「TWNIC 網路安全委員會」第十七次會議紀錄

開會時間：九十三年九月十日 星期五　下午 14:00~16:30
開會地點：台灣網路資訊中心四樓大會議室（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（林宜隆委員代）　**紀錄：**陳玉萱小姐
出席人員：
中央警察大學 林宜隆教授　東吳大學資管系 楊欣哲教授
精誠資訊股份有限公司 張輝觀協理(江嘉帆代)　樹德大學資管系 鄭進興教授
中華民國網路消費學會 林世華理事長　中山大學資管系 陳年興教授(林宜隆委員 代)
昇陽電腦股份有限公司 戴碧勳副總經理(請假) 淡江大學資訊中心 黃明達主任(請假)
台灣微軟股份有限公司 傅昭凱經理　電信總局公眾電信處 周永津科長(請假)
數位聯合電信公司 張富吉經理　中華電信數據通信分公司 林慶和科長(黃安賜先生 代)
優易資訊公司 陳勇君副總經理　國防部資通室　柴惠珍處長(由代理人員出席)
資訊管理學會 蕭瑞祥秘書長　行政院主計處電子資料處理中心 劉勝東副主任
台灣網路資訊中心 陳玉萱小姐及相關人員
台灣電腦網路危機處理暨協調中心相關人員
列席指導人員：
行政院國家資通安全會報綜合規劃組　陳如芬主任(方鴻春先生代)
行政院國家資通安全會報技術服務中心　劉培文主任

一、主席致詞(略)

二、報告事項

(一) 近期發布的重大弱點報告。

1. 報告摘要：請參考會議資料。
2. 討論及決議事項：目前網蟲肆虐的狀況依舊名列每月統計表前三名，企業及組織應妥善建立相關的修正管理及程序因應流程，以杜絕系統重複感染的可能性。

(二) 國際組織交流報告(略)。

(三) TWCERT/CC 簡介 SAS 弱點資料庫所提供的各項服務(略)。

(四) 本委員會建請行政院國家資通安全會報報告新的組織架構。

1. 報告摘要：請參考會議資料。
2. 討論及決議事項：此次簡報讓委員了解行政院國家資通安全會報的新組織架構，統合了分散於各相關政府單位的資源及功能，使各相關單位於資安事件發生之第一時間，能依照事件大小及嚴重程度來研判因應，並快速作出最適當的處理。

(五) 請本委員會之優易資訊、技服中心、東吳大學等產官學各界單位代表簡報 SOC 之功能、角色與定義等議題(報告時間為 15 分鐘)。

1. 報告摘要：請參考會議資料。
2. 討論及決議事項：請參考討論題綱。

(六) 報告 DNS 安全檢測及事件紀錄分析機制實作研究計畫進行情形。

1. 報告摘要：請參考會議資料。
2. 討論及決議事項：請參考討論題綱。

三、討論提綱

(一) 請各委員就今日產官學各界簡報 SOC 之功能、角色與定義等，建議未來國家及民間 SOC 的合作等相關議題。

1. 討論及決議事項：

(1) 本次報告分別以產官學界不同的角度來闡述 SOC 的功能、角色與定義，也說明了各種不同層面與規模的組織適用的 SOC 機制及成立時所需注意的必要條件。對於日益注重資訊安全的企業及組織來說,如何建立一個適合的 SOC 機制是很重要的。

(2) 目前政府及民間對 SOC 的定義及規範不盡相同,建議未來國家應制定 SOC 的資料共通規格，以促進彼此資訊交換及協防機制之共通。

(二) 請各委員就今日報告 DNS 安全檢測及事件紀錄分析機制實作研究計畫進行情形提供建議。

1. 討論及決議事項：

建議此計畫能藉由日益增長之 log 自動累積、學習與 DNS 資安事件相關之特徵值(pattern)成為 DNS 專家資料庫。

(三) TWNIC 目前所提供的 DNS 服務是否可以搭配 TWCERT/CC 的 SAS 檢測，以提供更有效的服務給更廣大的使用者。

1. 討論及決議事項：

以 TWCERT/CC 的中立角色及公信力而言，提供此項服務實為可行，但是在檢測報告的可信度部份，建議必須加註『此檢測報告是以當次掃描時間為準，非提供長期監測服務』字樣為佳。未來如有考慮在 TWNIC 之 DNS 相關服務搭配檢測服務，建議應提供消費者自行選擇『是否同意使用 SAS 檢測附加服務』之自由。

(四) 討論下一次會議召開時間。

1. 討論及決議事項：

預定下一次會議於 93 年十一月十二日下午 14:00 至 16:00 舉行。

四、臨時動議

1. 建議下次可增加的報告主題

(1) 建議可請傅委員介紹微軟企業內部因應系統安全的管理程序。

(2) 本次會議上討論到 SOC 之基本規格,建議可由優易資訊陳委員協助統整後提出報告供大家參考。

五、散會