# 國立清華大學電機系中毒 IP 處理程序及相關措施

93 年 3 月 5 日系務會議通過

1. 本系工作站室在收到本校計算機與通訊中心中毒 IP 通知後，將以電話通知該 IP 登記負責人，請受通知人員於 1 小時內做緊急處置回報處理（詳如第 2 項所述），並於 24 小時內依完整處理程序（詳如第 3 項所述）處理完畢且回報至工作站室或計算機與通訊中心。
   - 回報至工作站室：於完成完整處理程序後，該 IP 將可先行在本系內使用，待計算機與通訊中心處理完畢後，該 IP 方可連線至電機系以外網域。工作站室聯絡電話：1141。無法聯絡至工作站室者，請先聯絡電機系辦公室。
   - 回報至計算機與通訊中心：待計算機與通訊中心處理完畢後，工作站室將依據計算機與通訊中心—不當網路資訊篇，解除該 IP 的管制。計算機與通訊中心電話：1134
2. 緊急處置回報主要為確認中毒 IP 之相關使用者知曉中毒情事，並完畢緊急處置，例如拔除網路線。緊急回報內容需包含以下事項：
   I. 處置的人員及連絡方式
   II. 處置的中毒機器
   III. 處置的措施

   例如：小明找到中毒的電腦為小黃所有。小明先替小黃將電腦的網路線拔除，並通知小黃 24 小時內前來處理完畢，小黃確認他收到通知，聯絡電話為 xxxx。
3. 完整處理程序包含以下事項：
   I. 收到通知後，先行拔除網路線。
   II. 確實進行清理病毒動作或重新安裝作業系統。
   III. 如為 Windows 作業系統，請先離線安裝微軟公布之重大修補程式，進行 Windows Update。其他作業系統，請參考相關網站，進行 patch 更新。
   IV. 安裝防毒軟體或更新病毒定義檔。
   V. 設定 Windows 簡易防火牆(或其他進階防火牆)後，可插上網路線，回報處置完畢。
4. 若工作站室於一小時內連續三次（以工作站室日誌為基準）無法通知該中毒 IP 負責人緊急處置，為避免中毒情形加速擴散，工作站室將採取應變措施，先行關閉該中毒 IP 在電機系交換器上之網路埠，與該網路埠相關之所有實驗室網路將會受影響。同時工作站室會採取以下二步驟：
   I. 電話及 Email 通知該實驗室老師
   II. 發通知函於實驗室門口告知網路斷線緣由及處置狀況

   待中毒 IP 緊急處置後，將盡快恢復相關實驗室之網路使用。
5. 如中毒發生於例假日，並無法通知該中毒 IP 負責人緊急處置時，將依第 4 項之應變措施處理，但通知程序將於上班時間進行。如欲回報處置狀況且工作站室無人值班，請 Email 至 opr@ee.nthu.edu.tw 連絡。

6. 接獲工作站室通知後，但未於一小時內完成緊急處置者，依第 4 項之應變措施處理。若無不可抗拒之原因，該中毒 IP 將禁止使用一個月。工作站室並將公布該使用者、IP、實驗室及指導老師於電機系網頁上，且將名單函送電機系辦公室處理。
7. 未於 24 小時內完成完整處理程序回報者，若無不可抗拒之原因，該中毒 IP 禁止使用一個月。工作站室將公布該使用者、IP、實驗室及指導老師於電機系網頁上，且將名單函送電機系辦公室處理。
8. 連續於一小時內有 3 台以上電腦中毒之實驗室，依第 4 項之應變措施處理。該實驗室完成緊急處置後，將立刻開放網路埠。
9. 實驗室如於一星期內達 3 次以上緊急處置處理，將聯絡該實驗室指導老師，並輔導該實驗室改進一週（詳如第 10 項所述）。如未配合輔導辦法改善實驗室，工作站室將回收所有中毒 IP，並禁止該實驗室申請 IP 三個月。
10. 輔導改進項目包含以下事項：
    I. 與工作站室值班人員約定時間
    II. 工作站室值班人員前往檢查該實驗室所有電腦防護措施
        - 防毒軟體
        - 防火牆
        - Windows Update
11. 不當架設非研究或教學使用網站，或佔用大量網路資源，影響網路效能者，將聯絡該實驗室指導老師，請其督導該實驗室停止架設非法使用網站。如一週後該網站未下線，將公布該使用者、IP、實驗室及指導老師於電機系網頁上，回收不當使用 IP，並禁止該實驗室申請 IP 三個月。
12. IP 異動，包括變更使用負責人、聯絡電話（行動電話為佳）、使用機器、MAC 時，請主動告知工作站室更新資料，避免影響使用 IP 權益。