

# 財團法人台灣網路資訊中心

## 網路安全委員會第四次會議 會議紀錄

開會時間：九十一年三月十五日（星期五）下午 2:00~4:00

開會地點：台灣網路資訊中心會議室（台北市羅斯福路二段 9 號 4 樓之二）

主持人：陳年興主任委員

出席人員：

行政院研考會 何全德副處長 國防部通資局 秦雄飛副處長  
交通部電信總局 許錫蘭簡任技正(請假) 中研院資訊所 黃世昆研究員(請假)  
中華民國網路消費學會 林世華理事長(請假)  
財團法人資訊工業策進會 鄭祥勝顧問  
行政院主計處電子資料處理中心 劉勝東副主任  
中央警察大學 林宜隆教授 成功大學電機系 賴溪松教授  
交通大學資工系 謝續平教授(請假) 台灣大學電機系 雷欽隆教授(請假)  
中央大學資管系 陳奕明教授 中山大學資管系 陳年興教授  
中華電信數據通信分公司 林慶和科長 數位聯合電信公司 馮志弘經理(請假)  
昇陽電腦協銷系統工程 蘇炯心協理 台灣微軟股份有限公司 何俊明經理  
台灣網路資訊中心 許乃文組長、楊禎葆、陳玉萱  
台灣電腦網路危機處理中心 蕭群祐、周守廉、陳宗裕、王柔婷

記錄：陳玉萱

---

### 一、主席致詞：

本屆委員會新增 ISP 業者代表 (HiNet 與 Seednet) 與系統業者代表 (Microsoft 與 Sun)；學術界代表新增中央大學資管系陳奕明教授。

### 二、報告事項：

#### 壹、SNMP 漏洞的處理報告

報告人：TWCERT/CC 蕭群祐

報告摘要：

SNMPv1 漏洞由來已久，影響範圍擴及大多數使用到 SNMP 的軟硬體，包含系統、router、ADSL modem...等。系統方面，Unix-like 系統可被取得 root 權限，硬體設備方面，router、ADSL modem 會當機，造成對外網路斷線。Router 的當機對網路的影響較大。

解決方法有：

1. 請軟硬體廠商修正問題，但目前國內使用數量較多的 Zyxel ADSL modem 尚未出 patch；
2. 由網管人員在網段入口處攔截 SNMP 封包，但此方法可能造成不方便，另外仍可能由網段內部癱瘓自己的 router。

Microsoft 何俊明經理說明已在 2/15 釋出 patch，同時 SNMP 預設為不安裝。

## 貳、TWCERT/CC 會員收費系統及 SAS(Subscription-Auditing System)之報告

報告人：TWCERT/CC 周守廉

報告摘要：

遠端線上弱點掃描，可在 web 介面操作，容易擴充的後端弱點資料庫與 patch 資料庫，中文化報表。並對所掃描到的弱點詳細描述及說明解決方法。

會員可線上掃描、排程掃描、紀錄結果。TWCERT/CC 藉由 whois database 來限制會員只能掃描自己管理的網段。

SAS 系統主要是用於發佈安全通報後。能提供管理人員一項便於檢測的工具。

決議事項：

對於受檢測的主機資料，TWCERT/CC 內部應有控管制度，避免客戶敏感資料在組織內被任意流傳，並應有稽核制度。另應有責任歸屬宣告，說明掃描行為與結果的責任歸屬。如此才能建立公信力。

## 參、TWCERT/CC 年度工作計劃執行情形("TWNIC 對全國 DNS 安全防護之需求"執行情形)

報告人：TWCERT/CC 蕭群祐

報告摘要：

第一階段為第三階層網段 survey。第二階段需請 TWNIC 向第三階層發出通告，說明 TWCERT/CC 有檢測服務。TWCERT/CC 有提供獨立的檢測主機來服務 DNS server，檢測項目也不僅止於名稱服務的漏洞，而是檢測所有系統漏洞。檢測方式分為簡易與進階檢測。TWNIC 與 TWCERT/CC 每兩週固定舉行技術交流會議。

TWNIC 說明目前 DNS 的管理：目前有六部 DNS 及備援主機分佈於各網路，採用不同硬體與軟體(BIND 版本)，亦具有及時救援的機制。

決議事項：

可針對這一個議題，成立一個 DNS 的安全防護專業委託研究計畫。此委託研究計畫之需求請 TWNIC 併入委託 TWCERT/CC 之年度計劃中考慮。

### 三、提案討論

議題一：賴溪松教授研究計劃案審查(初審)。

說明：請參考附件〈網站安全認證機制規劃及系統開發〉

摘要：

本研究案目的在建置一套可用的、安全的網站認證發放與驗證系統，建構安全通道提供經過認證的網站一個合法標記，此標記的功用在提供一般使用者辨識此網站是否確為網站本身，而非被偽造的，以及標記的防偽功能。研究案內容請詳見計畫申請書與相關事項說明。

討論記要：

1. 本系統並不包括認證的行政程序，網站通過認證與否，需另訂配套措施。日本目前即已有完善的行政管理措施。
2. 認證之審核標準，行政程序，包含標記樣式，申請表格樣式等等，由 TWNIC 或相關單位訂定之。
3. 政府對於網站每年應有相關的檢查措施，包含網站的安全性檢查，營業方式，制度…等等之審查。
4. 應加強對使用者的教育，包括認證在網路交易扮演的角色與功用，以降低在網路交易承受的風險。
5. 認證若要被廣泛採用，必須為一個具有公信力或具政府公權力之機構來發放。
6. 此案之成果可提供 TWNIC 一套安全之發照機制，憑證的用途與審核程序請委員會提供相關意見。
7. TWNIC 可考慮扮演具公信力之機構，發放認證給商業網站。
8. 認證之標準應列出審核項目清單，例如網站安全認證應該有一串安全稽核項目，通過之網站才可發給認證。
9. TWNIC 網路安全委員會目前可以蒐集網安相關資料，提供給大眾知悉，但也要避免所提供的資訊造成商業網站無謂的損失。
10. TWNIC 應研究此認證機制可否使用於目前負責管理之國內 DNS 內。

決議事項：

1. 審查結果：初審通過
2. 建議事項：
  - (1) 針對研究案成果的品質、技術細節、運作方式，請研究案主持人提供具體方案，務必使本委託計畫之成果能夠具體拿來在實務上真正上線使用。
  - (2) 本次會議討論內容提供 TWNIC 在研究案內容與經費上作參考。

(3) 相關配套措施未來視用途再設計，討論。

議題二：SNMP 漏洞緊急防護及因應對策。

說明：SNMP(Simple Network Management Protocol)為運用在網際網路的一種通訊協定(服務)，通常是使用於網路設備的管理與監視。由於 SNMP 服務廣泛地使用在各類網路設備及作業系統中，影響的層面可能較為的深遠。此漏洞對於不同的產品之間可能會產生不同的影響，主要可能會造成的影響有阻斷式攻擊(DOS)、設備當機，進而造成網路中斷等。入侵者也可能利用此漏洞來取得不當的權限進行非法存取系統資訊。

決議事項：

1. 對於影響層面較大的弱點，請 TWCERT/CC 通知 GSN-CERT、N-CERT、軟硬體業者、電腦公會、軟體協會等，由以上各單位及時通報所屬的機構或廠商，來保障民間企業及政府單位的網路與主機。弱點通報內應說明檢測與修復的方法步驟。
2. 國內網路安全通報系統尚未健全，建議全力配合國家資通安全會報之通報體系，以落實資通安全體系之機制及功能。有關 DNS 安全之相關工作，建議持續委請 TWCERT/CC 於年度計劃中全力配合執行。

四、臨時動議

五、散會