



政府機關資安弱點通報機制 推廣說明

行政院國家資通安全會報技術服務中心

大綱

- 前言
- 政府機關資安弱點通報機制介紹
- 政府機關資安弱點通報系統介紹
- 後續推動重點

NCCST

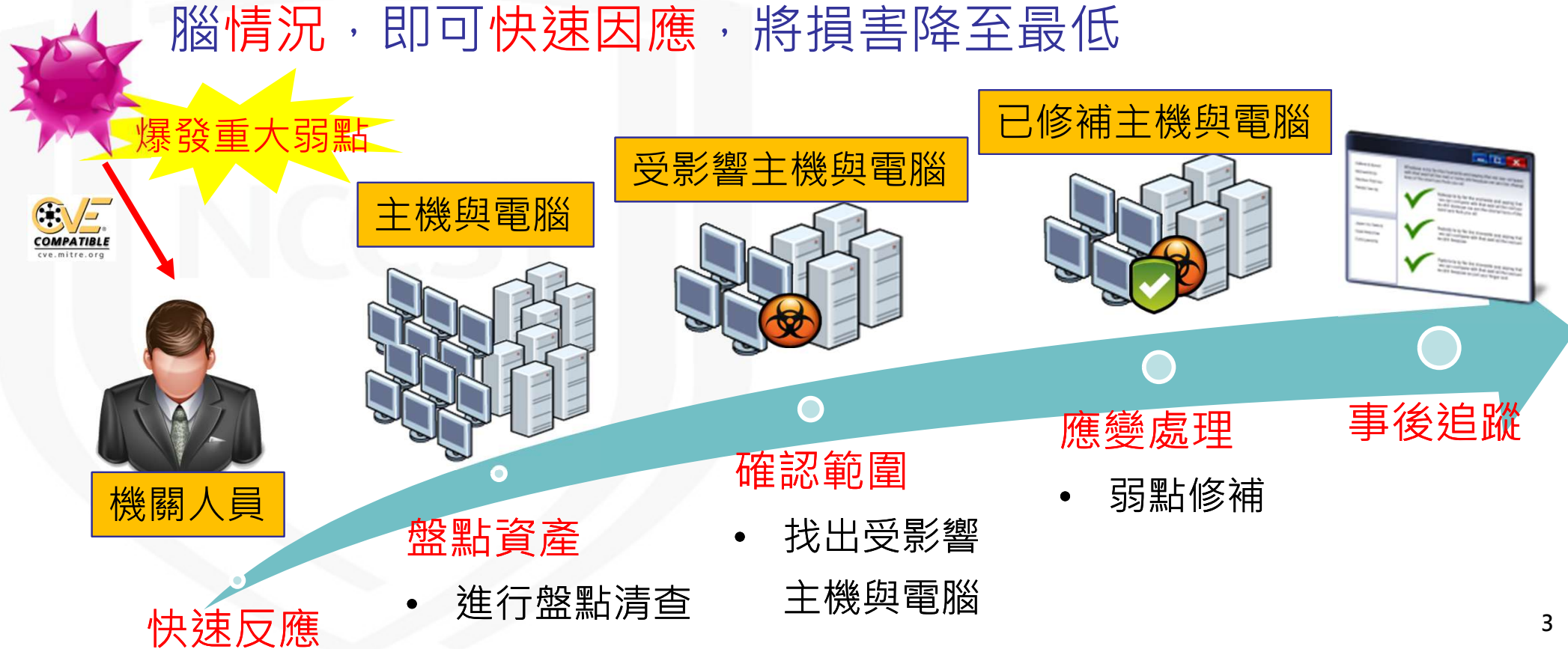
大綱

- 前言
- 政府機關資安弱點通報機制介紹
- 政府機關資安弱點通報系統介紹
- 後續推動重點

NCCST

前言

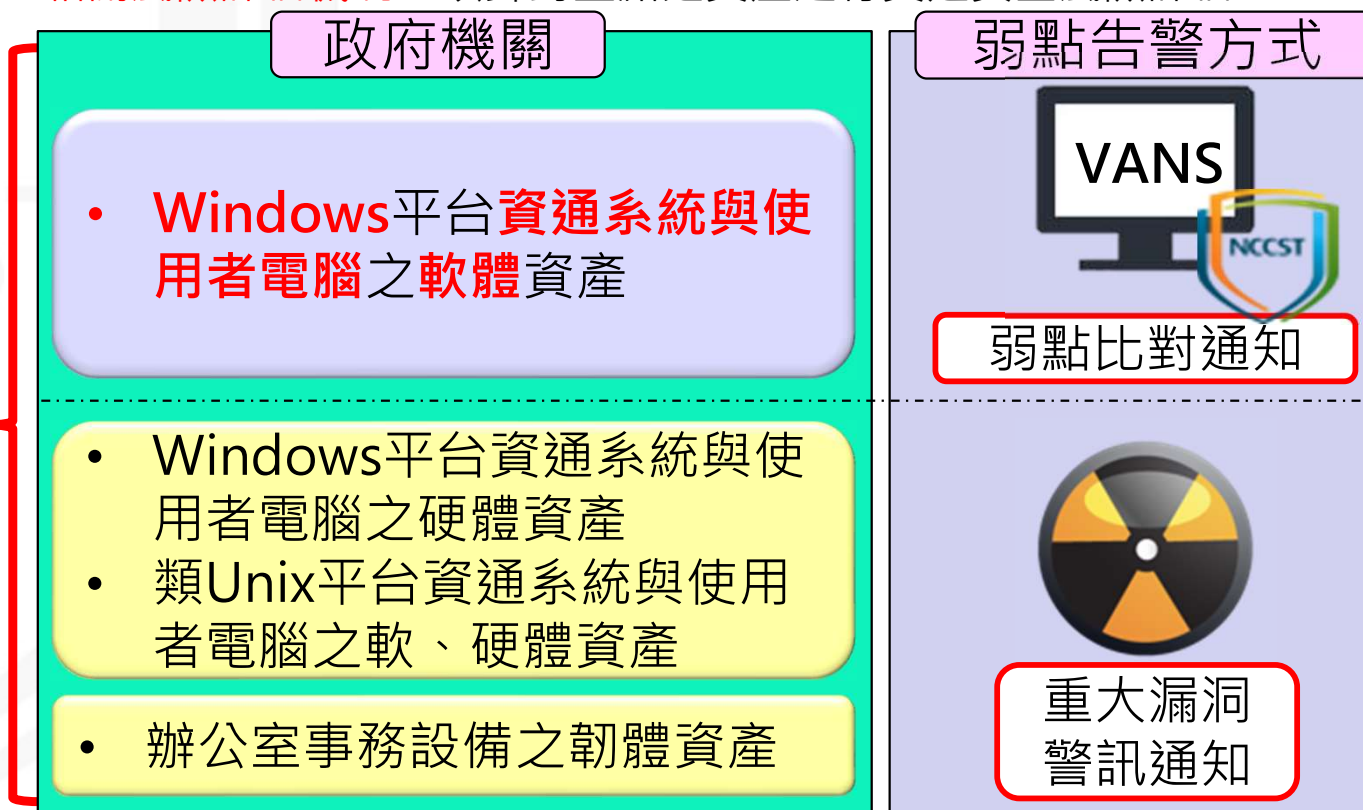
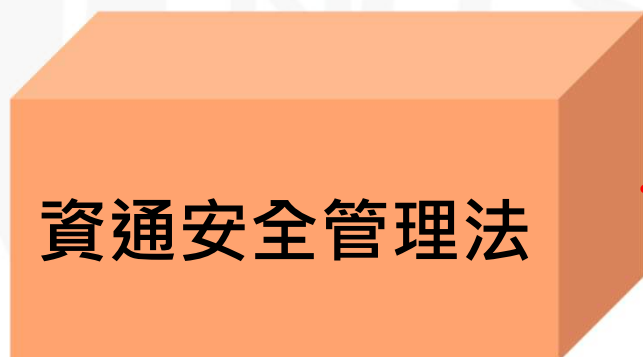
- 不定期爆發之重大弱點，若未能確實掌握機關資訊資產分布情況並即時因應，將嚴重影響機關業務運作，亦造成機關形象受損
- 當弱點爆發時，如能**確實掌握**機關資通系統與使用者電腦情況，即可**快速因應**，將損害降至最低



資通安全管理法相關規定(1/3)



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



資通安全管理法相關規定(2/3)



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

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

資通安全管理法相關規定(3/3)



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

國家資通安全發展方案

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

110年

- A級公務機關完成導入資安弱點通報機制

111年

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

112年

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

113年

- C級CI提供者完成導入資安弱點通報機制

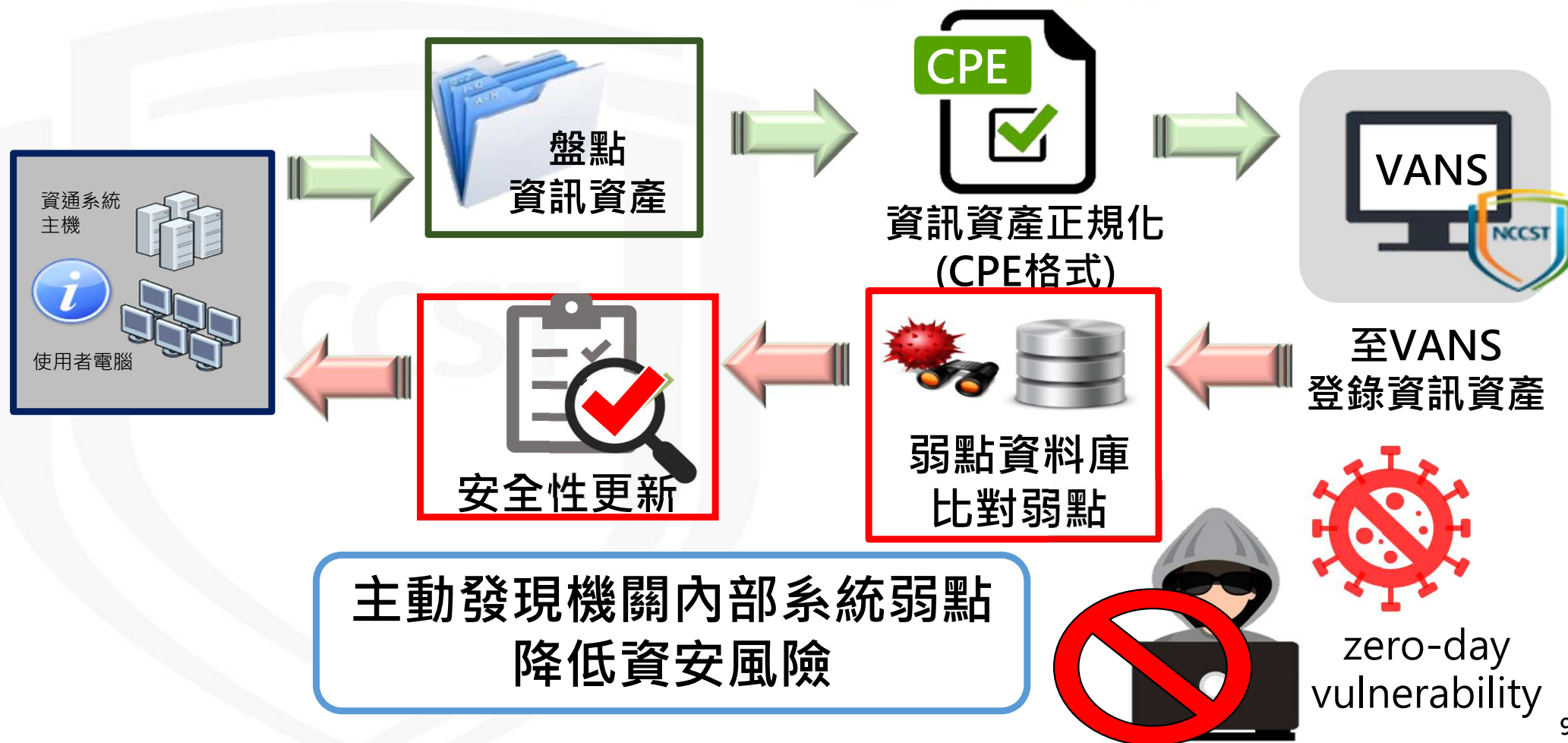
大綱

- 前言
- 政府機關資安弱點通報機制介紹
- 政府機關資安弱點通報系統介紹
- 後續推動重點

NCCST

機制介紹(1/2)

- 政府機關資安弱點通報機制(Vulnerability Alert and Notification System, VANS)結合資訊資產管理與弱點管理，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，並依風險情形完成安全性更新

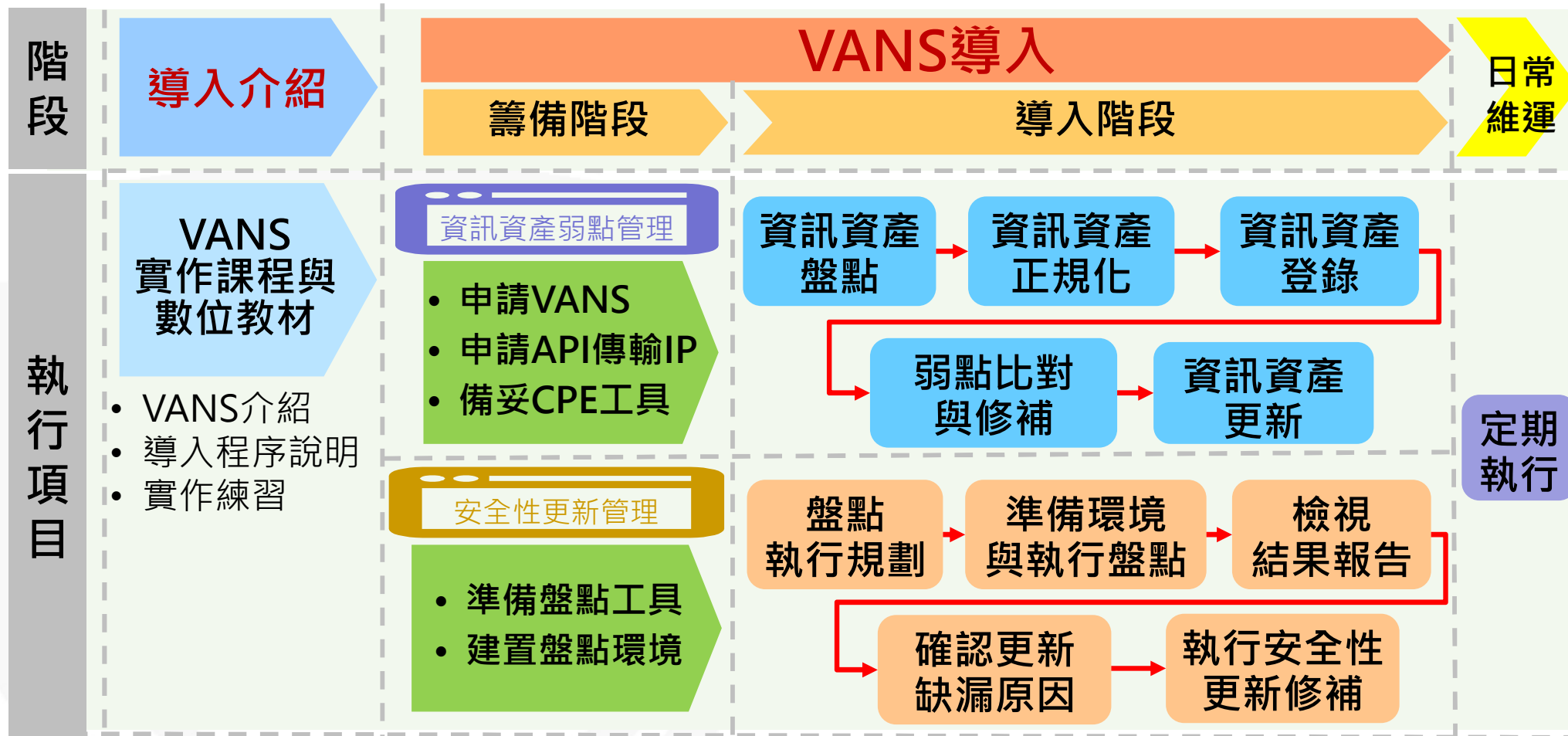


機制介紹(2/2)

- 資訊資產涵蓋範圍



VANS機制導入作業流程



大綱

- 前言
- 政府機關資安弱點通報機制介紹
- 政府機關資安弱點通報系統介紹
 - 系統介紹
 - 功能介紹
 - 作業流程
- 後續推動重點

系統介紹

- 政府機關資安弱點通報系統(簡稱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**掌握資安風險**，以強化資訊資產資安管理

政府機關資安弱點通報系統 (VANS)

[一般權限帳號登入](#) [機關管理者帳號登入](#)

公告

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

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



機關管理者帳號

iAuth個人帳號

密碼

[登入](#) [申請個人帳號](#) [忘記密碼](#)



NVD



資訊資產呈現方式(1/2)

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

弱點呈現方式

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

–CVE-YYYY-NNNNN

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CPE與CVE**資訊

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



大綱

- 前言
- 政府機關資安弱點通報機制介紹
- 政府機關資安弱點通報系統介紹
 - 系統介紹
 - **功能介紹**
 - 作業流程
- 後續推動重點

系統功能

VANS系統

資產管理



- 系統化管理資訊資產
- 下載軟體資產CPE清單
- 登錄資訊資產
- 編輯資訊資產
- 匯出資產報表

弱點管理



- 自動化弱點比對
- 接收弱點通知
- 確認弱點並記錄改善措施
- 回報弱點處理情形
- 掌握安全性更新落實程度
- 登錄已安裝KBID

資訊綜整



- 即時掌握機關弱點分布情形
- 掌握資訊資產受影響狀況

資產管理(1/6)

- 系統化管理資訊資產

– 提供使用者以系統化方式管理Windows平台資通系統
與使用者電腦之資訊資產



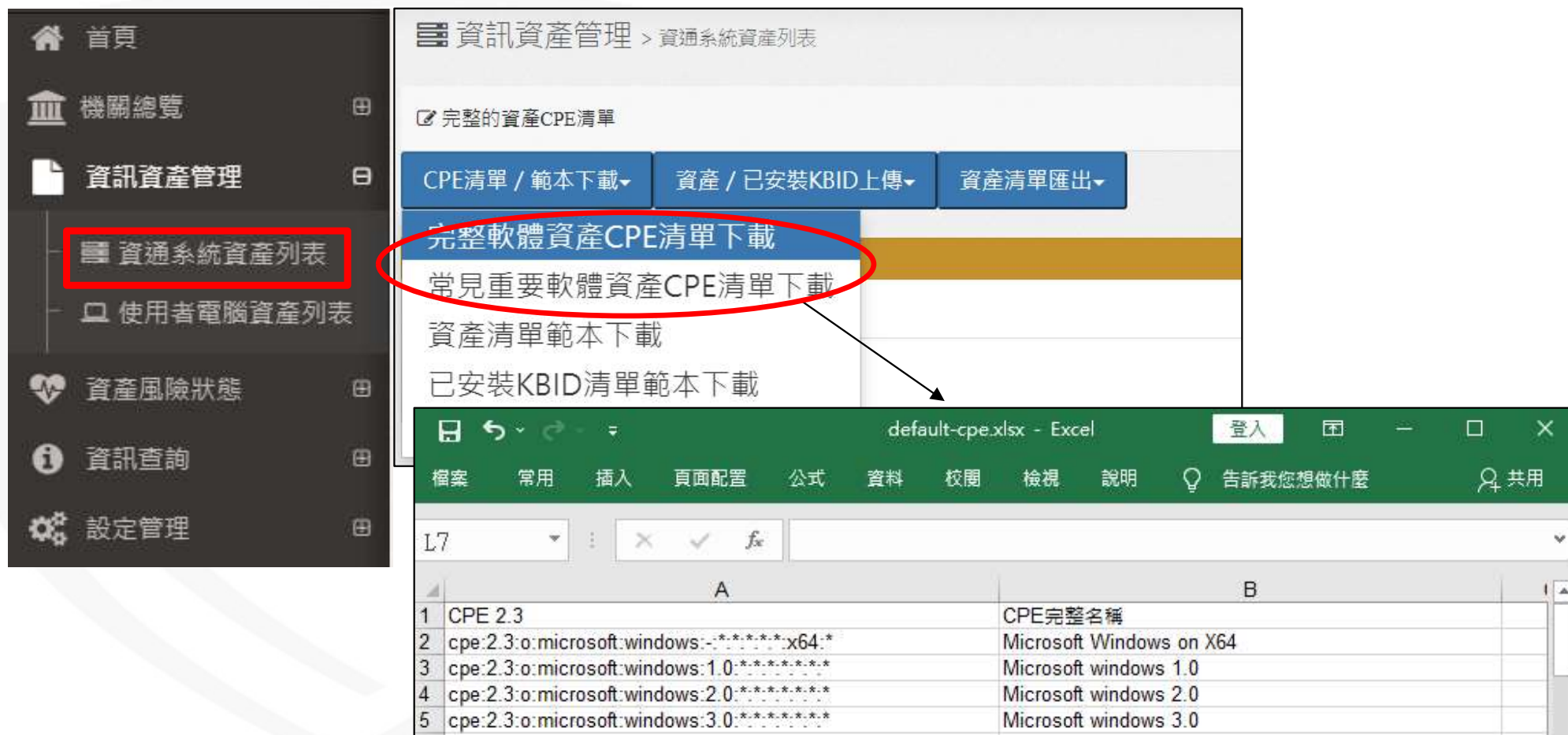
The screenshot displays the '資訊資產管理' (Information Asset Management) system interface. On the left is a dark sidebar with navigation options: 首頁 (Home), 機關總覽 (Organization Overview), 資訊資產管理 (Information Asset Management), 資通系統資產列表 (Communication System Asset List - highlighted with a red box), 使用者電腦資產列表 (User Computer Asset List), 資產風險狀態 (Asset Risk Status), 資訊查詢 (Information Query), and 設定管理 (Settings Management). The main content area shows the '資訊資產列表' (Information Asset List) for '資通系統資產列表' (Communication System Asset List). At the top right, there is a search bar and a dropdown menu. Below the header, there are three blue buttons: 'CPE清單 / 範本下載' (CPE List / Template Download), '資產 / 已安裝KBID上傳' (Asset / Installed KBID Upload), and '資產清單匯出' (Export Asset List). A red button on the right says '切換至已安裝KBID列表' (Switch to Installed KBID List). The main table lists assets with columns for '資產名稱' (Asset Name), '資產廠商' (Asset Manufacturer), '資產版本' (Asset Version), 'CPE2.3', '資產數量' (Asset Quantity), '編輯' (Edit), and '刪除' (Delete). The table contains three entries:

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	編輯	刪除
Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	8.0.30	cpe:2.3:a:apache:tomcat:8.0.30:*:*:*:*:*	1	編輯	刪除
Apache Tomcat 9.0 Tomcat9 (remove only)	The Apache Software Foundation	9.0.16	N/A	1	編輯	刪除
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beanutils:1.8.0:*:*:*:*:*	1	編輯	刪除

資產管理(2/6)

- 下載軟體資產CPE清單

–VANS系統每日與NVD更新「完整軟體資產CPE清單」，供機關查閱軟體資產CPE格式



資訊資產管理 > 資通系統資產列表

完整的資產CPE清單

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

完整軟體資產CPE清單下載

常見重要軟體資產CPE清單下載

資產清單範本下載

已安裝KBID清單範本下載

default-cpe.xlsx - Excel

	A	B
1	CPE 2.3	CPE完整名稱
2	cpe:2.3:o:microsoft:windows:-:*:*:*:*:x64:*	Microsoft Windows on X64
3	cpe:2.3:o:microsoft:windows:1.0:*:*:*:*:*	Microsoft windows 1.0
4	cpe:2.3:o:microsoft:windows:2.0:*:*:*:*:*	Microsoft windows 2.0
5	cpe:2.3:o:microsoft:windows:3.0:*:*:*:*:*	Microsoft windows 3.0

資產管理(3/6)

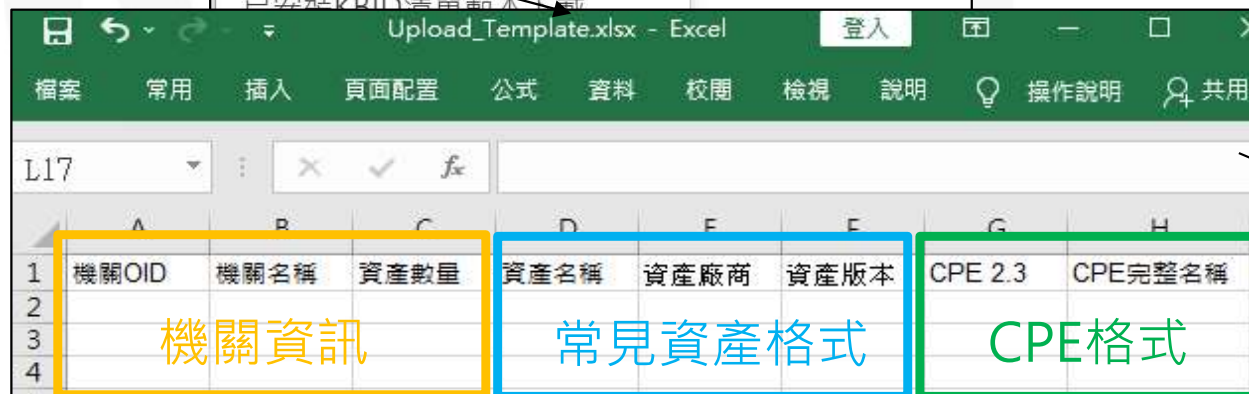
● 登錄資訊資產(網頁上傳)

– 提供資產清單範本，填寫常見資產格式與CPE格式

➢ 常見格式：便於使用者檢視與管理資產

➢ CPE格式：VANS系統進行弱點比對用

– 可透過網頁上傳資訊資產，選取填寫完成之資產清單，並以覆蓋方式上傳至VANS系統

Upload_Template.xlsx - Excel

1	機關OID	機關名稱	資產數量	資產名稱	資產廠商	資產版本	CPE 2.3	CPE完整名稱
2								
3								
4								

機關資訊 (highlighted in yellow)

常見資產格式 (highlighted in blue)

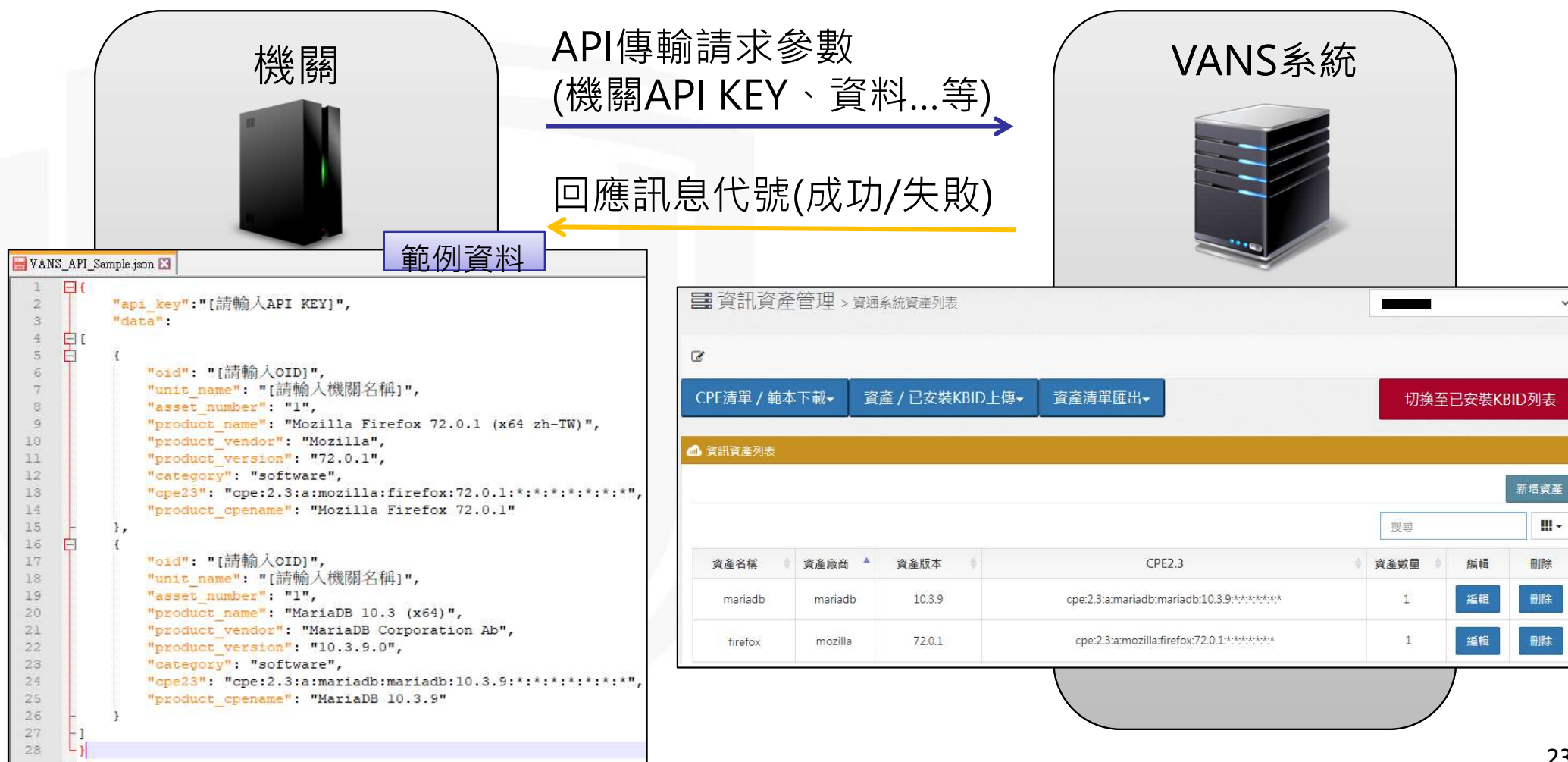
CPE格式 (highlighted in green)



資產管理(4/6)

● 登錄資訊資產(API介接)

– 可申請開通以採用API介接功能上傳資訊資產



資產管理(5/6)

● 編輯資訊資產

– 提供網頁編輯資訊資產之功能，方便使用者於VANS系統上進行資產新增、修改及刪除



資訊資產管理 > 資通系統資產列表

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

資訊資產列表

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	編輯	刪除
Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	8.0.30	cpe:2.3:a:apache:tomcat:8.0.30:*****	1	編輯	刪除

更新資產

廠商: apache

產品: tomcat

版本: 8.0.30

更新: *

版次: *

資產數量: 1

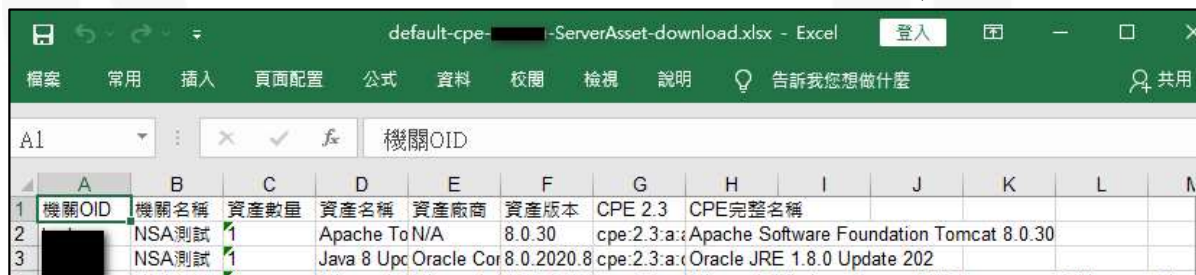
更新資產

取消

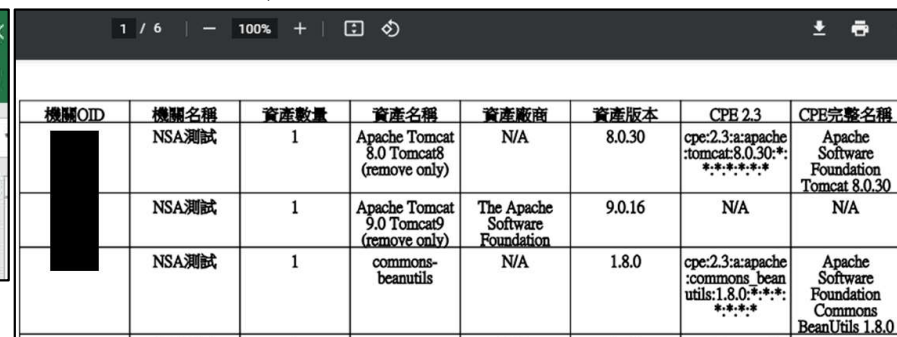
資產管理(6/6)

● 匯出資產報表

- 以Excel格式匯出已登錄VANS系統之資訊資產，便於使用者更新資訊資產後，再透過Excel上傳至VANS系統
- 以PDF格式匯出已登錄VANS系統之資訊資產

機關OID	機關名稱	資產數量	資產名稱	資產廠商	資產版本	CPE 2.3	CPE完整名稱
	NSA測試	1	Apache To	N/A	8.0.30	cpe:2.3:a:apache	Apache Software Foundation Tomcat 8.0.30
	NSA測試	1	Java 8 Upc	Oracle Cor	8.0.2020.8	cpe:2.3:a:oracle	Oracle JRE 1.8.0 Update 202



機關OID	機關名稱	資產數量	資產名稱	資產廠商	資產版本	CPE 2.3	CPE完整名稱
	NSA測試	1	Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	8.0.30	cpe:2.3:a:apache:tomcat:8.0.30:*:*:*:*	Apache Software Foundation Tomcat 8.0.30
	NSA測試	1	Apache Tomcat 9.0 Tomcat9 (remove only)	The Apache Software Foundation	9.0.16	N/A	N/A
	NSA測試	1	commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons-beanutils:1.8.0:*:*:*:*	Apache Software Foundation Commons BeanUtils 1.8.0

弱點管理(1/11)

● 自動化弱點比對

– 針對已登錄之資訊資產，以自動化方式進行弱點比對



資產風險狀態 > 資通系統風險狀態 > 資訊資產風險列表

[下載弱點清單](#)
[上傳弱點改善措施](#)
全部
██████

資訊

搜尋 ☰

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	風險指數	弱點數量	未填寫改善措施數量	弱點資訊
Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	8.0.30	cpe:2.3:a:apache:tomcat:8.0.30:*:*:*:*:*	1	5.63	25	17	詳細資訊
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beanutils:1.8.0:*:*:*:*:*	1	7.50	2	2	詳細資訊

弱點管理(2/11)

● 接收弱點通知

- 若比對出新的弱點，即會進行弱點通知
- 管理者可透過Email接收弱點通知

- 🏠 首頁
- 🏢 機關總覽
- 📁 資訊資產管理
- 📊 資產風險狀態
- 🚨 資通系統風險狀態
- 🛡️ 資訊資產風險列表
- 👥 弱點關聯列表
- 🔔 弱點比對通知
- 📈 弱點處理情形回報
- ⚠️ 使用者電腦風險狀態
- 🔍 資訊查詢
- ⚙️ 設定管理

🔔 資產風險狀態 > 資通系統風險狀態 > 弱點比對通知

弱點通知列表

通知時間	資產數量	弱點數量	詳細資訊	
2021-05-27 14:30:49	1	1096	開啟	匯出勾選弱點通知 全選
2021-05-21 17:15:45	1	1	開啟	
2021-05-19 09:10:52	1	26	開啟	

顯示第 1 到第 3 項記錄，總共 3 項記錄

VANS <vans@nccst.nat.gov.tw>
[VANS] 資通系統資訊資產風險項目通知

敬啟者 您好：
此為「政府機關資安弱點通報系統」之通知郵件。

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

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

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

弱點管理(3/11)

- 確認弱點並記錄改善措施
 - 檢視資訊資產存在之CVE弱點
 - 針對各CVE弱點進行改善措施填寫



The screenshot displays the 'Asset Risk Status' (資產風險狀態) interface. The left sidebar contains navigation options, with '資訊資產風險列表' (Information Asset Risk List) highlighted in red. The main content area shows a table of assets with columns for name, vendor, version, CPE2.3, quantity, risk index, number of vulnerabilities, and number of unrecorded improvement measures. Two rows are visible: Apache Tomcat 8.0 and commons-beanutils. The '詳細資訊' (Detailed Information) button for the Apache Tomcat entry is circled in red. Below this, a modal window titled '詳細資訊' (Detailed Information) is open, showing a table of CVE vulnerabilities. The '填寫改善措施' (Record Improvement Measure) button for CVE-2016-3092 is circled in red.

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	風險指數	弱點數量	未填寫改善措施數量	弱點資訊
Apache Tomcat 8.0 Tomcat8 (remove only)	N/A	8.0.30	cpe:2.3:a:apache:tomcat:8.0.30:****:*	1	5.63	25	17	詳細資訊
commons-beanutils	N/A	1.8.0	cpe:2.3:a:apache:commons_beanutils:1.8.0:****:*	1	7.50	2	2	詳細資訊

	CVE編號	CVSS	發佈時間	更新時間	改善措施
<input type="checkbox"/>	CVE-2016-3092	7.8	2016-07-05 06:59:00	2019-04-24 03:29:00	填寫改善措施
<input type="checkbox"/>	CVE-2018-8014	7.5	2018-05-17 00:29:00	2019-10-03 08:03:00	填寫改善措施

弱點管理(4/11)

● 安全性更新落實程度

– 針對微軟類資產，透過安全性更新修補之弱點，檢視電腦是否有應安裝但未安裝之更新

- 🏠 首頁
- 🏢 機關總覽
- 📄 資訊資產管理
- 📊 資產風險狀態
- ⚠️ 資通系統風險狀態
- 🛡️ 資訊資產風險列表
- 👤 弱點關聯列表
- 🔔 弱點比對通知
- 🔄 弱點處理情形回報
- 👤 使用者電腦風險狀態
- 🔍 資訊查詢
- ⚙️ 設定管理

詳細資訊

填寫勾選改善措施 全部勾選 全部取消

顯示已修補之弱點 on

	CVE編號	CVSS	發佈時間	更新時間	改善措施	查看修補KBID
<input type="checkbox"/>	CVE-2021-31205	4.3	2021-05-12 03:15:00	2021-05-19 03:50:00	填寫改善措施	1/10
<input type="checkbox"/>	CVE-2021-31194	6.5	2021-05-12 03:15:00	2021-05-18 03:41:00	填寫改善措施	1/10
<input type="checkbox"/>	CVE-2021-31193					
<input type="checkbox"/>	CVE-2021-31192					
<input type="checkbox"/>	CVE-2021-31191					

KBID資訊

搜尋

KBID	數量	受影響產品名稱
KB5003173	1	詳細清單

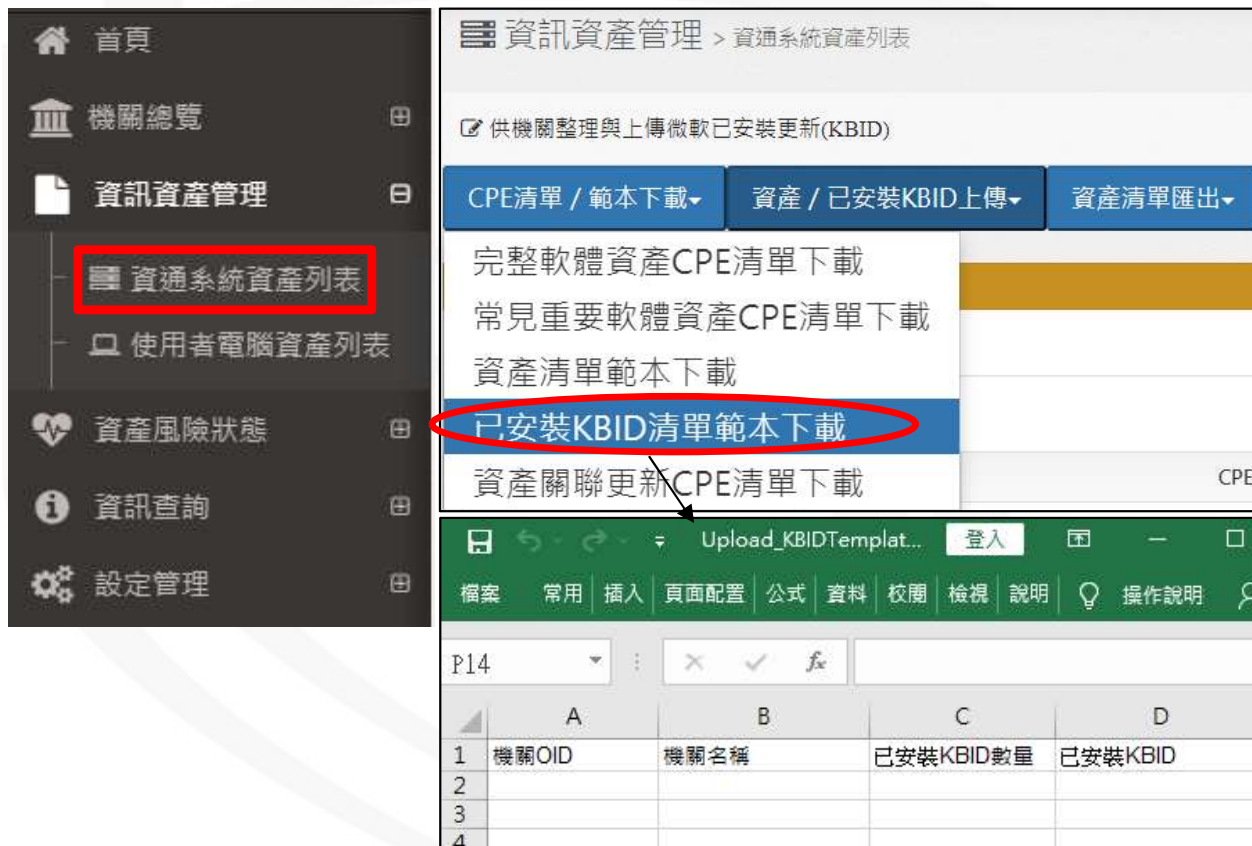
顯示第 1 到第 1 項記錄，總共 1 項記錄

關閉

弱點管理(5/11)

● 登錄已安裝KBID(網頁上傳)

- 提供已安裝KBID清單範本，彙整並填寫已安裝KBID
- 透過網頁上傳已安裝KBID，選取填寫完成之已安裝KBID清單，並以覆蓋方式上傳至VANS系統



資訊資產管理 > 資通系統資產列表

供機關整理與上傳微軟已安裝更新(KBID)

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

完整軟體資產CPE清單下載

常見重要軟體資產CPE清單下載

資產清單範本下載

已安裝KBID清單範本下載

資產關聯更新CPE清單下載

Upload_KBIDTemplat...

檔案 常用 插入 頁面配置 公式 資料 校閱 檢視 說明 操作說明

	A	B	C	D
1	機關OID	機關名稱	已安裝KBID數量	已安裝KBID
2				
3				
4				



資訊資產管理 > 資通系統資產列表

上傳資通系統已安裝KBID清單

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

資訊資產列表

資產清單上傳

已安裝KBID清單上傳



資訊資產管理 > 資通系統資產列表 > 已安裝KBID清單上傳

已安裝KBID清單上傳

選擇檔案 未選擇任何檔案

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

上傳

弱點管理(6/11)

- 登錄已安裝KBID(API介接)

– 可申請開通以透過API介接功能上傳已安裝KBID

機關



API傳輸請求參數
(機關API KEY、資料...等)

回應訊息代號(成功/失敗)

VANS系統



範例資料

```
VANS_KBID_Sample.json
1 {
2   "api_key": "[請輸入API KEY]",
3   "data":
4   [
5     {
6       "oid": "[請輸入OID]",
7       "unit_name": "請輸入機關名稱",
8       "kbid_number": "99",
9       "kbid": "KB4565489"
10    },
11    {
12      "oid": "[請輸入OID]",
13      "unit_name": "請輸入機關名稱",
14      "kbid_number": "123",
15      "kbid": "KB4565503"
16    }
17  ]
18 }
```

資訊資產管理 > 資訊系統資產列表

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

已安裝KBID列表

KBID	數量	受影響產品名稱	刪除
KB4565503	123	詳細清單	刪除
KB4565489	99	詳細清單	刪除

弱點管理(7/11)

- 回報弱點處理情形

– 技服中心設定須回報之重大弱點後，使用者可透過本功能查看受影響之各項弱點詳細資訊，並針對未回報之弱點選擇處理方式



資產風險狀態 > 資通系統風險狀態 > 弱點處理情形回報

弱點編號
弱點編號

開始時間*
2018-12-01

結束時間*
2021-01-11

弱點狀態*
未回報

查詢

搜尋

弱點編號	CVSS Score	發布時間	更新時間	個別回報	一次性回報
CVE-2019-1000011	5.5	2019/02/05 05:29:00	2020/08/25 01:37:00	個別回報	填寫改善措施

弱點管理(8/11)

- 弱點狀態：未回報

– 若需個別填寫不同資產修補方式，則可選擇**個別回報**，並依處理方式選擇「填寫改善措施」或「版本更新」

弱點狀態*

未回報

查詢

搜尋

弱點編號	CVSS Score	發布時間	更新時間	個別回報	一次性回報
CVE-2019-1000011	5.5	2019/02/05 05:29:00	2020/08/25 01:37:00	個別回報	填寫改善措施

資產風險狀態 > 資通系統風險狀態 > 弱點處理情形回報 > 個別回報

搜尋

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	個別回報
core	api-platform	2.2.3	cpe:2.3:a:api-platform:core:2.2.3:*:*:*:*:*	21	填寫改善措施 版本更新
core	api-platform	2.2.4	cpe:2.3:a:api-platform:core:2.2.4:*:*:*:*:*	22	填寫改善措施 版本更新

弱點管理(9/11)

- 弱點狀態：未回報

–若同一弱點為非透過版本更新方式修補，而是採用相同修補方式，則可選擇**一次性回報**之「填寫改善措施」功能批次進行填寫



The screenshot displays a web interface for vulnerability management. At the top, there is a dropdown menu for '弱點狀態*' (Vulnerability Status) set to '未回報' (Not Reported). Below this is a search bar with the text '搜尋' and a '查詢' (Search) button. A table lists vulnerabilities with columns: '弱點編號' (Vulnerability ID), 'CVSS Score', '發布時間' (Release Time), '更新時間' (Update Time), '個別回報' (Individual Report), and '一次性回報' (One-time Report). The first row shows 'CVE-2019-1000011' with a CVSS Score of 5.5, released on 2019/02/05 05:29:00, and updated on 2020/08/25 01:37:00. The '個別回報' button is red, and the '填寫改善措施' (Fill Improvement Measures) button is circled in red. A modal window titled '填寫改善措施' (Fill Improvement Measures) is open, showing a checkbox for '填寫改善措施' (Fill Improvement Measures) and a large text input area. A '送出' (Submit) button is at the bottom of the modal.

弱點編號	CVSS Score	發布時間	更新時間	個別回報	一次性回報
CVE-2019-1000011	5.5	2019/02/05 05:29:00	2020/08/25 01:37:00	個別回報	填寫改善措施

弱點管理(10/11)

- 弱點狀態：已填寫改善措施

– 針對已填寫改善措施之弱點，可檢視與修改已填寫之改善措施

弱點狀態*

已填寫改善措施

查詢

搜尋

弱點編號	CVSS Score	發布時間	更新時間	改善措施	版本更新
CVE-2019-100011	5.5	2019/02/05 05:29:00	2020/08/25 01:37:00	查看改善措施	版本更新

改善措施詳細資訊

資產名稱	資產廠商	資產版本	CPE2.3	資產數量	改善措施	修改改善措施
core	api-platform	2.2.0	cpe:2.3:a:api-platform:core:2.2.0:*:*:*:*:*	18	預計3/1完成資產下線	修改改善措施

✓ 關閉

弱點管理(11/11)

- 弱點狀態：已排除

– 針對透過資產刪除或版本更新進行修補之弱點，可分別檢視資產刪除紀錄與版本更新紀錄

弱點狀態*
已排除

查詢

搜尋

弱點編號	CVSS Score	發布時間	更新時間	資產刪除	資產更新
CVE-2019-100011	5.5	2019/02/05 05:29:00	2020/08/25 01:37:00	資產刪除紀錄	版本更新紀錄

資產版本更新紀錄

更新前					更新後				
資產名稱	資產廠商	資產版本	CPE2.3	資產數量	資產名稱	資產廠商	資產版本	CPE2.3	資產數量
core	api-platform	2.2.1	cpe:2.3:a:api-platform:core:2.2.1:****:*	19	core	api-platform	2.3.8	N/A	19

資產版本更新紀錄

更新前					更新後				
資產名稱	資產廠商	資產版本	CPE2.3	資產數量	資產名稱	資產廠商	資產版本	CPE2.3	資產數量
core	api-platform	2.2.2	cpe:2.3:a:api-platform:core:2.2.2:****:*	20	資產刪除				

資訊綜整(1/2)

- 即時掌握機關弱點分布情形

- 圖形化呈現資訊資產弱點分布概要統計圖，供機關掌握資訊資產弱點防護情形



資訊綜整(2/2)

● 掌握資訊資產受影響狀況

– 檢視機關與所屬機關之資產登錄，以掌握各機關資產更新情形與受影響之CVE種類數



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

機關總覽 > 機關列表

搜尋 ☰

機關名稱	機關資通安全責任等級	CVE種類數	最後上傳時間
機關A	A	2598	2021-06-03 16:21:17 網頁上傳
機關B	B	40	2021-05-31 10:40:21 API上傳
機關C	A	0	2016-10-11 17:44:33 網頁上傳
機關D	D	0	2019-03-08 11:58:21 網頁上傳

機關總覽 > 機關列表 > 弱點總覽

返回上一頁

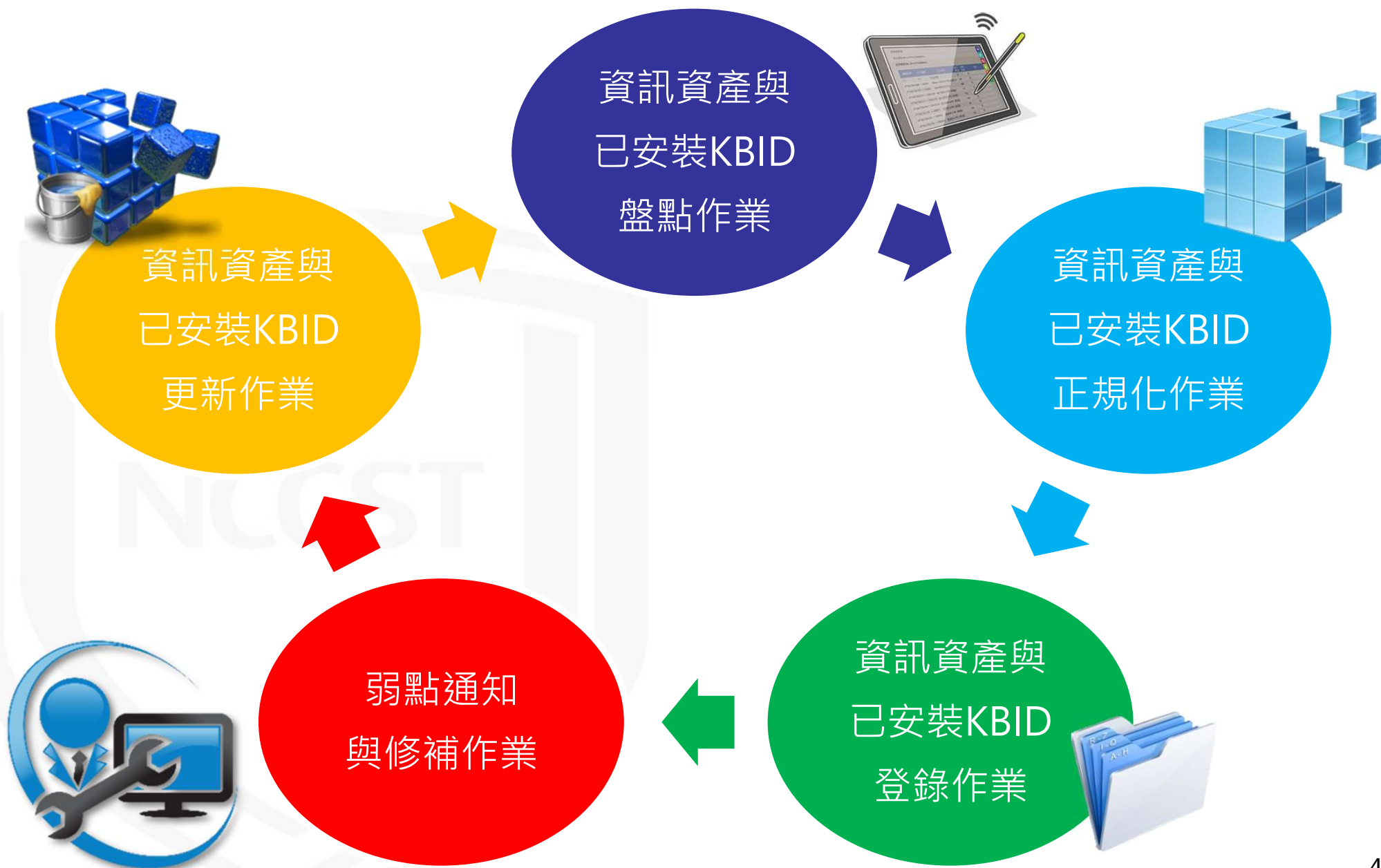
【 機關A 】

CVE種類數	伺服器主機	使用者電腦	總計
非微軟類	69	16	85
微軟類	1456	1285	2741
總計	1525	1301	2826

大綱

- 前言
- 政府機關資安弱點通報機制介紹
- 政府機關資安弱點通報系統介紹
 - 系統介紹
 - 功能介紹
 - **作業流程**
- 後續推動重點

導入作業流程



資訊資產與已安裝KBID盤點(1/2)

- 蒐集範圍：Windows平台資通系統與使用者電腦之軟體資產



應用程式

應用程式或網站伺服器

網站採用第三方元件

資料庫

程式語言執行環境

開發框架



作業系統

Windows Server



Windows



安全性更新

Windows Server

Windows



- 軟體名稱
- 開發廠商名稱

- 版本資訊
- 軟體安裝數量

- KBID編號
- KBID安裝數量

資訊資產與已安裝KBID盤點(2/2)

- 可透過自動化工具或系統內建工具，盤點資訊資產與已安裝KBID，並產出盤點清單

資訊資產盤點方式

透過自動化工具
盤點資訊資產



透過reg query
盤點資訊資產



產出



作業系統資料



軟體資產資料

KBID盤點方式

透過自動化工具
盤點已安裝KBID



透過WMIC盤
點已安裝KBID



產出



已安裝KBID資料

資訊資產與已安裝KBID正規化

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



作業系統資料



軟體資產資料



已安裝KBID資料

資訊資產正規化方式

透過自動化工具彙整為全機關資訊資產資料

透過Excel彙整為全機關資訊資產資料

透過自動化工具進行CPE轉換

透過完整軟體資產CPE清單進行CPE轉換

產出



CPE格式資產清單

已安裝KBID正規化方式

透過自動化工具彙整為全機關KBID資料

透過Excel彙整為全機關KBID資料

產出



已安裝KBID清單

資訊資產與已安裝KBID登錄

- 透過廠商工具或網頁方式，將CPE格式資訊資產清單與已安裝KBID清單登錄至VANS系統



CPE格式資產清單



資訊資產登錄方式

透過自動化工具
以API方式登錄

透過網頁以手動
方式登錄CPE格
式資訊資產清單

透過自動化工具
以網頁方式登錄

產出

VANS系統資訊資產列表



已安裝KBID清單



已安裝KBID登錄方式

透過自動化工具
以API方式登錄

透過網頁以手動
方式登錄已安裝
KBID清單

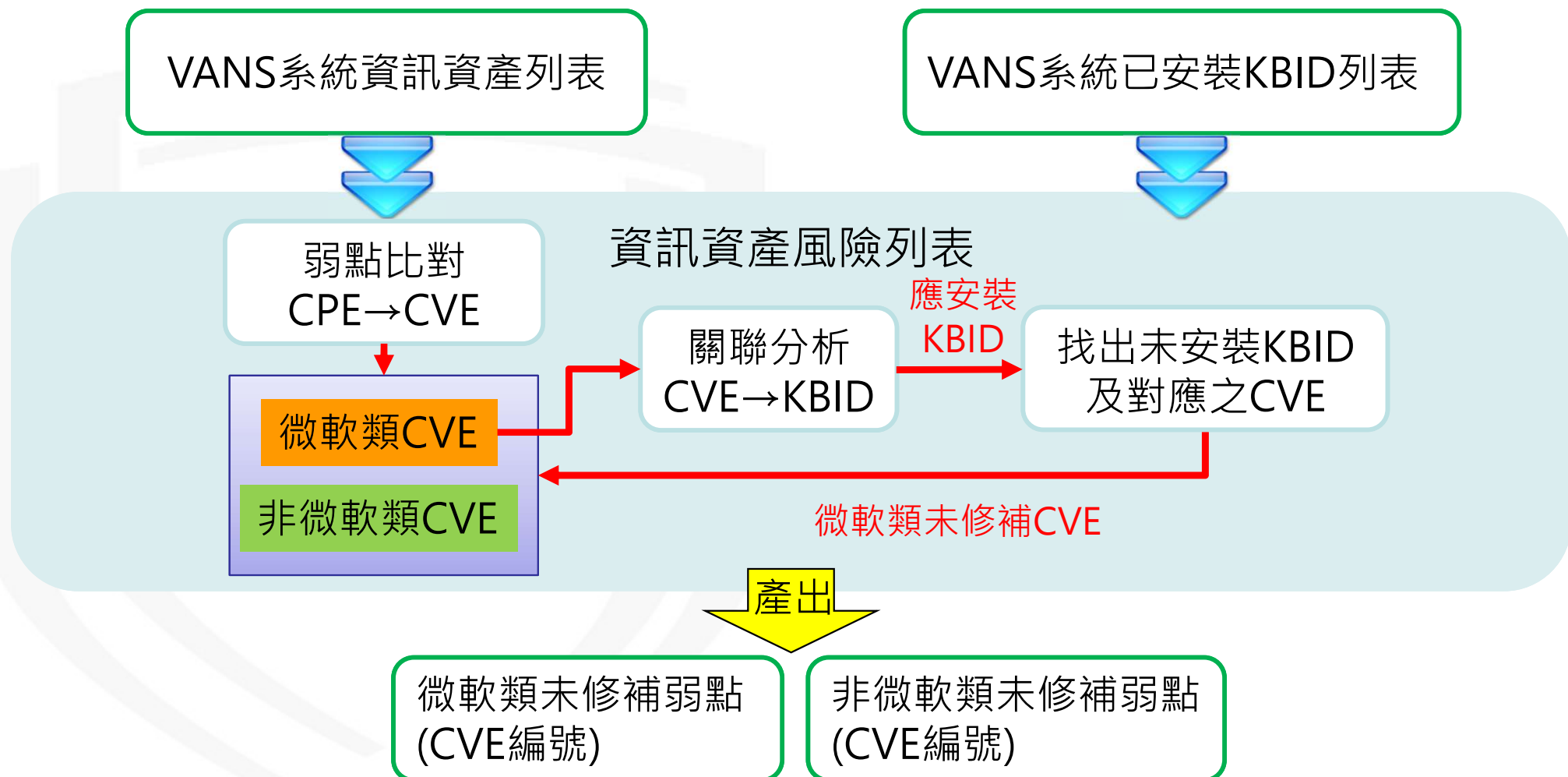
透過自動化工具
以網頁方式登錄

產出

VANS系統已安裝KBID列表

弱點通知與修補(1/2)

- VANS系統將自動比對機關登錄之資訊資產與已安裝KBID，並將結果顯示於資訊資產風險列表



弱點通知與修補(2/2)

- 機關可依據ISMS規範之弱點修補基準，執行弱點評估與修補

微軟類未修補弱點
(CVE編號)

非微軟類未修補弱點
(CVE編號)



弱點通知



弱點評估與修補

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？

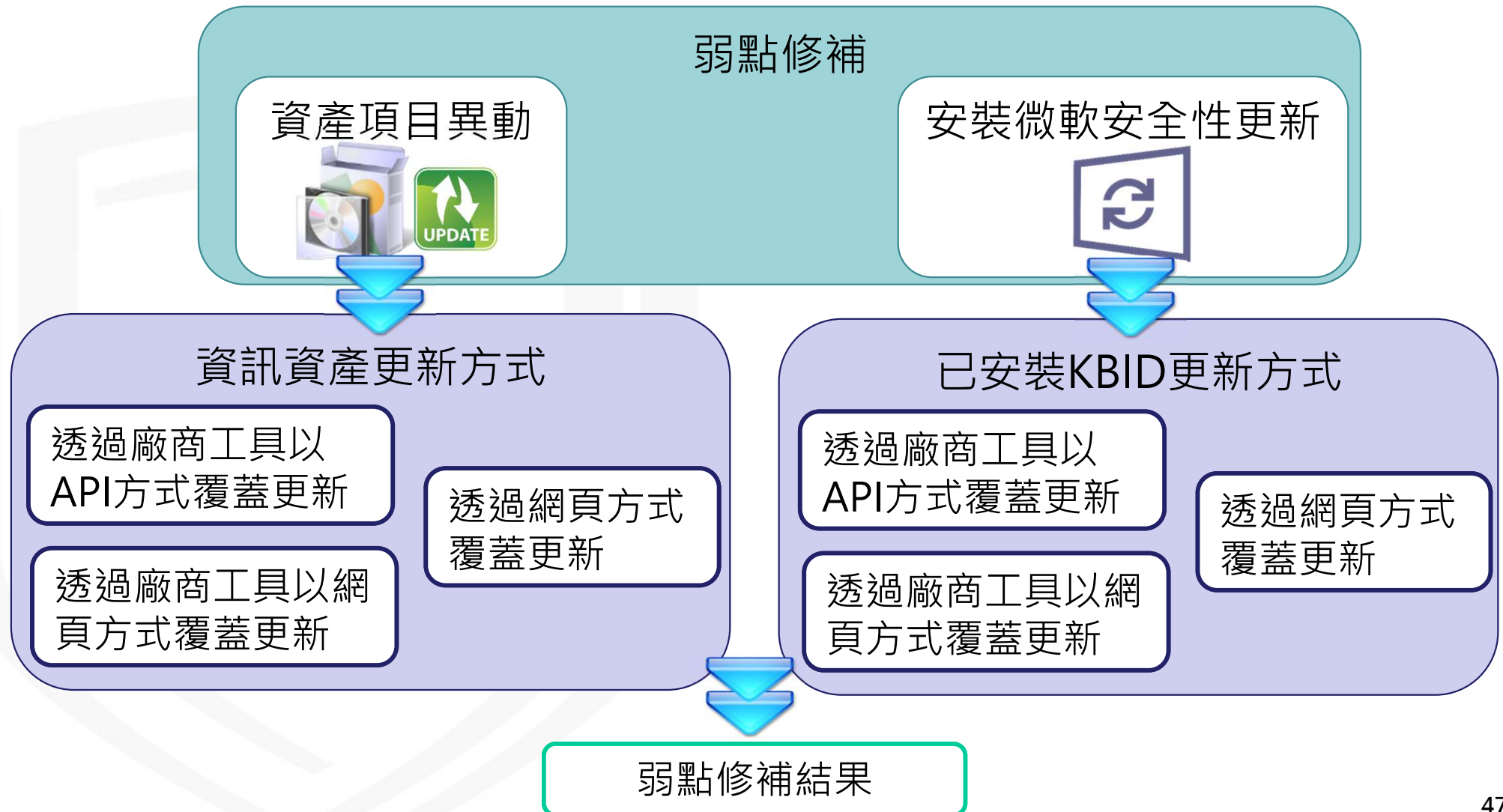


預定修補時程？



資訊資產與已安裝KBID更新

- 完成弱點修補，並至VANS系統更新資產與已安裝KBID資料後，系統再次進行弱點比對，呈現弱點修補結果



大綱

- 前言
- 政府機關資安弱點通報機制介紹
- 政府機關資安弱點通報系統介紹
- 後續推動重點

NCCST

後續推動重點

- VANS系統歷經試辦導入作業、推廣說明會、資安服務團等施行後，已依機關反映與建議精進強化
- VANS機制日趨完備，且**納入法遵要求**，後續將持續**協助A級、B級及C級之公務機關與CI提供者完成導入**，以期透過VANS系統進一步強化政府機關資訊資產之資安管理



報告完畢
敬請指教

NCCST