政府組態基準(GCB)實作研習活動
Microsoft Edge
組態設定與實作練習

行政院國家資通安全會報技術服務中心

大綱

- 發展緣由
- 發展目的
- 政府組態基準設定分類
- 政府組態基準設定項目
- 政府組態基準部署說明
- 實作練習

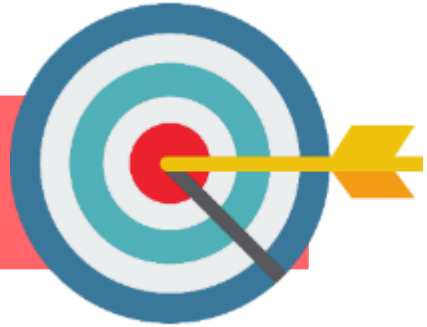
發展緣由

- Microsoft Edge於微軟最新版Windows 10作業系統中取代Internet Explorer成為預設瀏覽器，因此發展Microsoft Edge政府組態基準，並藉由一致性之安全性設定，提升政府機關網頁瀏覽器使用安全性

發展目的

- 針對機關微軟Windows作業系統環境所使用之Edge應用程式進行組態基準設定發展，其目的在於透過GCB的導入，以降低因不安全的設定造成瀏覽器成為駭客入侵管道，進而引發資安事件之疑慮

1. 發展一致的安全組態設定
2. 提升政府機關瀏覽器使用安全性



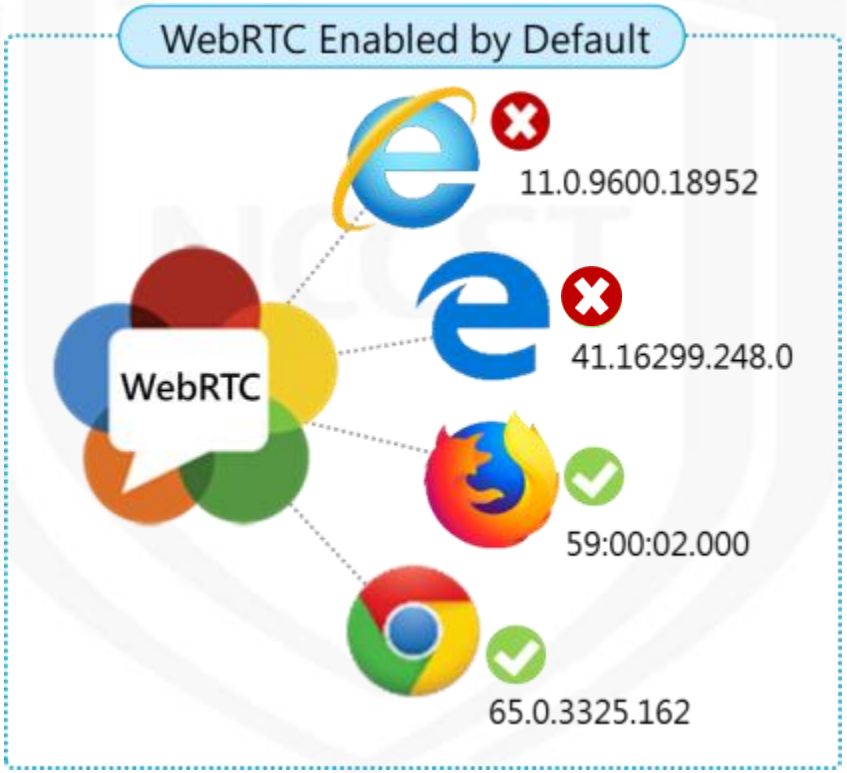
政府組態基準設定分類

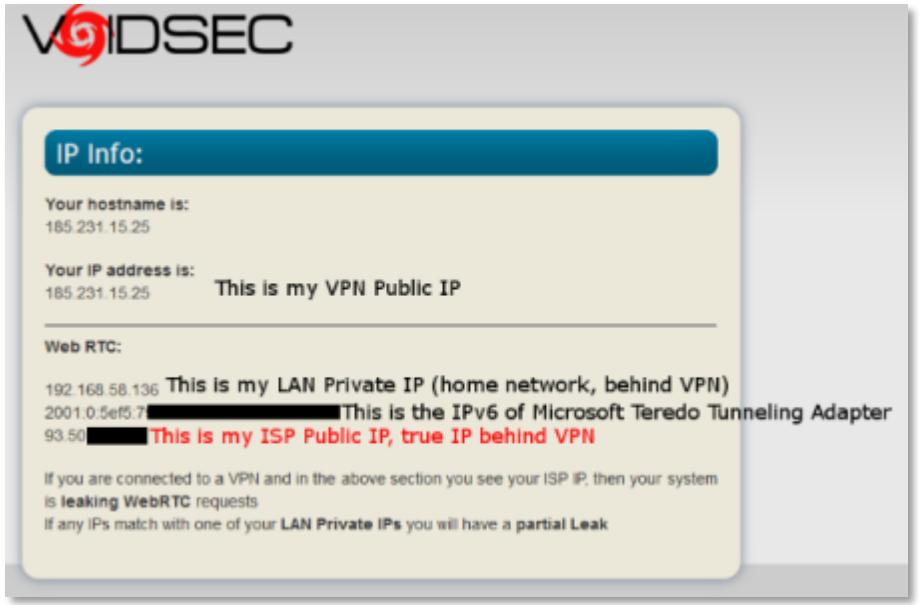
項次	組態基準設定分類	組態基準設定項數
1	安全性和隱私權	8
2	瀏覽器體驗	2
3	擴充功能	1
4	開發人員工具	1
	合計	12

政府組態基準設定項目

資安事件說明(1/2)

- 外國資安研究員Paolo Stagno於2018年3月發現，市面上有23%的VPN服務，透過瀏覽器的WebRTC技術洩漏使用者真實IP位置，而WebRTC在主流瀏覽器多數是預設啟用的，因此建議停用瀏覽器WebRTC





資安事件說明(2/2)

- 網頁即時通訊(Web Real-Time Communication, WebRTC)
  - 是一個支援網頁瀏覽器進行即時語音對話或影片對話的API，無需安裝其他外掛程式或第三方軟體，即可讓雙方使用者直接通訊或分享資料。它於2011年6月1日開源並在Google、Mozilla、Opera支援下被納入全球資訊網協會的W3C推薦標準

防止為WebRTC使用Local Host IP位址(1/2)

- 說明
  - 這項原則設定決定當使用WebRTC通訊協定撥打電話時，是否要顯示員工的Local Host IP位址
  - 若啟用此設定，會在使用WebRTC撥打電話時隱藏Local Host IP位址
- 設定路徑
  - 電腦設定\系統管理範本\電腦元件\Microsoft Edge
- 建議值
  - 啟用

防止為WebRTC使用Local Host IP位址(2/2)

- 群組原則設定前與設定後之差異

啟用前

啟用後

資安事件說明

- 趨勢科技在2018年底發布了2019年資安預測報告，以網路釣魚的威脅態勢而言，根據趨勢統計，攔截的網路釣魚相關網址數量逐年攀升，2019年還會更高。隨著行動平臺的盛行，如要針對不同系統開發漏洞攻擊套件變得費工，還要面臨廠商更新修補，因此，社交工程網路釣魚將是網路犯罪者更傾向採用的方式

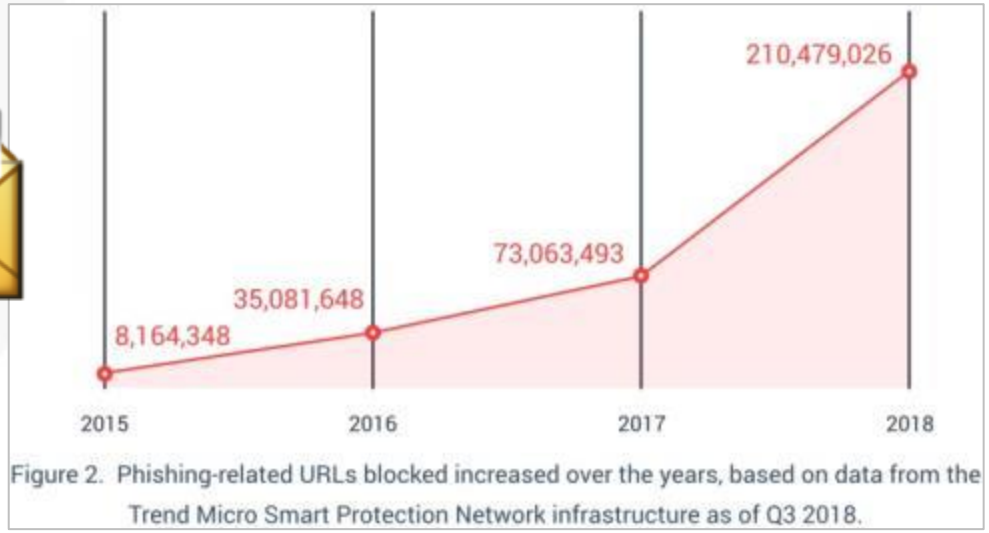
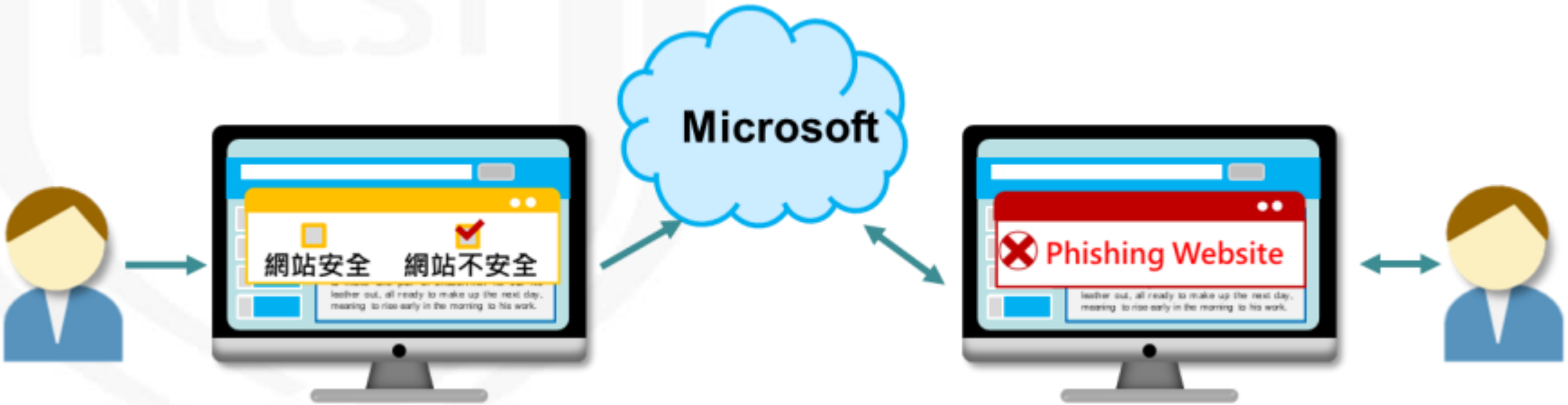


Figure 2. Phishing-related URLs blocked increased over the years, based on data from the Trend Micro Smart Protection Network infrastructure as of Q3 2018.

設定Windows Defender SmartScreen(1/3)

- Windows Defender SmartScreen
  - 有助於防止使用者進入Microsoft認定會嘗試竊取個人資訊的詐騙網站與下載惡意軟體。根據報告的網路釣魚網站、惡意程式碼、惡意探索和詐騙網站動態線上清單來檢查網站 (URL)。已下載之檔案的相關資訊，例如檔案的雜湊以及檔案的數位簽章，可以針對線上服務進行檢查，以判斷已下載之程式的評價



設定Windows Defender SmartScreen(2/3)

- 說明
  - 這項原則設定決定是否要開啟Windows Defender SmartScreen。Windows Defender SmartScreen可提供警告訊息，避免使用者受到潛在網路釣魚詐騙與惡意軟體的威脅。預設情況下，系統會開啟Windows Defender SmartScreen
  - 若啟用此設定，系統會開啟Windows Defender SmartScreen，使用者無法關閉
- 設定路徑
  - 電腦設定\系統管理範本\電腦元件\Microsoft Edge
- 建議值
  - 啟用

設定Windows Defender SmartScreen(3/3)

- 群組原則設定前與設定後之差異

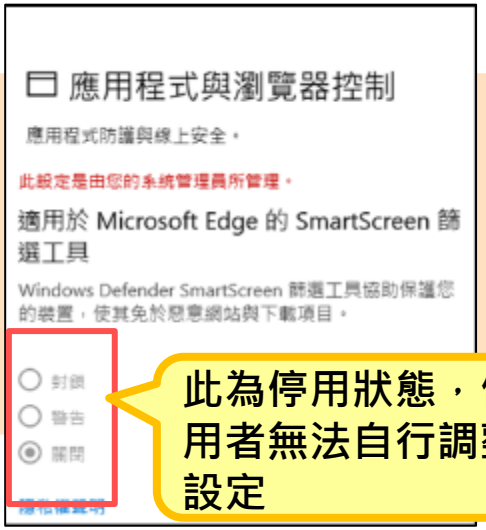
啟用前

使用者可自行決定是否啟用

雖看似未設定，但微軟預設為啟用

啟用後

使用者無法自行調整設定



此為停用狀態，使用者無法自行調整設定

防止略過網站的Windows Defender SmartScreen提示(1/2)

- 說明
  - 這項原則設定決定使用者是否可以覆寫有關潛在惡意網站的Windows Defender SmartScreen警告
  - 若啟用此設定，使用者無法略過Windows Defender SmartScreen警告，且系統會防止使用者繼續瀏覽該網站
- 設定路徑
  - 電腦設定\系統管理範本\電腦元件\Microsoft Edge
- 建議值
  - 啟用

防止略過網站的Windows Defender SmartScreen提示(2/2)

- 群組原則設定前與設定後之差異

啟用前

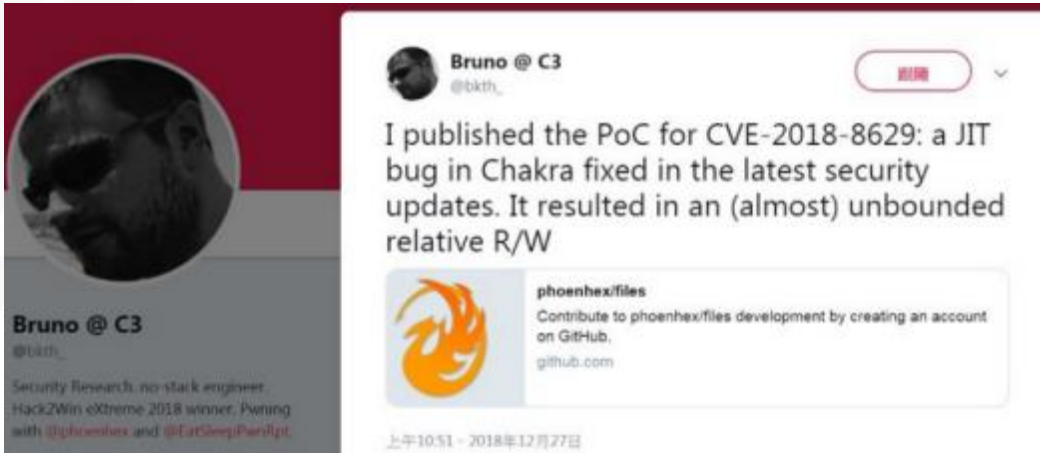
啟用後

防止略過檔案的Windows Defender SmartScreen提示

- 說明
  - 這項原則設定決定使用者是否可覆寫有關下載未經驗證之檔案的Windows Defender SmartScreen警告
  - 若啟用此設定，使用者無法略過Windows Defender SmartScreen警告，且系統會防止使用者繼續下載未經驗證的檔案
- 設定路徑
  - 電腦設定\系統管理範本\電腦元件\Microsoft Edge
- 建議值
  - 啟用

資安事件說明

- 2018年12月，軟體開發商Phoenix Technologies的研究人員Bruno Keith公布Microsoft Edge漏洞的攻擊程式，此漏洞編號為CVE-2018-8629漏洞。當Edge所使用的JavaScript引擎Chakra不當處理記憶體中的物件時，即會觸發該漏洞，駭客可架設一個惡意網站或是滲透正當網站誘導Edge使用者造訪，成功的開採即允許駭客取得使用者權限，包含安裝或移除程式、更改或刪除資料，以及建立帳號，掌控被駭系統



設定密碼管理員(1/3)

- 說明
  - 這項原則設定決定使用者是否可以使用「密碼管理員」在本機儲存其密碼。預設情況下，系統會開啟「密碼管理員」
  - 若停用此設定，使用者無法使用「密碼管理員」在本機儲存其密碼
- 設定路徑
  - 電腦設定\系統管理範本\電腦元件\Microsoft Edge
- 建議值
  - 停用

設定密碼管理員(2/3)

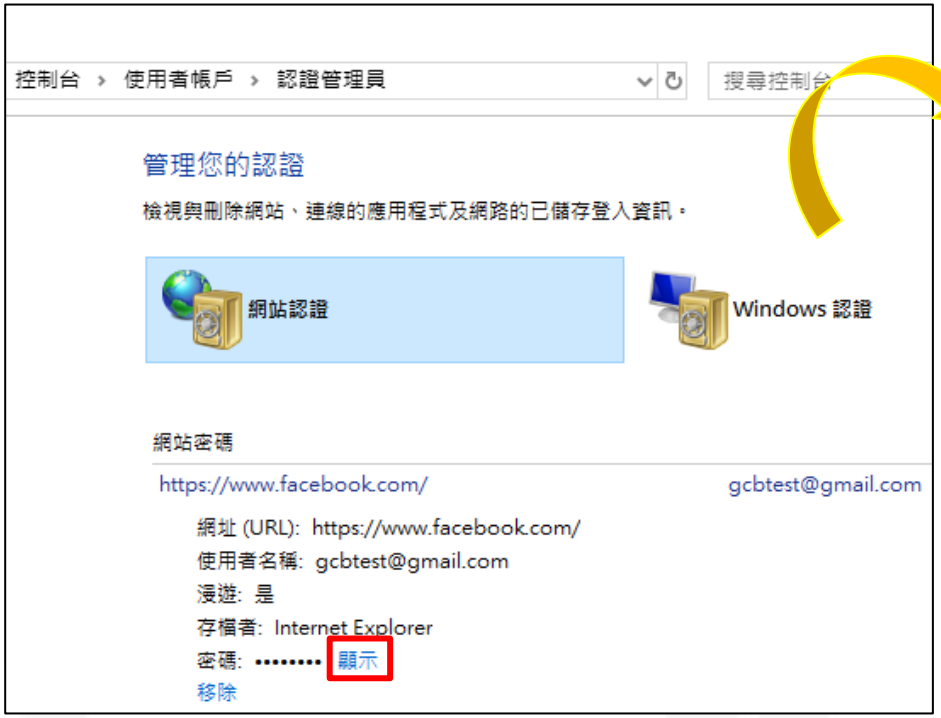
- 群組原則設定前與設定後之差異

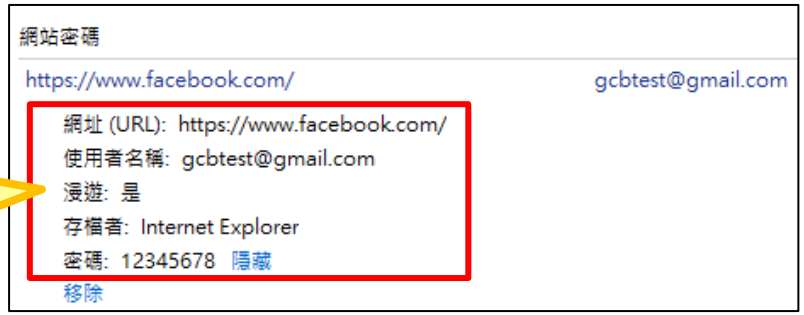
停用前

停用後

設定密碼管理員(3/3)

- 群組原則設定前與設定後之差異





當使用者電腦的帳號密碼外洩時，透過Edge所儲存的帳號密碼也面臨外洩風險

資安事件說明

- 內政部警政署發布防詐騙警訊，2019年6月出現常見的抽獎詐騙網頁惡意彈跳視窗，無論在Android、iOS系統或是電腦版網頁上都會出現，讓使用者誤以為真的中獎，而掉入詐騙陷阱。網頁跳出廣告通知中獎的詐騙手法，內容會隨著更新為目前市面上最新版的手機，並提出小問題，目的就是要竊取個人資料

設定快顯封鎖程式(1/2)

- 說明
  - 這項原則設定決定是否要開啟「快顯封鎖程式」。預設情況下，系統會開啟「快顯封鎖程式」
  - 若啟用此設定，系統會開啟「快顯封鎖程式」以防止顯示快顯視窗
- 設定路徑
  - 電腦設定\系統管理範本\電腦元件\Microsoft Edge
- 建議值
  - 啟用

設定快顯封鎖程式(2/2)

- 群組原則設定前與設定後之差異

啟用後

微軟預設情況下，系統會開啟「快顯封鎖程式」

若關閉

資安事件說明

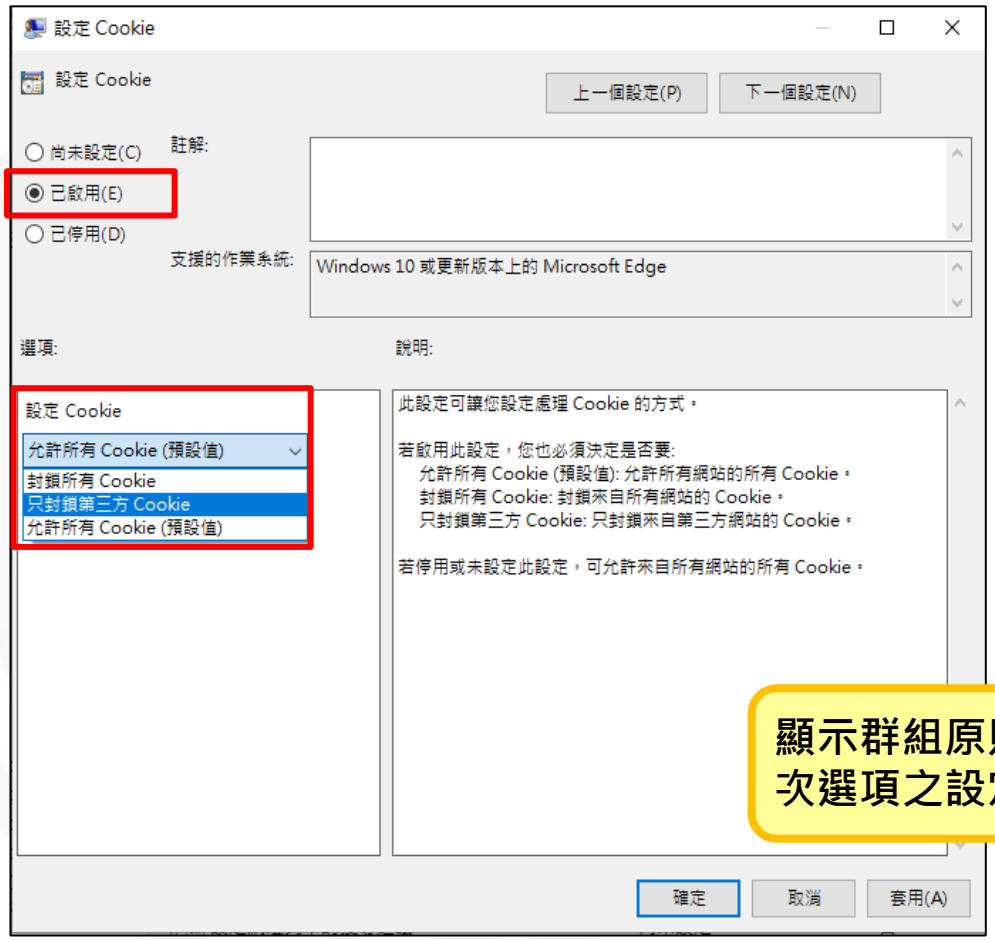
- 2018年3月爆發的劍橋分析醜聞，不當取得臉書8,700多萬用戶的個資。當用戶授權活動資訊的API後，第三方就能存取用戶個資、數位足跡及個人喜好等，且開發人員還能一併取得這些用戶好友們的各種資料，而不需要進一步獲得這群好友的授權，因此停用第三方cookie將可降低使用者行為等資訊被他人蒐集之風險

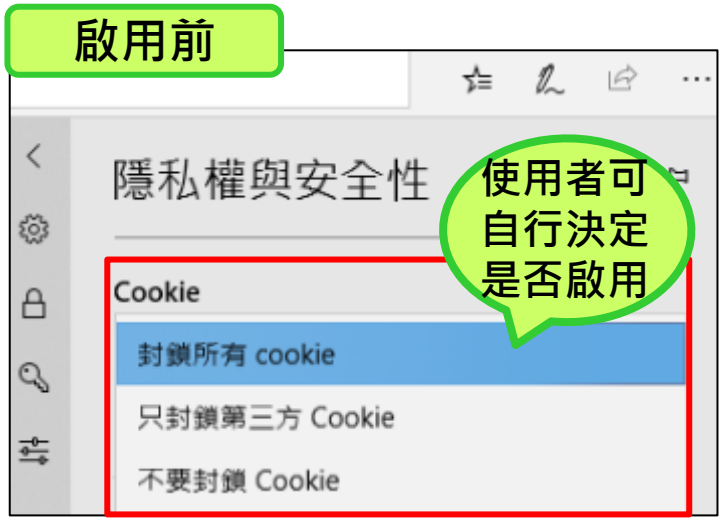
設定Cookie(1/2)

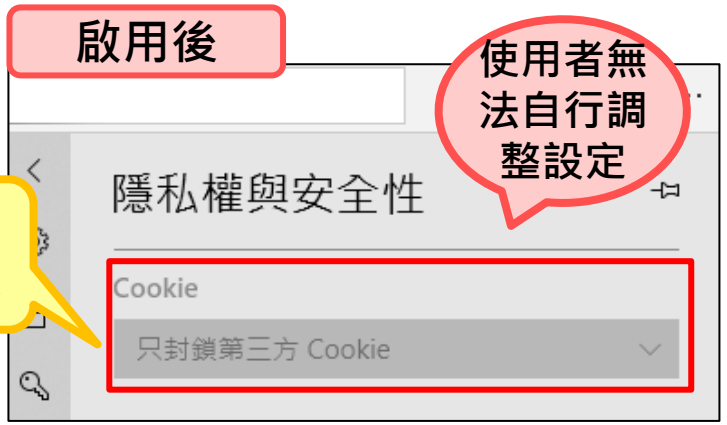
- 說明
  - 這項原則設定決定處理Cookie的方式
  - 若啟用此設定，必須決定是否要：
    - 允許所有Cookie(預設值)：允許所有網站的所有Cookie
    - 封鎖所有Cookie：封鎖來自所有網站的Cookie
    - 只封鎖第三方Cookie：只封鎖來自第三方網站的Cookie
- 設定路徑
  - 電腦設定\系統管理範本\電腦元件\Microsoft Edge
- 建議值
  - 啟用，只封鎖第三方Cookie

設定Cookie(2/2)

- 群組原則設定前與設定後之差異







顯示群組原則次選項之設定

資安事件說明

- 芬蘭的網頁開發人員Viljami Kuosmanen於2017年1月發現，包括Chrome與Safari等瀏覽器的自動填入(autofill)功能暗藏網釣風險，可能會曝露未經使用者同意的個人資訊。駭客透過藏匿表格資訊，看起來只要求使用者填入姓名及電子郵件，實際上卻可獲得使用者所儲存的所有個資，例如國別、地址、電話號碼等資訊

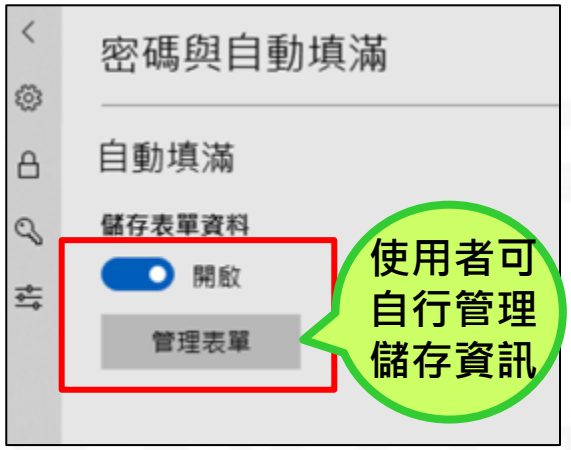
設定自動填寫(1/2)

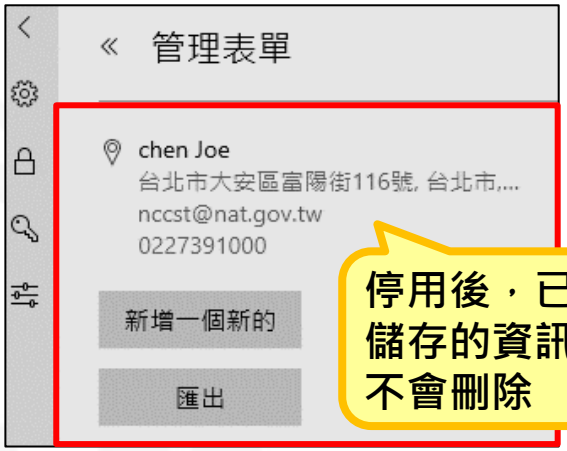
- 說明
  - 這項原則設定決定使用者是否可以在使用Microsoft Edge時，使用「自動填寫」來自動填寫表單欄位。預設情況下，使用者可以選擇是否要使用「自動填寫」
  - 若停用此設定，使用者無法在使用Microsoft Edge時，使用「自動填寫」來自動填寫表單
- 設定路徑
  - 電腦設定\系統管理範本\電腦元件\Microsoft Edge
- 建議值
  - 停用

設定自動填寫(2/2)

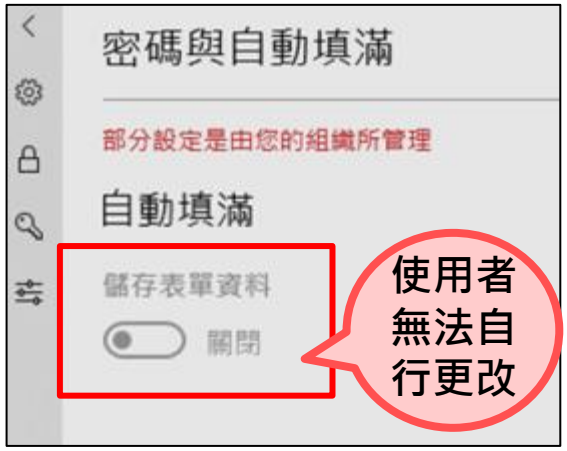
- 群組原則設定前與設定後之差異

停用前

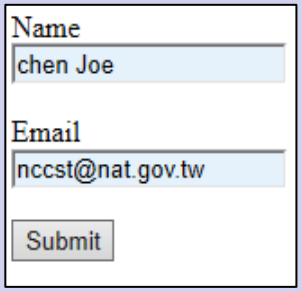


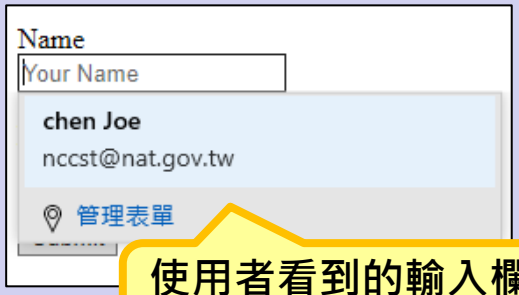


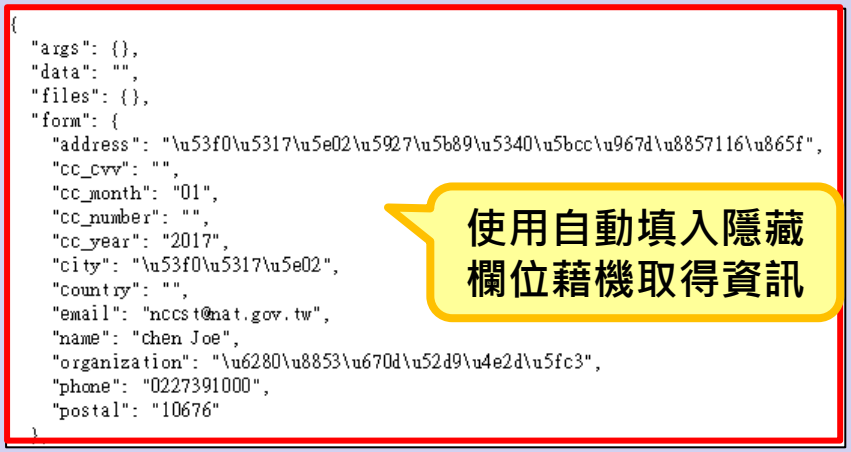
停用後



範例

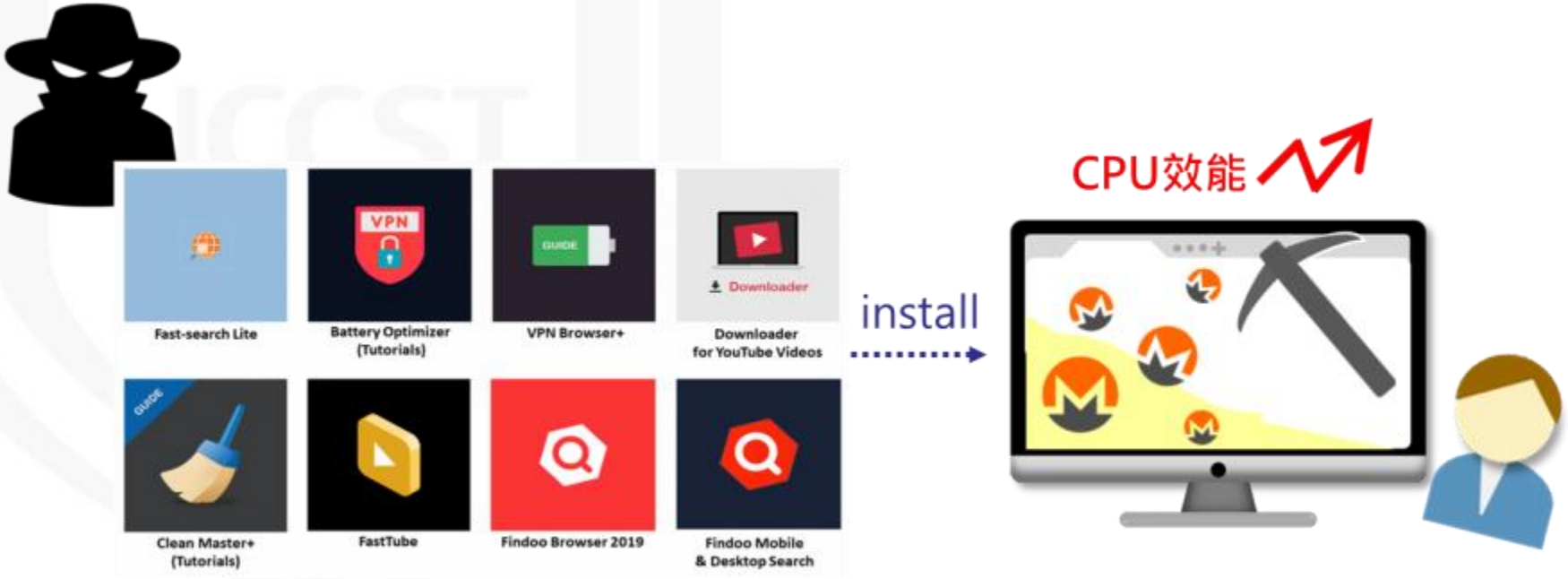






資安事件說明

- 賽門鐵克在2019年1月於微軟官方程式市集Microsoft Store中發現了8款程式，這些看似正常的合法程式卻藏有挖礦機制，可利用使用者的電腦資源來開採門羅幣(Monero)，這些程式可在Windows 10上執行，且在程式的描述中完全未提及挖礦功能



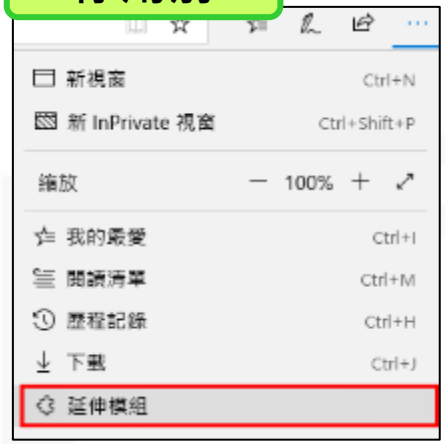
允許延伸模組(1/2)

- 說明
  - 這項原則設定決定使用者是否可以在Microsoft Edge中載入延伸模組
  - 若停用此設定，使用者無法使用Edge延伸模組
- 設定路徑
  - 電腦設定\系統管理範本\電腦元件\Microsoft Edge
- 建議值
  - 停用

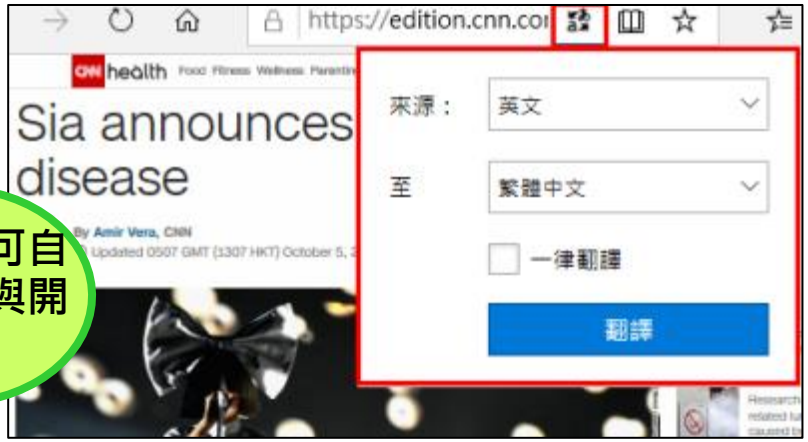
允許延伸模組(2/2)

- 群組原則設定前與設定後之差異

停用前



使用者可自行安裝與開啟功能



停用後

使用者無法自行更改

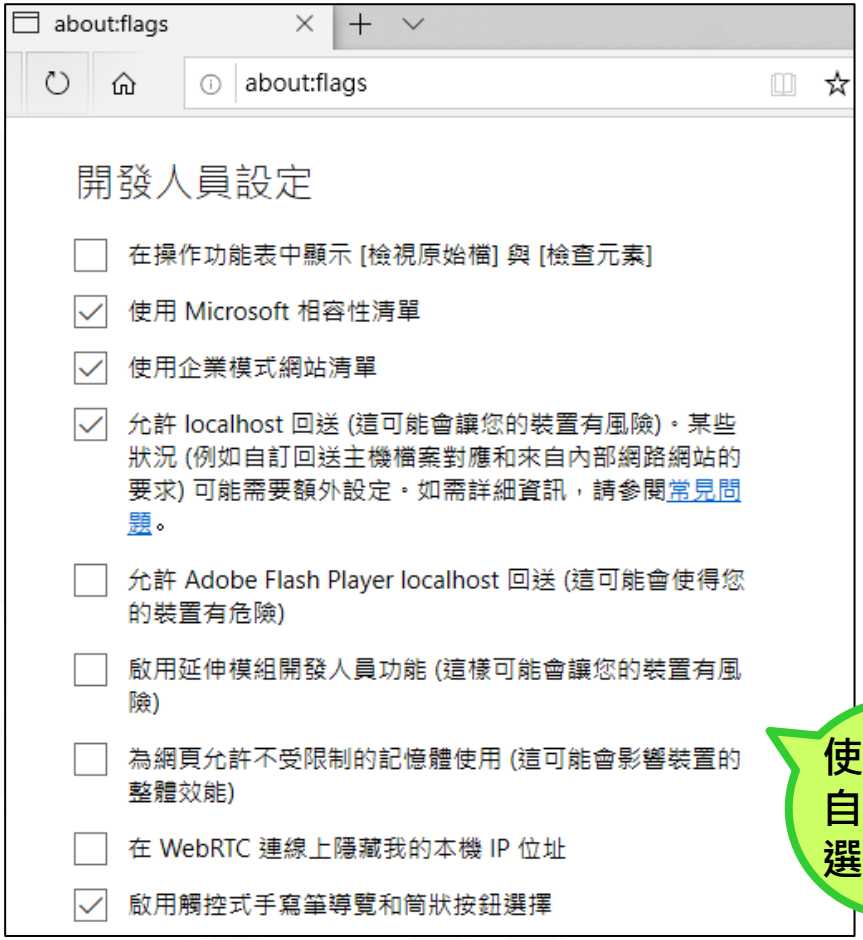
防止在Microsoft Edge中存取about:flags頁面(1/2)

- 說明
  - 這項原則設定決定使用者是否能存取about:flags頁面，此頁面是用來變更開發人員設定或啟用實驗性功能
  - 若啟用此設定，使用者將無法存取about:flags頁面
- 設定路徑
  - 電腦設定\系統管理範本\電腦元件\Microsoft Edge
- 建議值
  - 啟用

防止在Microsoft Edge中存取about:flags頁面(2/2)

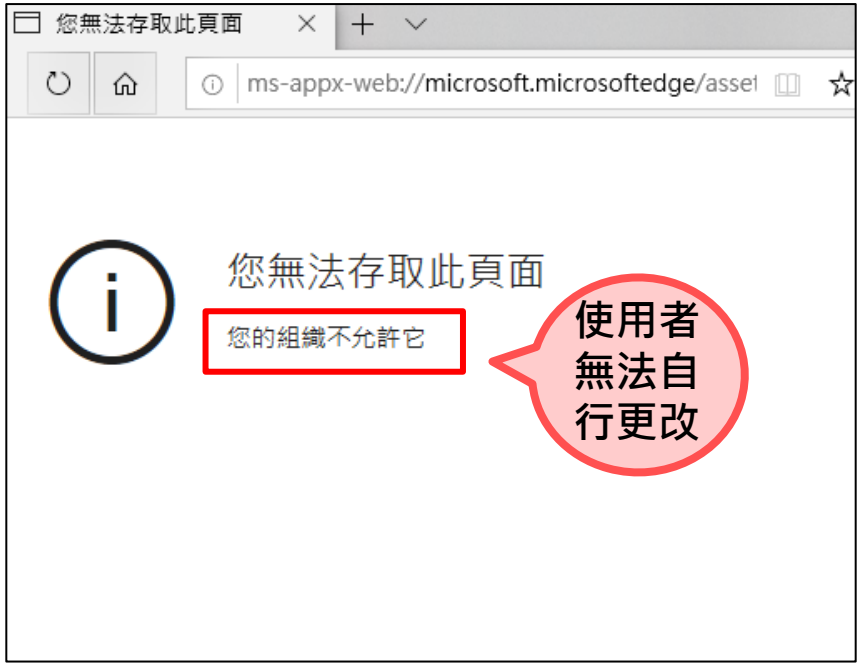
- 群組原則設定前與設定後之差異

啟用前



使用者可自行勾選選項

啟用後



使用者無法自行更改

允許InPrivate瀏覽(1/2)

- 說明
  - 這項原則設定決定使用者是否可使用InPrivate網站瀏覽功能進行瀏覽
  - 停用此設定，使用者無法使用InPrivate網站瀏覽功能
- 設定路徑
  - 電腦設定\系統管理範本\電腦元件\Microsoft Edge
- 建議值
  - 停用

允許InPrivate瀏覽(2/2)

- 群組原則設定前與設定後之差異

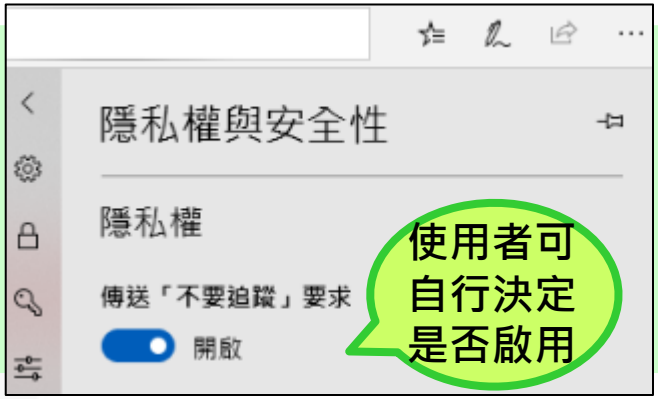
設定「不要追蹤」(1/2)

- 說明
  - 這項原則設定決定使用者是否可以傳送「不要追蹤」的註記到要求追蹤資訊的網站。預設情況下，系統不會傳送「不要追蹤」註記，但使用者可以選擇開啟並傳送註記
  - 若啟用此設定，系統一律會傳送「不要追蹤」的註記到要求追蹤資訊的網站
- 設定路徑
  - 電腦設定\系統管理範本\電腦元件\Microsoft Edge
- 建議值
  - 啟用

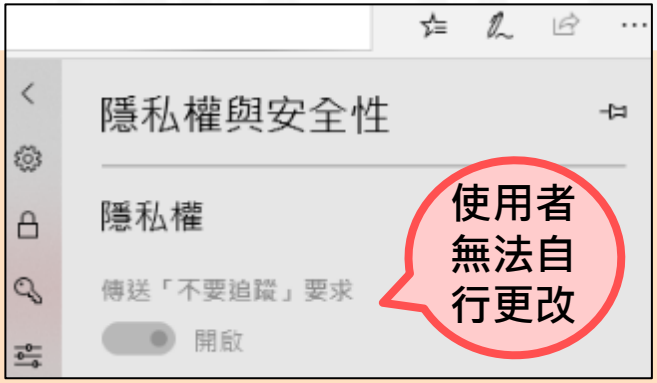
設定「不要追蹤」(2/2)

- 群組原則設定前與設定後之差異

啟用前



啟用後



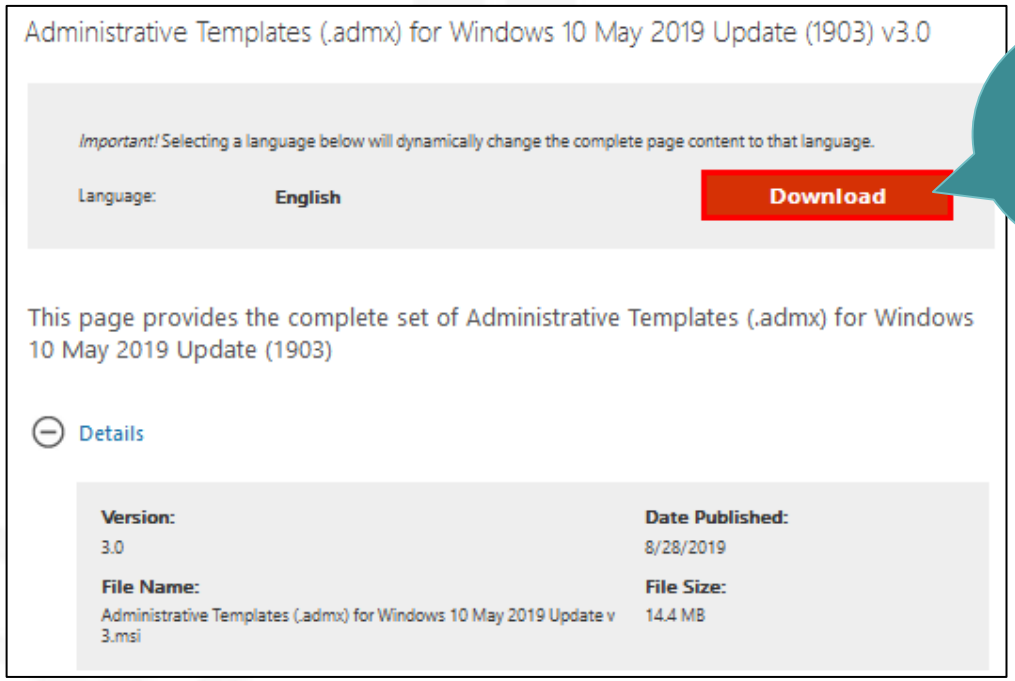
政府組態基準部署說明

AD環境部署說明

安裝Microsoft Edge
系統管理範本

安裝Microsoft Edge系統管理範本(1/3)

- Microsoft Edge系統管理範本說明
  - Microsoft Edge系統管理範本提供了Windows 10內建Edge瀏覽器之群組原則與設定路徑
  - 下載位置：https://www.microsoft.com/en-us/download/details.aspx?id=58495



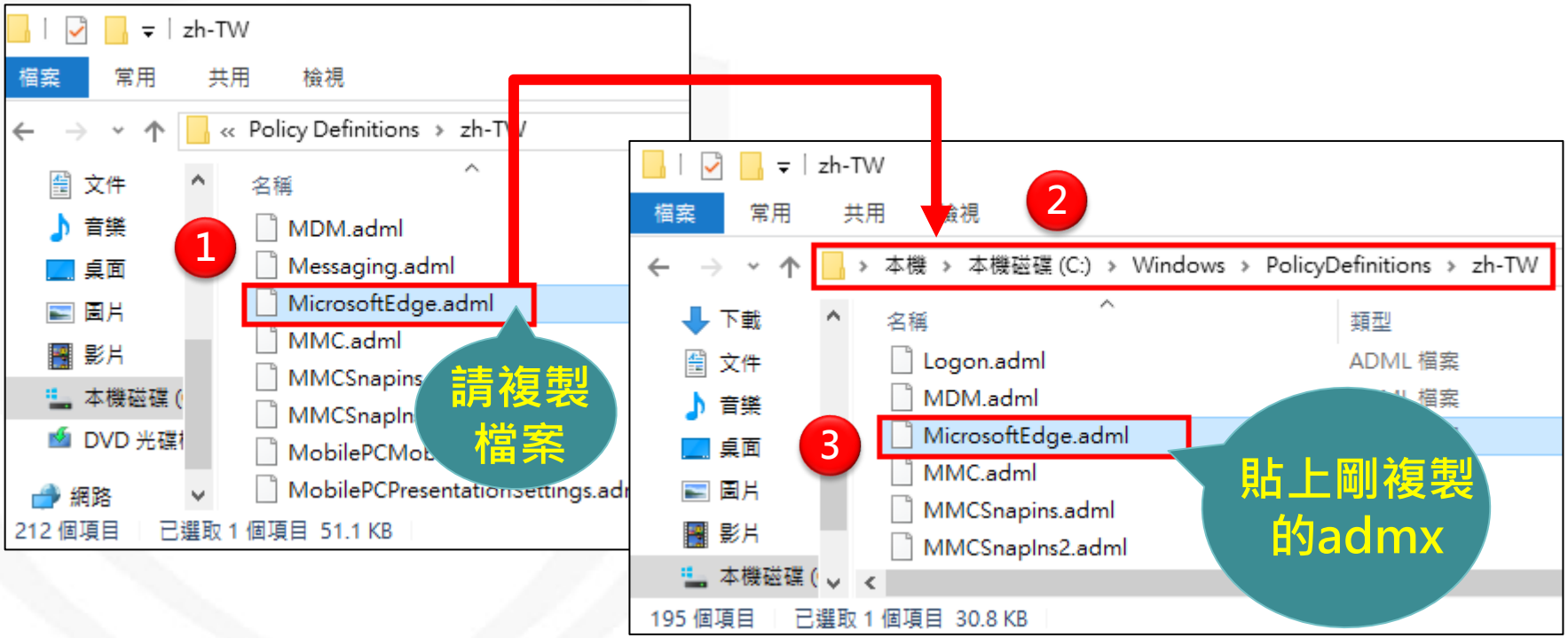
請點選此處會自動下載

安裝Microsoft Edge系統管理範本(2/3)

- Microsoft Edge系統管理範本安裝方式
  - 將下載的檔案解壓縮，並複製MicrosoftEdge.admx檔案至「C:\Windows\PolicyDefinitions」

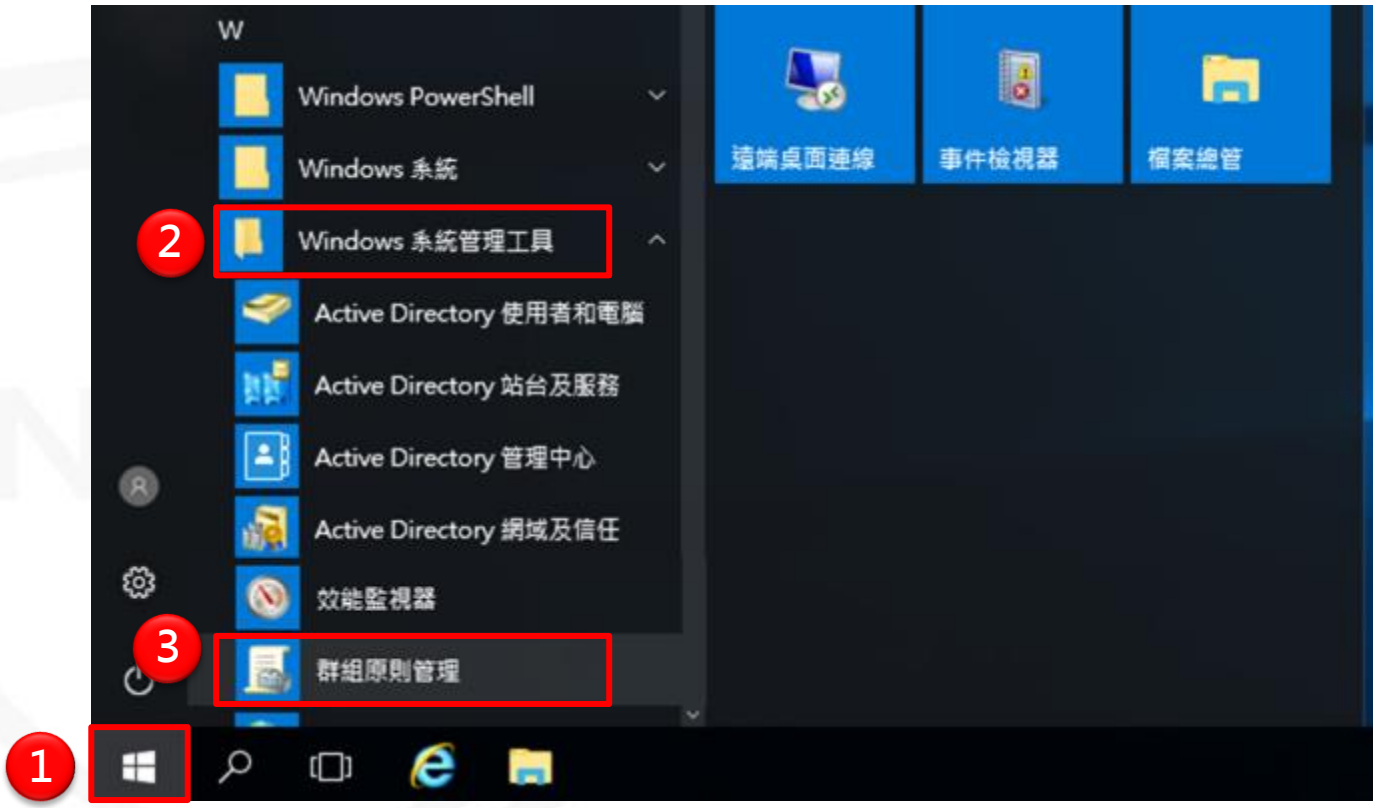
安裝Microsoft Edge系統管理範本(3/3)

- Microsoft Edge系統管理範本安裝方式
  - 將下載的檔案解壓縮，並複製MicrosoftEdge.adml檔案至「C:\Windows\PolicyDefinitions\zh-TW」



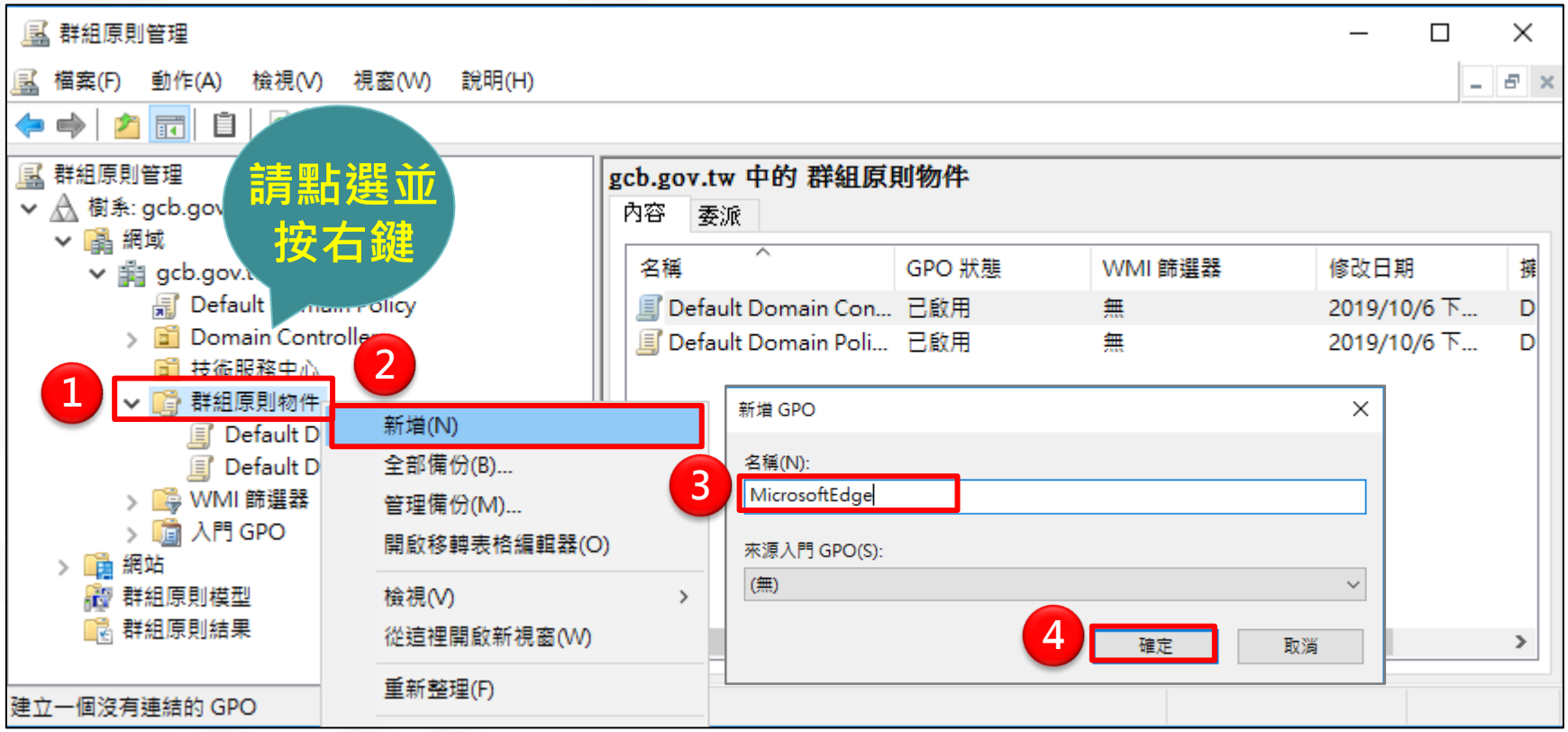
AD環境下的導入方式(1/6)

- 點擊開始→Windows系統管理工具→群組原則管理



AD環境下的導入方式(2/6)

- 在「群組原則物件」節點按滑鼠右鍵→選擇「新增」
- 在「名稱」欄位→輸入群組原則物件的名稱「MicrosoftEdge」→點選「確認」



AD環境下的導入方式(3/6)

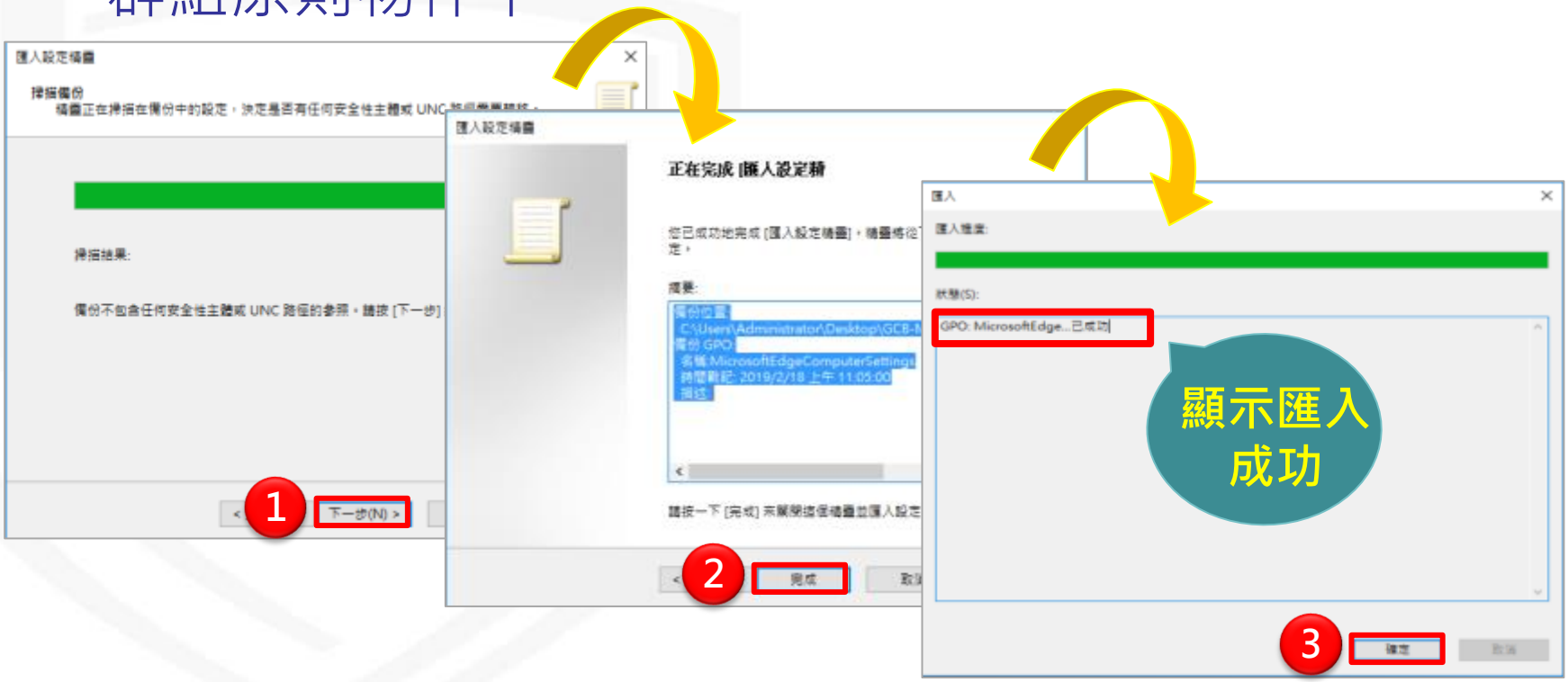
- 點選新建的群組原則物件「MicrosoftEdge」按滑鼠右鍵→選擇「匯入設定值」
- 在歡迎使用【匯入設定精靈】頁面→點選「下一步」

AD環境下的導入方式(4/6)

- 在備份GPO頁面→點選「下一步」
- 在備份位置頁面，點選「瀏覽」→選擇欲匯入的GPO資料夾，點選「確認」→點選「下一步」
- 在來源GPO頁面→選取欲匯入的GPO→點選「下一步」

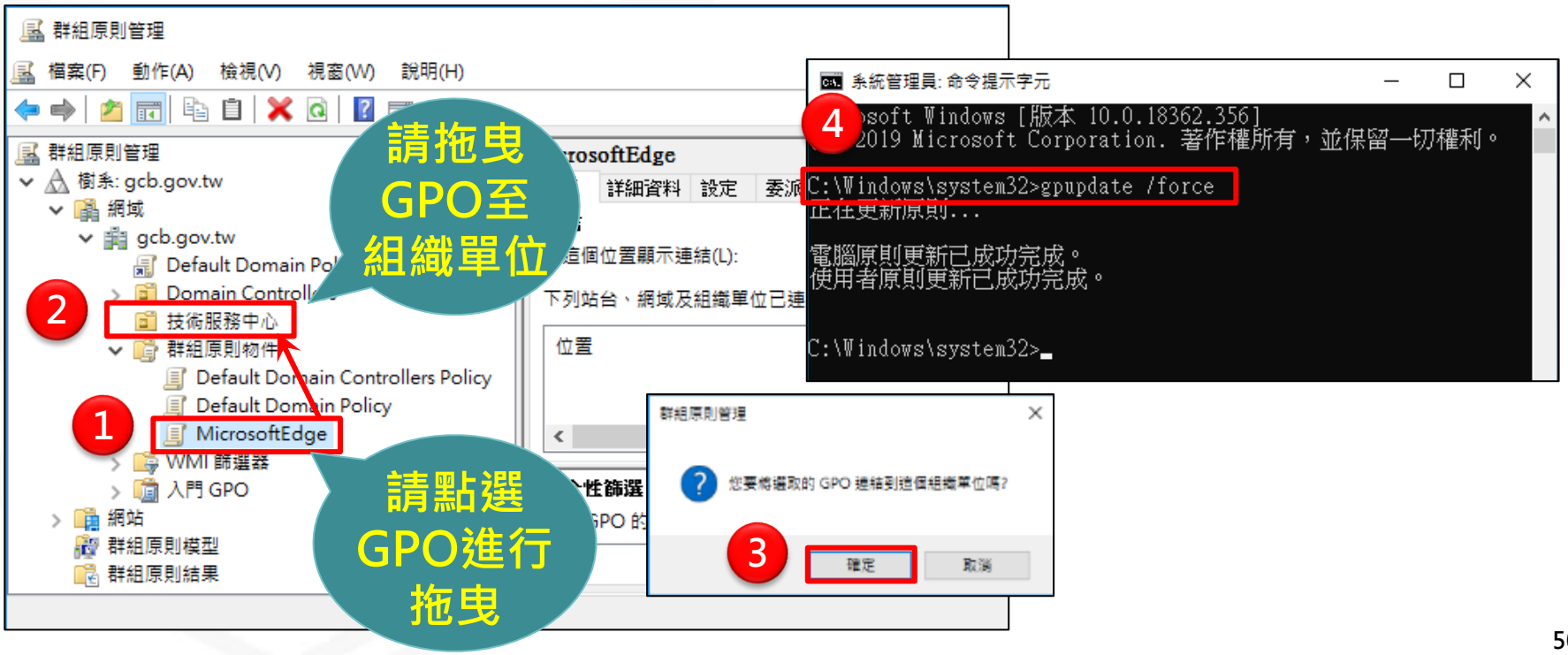
AD環境下的導入方式(5/6)

- 在掃描備份頁面→點選「下一步」
- 在正在完成匯入設定頁面→點選「完成」
- 在匯入進度的頁面→點選「確定」，完成匯入GPO至群組原則物件中



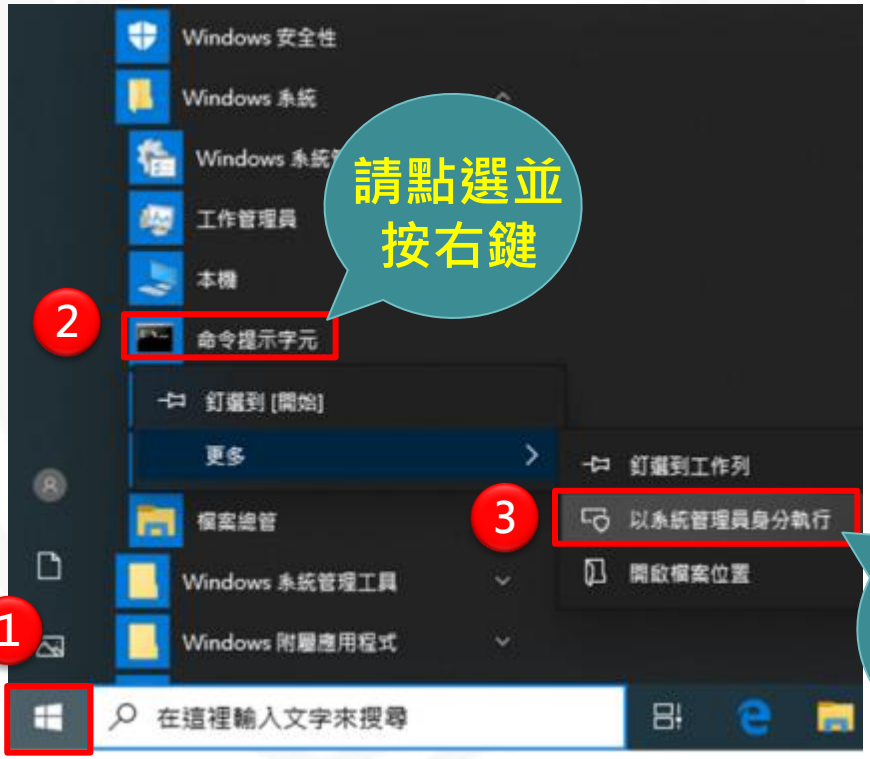
AD環境下的導入方式(6/6)

- 將新建的群組原則物件「MicrosoftEdge」拖曳至組織單位(OU) →點選「確定」按鈕，完成部署作業
- 使用者電腦重新開機或使用gpupdate /force指令更新組態，即可更新套用的GCB設定



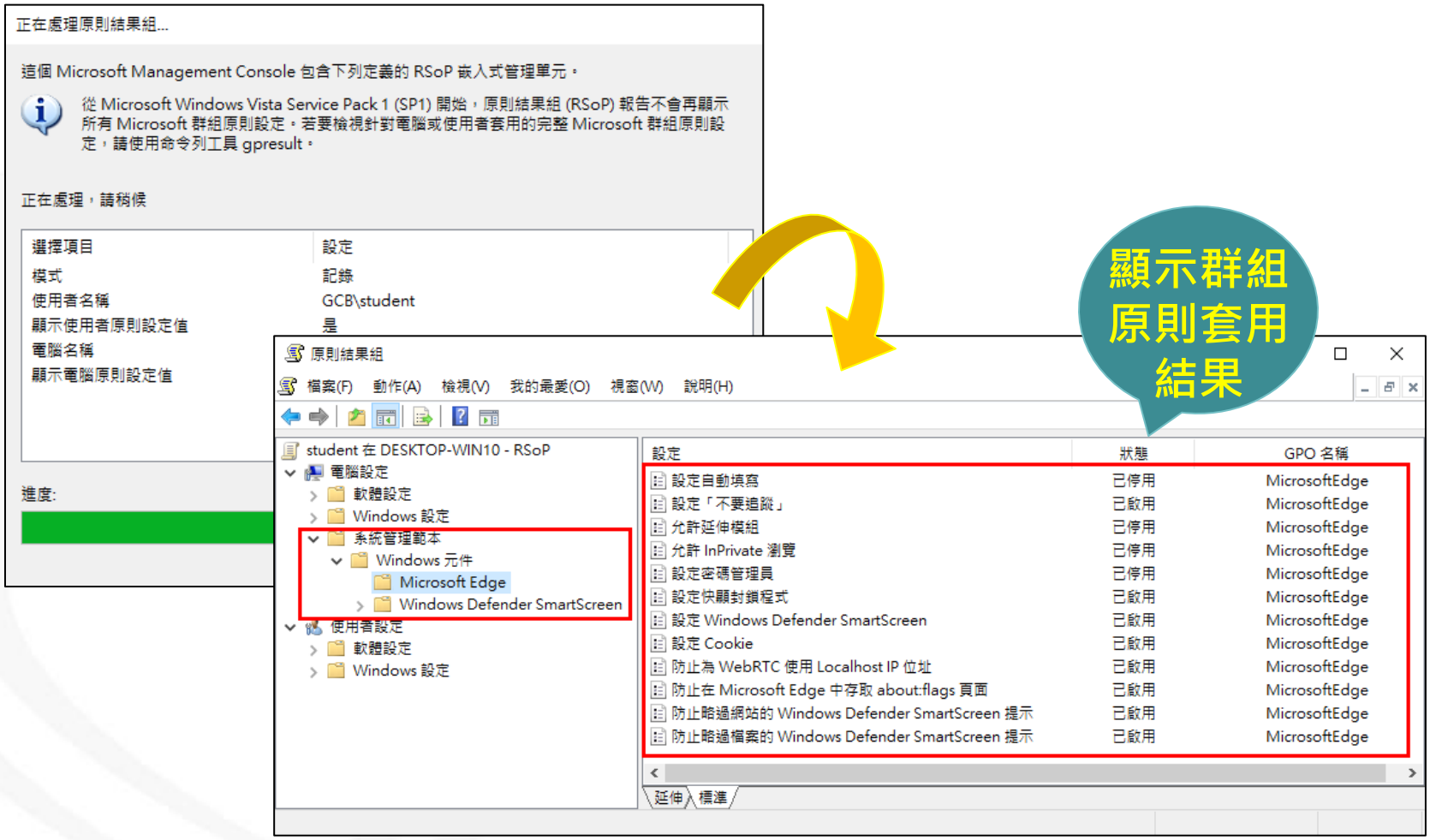
AD環境下的檢查方式(1/4)

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



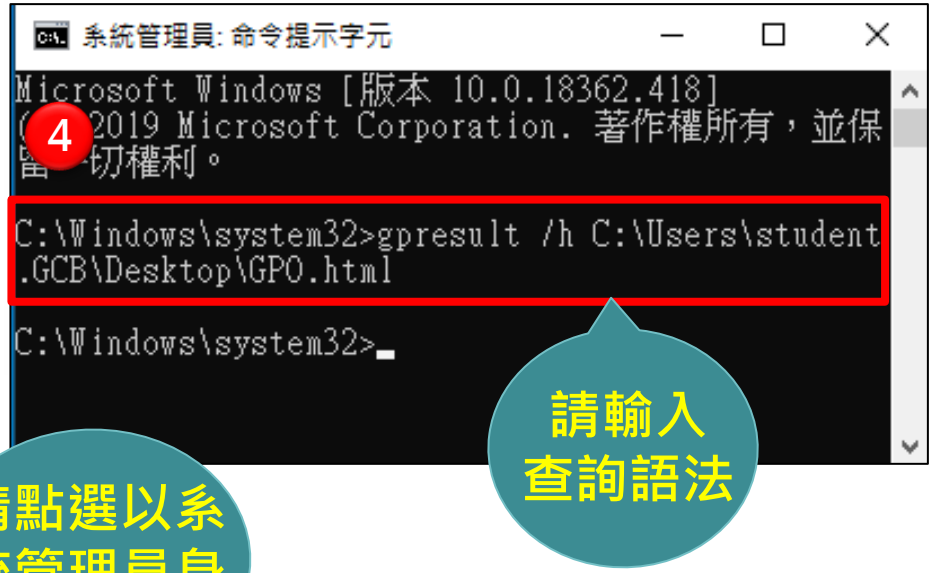
AD環境下的檢查方式(2/4)

- 使用RSOP檢查群組原則，顯示如下



AD環境下的檢查方式(3/4)

- 使用gpresult檢查群組原則
  - 點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→點選「以系統管理員身分執行」
  - 於「命令提示字元」輸入gpresult /h <檔案儲存路徑>\檔名.html

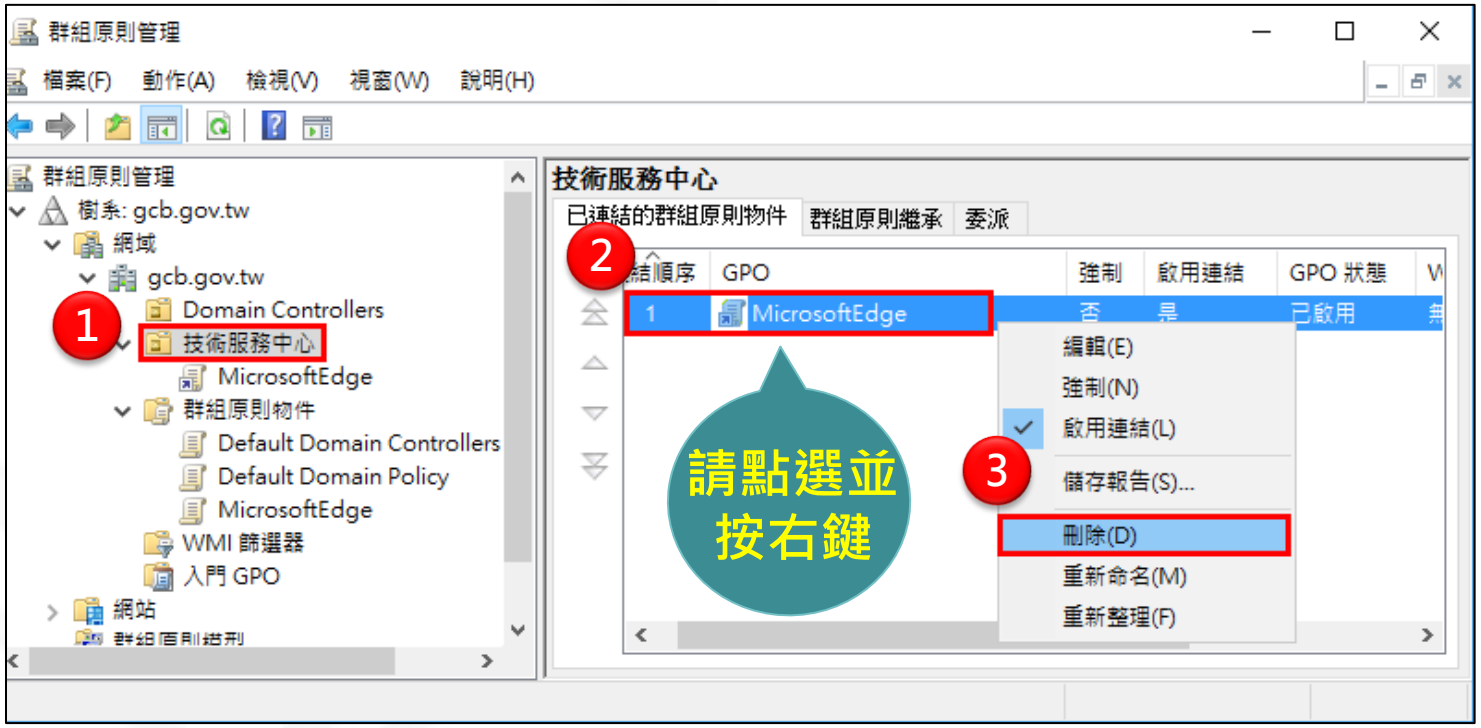


AD環境下的檢查方式(4/4)

- 使用gpresult檢查群組原則，顯示如下

AD環境下恢復原始設定方式

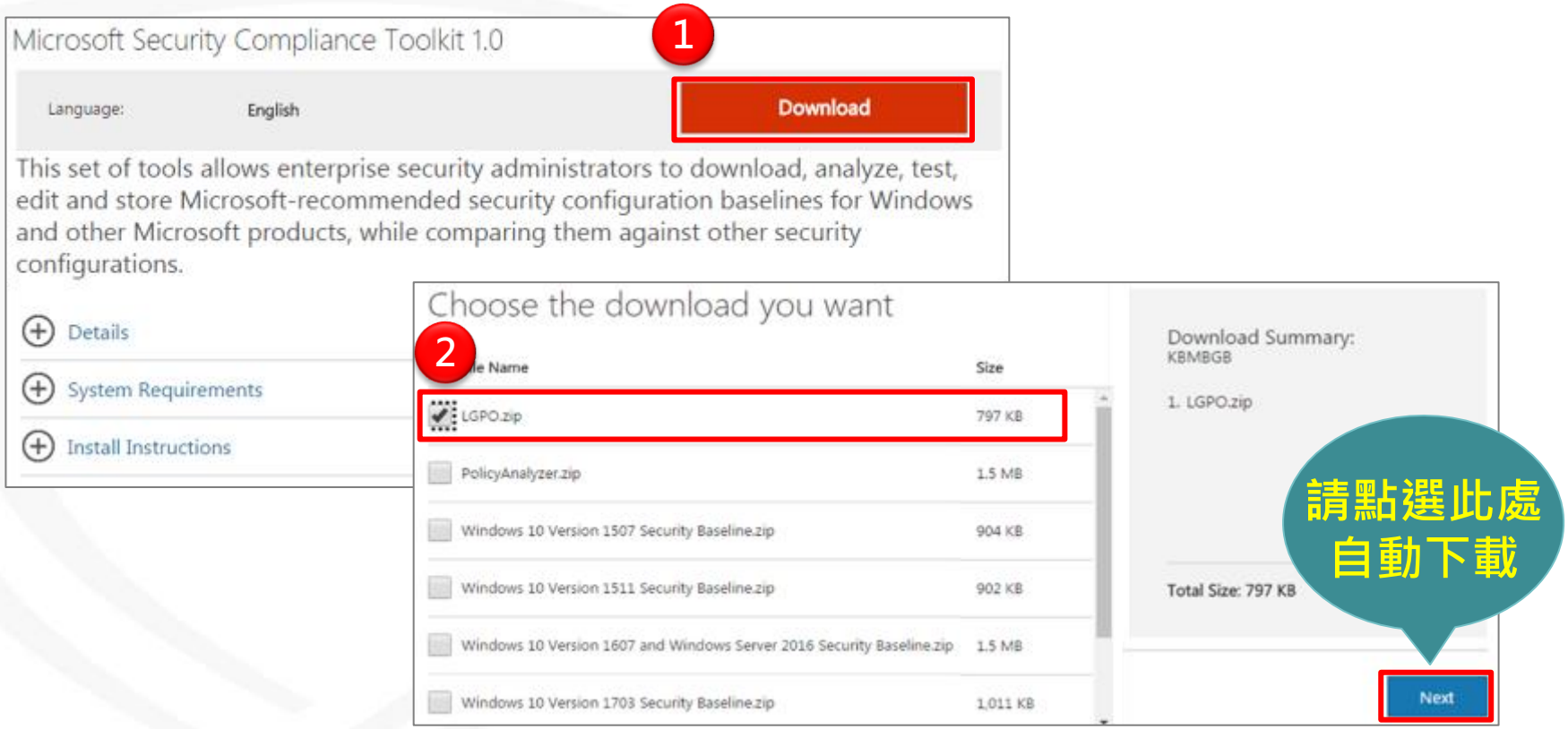
- 在欲取消連結的GPO上按滑鼠右鍵→點選「刪除」，即可將群組原則物件自組織單位(OU)中移除
- 使用者重新開機或使用gpupdate /force指令更新組態，即可恢復原始設定



單機環境部署說明

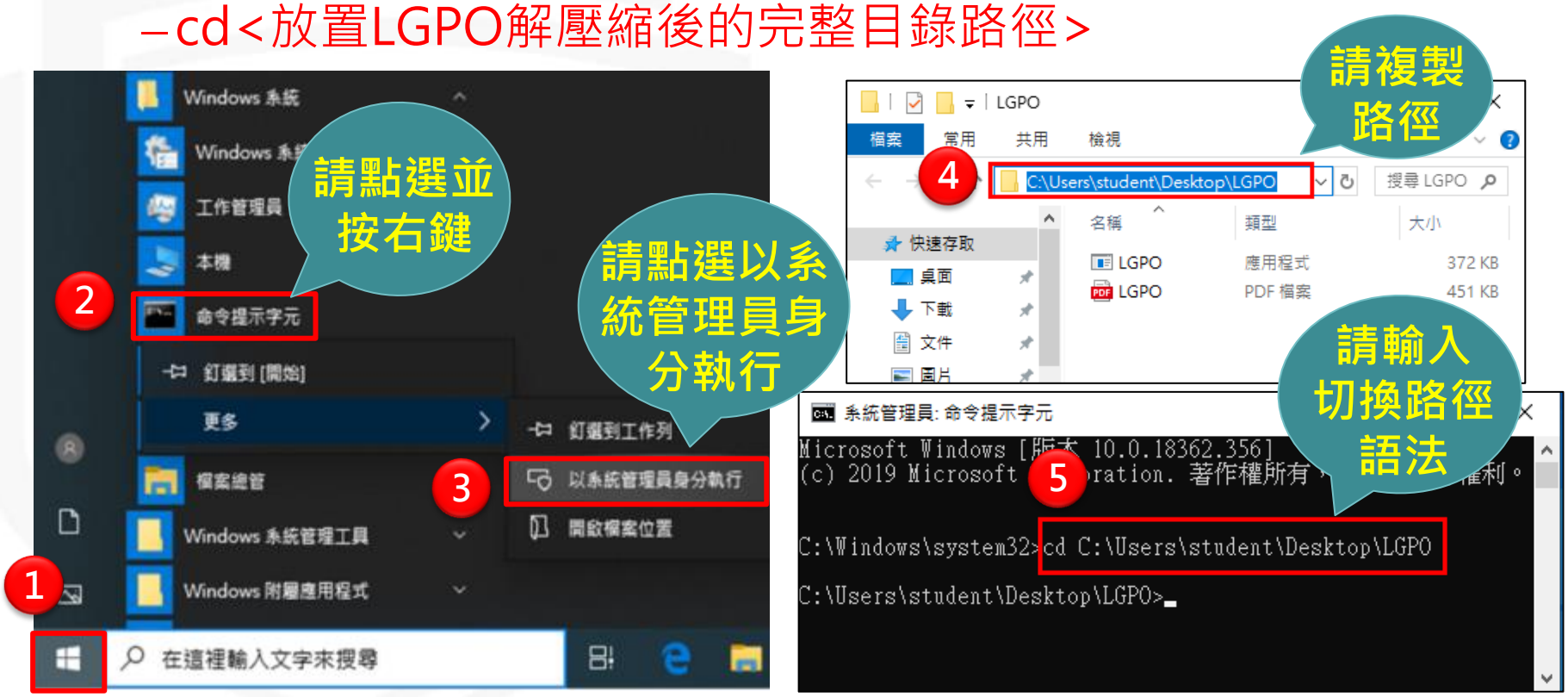
單機環境下的導入方式(1/4)

- 下載並解壓縮LGPO程式至電腦當中
- 下載網址：https://www.microsoft.com/en-us/download/details.aspx?id=55319



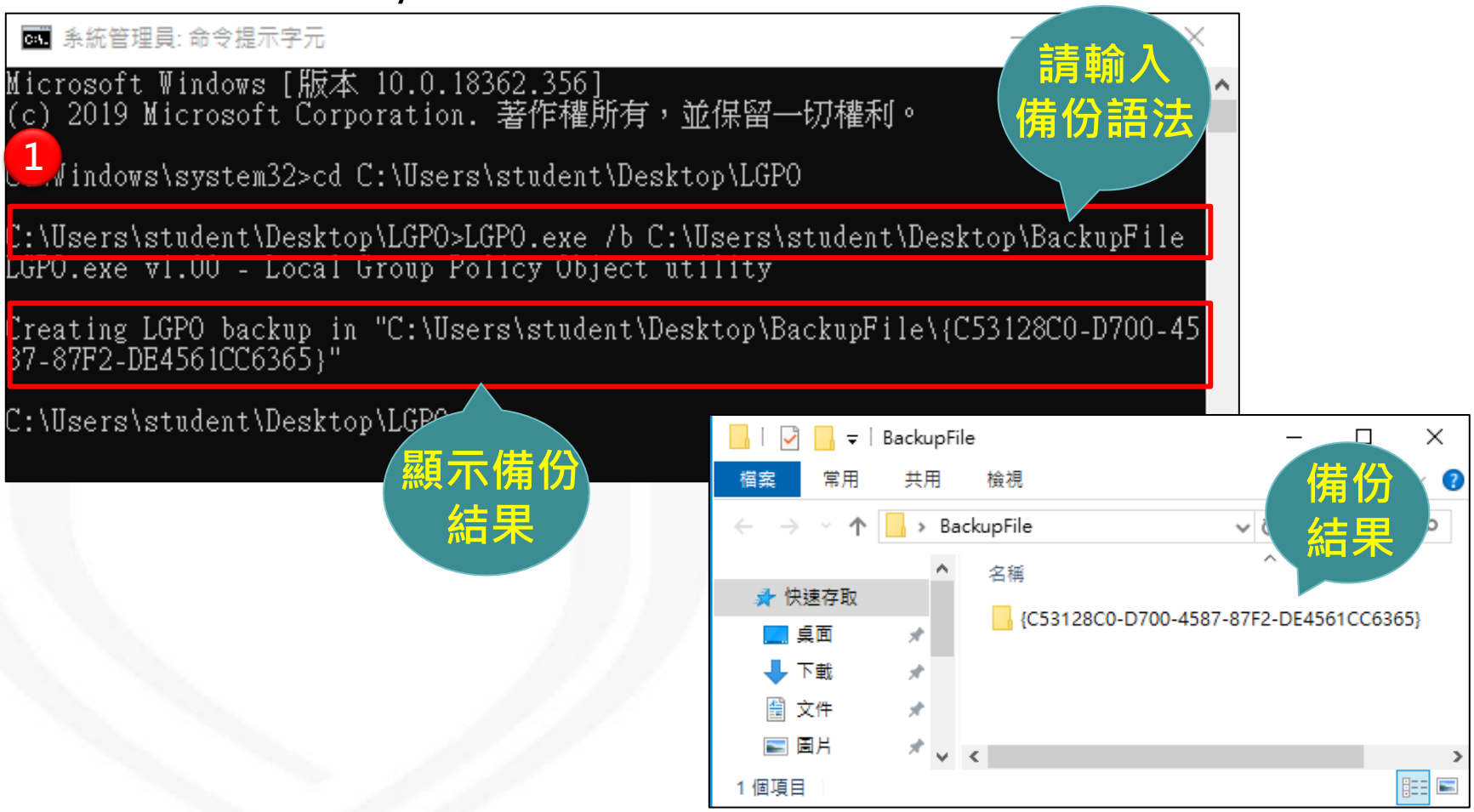
單機環境下的導入方式(2/4)

- 點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→選擇「以系統管理員身分執行」
- 於「命令提示字元」輸入語法切換至LGPO目錄
  - –cd<放置LGPO解壓縮後的完整目錄路徑>



單機環境下的導入方式(3/4)

- 於「命令提示字元」輸入語法，備份電腦組態設定
  - LGPO.exe /b <絕對路徑>

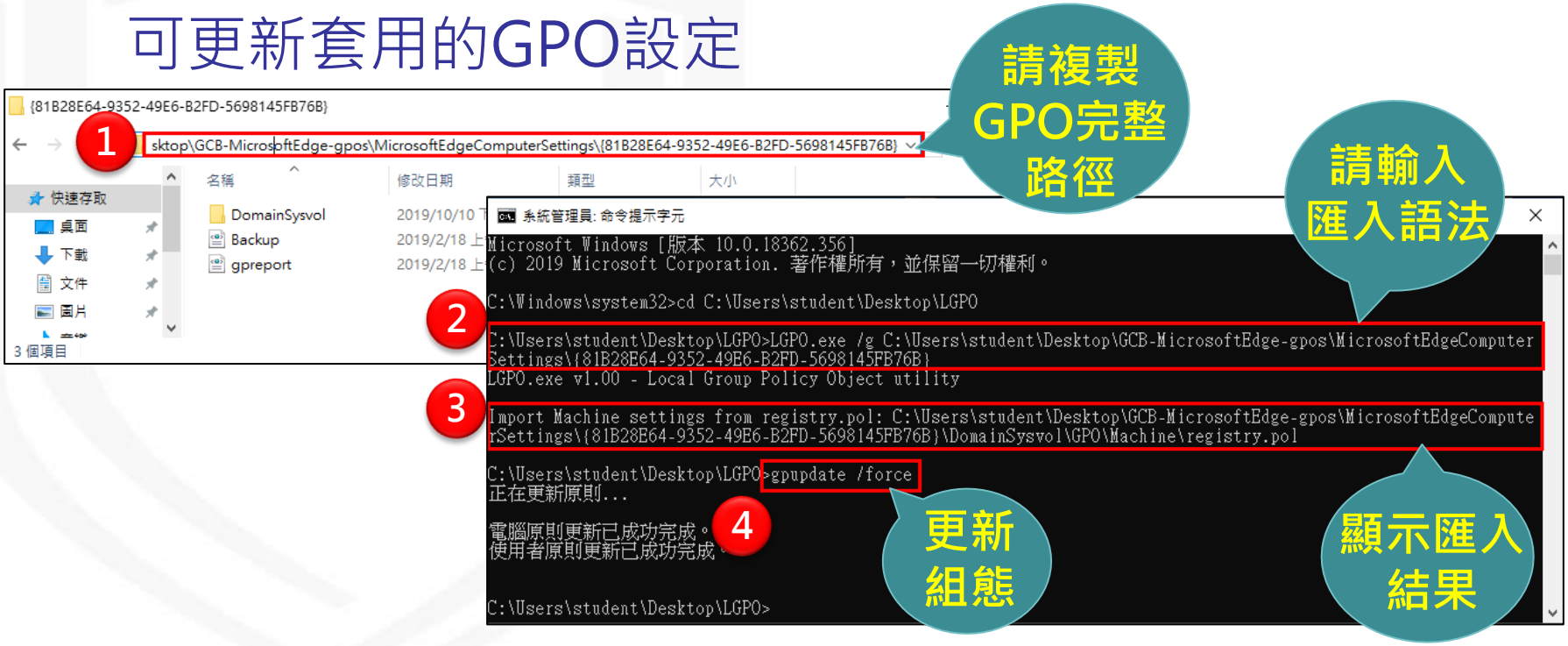


單機環境下的導入方式(4/4)

- 於「命令提示字元」輸入語法，匯入Microsoft Edge GPO組態設定

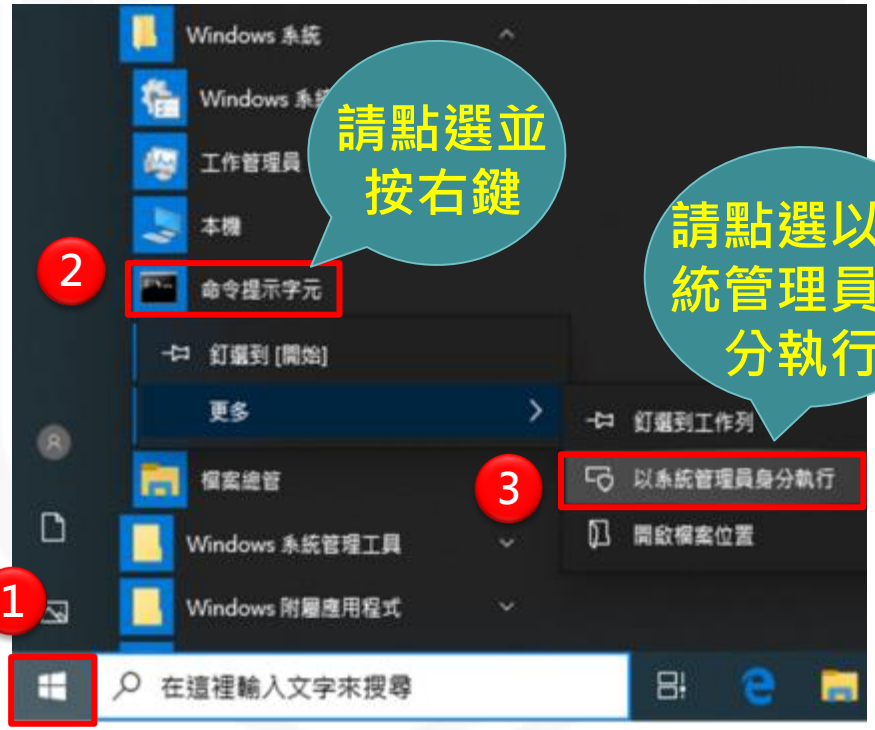
  –LGPO.exe /g <絕對路徑>

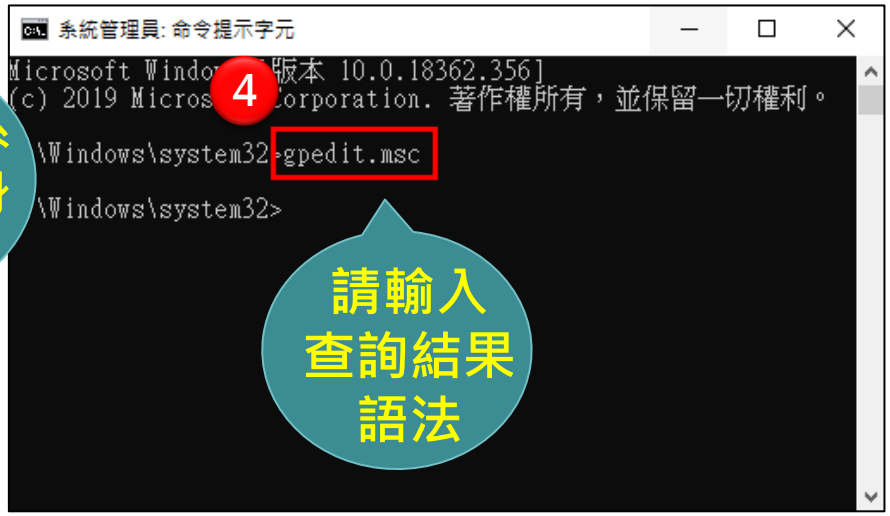
- 重新開機或使用gpupdate /force指令更新組態，即可更新套用的GPO設定



單機環境下的檢查方式(1/2)

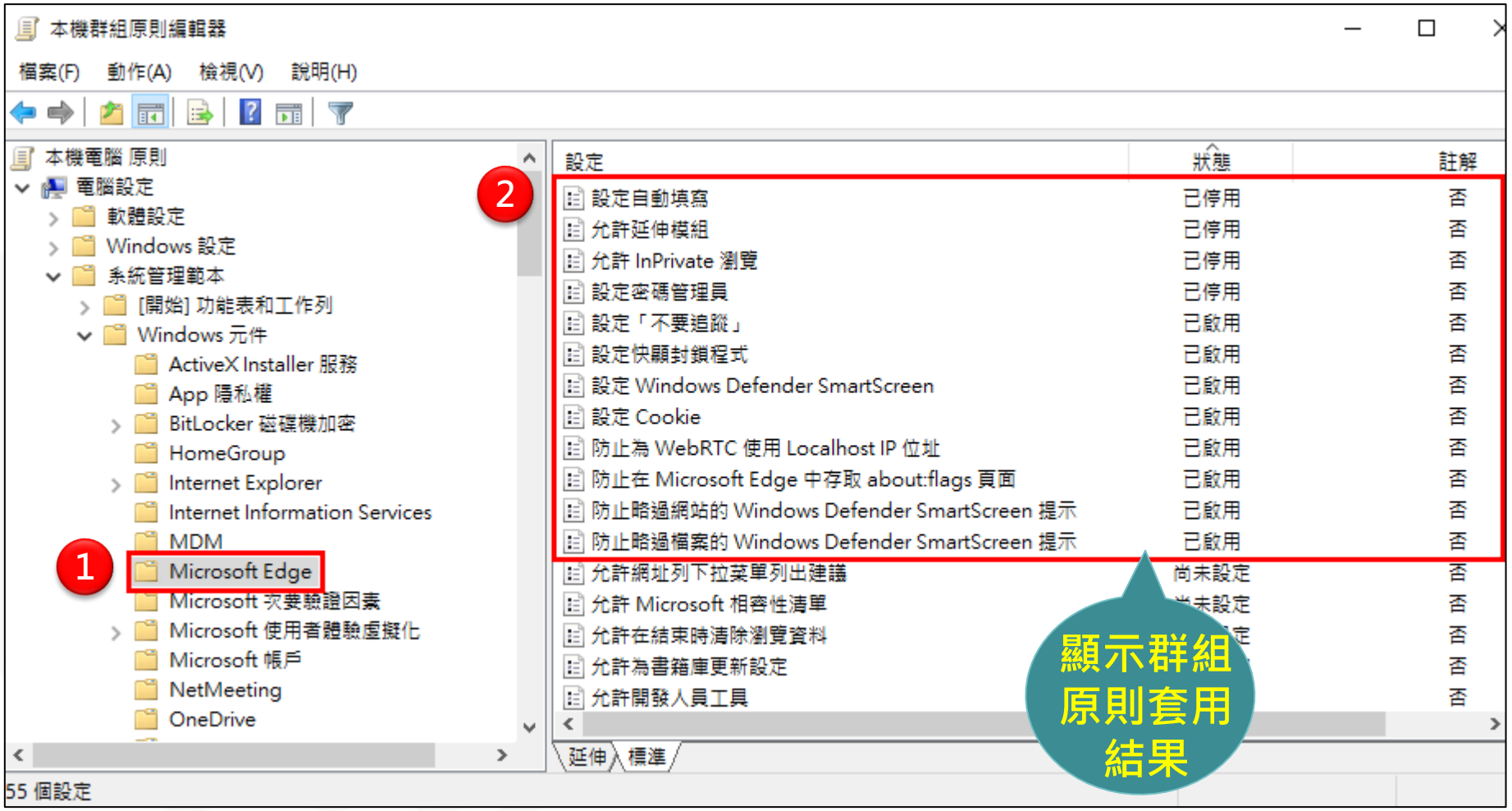
- 使用gpedit.msc檢查群組原則
  - 點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→選擇「以系統管理員身分執行」
  - 於「命令提示字元」輸入gpedit.msc





單機環境下的檢查方式(2/2)

- 使用gpedit.msc檢查群組原則，顯示如下



單機環境下恢復原始設定方式(1/2)

- 使用LGPO恢復原始設定
  - 點擊開始→Windows系統→在「命令提示字元」按滑鼠右鍵→選擇「以系統管理員身分執行」
  - 執行RD /S /Q C:\Windows\System32\GroupPolicy進行刪除

單機環境下恢復原始設定方式(2/2)

- 使用LGPO恢復原始設定
  - –於「命令提示字元」輸入語法切換至LGPO目錄
  - –執行LGPO.exe /g <絕對路徑>，匯入備份的GPO檔案
  - –重新開機或使用gpupdate /force指令更新組態

實作練習

實作練習-環境說明

環境說明

- 本次採用單機環境進行實作練習
- 單機部署環境說明
  - VM名稱：5.Microsoft Edge
  - 本機帳號：Student ；密碼：1qaz@WSX3edc
- VM環境皆已安裝實作練習所需之LGPO與LocalGPO軟體，並於桌面放置Microsoft Edge GPO檔與指令文字檔

實作練習1

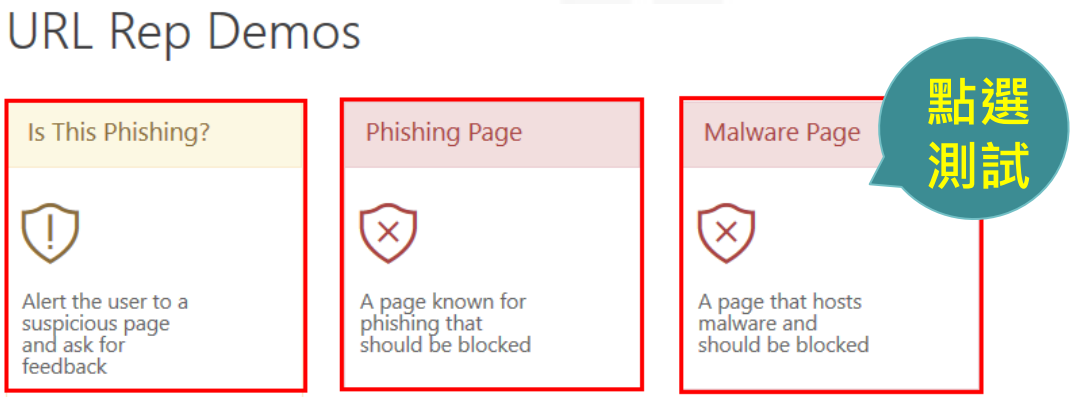
實作說明

- 請使用LGPO部署Microsoft Edge GPO
  - 步驟1：於「命令提示字元」按滑鼠右鍵，選擇「以系統管理員身分執行」
  - 步驟2：於「命令提示字元」輸入切換至LGPO目錄語法
  - 步驟3：於「命令提示字元」輸入備份電腦組態設定語法LGPO.exe /b <絕對路徑>
  - 步驟4：於「命令提示字元」輸入匯入GPO組態設定語法LGPO.exe /g <絕對路徑>
  - 步驟5：於「命令提示字元」輸入更新組態設定語法gpupdate /force

實作練習2(1/2)

實作說明

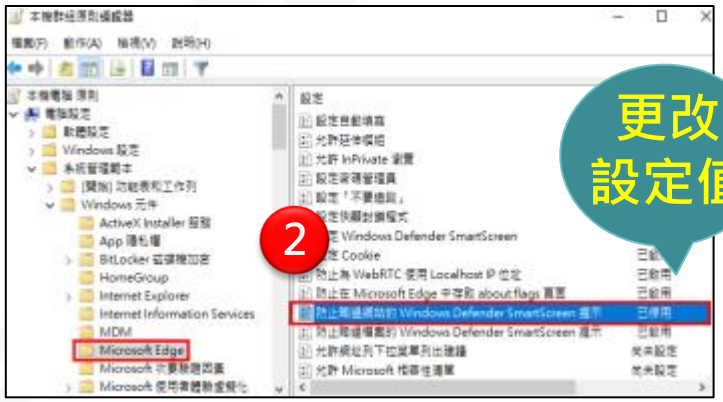
- 驗證「防止略過網站的Windows Defender SmartScreen提示」設定
  - 步驟1：請使用Edge開啟測試網址 https://nav.smartscreen.msft.net/
  - 步驟2：點選網頁中的URL Rep Demos畫面測試
  - 步驟3：檢視套用GPO狀況下，是否可防止使用者略過警示繼續存取網站



實作練習2(2/2)

實作說明

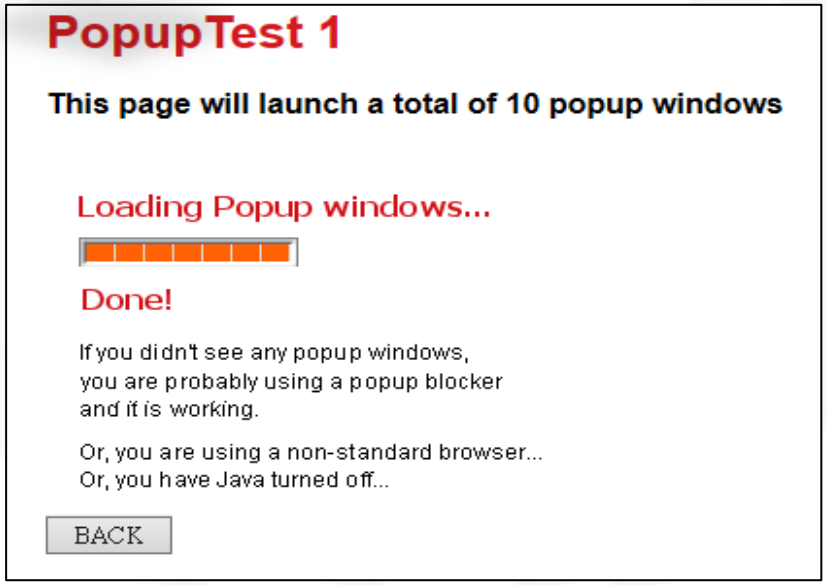
- 比對當「防止略過網站的Windows Defender SmartScreen提示」設定為「停用」之差異
  - 步驟1：於「命令提示字元」按滑鼠右鍵，選擇「以系統管理員身分執行」，輸入gpedit.msc
  - 步驟2：更改本項群組原則設定值為「停用」
  - 步驟3：關閉Edge瀏覽器，重新使用Edge開啟測試網址 https://nav.smartscreen.msft.net/
  - 步驟4：點選網頁中的URL Rep Demos畫面測試
  - 步驟5：檢視停用狀況下，是否可防止使用者略過警示繼續存取網站



實作練習3(1/2)

實作說明

- 驗證「設定快顯封鎖程式」設定
  - 步驟1：請使用Edge開啟測試網址 http://www.popuptest.com/popuptest1.html
  - 步驟2：檢視快顯示窗是否被阻擋



實作練習3(2/2)

實作說明

- 比對「設定快顯封鎖程式」設定「停用」之差異
  - 步驟1：於「命令提示字元」輸入gpedit.msc
  - 步驟2：更改本項群組原則設定值為「停用」
  - 步驟3：關閉Edge瀏覽器，重新使用Edge開啟測試網址 http://www.popuptest.com/popuptest1.html
  - 步驟4：檢視停用狀況下，是否可封鎖快顯程式

實作練習4

實作說明

- 驗證「設定密碼管理員」設定
  - 步驟1：請開啟Edge→點選「設定」 →點選「密碼與自動填滿 」，檢視儲存密碼功能是否關閉以及已儲存的資訊是否可以異動
  - 步驟2：點擊開始→搜尋「認證管理員」，檢視是否可以看到帳號密碼

實作練習5(1/2)

實作說明

- 驗證「設定自動填寫」設定
  - 步驟1：請使用Edge開啟測試網址 https://anttiviljami.github.io/browser-autofill-phishing/
  - 步驟2：點選Name的輸入欄位2下，點選自動填寫功能帶出之資訊，按下「Submit」
  - 步驟3：將網頁的address資訊進行編碼轉換，轉換網址https://www.ifreesite.com/unicode-ascii-ansi.htm

實作練習5(2/2)

實作說明

- 驗證「設定自動填寫」設定
  - 步驟4：檢視轉換後之資訊是否與Edge瀏覽器的「密碼與自動填滿 」儲存資訊一致

參考資料

- 市面近1/4的VPN服務有漏洞，隱匿不成反而洩漏用戶IP
- 2019資安預測趨勢提七大重點：資料外洩通報與網路釣魚將大增
- 鎖定Edge漏洞的攻擊程式曝光
- 查身分證功能防詐騙 網頁中獎廣告別上當
- Several Cryptojacking Apps Found on Microsoft Store
- 小心! 瀏覽器自動填入功能可能讓你儲存的個資被偷光光
- 你不曉得的「按讚」情報威力
- 資安業者在Microsoft Store發現8款程式暗藏挖礦功能
- Windows Defender SmartScreen 常見問題集
- 維基百科Wikipedia

報告完畢
敬請指教