因應微軟公司 Windows 7 作業系統終止支援服務之資安防護措施建議

1. 前言

微軟公司 2009 年推出 Windows 7(以下簡稱 Win7)，雖然歷經 Windows 8(以下簡稱 Win8)、Windows 8.1(以下簡稱 Win8.1)到現在的 Windows 10(以下簡稱 Win10)，至今已經過 10 年，仍有近 30%市占率[1]。自 2017/10/31 起停售 Win7 後，隨著時間的演進，已進入產品生命週期末端，將於 2020/1/14 終止支援(End of Support，以下簡稱 EOS)，不再針對 Win7 提供下述支援服務[2][3]：

●安全性更新

●非安全性修補程式及功能更新

●產品技術支援及線上技術內容更新

為加強 Win7 停止支援服務後之資安防護，謹提供「Win7 EOS 對資安影響」與「資安防護措施建議」等資訊供參。

2. Win7 EOS 對資安影響

微軟公司 Win7 作業系統於 2020/1/14 終止服務，將不再針對 Win7 提供程式修正、軟體更新及線上技術支援服務，對於 Win7 EOS 可能產生的影響分析如下：

●Win7 作業系統相關應用軟體弱點已無法確保可取得更新的修補程式

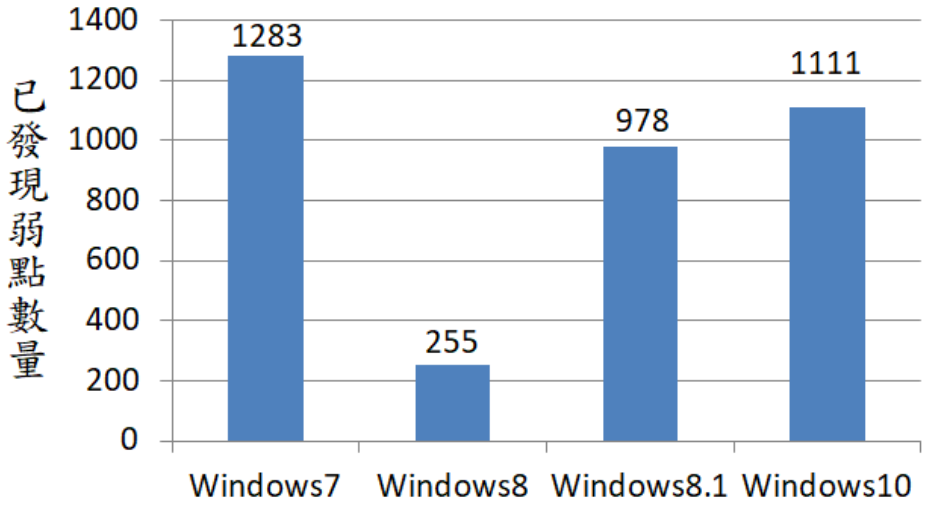
– Win7 作業系統上所安裝之 Internet Explorer 11 瀏覽器(以下簡稱 IE11)，因其修補程式係透過 Win7 作業系統之更新機制進行更新，但 Win7 作業系統之更新機制於 2020/1/14 終止運作，因此 Win7 作業系統上所安裝之 IE11 於 2020/1/14 後也將無法取得更新的修補程式。

– 微軟應用程式開發與執行環境(Runtime)的支援平台也會調整(如.NET

Framework 與 Visual C++可轉散發套件等)，相對應在 Win7 上的安全性更新也不再支援。

●Win7 作業系統已發現弱點數量多

根據 CVE Details 弱點資料庫統計數據顯示，Win7 作業系統已被發現弱點數量達 1,283 個(詳見圖 1)[4]，高於 Win8.1 與 Win10，繼續使用 Win7 將遭惡意人士利用弱點進行攻擊之風險相對較高。



資料來源：CVE Details 弱點資料庫[4]

圖1　各作業系統已發現弱點數量統計

●微軟公司建議 Win7 終止支援後轉移至 Win10

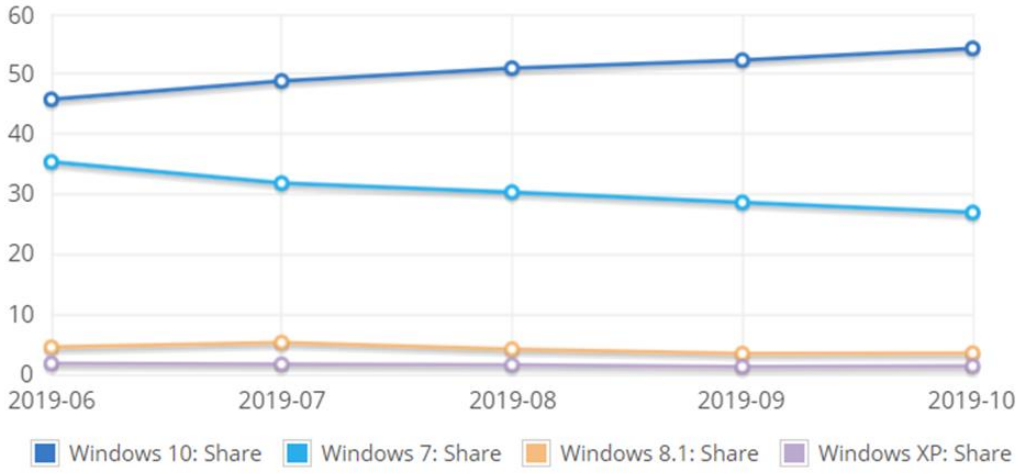
Win7 EOS 後在缺乏新的修補程式與安全性更新下，將面臨應用程式無法開發維護、系統效能、重大資安風險等挑戰，微軟公司基於下列原因建議升級至 Win10：

– 提供高度安全的內建保護，協助抵禦現代安全威脅。

– 可與現有基礎架構整合，繼續使用現有應用程式。

根據 NetApplications 作業系統市占率統計數據顯示[5]，Win7 市占率已降

低至 30%以下，Win10 市占率則提高至 50%以上，代表市場上已逐步轉移至 Win10(詳見圖 2)。



資料來源：資料來源：NetApplications[5]

圖2　桌上型電腦作業系統市占率統計

3. 資安防護措施建議

針對 Win7 EOS 可能產生之資安影響，提供下列資安防護措施建議供政府機關參考。在經費許可的情況下，建議採用「3.1 加速 Win7 升級至 Windows 新版作業系統」，盡速升級以確保資通安全。

若尚無經費可全面升級，建議參考「3.2 強化使用 Win7 電腦資安防護」，根據「部署 Win7 GCB」、「帳戶權限設定」、「軟體防護」及「監控防禦」等安全性設定，加強 Win7 之安全管理，並參考「3.3 透過網路區隔加強管理使用 Win7 電腦」規劃與部署資安防護強化措施，針對風險較高之使用 Win7 電腦虛擬區域網路(VLAN)，加強網路流量監控。

技服中心也將持續進行 Win7 弱點監測與通報作業，並透過「3.4 執行 Win7 弱點持續監測計畫」，掌握政府機關 Win7 相關資安事件與影響。

3.1.加速 Win7 升級至新版作業系統

將 Win7 升級至 Windows 新版作業系統為根本解決之道，微軟公司自 2017/10/31 起停售 Win7 作業系統，而 Win10 已於 2015/7/29 上市，請加速 Win7 升級作業。

若發現資安事件入侵原因來自 Win7 弱點，則可能該機關已遭鎖定，屬「Win7 高風險機關」，應先進行作業系統升級。

3.2.強化 Win7 電腦資安防護

若於微軟公司終止支援後仍需使用 Win7，應規劃與部署資安防護強化措施，透過「部署 Win7 GCB」、「帳戶權限設定」、「軟體防護」及「監控防禦」等 4 方面，說明如下。

3.2.1. 部署 Win7 GCB

部署 Win7 GCB，藉由規範電腦之組態安全設定(如密碼長度、更新期限等)，強化資安防護。

●使用 LocalGPO 工具部署 Win7 GCB

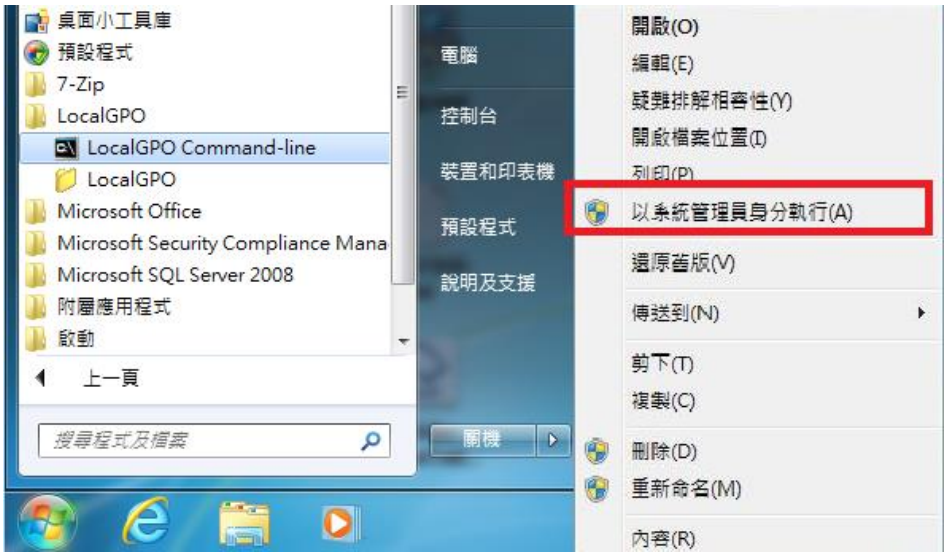
LocalGPO 是由微軟所開發的工具，其功能可在 Windows 平台個人電腦與伺服器主機中匯入、匯出或重置本機的群組原則設定。如需要下載 LocalGPO，可經由技服中心網站的「政府組態基準(GCB)」專區[6]取得 LocalGPO 安裝程式。

– 啟動 LocalGPO

(1) 以「系統管理員」身分登入，或以具有系統管理員權限的使用者身分登入。

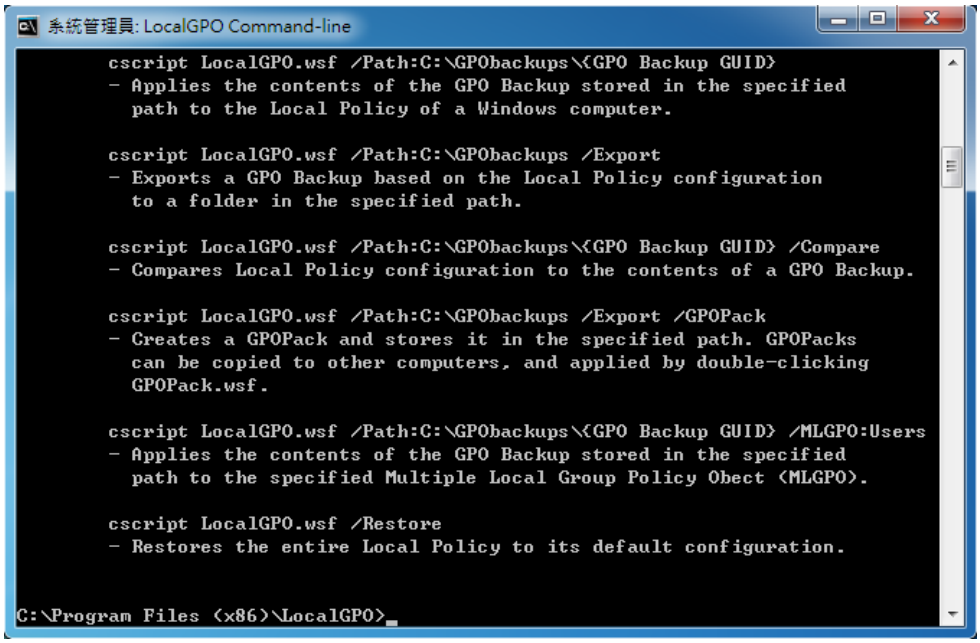
(2) 按一下「開始」→「所有程式」→「LocalGPO」，點選「LocalGPO Command-line」，並以右鍵選擇「以系統管理員身分

執行」，開啟「LocalGPO Command-line」。



資料來源：本中心整理

圖3　以系統管理員身分執行 LocalGPO

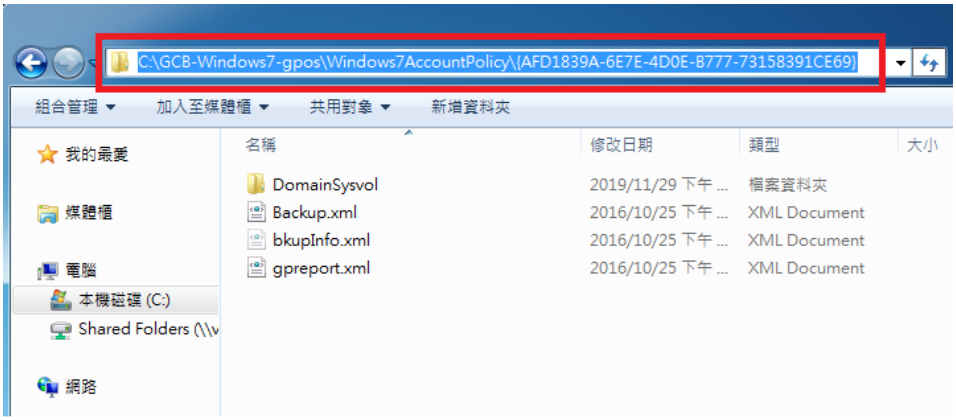


資料來源：本中心整理

圖4　LocalGPO Command-line

– 部署 Win7 GCB

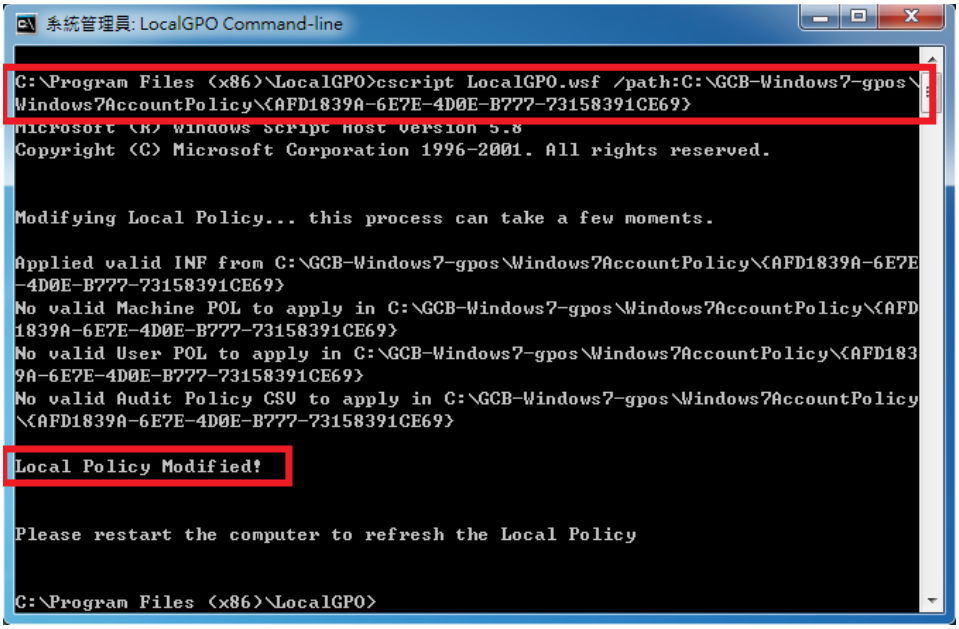
(1) 開啟 Win7 GCB GPO 資料夾，複製 GPO 所在的完整目錄路徑。



資料來源：本中心整理

圖5　複製 GPO 所在的完整目錄路徑

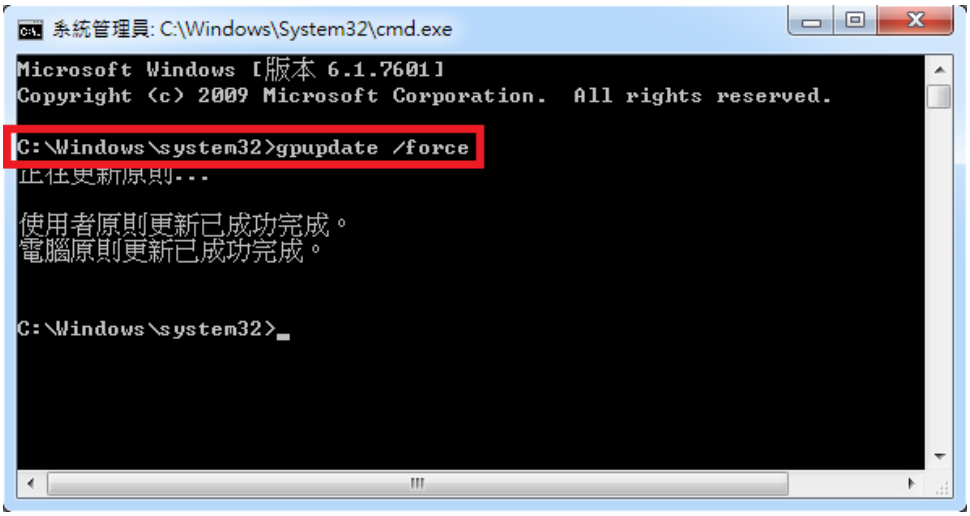
(2) 於「LocalGPO Command-line」輸入語法「cscript LocalGPO.wsf /path:<放置 GPO 的完整目錄路徑>」，匯入 GPO 設定值。



資料來源：本中心整理

圖6　匯入 GPO 設定值

(3) 重複步驟 2，將所需 GPO 逐一匯入後，重新開機或使用「gpupdate /force」指令更新組態。



資料來源：本中心整理

圖7 使用 gpupdate /force 指令更新組態

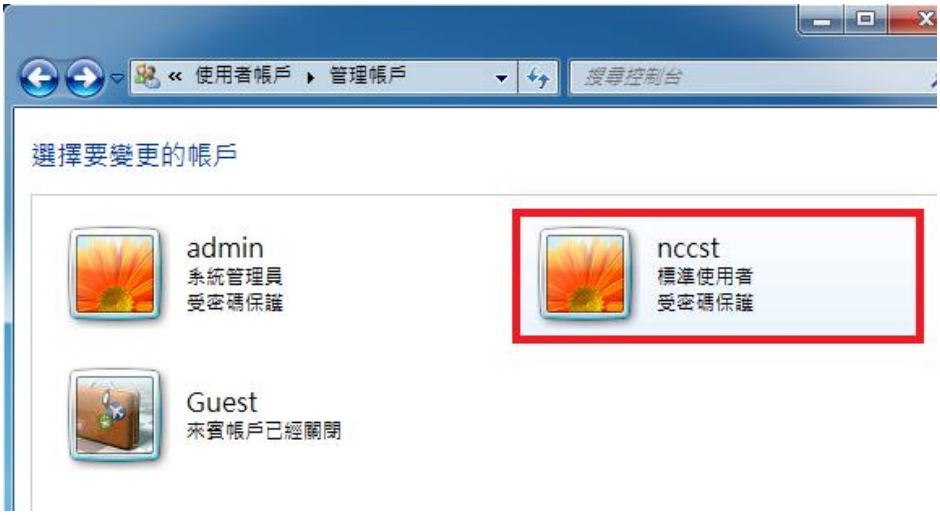
3.2.2. 帳戶權限設定

●賦予使用者帳戶符合業務需求之最小權限，儘量避免使用 Administrator 權限登入系統，以降低攻擊者取得電腦完整主控權之風險。將使用者帳戶權限設定為「標準使用者」方式如下：

(1) 以「系統管理員」身分登入，或以具有系統管理員權限的使用者身分登入。

(2) 按一下「開始」→「控制台」→「使用者帳戶和家庭安全」→「使用者帳戶」→「管理其他帳戶」。

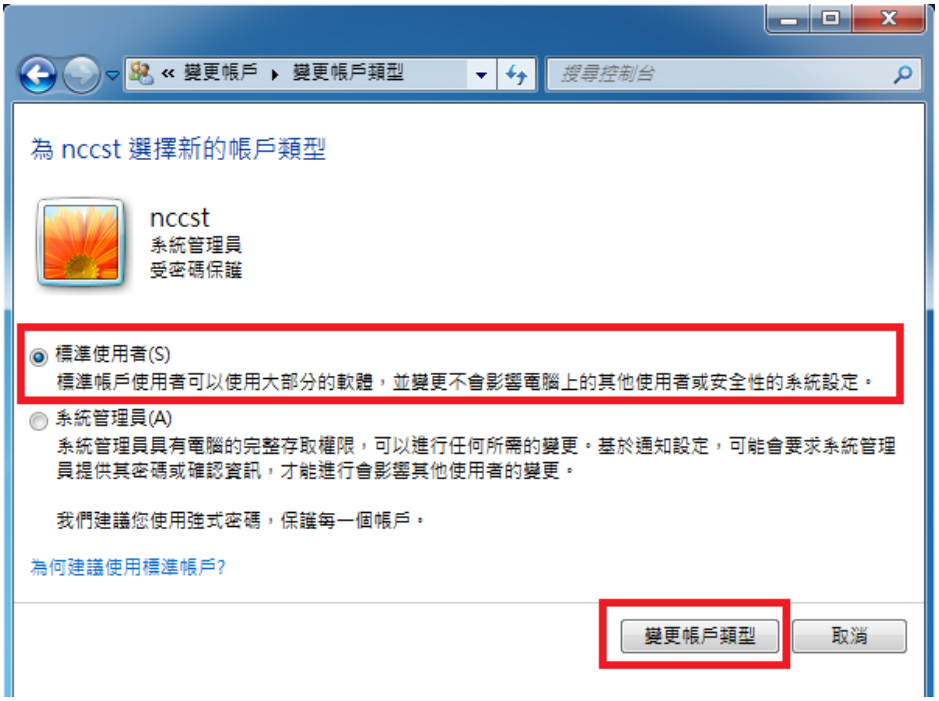
(3) 按一下要變更的使用者帳戶(如 nccst 等)。



資料來源：本中心整理

圖8　選擇要變更的帳戶

(4) 按一下「變更帳戶類型」，選取「標準使用者」，按一下「變更帳戶類型」，即可將帳戶權限設定為「標準使用者」帳戶類型。



資料來源：本中心整理

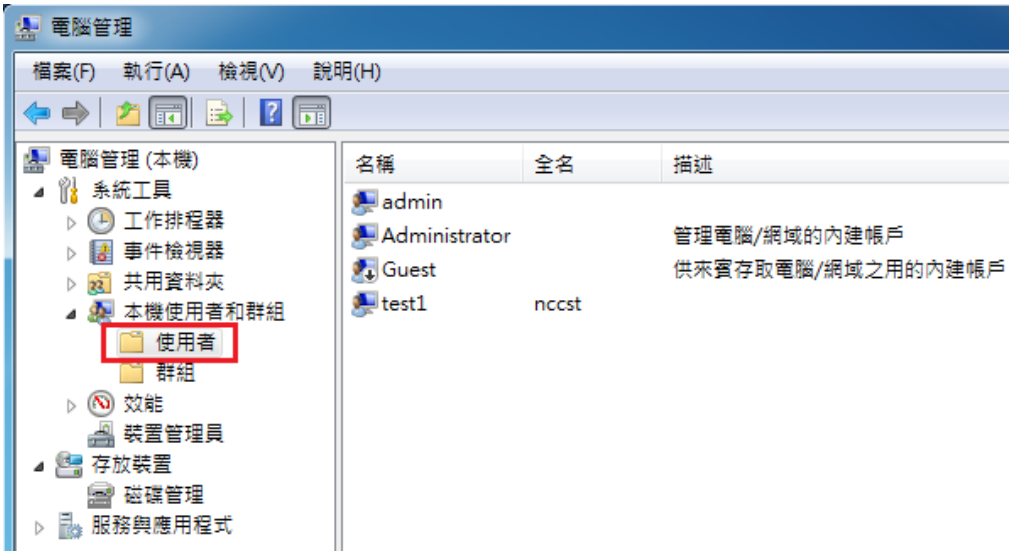
圖9　選取「標準使用者」帳戶類型

●若無使用需求，請停用本機「Administrator」帳戶，設定方式如下：

(1) 以「系統管理員」身分登入，或以具有系統管理員權限的使用者身分登入。

(2) 用滑鼠右鍵按一下「電腦」，然後按一下「管理」。

(3) 在左窗格中，展開「本機使用者和群組」節點，然後按一下「使用者」。

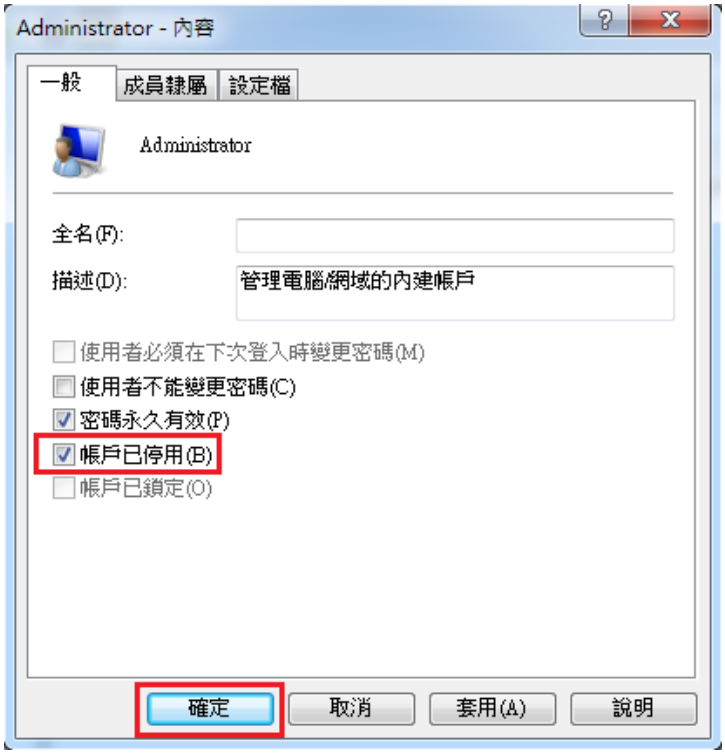


資料來源：本中心整理

圖10 使用者帳戶列表

(4) 在右窗格中，按兩下「Administrator」帳戶。

(5) 在「一般」索引標籤上，選取「帳戶已停用」核取方塊，然後按一下「確定」。



資料來源：本中心整理

圖11 選取「帳戶已停用」

(6) 重新開機後即無法使用本機「Administrator」帳戶登入系統。

資料來源：本中心整理

圖12 「Administrator」帳戶已停用登入訊息

3.2.3. 軟體防護

- 若無使用需求，請停止使用 IE 瀏覽器，改採其他如 Google Chrome 或 Mozilla Firefox 等仍會提供更新服務之替代瀏覽器，以提升瀏覽網頁之安全。

  (1) Google Chrome 瀏覽器下載網址：

  https://www.google.com.tw/intl/zh-TW/chrome/

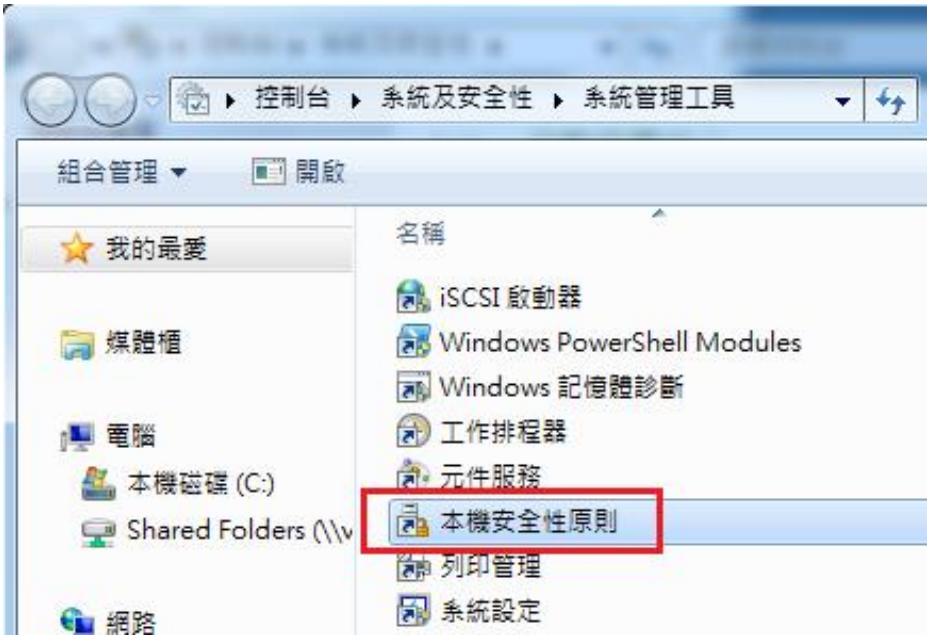
  (2) Mozilla Firefox 瀏覽器下載網址：

  https://www.mozilla.org/zh-TW/firefox/new/

- 建立允許使用者執行的已授權軟體完整清單，並利用 Win7 內建之「軟體限制原則(Software Restriction Policies)」功能[7]，確保已授權軟體能在電腦上執行。以下以「禁止所有軟體，僅允許執行 Google Chrome」為例進行說明。

  (1) 以「系統管理員」身分登入，或以具有系統管理員權限的使用者身分登入。

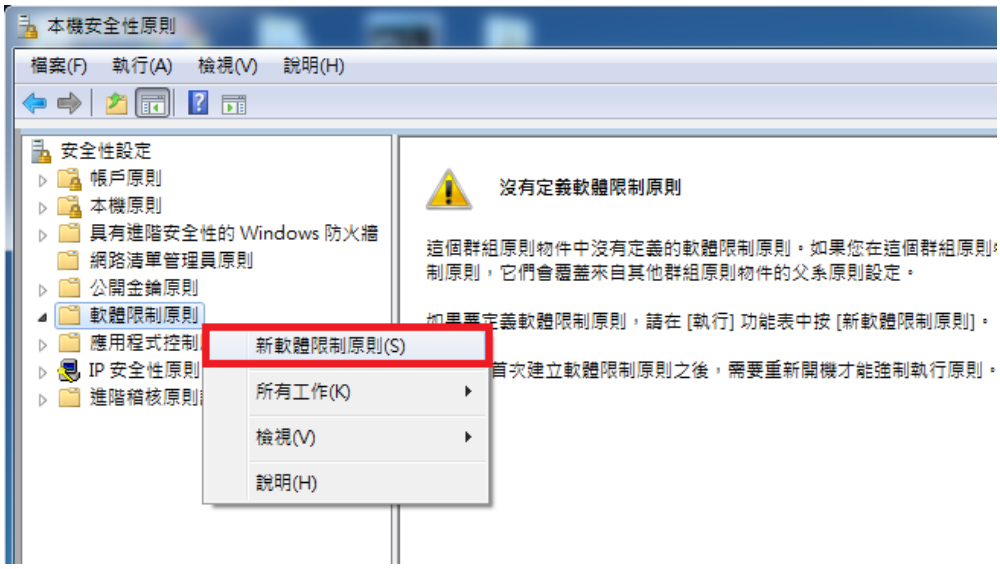
  (2) 按一下「開始」→「控制台」→「系統及安全性」→「系統管理工具」→「本機安全性原則」



資料來源：本中心整理

圖13 選擇「本機安全性原則」

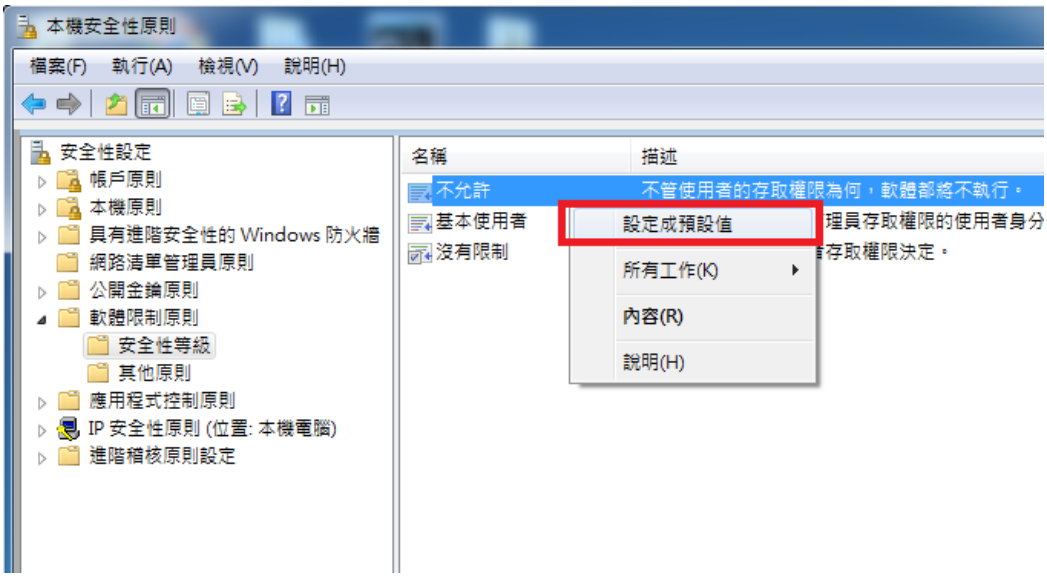
(3) 在左窗格中用滑鼠右鍵按一下「軟體限制原則」，然後按一下「新軟體限制原則」。



資料來源：本中心整理

圖14 新增軟體限制原則

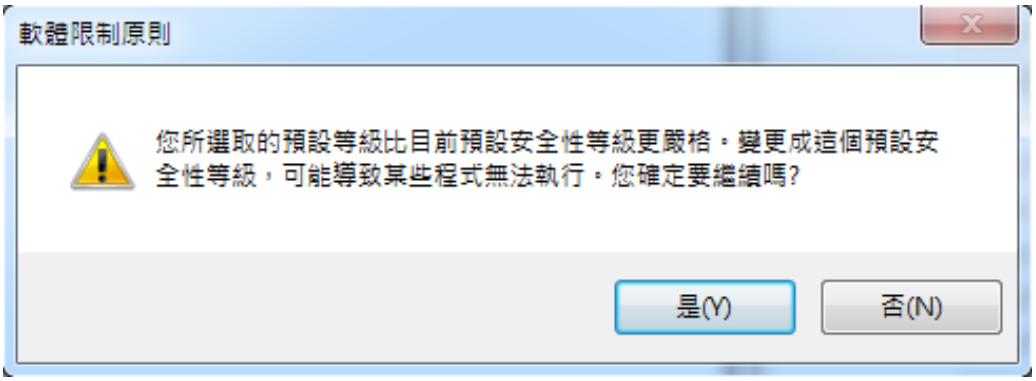
(4) 在左窗格中展開「軟體限制原則」節點，按一下「安全性等級」，用滑鼠右鍵按一下「不允許」，然後按一下「設成預設值」



資料來源：本中心整理

圖15 將「不允許」設成預設值

(5) 按一下「是(Y)」。

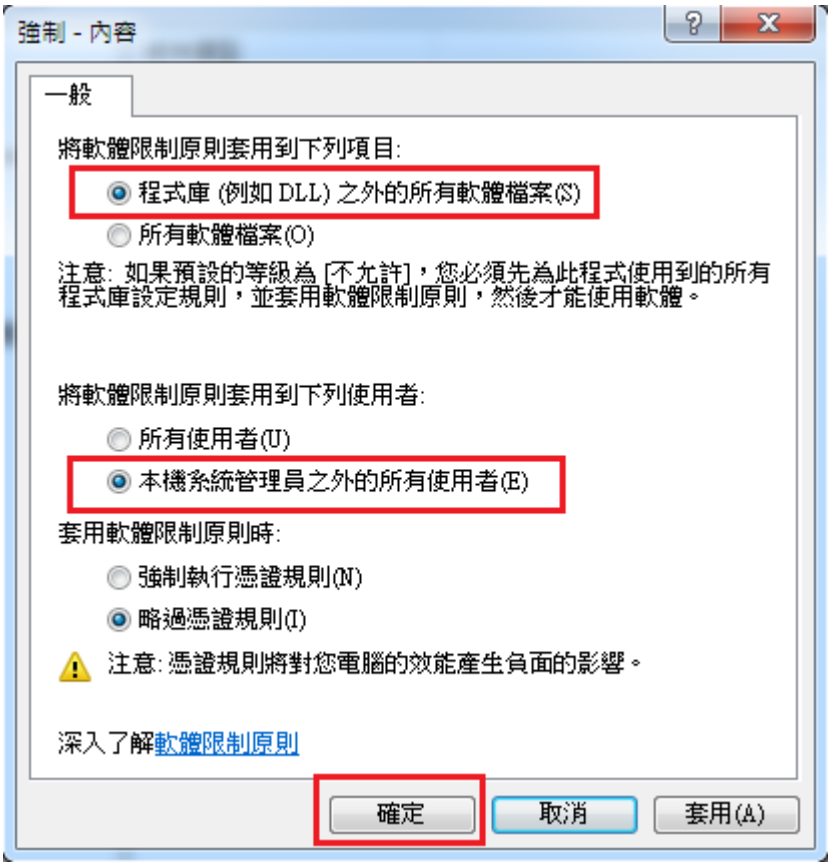


資料來源：本中心整理

圖16 將「不允許」設成預設值

(6) 在左窗格中按一下「軟體限制原則」，按兩下「強制」開啟設定視窗，選取「程式庫(例如 DLL)之外的所有軟體檔案(S)」與「本機系統

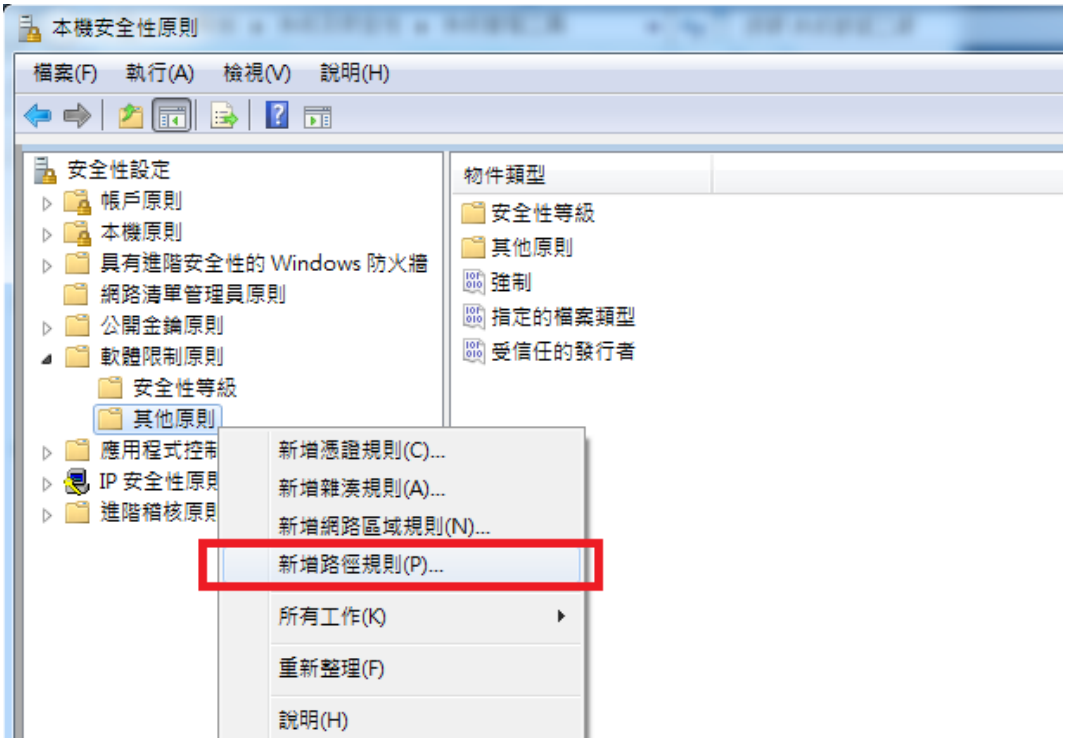
管理員之外的所有使用者」，然後按一下「確定」。



資料來源：本中心整理

圖17 設定強制內容

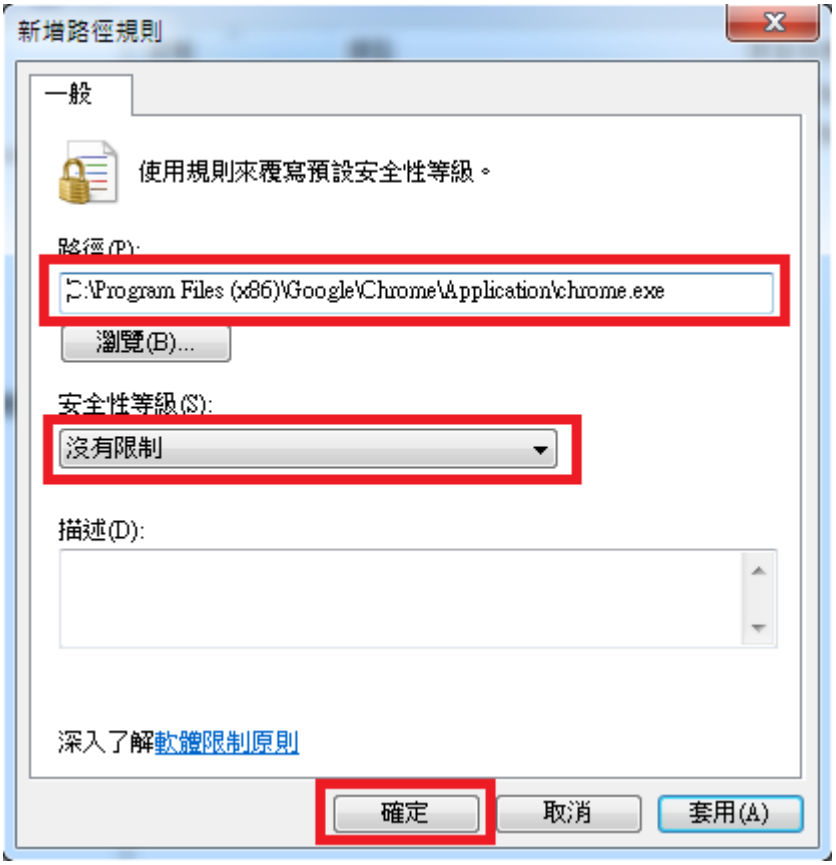
(7) 在左窗格中展開「軟體限制原則」節點，用滑鼠右鍵按一下「其他原則」，然後按一下「新增路徑規則」。



資料來源：本中心整理

圖18 選取「新增路徑規則」

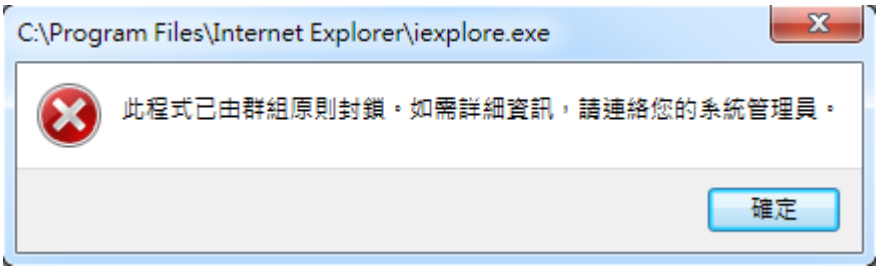
(8) 「路徑」中輸入 chrome.exe 路徑，「安全性等級」選取「沒有限制」，然後按一下「確定」。若有其他允許使用者執行的軟體，請重複執行此步驟。



資料來源：本中心整理

圖19 輸入路徑內容

(9) 以「標準使用者」的使用者身分登入後，可正常執行已授權的軟體(如 chrome.exe 等)。若執行其他未授權軟體(如 IE 等)，則會出現「此程式已被群組原則封鎖，需詳細資訊，請連絡您的系統管理員」之訊息。



資料來源：本中心整理

圖20 無法執行 IE 訊息

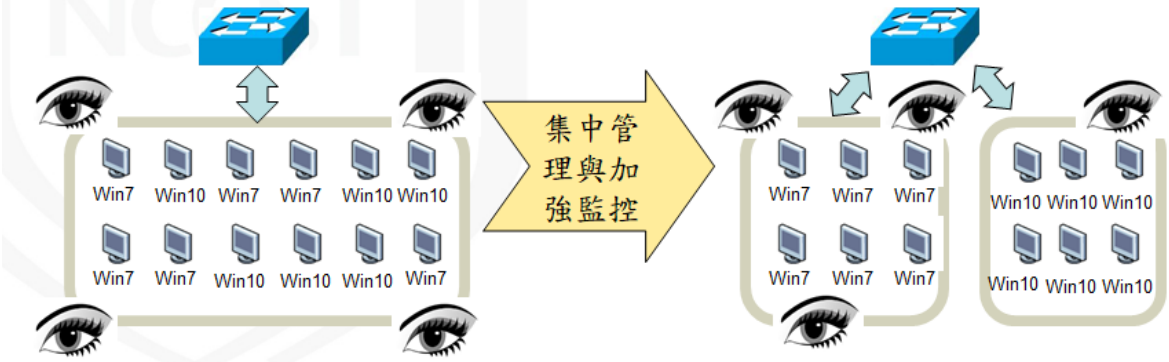
3.2.4. 監控防禦

- 確實安裝防毒軟體，即時更新病毒碼，並至少每週執行一次完整掃描與檢視防毒軟體掃描紀錄。
- 安裝主機端入侵防禦系統(H-IPS)，提升 Win7 電腦防禦能力。
- 在閘道端部署防火牆設備，並透過嚴謹的白名單管理機制，有效管理網路連線行為。
- 利用安全資訊與事件管理(SIEM)進行跨設備關聯式分析與監控，確實掌握使用 Win7 電腦之資安事件與安全防護狀態。

3.3.透過網路區隔加強管理使用 Win7 電腦

若同時存在不同作業系統版本之電腦，可透過下列措施集中管理與加強監控使用 Win7 電腦(詳見圖 21)：

- 利用 VLAN 進行網路區隔，將使用 Win7 電腦放入獨立 VLAN，除便於進行集中管理外，亦可避免影響其他 VLAN 之電腦。
- 針對風險較高之使用 Win7 電腦 VLAN，加強網路流量監控，以有效掌握異常連線行為。



資料來源：本中心整理

圖21 使用 Win7 電腦集中管理與加強監控示意圖

3.4.執行 Win7 弱點持續監測計畫

技服中心將持續進行 Win7 弱點監測與通報作業，包含：

- 蒐集共通弱點與揭露(CVE)網站[4]、美國國家弱點資料庫(NVD)[8]、微軟公司網站[9]及其他相關安全性網站 Win7 弱點資訊。
- 針對新發現之 Win7 弱點資訊，即時通知政府機關注意。
- 彙整政府機關已通報之 Win7 相關資安事件，掌握整體影響情形。

4. 結論

微軟公司已確定 2020/1/14 終止 Win7 支援(EOS)服務，因此政府機關應盡速了解 Win7 使用情形，以掌握可能產生的影響，並針對處理重要業務之電腦，優先完成升級；對於無法更新 Win7 之電腦，也應盡速透過「部署 Win7 GCB」、「安全性設定」及「帳戶權限管控」等措施，強化主機系統的安全。

同時規劃與部署資安防護強化措施，透過網路區隔加強使用 Win7 電腦管理，針對風險較高之使用 Win7 電腦 VLAN，加強網路流量監控。

技服中心也將持續進行 Win7 弱點監測與通報作業，蒐集 Win7 弱點資訊，並彙整政府機關通報之 Win7 相關資安事件，以掌握 Win7 資安事件與影響程度。

5. 參考文獻

[1]Net Applications: Windows 10 passes 50% market share, Windows 7 falls to 30%, https://venturebeat.com/2019/09/01/net-applications-windows-10-windows-7-market-share/。

[2]對 Windows 7 的支援即將終止, https://www.microsoft.com/zh-tw/windows/windows-7-end-of-life-support-information#why-windows-drawer-FAQ。

[3]Windows 7 將於 2020 年 1 月 14 日終止支援, https://support.microsoft.com/zh-tw/help/4057281/windows-7-support-will-end-on-january-14-2020。

[4]CVE Details 弱點資料庫, https://www.cvedetails.com/product/17153/Microsoft-Windows-7.html?vendor_id=26。

[5]NetApplications: Operating System Share by Version, https://netmarketshare.com/operating-system-market-share.aspx?id=platformsDesktopVersions。

[6]政府組態基準(GCB)專區, https://www.nccst.nat.gov.tw/GCB?lang=zh。

[7]軟體限制原則, https://docs.microsoft.com/zh-tw/windows-server/identity/software-restriction-policies/software-restriction-policies。

[8]National Vulnerability Database, http://nvd.nist.gov/。

[9]台灣微軟網站, https://www.microsoft.com/zh-tw/。