如何建構安全之網站

中華電信股份有限公司
數據通信分公司加值系統處

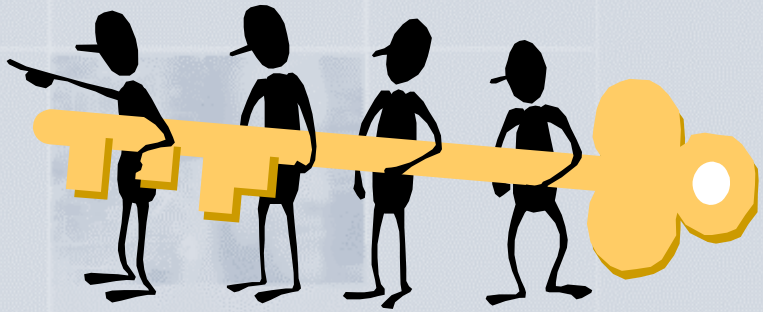
中華民國九十三年九月二十日

中華電信
Chunghwa Telecom

目錄

- 網站安全政策及隱私權保護
  - ✓個人資料保護法
  - ✓研考會網站安全政策及隱私權保護
  - ✓網路安全標章
- 網站防護
- 網站稽核

網站安全政策及隱私權保護



電腦處理個人資料保護法

- 第一條 立法目的：為規範電腦處理個人資料，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法
- 第二條 名詞定義：

✓個人資料：指自然人之姓名、出生年月日、身份證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。

✓個人資料檔案：指基於特定目的儲存於電磁紀錄物或其他類似媒體之個人資料之集合。

✓電腦處理：指使用電腦或自動化機器為資料之輸入、儲存、編輯、更正、檢索、刪除、輸出、傳遞或其他處理。

✓蒐集：指為建立個人資料檔案而取得個人資料。

電腦處理個人資料保護法

✓利用：指公務機關或非公務機關將其保有之個人資料檔案為內部使用或提供當事人以外之第三人。

✓公務機關：指依法行使公權力之中央或地方機關。

✓非公務機關：指前款以外之左列事業、團體或個人。

（一）徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。

（二）醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。

（三）其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。

✓當事人：指個人資料之本人。

✓特定目的：指由法務部會同中央目的事業主管機關定之者。

電腦處理個人資料保護法

➢第 四 條 當事人就其個人資料依本法規定行使之左列權利，不得預先拋棄或以特約限制之：

✓查詢及請求閱覽。

✓請求製給複製本。

✓請求補充或更正。

✓請求停止電腦處理及利用。

✓請求刪除。

電腦處理個人資料保護法

- 第 七 條 公務機關對個人資料之蒐集或電腦處理，非有特定目的，並符合左列情形之一者，不得為之：
  - ✓一、於法令規定職掌必要範圍內者。
  - ✓二、經當事人書面同意者。
  - ✓三、對當事人權益無侵害之虞者。
- 第 八 條 公務機關對個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。但有左列情形之一者，得為特定目的外之利用：
  - ✓一、法令明文規定者。
  - ✓二、有正當理由而僅供內部使用者。
  - ✓三、為維護國家安全者。
  - ✓四、為增進公共利益者。

電腦處理個人資料保護法

- ✓五、為免除當事人之生命、身體、自由、或財產上之急迫危險者。
- ✓六、為防止他人權益之重大危害而有必要者。
- ✓七、為學術研究而有必要，且無害於當事人之重大利益者。
- ✓八、有利於當事人權益者。
- ✓九、當事人書面同意者。

➢第 九 條 公務機關對於個人資料之國際傳遞及利用，應依相關法令為之。

➢第 十 條 公務機關保有個人資料檔案者，應在政府公報或以其他適當方式公告左列事項；其有變更者，亦同：

- ✓一、個人資料檔案名稱。
- ✓二、保有機關名稱。
- ✓三、個人資料檔案利用機關名稱。

電腦處理個人資料保護法

- ✓四、個人資料檔案保有之依據及特定目的。
- ✓五、個人資料之類別。
- ✓六、個人資料之範圍。
- ✓七、個人資料之蒐集方法。
- ✓八、個人資料通常傳遞之處所及收受者。
- ✓九、國際傳遞個人資料之直接收受者。
- ✓十、受理查詢、更正或閱覽等申請之機關名稱及地址。

歐盟對於公司在網際網路上處理顧客資料時的隱私保護

- 全部過程公正合法
- 具有明明白白合理合法之目的，才能蒐集處理個人資料
- 提供正確的資訊
- 在目的完成後，未獲顧客同意，就不能再利用顧客資料

使用者具有以下權利:

- 進入取得的權利
- 修改刪除或者不公開部分資訊的權利
- 對使用上表示疑義的權利

行政院研考會全球資訊網隱私保護及安全政策

隱私保護及安全政策

行政院研究發展考核委員會(以下簡稱本會)尊重並保護您在使用網際網路時的安全及隱私保護利，為了幫助您瞭解「行政院研考會全球資訊網」如何保護您在使用本網站各項服務的安全、及如何蒐集、應用及保護您所提供的個人資訊，請您詳細閱讀「行政院研考會全球資訊網」的隱私保護及安全政策。請您仔細閱讀以下各項說明，也歡迎您告訴我們您的想法，若有任何意見或疑問，請E-mail至rdec@rdec.gov.tw。

行政院研考會全球資訊網隱私保護及安全政策

網路安全保護措施

- 自動接收所有來自相關作業系統廠商或應用程式廠商所寄發的安全維護電子信通知，並依照電子信的建議，安裝適當的修改程式(PATCH)。
- 任何未經授權而企圖上載或更改本會所提供的各項服務及相關資訊的行為，都是嚴厲禁止而且可能觸犯法律。
- 為了網站安全的目的和確保這項服務能夠繼續服務所有的網路使用者，本網站提供了以下的安全保護措施，
  - ✓使用網路入侵偵測系統，監控網路流量，以確認未經授權而企圖上載或更改、網頁資訊或蓄意破壞者。

行政院研考會全球資訊網隱私保護及安全政策

網路安全保護措施(續)

- ✓裝設防火牆防止非法入侵、破壞或竊取或破壞資料，以避免網站遭到非法使用，以保障使用者的權益。
- ✓裝設掃毒軟體，定期掃毒，以提供使用者更安全的網頁瀏覽環境。
- ✓不定期摹擬駭客攻擊，演練發生安全事件時的系統回復程序，並提供適當的安全防禦等級。
- ✓每日進行備份作業，將所有資料備份到備援主機。

行政院研考會全球資訊網隱私保護及安全政策

隱私保護政策

適用範圍

※ 「行政院研考會全球資訊網」個人資料之蒐集政策

※ 「行政院研考會全球資訊網」上述蒐集資料之運用政策

※ 「行政院研考會全球資訊網」cookie運用政策

※ 「行政院研考會全球資訊網」與第三者共用個人資料之政策

※ 「行政院研考會全球資訊網」傳送電子郵件之政策

※ 「行政院研考會全球資訊網」個人資料修改之政策

※ 行政院研考會對於隱私保護條款的修改

※ 「行政院研考會全球資訊網」隱私保護保護政策諮詢

網站安全政策及隱私權保護範例

行政院研考會全球資訊網隱私保護及安全政策

行政院研考會全球資訊網」個人資料之蒐集政策

行政院研考會將在以下所述狀況，根據「行政院研考會全球資訊網」所提供的不同服務，因需要而請您提供相關資料：

1. 線上活動及網路調查
   當您參與線上活動或網路調查時，我們將視活動性質的不同而請您登錄其他必需的個人資訊。

2. 電子郵件或意見信箱
   如果您使用電子郵件或網站上的意見信箱與我們聯繫時，我們需要您提供正確的個人資料，作為回復您的依據。

3. 訂閱電子報
   當您訂閱我們的電子報時，我們需要您登錄姓名及電子郵件信箱地址。

4. 其他
   請您注意，在「行政院研考會全球資訊網」所連結的網站，也可能蒐集您個人的資料。對於您主動提供的個人資訊，這些連結網站有其個別的隱私保護保護政策，其資料處理措施不適用「行政院研考會全球資訊網」隱私保護保護政策，「行政院研考會全球資訊網」不負任何連帶責任。

網站安全政策及隱私權保護範例

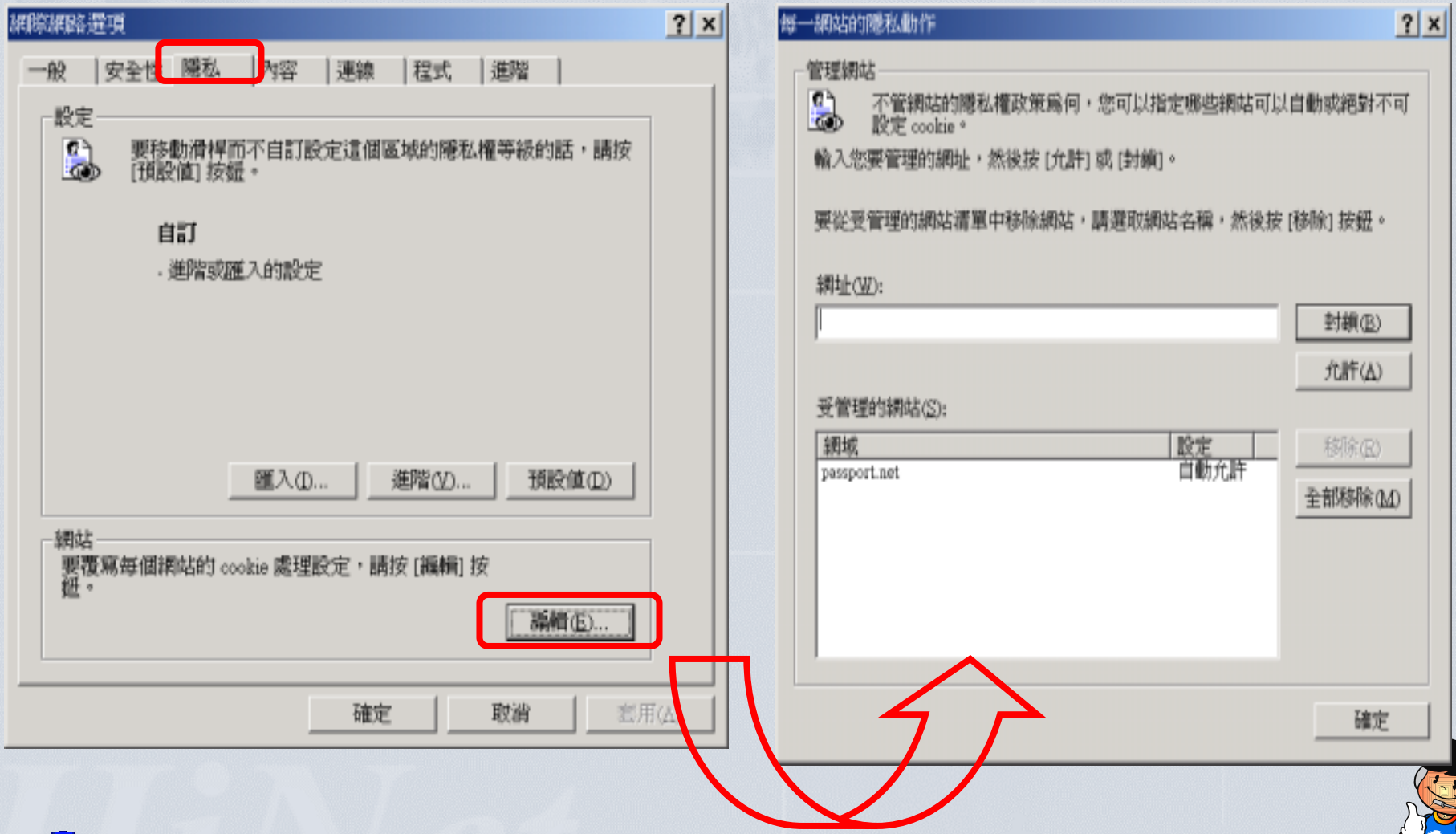
行政院研考會全球資訊網隱私保護及安全政策

「行政院研考會全球資訊網」cookie運用政策

Cookie是伺服端為了區別使用者的不同喜好，經由瀏覽器寫入使用者硬碟的一些簡短資訊。您可以在Netscape的「功能設定」的「進階」或是IE的「Internet選項」的「安全性」中選擇修改您瀏覽器對cookie的接受程度，包括接受所有cookie、設定cookie時得到通知、拒絕所有cookie等三種。如果您選擇拒絕所有的cookie，您可能無法使用部份個人化服務，或是參與部份的活動。

網站安全政策及隱私權保護範例

MS Internet Explorer 6.x->工具->網際網路選項->隱私



網站安全政策及隱私權保護範例

行政院研考會全球資訊網隱私保護及安全政策

「行政院研考會全球資訊網」cookie運用政策

依據以下目的及情況，「行政院研考會全球資訊網」會在本政策原則之下，在您瀏覽器中寫入並讀取cookie：

1. 為提供更好的個人化服務，以及方便您參與個人化的互動活動。cookie在您註冊或登入時建立，並在您登出時修改。
2. 為統計瀏覽人數及分析瀏覽模式，以了解網頁瀏覽的情況，做為「行政院研考會全球資訊網」改善服務的參考。

網站安全政策及隱私權保護範例

行政院研考會全球資訊網隱私保護及安全政策

「行政院研考會全球資訊網」與第三者共用個人資料之政策

「行政院研考會全球資訊網」絕不會任意出售、交換、或出租任何您的個人資料給其他團體或個人，但會在本政策原則之下，與第三者共用您的個人資料。

本會雖已在前述政策說明向您保證，絕不在未經您同意的狀況下將您的個人資訊任意揭露。但是，在以下幾個特殊的狀況下，本會將依相關法令處理您的個人資料，不是用前述保護規定。這些狀況包括（但不限於）：

1. 當您在本網站的行為，違反本會的服務條款或可能損害或妨礙本會權益或導致任何人遭受損害，經本會研析揭露您的個人資料是為了辨識、聯絡或採取法律行動所必要者。
2. 基於善意相信揭露您的個人資料為法律所需要。
3. 司法單位因公眾安全，要求「行政院研考會全球資訊網」公開特定個人資料時，「行政院研考會全球資訊網」將視司法單位適法性及是否遵照法定之程序，以及考量對「行政院研考會全球資訊網」所有使用者安全，採行可能必要的配合措施。

網站安全政策及隱私權保護範例

行政院研考會全球資訊網隱私保護及安全政策

行政院研考會對於隱私保護條款及安全政策的修改

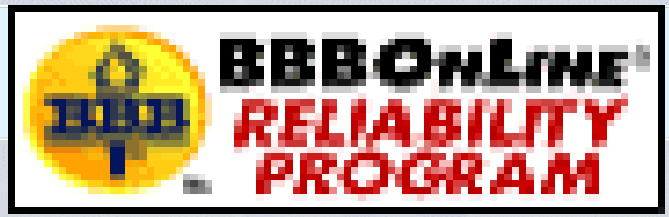
由於科技發展的迅速，相關法規訂定未臻完備前，以及未來可能難以預見的環境變遷等因素，本會將會視需要修改網站上所提供的隱私保護及安全政策的說明，以落實保障您隱私權及網路安全的立意。當本會完成隱私保護條款及安全政策的修改時，我們會立即將其刊登於本會的網站中，並以醒目標示提醒您前往點選閱讀。

「行政院研考會全球資訊網」隱私保護及安全政策諮詢

若您對「行政院研考會全球資訊網」的隱私保護及安全政策有任何疑問，都歡迎您隨時 與我們聯絡 (rdec@rdec.gov.tw)

網路認證標章

BBB Online Privacy Program
http://www.bbbonline.org/



北美著名的 **Better Business Bureau** (功能似台灣的消費者文教基金會) 的分機構，發行隱私權標章給符合**BBBOnLine**隱私權標準的網路商家。

Truste http://www.truste.org/
提供網路交易隱私保護之認證標章機構

網路認證標章

SOSA 台北市消費者電子商務協會

成立宗旨:

以非營利為目的，依法設立之社會團體，以推廣電子商務之應用、建立自律有序、公平效率、明確安全的電子商務環境、協助消費者和會員間紛爭的協調與解決為宗旨。

該會任務如下：

1.協會政策之擬定。
2.會員之認證與監督。
3.核發電子商務各消費者保護之相關認證標章。
4.訂定會員管理辦法。
5.辦理各項電子商務相關之研討及展示活動。
6.提供消費者申訴管道，協調會員解決。

網路認證標章

為建立自律有序、公平效率、明確安全的電子商務環境，SOSA乃創訂『優良電子商店』標章，並藉由此標章之核發，以謀消費者與電子商務業者雙方最大之福址。

- 凡經SOSA審查委員會審核通過之業者，SOSA即頒予『優良電子商店』標章，該業者即得將『優良電子商店』標章張貼於網站之首頁…等處。

審核評鑑標準

經SOSA核發『優良電子商店』標章者，其所代表之意義乃該公司認同SOSA精神，加入自律方案，願意確實遵行SOSA《優良電子商務行為準則》。SOSA將對使用『優良電子商店』標章之業者，作定期與不定期之查核，並公佈相關事實。

SOSA乃非營利之公益性組織，對該業者所具體提供之商品或服務，不負保證之責，但仍將盡最大之努力，與消費者一起督促業者，確實自律，遵行SOSA《優良電子商務行為準則》。

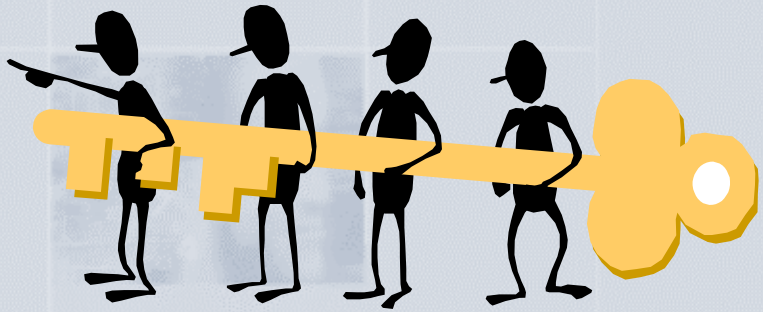
課後練習

瀏覽十個電子化政府或電子商務相關網站,記下其網址,

- 檢視有沒有掛上任何網路標章?
- 瀏覽其網站的隱私權政策,他們有沒有將民眾或用戶賣出或交易的權利?
- 該網站上有沒有使用Cookie?

☞ 瀏覽電子簽章法、電腦個人資料保護法、著作權法、通訊保障及監察法

網站防護



網站防護之一些問題

SSL 只能保證連結之網站收到的公鑰憑證不是偽造的,傳遞的個人資料在傳輸期間有經過加密不會被窺視,但不能保證這家公司本身沒有問題。就算這家公司本身沒有問題，也不能保證這家公司網站會不會成為別人入侵、竊取資料的目標?

網站防護之一些問題

資訊聚集攻擊(Information Gathering Attacks)

使用第三者軟體可能暴露用戶資訊

阻斷式攻擊

用戶簽退過程

緩衝區滿溢攻擊(Buffer Overflows)

伺服器端邏輯

網路瀏覽器安全性問題、

用戶密碼蒐集與破解

作業系統和網站伺服器端弱點

網站惡意程式碼之避免

- 你如何信任從網站所下載的程式碼?須確定
  - 誰出品此程式碼?
  - 程式碼之真確性(integrity)
- 受信任之軟體藉由
  - PKI應用程式提供 “軟體簽章” (code signing)
  - 鑑別性(Authentication):憑證機構簽發給軟體發行者一張特定的憑證.
  - 真確性 :軟體程式碼已經過數位簽章保護

ActiveX COM 元件安裝

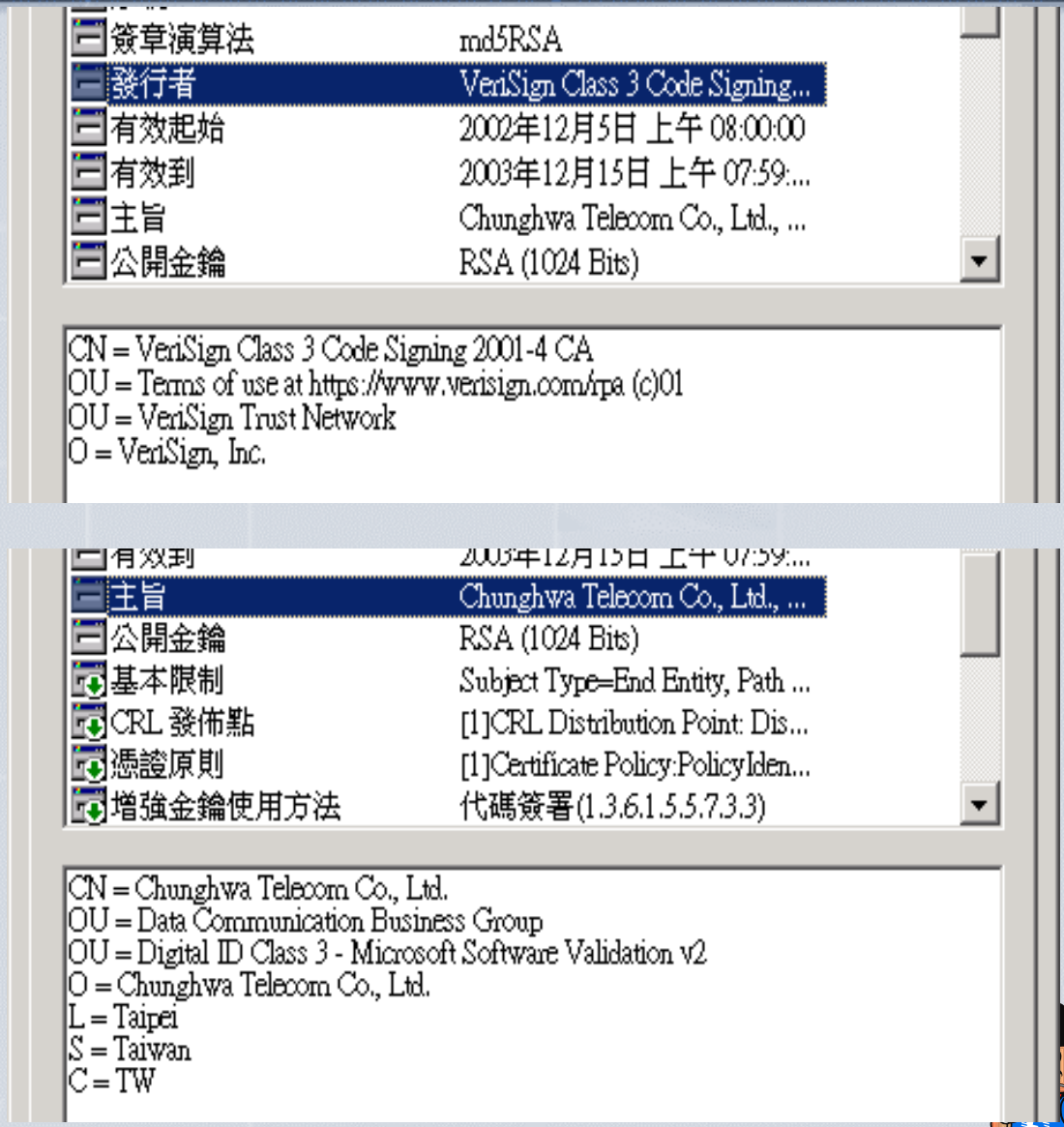
- 瀏覽器之安全性警告

程式碼之驗證(1)

☞軟體發行者之憑證

程式碼之驗證(2)

- 憑證簽發者
- 軟體發行者之名稱



程式碼之接受或拒絕

- 憑證之驗證已經成功

- 此公司可被用戶鑑別
- 用戶可信任此公司以及此公司所發行的軟體
- 因此用戶有信心可安裝此軟體

掃瞄工具及伺服器廠商安全資源

- Web Server廣泛用途的安全工具，在開放程式碼部分以www.nessus.org所提供的Nessus最有名
- 商用

  www.iss.net之ISS以主機式弱點掃瞄工具

  www.intrusion.com 之Security Analyst

- Windows: http://www.microsoft.com/technet/security/default.mspx；
  iPlanet:http://developer.iplanet.com/tech/security/；
  Apache Tutorials: http://httpd.apache.org/docs/misc/tutorials.html
- Security Tips: http://httpd.apache.org/docs/misc/security_tips.html

保護網站安全，以IIS為例

- 瀏覽目錄：最好關閉瀏覽目錄功能
- 控制指令碼目錄： Script 或 CGI目錄具備「僅指令碼」執行權。其他如讀取、寫入和目錄瀏覽等許可權，則要審慎評估。
- 在虛擬目錄設定適當的 ACL
- 設定 IUSR_*computername* 帳戶的存取控制權：保護匿名帳號
- 同步處理 Web 和 NTFS 許可權
- 設定適當的 IIS 記錄檔 ACL
  - IIS 產生之記錄檔 (%Systemroot%\System32\LogFiles)
  - 用記錄功能，而且最好能夠使用 W3C 延伸記錄格式，在擴充內容索引標籤上設定下列內容：
    用戶端 IP 位址、使用者名稱、方法、URI 主體、HTTP 狀態 、Win32 狀態、使用者代理程式、伺服器 IP 位址 。

虛擬目錄下的ACL

檔案類型	存取控制清單
CGI (.exe、.dll、.cmd、.pl)	每個人 (X) 管理員 (完整的控制權) 系統 (完整的控制權)
指令碼檔案 (.asp)	每個人 (X) 管理員 (完整的控制權) 系統 (完整的控制權)
Include 檔 (.inc、.shtm、.shtml)	每個人 (X) 管理員 (完整的控制權) 系統 (完整的控制權)
靜態內容 (.txt、.gif、.jpg、.html)	每個人 (R) 管理員 (完整的控制權) 系統 (完整的控制權)

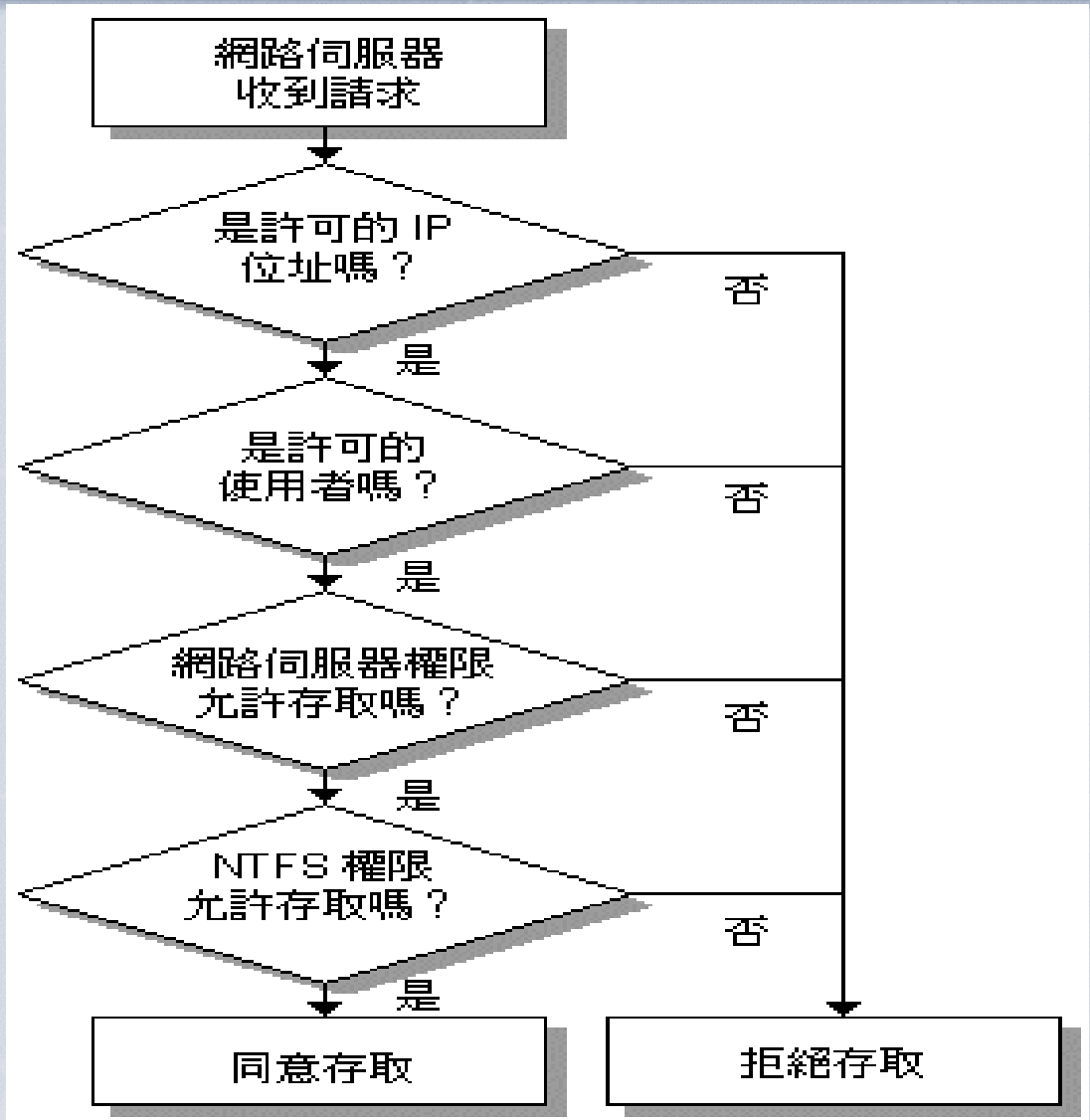
- 為每個檔案類型設定ACL目錄

C:\Inetpub\Wwwroot\Myserver\Static (.html)
C:\Inetpub\Wwwroot\Myserver\Include (.inc)
C:\Inetpub\Wwwroot\Myserver\Script (.asp)
C:\Inetpub\Wwwroot\Myserver\Executable (.dll)
C:\Inetpub\Wwwroot\Myserver\Images (.gif, .jpeg)

- 同時, 請特別注意下面這兩個目錄：

C:\Inetpub\Ftproot (FTP 伺服器)
C:\Inetpub\Mailroot (SMTP 伺服器)

IIS許可權流程圖


網路伺服器
收到請求
是許可的 IP
位址嗎？
否
是
是許可的
使用者嗎？
否
是
網路伺服器權限
允許存取嗎？
否
是
NTFS 權限
允許存取嗎？
否
是
同意存取
拒絕存取

保護IIS安全

- 停用或移除所有的範例應用程式
- 移除 IISADMPWD 虛擬目錄：這個目錄可以重設 Windows NT 和 Windows 2000 密碼
- 移除不用的指令碼對應：IIS 被預設要支援一般的副檔名，如 .asp 和 .shtm。當 IIS 接獲索取這類檔案的要求時，這個呼叫是由對應的 DLL 所處理。
- 套用最新的修正程式 ：
  http://www.microsoft.com/technet/itsolutions/security/tools/tools.asp

停用或移除所有的範例應用程式

範例	虛擬目錄	位置
IIS 範例	\IISSamples	C:\ Inetpub\Iissamples
IIS 文件	\IISHelp	C:\Winnt\Help\iishelp
資料存取	\MSADC	C:\Program files\Common files\System\Msadc

移除不用的指令碼對應

如果不用	請移除這個項目
Web 密碼重設功能	.htr
網際網路資料庫連接器	.idc
伺服器端 Include	.stm、.shtm 和 .shtml
網際網路列印	.printer
索引伺服器	.htw、.ida 和 .idq

網站稽核

稽核網站伺服器

☞高階的檢查表

1	獲得官方公司的政策、程序以及標準/指引，為求完整性，將之與最佳實務(Best Practice)比較，記下差異之處。尤其必須注意作業系統網站伺服器、第三方產品以及編碼的安全實務
2	對應相關安全政策與標準，稽核作業系統，記下其差異之處。
3	針對相關政策與指引稽核網站伺服器並記下其差異，尤其是不需要或有危險的檔案、網站伺服器的使用者帳號與權限、 Log檔案
4	以相關的政策、標準稽核第三方的軟體(例如Application Server)
5	記下相關補強(patch)程序與工具，如果遺失必須記下來
6	使用掃瞄工具並記下結果
7	掃瞄預設及實質的目錄
8	根據使用的軟體或網站產生弱點的表列例如透過 http://www.securityfocus.com/bid弱點資料庫或是根據供應商名稱、產品名稱以及關鍵字在 Cassandra網頁之https:// assandra.cerias.purdue.edu/main/index.html 入侵事件回應料庫產生弱點剖繪檔案)

稽核網站伺服器

- IIS 5.0基礎的安全檢查表

1	對於虛擬目錄設定適當的存取控制表(ACLs)
2	設定適當的IIS Log檔存取控制表
3	啟動Logging
4	移除所有的範例應用程式
5	移除所有的IISADMPWD虛擬目錄
6	移除不用的script mappings

稽核網站伺服器

- 隱藏的內容(Hidden Content)的安全檢查表

1	分析用戶端程式碼是否有不需要的資訊，例如註解(Comments)或Meta tags
2	從伺服器端分析HTTP協定是否有不需要的資訊，例如伺服器標頭檔Server Header、用戶的標頭檔(X-)
3	分析位址列(URLs)及鑑別碼(authentication credentials)是否有可能Java applets等被反組譯?
4	從每一個已知的目錄擷取robots.txt檔案並做檢視

稽核網站伺服器

- 加密與鑑別的安全檢查表

1	驗證所有顯示敏感資訊的的網頁都使用加密送出
2	驗證所有需求敏感資訊的的網頁都使用加密送出(例如可見SSL的加密鎖)
3	驗證所有需求敏感資訊的的網頁都將使用加密送出
4	執行加密模組清查，並以目前的最佳實務或政策確認

稽核網站伺服器

- 敏感性輸出的安全檢查表

1	是否使用加密?
2	是否顯示瀏覽器加密鎖
3	是否對於伺服器使用反快取(anti-caching)技術
4	是否對於使用者下載安全資料檔案提供告警訊息

稽核網站伺服器

- 鑑別方法(Authentication Method)的安全檢查表

1	用戶端憑證: 確保任何有PKI Enabled的系統都被稽核 測試被廢止之憑證能否被允許存取
2	Form-Based: 確保form方法為Post並使用加密
3	HTTP Basic Auth: 確保所有附帶信物的需求檔都被加密
4	所有的鑑別方法 參見Sign-On稽核方法

稽核網站伺服器

- Sign-On稽核方法

1	經法律核准的告警橫幅(訊息,warning banner)
2	使用簡要的錯誤訊息避免用戶資訊洩漏
3	所有牽涉信物(credentials)的都經加密
4	密碼輸入數次以上強迫登出機制(Confirm Lockout Mechanism) 降低暴力攻擊法
5	對於DDos之攻擊防範
6	登入程序若不活動則timeout以避免半開程序

稽核網站伺服器

- Sign-Off稽核方法

1	建議使用簽退(Sign-off)過程
2	確認網頁使用反快取(anti-caching)技術
3	是否在某交易期(Session)內不活動會自動簽退?

稽核網站伺服器

- 用戶輸入敏感性資料之安全檢查表

1	記下所有的Form方法，對於敏感性輸入必須使用post
2	參見encryption安全檢查表(SSL、frames等)

稽核網站伺服器

- 用戶輸入測試的安全檢查表

1	測試每一個form element --記錄使用的permutation list --記錄每一個verbose 錯誤訊息
2	測試所有作為輸出的HTTP標頭檔案 --記錄使用的permutation list --記錄每一個verbose 錯誤訊息

報告完畢
敬請指教