財團法人台灣網路資訊中心

網路安全委員會第七次會議會議紀錄

開會時間：九十一年十二月十八日（星期三）上午 10:00 至 12:30
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(請假)　　國防部通信資訊參謀次長室　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
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(請假)
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(請假)　　成功大學電機系　賴溪松教授(請假)、陳坤元先生
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
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(請假)　昇陽電腦股份有限公司 戴碧勳協理（請假）
台灣微軟股份有限公司 傅昭凱經理
台灣網路資訊中心　　許乃文組長、陳玉萱小姐、楊禎葆先生
台灣電腦網路危機處理暨協調中心　　鄭進興教授、蕭群祐先生、周守廉先生、魏銷志先生、陳宗裕先生、林岳生先生、吳孟翎小姐

記錄:陳玉萱

一、**主席報告：**(略)

二、 報告事項：

1. TWCERT/CC 年度計劃執行情形報告

題目一：TWCERT/CC 網路安全相關工作任務執行情形
報告人：TWCERT/CC 魏銷志先生
報告摘要：(1) 報告內容請參閱會議資料。

(2) 針對國內外 IR 處理狀況分析，國外 IR 大多屬於通報性質(complaint letter;而國內 IR 則多屬遭受入侵的求助，另外有一部分是中了求職信病毒的詢問。

(4) TWCERT/CC 對於 ISP 並無強制力, 對於國外通報的 IR, TWCERT/CC 僅能通報給國內的 ISP, 並將 ISP 所回應的處理方式告知國外的通報單位。

(6) TWCERT/CC 的 IR 主要是以已經發生的事件為主, 除了通報表格的資料蒐集外, 後續並會以電子郵件或電話與對方聯繫, 以得知較完整的事件狀況及網路建置環境, 是否建置無線連線環境可由此管道得知。

建議事項：請 TWCERT/CC 針對下列事項進行補充或改進：

（1） 統計 IR 報告中的 IP 範圍，依據 ISP 來分別統計，並特別注意次數較多的 ISP。

（2） IR 回報的表格中，建議增加一個項目，請回報者告知是否有建置無線上網環境，以作為處理 IR 的一個判斷項目。

題目二：近期發布的重大弱點報告及 ROOT Servers Attacks Report

報告人：TWCERT/CC 陳宗裕先生

報告摘要：

（1） 報告內容請參閱會議資料。

（2） DNS 根伺服器遭受攻擊的時間大約在台北時間 2002/10/22 星期二上午 4:45，全世界主要 13 部 DNS 根伺服器遭受攻擊。主要的攻擊方式是以大量 ICMP 封包進行分散式的阻斷攻擊，使得 ICMP 的量為平常的 30-40 倍，而時間大約持續一個小時，造成 7 部 DNS 根伺服器癱瘓，及另 2 部僅能間歇性的運作。但因受創時間沒有持續延長，所有大部份使用者沒有感覺到異狀，而網路的連通運作也沒有受到更嚴重的影響。

（3） 過去以攻擊企業或某一單位組織為主，而這次的攻擊的目標是針對整個網路的基礎建設。

建議事項：建議 TWNIC 建立一套應變措施，以因應萬一國內六部 root server 遭受攻擊時，能夠緊急應變維持正常運作，並建議估計需要在幾部 Server 正常運作的情況下才不會影響網路使用。

三、 討論題綱：

議題一：討論變更委員人選

說明：1. 台灣微軟股份有限公司原委員為何俊明經理，擬改派傅昭凱經理擔任委員，提請討論。

2. 昇陽電腦公司原委員為蘇炯心協理，擬改派戴碧勳協理擔任委員，提請討論。

決議事項：何俊明、蘇炯心委員因有其他的職務任用，遂改派傅昭凱、戴碧勳委員，全體委員無異議通過。

議題二：網站安全認證機制規劃及系統開發計劃期末報告

報告人：成功大學陳坤元先生

報告摘要：(略)

決議事項：通過本案期末報告。

議題三： DNS 伺服器安全檢測與防護體系之建置與運作計劃期中報告

報告人：中山大學鄭進興教授

報告摘要：(略)

決議事項：

1. 通過本案期中報告。
2. 針對未來推動我國 DNS 安全方面的工作，建議考慮下列建議之可行性。
   （1） 目前申請使用 DNS 安全掃描系統之服務者約有 800 人次，相對於全國 DNS 主機的數量來說相對少很多，建議應有加強推廣的機制，例如：加強突顯 DNS 安全掃描重要性、增加提供服務之網站連結、列入 DNS 的教育訓練的相關主題中。
   （2） 增開網路形式之 DNS 技術教育訓練課程，未來並考慮 DNS 技術方面的證照認證制度。
   （3） 本檢測系統是 TWNIC 以專案委託計劃開發的，建議考慮往後是否仍然繼續以專案方式提供 DNS 檢測服務，或是考慮將此服務做為申請 domain name 的附加服務項目，並考慮每年收取 domain name 續用費用時同時收取檢測的服務費。
   （4） 請委員提供收取檢測服務費的具體建議，下次委員會提出討論。

議題四：TWCERT/CC「台灣地區網路伺服器年度調查研究」計劃執行情形討論

報告人：中山大學鄭進興教授

說明：此系統 TWCERT/CC 已在 6 月份發展完成，其目的為建立網路節點之系統平台與應用服務之資料庫，同時增進自動化分析的能力，使得能在最快時間掌握最新網路資訊狀況，並以台灣網域作為實測的目標。

決議事項：

1. 建議了解 TWCERT/CC 之全國網站安全檢測風險評估指標中，今年和去年的 DNS 整體性安全指標有何不同，以分析了解 DNS 安全掃描服務施行以來改變的情形。
2. 建議針對 DNS 伺服器之檢測方式，能提供由使用者自行啟動的機制，提供非破壞性的檢測方法。
3. 建議請 TWCERT/CC 將歷年來大規模的網站安全檢測情形，依各年度資料統計歸納分析，未來提至本委員會議中報告。

議題五：我國網際網路骨幹之整體流量、收集、統計與分析之規劃

報告人：中山大學鄭進興教授

說明：(略)

決議事項：因時間的關係移至下次委員會再進行討論。

議題六：討論 TWNIC「資通安全緊急應變計劃暨作業處理程序」及成立「資通安全處理小組」

報告人：TWNIC 陳玉萱小姐

說明：依據交通部電信總局來函，請各重要公民營事業機構成立「資通安全處理小組」

常態任務編組，負責處理安全預防及危機處理相關事宜，並落實資通安全事件之危機通報及緊急應變作業。TWNIC 草擬「資通安全緊急應變計劃暨作業處理程序」（草案），提請討論。

決議事項：

1. 請 TWNIC 配合交通部電信總局來函，儘速成立「資通安全處理小組」。
2. 有關 TWNIC「資通安全緊急應變計劃暨作業處理程序」，提供下列參考建議：
   (1)建議儘量調整以條列式或依先後流程為順序的文體較為簡捷。
   (2)建議加強本小組與上層單位間縱向以及各工作組間橫向的運作機制。
   (3)建議並重平時的安全預防及事發時的即時應變危機處理的運作機制。
   (4)建議確立本小組之核心成員並設立緊急聯絡電話等聯絡方式，以因應突發狀況時緊急聯絡之需。

四、 臨時動議：

五、散會