財團法人國家實驗研究院
國家地震工程研究中心

資訊安全管理制度輔導顧問案

資訊安全技術課程

講師：邱瑩青

NII財團法人中華民國國家資訊基本建設產業發展協進會

課程大綱

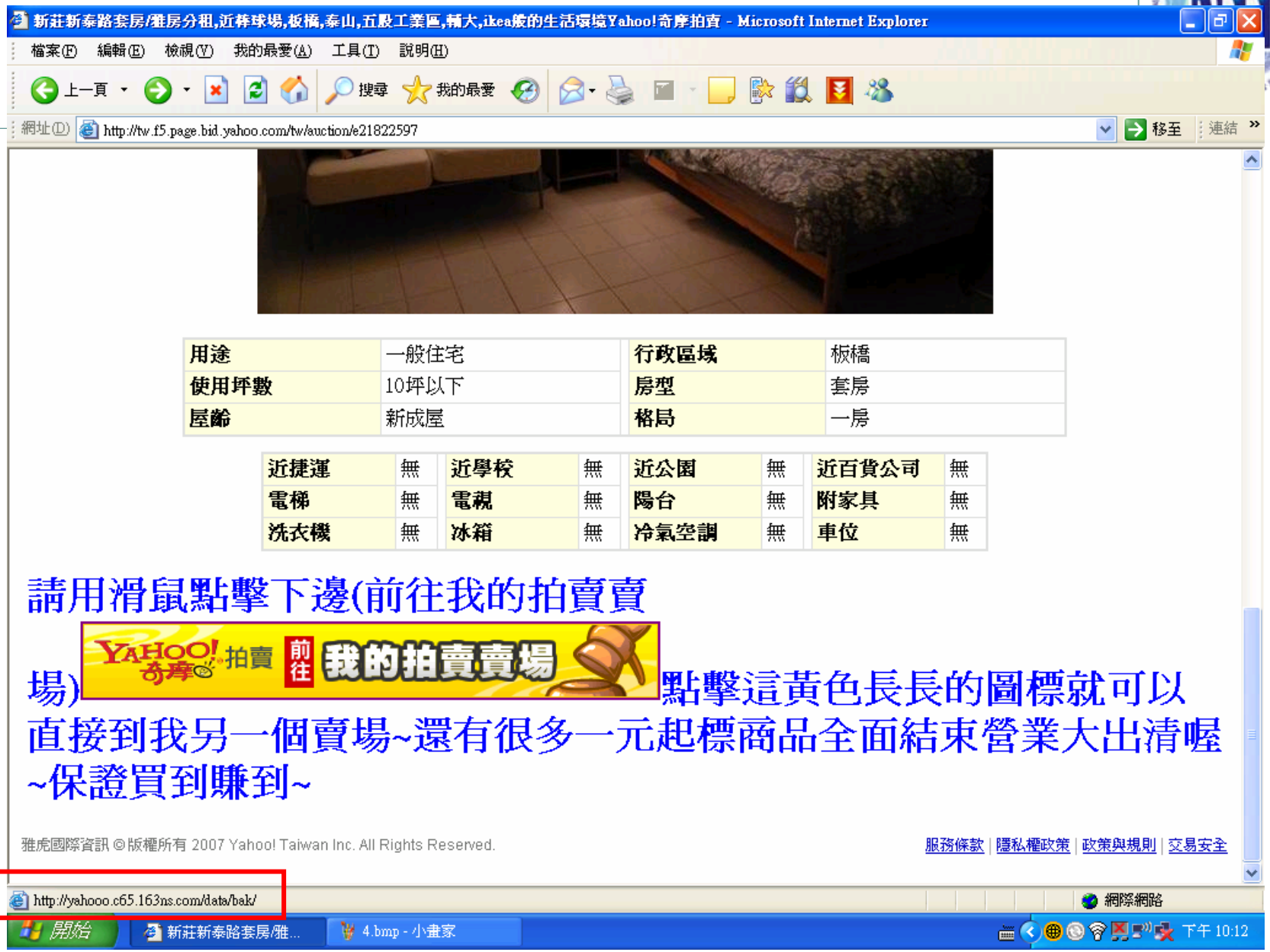
- 網路安全概論
- 駭客概述
- 電腦病毒
- 木馬及後門程式
- 常見入侵來源
- 惡意程式防護
- 資料及隱私權保護
- 防範SQL Injection攻擊
- 行動設備安全
- 無線網路安全

這天，

發現網路上詐騙集團正在進行詐騙...

10月9日晚上10點，發現Yahoo拍賣的釣魚網頁...

建立一個偽「我的拍賣賣場」釣魚網頁...



盜取帳號密碼，成為犯案冤大頭...

更多的是進入信箱查看買賣記錄來進行電話詐騙...

網路釣魚Phishing

- 利用偽造電子郵件與網站作為誘餌，詐騙使用者洩漏如帳戶密碼等個人機密資料
- 釣魚電子郵件中所提供的超連結，其網址會與你實際所前往網址不同
- 乍看下為知名公司網址，但這個網址其實並非官方網站

- 網路安全概論
- 駭客概述
- 電腦病毒
- 木馬及後門程式
- 常見入侵來源
- 惡意程式防護
- 資料及隱私權保護
- 防範SQL Injection攻擊
- 行動設備安全
- 無線網路安全

關於資訊安全

- 早期的資訊安全
  - 保護機密資料，防止未經授權的竊取
  - 多為國防等政府機構
- 現在的資訊安全
  - 技術面＋管理面
  - 資料及系統的機密性、完整性、可用性
  - 政府機構、企業等皆已正視資訊安全的重要性

網路安全資安威脅

- 中斷威脅
  - 使系統資源遺失、無法取用
    - 惡意破壞硬體設備
    - 刪除程式或資料檔
    - 阻絕服務

網路安全資安威脅

- 截取威脅
  - 非授權使用者非法存取系統
    - 拷貝資料
    - 截聽封包

網路安全資安威脅

- 更改威脅
  - 非授權使用者非法異動系統
    - 篡改資料庫或傳輸的資料
    - 更改程式

網路安全資安威脅

- 仿冒威脅
  - 惡意人士仿造資料，資料使用者或接收端無法分辨真偽
    - 插入其他交易資料
    - 偽造資料記錄

關於網路入侵

- 網路攻擊三階段
  - 準備階段
    - 目標掃瞄、弱點試探...
  - 攻擊及攻佔後之階段
    - 密碼破解、利用漏洞攻擊、植入後門...
  - 毀滅階段
    - 阻絕服務、置換網頁、刪除資料...

2004年，中國保釣聯合會網站遭日本黑客攻擊，
首頁被篡改、論壇被刪除...

中國黑客八一反擊戰...

中國最有影響力的幾個黑客組織共組織了1900餘人參與了這一「反擊戰」，

攻擊對像包括日本、台灣等200餘個包括靖國神社、衛生部、學生部等官方商業廣告網站...

- 掃瞄組
  - 負責收集日本的IP地址，以及進行漏洞分析
- 入侵組
  - 負責入侵日本主機修改其資料，留下後門
- 攻擊組
  - 負責使用暴力DDOS等方法攻擊日本主機
- 安全組
  - 負責網路安全防禦，防止國外的駭客發動網路入侵
- 戰績統計組
  - 負責收集所有的成果進行記錄統計並及時登錄在其網站上

2006年，中國黑客襲擊日本政府網站
發動新的『抗日戰爭』...

在1月24日到2月13日期間
曾襲擊約30個日本網站...

2006年11月，無名小站遇駭事件...

13 筆資料外洩 …？

- XSS（Cross Site Scripting) 攻擊
  - 手法類似於釣魚詐騙，誘騙使用者點擊陷阱頁面，截獲Cookie
  - 再以該使用者的 Cookie 偽造成當事人，對Server發出要求送出某資料或是接收某資料要求
  - 接收某資料可能就是接收你的「個人資料」頁面（可能含密碼與真實個人資訊）
  - 送出某資料可能就是送出修改你的「某個公開頁面」之要求，製造出下一個詐騙網頁

- XSS（Cross Site Scripting) 攻擊 (續)
  - 造成這種安全隱憂的前提，是網頁程式沒有寫好，沒有把使用者所送出的某些可在瀏覽器執行之程式碼，(例如 JavaScript)譯碼成純文字內文送出所發生的

- XSS（Cross Site Scripting) 攻擊 (續)
  - XSS 攻擊受到威脅的是瀏覽無名網站的使用者，資料會被竊的也是在這段期間瀏覽無名網站的使用者
  - 在使用者瀏覽被植入惡意資料的頁面時，個人資料會被竊
  - 因此，就算無名及時把 XSS 漏洞補起來，在使用者瀏覽已被植入惡意資料的回應及文章時，個人資料仍會被竊

遭竊的會員資料部分流傳到中國大陸，中國一個駭客論壇發表了「號稱台灣最大Blog站點(無名小站)存在嚴重XSS漏洞」文章

甚至提供檔案連結下載無名小站用戶資料...

站方在這次教訓後，

立刻修補系統漏洞...

- 網路安全概論
- 駭客概述
- 電腦病毒
- 木馬及後門程式
- 常見入侵來源
- 惡意程式防護
- 資料及隱私權保護
- 防範SQL Injection攻擊
- 行動設備安全
- 無線網路安全

駭客概述 (1/4)

- 駭客
  - 飛客(Phreak)
    - 「飛客」是「駭客」的前身，許多網路入侵、破解密碼的知識技巧，都是早期「飛客」的經驗累積
  - 駭客(Hacker)
    - 技術專才
  - 怪客(Cracker)
    - 入侵、破壞與偷取資料

駭客概述 (2/4)

- 媒體上所謂的駭客
  - 專門入侵他人系統進行不法行為的電腦高手
- 為什麼駭客要入侵您的電腦
  - 玩家
  - 心術不正的駭客

駭客概述 (3/4)

- 駭客生態的演變
  - 動機 → 錢財
    - 尋找安全漏洞入侵，綁架電腦、出租作為垃圾郵件跳板，或參與竊取企業機密資料的攻擊行動
    - 駭客有一個地下市場，若能找到微軟或其他人沒有發現到的可攻擊安全漏洞，就可以獲得一千美元的獎賞 (資料來源：CipherTrust)
    - 這些被入侵的系統稱為殭屍電腦，可以用來轉發垃圾郵件、架設惡意程式網站或發動阻斷DoS攻擊
    - 惡意程式作者是過去把撰寫程式當休閒娛樂，現在則把它當成賺錢事業

駭客概述 (4/4)

- 駭客生態的演變 (續)
  - 駭客轉趨無聲，發動緩慢、鬼祟的攻擊
  - 網釣漸漸變成鎖定特定受害者
    - 魚叉式網路釣魚：針對特定目標進行攻擊的網路釣魚攻擊，假冒該公司寄釣魚郵件，誘使員工登錄其帳號密碼
  - 也有木馬程式鎖定企業網路帳號，遂利商業間諜目的
    - 一旦有利可圖，攻擊手法也會愈來愈複雜
  - 網路釣魚增加最快
  - 蒐集個人資料的攻擊程式佔一半以上的比例

- 網路安全概論
- 駭客概述
- 電腦病毒
- 木馬及後門程式
- 常見入侵來源
- 惡意程式防護
- 資料及隱私權保護
- 防範SQL Injection攻擊
- 行動設備安全
- 無線網路安全

電腦病毒 (1/2)

- 以前的電腦病毒
  - 所謂電腦病毒在技術上來說，是一種會自我複製的可執行程式
- 現在的電腦病毒
  - 包括利用Java和ActiveX的特性來撰寫病毒
  - 對使用者會造成不便的這些不懷好意的程式碼，泛稱為病毒

電腦病毒 (2/2)

- 瞭解現在的病毒
  - 第一代病毒常見的是一些可執行檔，像副檔名為.exe及.com的檔案
  - MS Office所提供的巨集功能甚強, 使用Office巨集寫的病毒也愈來愈多
  - 第二代病毒可謂寄生在網路上→Java和ActiveX

USB病毒 …

如果您的USB儲存媒體，安裝到電腦以後，無法從我的電腦中直接開啟，那麼你的電腦就可能已經感染了USB病毒...

- 各種可能中毒徵兆尚包括
  - 無法在我的電腦中點選硬碟進入、
  - 隨身碟出現 RECYCLER資料夾、
  - 硬碟根目錄中出現autorun.inf 檔案等...

USB病毒會主動感染隨身碟，

只要電腦插上受病毒感染的USB隨身碟，該台電腦就會跟著中毒...

- USB病毒感染說明
  - 當電腦接上隨身碟時，系統會自動通知事件記錄器，而病毒程式也由事件記錄器得知已連接USB隨身碟，並將病毒寫入至隨身碟。
  - 由於一般隨身碟皆設定為可讀寫模式，因此病毒能順利寫入autorun.inf檔案和其他病毒檔案。

- USB病毒特性
  - USB隨身碟的病毒與一般電腦病毒相似，只是此類型的病毒通常會搭配autorun.inf檔案，從USB隨身碟感染至電腦。
  - autorun.inf是一個自動執行的指令檔，內容是設定電腦在新增外接式媒介（例如VCD、DVD）的連結時，自動讀取相關資料並執行程式。如果您確定自己並沒有在隨身碟上撰寫過任何autorun.inf檔案，那麼這個檔案就一定是電腦病毒產生的。
  - 並且可以用記事本打開autorun.inf，看它內容自動執行了哪一個程式。

- 正確開啟隨身碟
  - 檢視隨身碟是否有autorun.inf檔案。為避免開啟隨身碟時自動執行了autorun.inf，而將病毒感染至電腦，應使用不會執行autorun.inf的正式操作方式開啟，說明如下：
    - 插入隨身碟前，先按住「Shift」鍵再插入隨身碟，這樣的開啟方式可取消自動執行動作
    - 勿直接點選在隨身碟磁碟機使用滑鼠左鍵Double Click的方式開啟，Double Click方式仍可能啟動autorun.inf

- 關閉電腦的自動執行設定
  - 開始 → 執行 → 輸入 gpedit.msc
  - 「群組原則」視窗，左邊的電腦設定 → 系統管理範本 → 系統
  - 右邊的「關閉自動播放」，滑鼠左鍵雙擊
  - 出現「關閉自動播放內容」對話窗，點選「已啟用」
  - 在「停用自動播放在」的下拉選單，選擇「所有裝置」
  - 完成，插上隨身碟就不會再自動執行了

- 關閉電腦的自動執行設定（Windows XP Home Edition）
  - 開始 → 執行 → 輸入 regedit
  - 尋找機碼 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun
  - 若不為16進制的255，則改成255；若需要設定光碟機保持自動播放，則改成95（同樣16進制），修改完畢重開機

- 手動刪除USB病毒
  - 開啟命令提示字元（「開始」→ 點選「執行」）
  - 切換至隨身碟磁碟機代號，如「F:」
  - dir /a（檢視有無autorun.inf及奇怪的.exe檔）
  - attrib -s -h -r *.inf
  - type autorun.inf
  - 查看可疑的.exe檔在哪裡
  - 切換至可疑的.exe所在目錄，同樣attrib -s -h -r *.exe
  - del所有可疑的.exe檔
  - del autorun.inf

- 電腦的USB病毒防範
  - 關閉自動播放功能
  - 插入隨身碟時，先按住「Shift」鍵，停止自動執行
  - 開啟隨身碟請用滑鼠右鍵→「內容」或以「檔案總管」瀏覽，勿用滑鼠左鍵雙擊
- 隨身碟的USB病毒防範
  - 在他人電腦上使用隨身碟，先將隨身碟切至防寫模式（如果有）

- 網路安全概論
- 駭客概述
- 電腦病毒
- 木馬及後門程式
- 常見入侵來源
- 惡意程式防護
- 資料及隱私權保護
- 防範SQL Injection攻擊
- 行動設備安全
- 無線網路安全

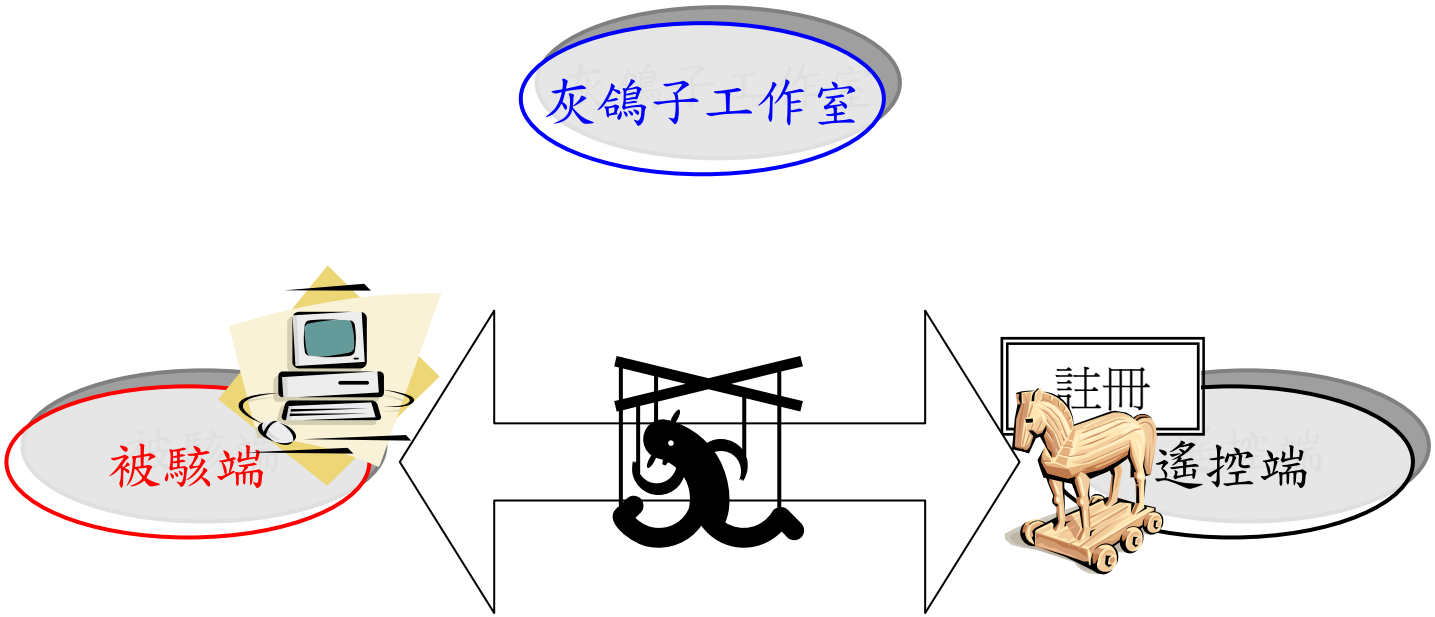
木馬及後門程式 (1/2)

- 後門程式簡介
  - 不懷好意的後門程式
  - 遠端管理程式
- 定義
  - 廣義的木馬後門程式
    - 在使用者不知情的情況下，就對外通訊的程式
  - 狹義的木馬後門程式
    - 竊取電腦內的資料與操控對方的電腦

木馬及後門程式 (2/2)

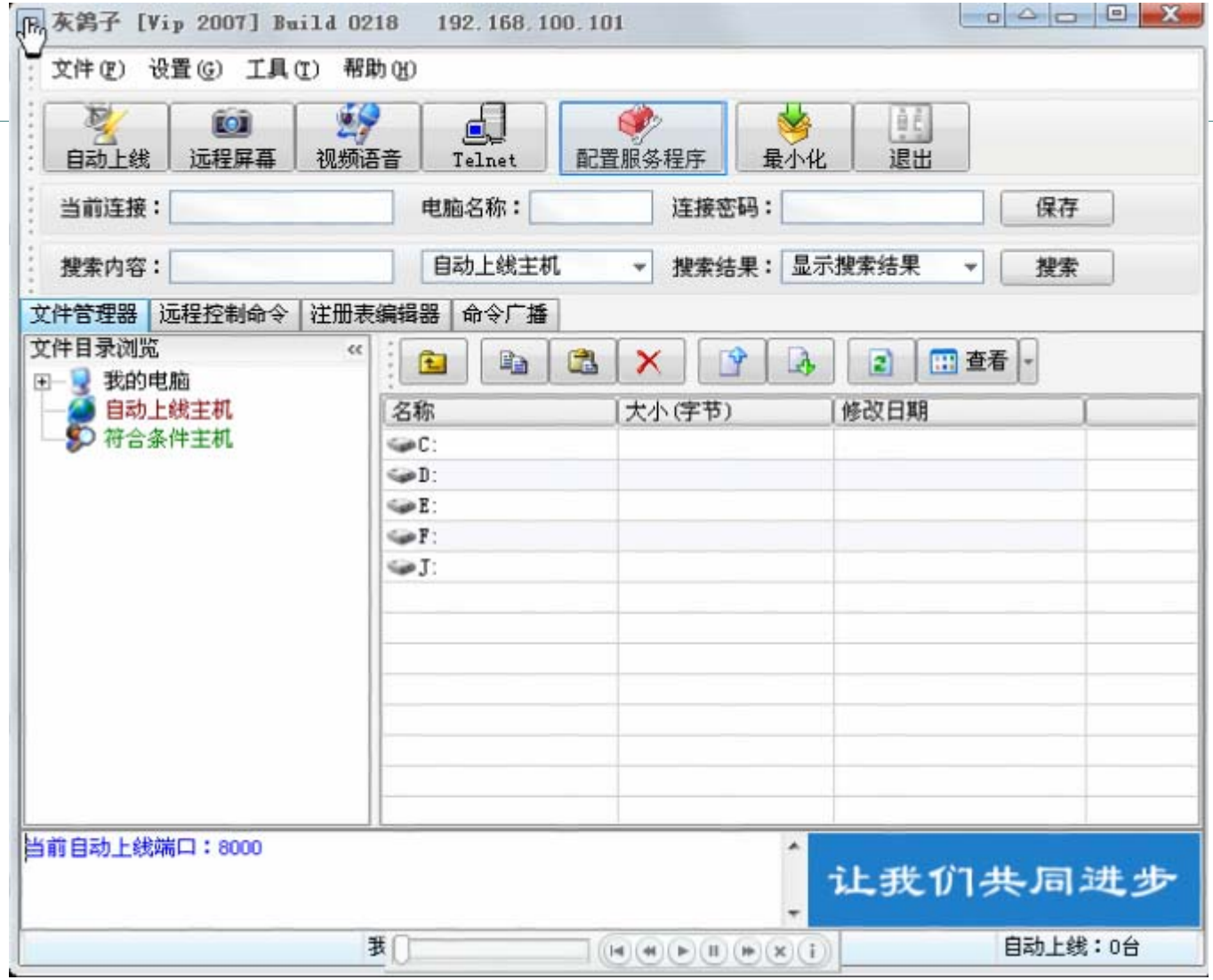
- 植入木馬後門程式的方法
  - 主動植入
    - 電腦本身有漏洞
    - 被攻擊的人通常是攻擊者的熟人
  - 被動植入
    - 駭客引誘使用者下載木馬後門程式
    - 電子郵件
    - 圖片下載
    - 程式下載
    - 破解軟體

中國的頭號木馬程式「灰鴿子」..

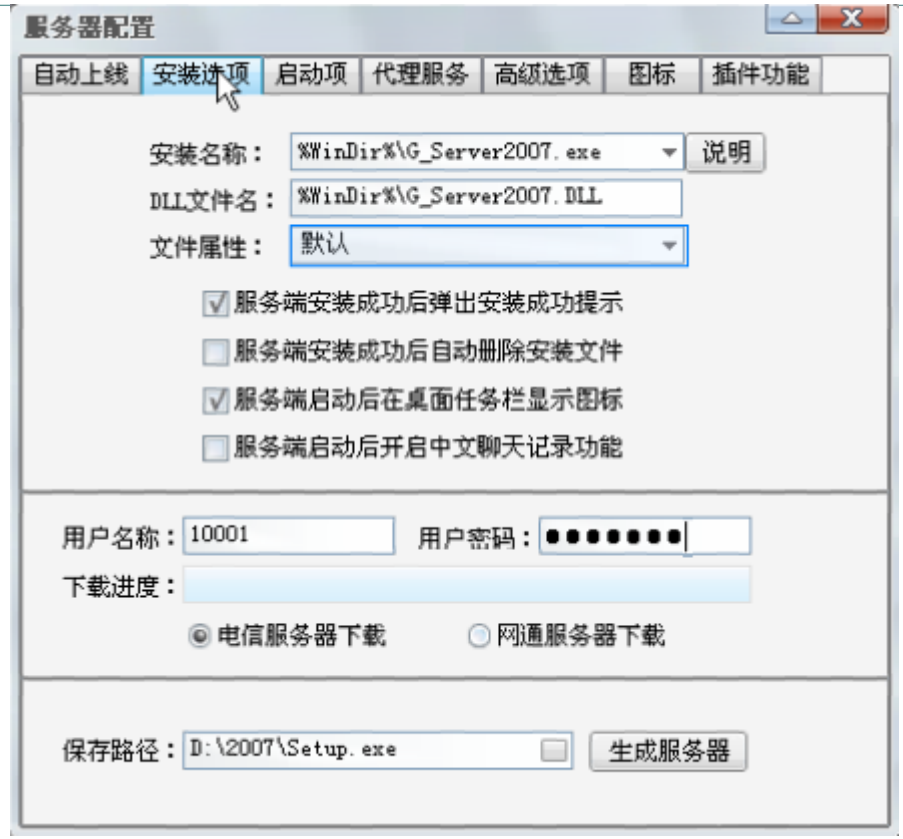


產生「灰鴿子」木馬程式..

灰鴿子遙控端畫面...

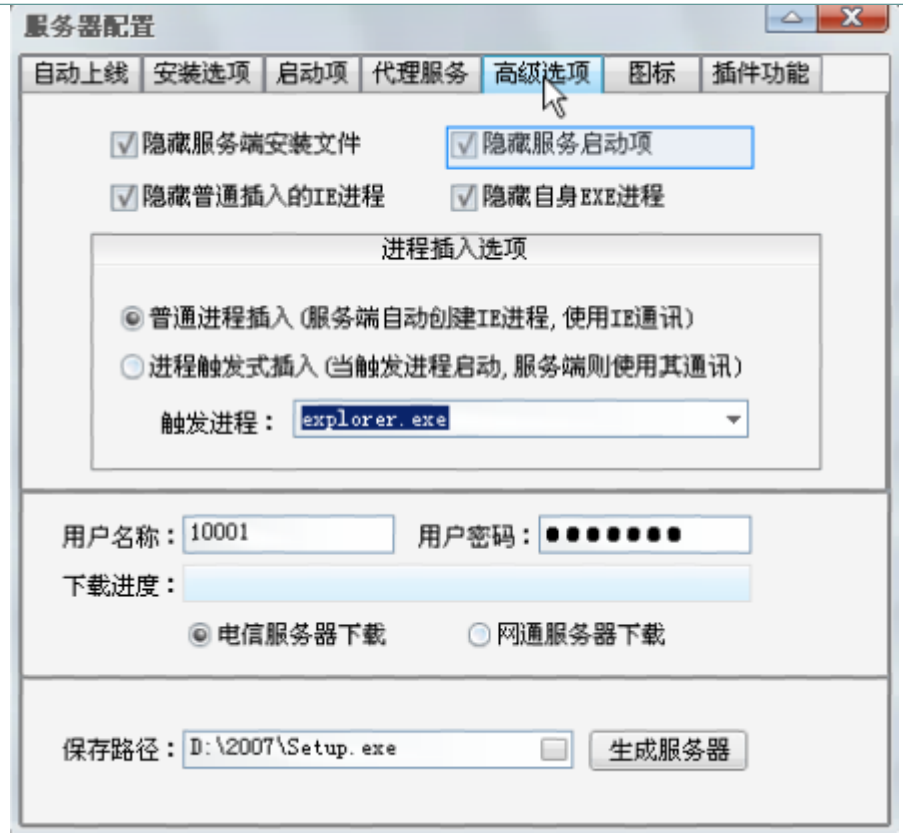


偽裝灰鴿子執行程式...

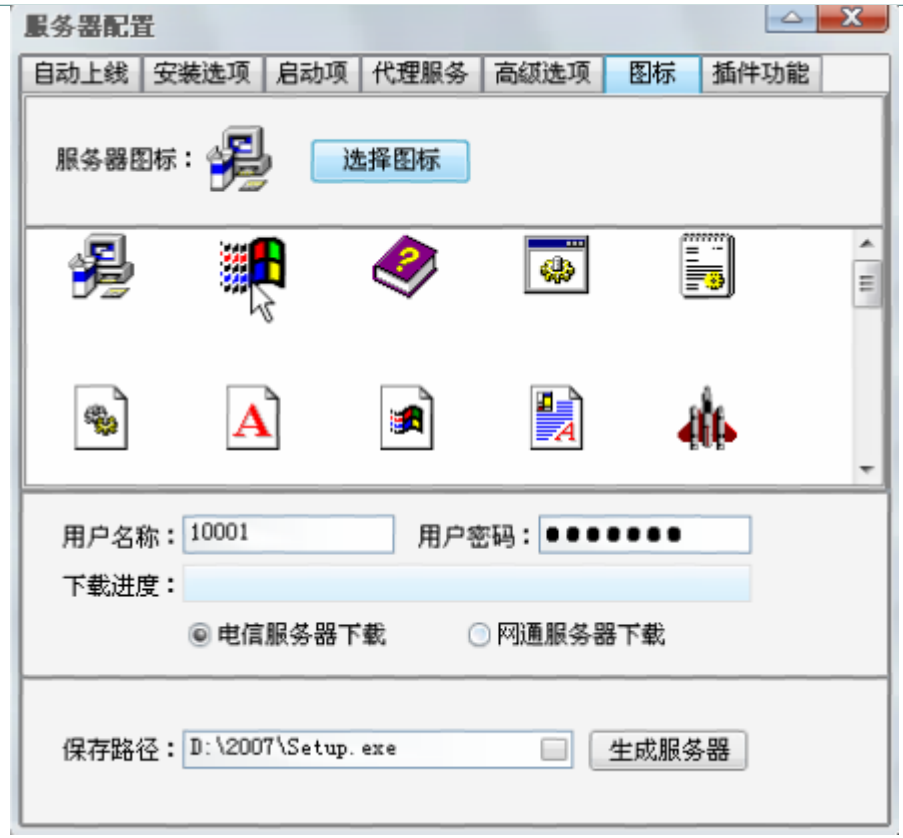


偽裝顯示名稱與描述...

隱藏服務...



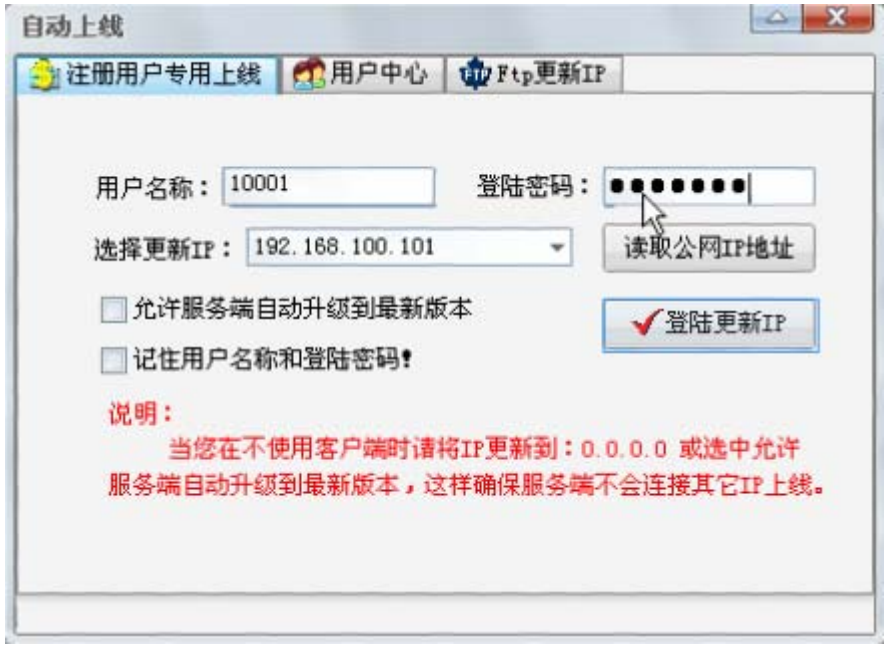
偽裝令人不會起疑的圖示...



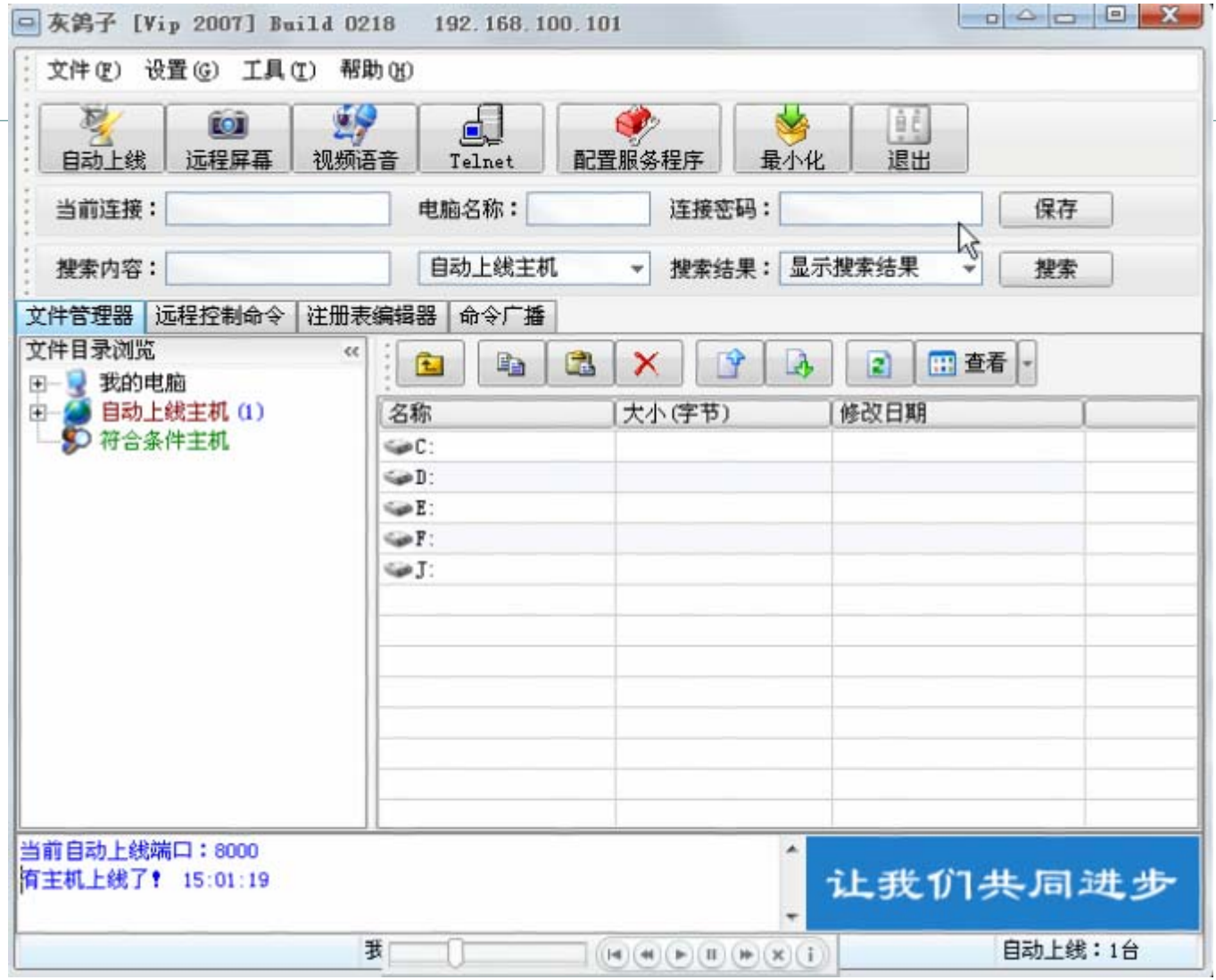
產生被遙控端的安裝程式...

「灰鴿子」可以作什麼..

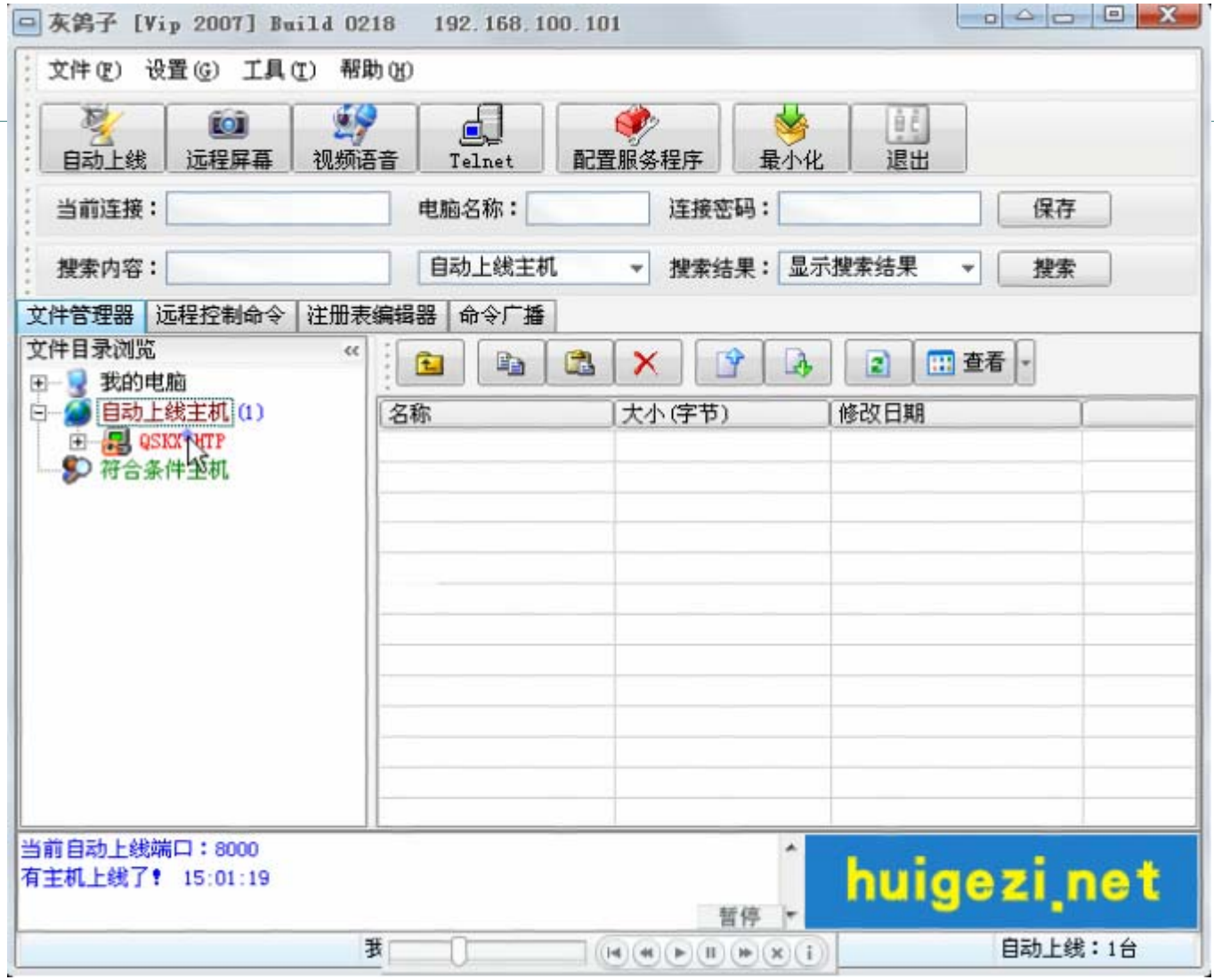
遙控端登入...



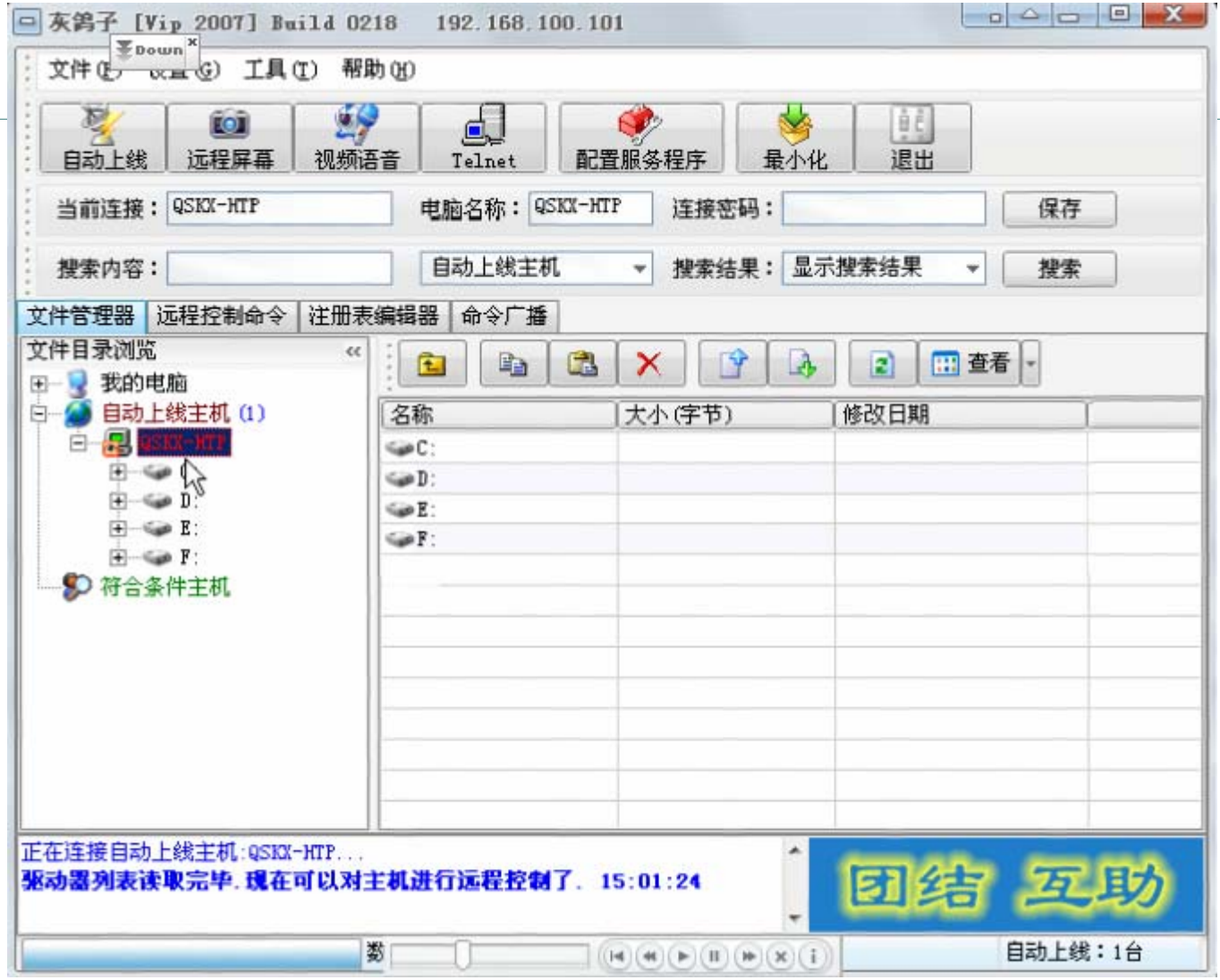
等待「肉雞」上線...



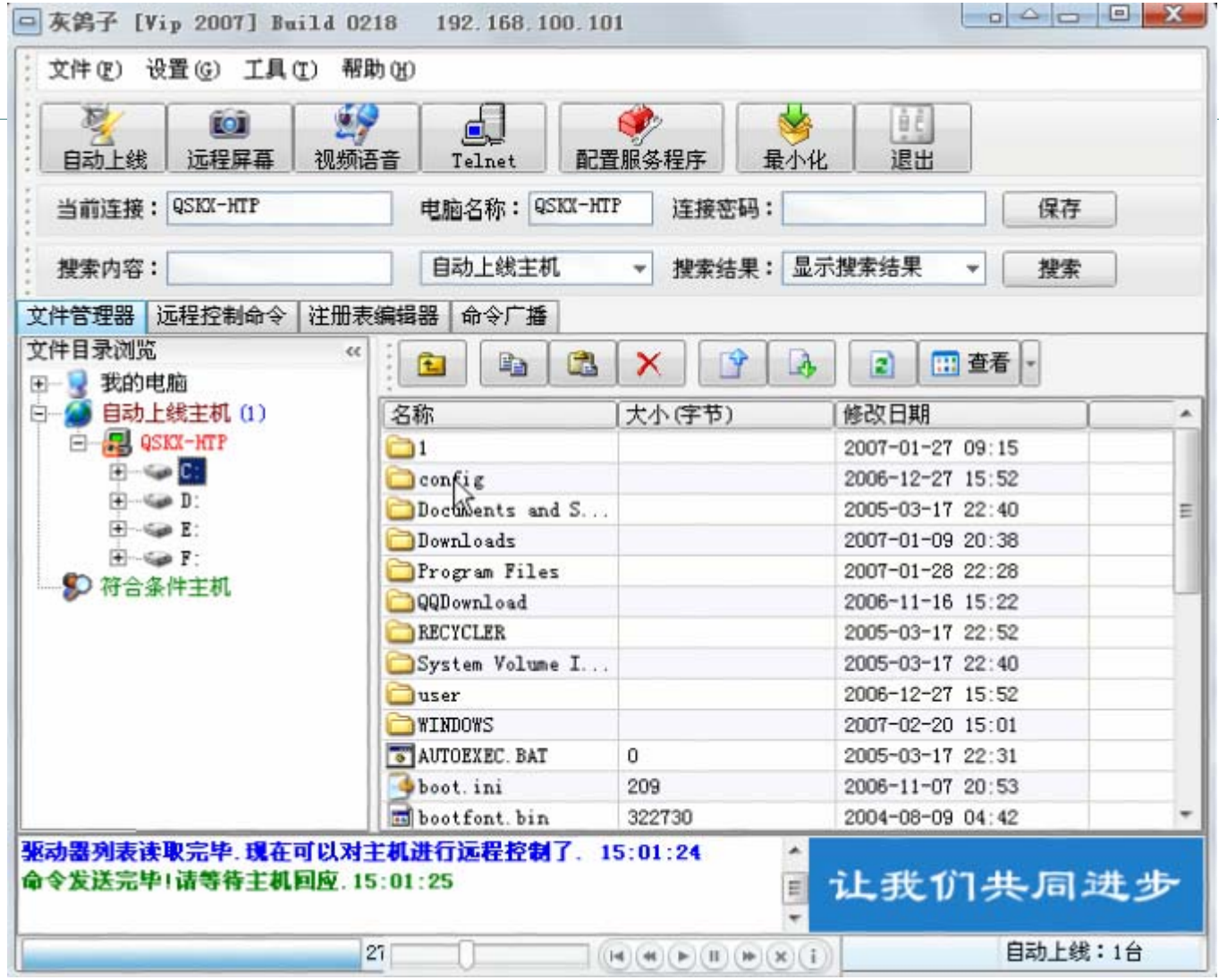
有「肉雞」上線了...



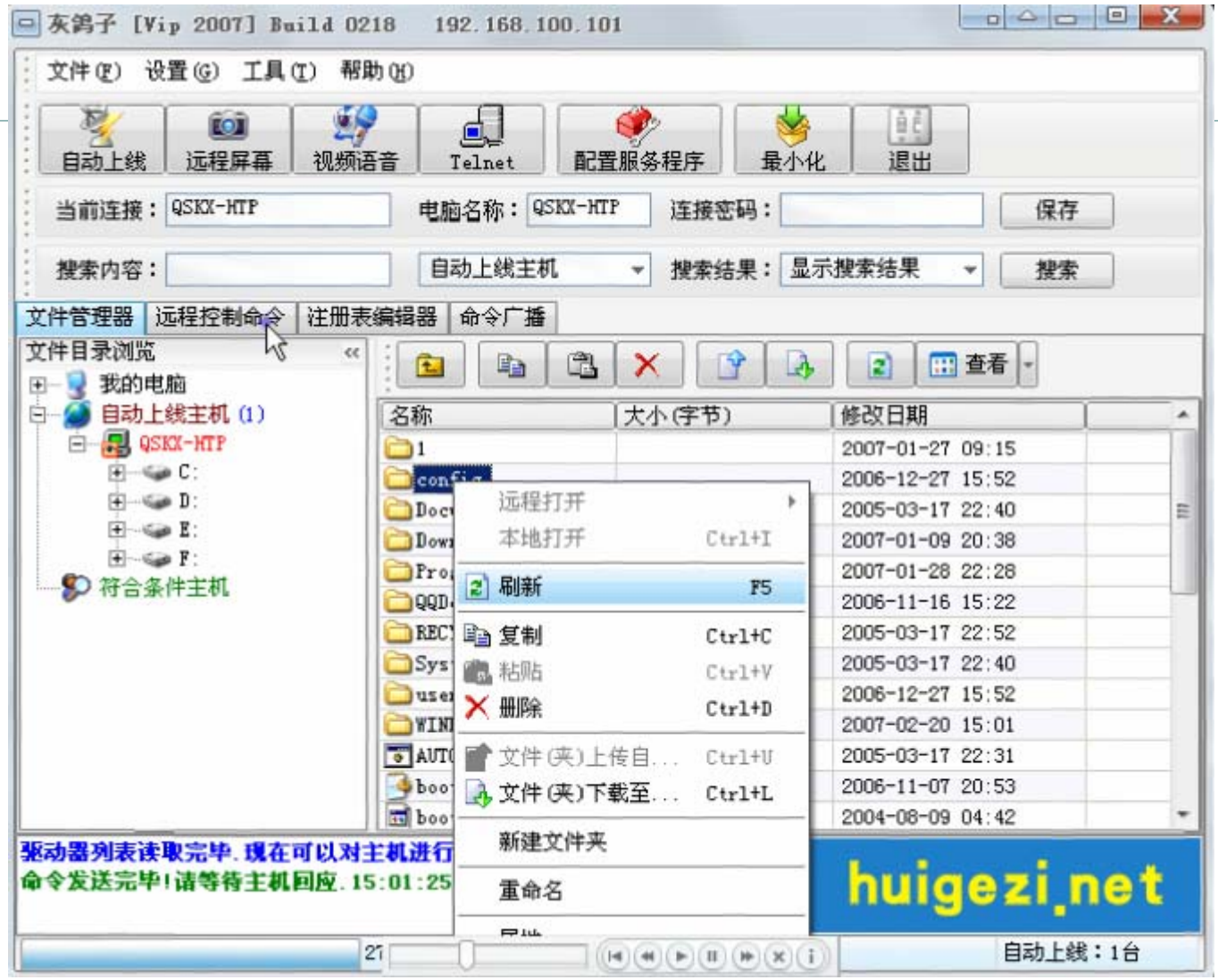
可以瀏覽「肉雞」的電腦目錄...



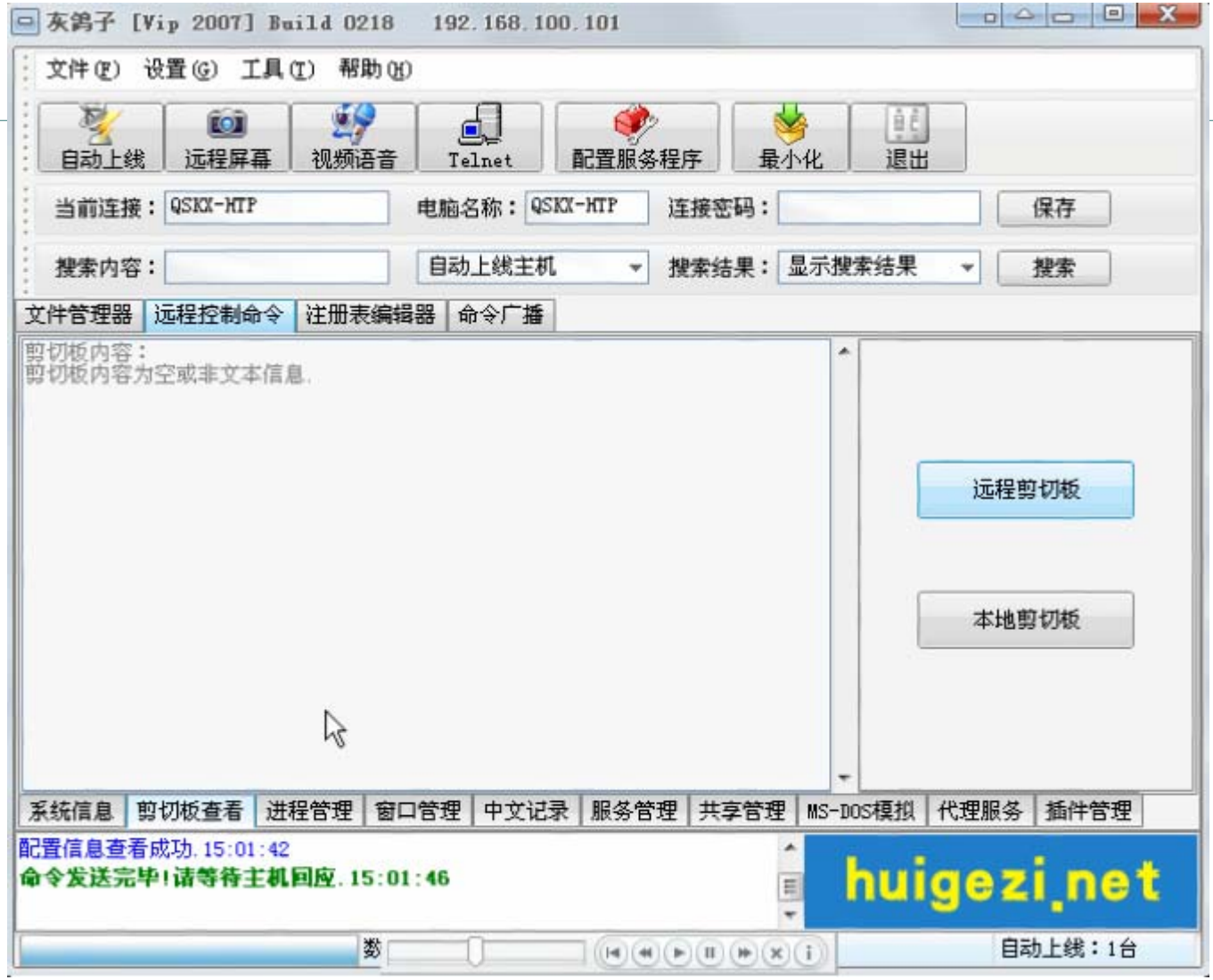
瀏覽電腦目錄內容...



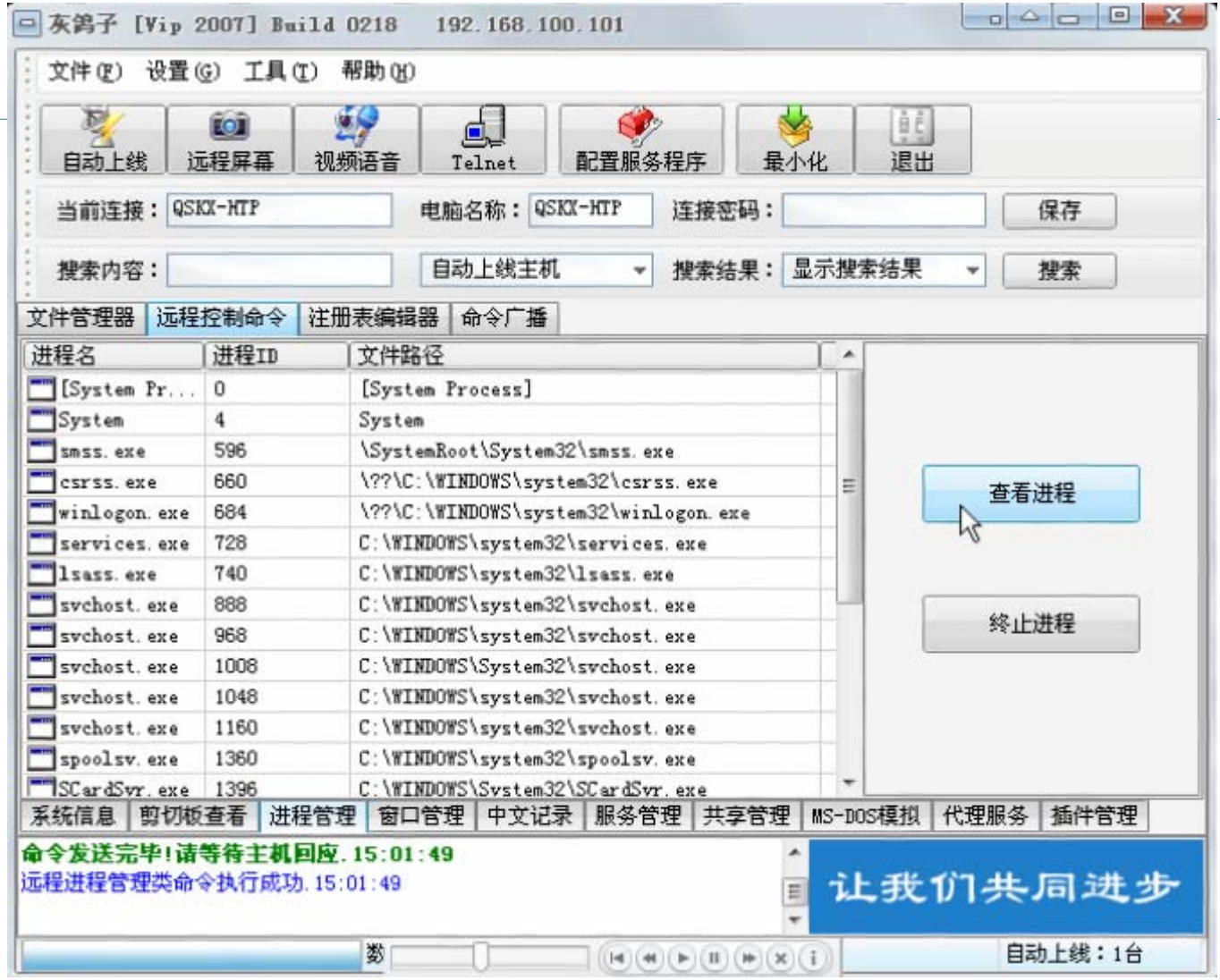
可以對目錄或檔案直接操作...



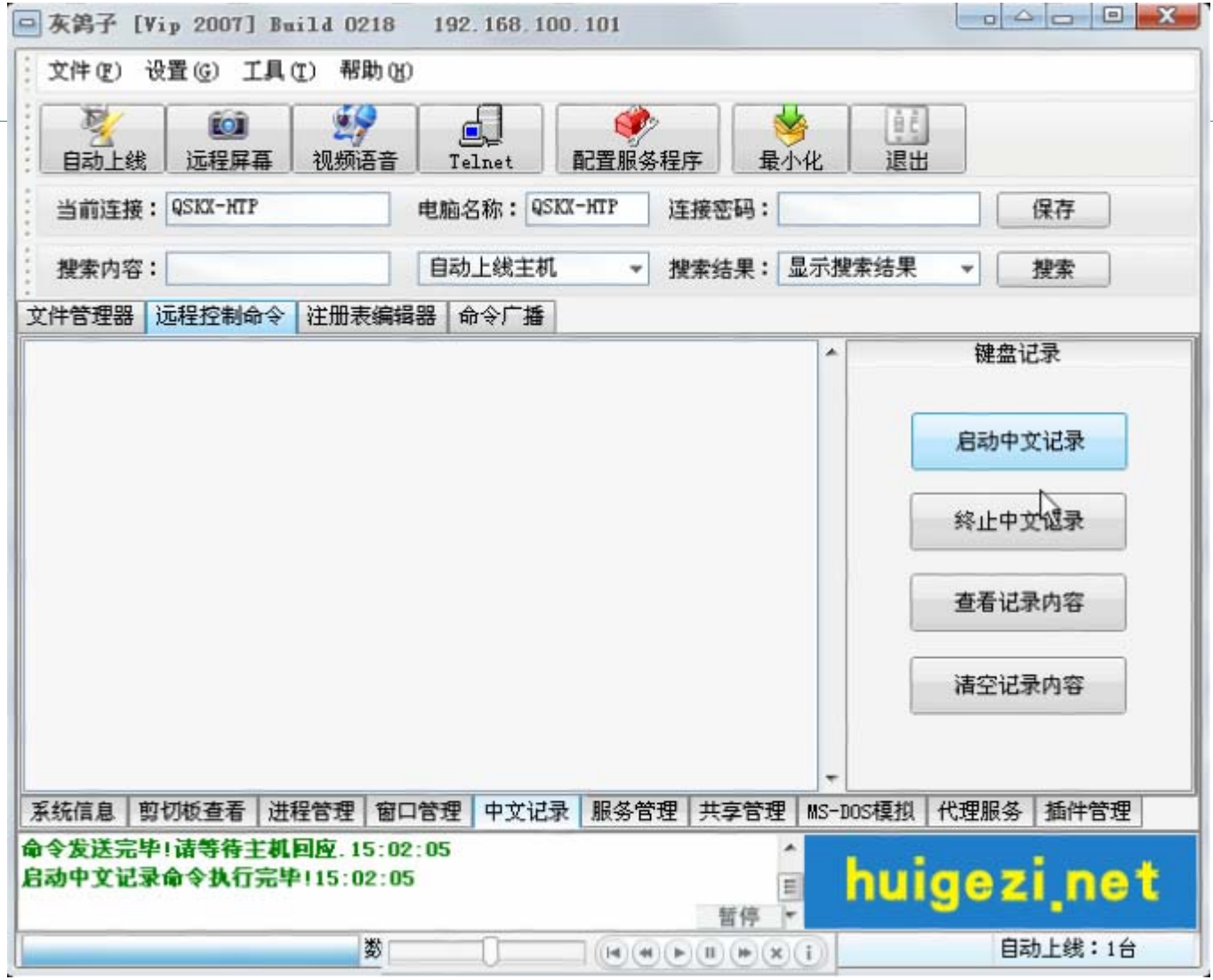
使用本機或遠端剪貼簿...



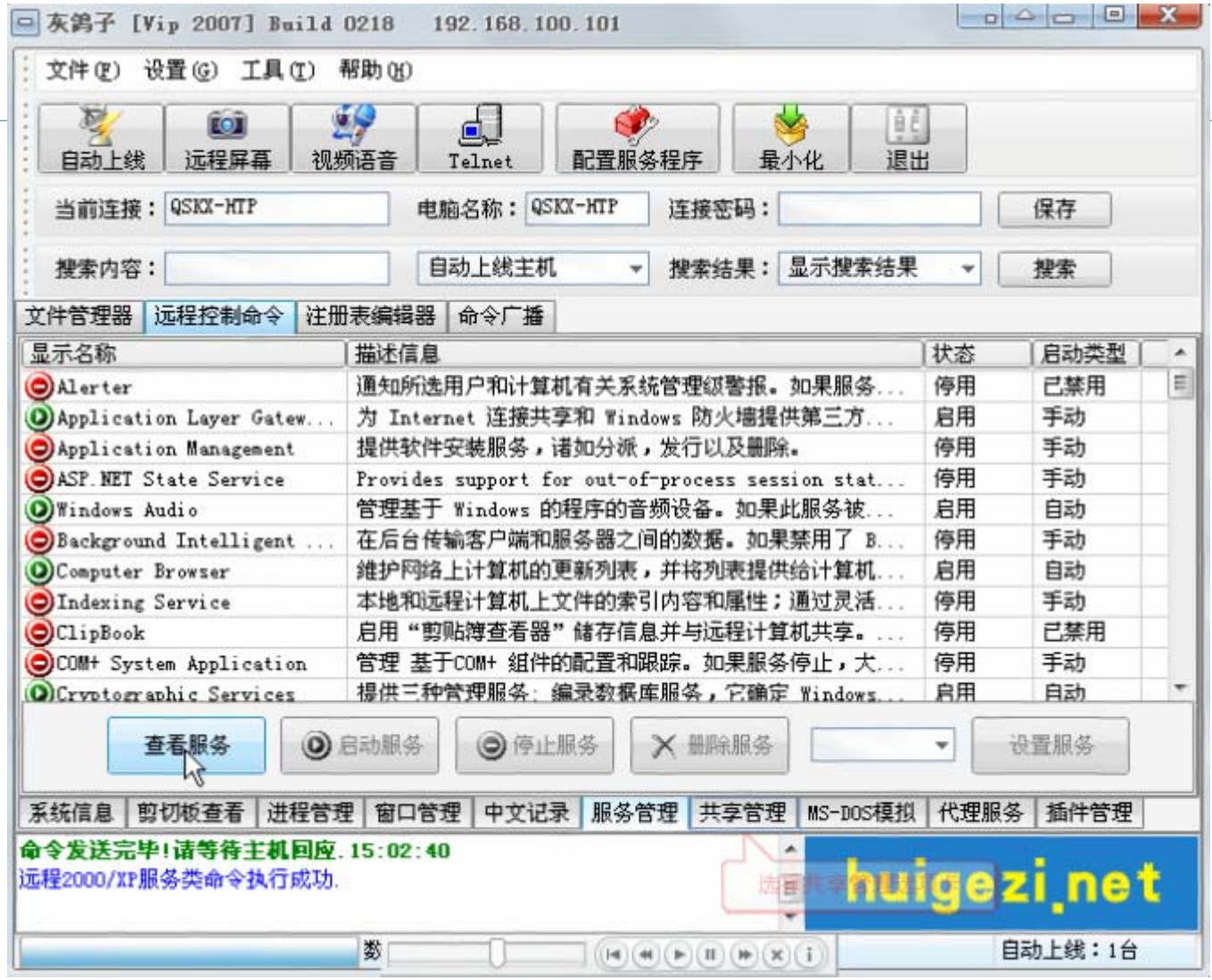
瀏覽執行程序...



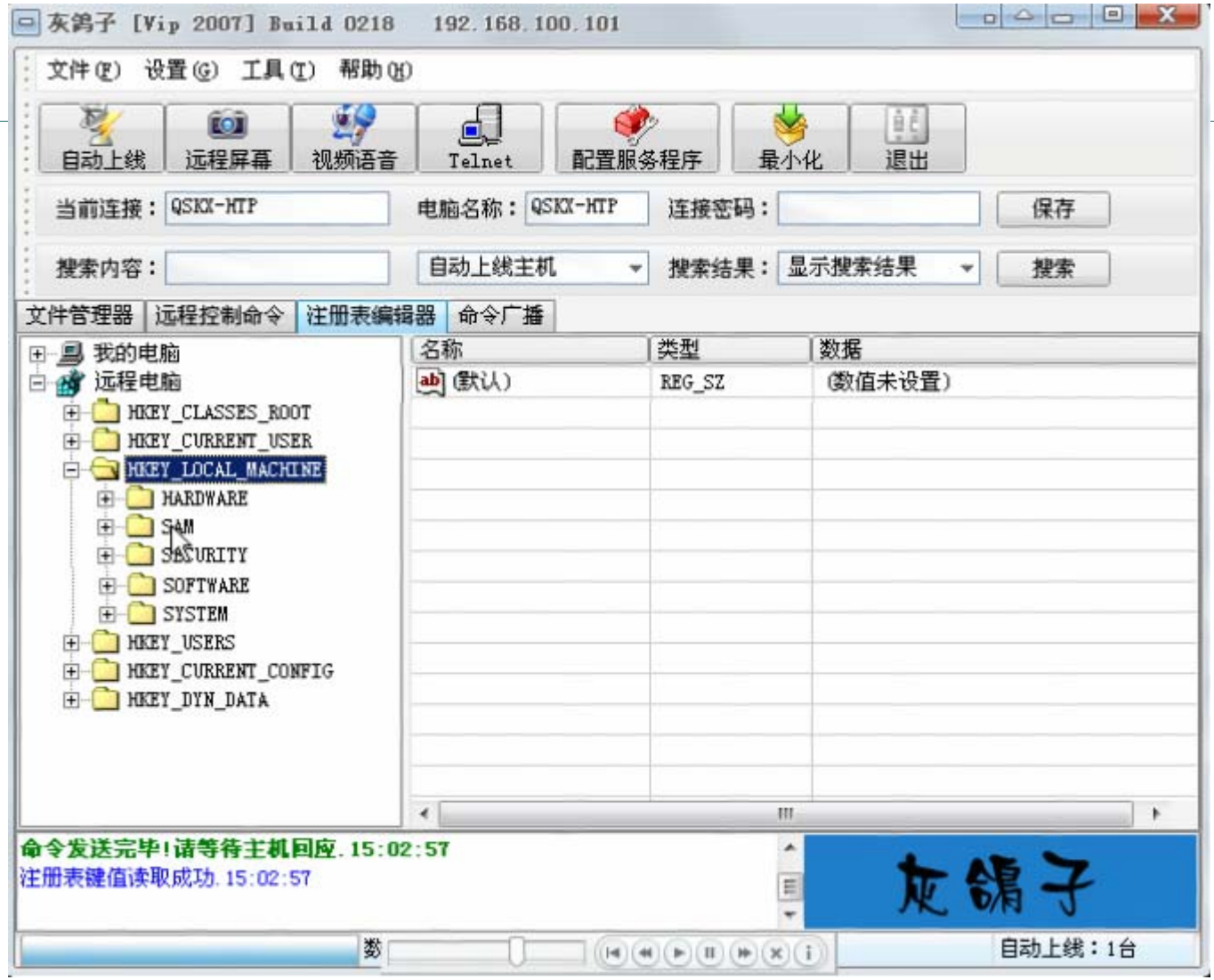
鍵盤操作記錄...



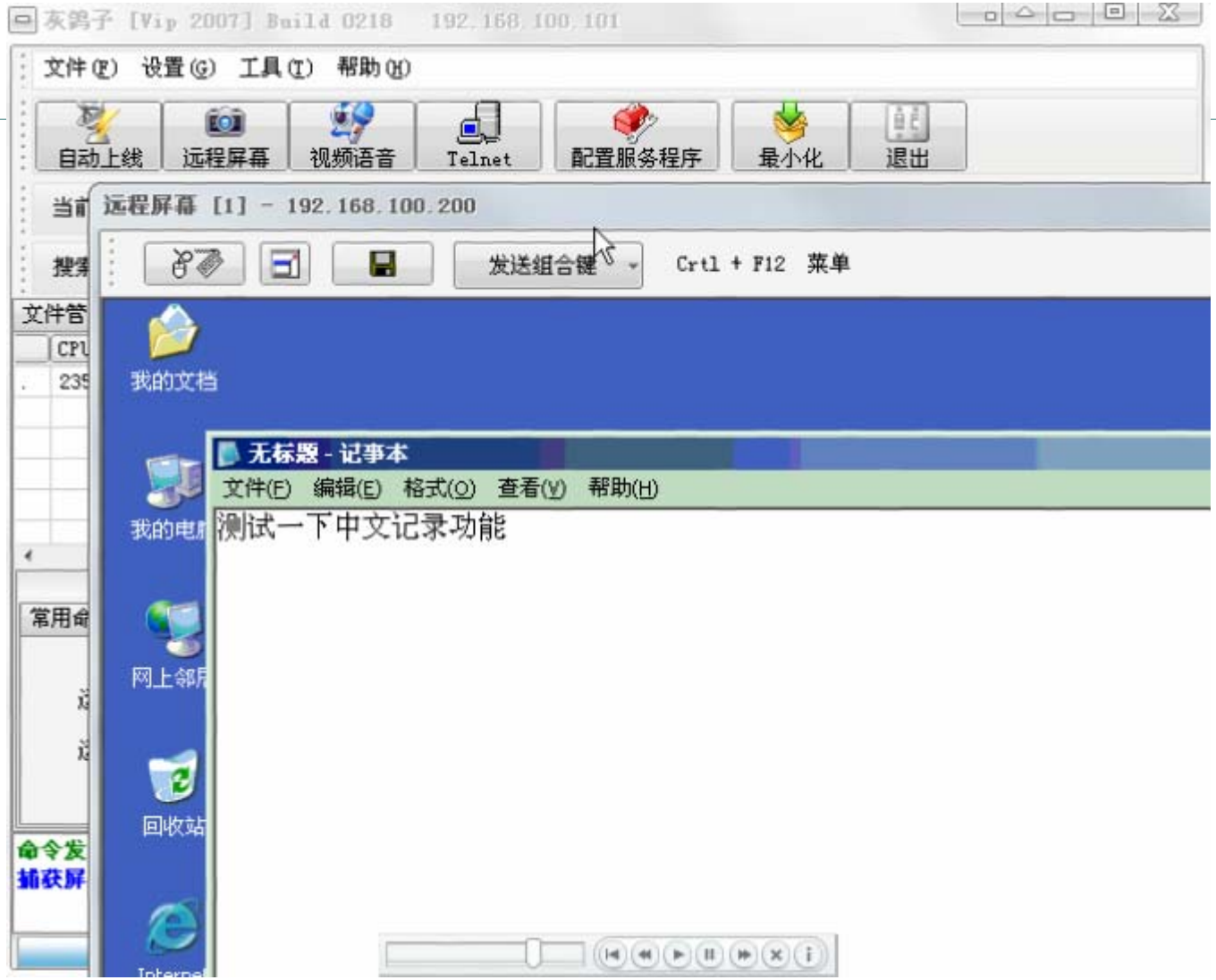
也可以操作服務...



還有機碼...



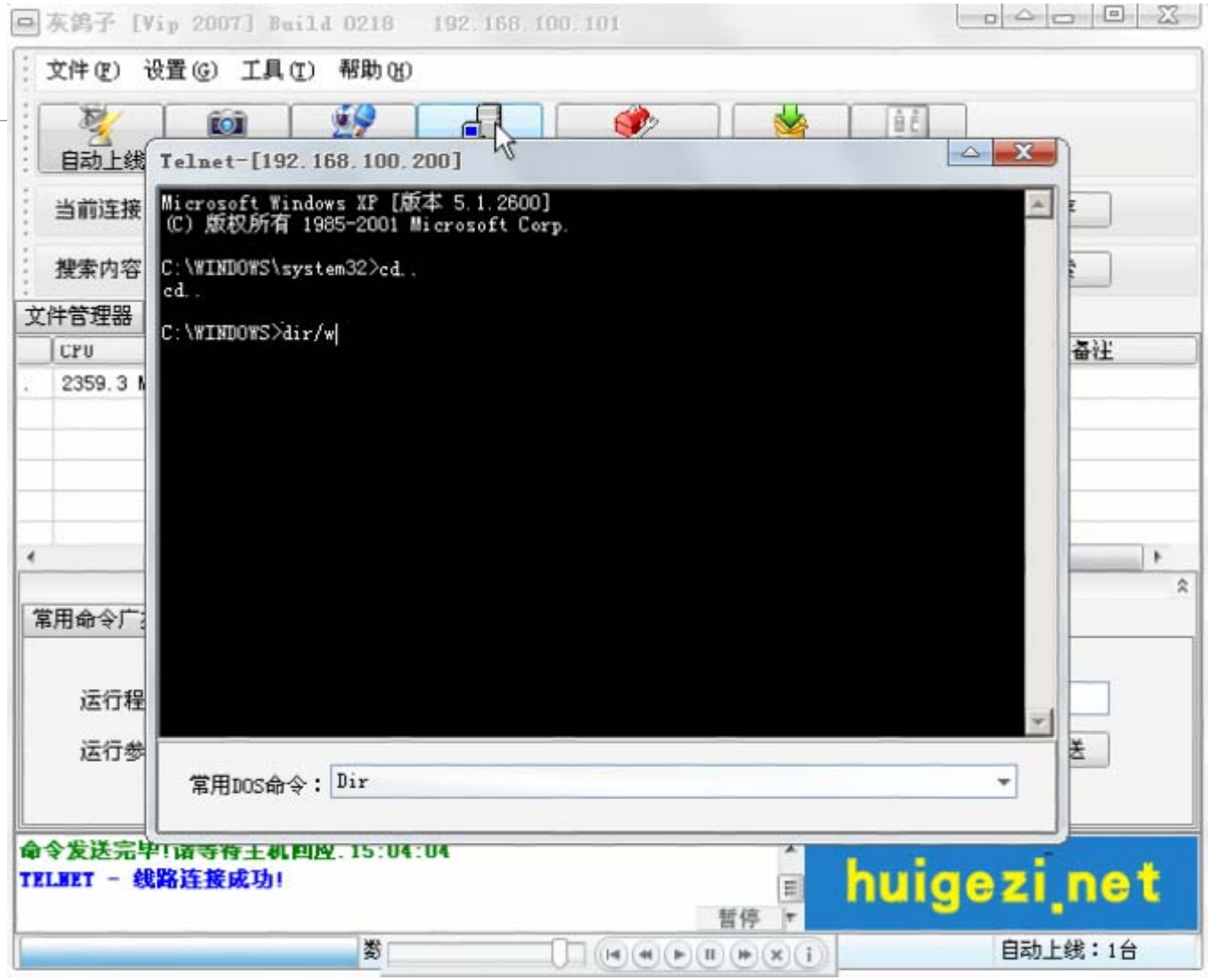
當然也可以遠端窺視畫面...



竟然還可以逕自啟動WebCam...

以及麥克風接收...

也可以Telnet…



灰鴿子工作室

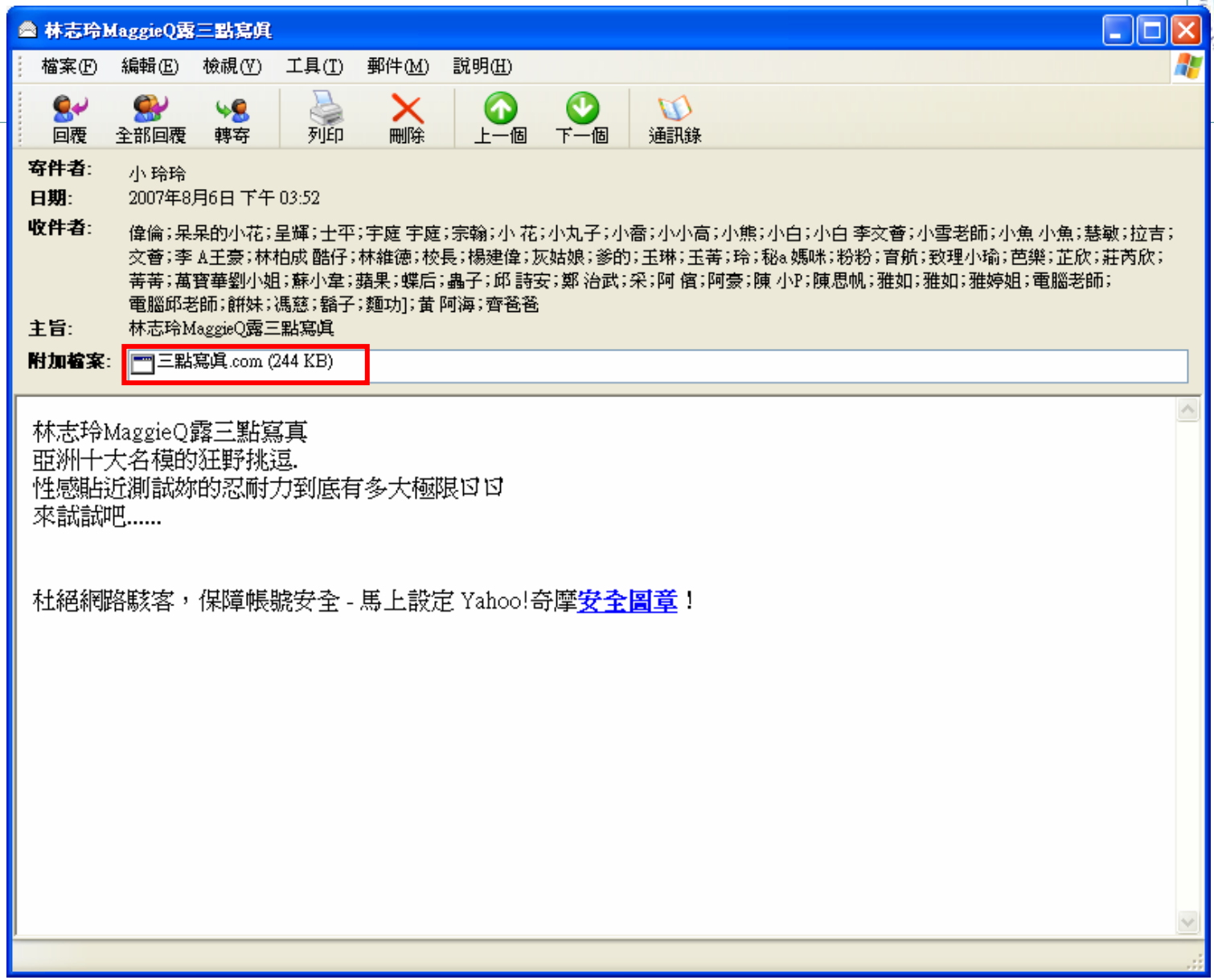
已於2007年3月16日關閉...

- 網路安全概論
- 駭客概述
- 電腦病毒
- 木馬及後門程式
- 常見入侵來源
- 惡意程式防護
- 資料及隱私權保護
- 防範SQL Injection攻擊
- 行動設備安全
- 無線網路安全

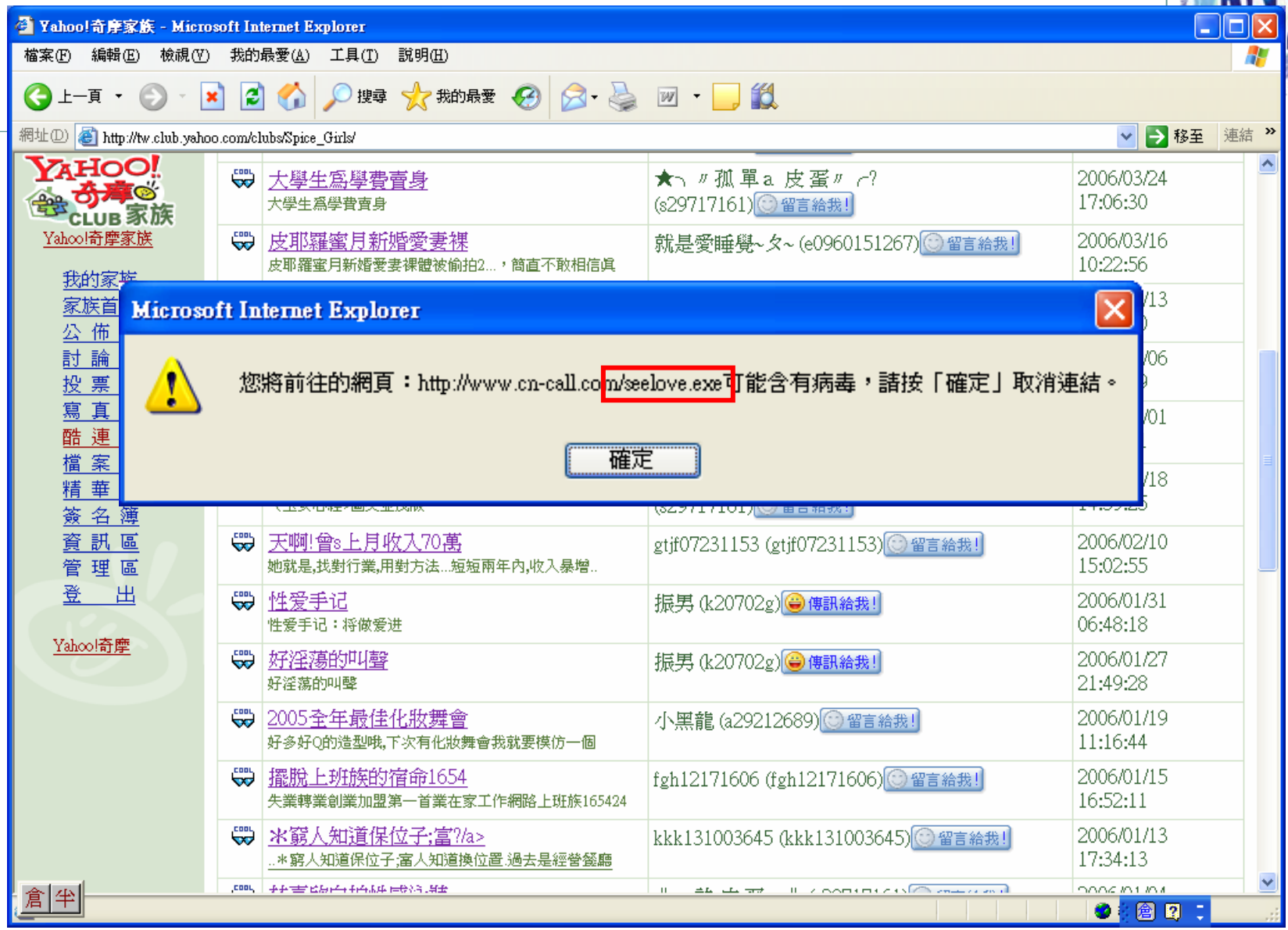
常見入侵來源 (1/2)

- 木馬後門程式的散播
  - 網頁中的惡意程式下載
    - 身材超火辣,有人聊嗎？我有照片哦,還可以激情視屏,更多内容请看http://www.c*-call.com/sixnsy.exe
  - 透過電子郵件
  - 透過即時通
    - 論名專家是根據台灣當前最為流行的判斷名字吉凶的方法編寫的軟體，它可以非常方便地算 ... http://http://dajiawang.w67a.chinan...om/zhiugong.exe

利用色情標題誘騙收件人開啟郵件...



惡意程式執行檔...



常見入侵來源 (2/2)

- 常見的木馬後門程式檔案類型
  - .exe、.scr、.com…
  - 經過轉址後的惡意程式連結

轉譯短網址...

短網址...

- http://www.fdkc.gov.tw/typhoonfiles/images/typ041.jpg
- http://0rz.tw/753cU

- 網路安全概論
- 駭客概述
- 電腦病毒
- 木馬及後門程式
- 常見入侵來源
- **惡意程式防護**
- 資料及隱私權保護
- 防範SQL Injection攻擊
- 行動設備安全
- 無線網路安全

惡意程式

- 對使用者會造成不便的這些不懷好意的程式碼，泛稱為病毒、惡意程式

惡意程式防護 (1/5)

- 主動防禦 (個人)
  - 防毒軟體、防火牆
  - 修補系統漏洞
  - 網路分享檔案權限要設定只需使用的權限
  - 使用防間諜軟體
  - 正確的密碼使用觀念
  - 定期更新防止惡意軟體入侵的知識
    - 注意重大資安事件的發佈

惡意程式防護 (2/5)

- 正確的防範認知 (個人)
  - 防範網路釣魚
    - 不明郵件、不明連結...
  - 防範ActiveX惡意程式

惡意程式防護 (3/5)

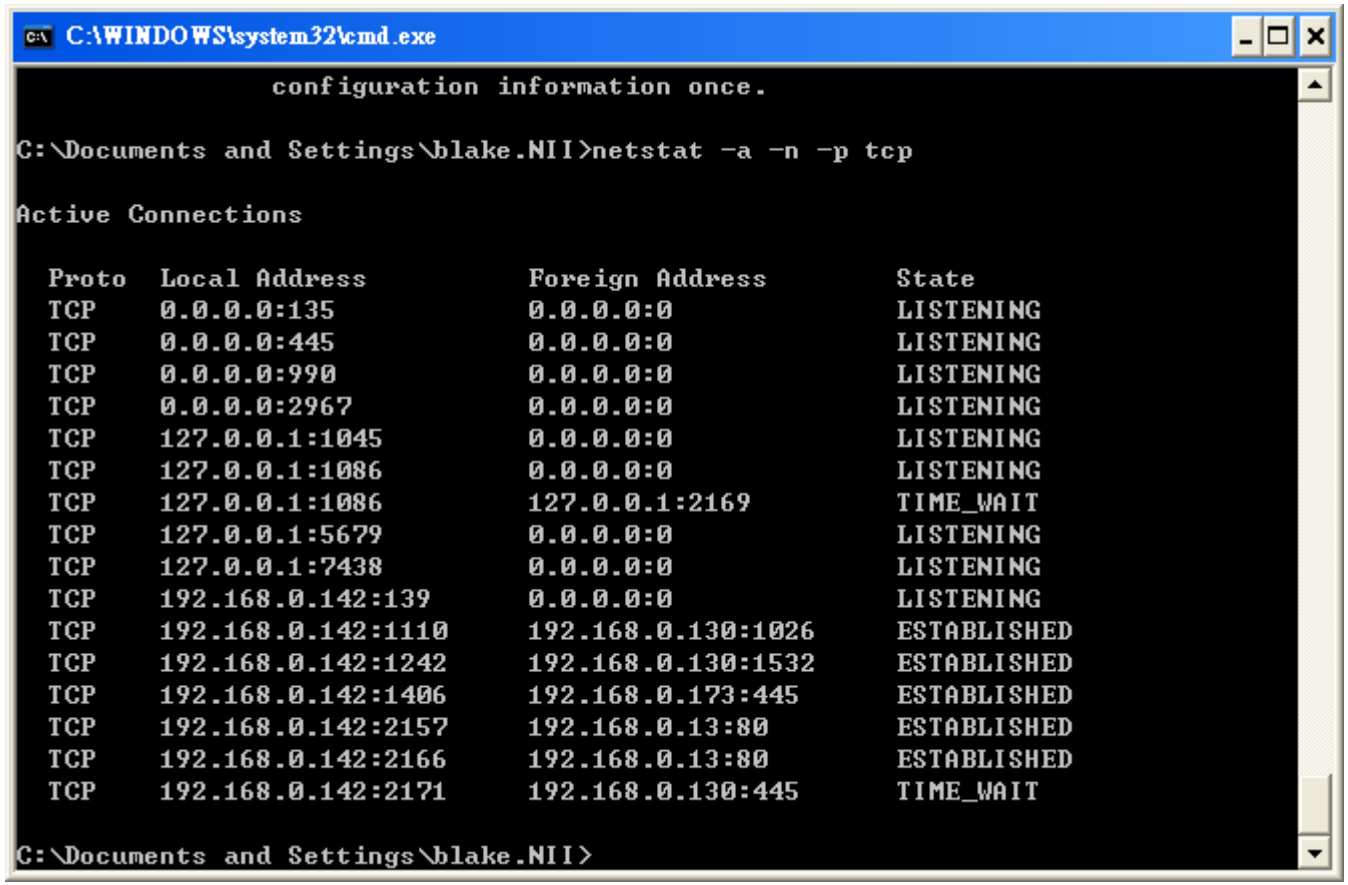
- 主動防禦 (管理)
  - 駭客之所以能入侵網站，通常都是網站的伺服器設定上出現漏洞，或是修補程式沒有安裝，使得駭客入侵取得了控制權限，進而竄改網頁、 加入惡意連結
  - 網站管理者平時在進行維護工作時，必須要加留意是否出現漏洞，仔細檢查是否有不該存在的對外連結，才能及早發現是否有惡意程式植入

惡意程式防護 (4/5)

- 主動防禦 (管理) (續)
  - 任何防毒措施，都是在攻擊出來之後，才會有相對的解決方案，期間還是可能讓駭客有可趁之機
  - 由於網站用的伺服器其實工作項目很單純，最好的防護方法可以用「鎖定」的方式進行主機系統防護
    - 列出來這台伺服器能做哪些事情，只要不是允許的項目，全部不能做

惡意程式防護 (5/5)

- 偵測惡意程式
  - 檢查是否有異常連線
    - 關閉所有已知對外連線程式，在確定網路沒有正常對外連線情況下，在DOS模式下，輸入利用「netstat -a -n -p tcp」指令清查異常對外通訊的應用程式，檢查是否有異常連線



- 網路安全概論
- 駭客概述
- 電腦病毒
- 木馬及後門程式
- 常見入侵來源
- 惡意程式防護
- 資料及隱私權保護
- 防範SQL Injection攻擊
- 行動設備安全
- 無線網路安全

資料及隱私權保護

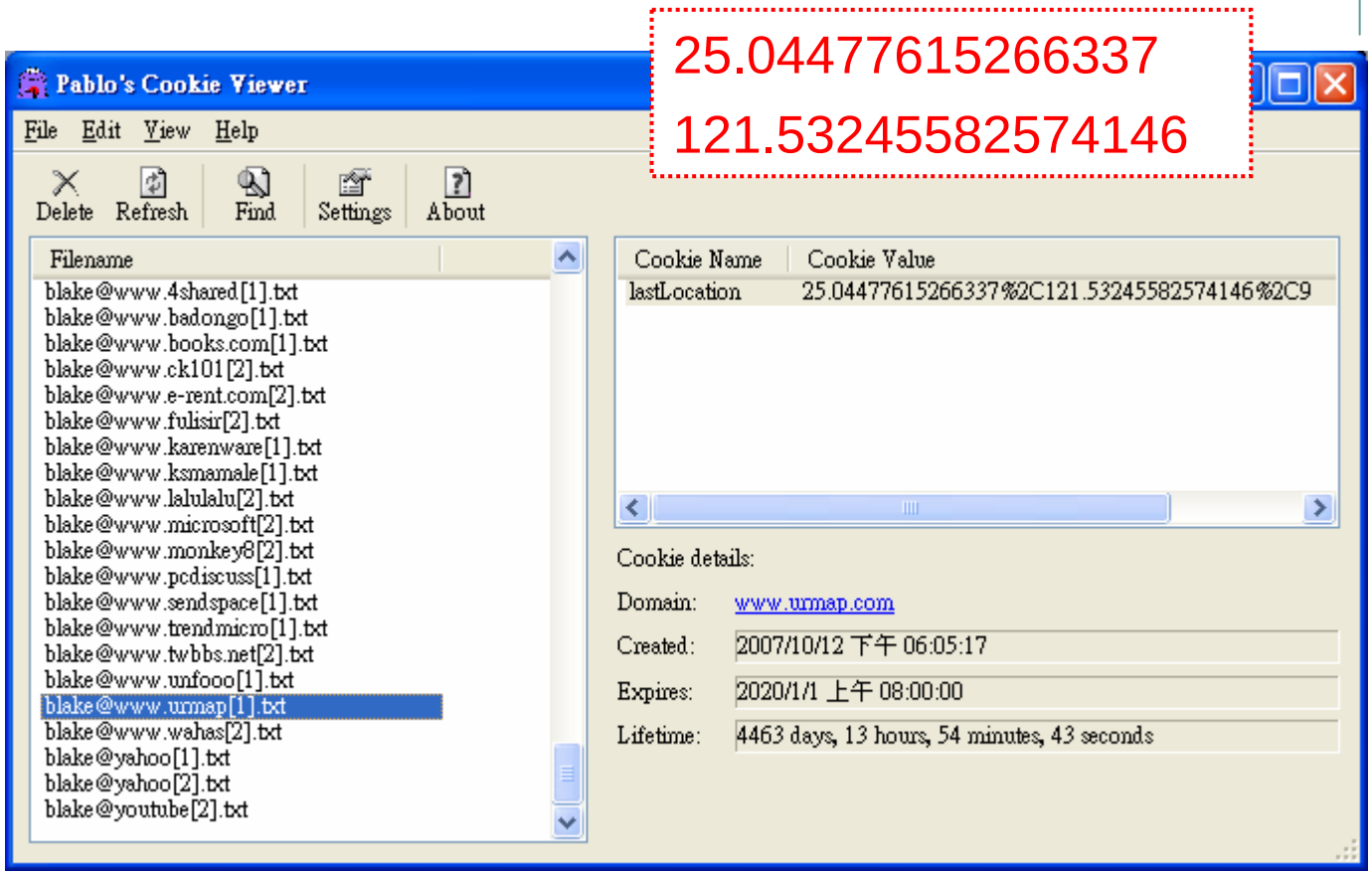
- 小心網路釣魚與詐騙網站
- 慎防cookie遭濫用
- 關於免費網路空間的使用
- 安全密碼保護

Cookies說明

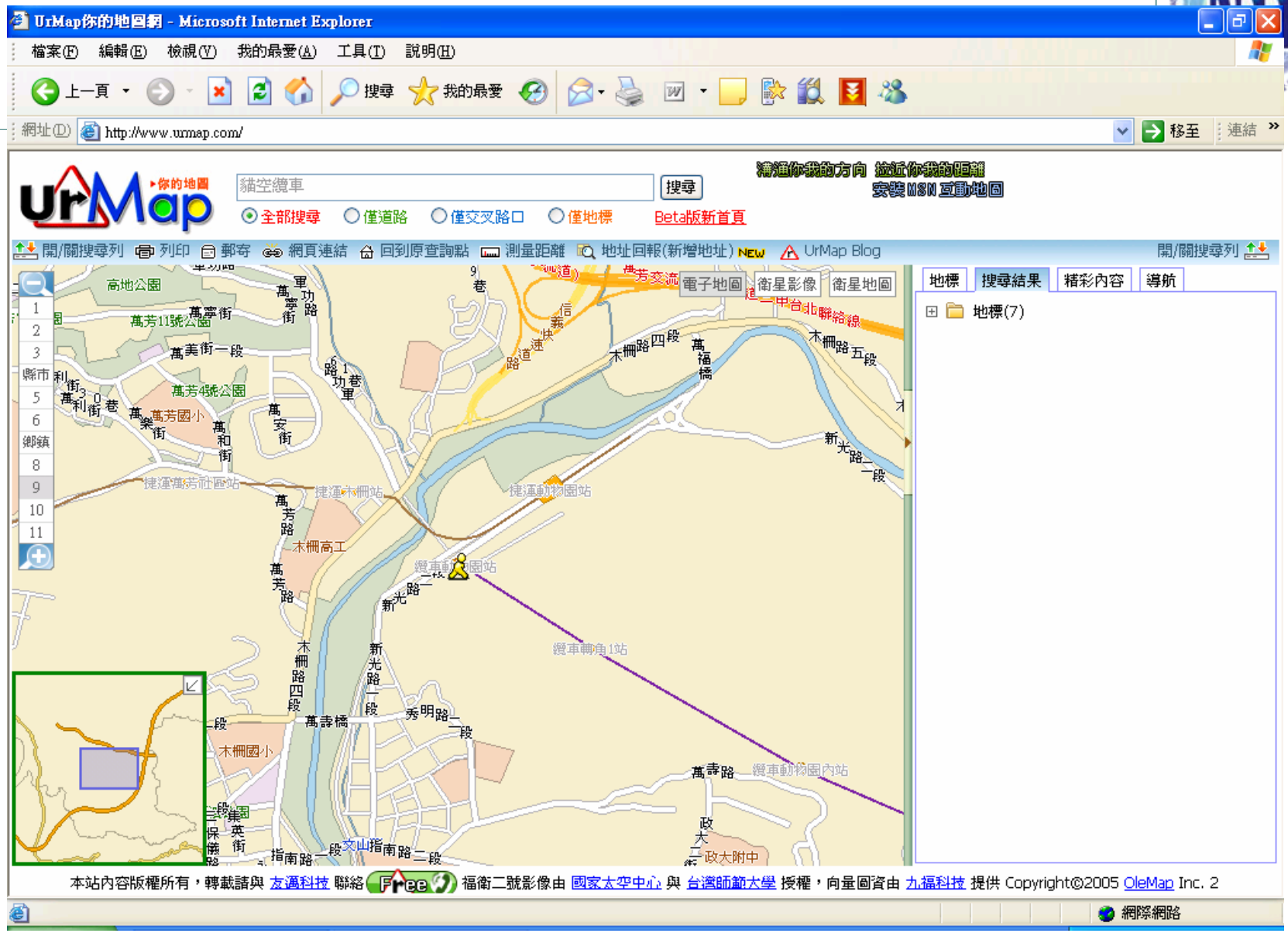
- 何謂Cookies
  - Cookies是存在瀏覽器中的小型文字檔，記錄使用者瀏覽網頁的資訊，例如瀏覽的網站位址、使用者曾經輸入的資訊等，當使用者下次再度使用瀏覽器時，電腦能自動顯示最近使用過的網頁
  - cookie也能紀錄使用者的帳號與密碼，因此在使用者再次進入相同頁面時，可以不需要重新輸入名稱與密碼

Cookie確實能顯示您的使用資訊...

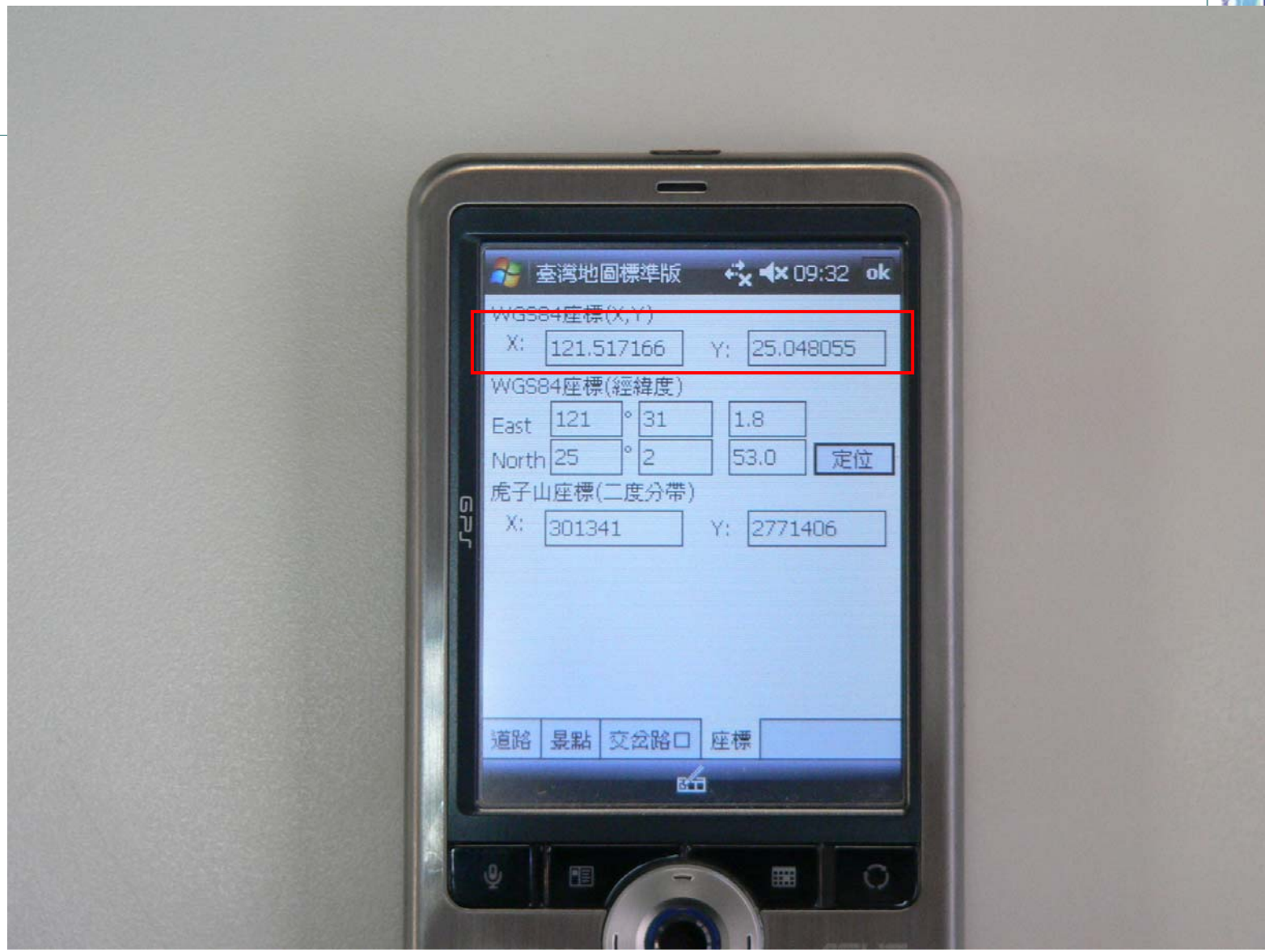
瀏覽Cookie的軟體…



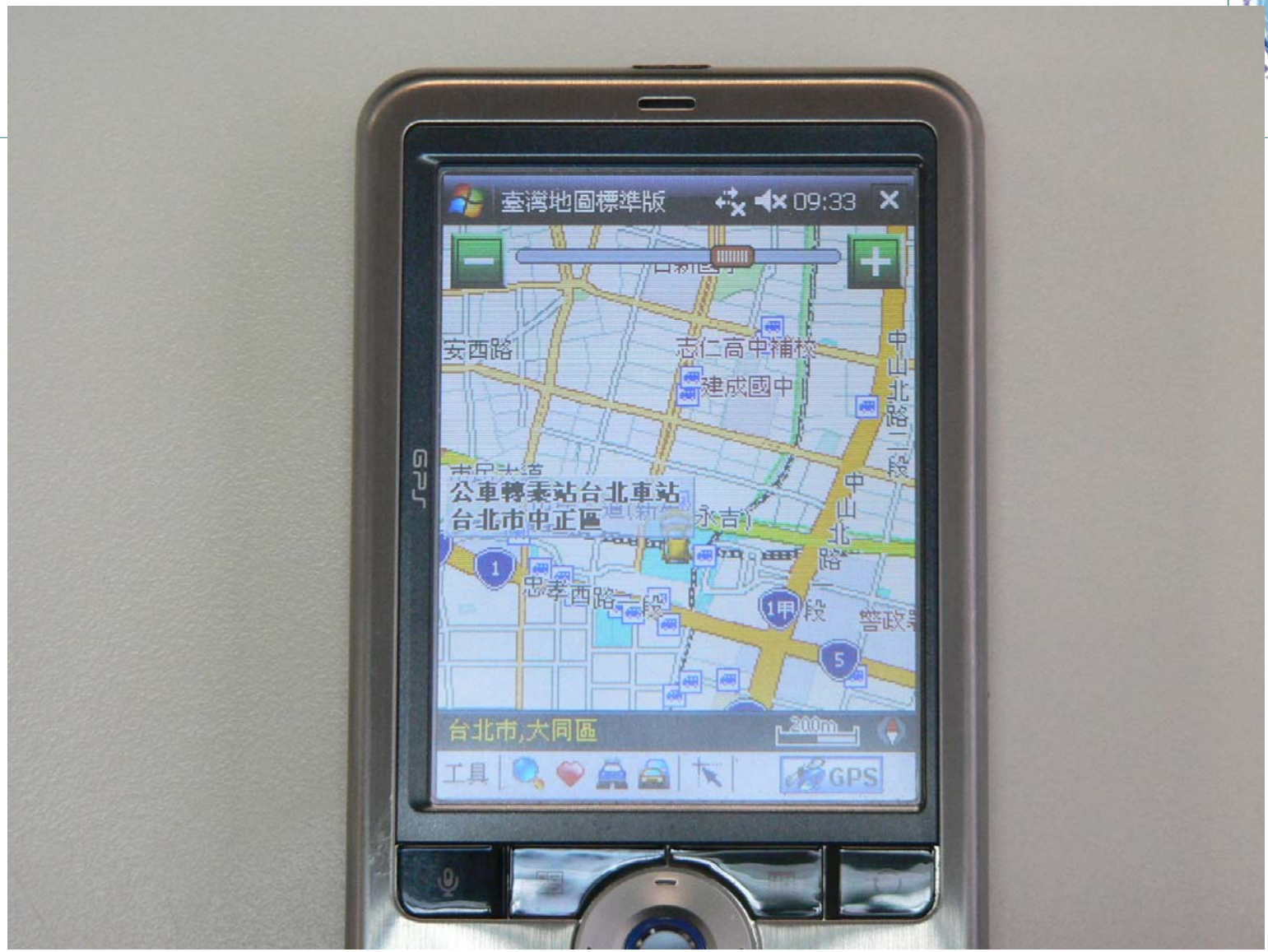
UrMap是一個電子地圖瀏覽網站...



輸入Cookie的資訊作查詢...

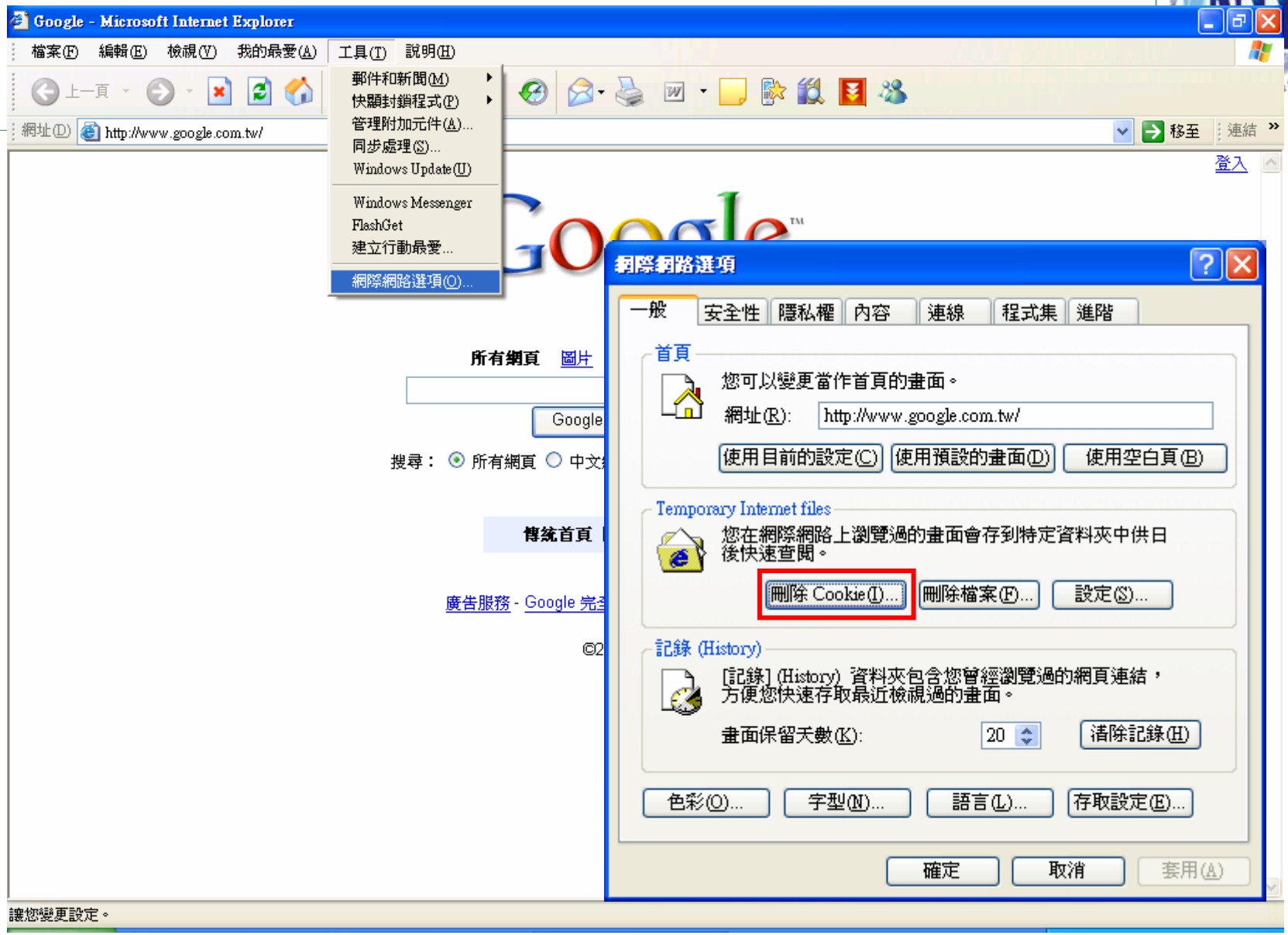


獲知使用者所查詢的資料...

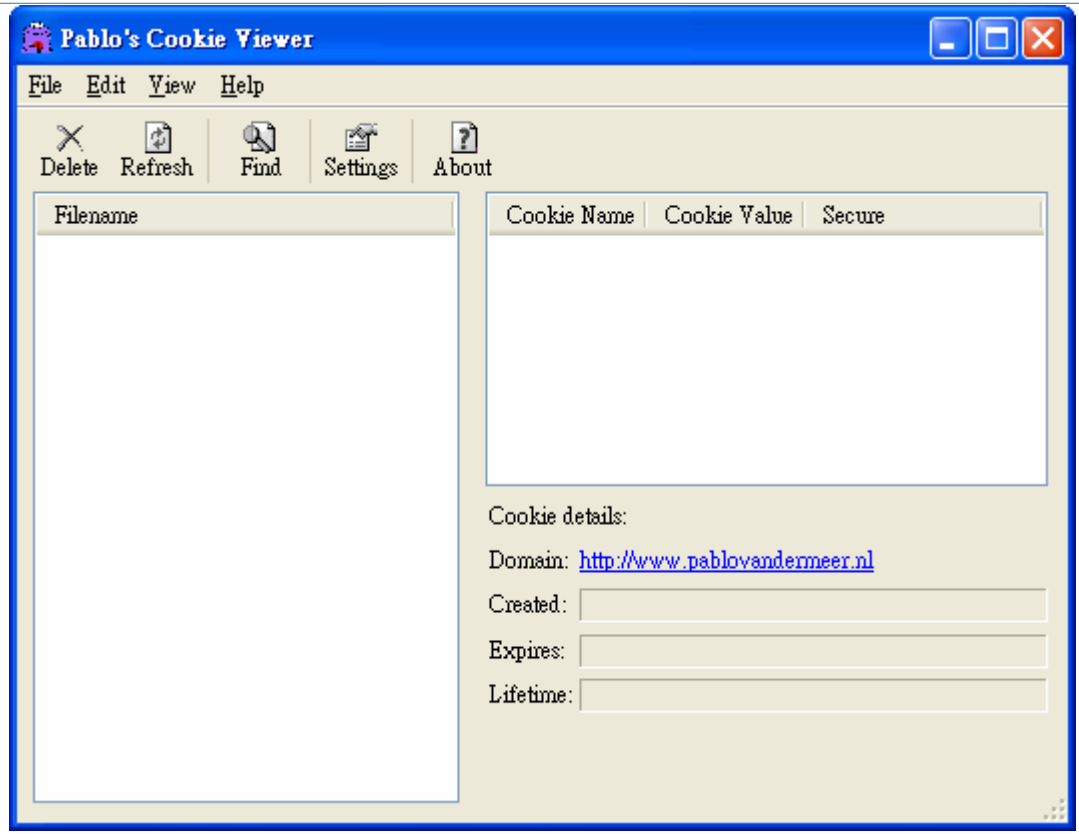


適時地清除Cookie…

刪除Cookie…



已無Cookie記錄…

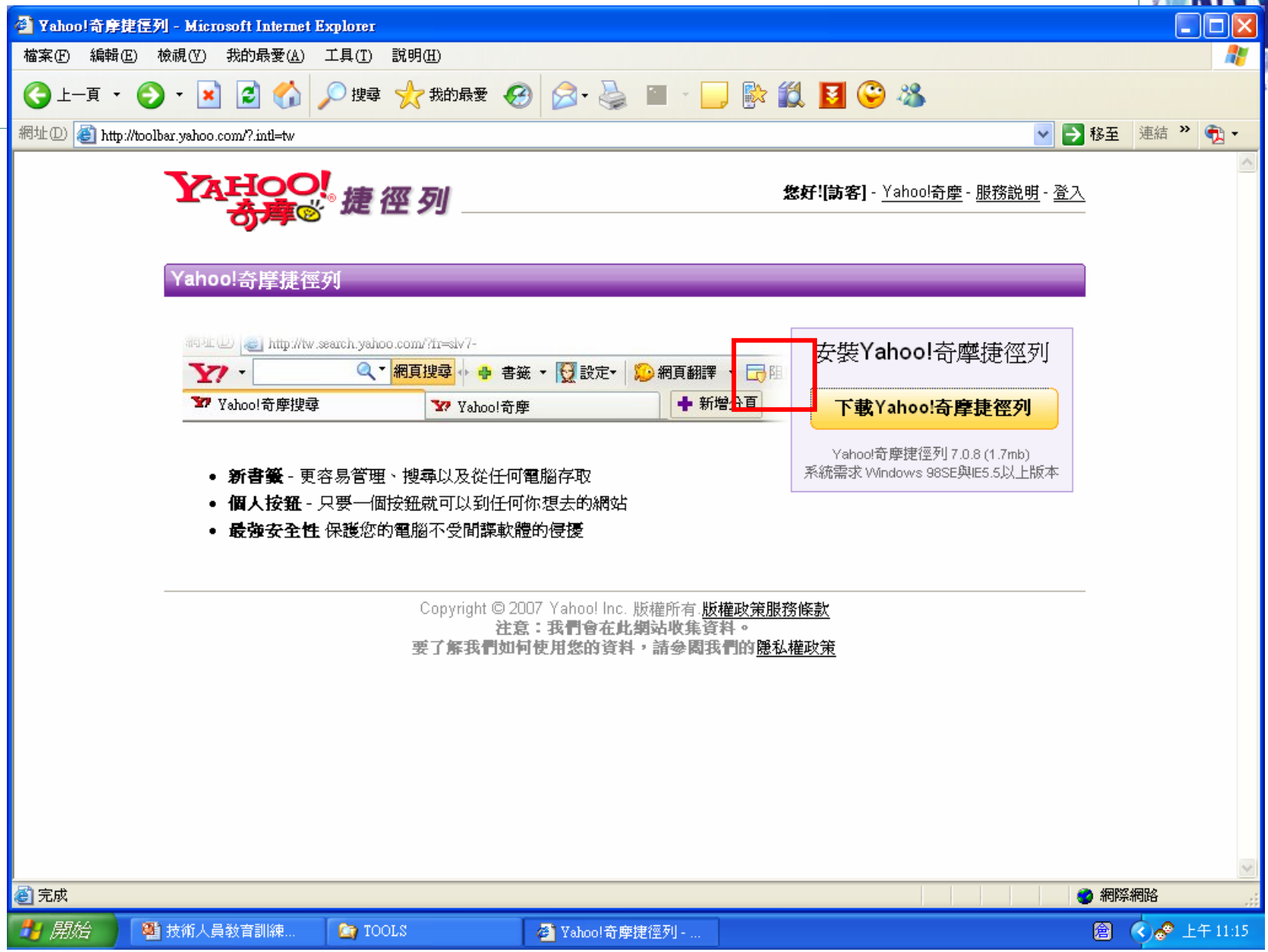


防範間諜軟體與廣告軟體

- 檢查電腦是否有間諜軟體或廣告軟體
- 使用反間諜或反廣告軟體
- 免費的瀏覽器工具列
- 防範遭植入間諜或廣告軟體
  - 安裝軟體前詳閱使用者同意書
  - 不隨意安裝軟體
  - 不隨便同意網站安裝程式

Google工具列…

Yahoo捷徑列…



- 安裝軟體前詳閱使用者同意書
  - 安裝免費軟體時，冗長的使用者條款可能會加註另外安裝廣告軟體之說明，通常使用者都不看條款而直接按下「我同意」或「確認」鍵
- 不隨便同意網站安裝程式
  - 連結該網站時會彈出一個對話方塊，要求安裝 ActiveX 物件

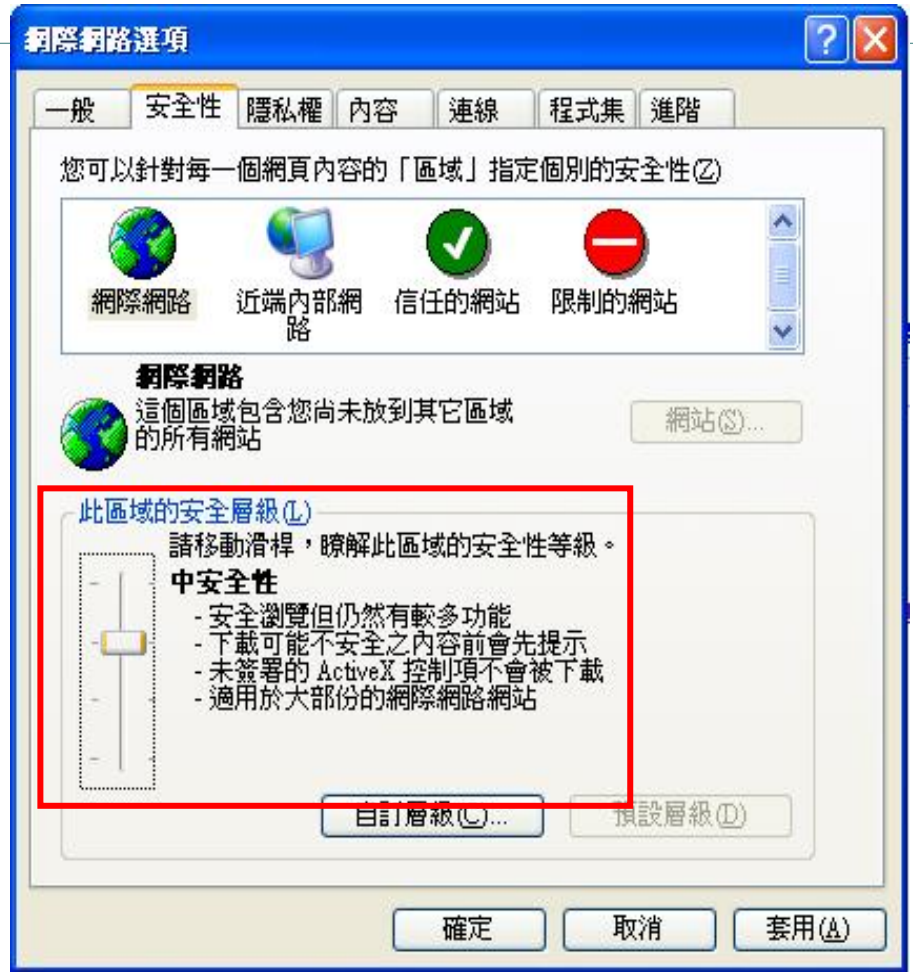
間諜/廣告軟體如何進入電腦

- 間諜軟體通常隨同網路上免費下載的程式軟體
  - 免費工具軟體
  - 免費下載的螢幕保護程式

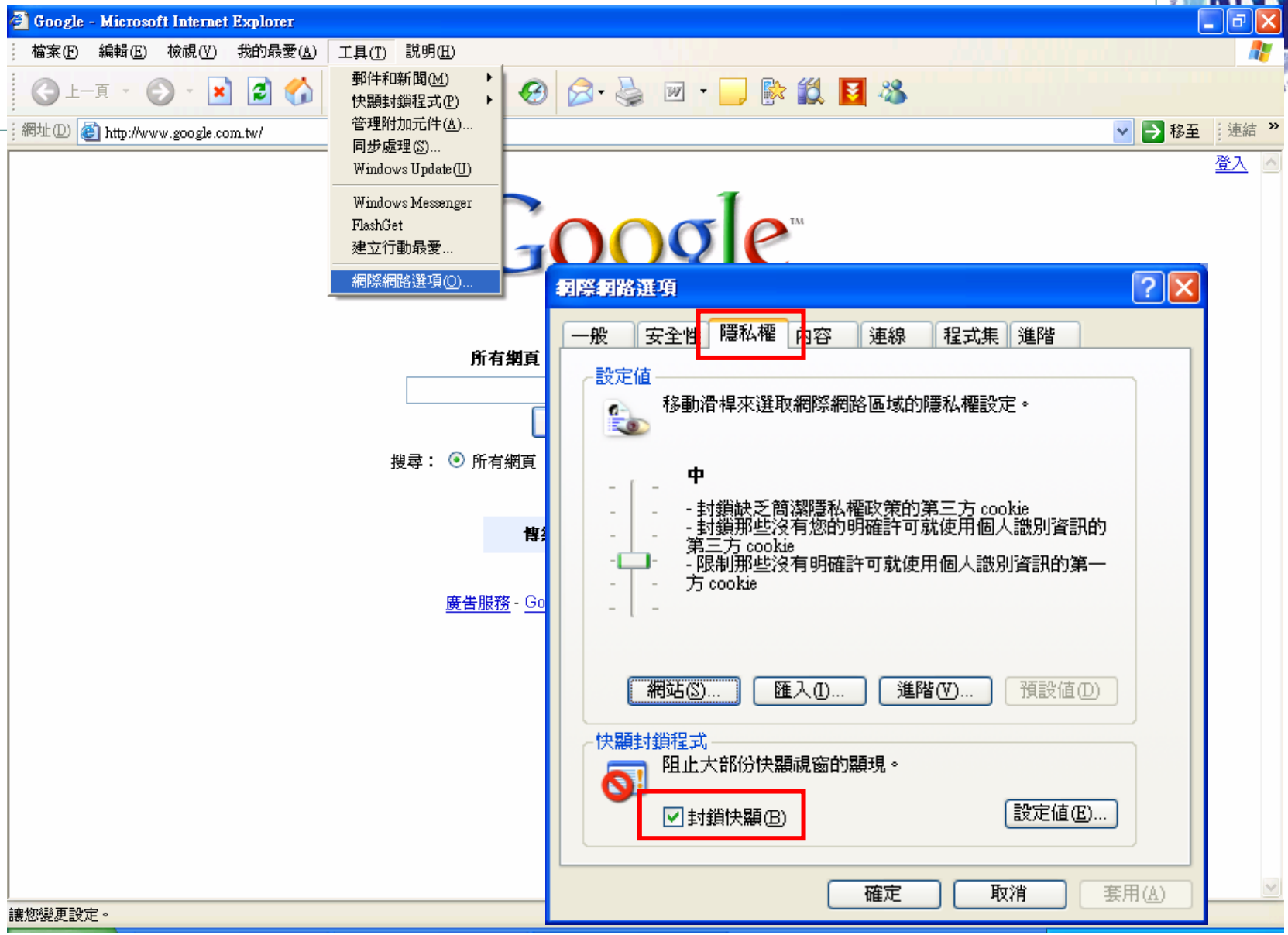
檢查電腦是否有間諜/廣告軟體

- 接連不斷出現的彈跳視窗廣告
- 首頁被劫持，無論輸入哪個網址，都只連結某頁面
- 瀏覽器上方出現新的、不是自己安裝的工具列
- 電腦螢幕右下方出現未知的圖示
- 螢幕上隨機出現的錯誤訊息

設定瀏覽器的安全等級至少「中級」



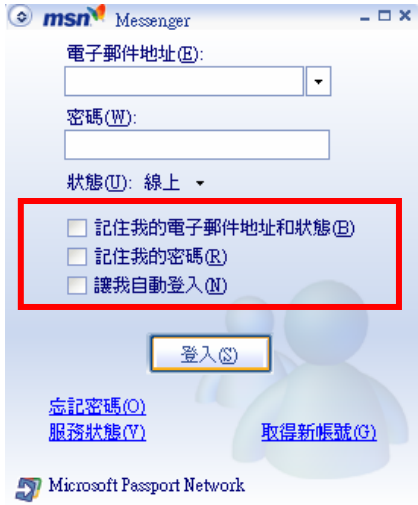
瀏覽器是否有開啟封鎖快顯視窗...



點選彈跳廣告視窗內的超連結與按鍵，
使用視窗右上角的X記號關閉視窗！

登入網路服務的保護

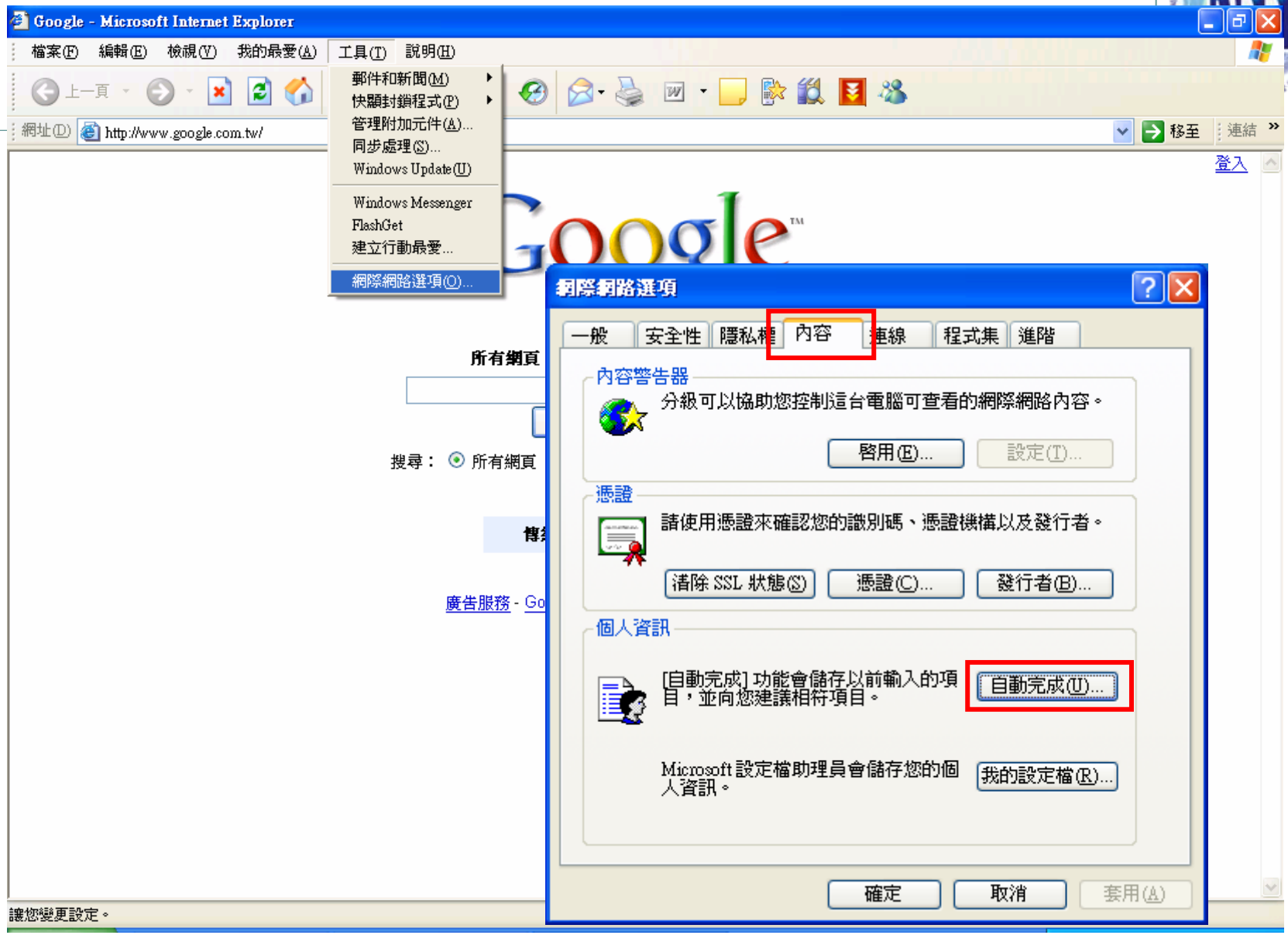
- 使用公共電腦時，避免勾選任何記住帳號或密碼的功能



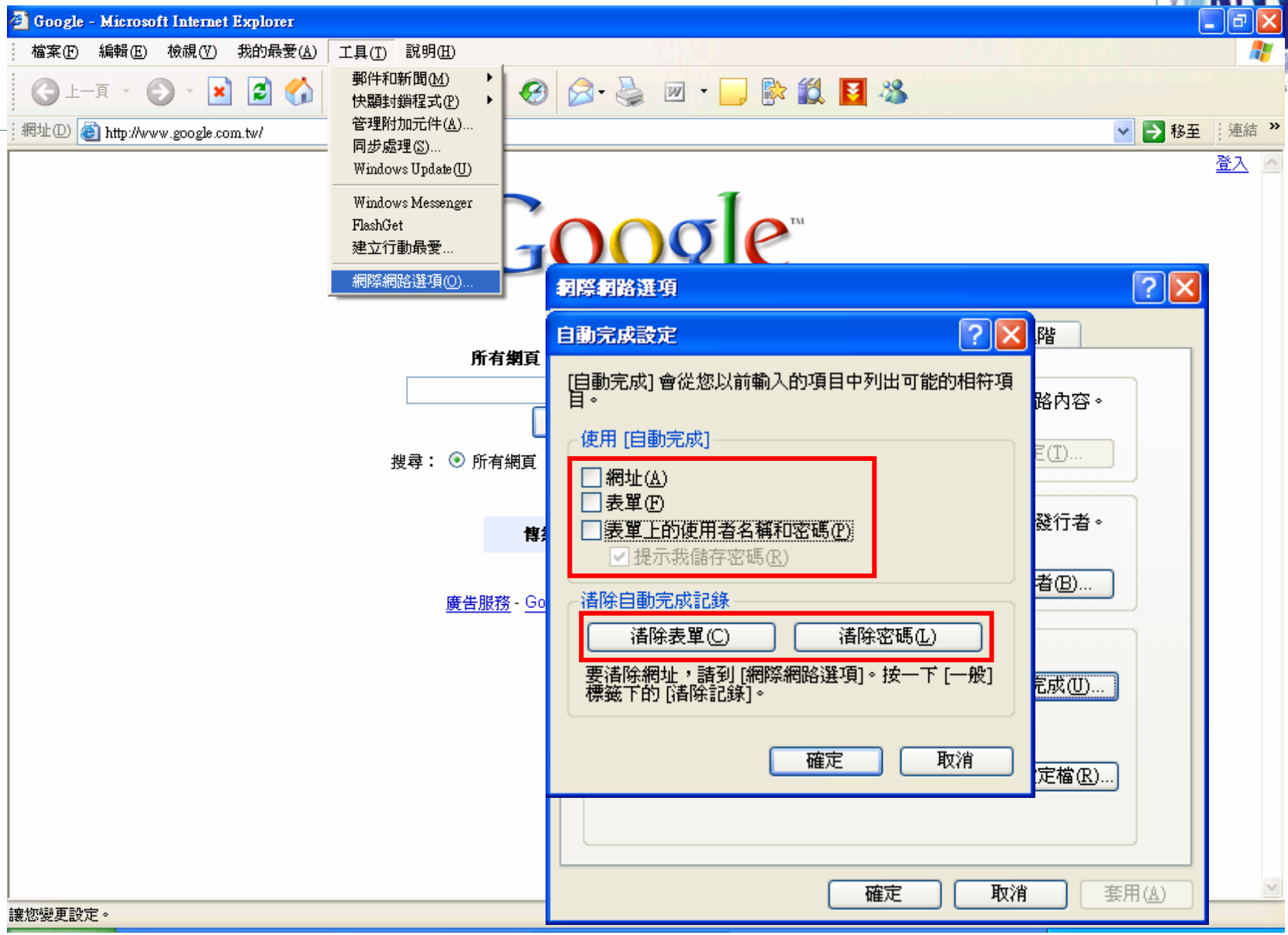
清除電腦上所留的登入資料

- 以使用Internet Explorer瀏覽器為例
  - Internet Explorer中提供了「自動完成」功能，該功能主要是方便使用者記住曾經在瀏覽器中輸入先前輸入的網址、表單及密碼等訊息。使用者可以調整「自動完成」之設定內容，包括只儲存想要存的資訊，或者根本就不使用該功能
  - 也可清除已經保留的記錄

清除電腦上所留的登入資料...



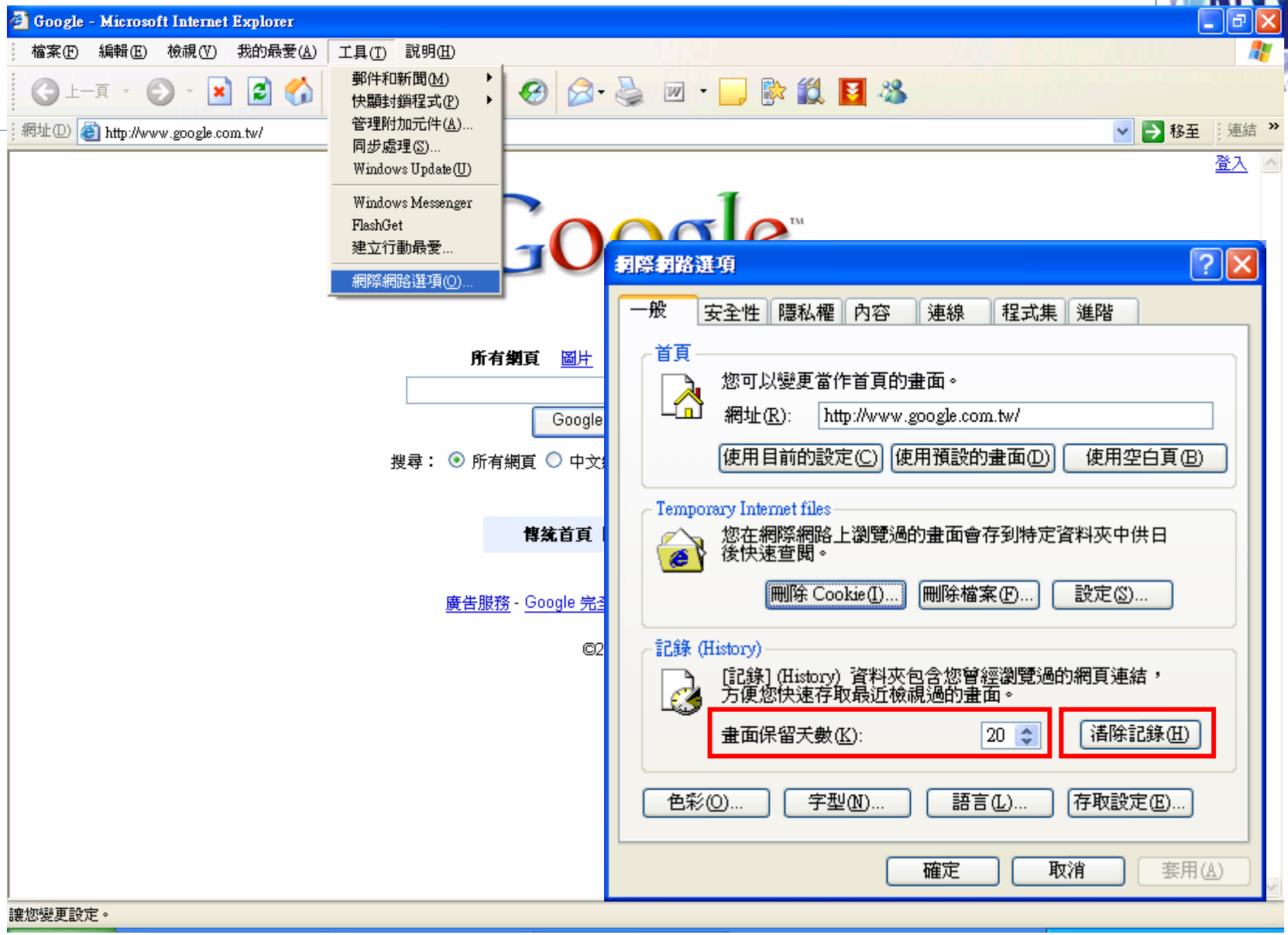
清除電腦上所留的登入資料...



清除網頁瀏覽記錄

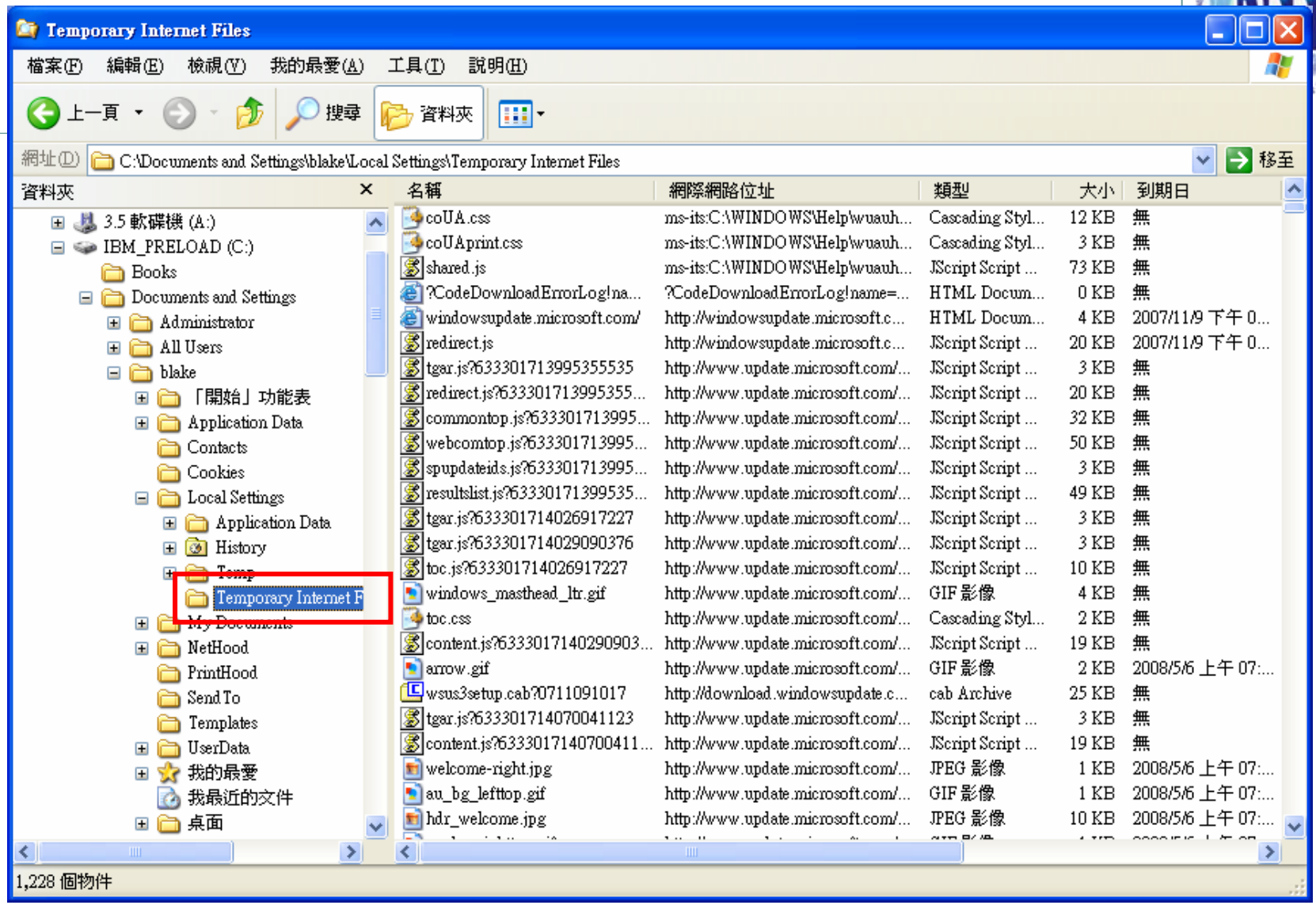
- 以使用Internet Explorer瀏覽器為例
  - Internet Explorer的預設值，記錄過去20天的曾經瀏覽過的網頁；若不希望別人知道自己曾經瀏覽過哪些網站，可以清除網頁瀏覽記錄

清除網頁瀏覽記錄...

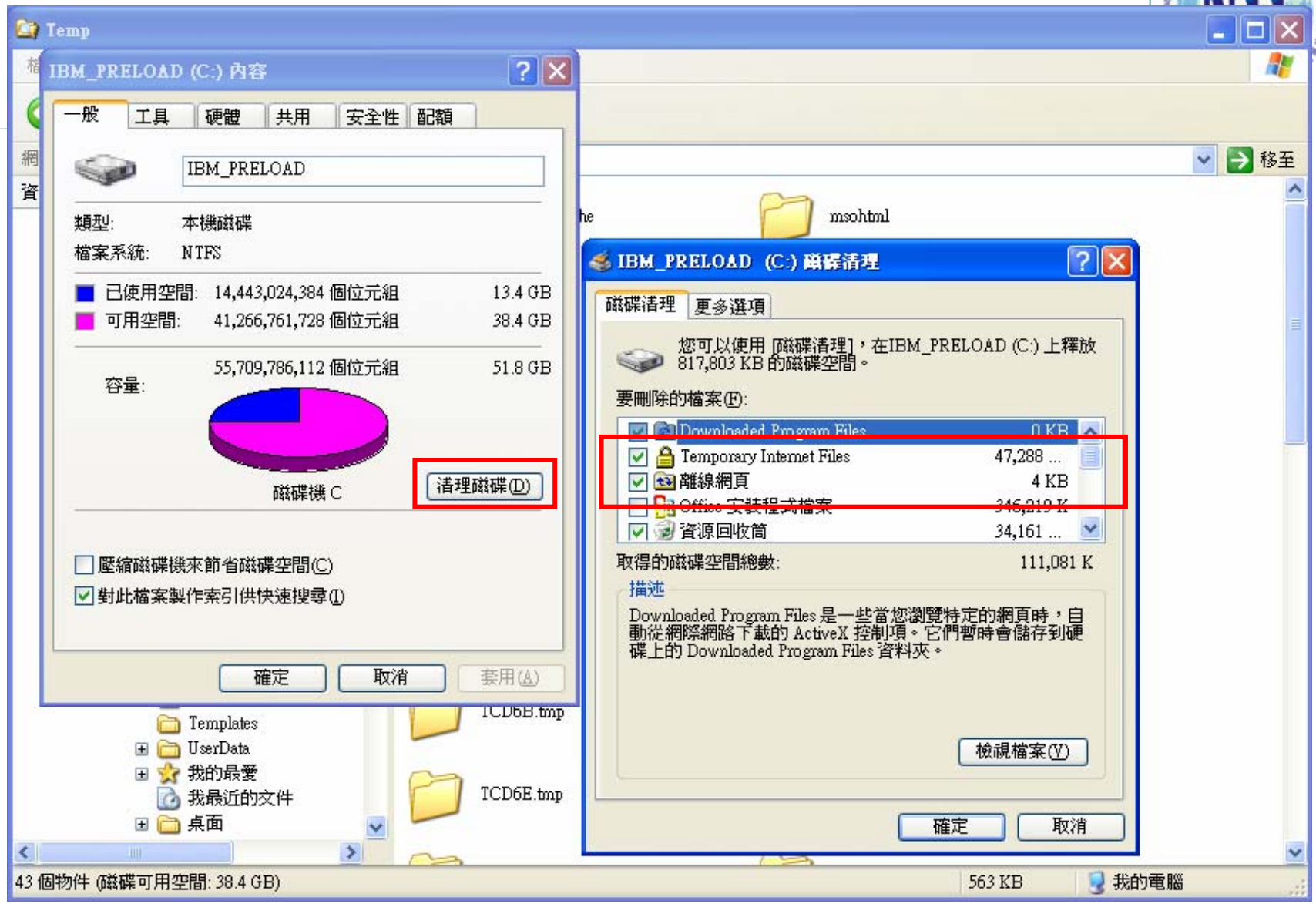


刪除電腦上的暫存檔案...

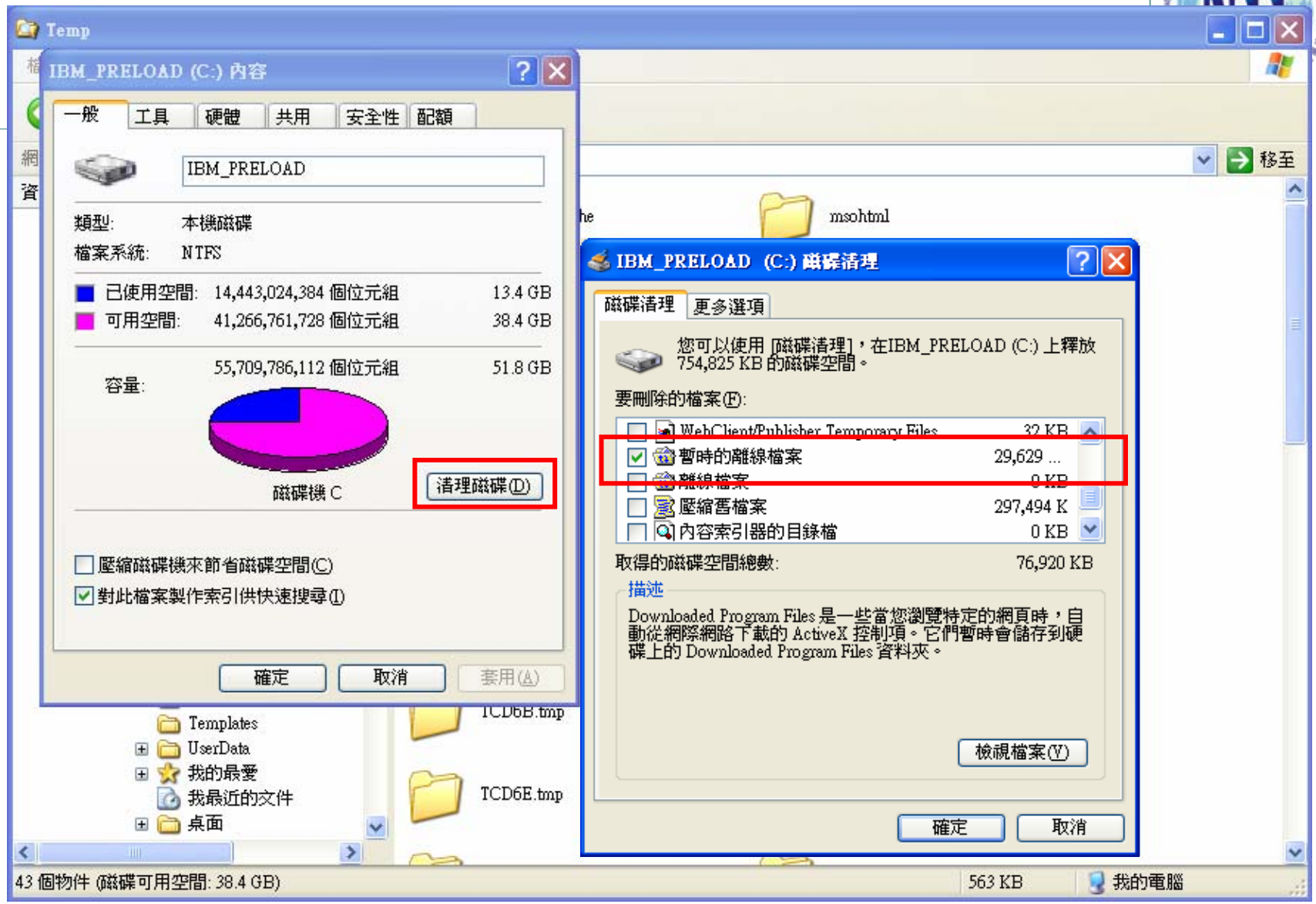
電腦上的暫存檔 - Temporary Internet Files



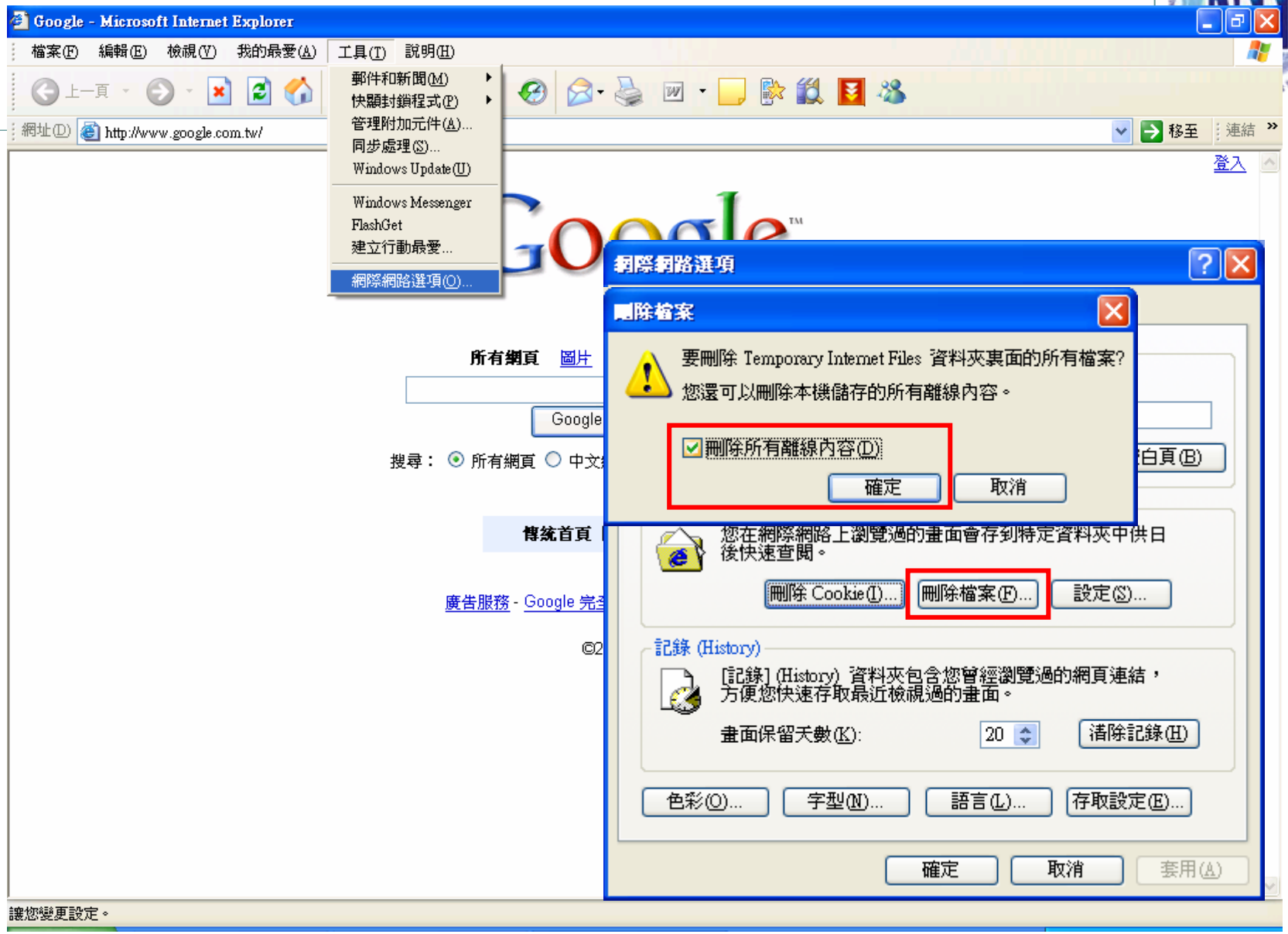
清除磁碟...



清除磁碟...

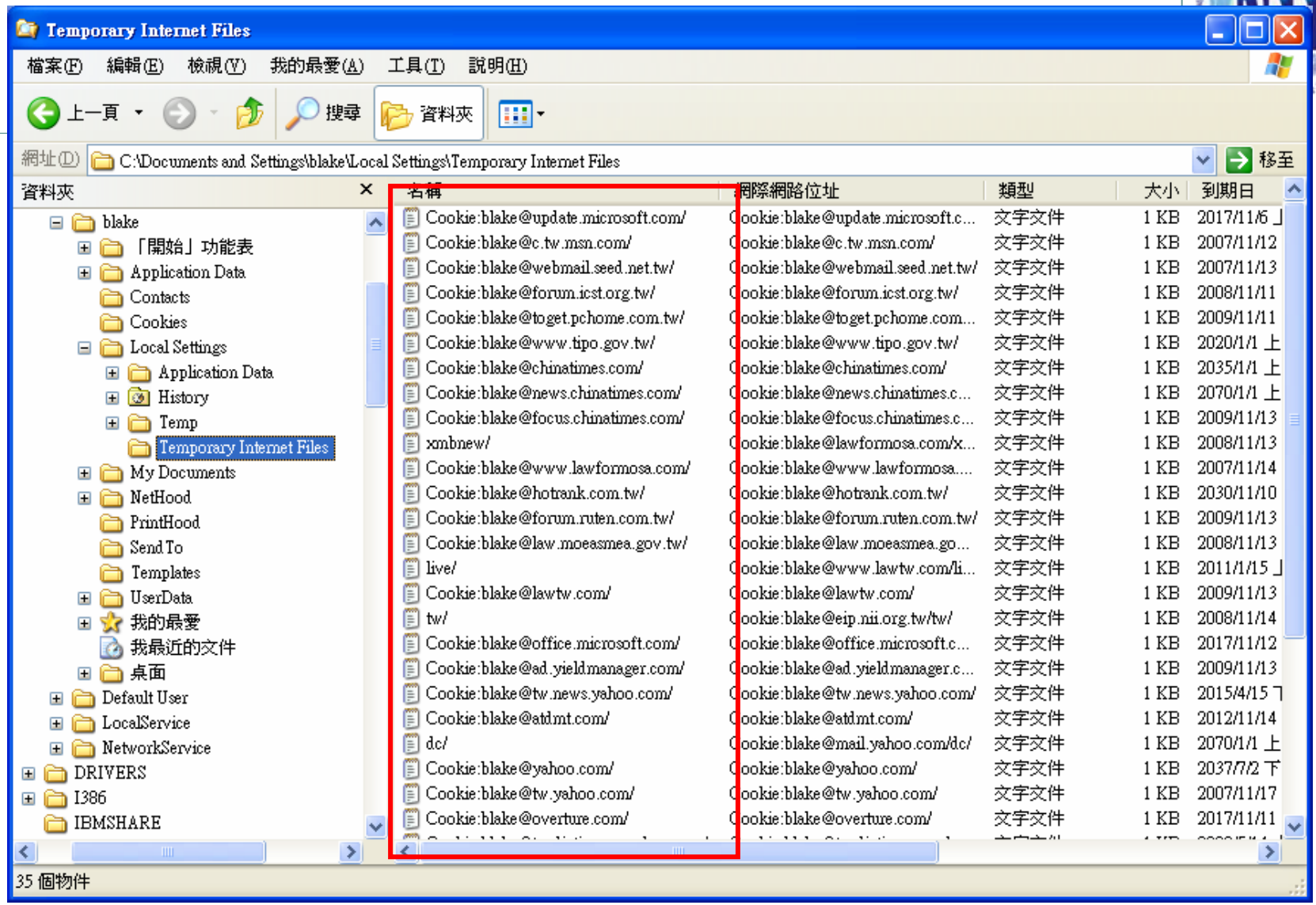


使用瀏覽器選項清除檔案...



清除完畢後...

Cookies尚未清除...

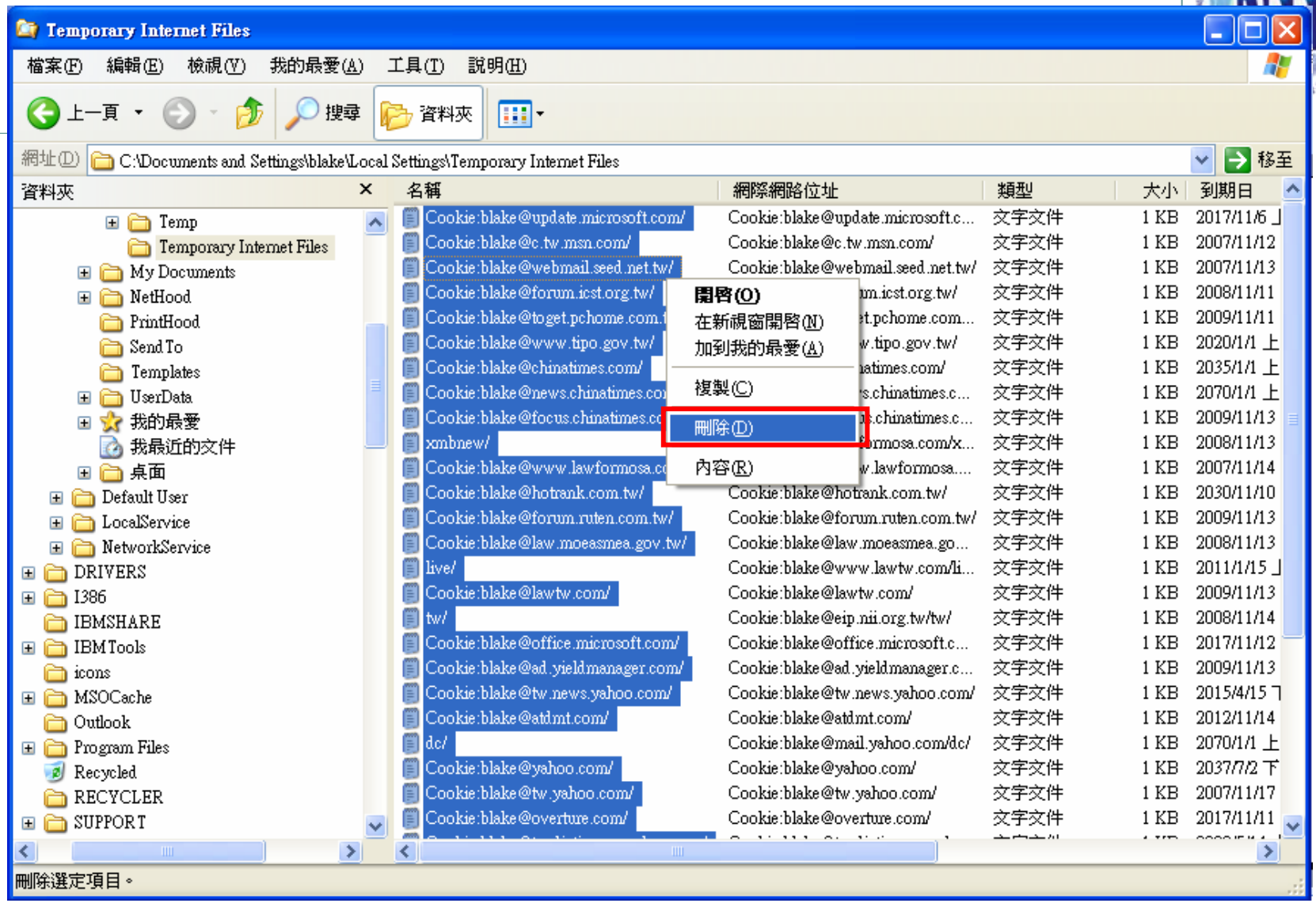


兩個清除方法：

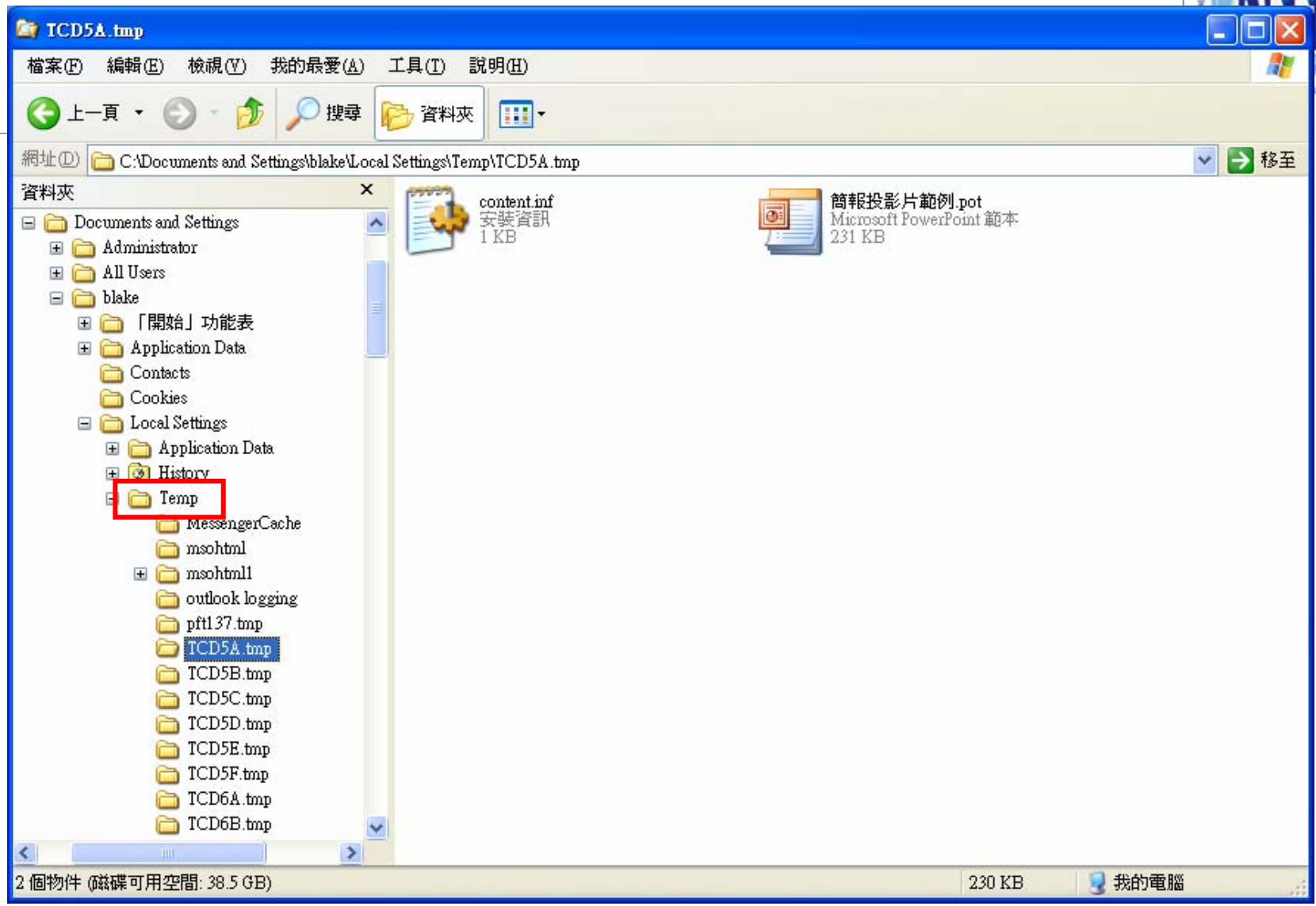
(1) 清除暫存檔 + Cookies

(2) 由檔案總管直接刪除Temporary Internet Files 全部檔案

由檔案總管直接刪除...



電腦上的暫存檔 - Temp

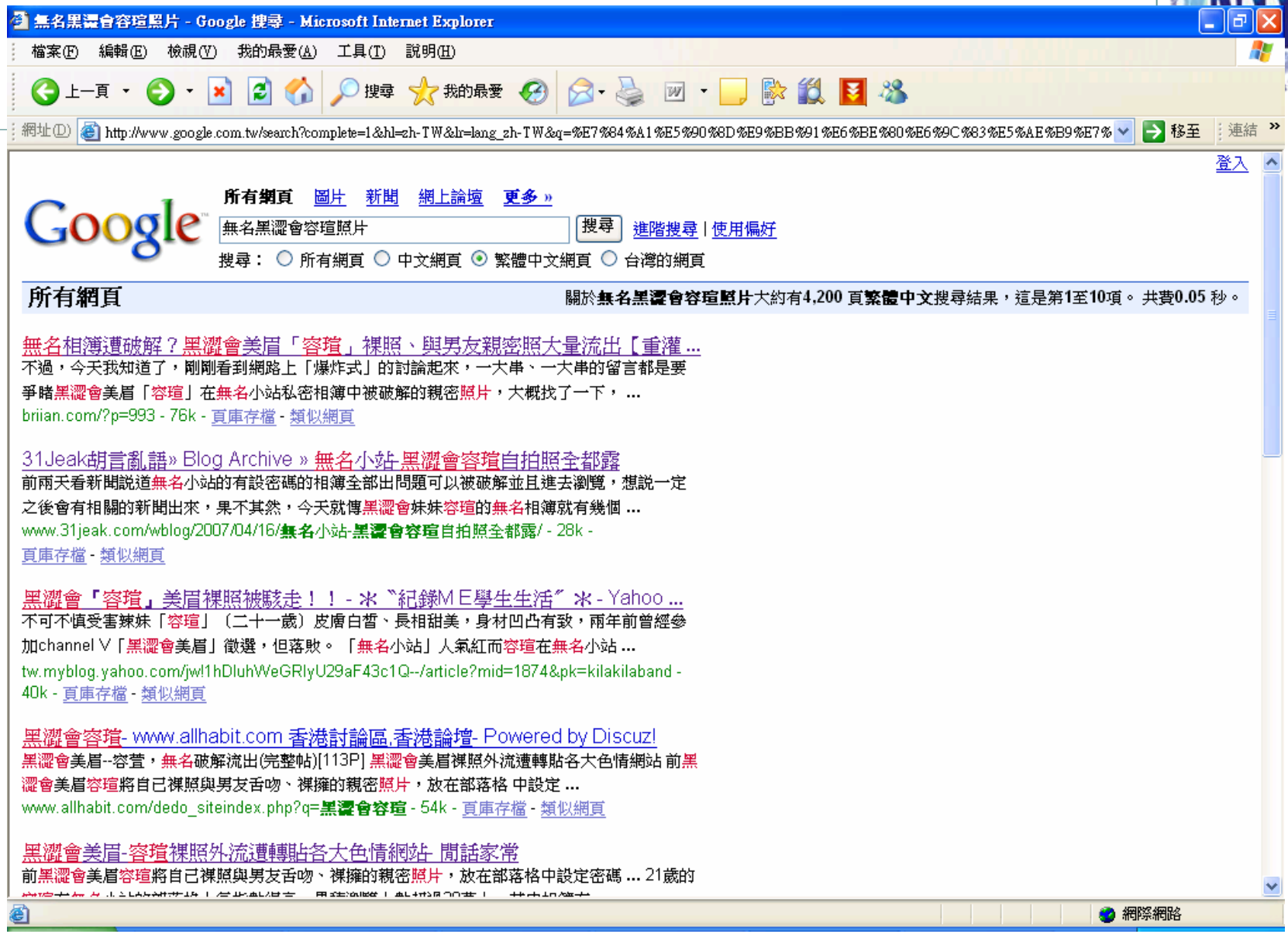


您在網路空間上的資料安全嗎...

黑澀會美眉裸照外流事件...

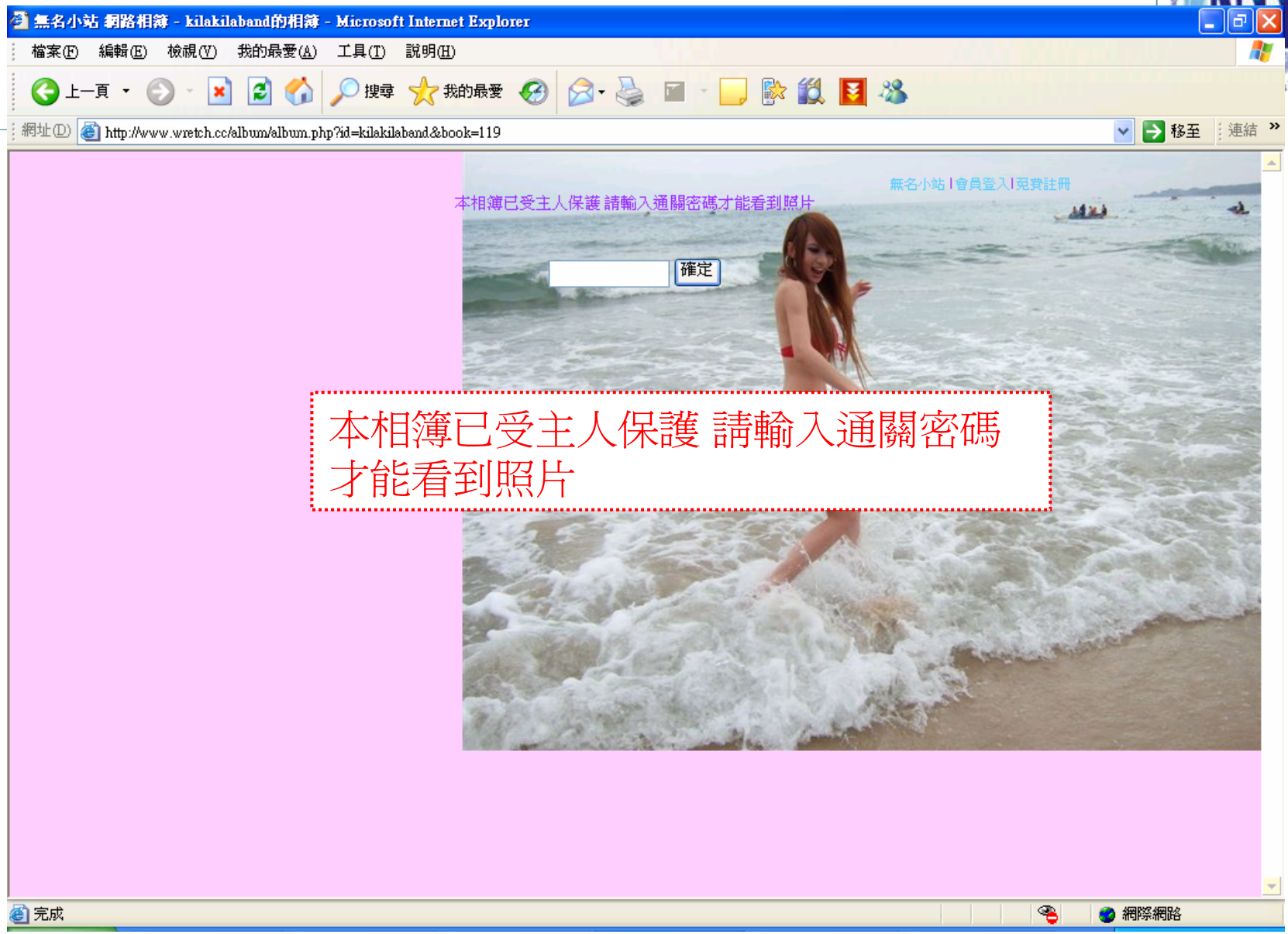
網路無遠弗界，一旦散播即覆水難收...

關了部落格也沒用，到處都有轉貼...



無名小站存有近兩百萬會員個人檔案的資料庫，
因此成為駭客練功的最愛之一。
陳嫌以XSS漏洞入侵無名小站，
同時還在台灣駭客年會發表專題時，
發表自己入侵無名小站的方法與駭客分享...

您的密碼真的保護了您的隱私照了嗎...



大部分仍都是密碼不夠嚴謹...

認知您隱私資料的保護，

以及安全密碼的重要...

PTT全站使用者升等站長事件 ...

PTT站長侵入情敵帳號侵犯隱私權事件 …

網站要求真實資料

但能夠保證真實資料的安全嗎 ...

- 網路安全概論
- 駭客概述
- 電腦病毒
- 木馬及後門程式
- 常見入侵來源
- 惡意程式防護
- 資料及隱私權保護
- 防範SQL Injection攻擊
- 行動設備安全
- 無線網路安全

防範SQL Injection攻擊 (1/6)

- SQL語法
  - SELECT * FROM tbUser
  - SELECT * FROM tbUser WHERE UserName='john' AND Password=' password1234'

駭客的 SQL填空遊戲 …

防範SQL Injection攻擊 (2/6)

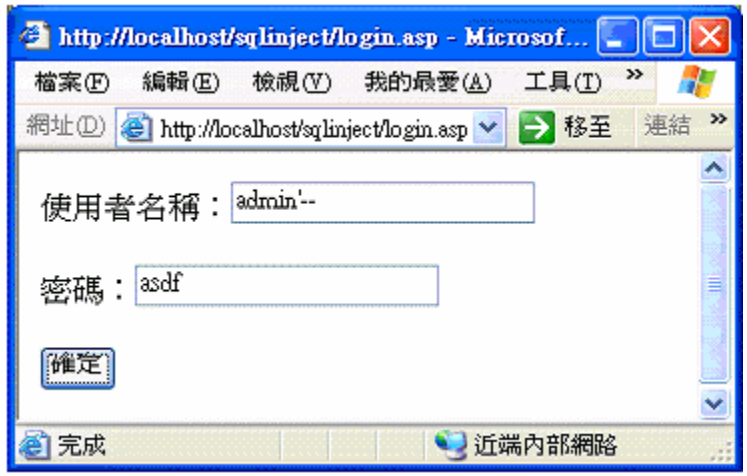
- SQL Injection
  - 資料隱碼攻擊
  - 網管人員可能架設了防火牆，設計非軍事區，限制網站登入者的身分等等
  - 但由於缺乏對 SQL 語言及資料庫管理系統的認知，而大開系統的後門

- 利用使用者輸入的資料來組合 SQL 語法
  strSQL="SELECT * FROM tblUser WHERE UserName='" & 輸入的帳號 & "' AND Password='" & 輸入的密碼 & "'"

- 直接交給 SQL Server 執行，這是最危險的

防範SQL Injection攻擊 (3/6)

- 利用任何已知的使用者名稱登入網站



防範SQL Injection攻擊 (4/6)

- 利用任何已知的使用者名稱登入網站 (續)
  - SQL語法本身擁有一些特殊字元
  - 例如在帳號輸入「admin‘--」；密碼輸入「asdf」
    - SELECT * FROM tbUser WHERE UserName=‘admin’--‘ AND Password=’asdf‘
    - 「--」代表刪除後面字串
    - SELECT * FROM tbUser WHERE UserName='admin'

防範SQL Injection攻擊 (5/6)

- 用未知的使用者名稱登入網站
  - 例如在帳號輸入「‘ or 1=1--」；密碼輸入「123」
    - SELECT * FROM tblUser WHERE UserName='' or 1=1--' AND Password='123'
    - or 1=1 → 則不管之前的條件為合，只要某個條件為真，整個判斷式就都為真

防範SQL Injection攻擊 (6/6)

- 防範措施
  - SQL所有輸入值都必須針對SQL特殊字元和長度、型態做檢查
  - 結合SQL 字串前應先檢查輸入值內容，同時若有帳號密碼比對時，應在程式中執行
  - 網頁上不可顯示資料庫的錯誤訊息，程式應攔截所有錯誤訊息，並用錯誤代碼或是其他說明文字替代
  - 程式存取資料庫的權限應提供最小權限
  - 不應使用常用管理帳號，或是前台不應設置管理帳號

- 網路安全概論
- 駭客概述
- 電腦病毒
- 木馬及後門程式
- 常見入侵來源
- 惡意程式防護
- 資料及隱私權保護
- 防範SQL Injection攻擊
- 行動設備安全
- 無線網路安全

行動設備安全 (1/2)

- 資料安全
  - 失竊風險
    - 不要離開您的視線
    - 使用防盜鎖
  - 各項資料保護措施
    - 作業系統密碼 / 指紋認證
    - 檔案加密

行動設備安全 (2/2)

- 使用安全
  - 系統修補、嚴謹密碼、防火牆、防毒軟體...
  - 備份重要資料
  - 設定螢幕保護密碼
  - 使用安全的無線網路

- 網路安全概論
- 駭客概述
- 電腦病毒
- 木馬及後門程式
- 常見入侵來源
- 惡意程式防護
- 資料及隱私權保護
- 防範SQL Injection攻擊
- 行動設備安全
- 無線網路安全

無線網路安全 (1/3)

- 使用無線網路需要注意的問題
  - 網路監聽
    - 透過無線電波傳輸訊息，容易遭到竊聽、截取等攻擊
  - 偽造身份認證
    - 無線網路使用端需與無線基地台做認證，因此惡意人士可能利用偽造身份認證，與基地台建立連線
  - 竄改傳送訊息
    - 不論是有線或無線網路，都有可能面臨訊息遭到竄改的危險，而無線網路由於容易被監聽，因此在訊息的機密性和完整性上需特別注意

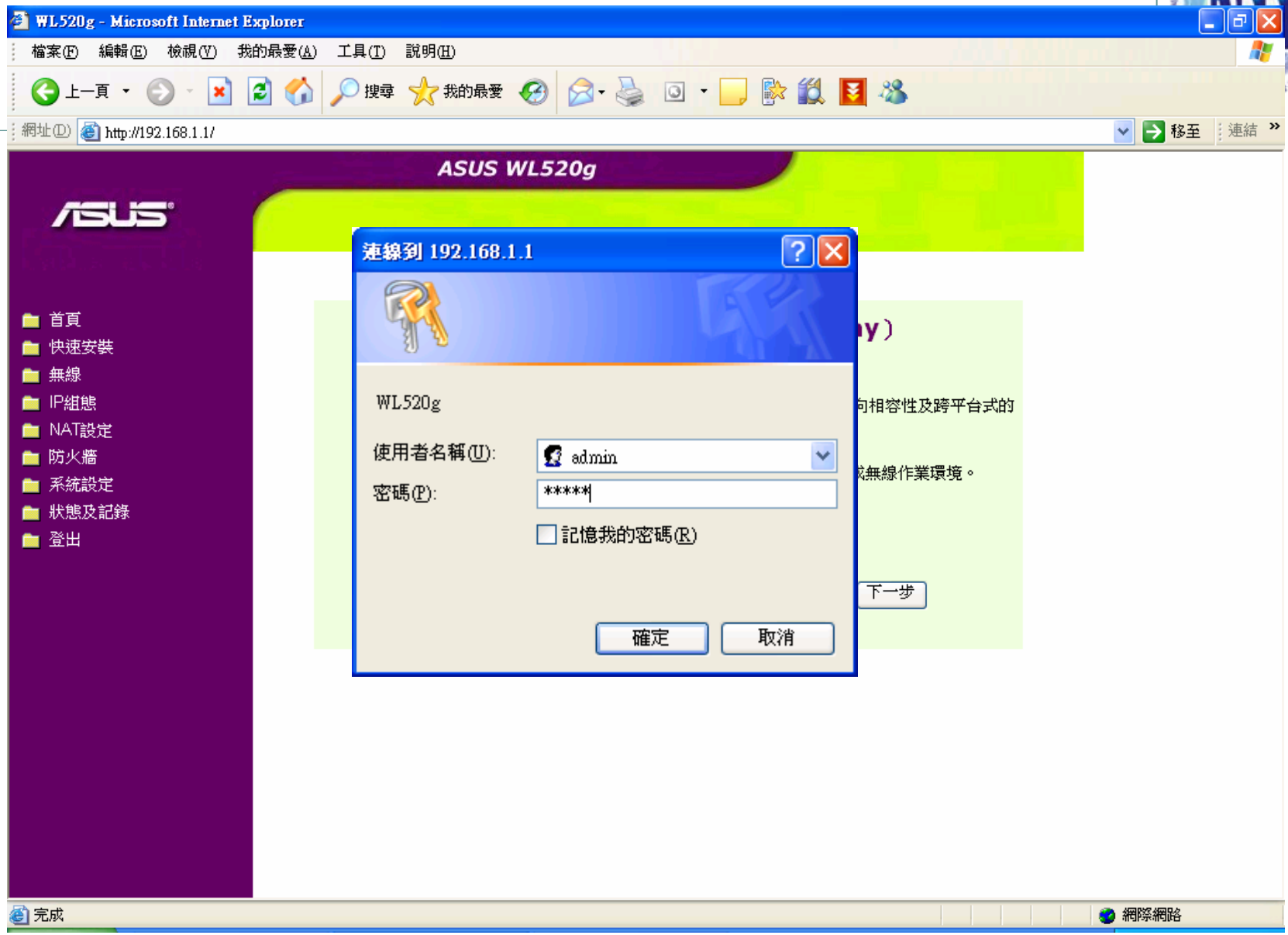
無線網路安全 (2/3)

- 如何加強無線網路的安全
  - 修改登入帳號密碼
    - 企業購置無線基地台後，應修改無線基地台的預設登入帳號密碼

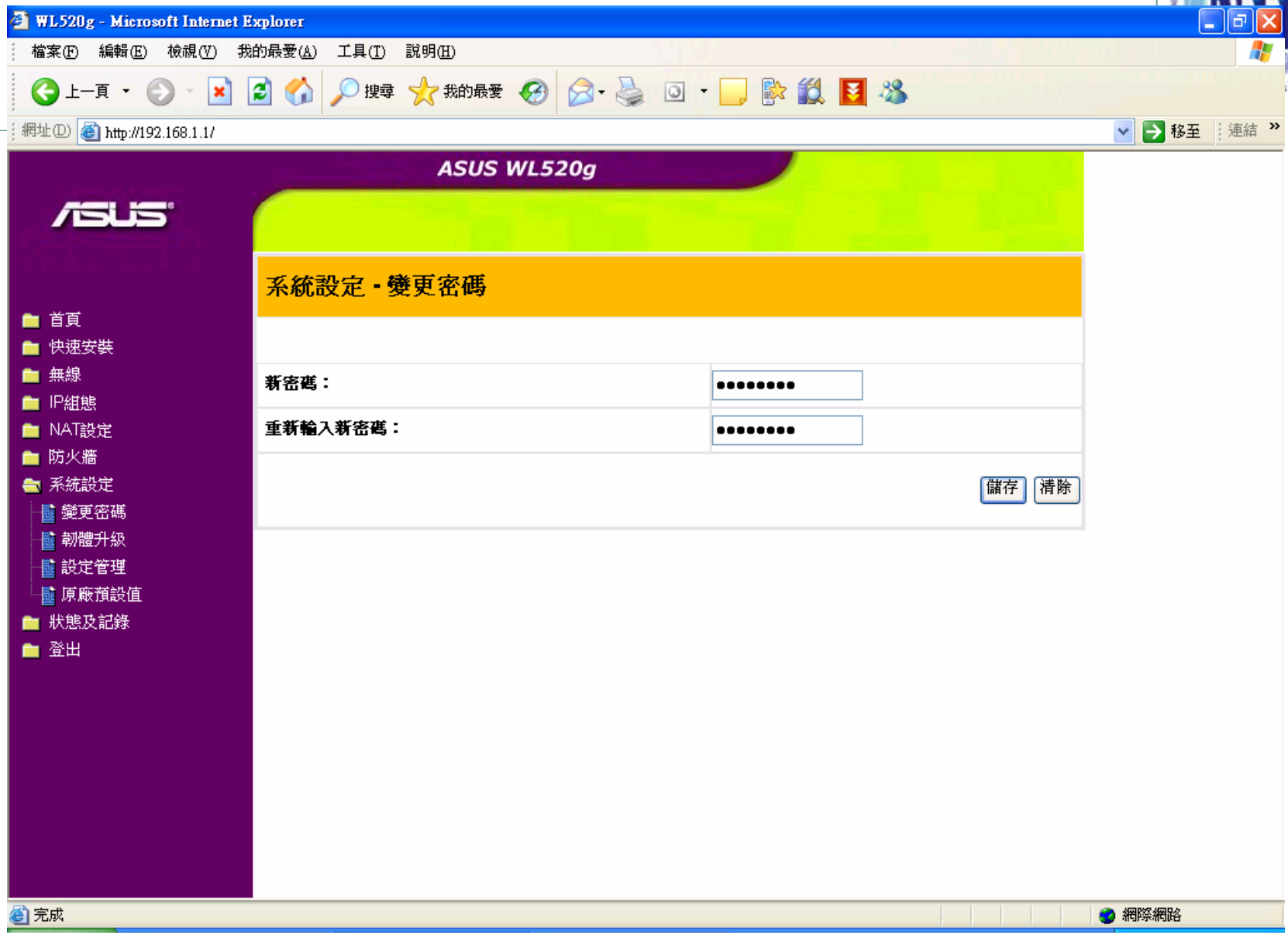
無線網路安全 (2/3)

- 如何加強無線網路的安全 (續)
  - 採用WPA / WPA2加密傳輸資料
    - WEP： IEEE 802.11b規範的128 bit加密方式
    - 採用單向、靜態的認證機制，被發現漏洞百出，且容易受到中間人攻擊(man-in-the-middle attack)入侵，駭客僅需利用偽裝的存取設備攔截資訊，再經由用戶端收集認證資料，接著複製或更動封包，就能將這些封包偽裝成合法封包，成功進入無線網路
    - WPA：因應WEP中找到嚴重弱點而產生的，WPA實作了大部分的 IEEE 802.11i標準
  - 管制網路卡卡號(MAC)

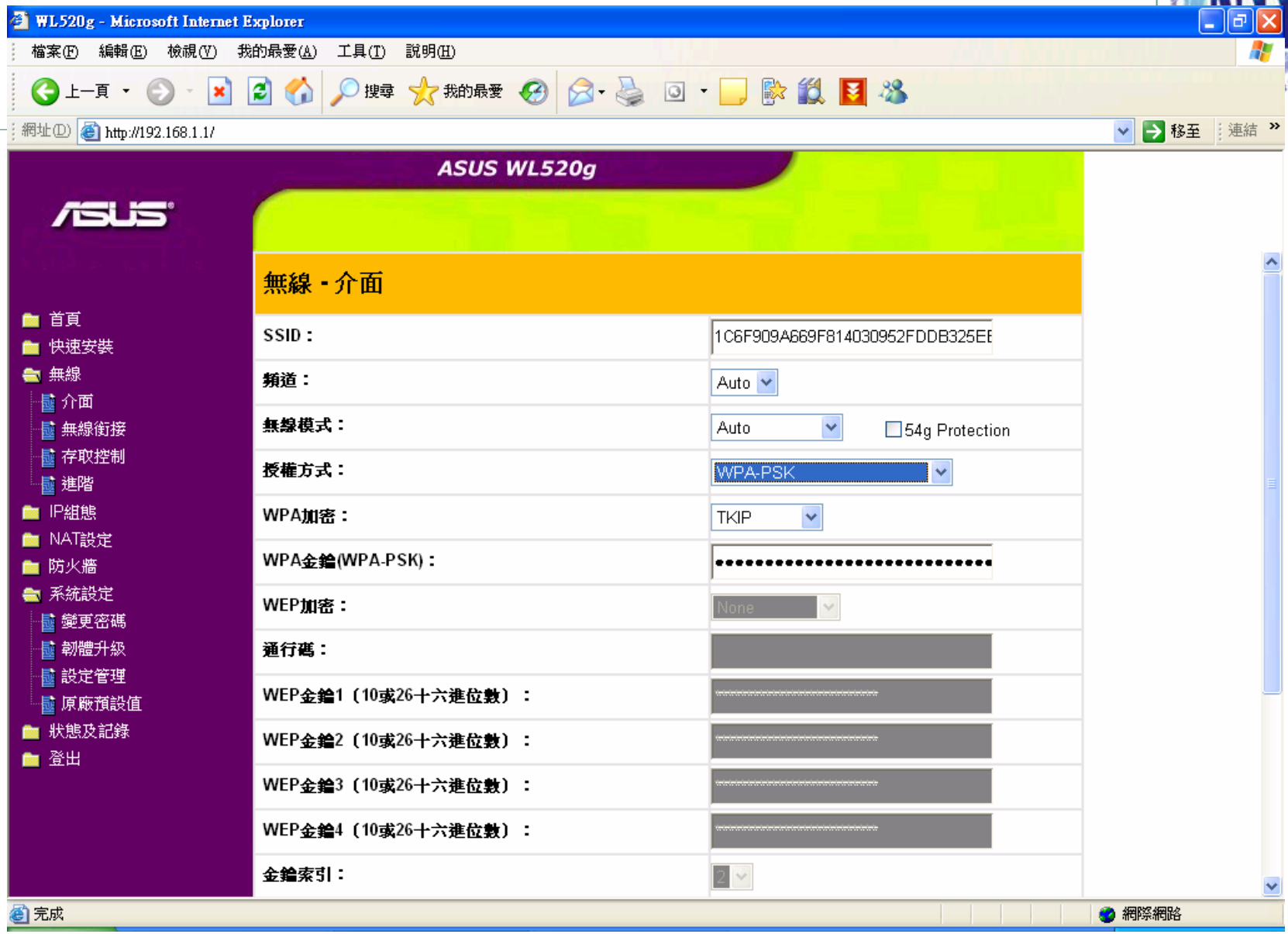
這是預設的帳號密碼...



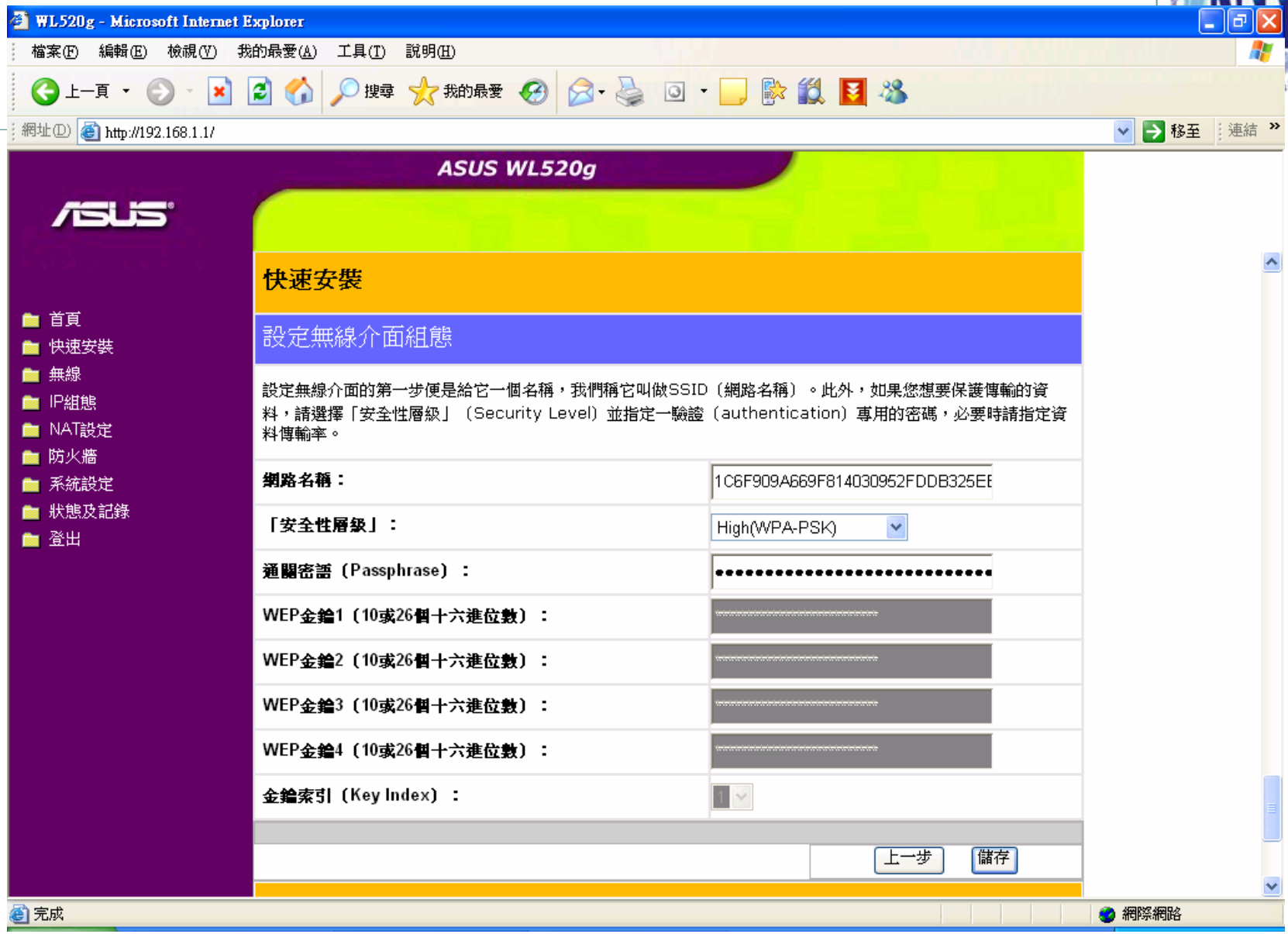
一定要改掉...



使用WPA / WPA2加密...

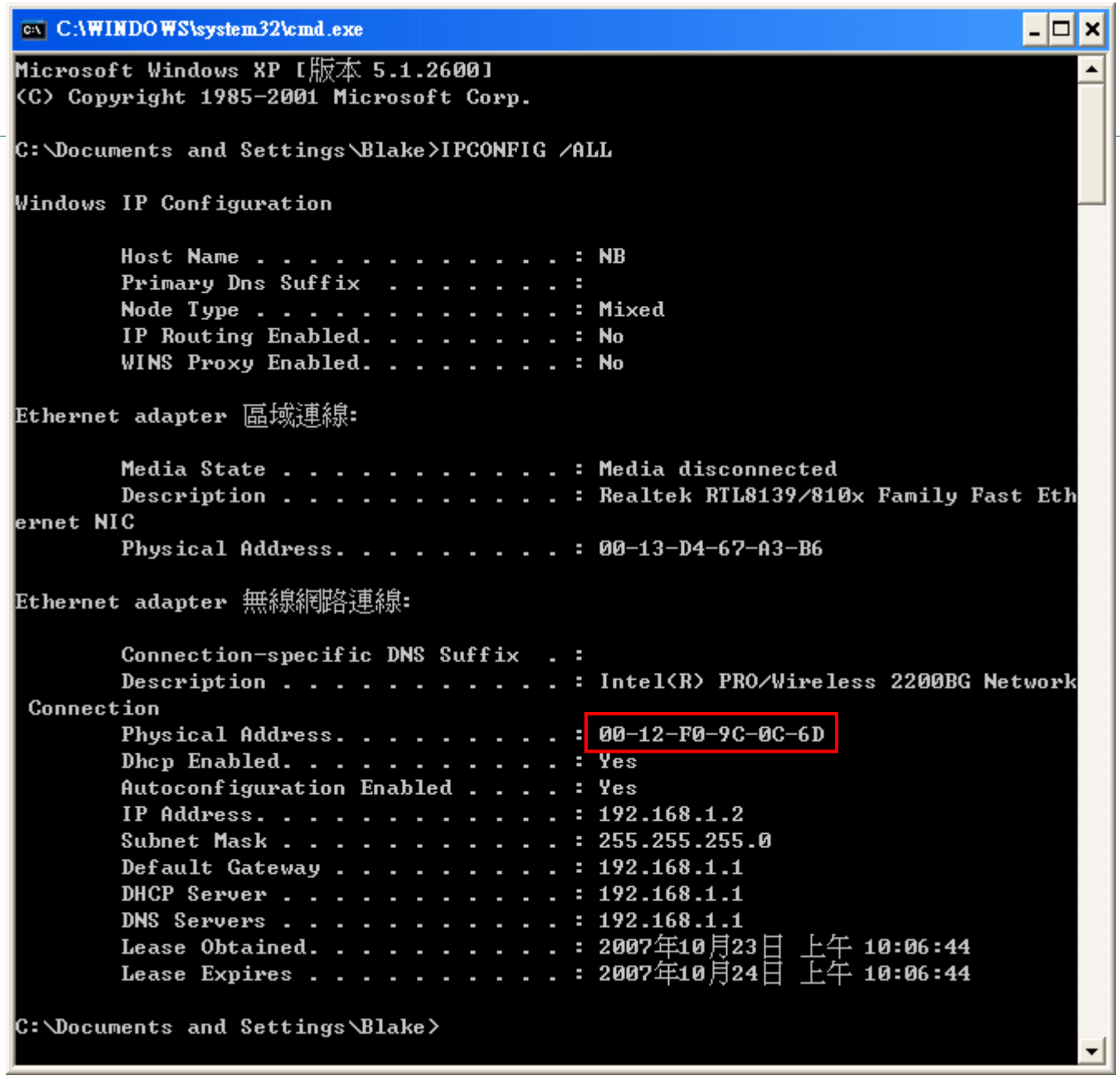


或在安裝時就應選用WPA / WPA2加密...



設定允許連線的MAC...

查詢網路卡MAC…


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Blake>IPCONFIG /ALL
Windows IP Configuration
Host Name . . . . . : NB
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter 區域連線:
Media State . . . . . : Media disconnected
Description . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
Physical Address. . . . . : 00-13-D4-67-A3-B6
Ethernet adapter 無線網路連線:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/Wireless 2200BG Network Connection
Physical Address. . . . . : 00-12-F0-9C-0C-6D
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1
Lease Obtained. . . . . : 2007年10月23日 上午 10:06:44
Lease Expires . . . . . : 2007年10月24日 上午 10:06:44
C:\Documents and Settings\Blake>

無線網路安全 (3/3)

- 無線網路使用安全
  - 確認無線網路傳輸使用加密通訊協定
  - 不隨意連線到不明之無線存取點
  - 避免使用不安全的無線網路傳輸重要資料

- 補充A：電腦犯罪
- 補充B：資安案例

- 補充A：電腦犯罪
- 補充B：資安案例

網路常見犯罪類型

- 妨害風化
- 網路竊盜
- 網路詐欺
- 偽造文書
- 公然侮辱、誹謗
- 煽惑他人犯罪
- 侵害著作權
- 其他犯罪

參考資料：花蓮縣資訊法律研習

妨害風化

- 網路援交
  - 刊登網路援助交際訊息
  - 違反兒童及少年性交易防制條例第二十九條之「以電腦網路散布使人為性交易訊息罪」，最重可處有期徒刑五年

妨害風化

- 貼圖、以電子郵件散布色情圖片
  - 圖片若為未滿十八歲之人：兒童及少年性交易防制條例第二十八條之「散布未滿十八歲之人性交或猥褻圖片罪」，最重可處有期徒刑三年
  - 圖片若已滿十八歲之人：刑法第二百三十五條第一項：散布猥褻圖片罪，最重可處有期徒刑二年

妨害風化

- 販賣色情光碟
  - 刑法第二百三十五條

網路竊盜

- 線上遊戲寶物、天幣竊盜案件，以竊盜罪移送。「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者」最重可處有期徒刑五年

網路詐欺

- 網路拍賣交易詐欺：刑法第三三九條，最重可處有期徒刑五年
- 不正當利用電腦取財：以不正當方法製作財產之變更，而取得他人財產者，最重可處七年有期徒刑

偽造文書

- 冒用他人名義刊登援交訊息：最重可處五年有期徒刑
- 上網竄改他人資料：該當於「電腦處理個人資料保護法」第三十四條，最重可處有期徒刑三年

公然侮辱、誹謗

- 意圖散布於公眾，足以毀損他人名譽之事者
  - 刑法第 309 條之公然侮辱罪與第 310 條之誹謗罪，公然侮辱罪可處拘役或三百元以下罰金，如果以暴力公然侮辱人者，可處一年以下有期徒刑、拘役或五百元以下罰金
  - 政大學生在 BBS 上罵老師事件
  - 某大學生因為不滿某教授之教學及考試方式，在校園的網際網路上指責某甲教授如何抄襲學生的研究報告當其論文，經某甲教授提出誹謗告訴，法院以違反刑法第310條第二項判處該大學生拘役55天確定

煽惑他人犯罪

- 刑法第一五三條第一款之「以文字煽惑他人犯罪」罪，最重可處有期徒刑二年
  - 「軍火教父」網站以文字及圖片內容介紹「貝瑞塔」槍枝廠牌、規格、性能、配件、裝填子彈數、相片及販賣價格、訂購方法、劃撥帳號、交槍時間及交槍方法等資訊。經台北地院以被告涉嫌煽惑他人違背我國之槍砲彈藥刀械管理條例法律，造成網路使用者有進而透過該管道取得槍枝而觸法之虞，予以判刑

侵害著作權

- 販賣盜版軟體：最重可處有期徒刑二年，若為常業犯，則為一年至七年有期徒刑

其他犯罪

- 製造電腦病毒程式導致他人遭到損害，最重可處五年有期徒刑
- 無故以電子郵件灌爆別人的電子信箱，最重可處三年有期徒刑（刑法第三百六十條）

網路拍賣影音等光碟...

- 民眾於網路上拍賣影音光碟的違法情況
  - 將自實體世界（零售店、夜市等）買來之盜版影音光碟提出於網路，再予販售
  - 將自網路買來之盜版影音光碟提出於網路，再予販售
- 不可以做盜版品，也不可以賣盜版品，賣盜版品者會構成侵害散布權

資料來源：智慧財產局

「廿三歲的何姓女學生在網站以二百元購買日劇「流星花園」一套三片光碟。去年一月她在拍賣網站以同價格出售，被基本國際公司指控涉及違反著作權法，父母拿出20萬元和解，才獲檢方不起訴...」

「很多網友在網路上販賣盜版光碟，被影音代理商抓包索賠10萬塊和解，很多網友不滿這家代理商用釣魚的方式，坑殺他們的荷包，在網路上留言抗議，但智財局強調，就算只在網路上賣一片盜版光碟，都是違法...」

「被網友點名的基本國際公司，代理很多知名日劇，經常在拍賣網站上裝成買家搜尋一些賣盜版光碟的網友。像台北有位盧小姐，花350塊買一套盜版韓劇，拿到網路上拍賣，沒賺到錢卻被基本國際抓包，最後花了10萬塊和解，很多賣家在網路上留言，自己被代理商設局，不想吃上官司，就得賠償一大筆錢...」

「我個人從被警方通知做筆錄到接獲傳票上偵察庭，來自家人的壓力，自身的譴責與懊悔，都讓我沒辦法好好上班，每天都在想著訴訟事件，時常精神恍惚...」

「小弟因看完一片香港正版的平行輸入真品DVD
，在拍賣賣出，4月2日郵寄賣出，
前兩天被自稱基本國際股份有限公司的法務代理
商帶警察來家裡抓人...我真的傻眼！

在此之前我完全不知道原來正版的也有罪??
而且只是販售一件真品平行輸入可以搞的像殺人
強盜一般直接帶警察來家裡抓人??... 」

「也有人被抓後堅持不和解，循司法途徑解決的反賠得較少。卅六歲黃姓水電工，在拍賣網站以250元買了一套「在世界中心呼喊愛」，看完後，以150元上網出售。交貨時，基本國際公司法務部副理會同警方以違反著作權法逮捕他。

黃姓水電工沒有錢和解，經台北地方法院判處徒刑六月，緩刑二年。基本國際再提民事訴訟求償廿萬元，法官認為才兩片光碟損害不大，求償廿萬元太高，判賠兩萬元...」

- 補充A：電腦犯罪
- 補充B：資安案例

案例(一)

- 2006年2月，日本海上自衛隊發現，有部分機密資料因隊員個人電腦使用的資訊交換軟體Winny感染電腦病毒而外洩，日本防衛廳證實外洩機密包括海上自衛隊曾實施之最大海上演習的作戰計畫，資料總數多達3,000件，包括美日海軍共同使用的通信與暗號。
- 防衛廳調查結果確認一名護衛艦隊員於一月份外洩資料，這名隊員在2004年即開始使用Winny，而海上自衛隊是在二月中發現機密文件外洩，五天後才找到外洩出處。朝日新聞引述海上幕僚長（海軍參謀長）發言表示，對發生這種洩密事件極為痛心，報導並指出，海上自衛隊內部有人認為這項事件造成日本嚴重信用破產，數年內難以恢復。

案例(二)

- 2005年3月，日本某防毒軟體廠商證實公司營業資料被經由P2P軟體Winny外流，流出的資料包括專題資料、行銷計畫與外部契約等。
- 這些資料是由一名員工的家用電腦所外流，這名員工將公司業務資料帶回家作業，而這台家用電腦沒有安裝防毒軟體。該公司表示，當時並沒有明令公司資料不許私自攜出，但之後已明文規定，今後不會再發生類似事件。

案例(三)

- 2005年3月，柏克萊加州大學發布消息表示，該校研究所部的辦公室失竊一台筆記型電腦，可能導致超過98,000筆個人資料外洩。這些資料包括研究生或申請就讀研究所人士的姓名、出生日期、住址和社會安全號碼，有的檔案的建檔歷史已長達30年。
- 雖尚未傳出與這起竊案相關的身分盜竊事件，不過柏克萊加大仍敦促受影響的個人考慮向信用徵信單位提出預警。

案例(四)

- 2006年11月，職棒簽賭案某投手教練遭恐嚇案，刑事局逮捕一名況姓女子，搜索時發現一部刑事局預防科警官的電腦，除了他和況女七年以上的婚外情因此曝光，督察室也擔心他和職棒簽賭有掛勾，記兩大過等待調查。
- 刑事局抓到況姓女子，查出她是綁架案田姓主嫌的乾妹妹，原本應士氣大振，卻在搜索況女嫌家時，發現她用的筆記型電腦赫然貼著警政署刑事局公務標籤，所有人是預防科兩線三星警官。據了解，該警官從省刑大時代就和況女在一起，藕斷絲連達7年之久，電腦給女友用了快一個月。警方督察室亦立刻以公物外流處分，並加緊限期破案。

案例(五)

- 2007年3月，駭客組織利用Windows作業系統處理游標圖示（*.ani）攻擊，微軟於三月底發佈警告，指出安全漏洞可能讓Windows用戶遭到嚴重網路攻擊，但當時微軟尚無解決方法。
- 此「零日攻擊」（zero day attack）弱點影響包括Vista在內的所有版本Windows，攻擊者甚至只需將惡意的游標圖示（*.ani）或將副檔名更換成影像檔（*.jpg）後，放在網頁或透過電子郵件便可以在受害者的電腦上植入惡意程式。

案例(六)

- 2006年3月，根據iThome電腦報發布的「台灣三百大企業即時通訊使用政策調查報告」，結果顯示，其中有四分之一左右的受訪企業完全禁止使用即時通訊，38%的企業則表示有條件開放，另有25%的受訪企業表示採完全開放。
- iThome電腦報表示，國內大型企業已經意識到，使用即時通訊會對企業的營運會帶來一些影響，在此情況下，部份企業已把即時通訊的使用政策，拉高到企業經營策略的層級來考量。

案例(七)

- 2007年2月，國內某大型ISP業者遊戲網站遭駭客入侵，會員個人資料外洩、信用卡被盜刷，被盜刷的信用卡張數約1840張，總金額超過5百萬。
- 由於網站可能未盡到保護客戶資料職責，銀行認為這些損失應由業者負責，但還得經深入調查才能釐清責任歸屬。初步調查每張卡損失約有數百元到數千元間，雖然損失金額有限，但警方擔心這些資料可能成為詐騙集團的行騙工具。

案例(八)

- 2004年6月，某知名線上遊戲公司向刑事局偵九隊報案，指稱該公司網站上供玩家以線上付費購買遊戲點數的數位銀行，遭不明人士盜刷他人信用卡大量騙取遊戲點數。
- 偵九隊清查所有盜刷信用卡交易的上線來源記錄後，發現上線地址均位於臺北市林森北路310巷週邊且呈不規則跳動分佈，經偵九隊派員前往上述地區周邊探訪，結果發現該地區鄰近住戶均設有無線網路上網設備，且有強烈的無線網路溢波，任何人只要利用一台筆記型電腦配合無線網卡及掃描程式，即可竊用住戶無線網路來上網。

案例(八) (續)

- 由於本案係國內首次發現嫌犯盜用他人無線網路並從事網路犯罪之案例，經局長指示，隨即組成專案小組全力偵辦。
- 專案小組多次前往實地現場定位測試後，追蹤發現林森北路某大樓住戶涉有重嫌，另請相關ISP業者及遊戲公司配合，對相關帳號展開即時監控。復經偵查人員監控多日，見時機成熟，遂於北投某網咖將還沉溺在網路遊戲的犯罪嫌疑人莊嫌等三人逮捕

謝謝各位撥冗上課

Question

& Answer ...