因應微軟公司 Windows XP 作業系統終止支援服務之防護措施建議

行政院國家資通安全會報技術服務中心

1. 前言

微軟公司 2001 年推出 Windows XP(以下簡稱 XP)，雖然歷經 Windows Vista(以下簡稱 Vista)、Windows 7(以下簡稱 Win7)到現在的 Windows 8.1(以下簡稱 Win8.1)，至今仍為微軟公司使用期間最長的作業系統[1]。自 2008/6/30 起停售 XP 後，隨著時間的演進，已進入產品生命週期末端，將於 2014/4/8 終止支援(End of Support，簡稱 EOS)，不再針對 XP 提供下述支援服務[2][3]：

- 安全性系統更新檔
- 非安全性系統更新檔
- 修補程式協議支援(付費服務)
- 按事件處理的付費支援服務
- 產品線上支援及線上技術內容更新服務

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

2. XP EOS 對資安影響

微軟公司 XP 作業系統於 2014/4/8 終止服務，將不再針對 XP 提供程式修正、軟體更新及線上技術支援服務，對於 XP EOS 可能產生的影響分析如下：

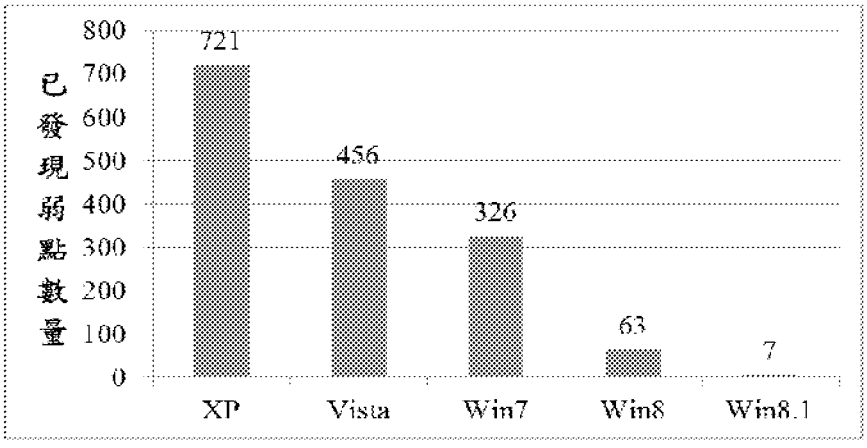
- XP 作業系統相關應用軟體弱點已無法確保可取得更新的修補程式
  - XP 作業系統上所安裝之 Internet Explorer 瀏覽器(以下簡稱 IE)，因其修補程式係透過 XP 作業系統之更新機制進行更新，但 XP 作業系統之更

新機制於2014/4/8終止運作，因此XP作業系統上所安裝之IE於2014/4/8後也將無法取得更新的修補程式。

– 微軟公司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 DirectX)，相對應在 XP 上的安全性更新也不再支援。

●XP 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，XP 作業系統已被發現弱點數量達 721 個(詳見圖 1)[4]，明顯高於 Win7 與 Win8，繼續使用 XP 將可能容易遭惡意人士利用弱點進行攻擊之風險相對較高。



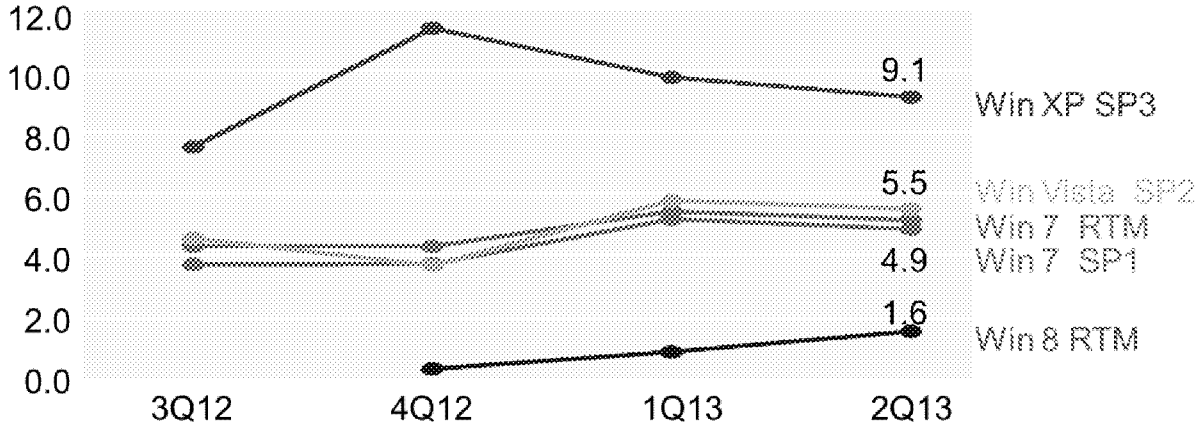
資料來源：CVE Details 弱點資料庫[4]

圖1　各作業系統已發現弱點數量統計

●XP 作業系統惡意程式感染率高

根據微軟公司第十五期資訊安全情報報告[5]，平均每 1000 台 XP 電腦掃描結果含有惡意程式的電腦數量達 9.1 台(0.91%)，遠高於 Win7 與 Win8(詳見圖 2)。此外，微軟公司可信賴運算部門總監 Tim Rains 表示，根據過往經驗，當微軟公司停止支援 XP 更新修補程式後，其他新版如 Win7 或 Win8 等作業系統仍會持續針對新發現弱點按月釋出安全性更新，攻擊者可嘗試

藉由逆向工程手法，確認新發現弱點是否仍存在於 XP 中，並針對確認存在之新弱點開發攻擊碼，使得惡意程式感染率預期大幅攀升至 66%，將可能導致機敏資料外洩[6]。



資料來源：微軟公司第十五期資訊安全情報報告[5]

圖2　各作業系統惡意程式感染率趨勢

3. 防護措施建議

針對 XP EOS 可能產生之資安影響，提供下列防護措施建議供各機關參考。在經費許可的情況下，建議機關應採用「3.1 加速 XP 升級至 Windows 新版作業系統」，盡速升級以確保資訊安全。

若機關尚無經費可全面升級，建議參考「3.2 強化使用 XP 電腦之資安防護」，根據帳戶權限設定、軟體防護及監控防禦等安全性設定，加強 XP 之安全管理。

若機關因應用服務限制而仍須使用 XP，建議參考「3.3 保留 XP 映像檔與使用還原卡」，進行日常電腦安全維護，並參考「3.4.透過網路區隔加強管理使用 XP 電腦」規劃與部署資安防護強化措施，針對風險較高之使用 XP 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 XP 弱點監測與通報作業，並透過「3.5 執行 XP 弱點持續監測計畫」，掌握政府機關 XP 相關資安事件與影響。

3.1.加速 XP 升級至 Windows 新版作業系統

XP 升級至 Windows 新版作業系統為根本解決之道。微軟公司自 2008/6/30 起停售 XP 後，Win7 與 Win8 已分別於 2009/10/22 與 2012/10/26 上市，請各機關加速 XP 升級作業。

若機關發現資安事件入侵原因來自 XP 弱點，則可能該機關已遭鎖定，屬「XP 高風險機關」，應先進行 XP 升級作業。

3.2.強化 XP 電腦資安防護

若機關於微軟公司終止支援後仍需使用 XP，應規劃與部署資安防護強化措施，可透過帳戶權限設定、軟體防護及監控防禦等 3 方面進行，說明如下。

3.2.1. 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機會。將使用者帳戶權限設定為「受限制的」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。

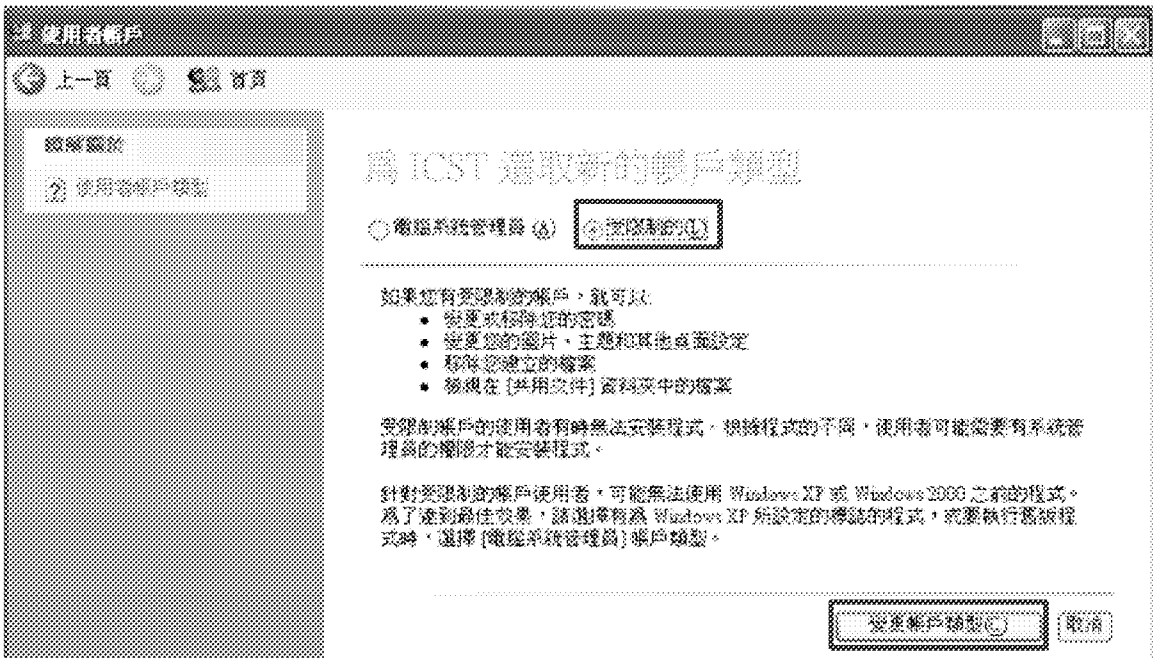
  (2) 按一下「開始」→「控制台」→「使用者帳戶」→「變更帳戶」。

  (3) 按一下要變更的使用者帳戶(例如：ICST)。

資料來源：本計畫整理

圖3　選擇要變更的帳戶

(4) 按一下「變更帳戶類型」，選取「受限制的(L)」，按一下「變更帳戶類型」，即可將帳戶權限設定為「受限制的」帳戶類型。



資料來源：本計畫整理

圖4　選取「受限制的」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「Administrator」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「我的電腦」，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」。

(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：本計畫整理

圖5　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：本計畫整理

圖6 「Administrator」帳戶已停用登入訊息

3.2.2. 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。

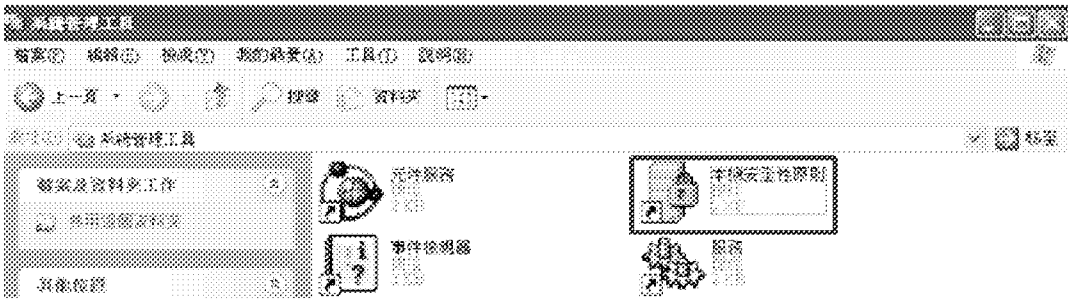
  (1) Google Chrome 瀏覽器下載網址：
  http://www.google.com.tw/intl/zh-TW/chrome/browser/

  (2) Mozilla Firefox 瀏覽器下載網址：
  http://mozilla.com.tw/firefox/download/

- 建立允許使用者執行的已授權軟體完整清單，並利用 XP 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」→「效能及維護」→「系統管理工具」→「本機安全性原則」。



資料來源：本計畫整理

圖7　選擇「本機安全性原則」

(3) 用滑鼠右鍵按一下「軟體限制原則」，然後按一下「建立新原則」。

資料來源：本計畫整理

圖8　建立新原則

(4) 用滑鼠右鍵按一下「軟體限制原則」→「安全性等級」→「不允許」，然後按一下「設成預設值」。

資料來源：本計畫整理

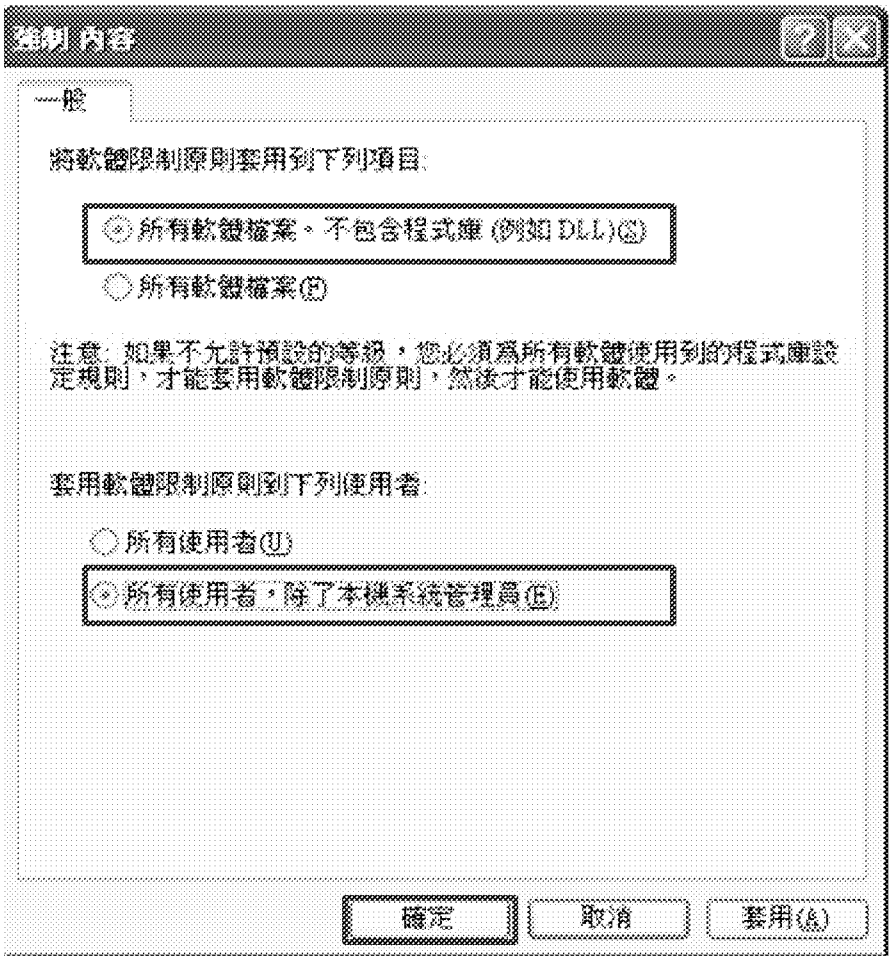
圖9　將「不允許」設成預設值

(5) 按一下「是(Y)」。

資料來源：本計畫整理

圖10 確認將「不允許」設成預設值

(6) 按兩下「軟體限制原則」→「強制」，選取「所有軟體檔案，不包含程式庫」與「所有使用者，除了本機系統管理員」，然後按一下「確定」。



資料來源：本計畫整理

圖11 設定強制內容

(7) 用滑鼠右鍵按一下「軟體限制原則」→「其他原則」，然後按一下「新增路徑規則」。

資料來源：本計畫整理

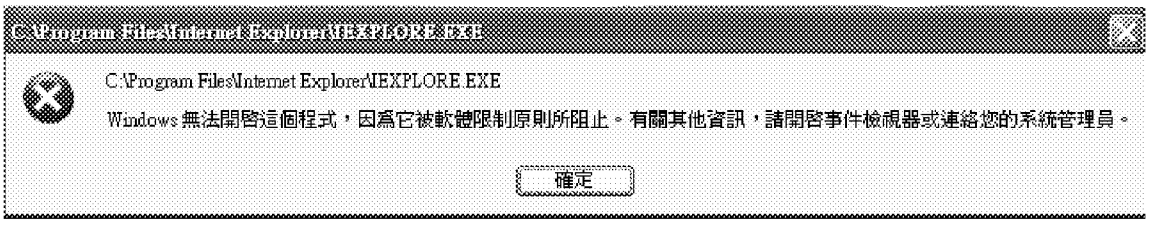
圖12 選取「新增路徑規則」

(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：本計畫整理

圖13 輸入路徑內容

(9) 以「受限制的」的使用者身分登入後，可正常執行已授權的軟體(例如：chrome.exe)。若執行其他未授權軟體(例如 IE)，則會出現「Windows 無法開啟這個程式，因為它被軟體限制原則所阻止」之訊息。



資料來源：本計畫整理

圖14 無法執行 IE 訊息

- 針對已安裝之所有應用程式即時進行更新，避免應用程式漏洞危害系統安全。

3.2.3. 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 XP 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 XP 電腦之資安事件與安全防護狀態。

3.3.保留 XP 映像檔與使用還原卡

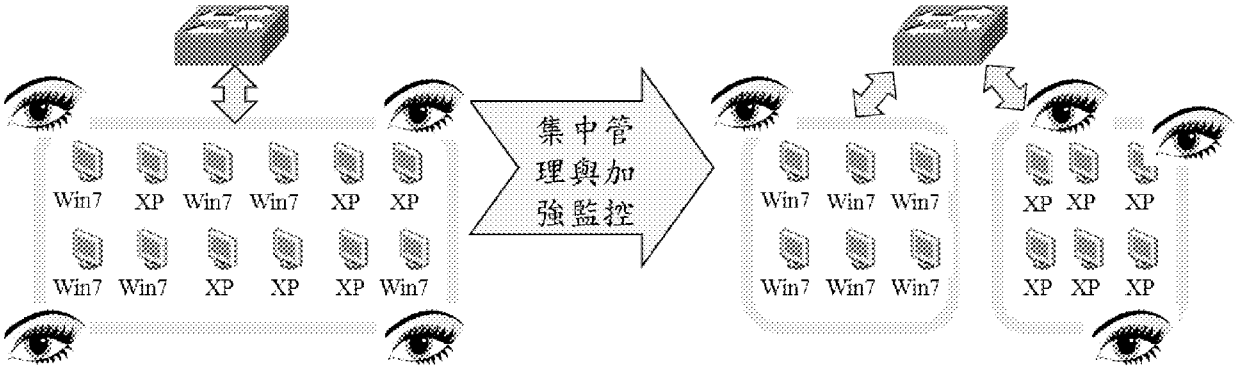
當 XP 於 2014/4/8 正式終止支援服務後，機關內重新安裝之 XP 作業系統已無法連線至微軟公司更新伺服器進行更新作業，若機關仍需繼續使用 XP，建議可進行下列保護 XP 作業系統環境措施：

- 建置乾淨的 XP 作業系統環境母機，持續更新至 2014/4/8，並保留該母機之映像檔，供日常電腦維護之用。
- 將作業環境與資料分開存放，並透過還原卡保護系統安全，使得電腦開機後可回復系統碟至原始乾淨母機狀態。

3.4.透過網路區隔加強管理使用 XP 電腦

機關內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 XP 電腦(詳見圖 15)：

- 利用 VLAN 進行網路區隔，將使用 XP 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 內之電腦。
- 針對風險較高之使用 XP 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：本計畫整理

圖15 使用 XP 電腦集中管理與加強監控示意圖

3.5.執行 XP 弱點持續監測計畫

技服中心將持續進行 XP 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 XP 弱點資訊。
- 針對新發現之 XP 弱點資訊，即時通知各機關注意。
- 彙整政府機關已通報之 XP 相關資安事件，掌握整體影響情形。

4. 結語

微軟公司已確定 2014/4/8 終止 XP 支援(End of Support，簡稱 EOS)服務，因此各機關應盡速了解機關內部 XP 的使用情形，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 XP 之電腦，也應盡速透過 XP 的安全性設定與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 XP 電腦管理，針對風險較高之使用 XP 電腦 VLAN，加強網路流量監控。

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

5. 參考文獻

[1] Windows XP 終止支援倒數 99 天, http://www.ithome.com.tw/itadm/article.php?c=84554。

[2] Windows XP – Support stops on 8. April 2014 ,http://download.microsoft.com/download/5/D/A/5DAF3FBA-8145-4E4E-8E5D-CDFED1EF1D13/FINAL_XP-EoS-Whitepaper.pdf。

[3] Windows XP 暨 Office 2003 產品終止支援服務說明, https://ca.nctu.edu.tw/files/MS_public_1020603108.pdf。

[4] CVE Details 弱點資料庫, http://www.cvedetails.com/product/739/Microsoft-Windows-Xp.html?vendor_id=26。

[5] Microsoft SecurityIntelligenceReportVolume15, http://download.microsoft.com/download/5/0/3/50310CCE-8AF5-4FB4-83E2-03F1DA92F33C/Microsoft_Security_Intelligence_Report_Volume_15_English.pdf

[6] New cybersecurity report details risk of running unsupported software, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/10/29/new-cybersecurity-report-details-risk-of-running-unsupported-software.aspx。

[7] 軟體限制原則，在 Windows XP 中的描述, http://support.microsoft.com/kb/310791/zh-tw

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

[9] 台灣微軟網站, http://www.microsoft.com/taiwan。