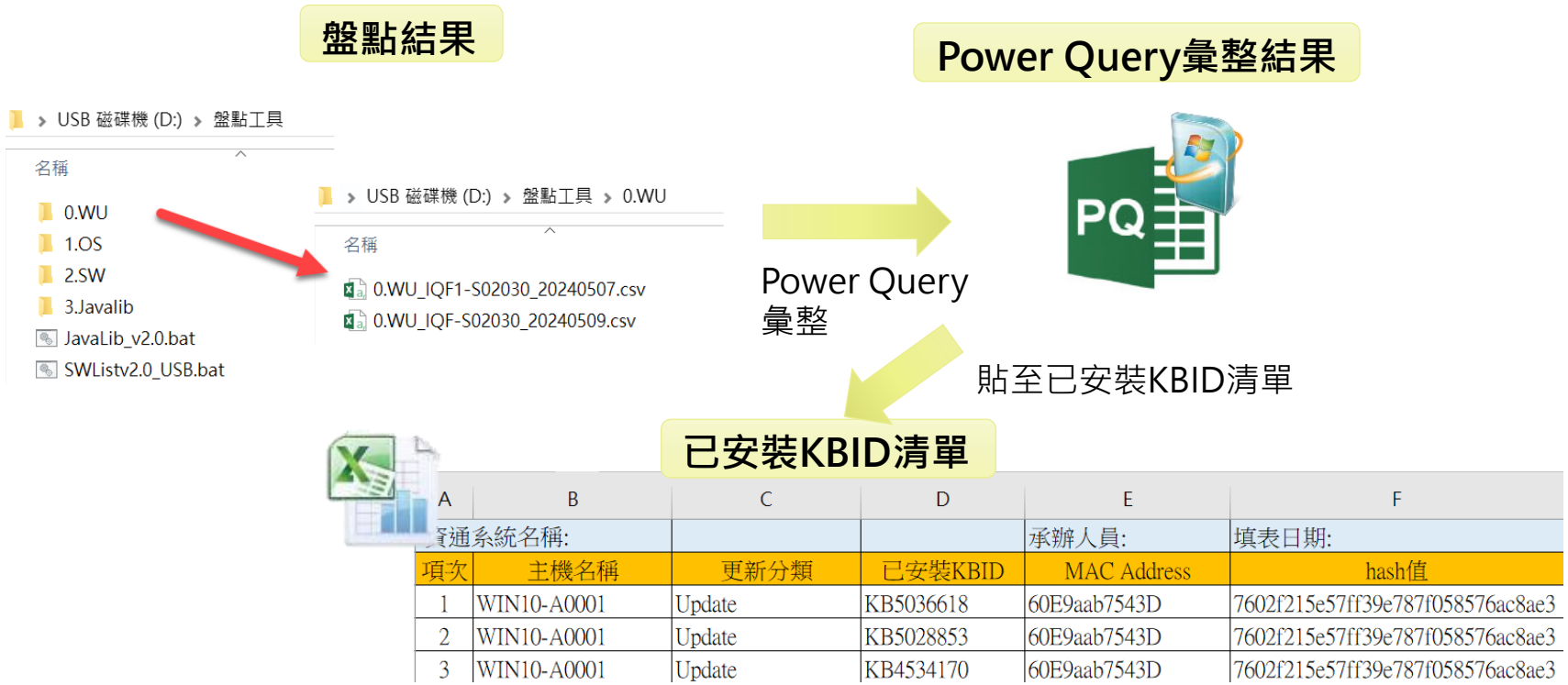
已安裝KBID正規化作業流程



彙整KBID清單

國家資通安全研究院
National Institute of Cyber Security

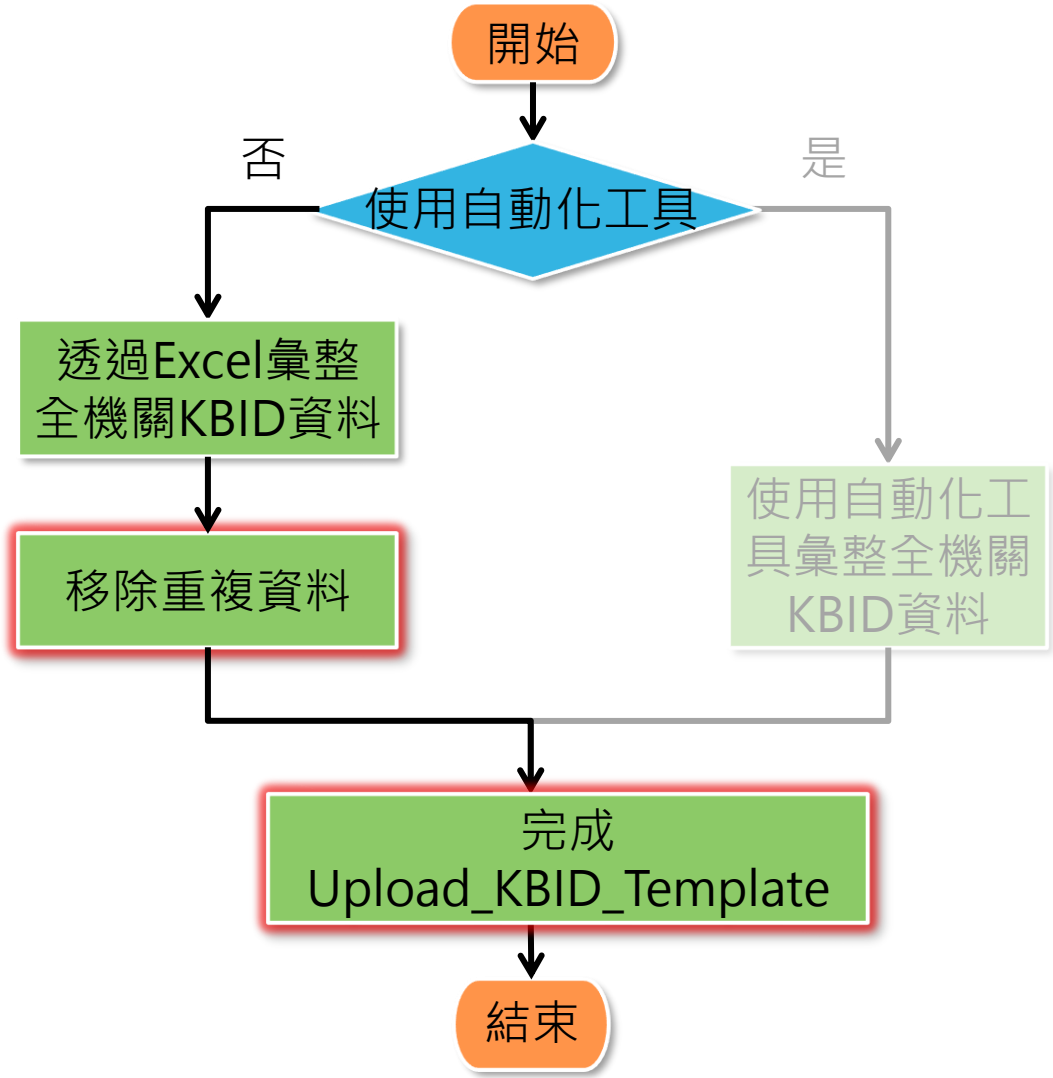
- 透過Power Query彙整歸類後已安裝KBID之盤點結果
  - 若欲了解彙整步驟，請參閱「資通安全弱點通報系統操作手冊(註1)」v2.0 或更新版本
- 將已安裝KBID彙整結果，整合至已安裝KBID清單(註2)，以留存查看



A	B	C	D	E	F
資通系統名稱:				承辦人員:	填表日期:
項次	主機名稱	更新分類	已安裝KBID	MAC Address	hash值
1	WIN10-A0001	Update	KB5036618	60E9aab7543D	7602f215e57ff39e787f058576ac8ae3
2	WIN10-A0001	Update	KB5028853	60E9aab7543D	7602f215e57ff39e787f058576ac8ae3
3	WIN10-A0001	Update	KB4534170	60E9aab7543D	7602f215e57ff39e787f058576ac8ae3

註1：操作手冊：機關管理者帳號開通之通知信提供或透過VansService服務信箱索取
註2：已安裝KBID清單：課堂中提供

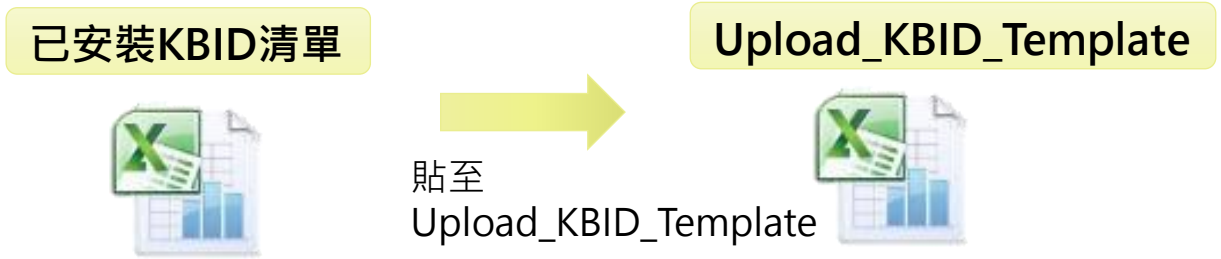
已安裝KBID正規化作業流程



完成Upload_KBID_Template

國家資通安全研究院
National Institute of Cyber Security

- 移除重複資料
  - 利用移除重複項功能，以避免上傳相同之KBID
- 完成Upload_KBID_Template
  - 將已安裝KBID清單彙整至Upload_KBID_Template(註)
  - 填寫機關OID與機關名稱

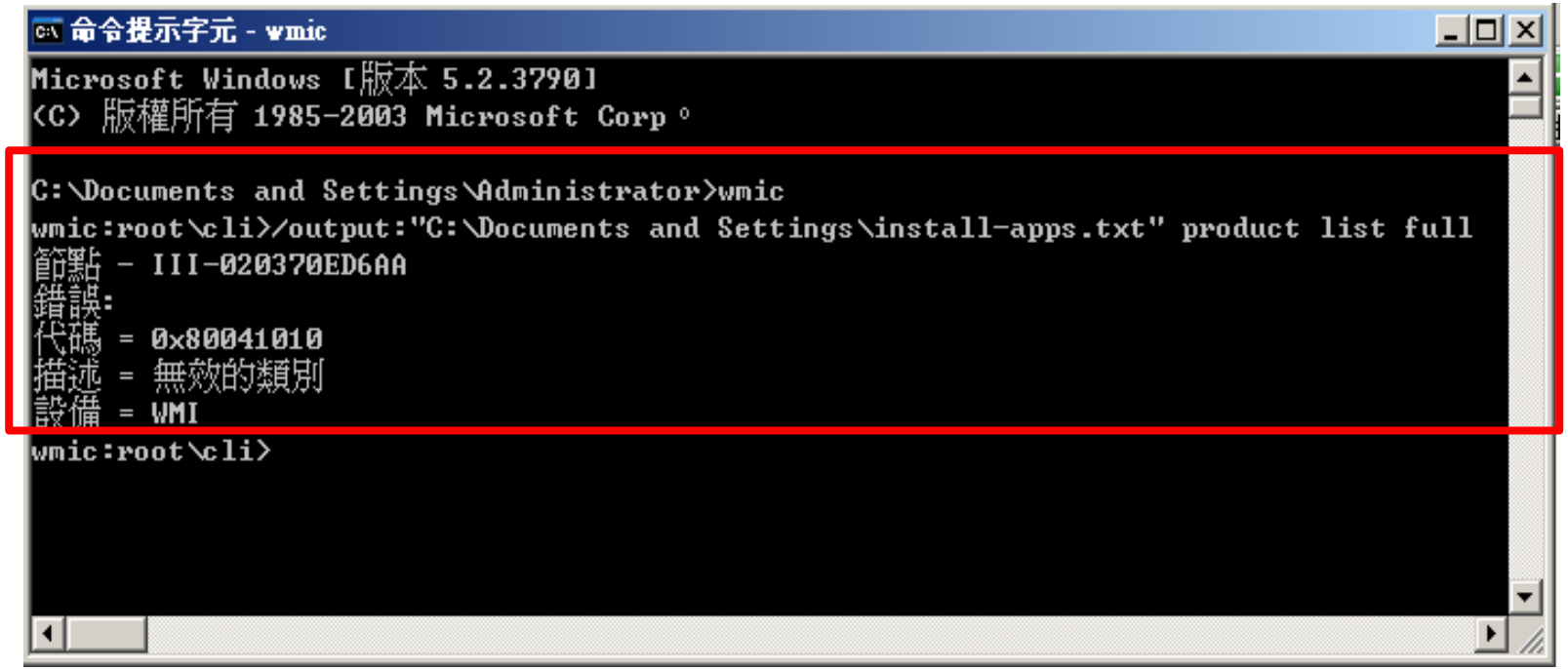


註：Upload_KBID_Template：於VANS系統下載

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



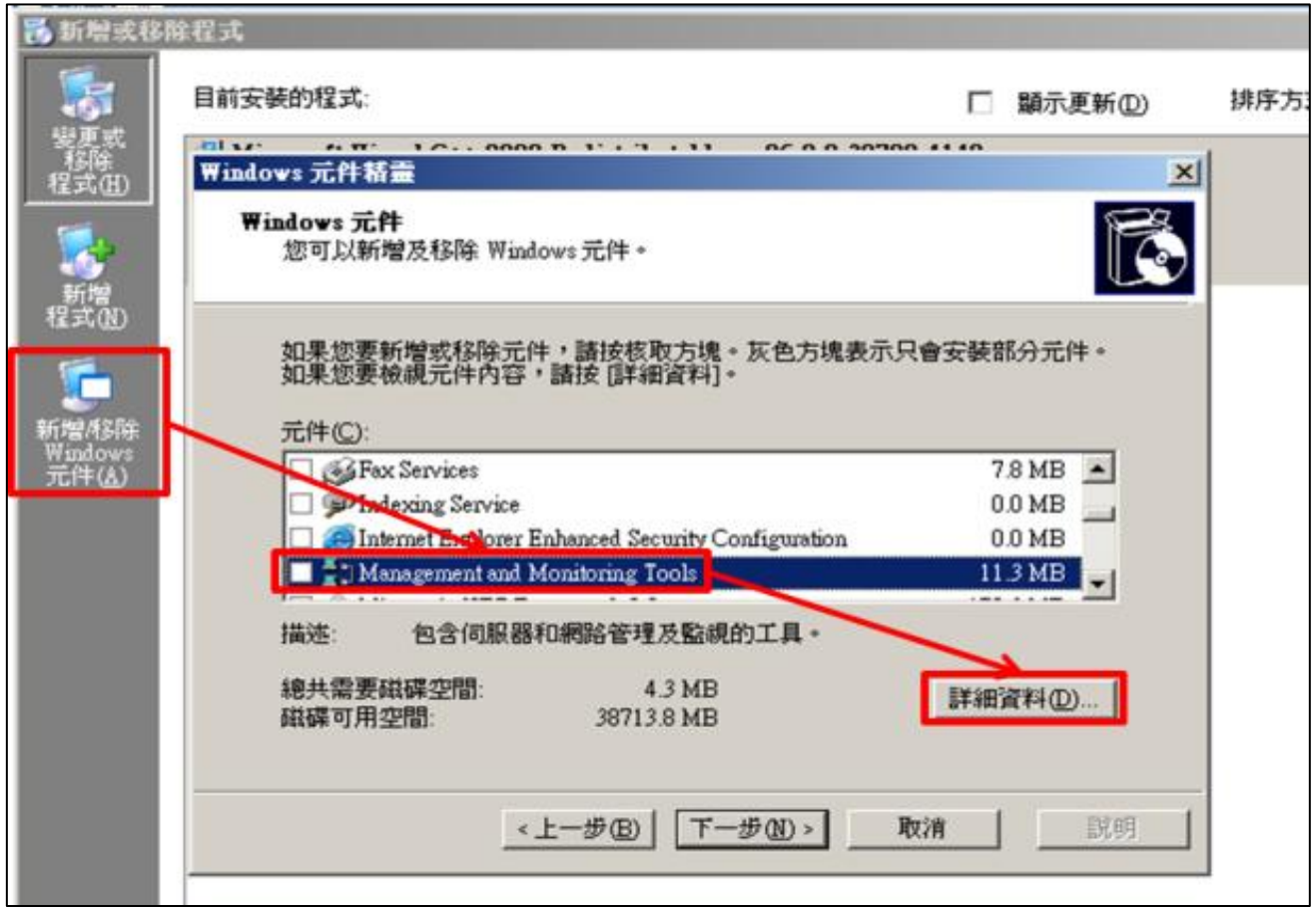
安裝WMI Windows Installer(2/7)

- 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)

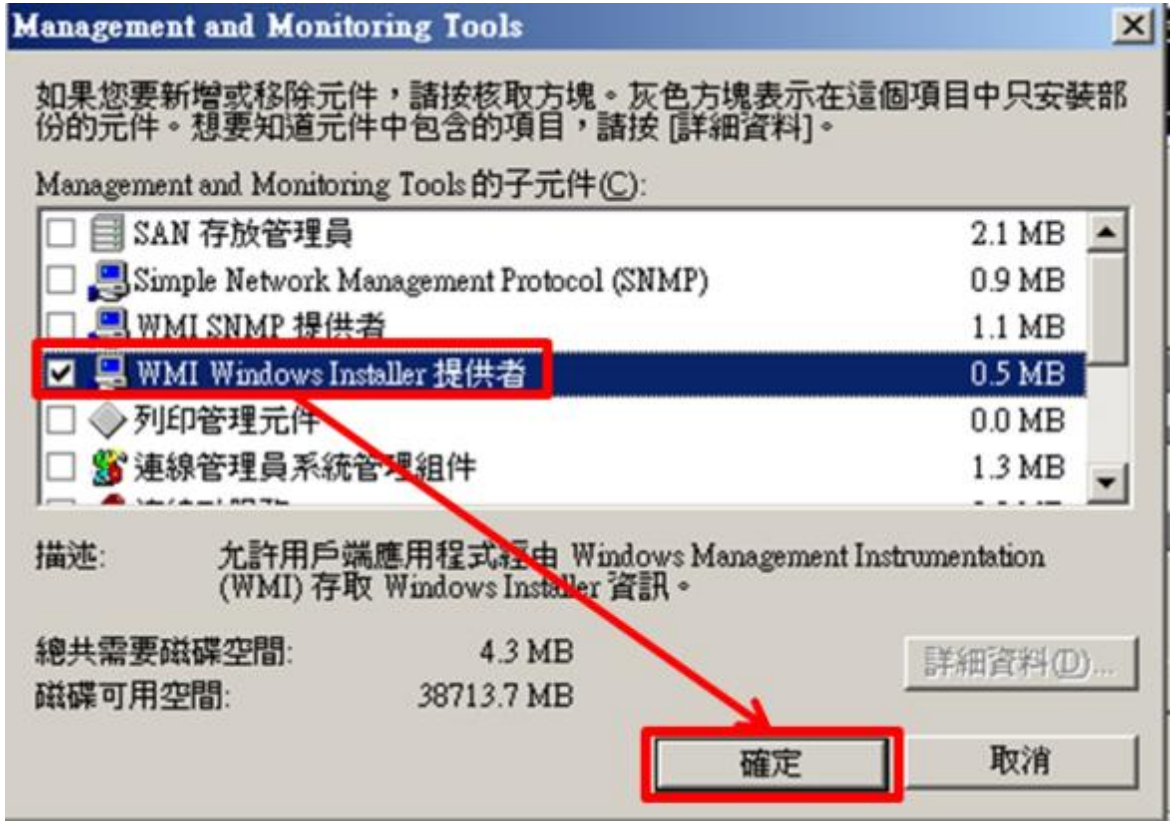
國家資通安全研究院
National Institute of Cyber Security

- 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



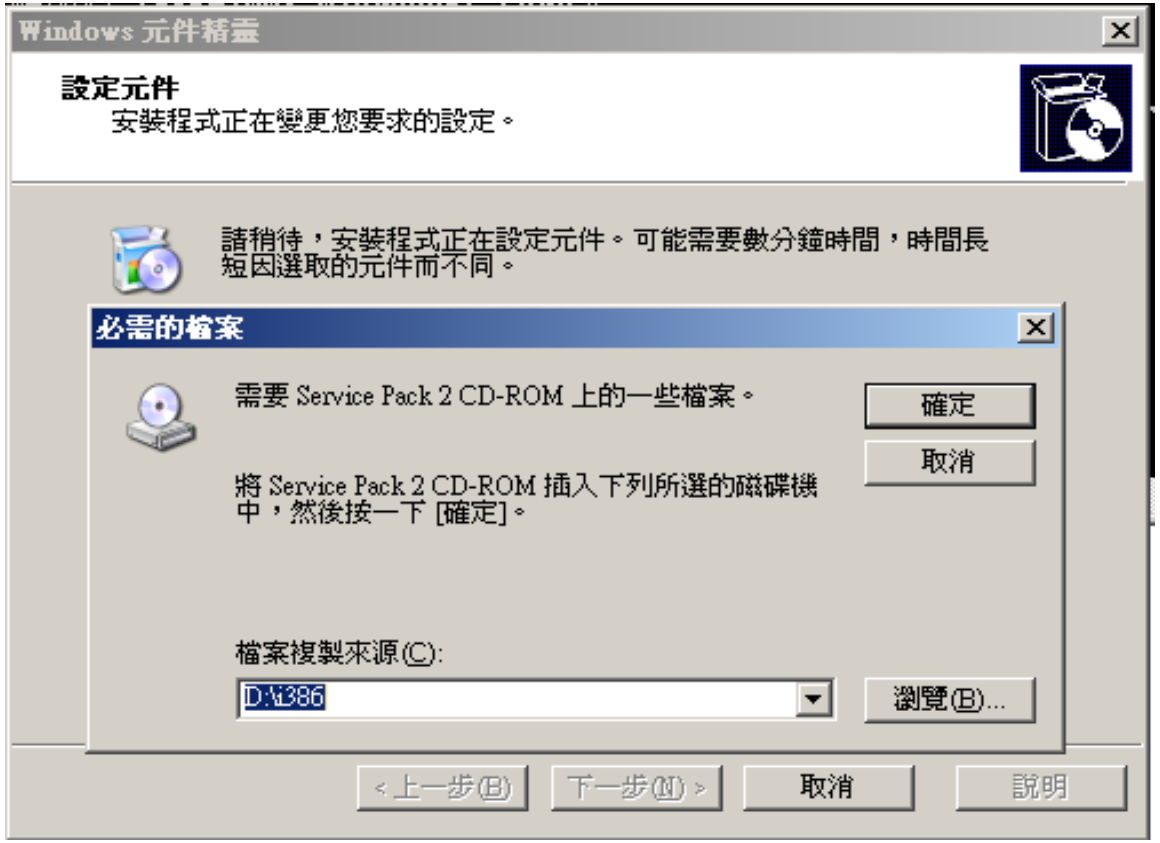
安裝WMI Windows Installer(4/7)

- 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」



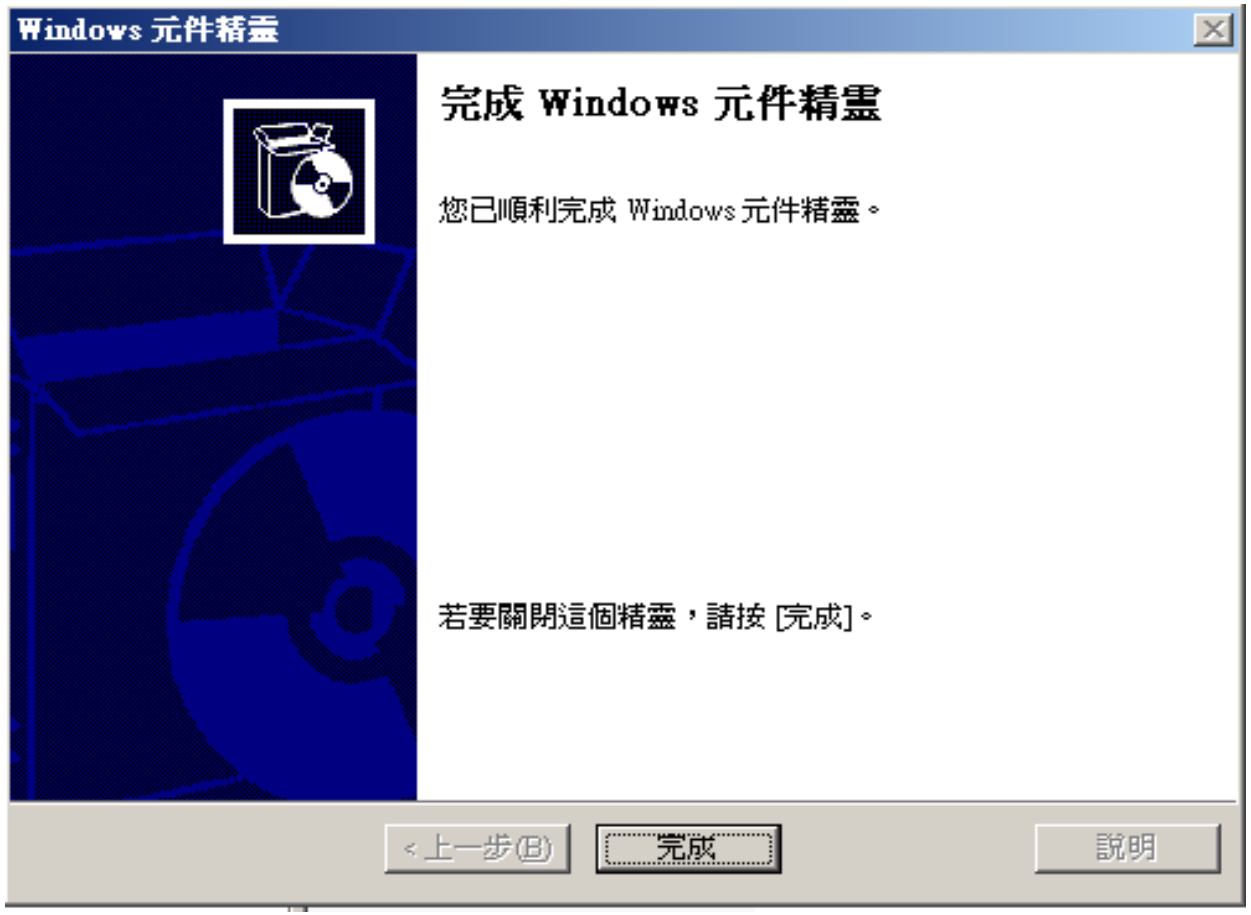
安裝WMI Windows Installer(5/7)

- 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)

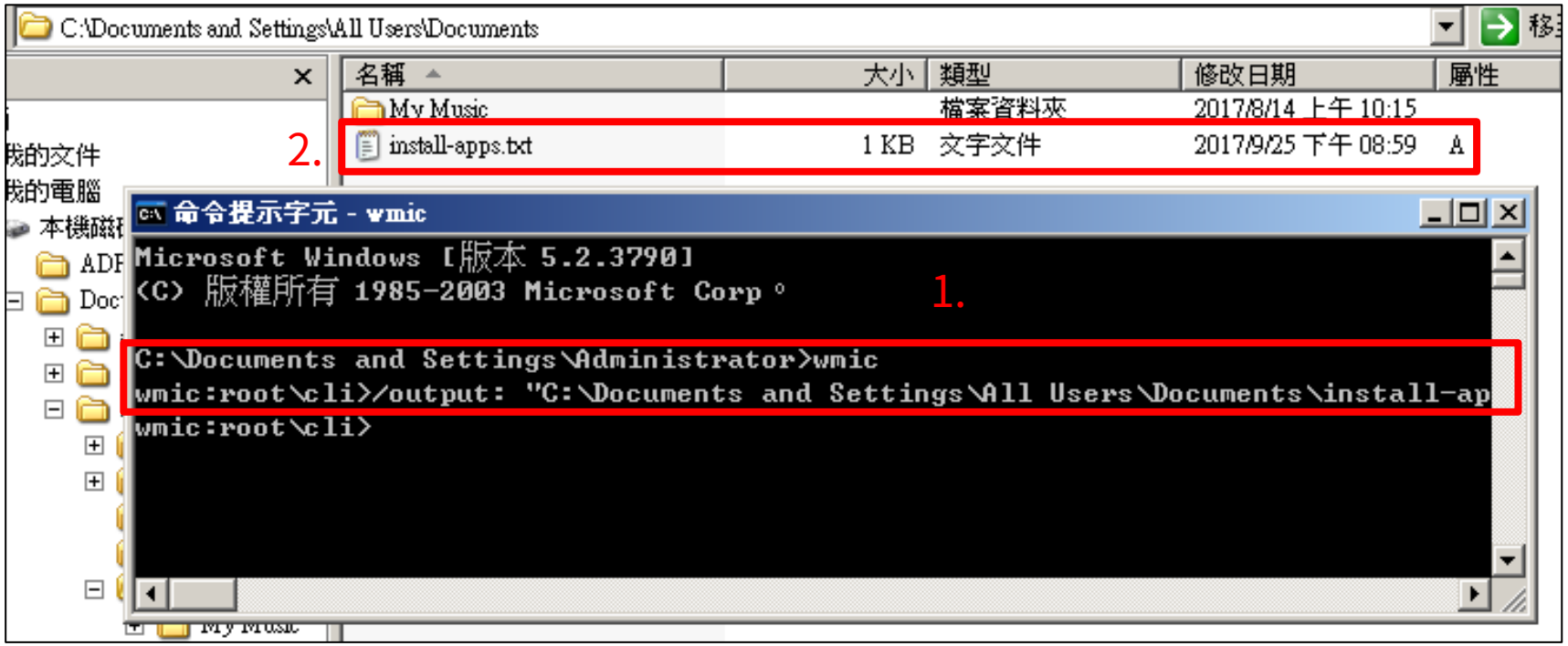
- 步驟五：完成安裝



安裝WMI Windows Installer(7/7)

國家資通安全研究院
National Institute of Cyber Security

- 步驟六：安裝完成後，即可執行WMIC

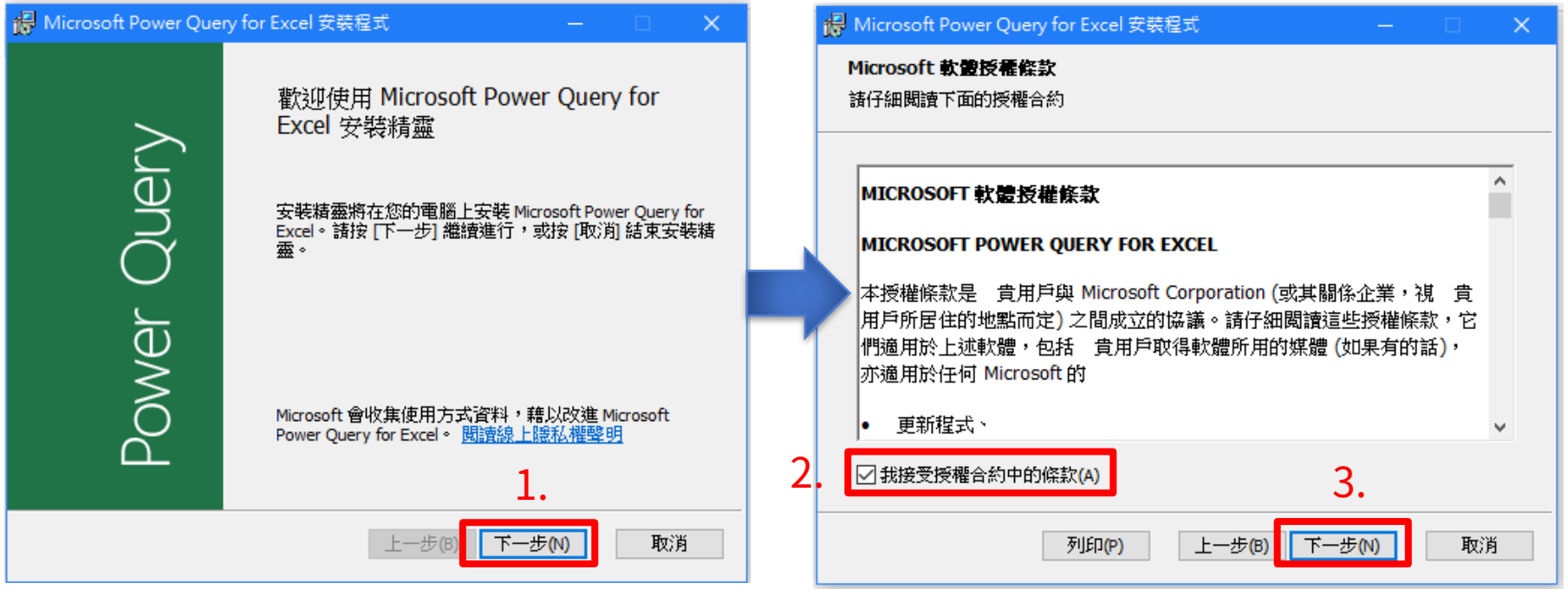


國家資通安全研究院
National Institute of Cyber Security

附件3
Microsoft Power Query for Excel
安裝步驟

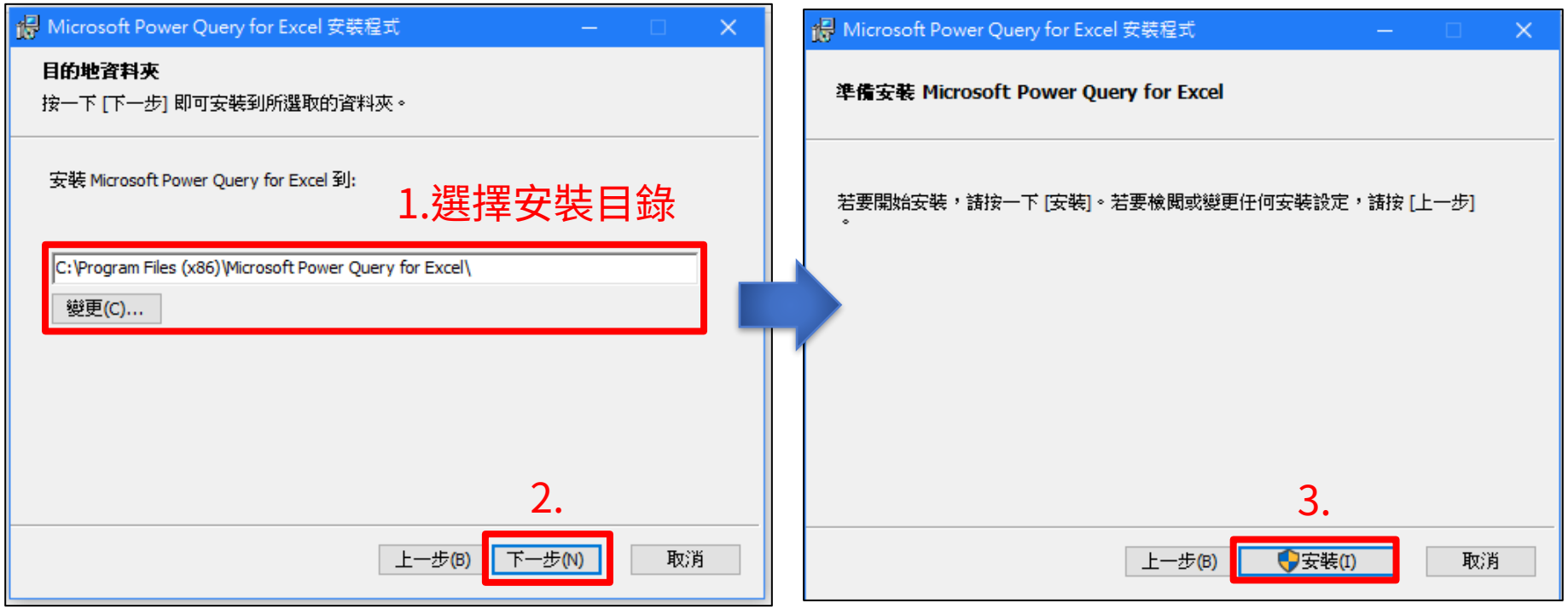
安裝Microsoft Power Query for Excel(1/3)

- 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



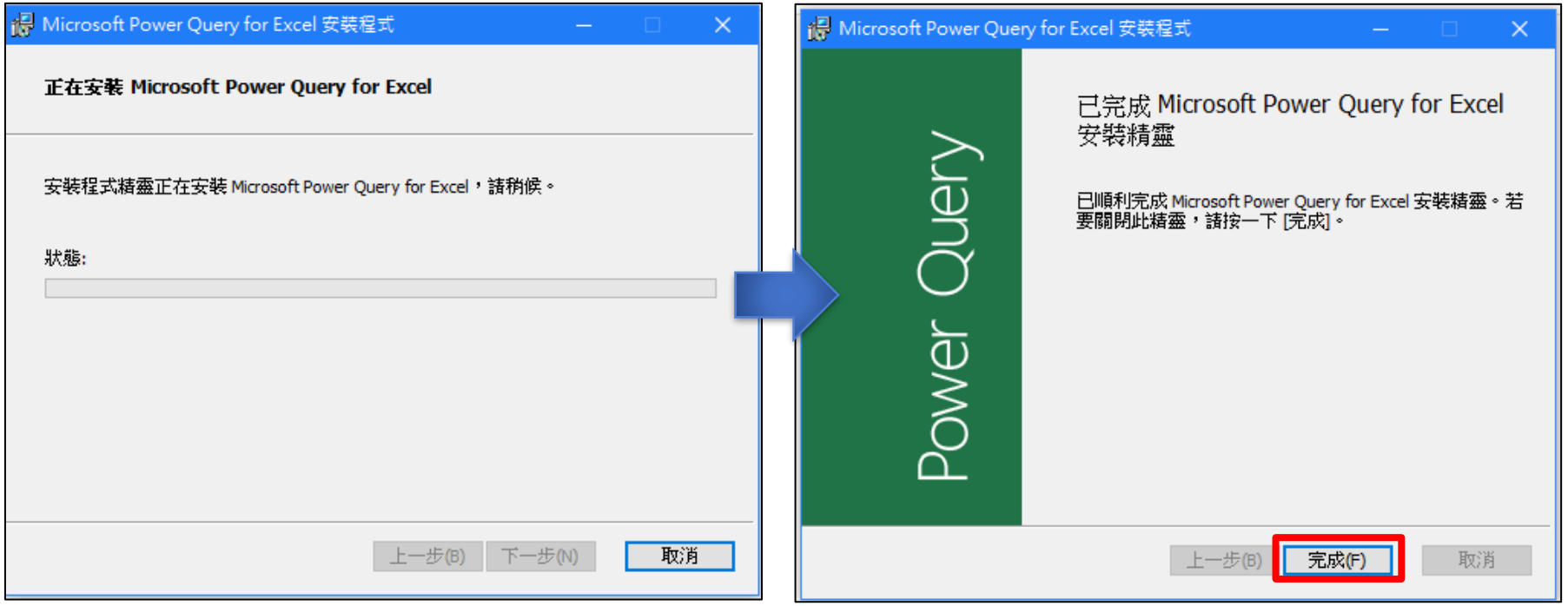
安裝Microsoft Power Query for Excel(2/3)

- 選擇安裝目錄，準備安裝



安裝Microsoft Power Query for Excel(3/3)

- 進行安裝



報告完畢
敬請指教

國家資通安全研究院
National Institute of Cyber Security