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

政府組態基準(GCB)實作文件
Windows Server 2022

國家資通安全研究院

簡報大綱

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

- 發展緣由
- 發展目的
- 政府組態基準說明
- 資安防護情境
- 政府組態基準部署實作
- 參考資料

發展緣由

- 自102年起，我國逐步發展與推廣使用者電腦與伺服器主機之政府組態基準(Government Configuration Baseline，簡稱GCB)
- 111年針對機關環境常用之Windows Server 2022著手發展組態基準設定，並於112年公告周知，期望藉由提供電腦作業環境一致性資安防護基準與實作指引，供政府機關透過建立安全組態，提升資安防護能力

發展目的

- 發展Windows Server 2022組態基準設定之目的，在於規範機關內Windows Server 2022作業系統之一致性安全設定(如密碼最小長度)，以降低成為駭客入侵管道，進而引發資安事件之風險

1 發展一致性安全組態設定

2 提升作業系統使用安全性

政府組態基準說明

政府組態基準適用環境與項數統計(1/2)

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

- 適用環境
  - 微軟公司所發行之Windows Server 2022作業系統
- 項數統計
  - Windows Server 2022 GCB須部署之基本項目，包含Account Settings與Common Settings共計323項設定項目，項目統計如下：

基本項目GPO

項次	GPO名稱	項數	小計
1	Windows Server 2022 Account Settings	9	323
2	Windows Server 2022 Common Settings	314	
3	Windows Server 2022 DC Server	29	29
4	Windows Server 2022 DNS Server	115	115
5	Windows Server 2022 File Server	120	120
6	Windows Server 2022 Web Server	117	117

政府組態基準適用環境與項數統計(2/2)

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

–基本項目部署完成後，再依系統所安裝使用之**伺服器角色**，額外部署相對應之組態基準設定，包含**網域控制站**(以下簡稱**DC Server**)組態基準29項設定項目、**DNS Server**組態基準115項設定項目、**File Server**組態基準120項設定項目及**Web Server**組態基準117項設定項目，項目統計如下

項次	GPO名稱	項數	小計
1	Windows Server 2022 Account Settings	9	323
2	Windows Server 2022 Common Settings	314	
3	Windows Server 2022 DC Server	29	29
4	Windows Server 2022 DNS Server	115	115
5	Windows Server 2022 File Server	120	120
6	Windows Server 2022 Web Server	117	117

伺服器角色專用GPO

資安防護情境

資安防護情境-1

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

資安案例

駭客透過遙控程式使用RDP(Windows遠端桌面程式)發動攻擊，並針對資料庫檔案加密，要求贖金解碼，造成網站內容無法開啟，系統服務中斷

Windows Server 2022 GCB設定

- **TWGCB-01-011-0062**
  帳戶：重新命名系統管理員帳戶：
  變更系統內建之Administrator帳戶名稱，降低被駭客猜測到具特殊權限之使用者名稱與通行碼組合之機率
- **TWGCB-01-011-0108 拒絕透過遠端桌面服務登入：**
  拒絕Guests群組與本機帳戶登入，確保只有被授權之管理者帳戶才能使用遠端桌面服務登入主機
- **TWGCB-01-011-0117 允許透過遠端桌面服務登入：**
  僅允許管理者之Administrators群組進行登入

資安防護情境-2

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

資安案例

鎖定畫面可顯示背景執行之應用程式狀態與通知，當管理者離開伺服器主機，系統進入鎖定畫面時，可能會因應用程式通知而洩露資訊

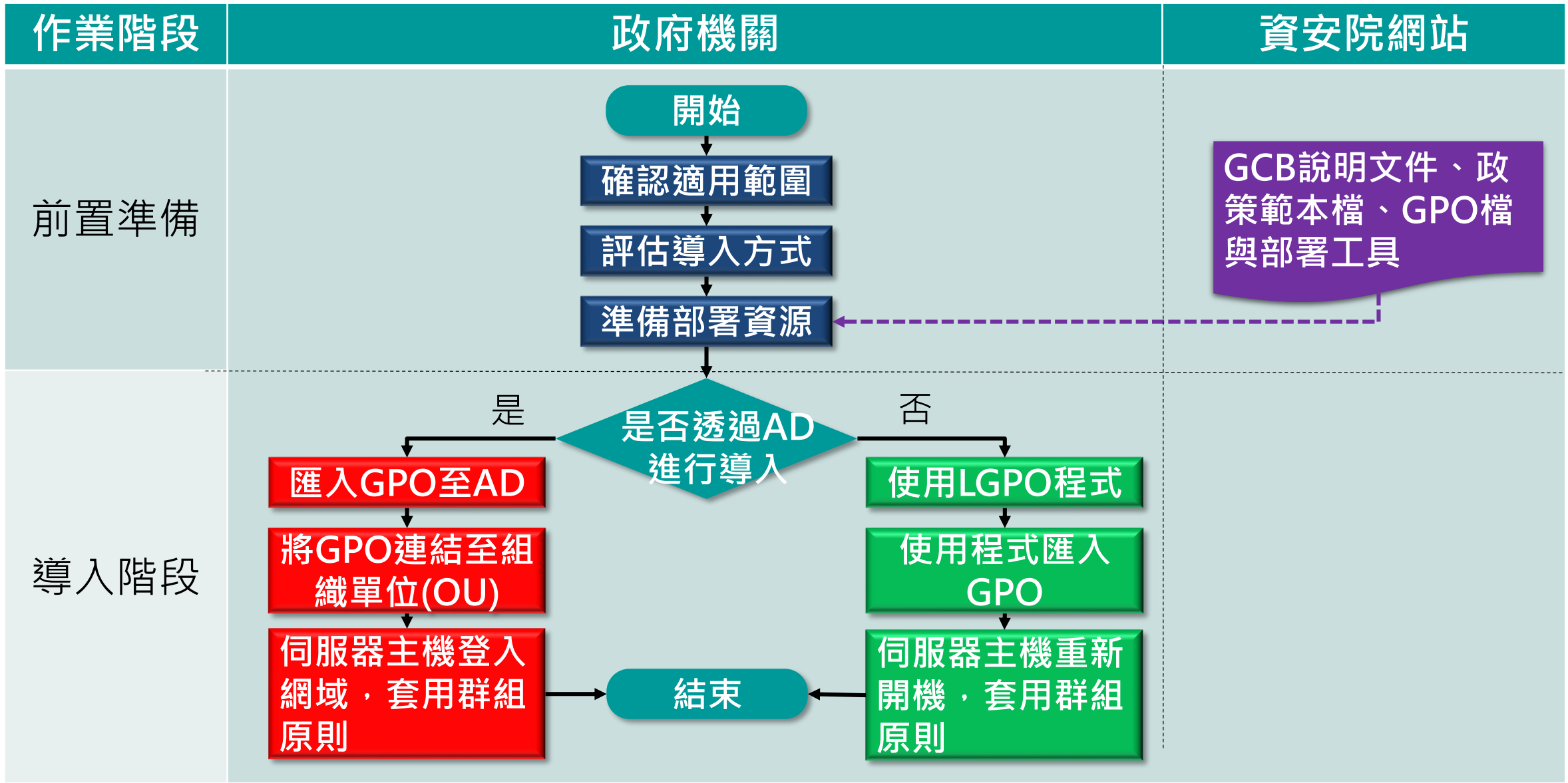
Windows Server 2022 GCB設定

- **TWGCB-01-011-0173 關閉鎖定畫面上的應用程式通知：**
  禁止鎖定畫面上應用程式之啟動與通知，避免因鎖定畫面之應用程式，而導致敏感商務或個人資料洩露
- **TWGCB-01-011-0187 防止啟用鎖定畫面投影片放映：**
  停止「電腦設定」中鎖定畫面投影片放映設定，並防止在鎖定畫面上播放投影片放映，避免從登錄使用者的圖片資料夾中所顯示潛在的敏感資訊而導致資訊洩漏

政府組態基準部署實作

部署流程

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



1.前置作業

1.1 安裝SecGuide系統管理範本

安裝SecGuide系統管理範本(1/6)

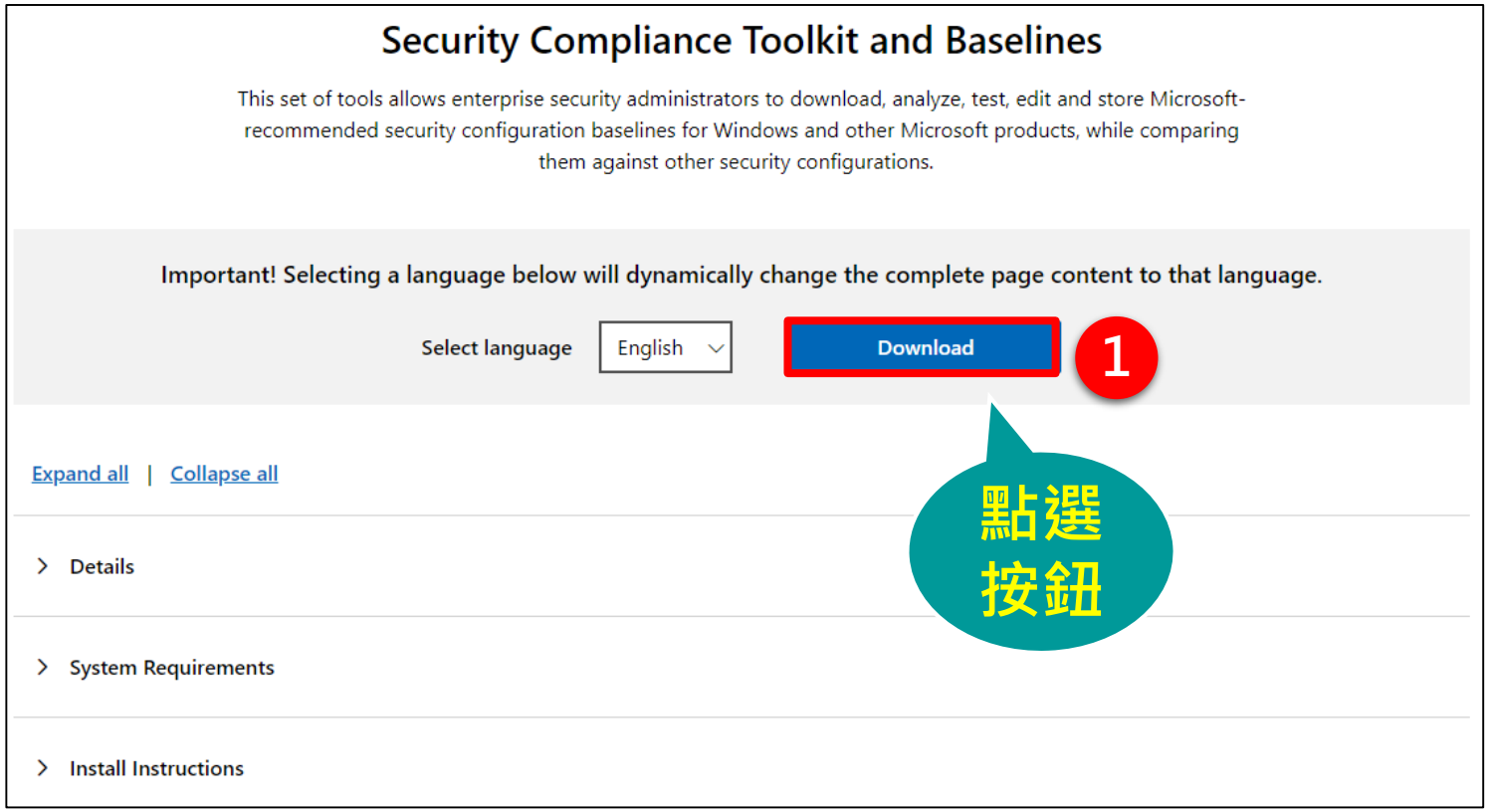
國家資通安全研究院
National Institute of Cyber Security

- SecGuide系統管理範本
  - 若須於本機群組原則編輯器(Gpedit.msc)或群組原則管理(Gpmc.msc)等工具中顯示「Configure SMB v1 client driver」、「Configure SMB v1 server」及「Enable Structured Exception Handling Overwrite Protection (SEHOP)」群組原則設定，須安裝SecGuide系統管理範本

安裝SecGuide系統管理範本(2/6)

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

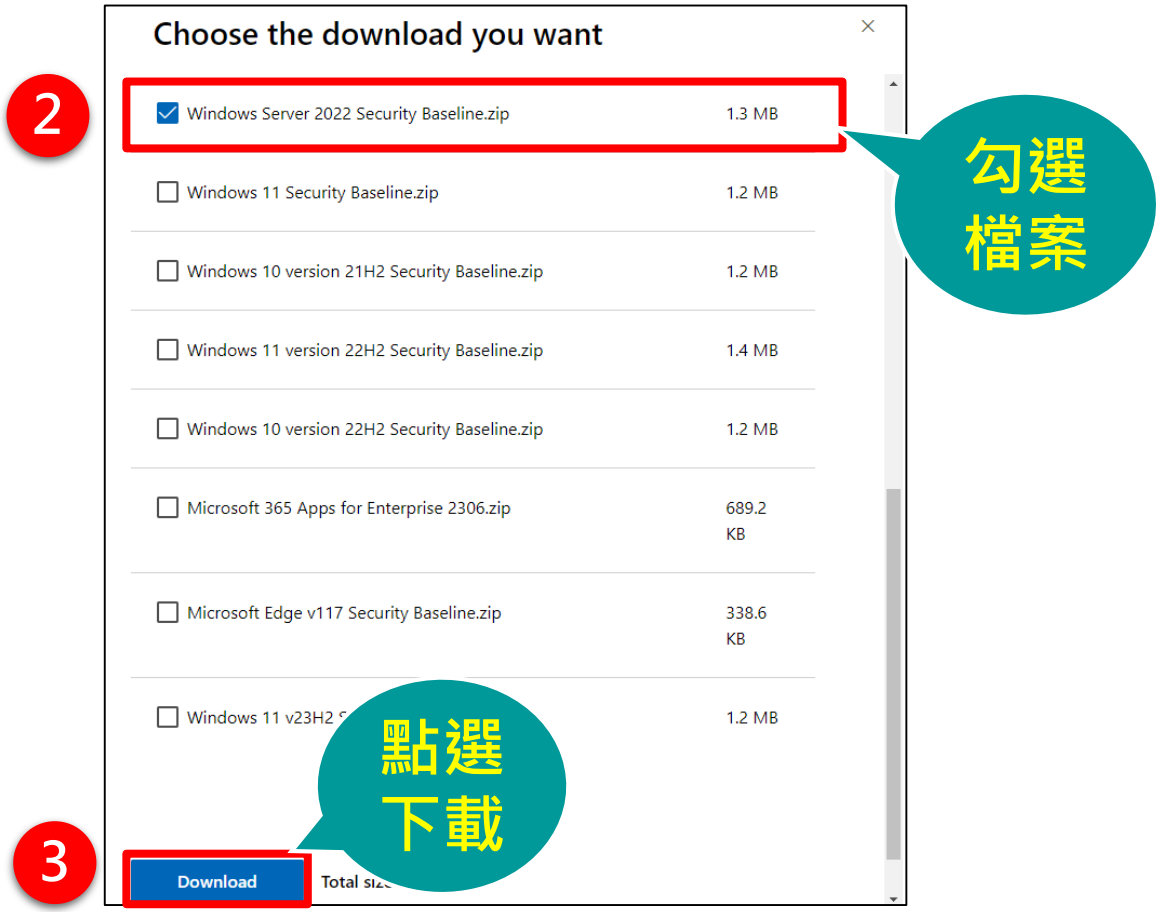
- 下載SecGuide系統管理範本
  - 步驟1：至https://www.microsoft.com/en-us/download/details.aspx?id=55319，點選「Download」按鈕



安裝SecGuide系統管理範本(3/6)

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

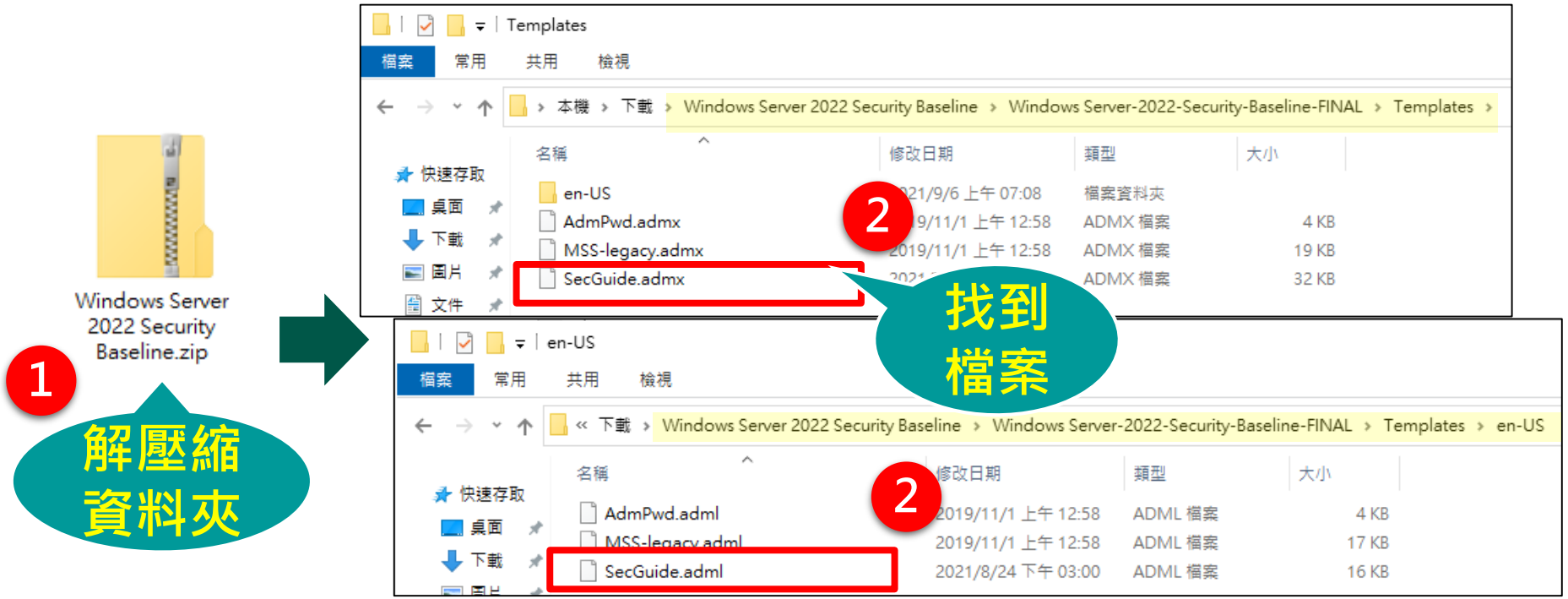
- 步驟2：在「Choose the download you want」頁面， 勾選「Windows Server 2022 Security Baseline.zip」
- 步驟3：點選「Download」按鈕



安裝SecGuide系統管理範本(4/6)

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

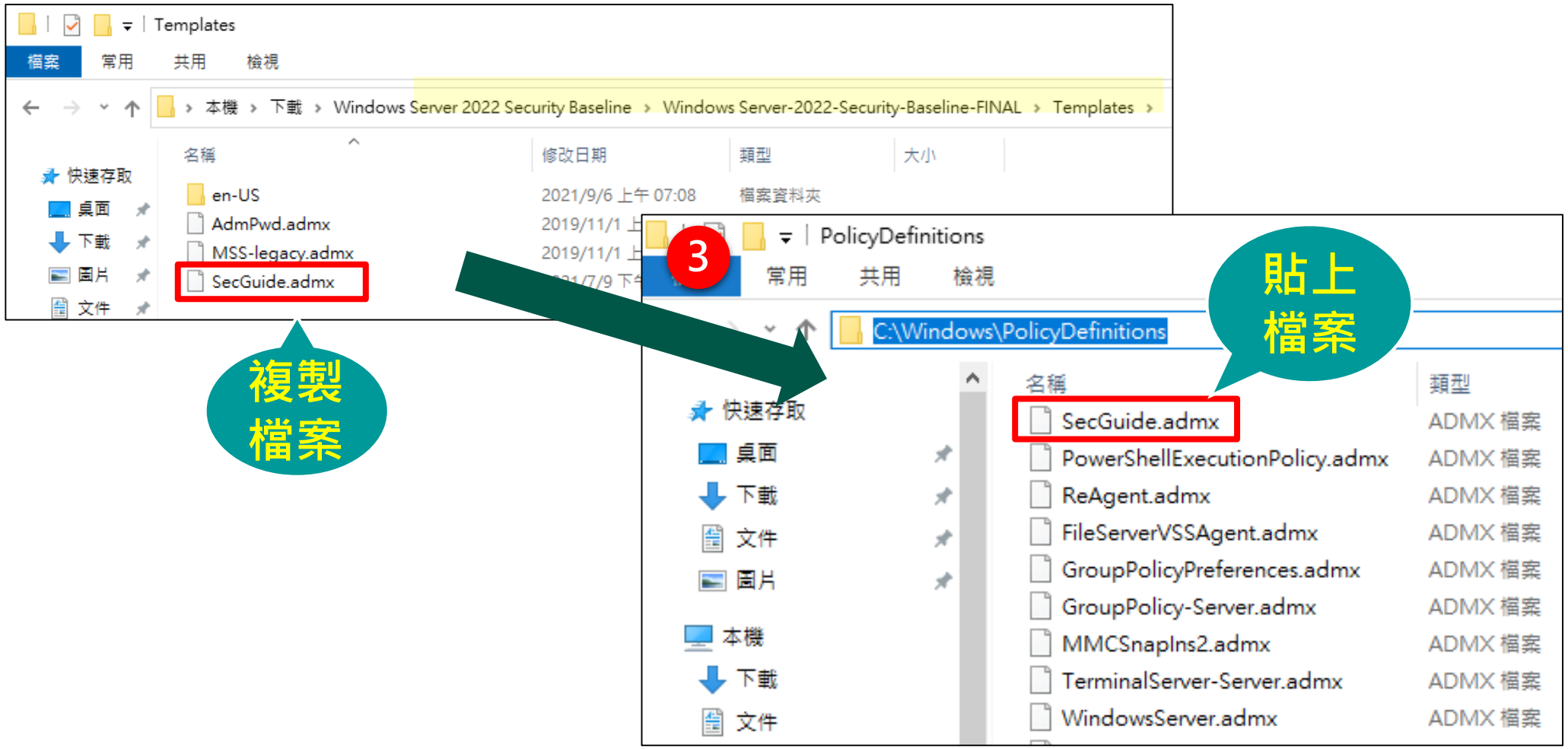
- 安裝SecGuide系統管理範本
  - 步驟1：將「 Windows Server 2022 Security Baseline.zip 」解壓縮
  - 步驟2：進入「Templates」資料夾，找到SecGuide.admx 與 SecGuide.adml檔案



安裝SecGuide系統管理範本(5/6)

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

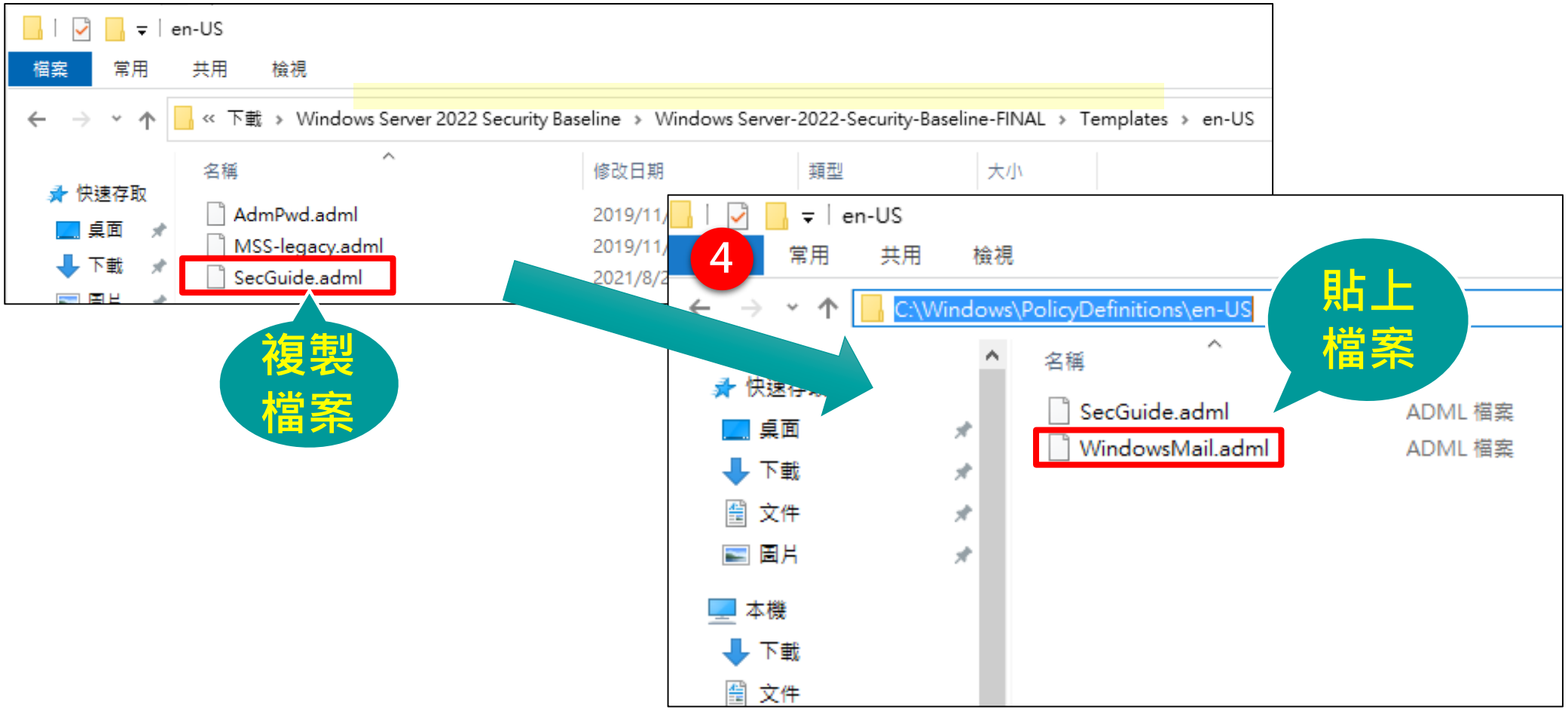
–步驟3：將「SecGuide.admx」複製到「C:\Windows\PolicyDefinitions」目錄下



安裝SecGuide系統管理範本(6/6)

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

–步驟4：將「SecGuide.adml」複製到「C:\Windows\PolicyDefinitions\en-US」目錄下

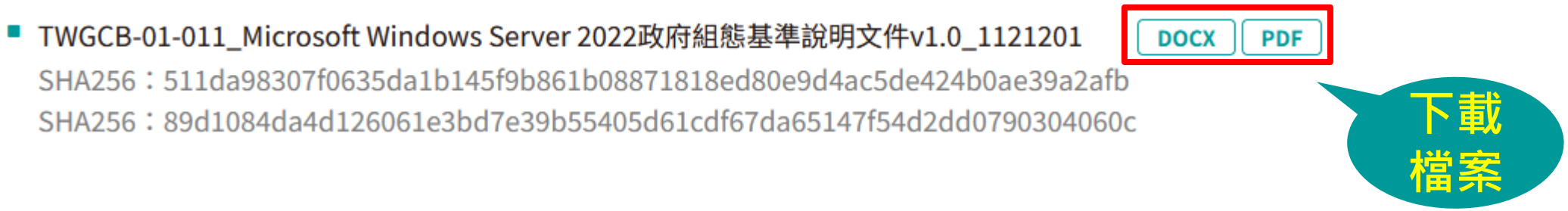


1.2 GPO檔案與單機部署工具下載

GPO檔案與單機部署工具下載(1/4)

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

- 下載Windows Server 2022政府組態基準說明文件
  - 至資安院官網下載Windows Server 2022政府組態基準說明文件，並參閱詳細條目內容說明
  - 下載網址：
    https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/GCB_Documentation/



GPO檔案與單機部署工具下載(2/4)

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

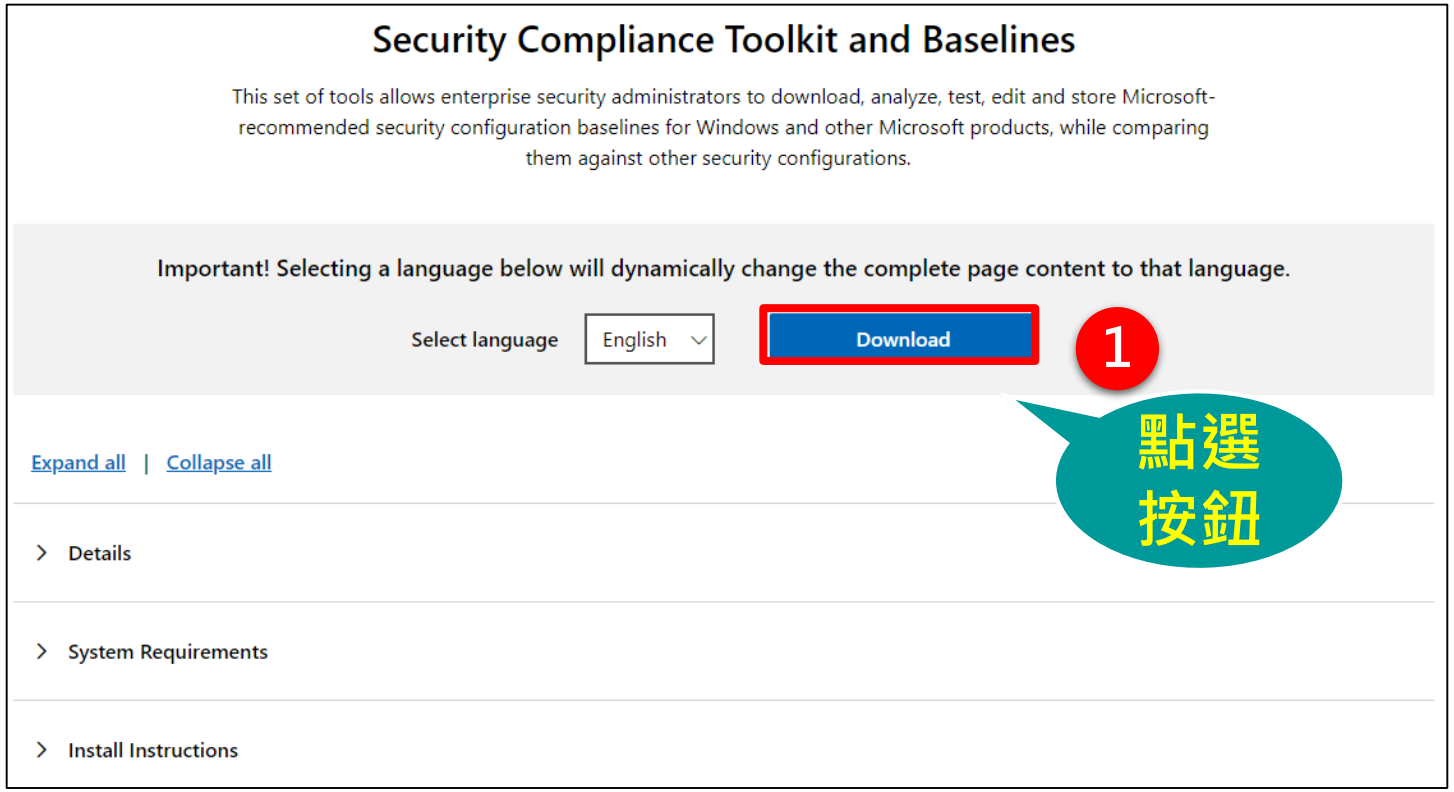
- 下載Windows Server 2022 GPO檔案
  - 至資安院官網下載Windows Server 2022 GPO檔案，並以此為基準部署GCB
  - 下載網址：

https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/GCB_Deployment_Resources/

GPO檔案與單機部署工具下載(3/4)

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

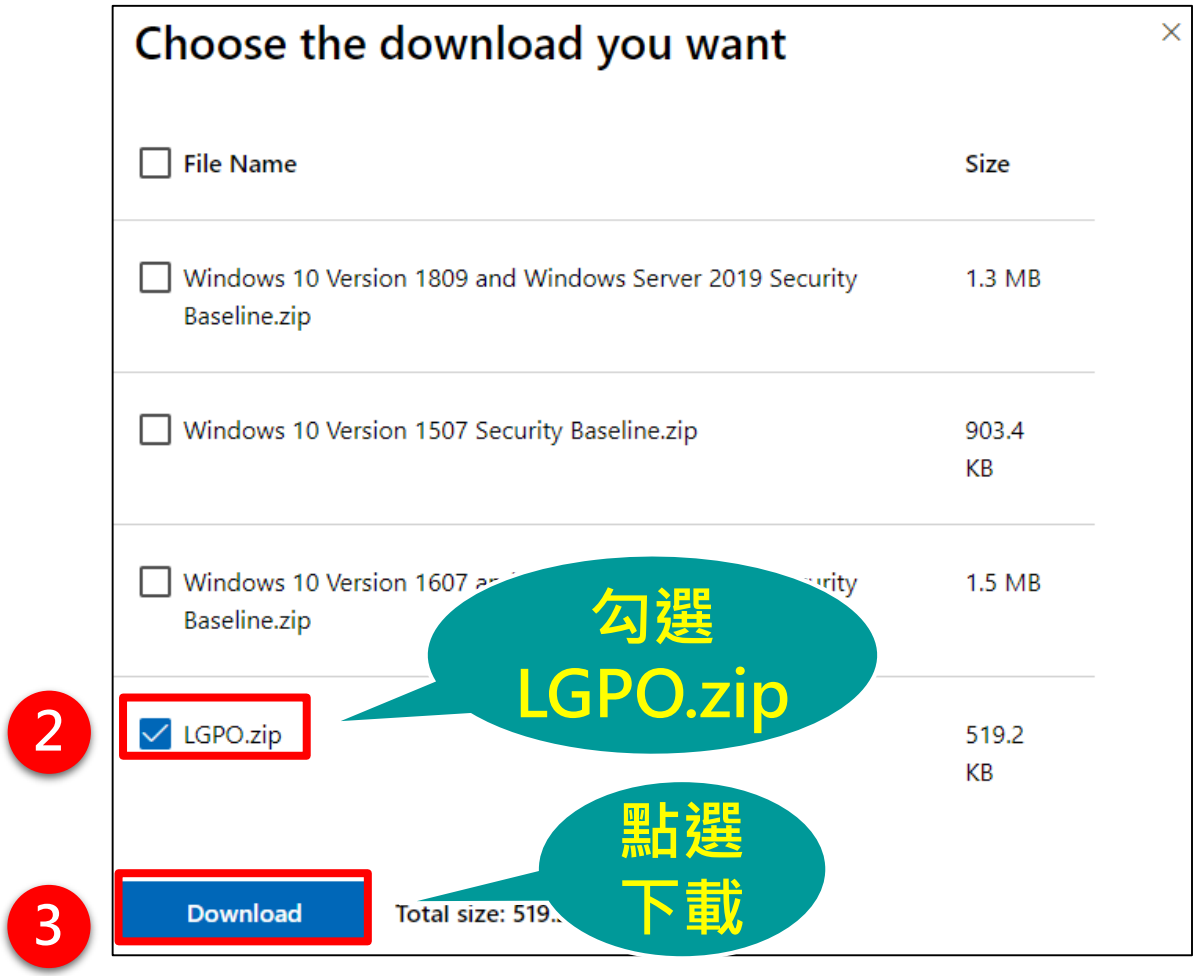
- 下載LGPO程式(僅適用於單機部署)
  - 步驟1：至https://www.microsoft.com/en-us/download/details.aspx?id=55319，點選「Download」按鈕



GPO檔案與單機部署工具下載(4/4)

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

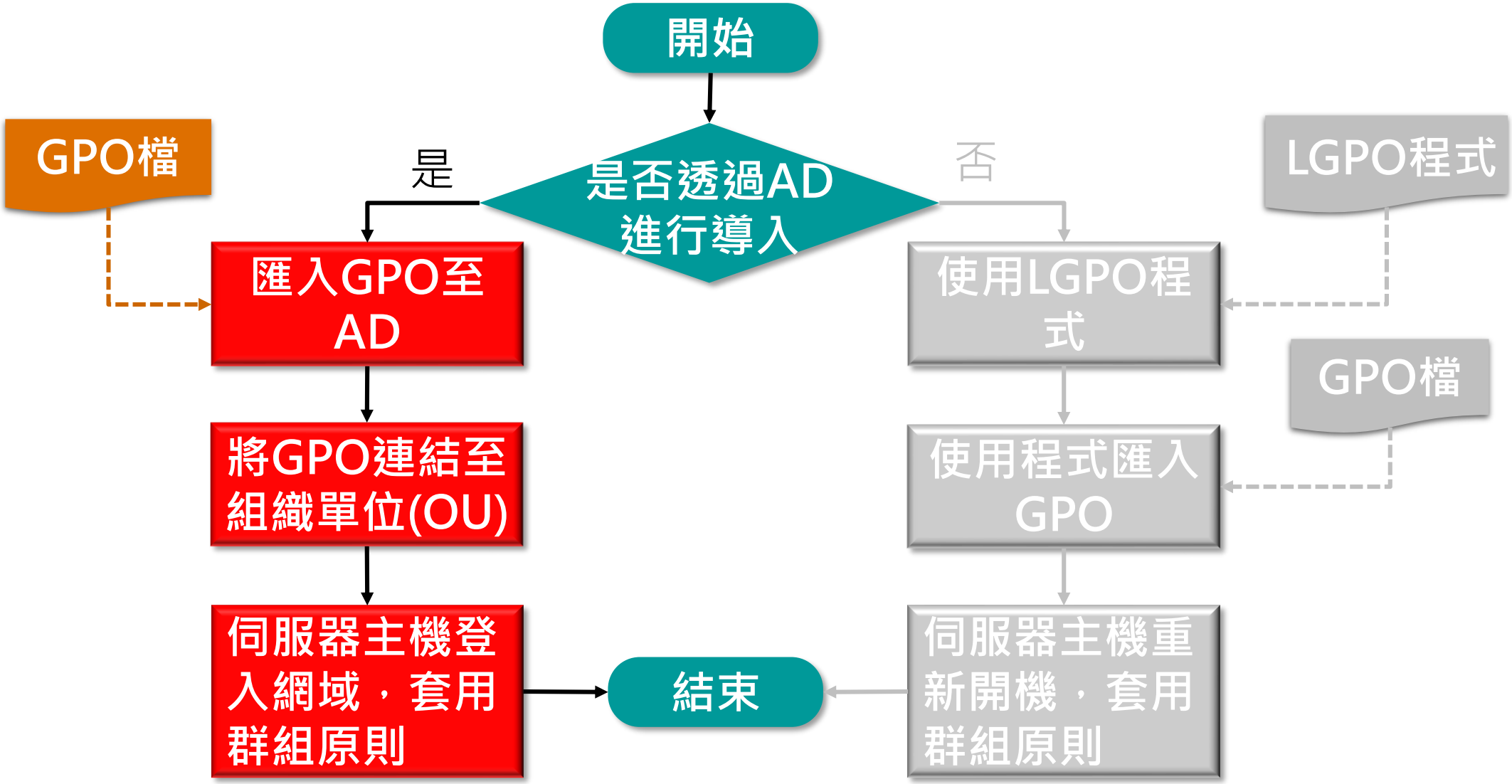
- 步驟2：在「Choose the download you want」頁面，勾選「LGPO.zip」
- 步驟3：點選「Download」按鈕



2.導入階段

2.1 網域環境部署

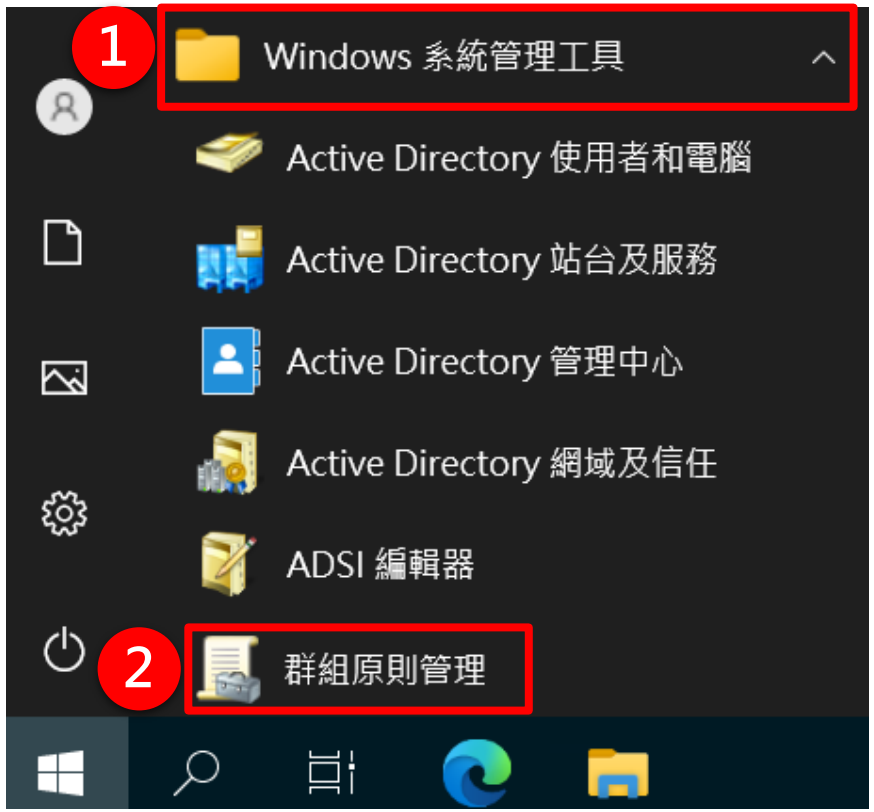
網域環境部署流程


開始
是否透過AD進行導入
是
否
GPO檔
匯入GPO至AD
將GPO連結至組織單位(OU)
伺服器主機登入網域，套用群組原則
結束
LGPO程式
使用LGPO程式
GPO檔
使用程式匯入GPO
伺服器主機重新開機，套用群組原則

2.1.1 使用AD部署GPO

建立GPO(1/3)

- 步驟1：點擊開始→Windows系統管理工具
- 步驟2：點擊群組原則管理



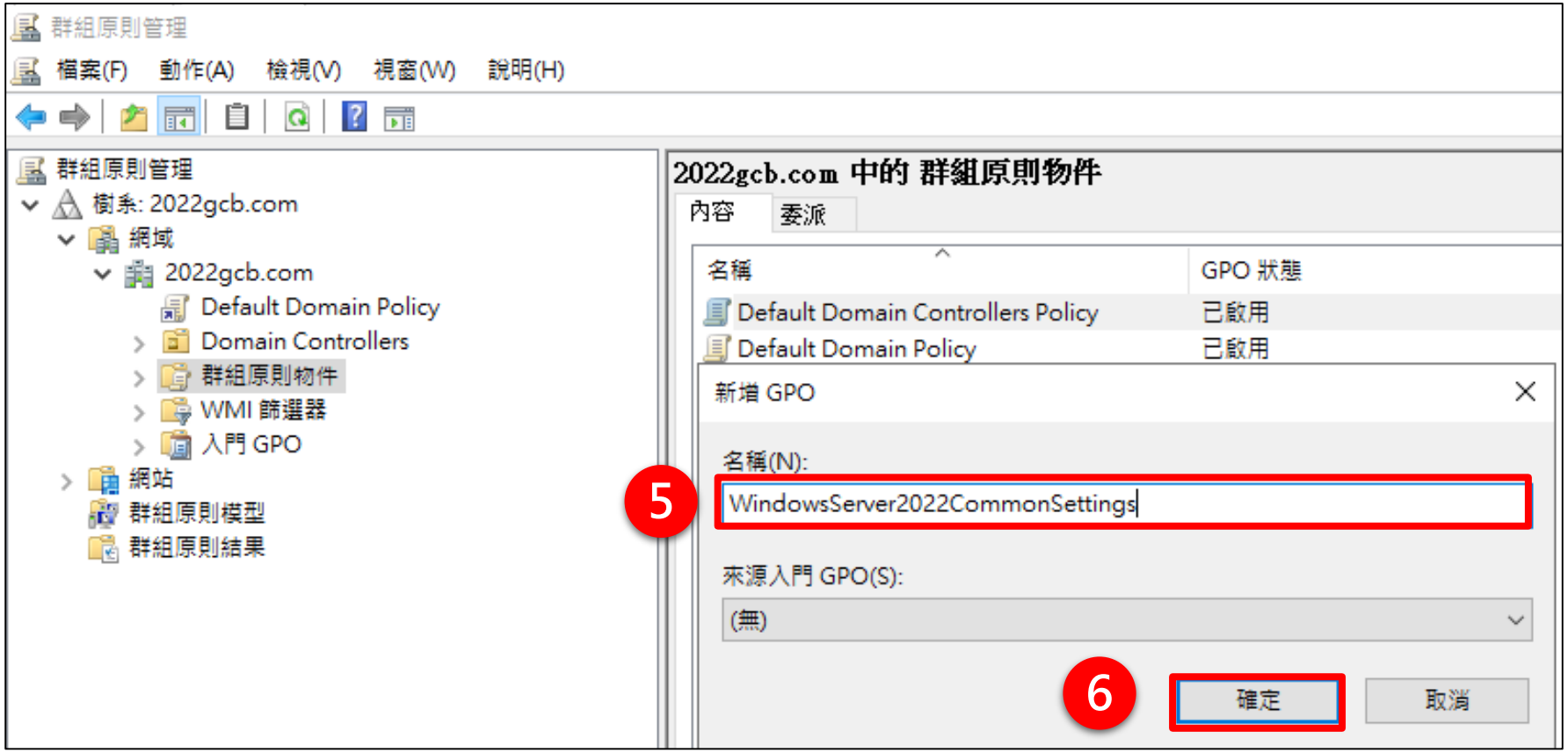
建立GPO(2/3)

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

- 步驟3：在群組原則物件節點按滑鼠右鍵
- 步驟4：點選「新增」

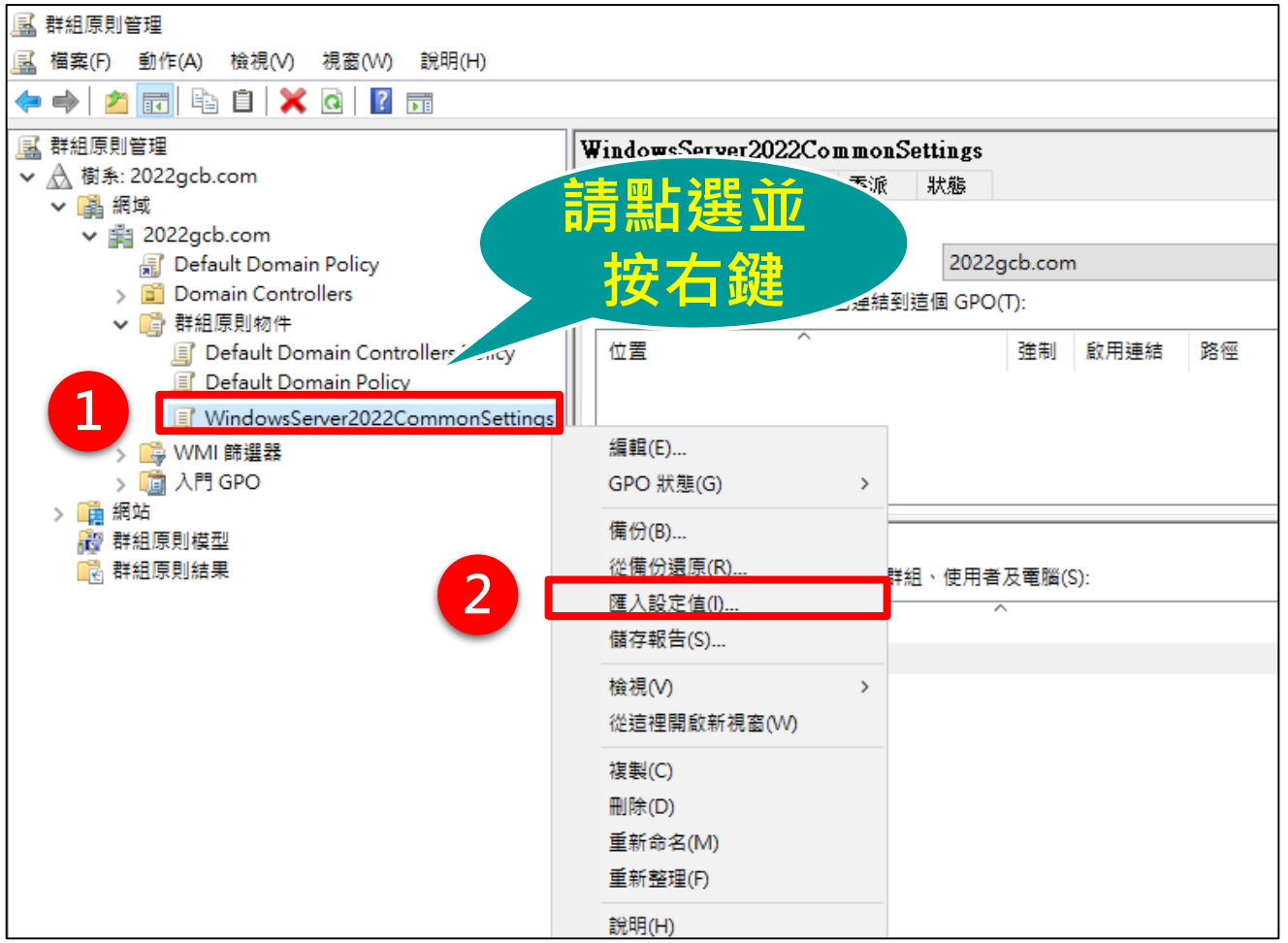
建立GPO(3/3)

- 步驟5：在「名稱」欄位輸入群組原則物件的名稱(如：WindowsServer2022CommonSettings)
- 步驟6：點選「確定」按鈕



匯入公告之GPO至AD(1/5)

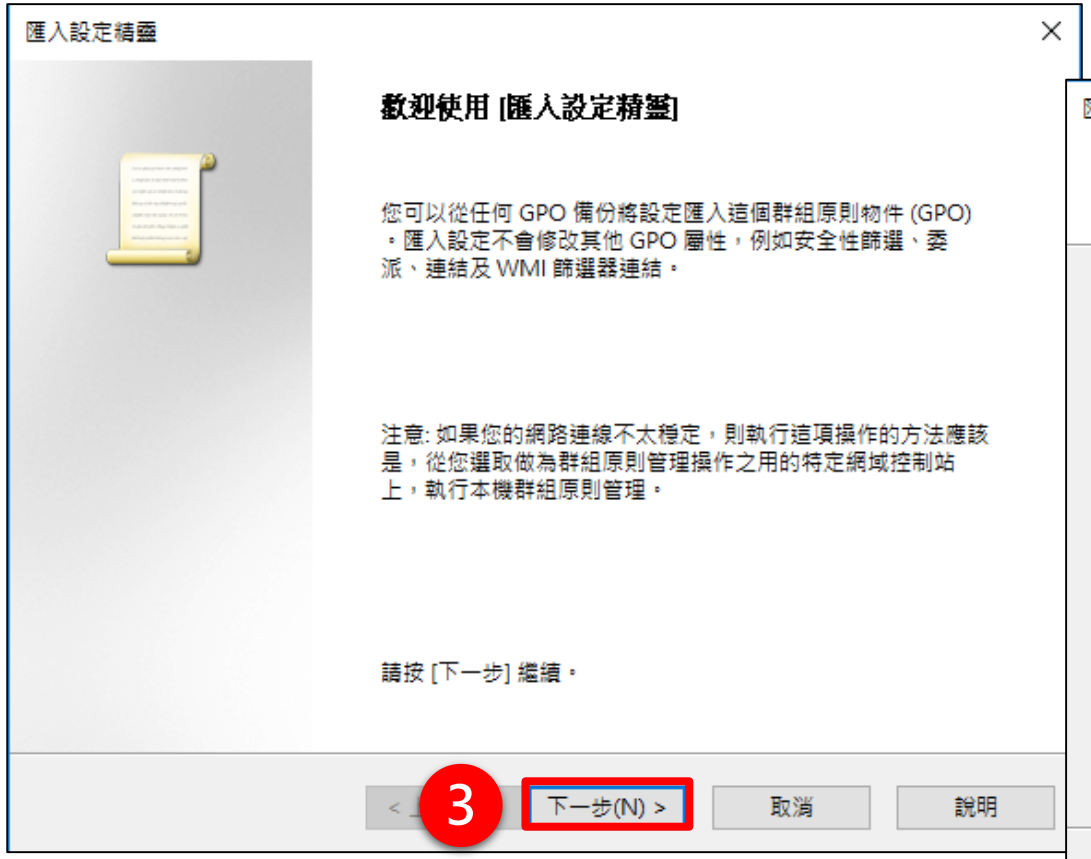
- 步驟1：點選新建的群組原則物件後按滑鼠右鍵
- 步驟2：選擇「匯入設定值」

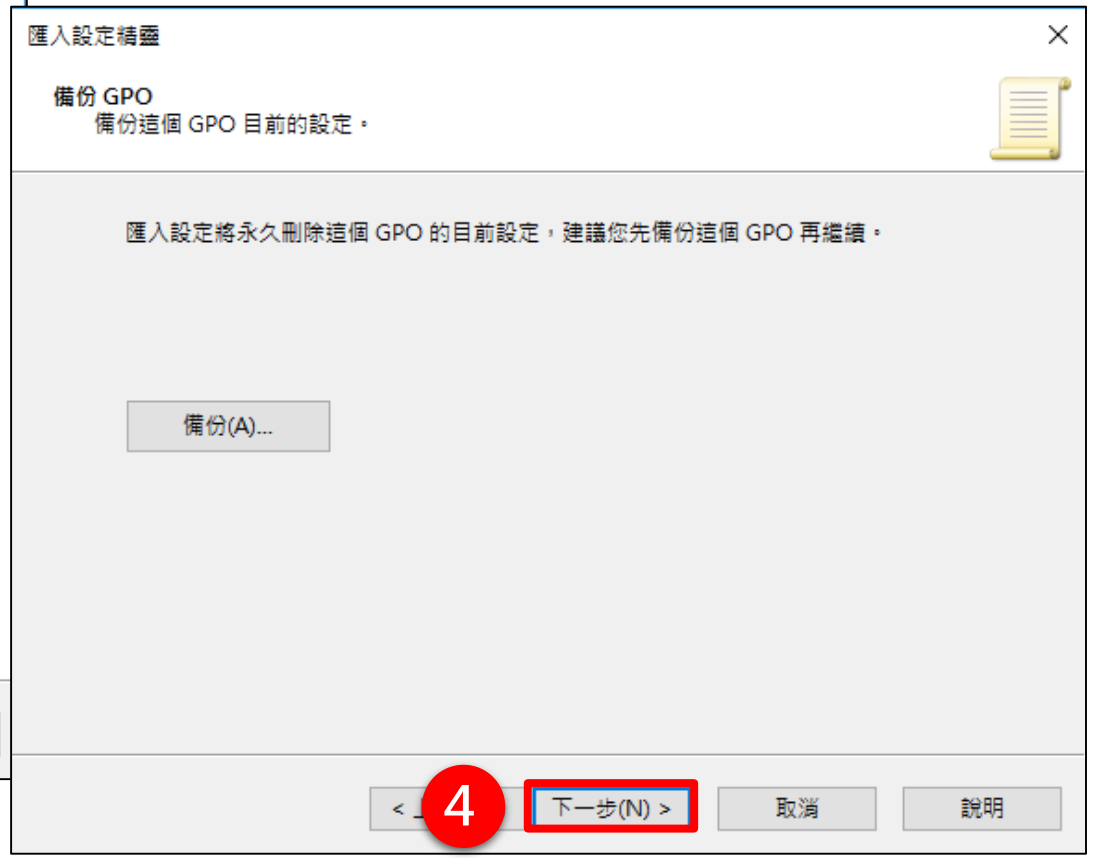


匯入公告之GPO至AD(2/5)

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

- 步驟3：在歡迎使用【匯入設定精靈】頁面，點選「下一步」按鈕
- 步驟4：在備份GPO頁面，點選「下一步」按鈕

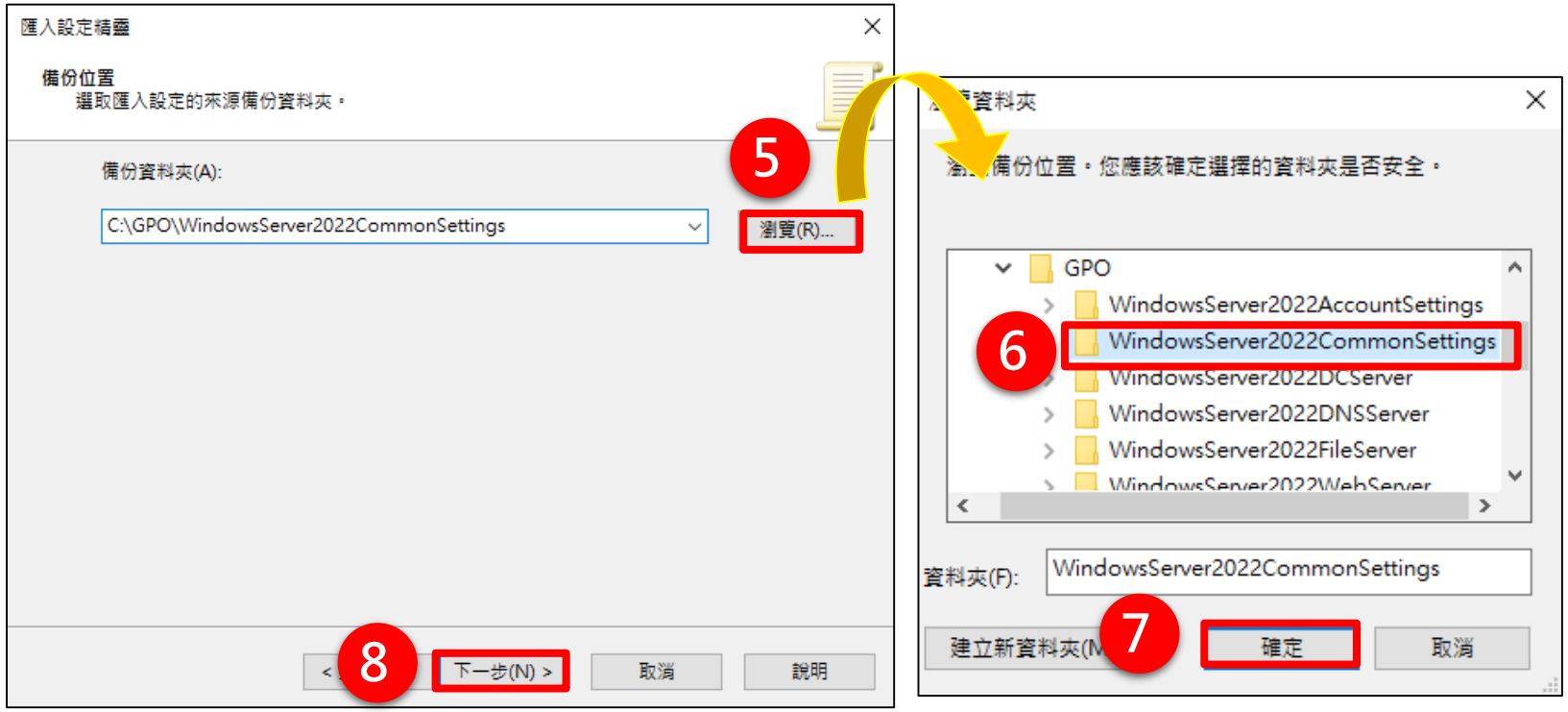




匯入公告之GPO至AD(3/5)

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

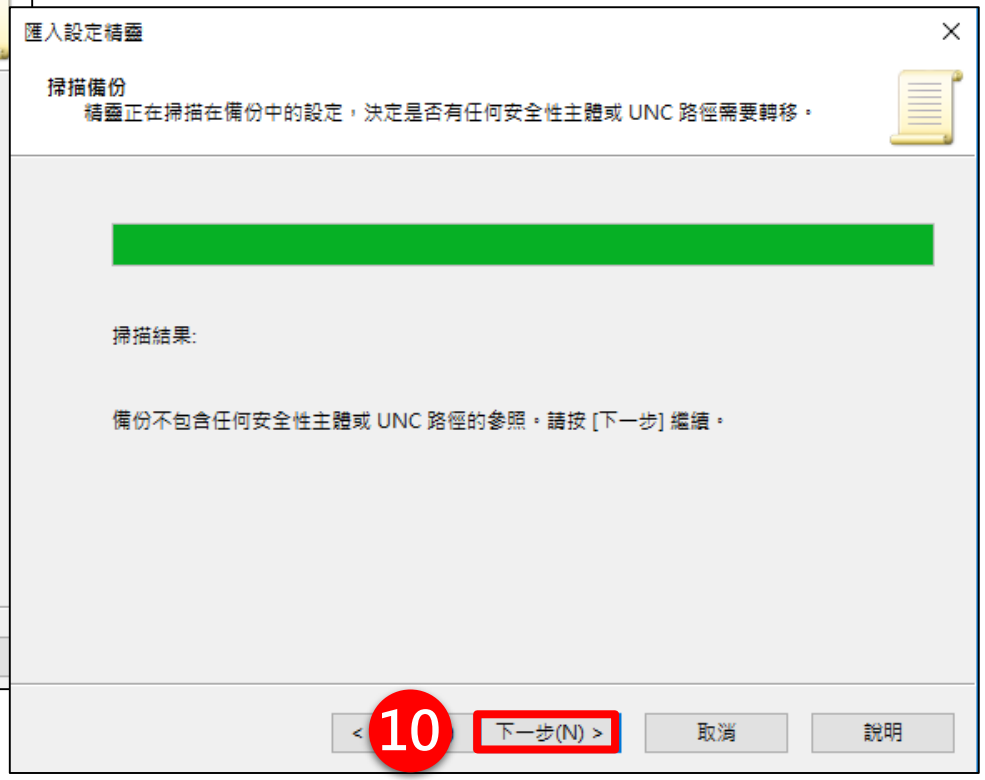
- 步驟5：在備份位置頁面，點選「瀏覽」按鈕
- 步驟6：選擇欲匯入的GPO資料夾
- 步驟7：點選「確定」按鈕
- 步驟8：在備份位置頁面，點選「下一步」按鈕



匯入公告之GPO至AD(4/5)

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

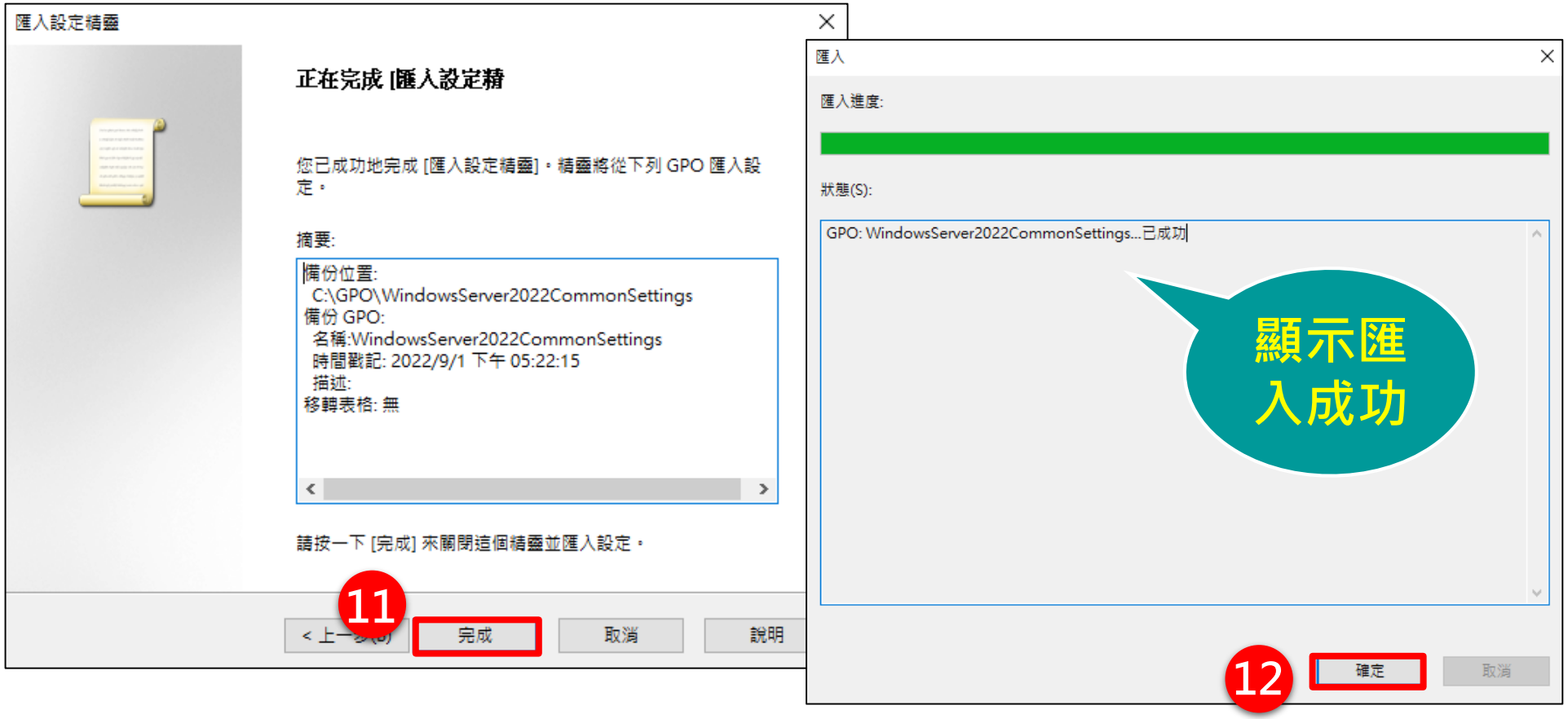
- 步驟9：在來源GPO頁面，確認匯入之GPO正確後，點選「下一步」按鈕
- 步驟10：在掃描備份頁面，點選「下一步」按鈕



匯入公告之GPO至AD(5/5)

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

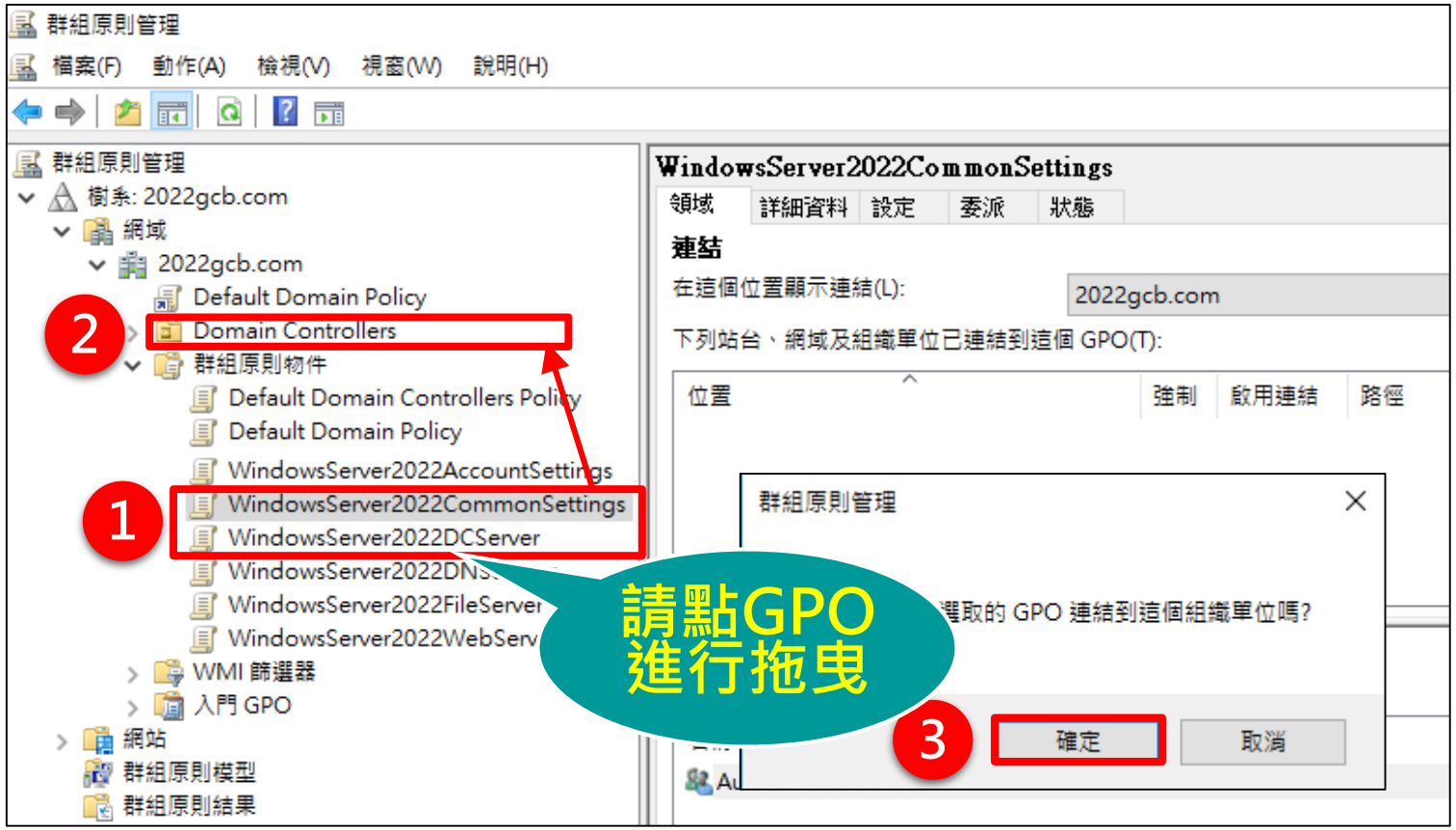
- 步驟11：在正在完成匯入設定精靈頁面，點選「完成」按鈕
- 步驟12：在匯入進度頁面，點選「確定」按鈕，完成匯入GPO至群組原則物件中



將GPO連結至組織單位(OU)(1/2)

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

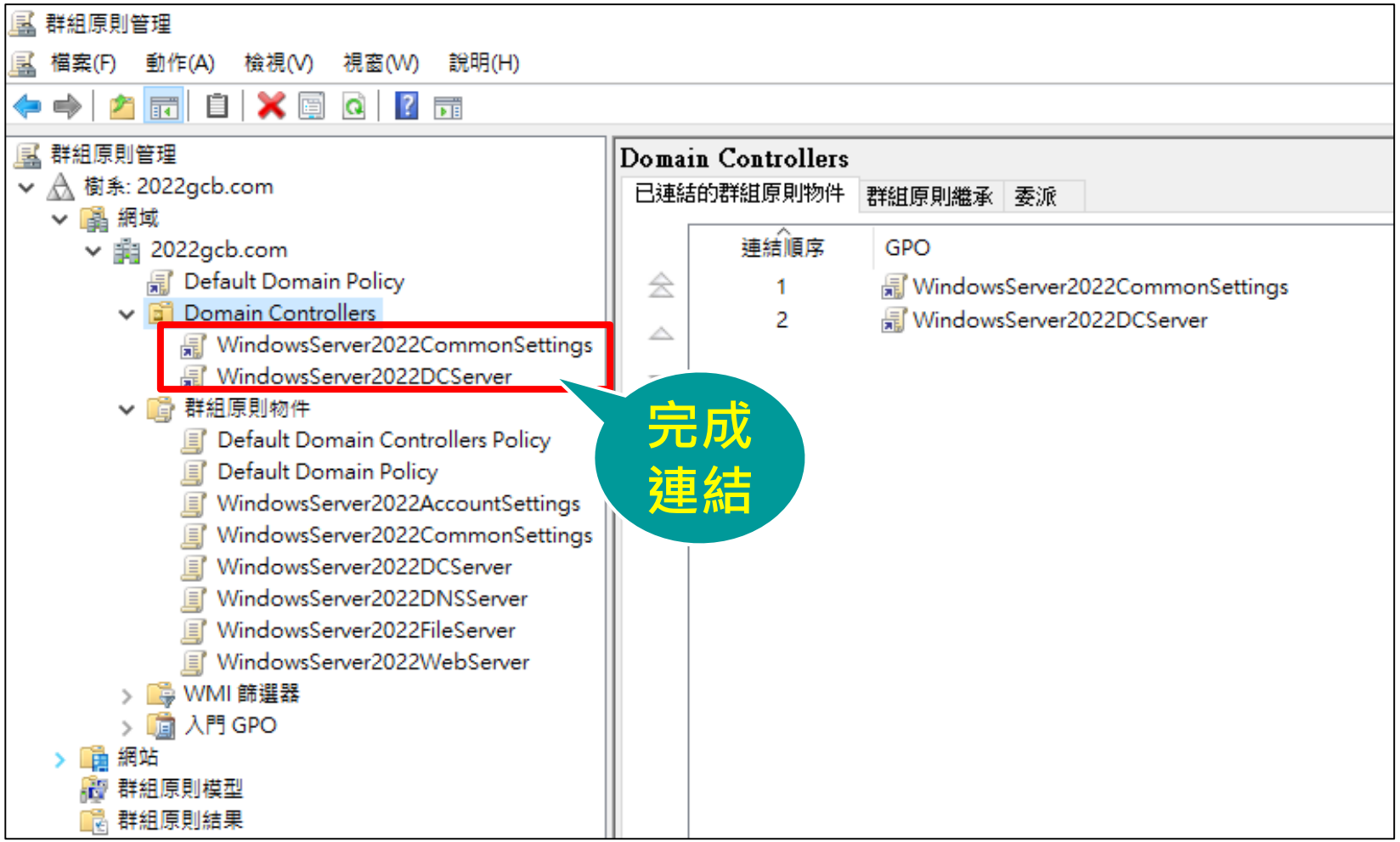
- 步驟1：點選已匯入GPO之群組原則物件
- 步驟2：拖曳至組織單位(OU)(此範例為Domain Controllers)
- 步驟3：點選「確定」按鈕，完成GPO連結至組織單位



將GPO連結至組織單位(OU)(2/2)

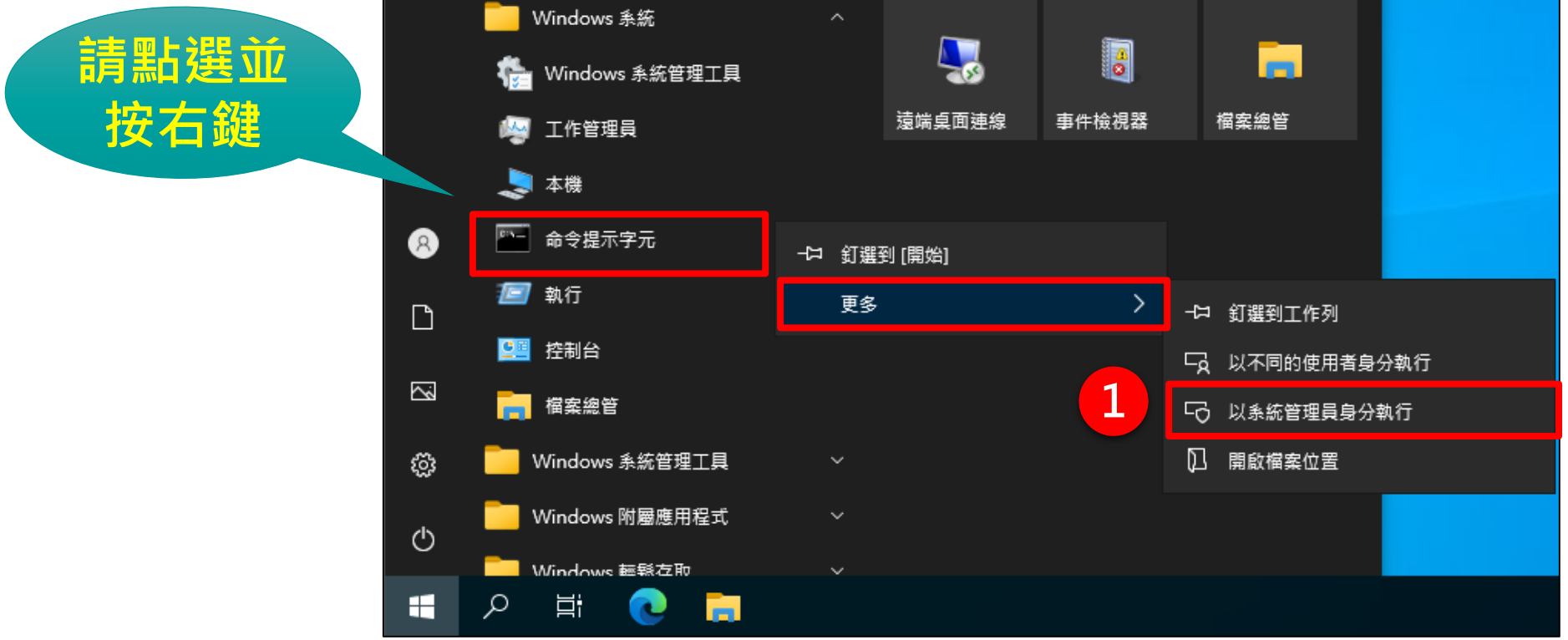
國家資通安全研究院
National Institute of Cyber Security

- 完成將GPO連結至組織單位



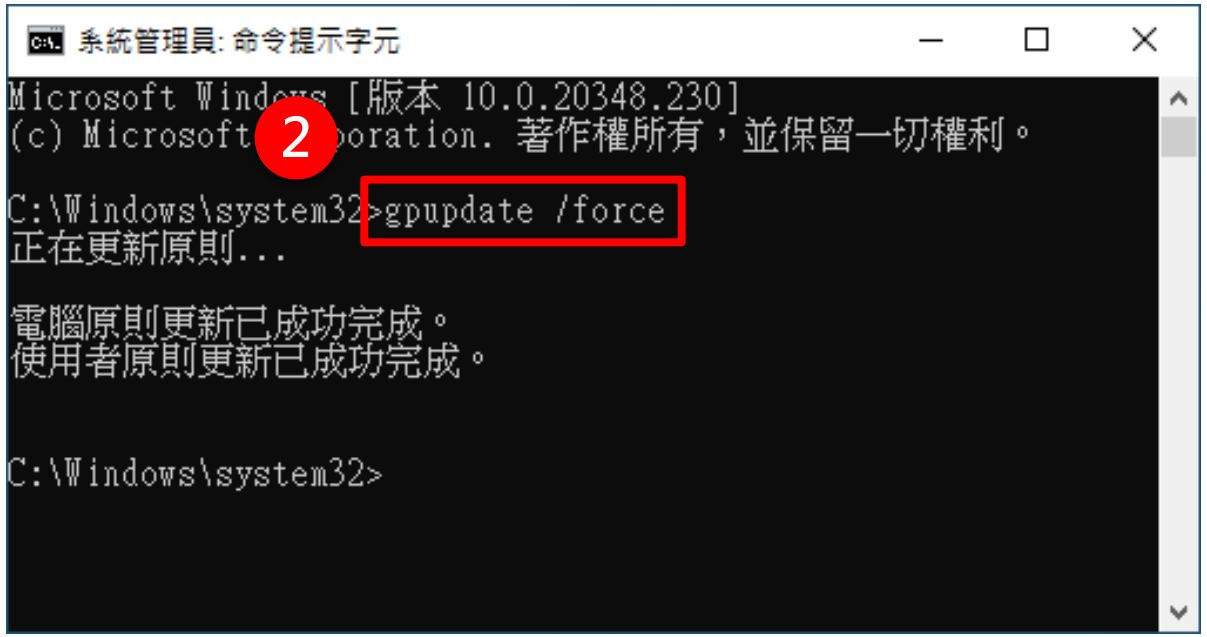
更新群組原則(1/2)

- 請選擇網域內之Windows Server 2022更新群組原則
  - 方法1：將網域內Windows Server 2022重新開機
  - 方法2：以系統管理者權限開啟命令提示字元(點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」)



更新群組原則(2/2)

- 請選擇網域內之Windows Server 2022更新群組原則
  - –再輸入gpupdate /force指令更新群組原則，即可套用GCB設定

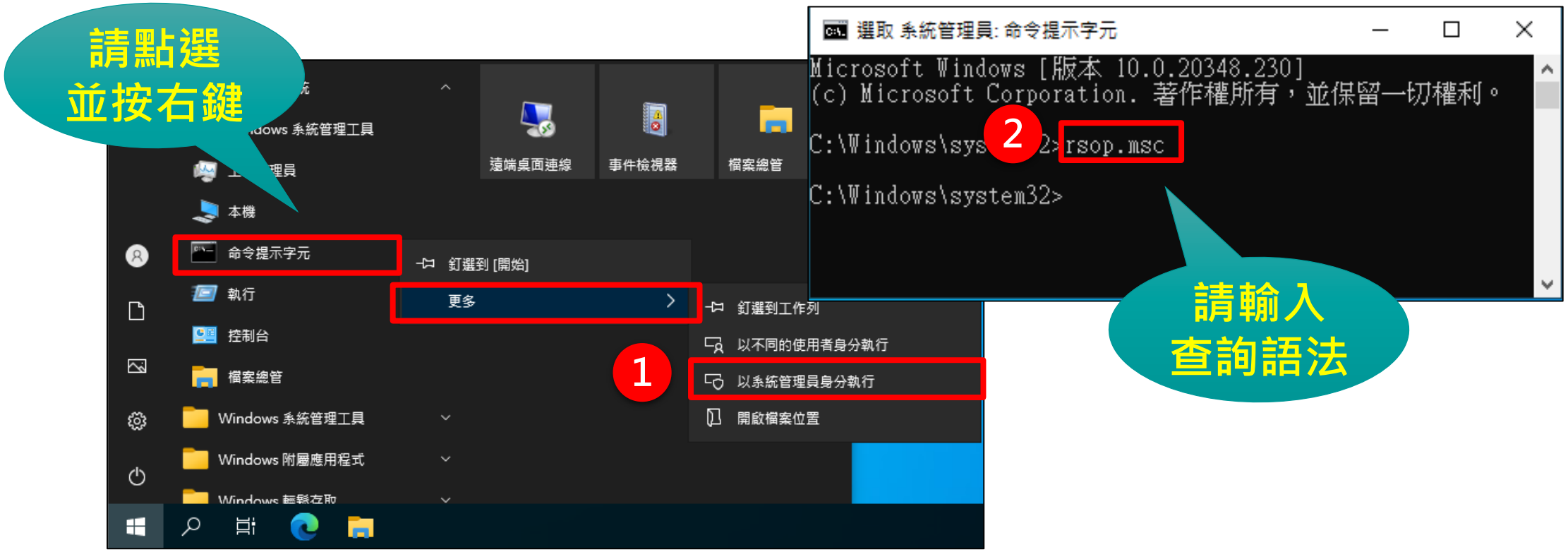


2.1.2 GPO套用狀況檢查方式

AD環境下的檢查方式一(1/2)

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

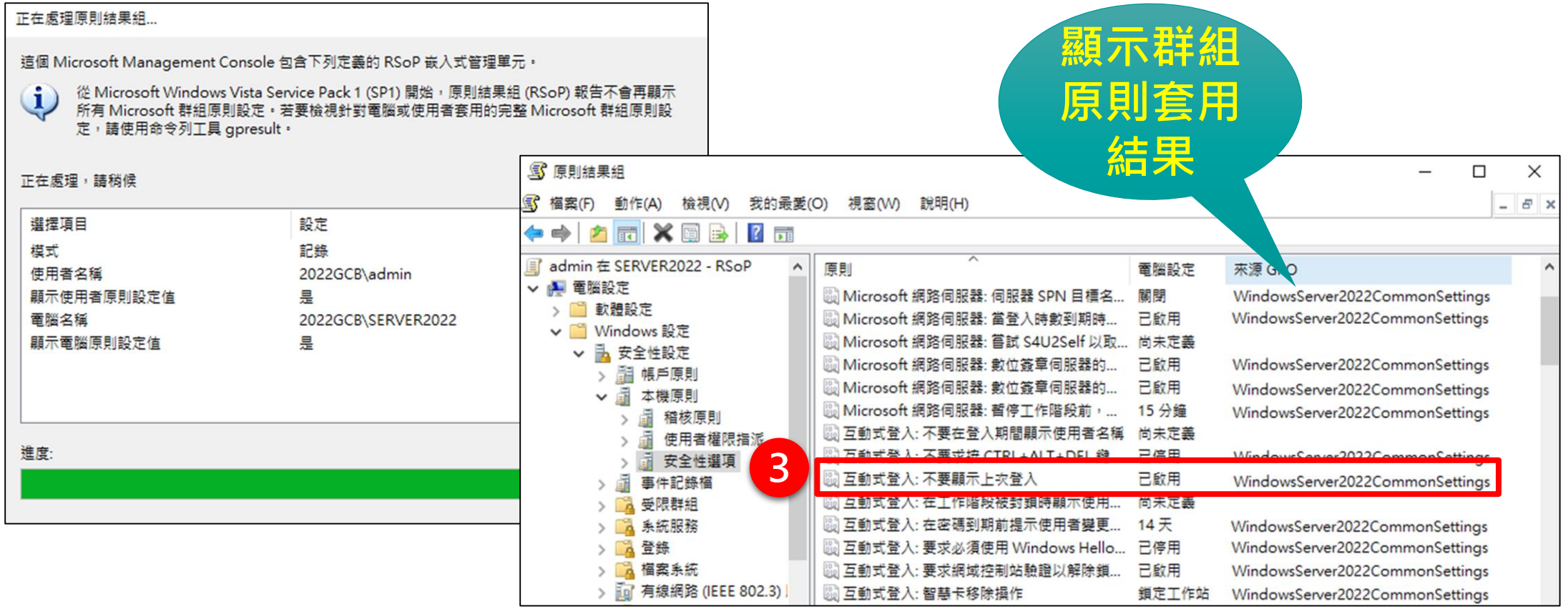
- 使用RSOP檢查群組原則
  - –步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」
  - –步驟2：於「命令提示字元」輸入rsop.msc查詢群組原則結果



AD環境下的檢查方式一(2/2)

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

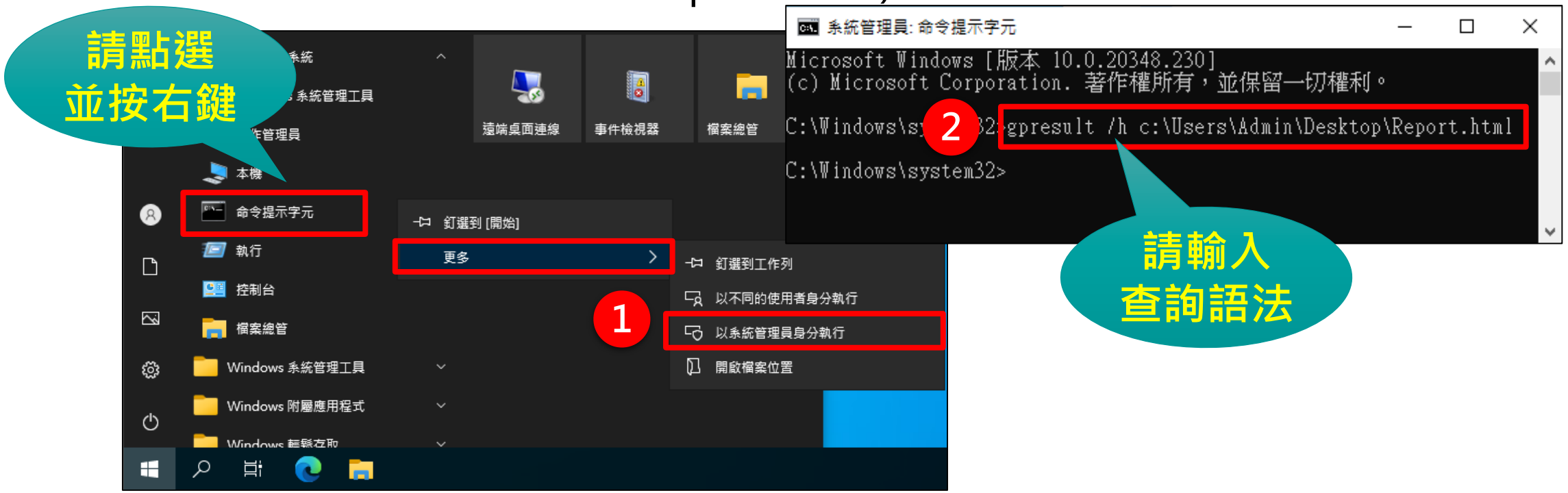
- 使用RSOP檢查群組原則
  - –步驟3：檢視GCB項目，確認是否確實套用(如：電腦設定\Windows設定\安全性設定\本機原則\安全性選項\互動式登入：不要顯示上次登入)



AD環境下的檢查方式二(1/2)

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

- 使用Gpresult檢查群組原則
  - 步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」
  - 步驟2：於「命令提示字元」輸入gpresult /h <檔案儲存路徑>\檔名.html(此範例儲存於桌面，並命名為Report.html)



AD環境下的檢查方式二(2/2)

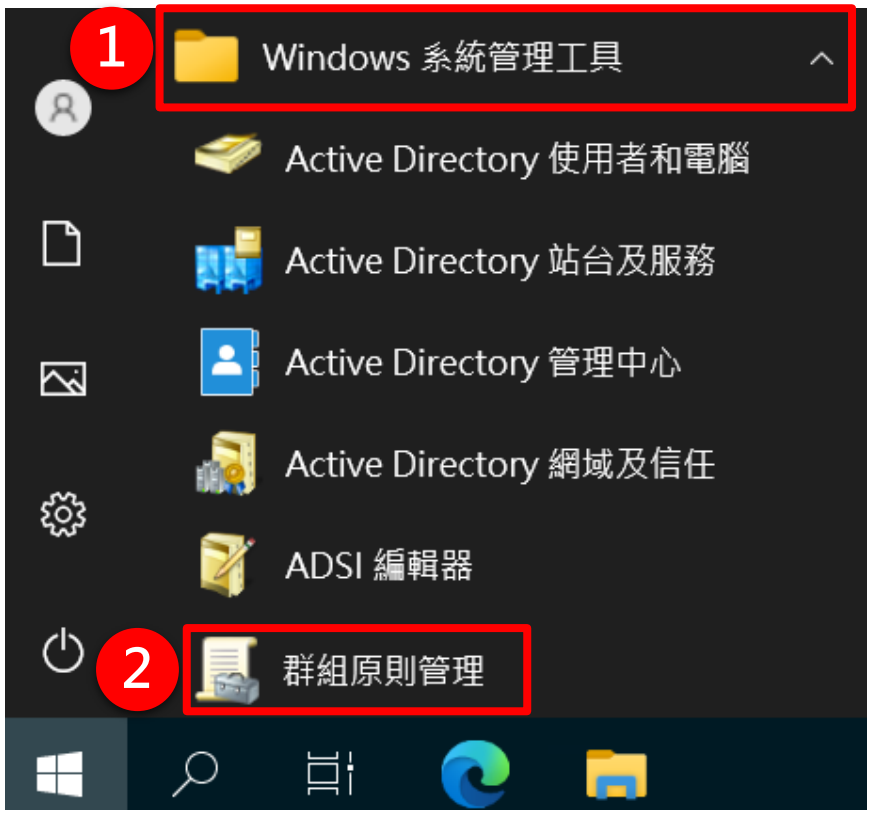
國家資通安全研究院
National Institute of Cyber Security

- 步驟3：開啟.html檔案，確認是否確實套用(如：電腦設定\Windows設定\安全性設定\本機原則\安全性選項\互動式登入\互動式登入：不要顯示上次登入)

2.1.3 恢復原始設定之方式

恢復原始設定之方式(1/3)

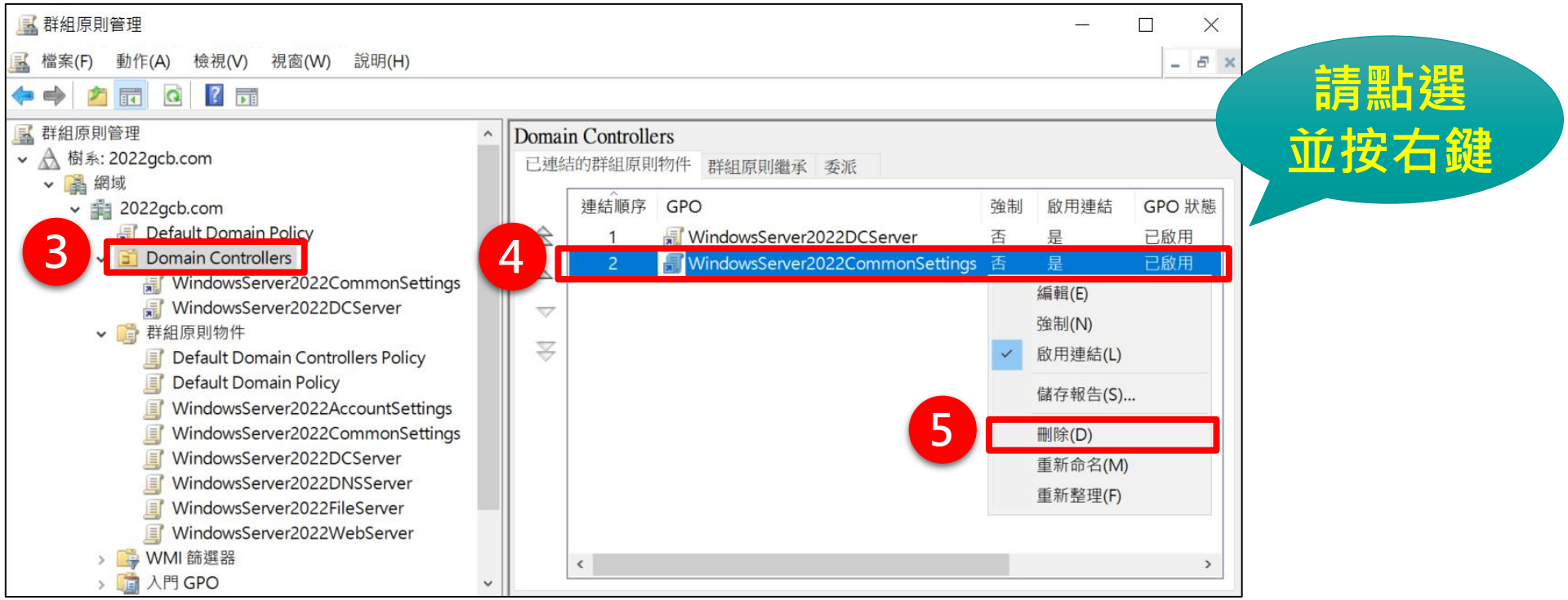
- 步驟1：點擊開始→Windows系統管理工具
- 步驟2：點擊群組原則管理



恢復原始設定之方式(2/3)

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

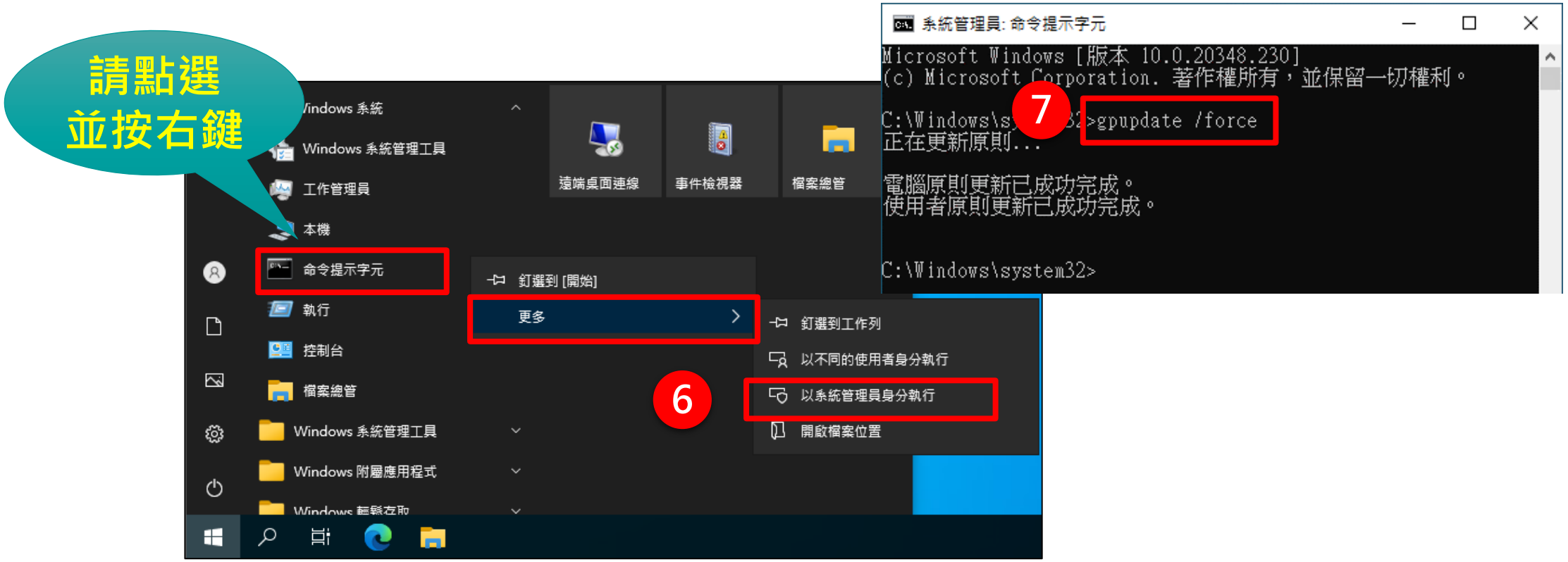
- 步驟3：點選欲取消GPO連結之組織單位(OU)
- 步驟4：在已連結的群組原則物件頁面，選取欲取消連結的GPO按滑鼠右鍵
- 步驟5：點選「刪除」將GPO自組織單位中移除



恢復原始設定之方式(3/3)

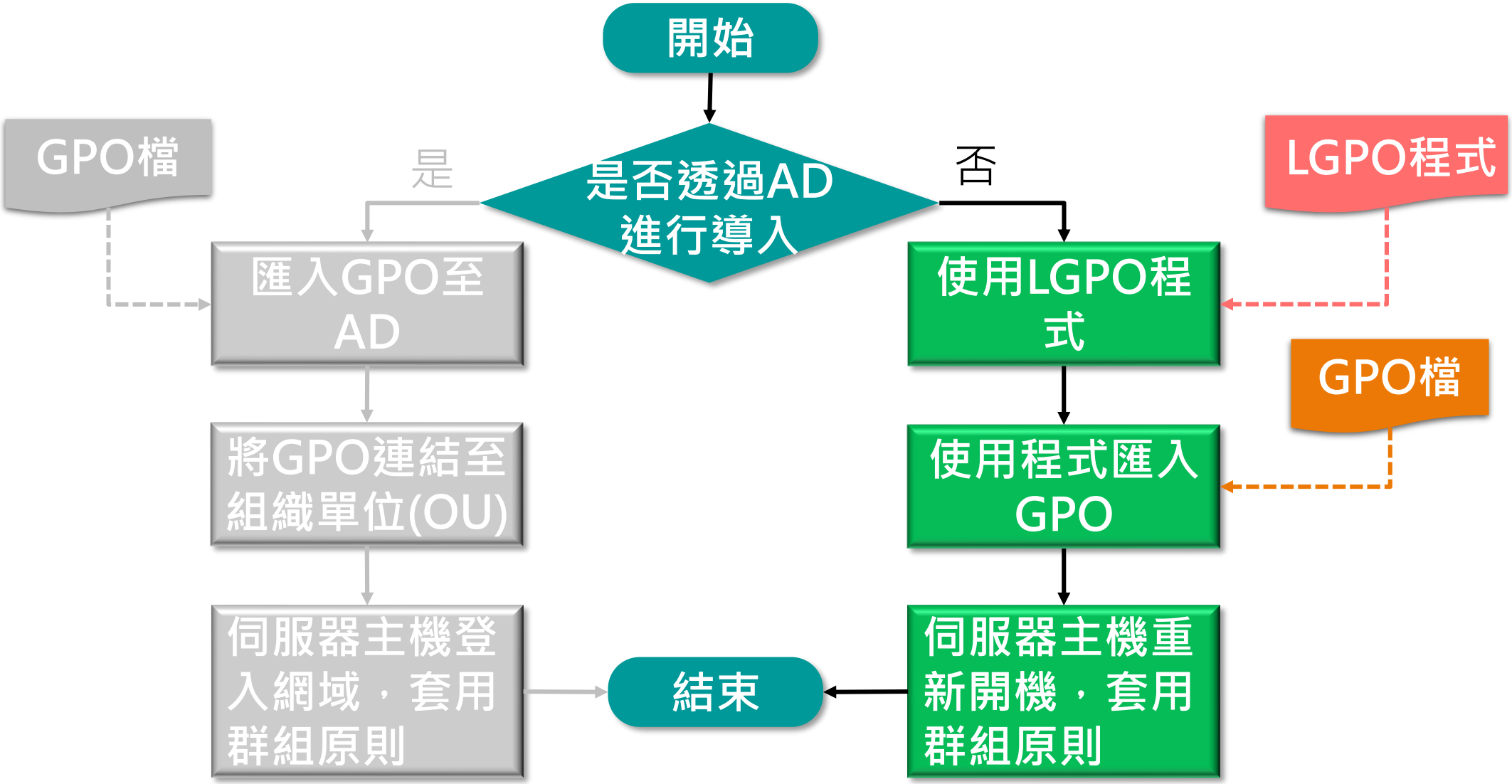
國家資通安全研究院
National Institute of Cyber Security

- 步驟6：請將網域內之Windows Server 2022重新開機，或以系統管理者權限開啟命令提示字元(點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」)
- 步驟7：輸入gpupdate /force指令更新群組原則，即可恢復原始設定



2.2 單機環境部署

單機環境部署流程

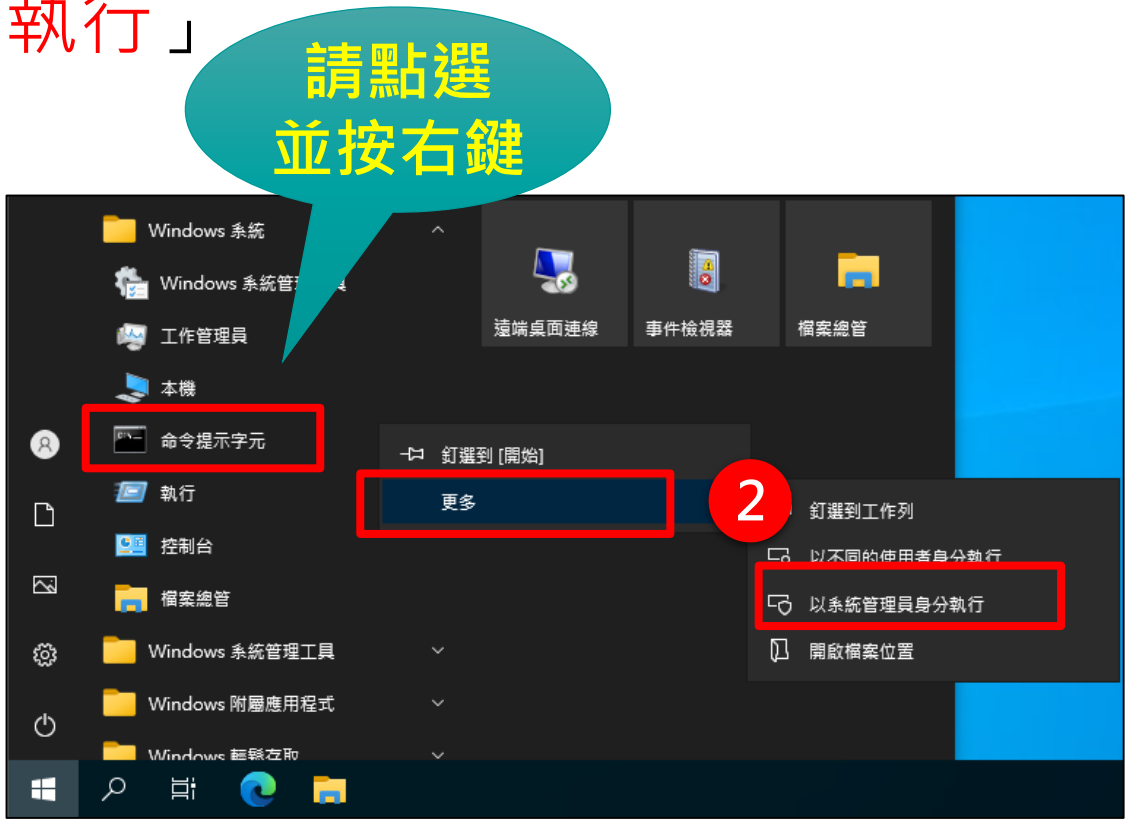

開始
是否透過AD進行導入
是
否
GPO檔
匯入GPO至AD
將GPO連結至組織單位(OU)
伺服器主機登入網域，套用群組原則
結束
LGPO程式
使用LGPO程式
GPO檔
使用程式匯入GPO
伺服器主機重新開機，套用群組原則

2.2.1 使用LGPO程式導入GCB

使用LGPO部署GPO(1/5)

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

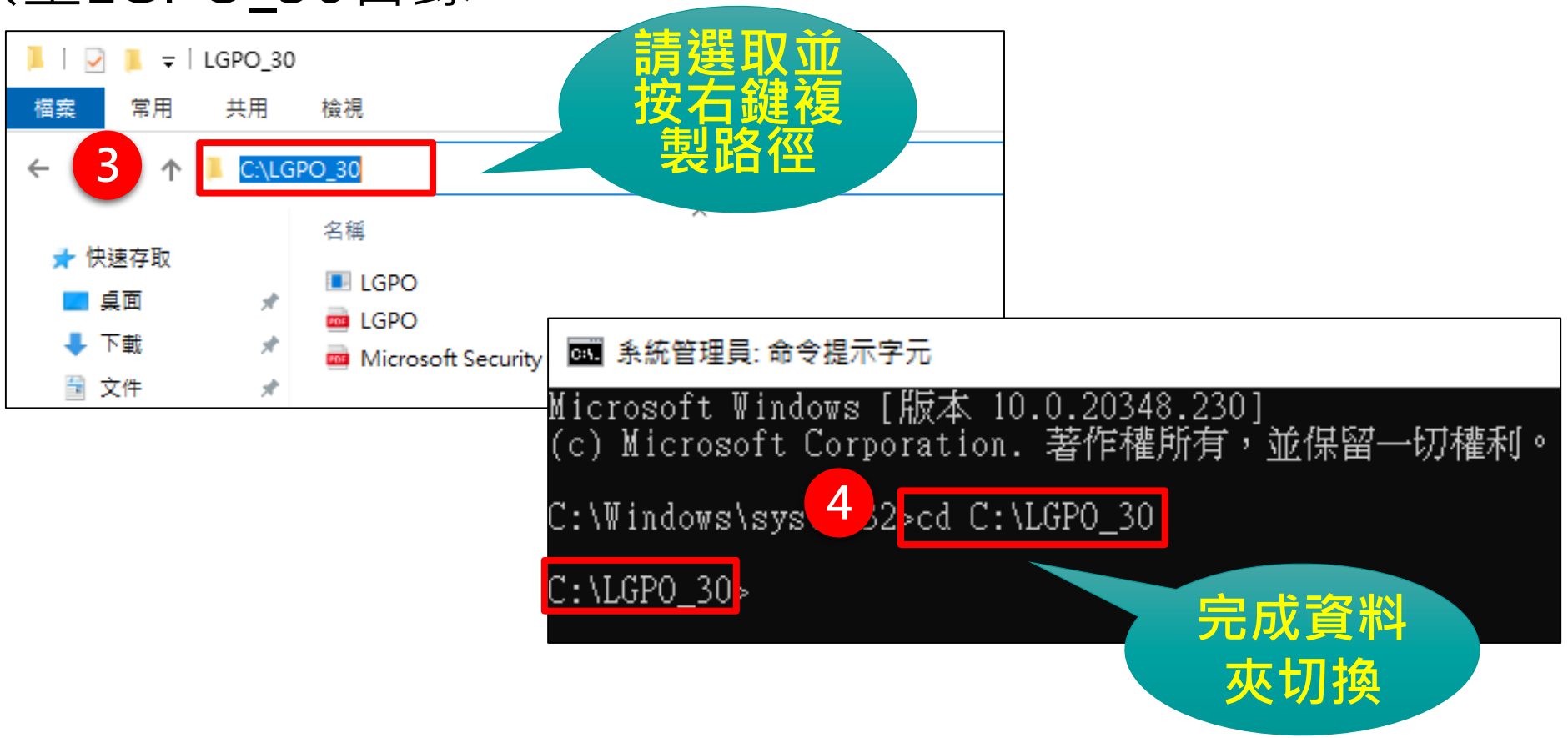
- 步驟1：請將下載之LGPO.zip程式解壓縮至C:\LGPO_30
- 步驟2：點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」



使用LGPO部署GPO(2/5)

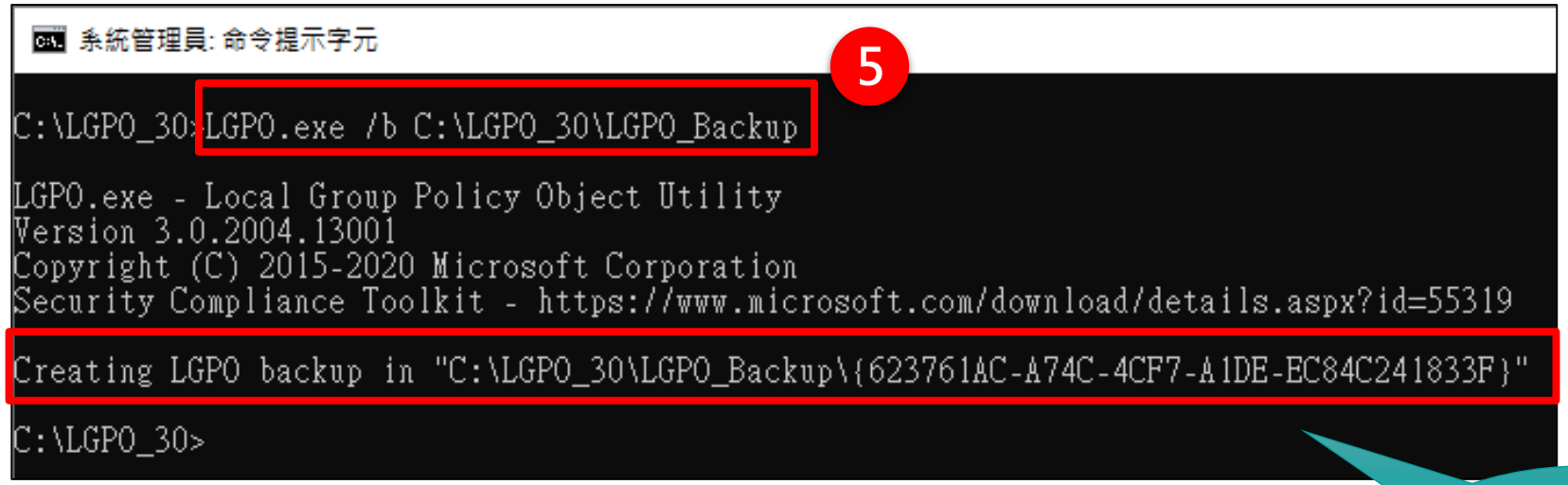
國家資通安全研究院
National Institute of Cyber Security

- 步驟3：複製LGPO應用程式解壓縮後之完整目錄路徑
- 步驟4：於「命令提示字元」輸入cd <LGPO_30完整目錄路徑>，切換至LGPO_30目錄



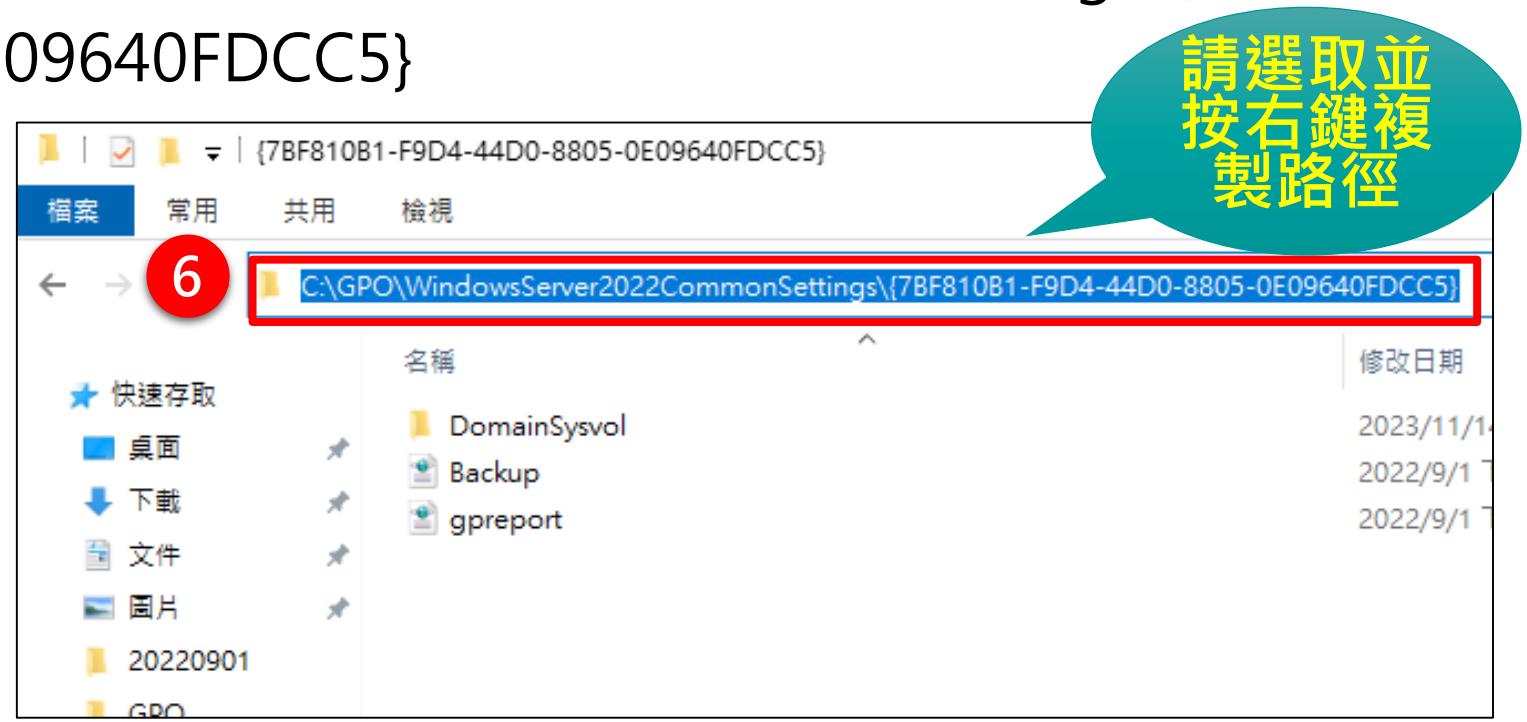
使用LGPO部署GPO(3/5)

- 步驟5：於「命令提示字元」輸入指令 LGPO.exe /b <絕對路徑>，備份電腦當下組態設定
  - 此範例備份電腦當下組態設定，儲存於C:\LGPO_30\LGPO_Backup資料夾



使用LGPO部署GPO(4/5)

- 步驟6：複製欲匯入之GPO完整目錄路徑
  - 此範例將GPO放置於C:\GPO資料夾，GPO完整目錄路徑為C:\GPO\WindowsServer2022CommonSettings\{7BF810B1-F9D4-44D0-8805-0E09640FDCC5}

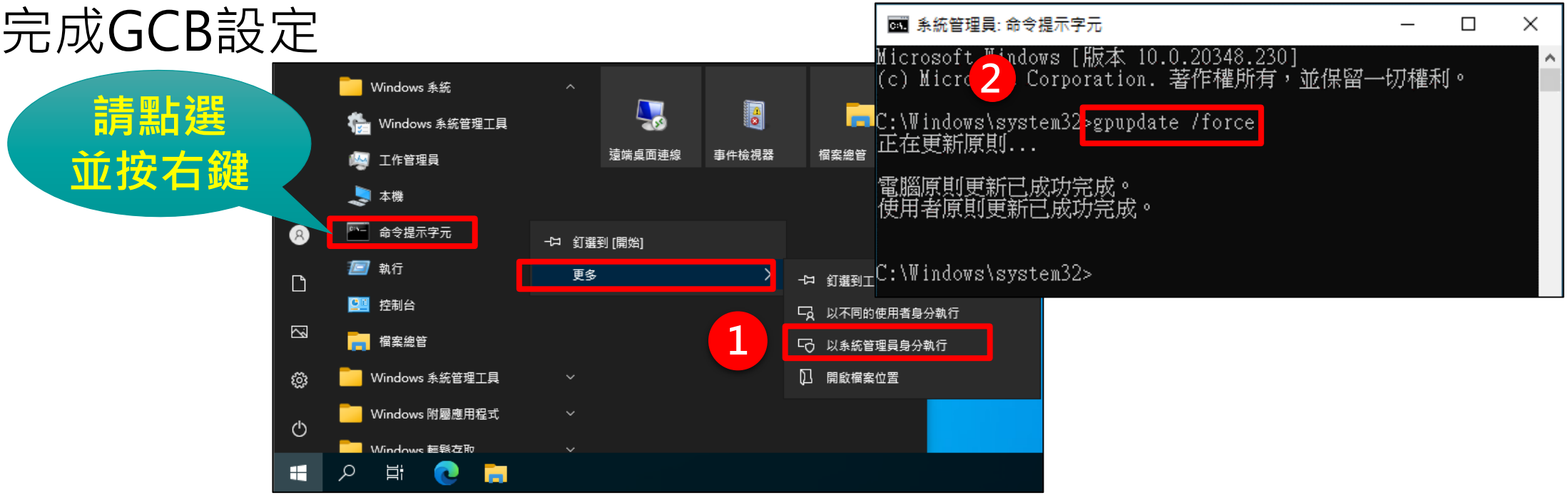


使用LGPO部署GPO(5/5)

- 步驟7：於「命令提示字元」輸入指令 LGPO.exe /g <GPO完整目錄路徑>，將GPO檔案匯入電腦

更新群組原則

- 方法1：將Windows Server 2022重新開機。
- 方法2：以系統管理者權限開啟命令提示字元(點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」)，再輸入gpupdate /force指令更新群組原則，即可完成GCB設定

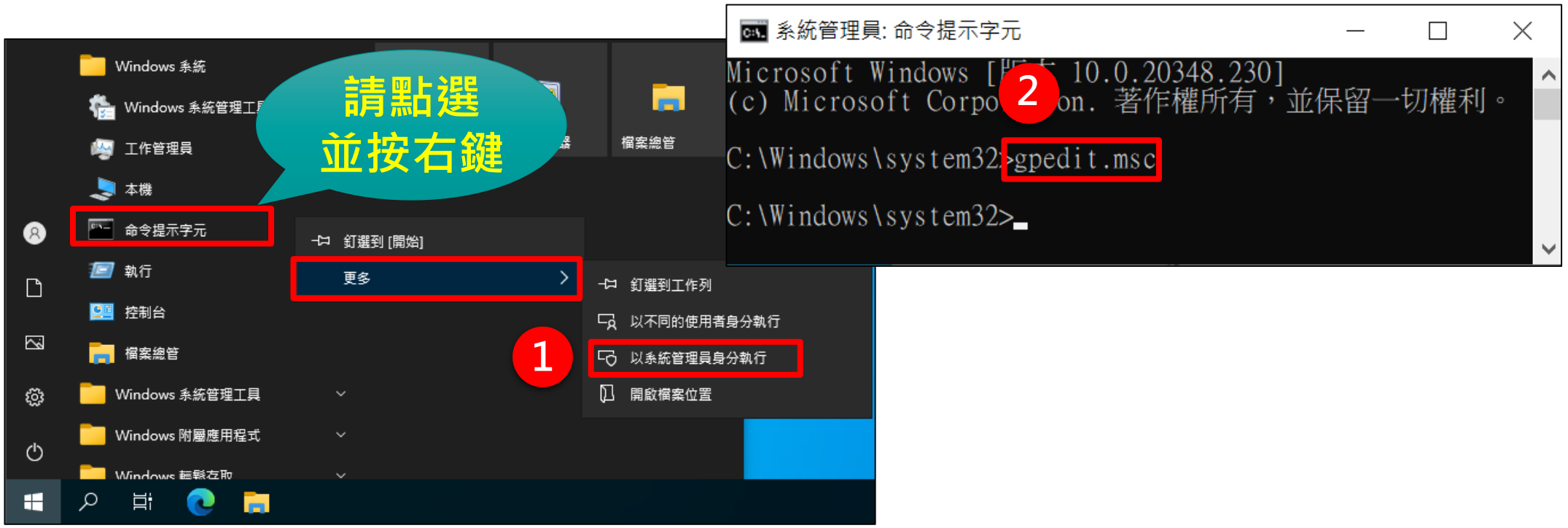


2.2.2 GPO套用狀況檢查方式

GPO套用狀況檢查方式(1/2)

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

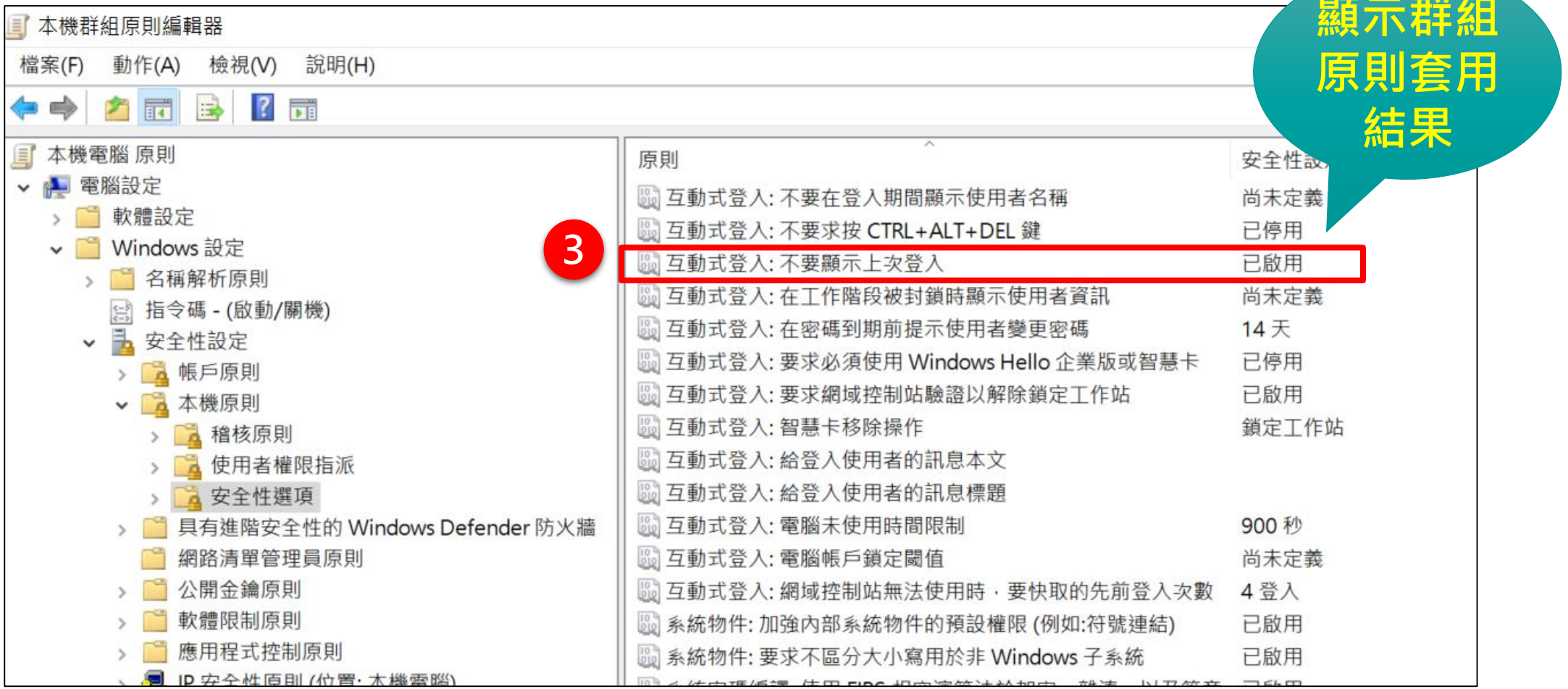
- 使用GPEdit檢查本機群組原則
  - –步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」
  - –步驟2：於「命令提示字元」輸入gpedit.msc查詢本機群組原則結果



GPO套用狀況檢查方式(2/2)

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

–步驟3：抽檢GCB項目，確認是否確實套用(如：電腦設定\Windows設定\安全性設定\本機原則\安全性選項\互動式登入：不要顯示上次登入)



2.2.3 恢復原始設定之方式

恢復原始設定之方式(1/4)

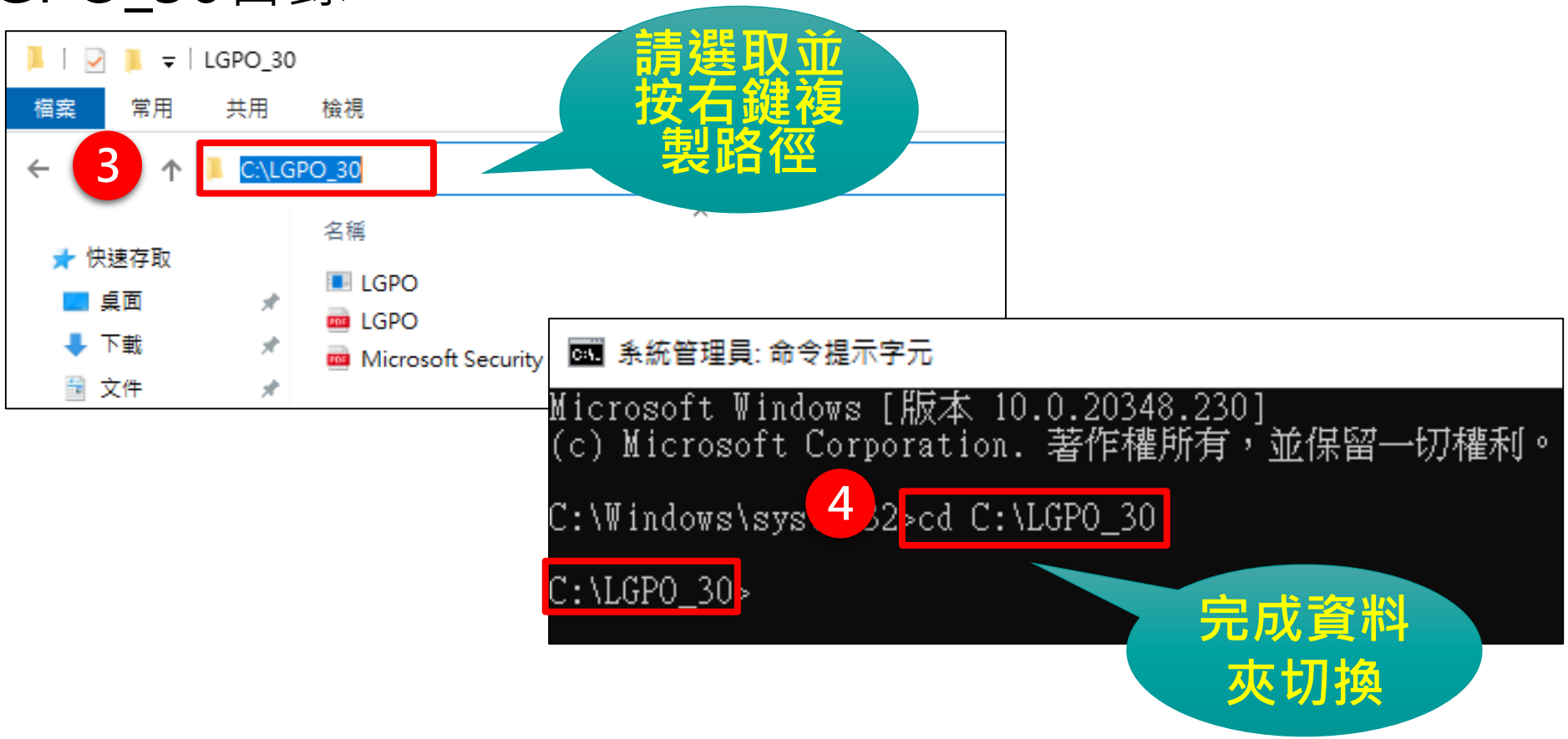
國家資通安全研究院
National Institute of Cyber Security

- 步驟1：點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」)
- 步驟2：於「命令提示字元」輸入刪除本機群組原則資料夾指令 RD /S /Q C:\Windows\System32\GroupPolicy

恢復原始設定之方式(2/4)

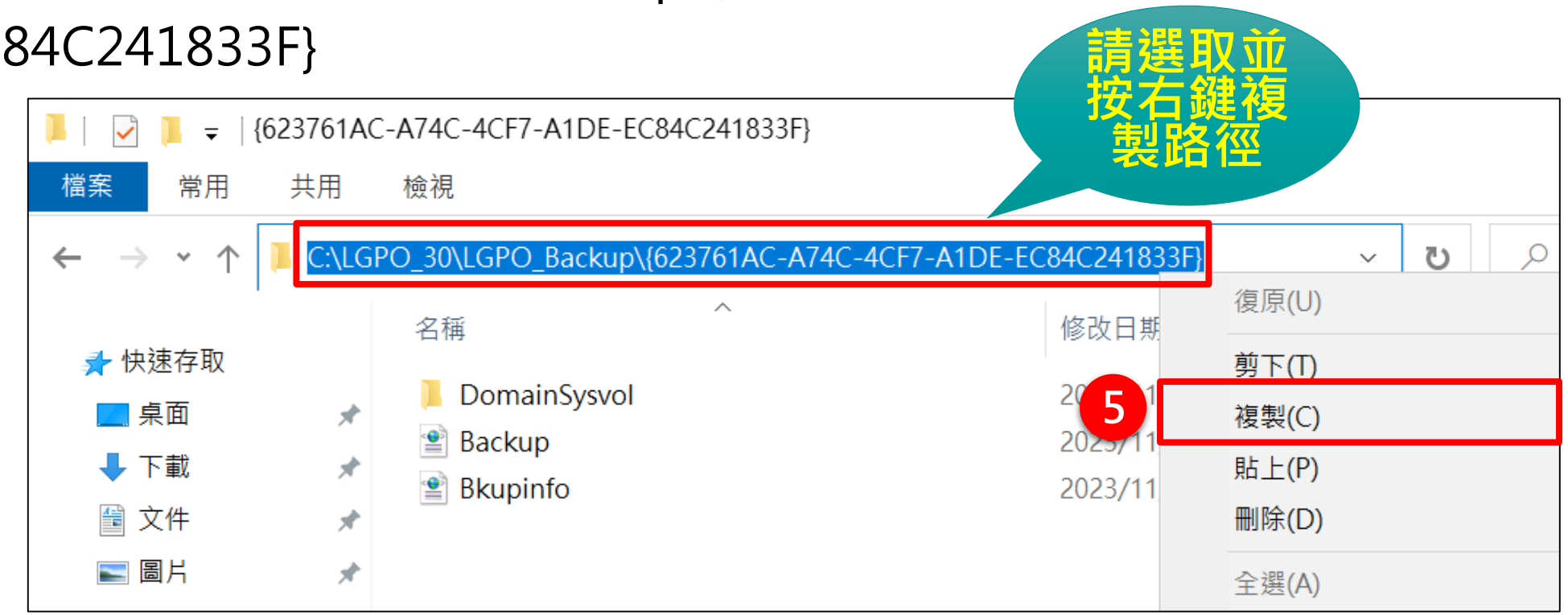
國家資通安全研究院
National Institute of Cyber Security

- 步驟3：複製LGPO應用程式解壓縮後之完整目錄路徑
- 步驟4：於「命令提示字元」輸入cd <LGPO完整目錄路徑>，切換至LGPO_30目錄



恢復原始設定之方式(3/4)

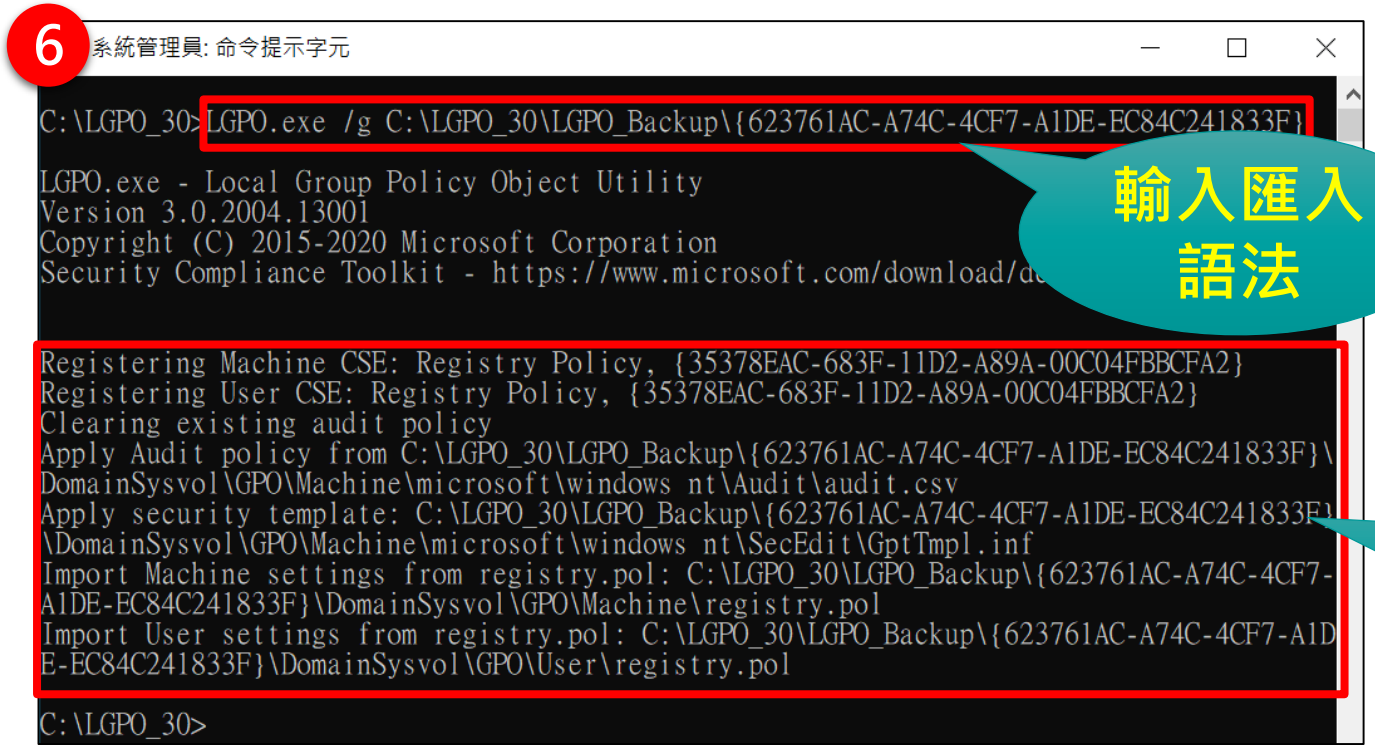
- 步驟5：複製備份的GPO完整目錄路徑
  - 此範例備份之GPO，儲存於C:\LGPO_30\LGPO_Backup資料夾，完整目錄路徑為C:\LGPO_30\LGPO_Backup\{623761AC-A74C-4CF7-A1DE-EC84C241833F}



恢復原始設定之方式(4/4)

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

- 步驟6：於「命令提示字元」輸入LGPO.exe /g <備份的GPO完整目錄路徑>，還原部署Windows Server 2022 GPO前之設定
- 步驟7：請將Windows Server 2022重新開機，或輸入gpupdate /force指令更新群組原則，即可完成恢復原始設定



3. 伺服器角色專用GPO部署方式

共用與專用群組原則GPO

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

- Account Settings與Common Settings為**共用群組原則GPO**
- DC Server、DNS Server、File Server及Web Server為**專用群組原則GPO(伺服器角色專用GPO)**

共用群組原則GPO

專用群組原則GPO(伺服器角色專用GPO)

項次	GPO	項數
1	Windows Server 2022 Account Settings	9
2	Windows Server 2022 Common Settings	314
3	Windows Server 2022 DC Server	29
4	Windows Server 2022 DNS Server	115
5	Windows Server 2022 File Server	120
6	Windows Server 2022 Web Server	117

檢查安裝之伺服器角色(1/5)

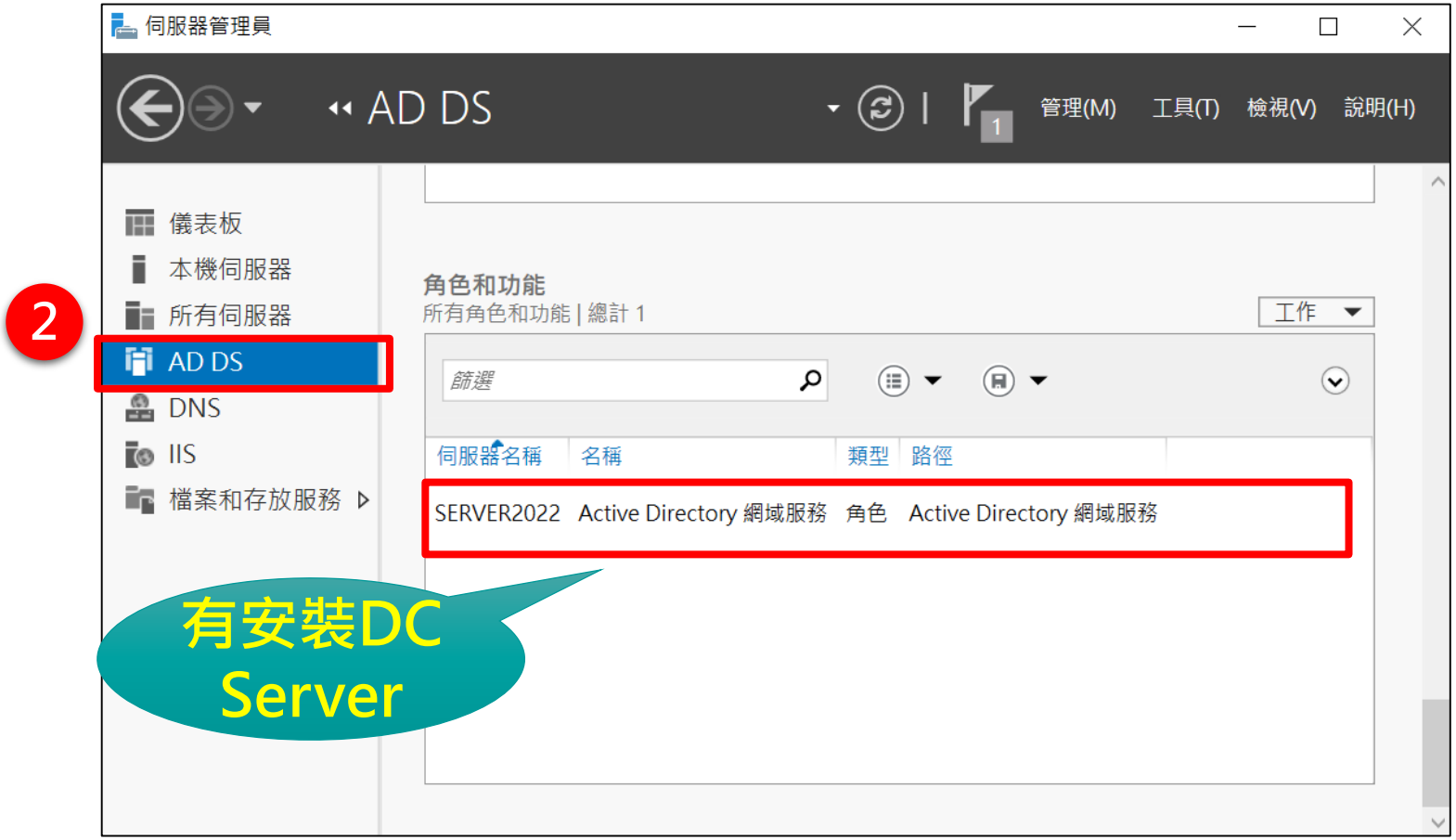
國家資通安全研究院
National Institute of Cyber Security

- Windows Server 2022 GCB定義之伺服器角色，係指於「伺服器管理員」安裝之角色，各角色於「伺服器管理員」之確認方式如下
  - 步驟1：點擊開始→伺服器管理員

檢查安裝之伺服器角色(2/5)

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

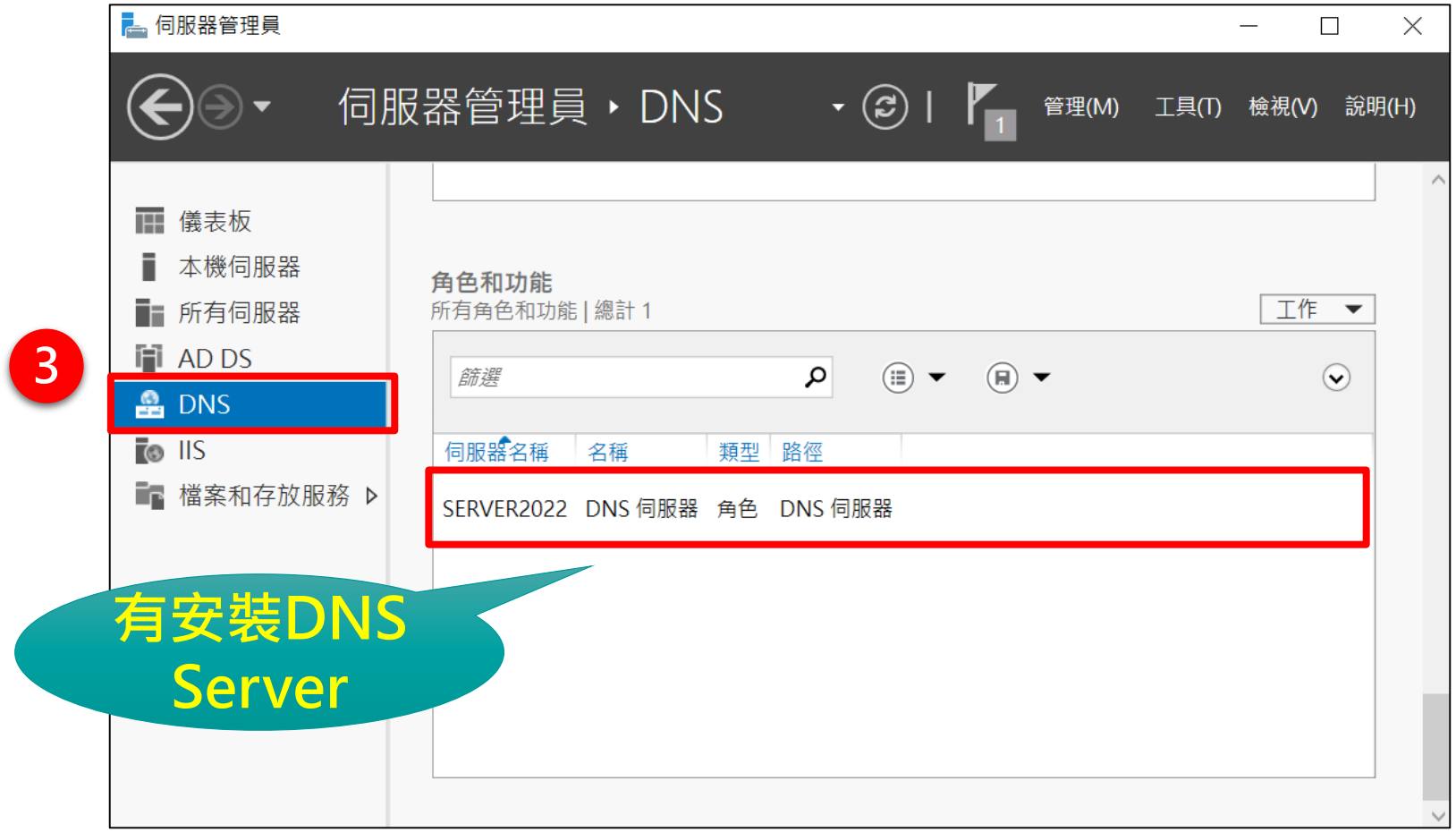
–步驟2：在「伺服器管理員」檢查是否安裝**網域控制站(DC Server)**，點選「AD DS」進入「伺服器」畫面，檢查「角色和功能」列表中是否包含「**Active Directory 網域服務**」角色服務



檢查安裝之伺服器角色(3/5)

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

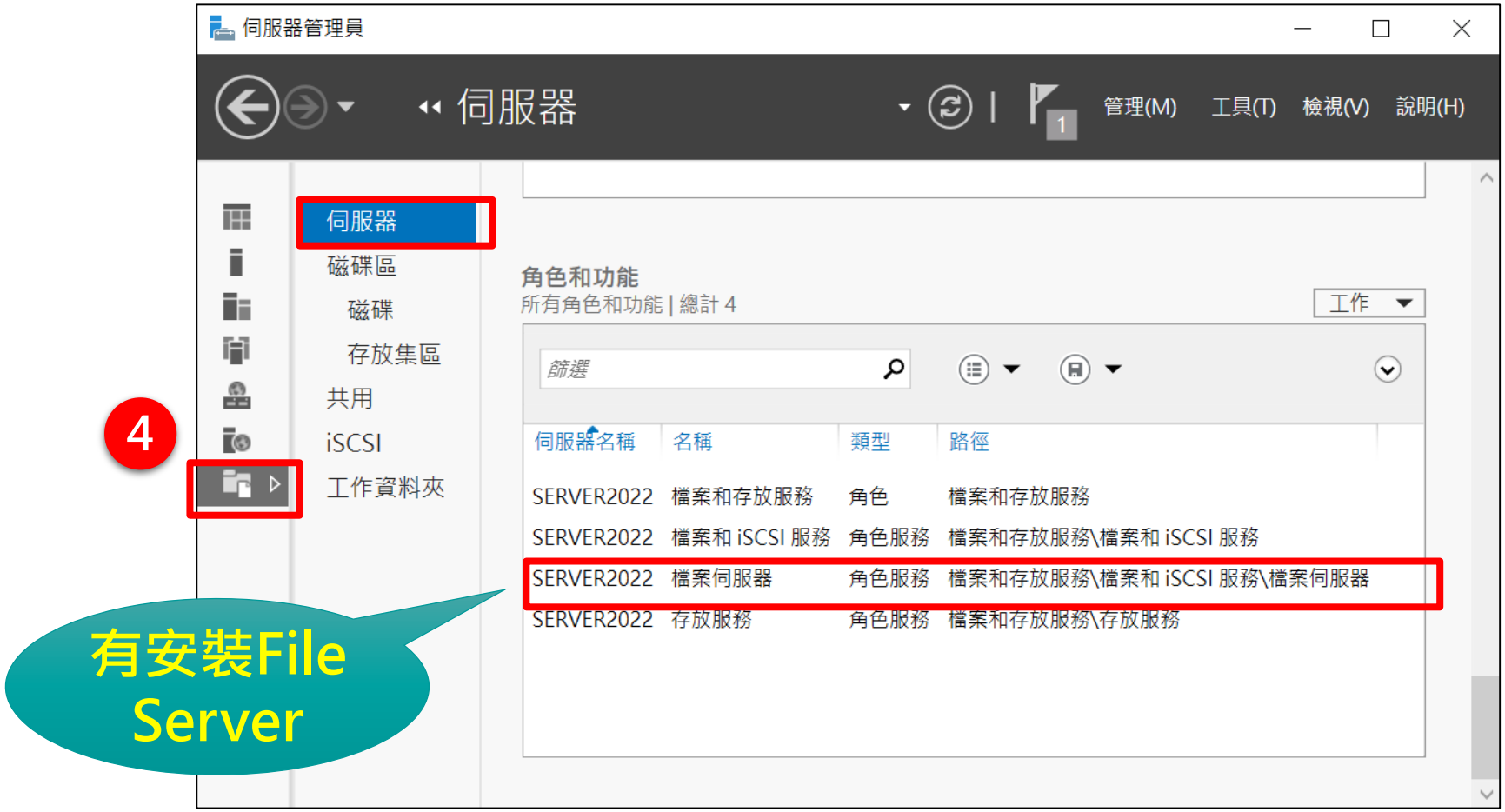
–步驟3：在「伺服器管理員」檢查是否安裝**DNS伺服器(DNS Server)**，點選「DNS」進入「伺服器」畫面，檢查「角色和功能」列表中是否包含「**DNS伺服器**」角色服務



檢查安裝之伺服器角色(4/5)

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

–步驟4：在「伺服器管理員」檢查是否安裝**檔案伺服器(File Server)**，點選「檔案和存放服務」進入「伺服器」畫面，檢查「角色和功能」列表中是否包含「**檔案伺服器**」角色服務



檢查安裝之伺服器角色(5/5)

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

–步驟5：在「伺服器管理員」檢查是否安裝**網頁伺服器(Web Server)**，點選「IIS」進入「伺服器」畫面，檢查「角色和功能」列表中是否包含「**網頁伺服器**」角色服務

3.1 非安裝網域控制站、DNS伺服器、檔案伺服器及網頁伺服器角色之部署說明

GPO部署說明

- 非安裝**網域控制站、 DNS伺服器、檔案伺服器及網頁伺服器**角色之Windows Server 2022伺服器，僅需套用**共用群組原則**的2個GPO，不需套用**專用群組原則**GPO

項次	GPO	分類
1	Windows Server 2022 Account Settings	共用群組原則
2	Windows Server 2022 Common Settings	共用群組原則

3.2 安裝網域控制站、DNS伺服器、檔案伺服器及網頁伺服器角色之部署說明

GPO部署說明(1/4)

- 安裝**網域控制站、 DNS伺服器、檔案伺服器及網頁伺服器**角色之Windows Server 2022伺服器，除了要套用**共用群組原則**的2個GPO，必須再套用其專屬之**專用群組原則**GPO

項次	GPO	分類
1	Windows Server 2022 Account Settings	共用群組原則
2	Windows Server 2022 Common Settings	共用群組原則
3	Windows Server 2022 DC Server	專用群組原則
4	Windows Server 2022 DNS Server	專用群組原則
5	Windows Server 2022 File Server	專用群組原則
6	Windows Server 2022 Web Server	專用群組原則

GPO部署說明(2/4)

- 網域控制站、DNS伺服器、檔案伺服器及網頁伺服器所需套用之**GPO**與其**優勢順序**列表

伺服器角色	GPO優勢順序	GPO	分類
網域控制站	1	Windows Server 2022 DC Server	專用群組原則
	2	Windows Server 2022 Account Settings	共用群組原則
	3	Windows Server 2022 Common Settings	共用群組原則
DNS伺服器	1	Windows Server 2022 DNS Server	專用群組原則
	2	Windows Server 2022 Account Settings	共用群組原則
	3	Windows Server 2022 Common Settings	共用群組原則
File伺服器	1	Windows Server 2022 File Server	專用群組原則
	2	Windows Server 2022 Account Settings	共用群組原則
	3	Windows Server 2022 Common Settings	共用群組原則
Web伺服器	1	Windows Server 2022 Web Server	專用群組原則
	2	Windows Server 2022 Account Settings	共用群組原則
	3	Windows Server 2022 Common Settings	共用群組原則

GPO部署說明(3/4)

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

- GPO部署的優勢順序說明
  - 當**專用群組原則**與**共用群組原則**之GPO同時套用於伺服器時，**專用群組原則**應優勢於**共用群組原則**GPO
- 以網域控制站GPO部署為範例
  - 單機部署：使用LGPO程式導入
    - 單機部署情況下，後匯入之GPO會優勢於之前匯入的GPO
    - 要先匯入**共用群組原則**的2個GPO後，接續再將**專用群組原則**Windows Server 2022 DC Server GPO匯入

伺服器角色	GPO優勢順序	GPO	分類
網域控制站	1	Windows Server 2022 DC Server	專用群組原則
	2	Windows Server 2022 Account Settings	共用群組原則
	3	Windows Server 2022 Common Settings	共用群組原則

GPO部署說明(4/4)

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

–AD部署：使用群組原則管理工具導入

➢在已連結之群組原則物件中的優先順序，將**專用群組原則**之Windows Server 2022 DC Server GPO調整到優勢於**共用群組原則**GPO

網域控制站伺服器部署說明

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

- Windows Server 2022 GCB中有4項群組原則針對網域控制站與非網域控制站伺服器有不同建議設定值，此4項群組原則同時存在於DC Server與Common Settings之GPO中，網域控制站導入GCB時，會同時套用DC Server與Common Settings之GPO ，需以**專用群組原則**的**DC Server GPO設定值為優先使用**

原則設定名稱	分類	DC Server設定值	Common Settings設定值
互動式登入：網域控制站無法使用時，要快取的先前登入次數	安全性選項	0次	4次以下
拒絕從網路存取這台電腦	使用者權限指派	Guests,本機帳戶	Guests,本機帳戶與Administrators群組的成員
從網路存取這台電腦	使用者權限指派	Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS	Administrators, Authenticated Users
稽核電腦帳戶管理	進階稽核原則	成功及失敗	成功

3.3 安裝複數伺服器角色之部署說明

複數伺服器角色部署說明(1/3)

- 安裝複數**專用群組原則**伺服器角色之部署說明
  - 在網域控制站伺服器、DNS伺服器、檔案伺服器及網頁伺服器之**專用群組原則**GPO中，有3項**系統服務**，對前述伺服器角色分別有不同建議設定值

系統服務	DC Server 建議設定值	DNS Server 建議設定值	File Server 建議設定值	Web Server 建議設定值
Application Identity	自動	手動	手動	手動
Distributed Link Tracking Client	手動	自動	自動	自動
Windows Time	自動	手動	手動	手動

  - 在需要同時部署複數**專用群組原則**GPO的情況，為確保上表的3項系統服務符合GCB建議之啟動狀態，在各GPO有不同建議設定值時，GCB的部署設定值須以「**自動**>**手動**>**已停用**」之優先度進行調整

複數伺服器角色部署說明(2/3)

- 複數伺服器角色中**包含網域控制站**之部署說明
  - 以同時部署**網域控制站**與**DNS**伺服器之GPO為範例說明，需以「**自動>手動>已停用**」之優先度調整下列3項系統服務的**設定值**
    - Application Identity
    - Distributed Link Tracking Client
    - Windows Time
  - 依**優先度調整後的設定值**如下表

系統服務	DC Server 建議設定值	DNS Server 建議設定值	依優先度調整後的設定值
Application Identity	自動	手動	自動
Distributed Link Tracking Client	手動	自動	自動
Windows Time	自動	手動	自動

複數伺服器角色部署說明(3/3)

- 複數伺服器角色中**不包含網域控制站**之部署說明
  - 以同時部署DNS、File及Web伺服器之GPO為範例說明，因下列3項系統服務之建議設定值是一致的，**不需要調整設定值**
    - Application Identity
    - Distributed Link Tracking Client
    - Windows Time
  - 依**優先度調整後的設定值**如下表

系統服務	Web Server 建議設定值	File Server 建議設定值	DNS Server 建議設定值	依優先度調整後的設定值
Application Identity	手動	手動	手動	無需調整
Distributed Link Tracking Client	自動	自動	自動	無需調整
Windows Time	手動	手動	手動	無需調整

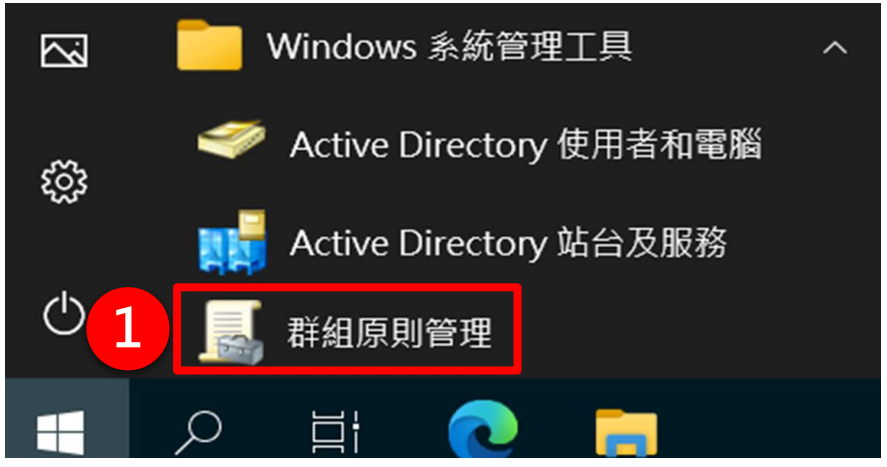
複數伺服器角色AD部署方式(1/12)

- 以同時安裝網域控制站與DNS伺服器角色為範例說明

1. 逐一建立網域控制站與DNS伺服器2個**專用群組原則**GPO，以及2個**共用群組原則**GPO

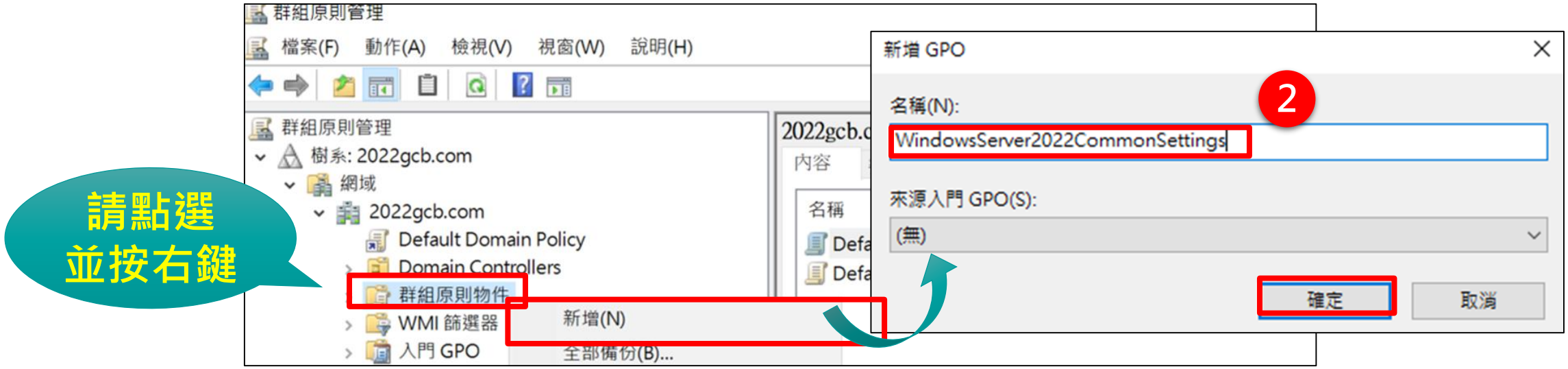
伺服器角色	GPO	分類
網域控制站 兼 DNS伺服器	Windows Server 2022 DC Server	專用群組原則
	Windows Server 2022 DNS Server	專用群組原則
	Windows Server 2022 Account Settings	共用群組原則
	Windows Server 2022 Common Settings	共用群組原則

– 步驟1：點擊開始→Windows系統管理工具→群組原則管理



複數伺服器角色AD部署方式(2/12)

– 步驟2：在群組原則物件節點按滑鼠右鍵→新增→輸入群組原則物件之名稱

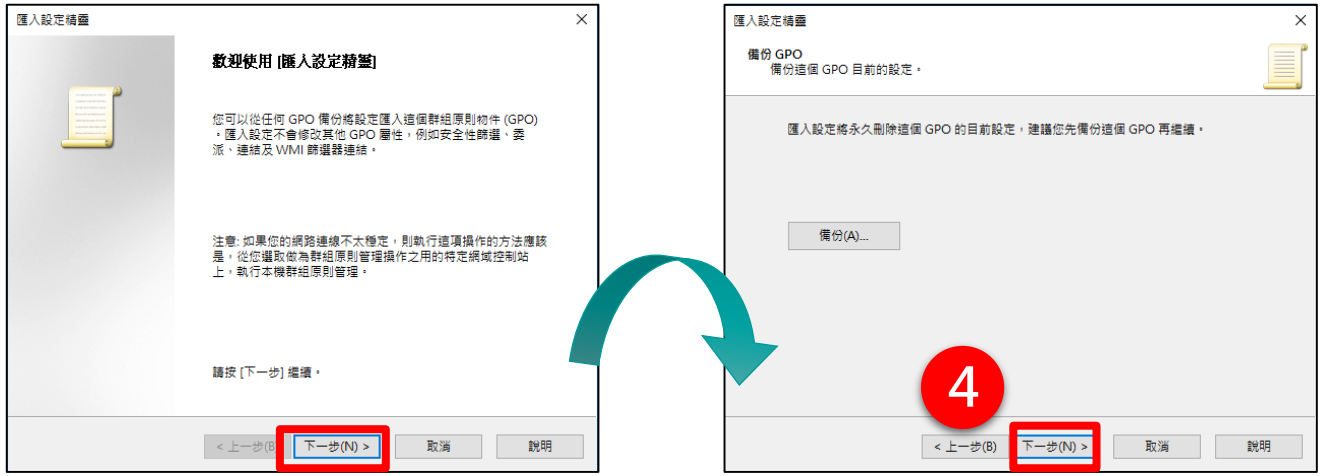


– 步驟3：點選新建之群組原則物件按滑鼠右鍵→選擇「匯入設定值」

複數伺服器角色AD部署方式(3/12)

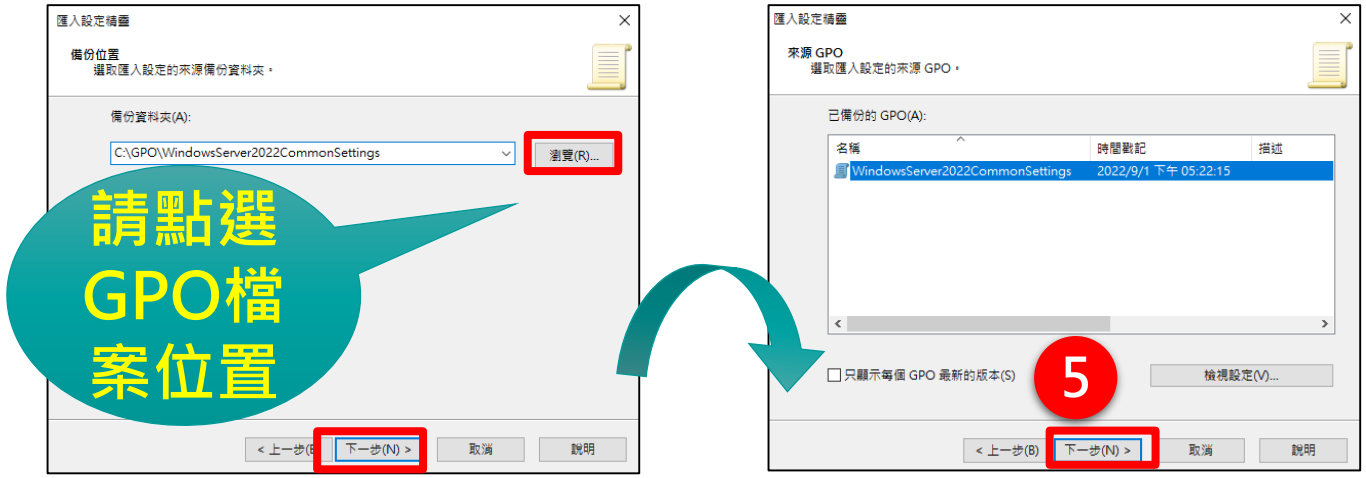
國家資通安全研究院
National Institute of Cyber Security

– 步驟4：在歡迎使用【匯入設定精靈】與備份GPO頁面→點選「下一步」



– 步驟5：在備份位置頁面→選取放置GPO之資料夾→點選「下一步」，

在來源GPO頁面→選取欲匯入之GPO→點選「下一步」



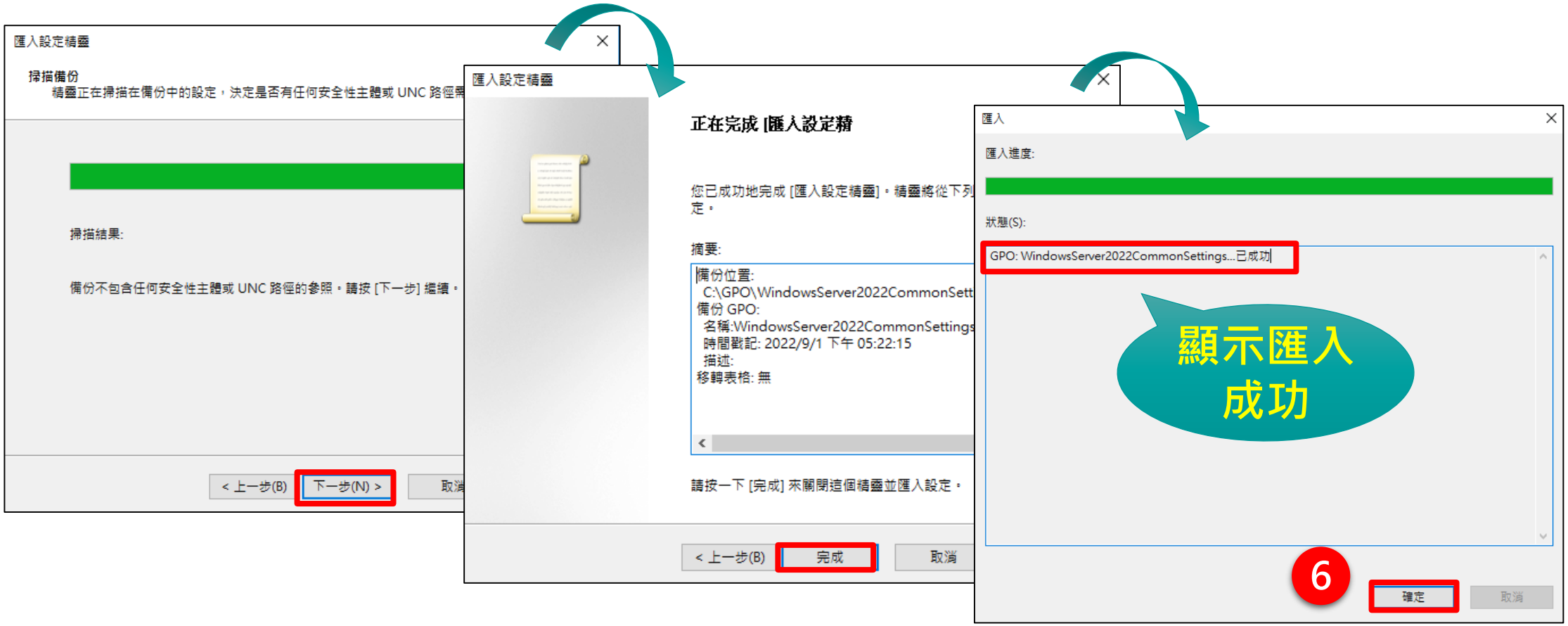
複數伺服器角色AD部署方式(4/12)

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

–步驟6：在掃描備份頁面→點選「下一步」，

在正在完成匯入設定精靈頁面→點選「完成」，

在匯入進度頁面→點選「確定」，完成匯入GPO



複數伺服器角色AD部署方式(5/12)

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

2. 將建立的GPO，逐一**拖曳**至Windows Server 2022伺服器所在之組織單位(此範例為Domain Controllers)進行連結
   - 步驟1：點選已匯入GPO之群組原則物件
   - 步驟2：拖曳至組織單位
   - 步驟3：點選「確定」按鈕，完成將GPO連結至組織單位

請點GPO進行拖曳

複數伺服器角色AD部署方式(6/12)

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

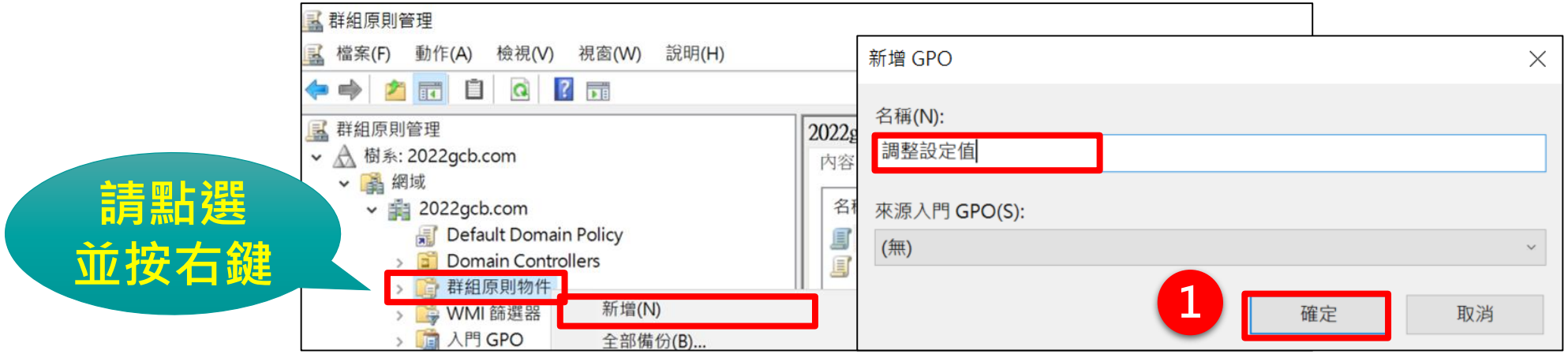
3. 將**專用群組原則**GPO調整到優先於**共用群組原則**GPO
   - 步驟1：點選組織單位(此為Domain Controllers)→已連結的群組原則物件，調整DC Server與DNS Server GPO之連結順序，優先於**共用群組原則**
   - 步驟2：點選「群組原則繼承」，確認GPO之優先順序符合**專用群組原則**優先於**共用群組原則**

複數伺服器角色AD部署方式(7/12)

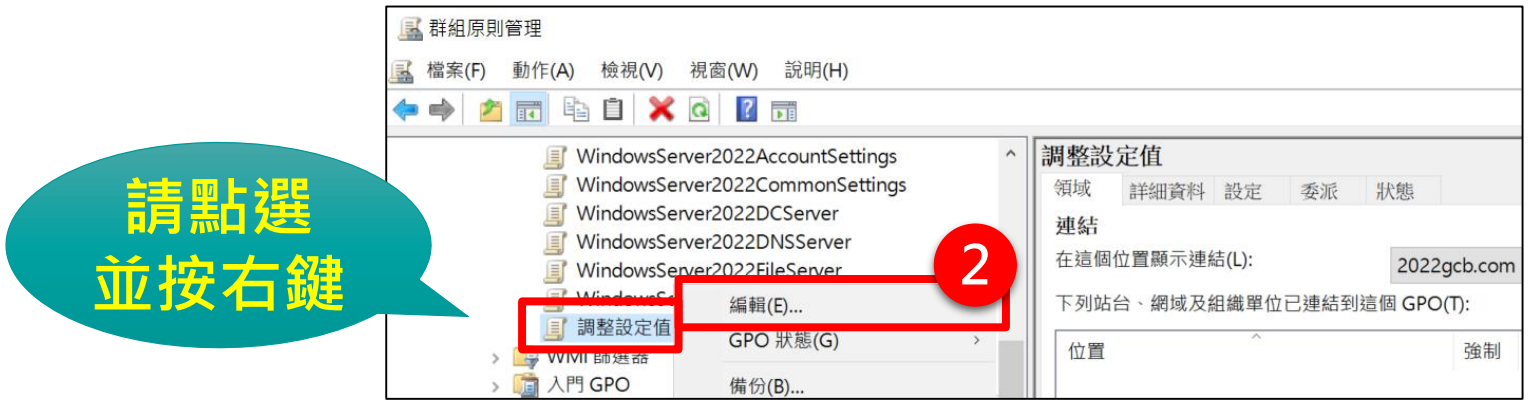
國家資通安全研究院
National Institute of Cyber Security

4. 調整「Application Identity」、「Distributed Link Tracking Client」及「Windows Time」三項系統服務之設定值為「自動」

– 步驟1：在群組原則物件節點按滑鼠右鍵→新增→名稱輸入「調整設定值」



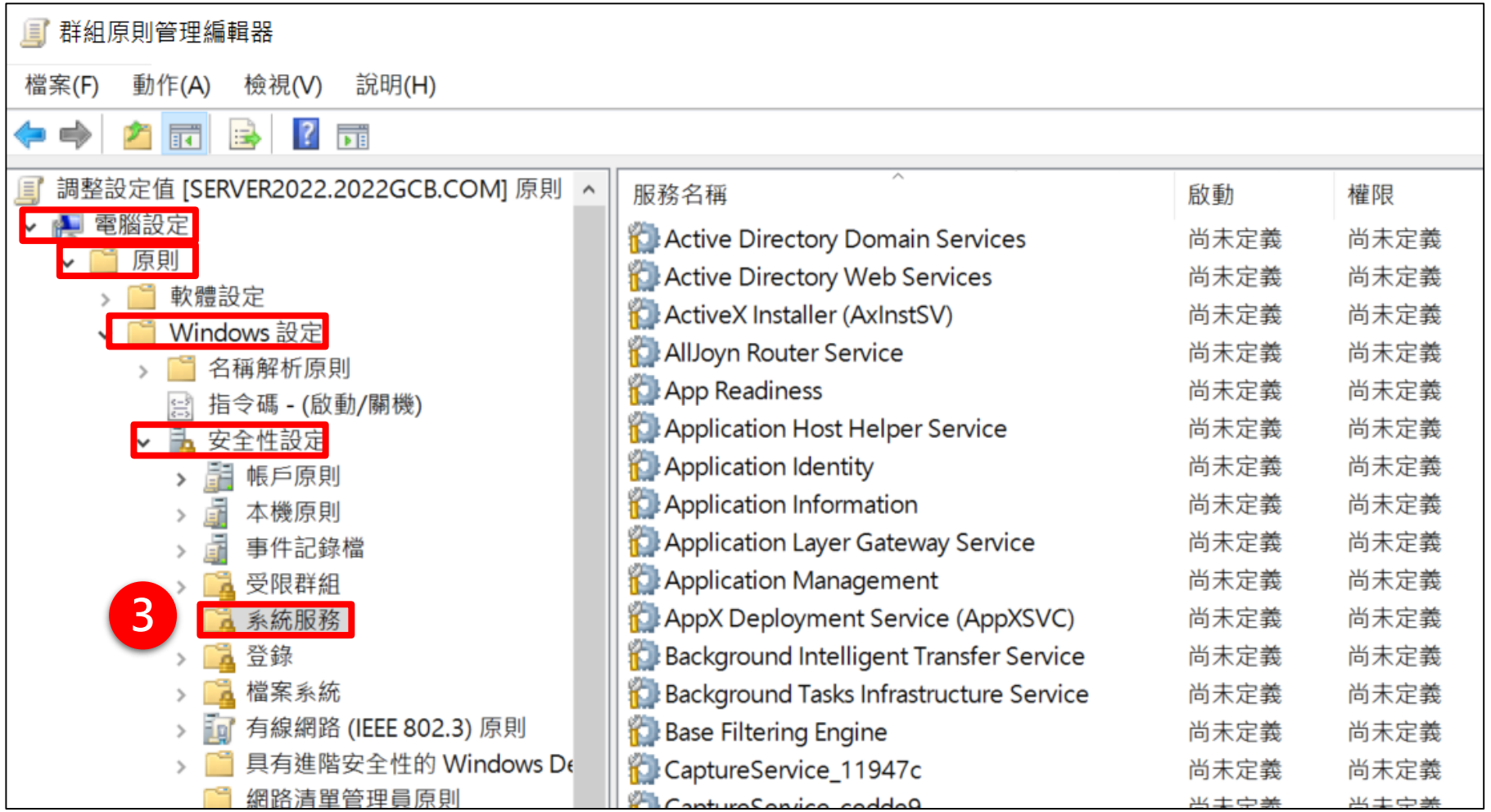
– 步驟2：點選「調整設定值」GPO，按滑鼠右鍵→選擇「編輯」



複數伺服器角色AD部署方式(8/12)

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

–步驟3：在「群組原則管理編輯器」視窗，點選電腦設定→原則→Windows設定→安全性設定→系統服務



複數伺服器角色AD部署方式(9/12)

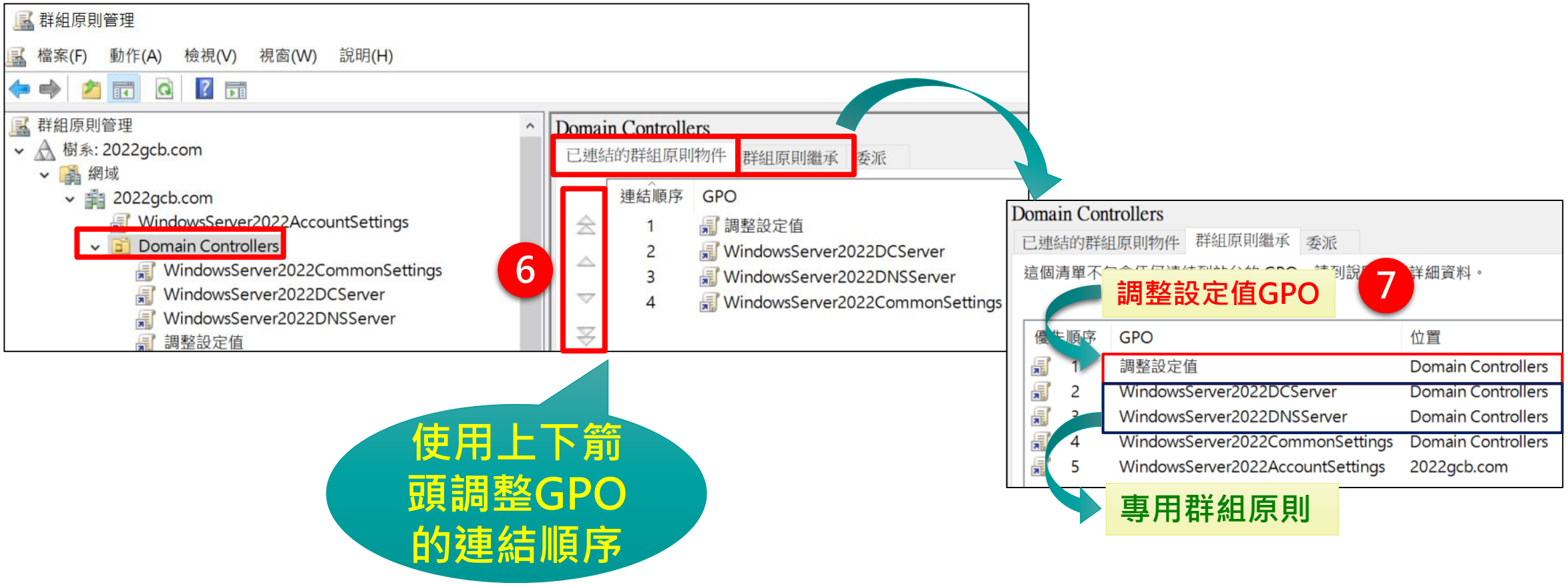
–步驟4：在「系統服務」中，逐一點擊「Application Identity」、「Distributed Link Tracking Client」及「Windows Time」此3項系統服務，進入「內容」頁面，將服務啟動模式設定為「**自動**」

複數伺服器角色AD部署方式(10/12)

–步驟5：將「調整設定值」GPO**拖曳**至組織單位(此為Domain Controllers)進行連結

複數伺服器角色AD部署方式(11/12)

- 步驟6：點選組織單位→已連結的群組原則物件，調整「調整設定值」GPO之連結順序，優先於DC Server與DNS Server GPO
- 步驟7：點選「群組原則繼承」，確認「調整設定值」GPO順序為最優先



複數伺服器角色AD部署方式(12/12)

5. 更新群組原則

– 步驟1：請將Windows Server 2022重新開機，或以系統管理者權限開啟命令提示字元(點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→更多→點選「以系統管理員身分執行」)

– 步驟2：輸入gpupdate /force指令更新群組原則，即可套用GCB設定

參考資料

參考資料

- TWGCB-01-011_Microsoft Windows Server 2022政府組態基準說明文件
  - https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/GCB_Documentation/
- 作業系統GPO
  - https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/GCB_Deployment_Resources/
- Microsoft Security Compliance Toolkit and Baselines
  - https://www.microsoft.com/en-us/download/details.aspx?id=55319

報告完畢 敬請指教

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