

「TWNIC 網路安全委員會」第八次會議會議紀錄

開會時間：九十二年四月二十五日 星期五下午 14:00~17:00

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：

中央警察大學林宜隆教授
中山大學資管系陳年興教授
台灣大學電機系雷欽隆教授（請假）
國防部通資局秦雄飛副處長（請假）
精誠資訊股份有限公司 張輝觀協理
中華民國網路消費學會 林世華理事長
寬華網路科技股份有限公司 周頌鈞協理
台灣微軟股份有限公司 傅昭凱經理
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 陳文生執行長、許乃文組長、陳玉萱小姐
台灣電腦網路危機處理暨協調中心相關人員

東吳大學資管系 楊欣哲教授
樹德大學資管系 鄭進興教授
淡江大學資訊中心 黃明達主任（請假）
中研院資訊所黃世昆研究員（請假）
數位聯合電信公司 馮志弘經理
電信總局公眾電信處 周永津科長
昇陽電腦協銷系統工程 戴碧勳協理
中華電信數據通信分公司 林慶和科長

列席指導人員：

資通安全會報綜合業務組方鴻春主任（請假）

技服中心 辜國隆主任（請假）

一、主席報告：

1. 介紹第三屆委員暨委員致詞：略

二、報告事項

1. DNS 伺服器安全檢測與防護體系之建置與運作計畫執行情形報告(鄭進興教授)

(1) 報告摘要：略

(2) 建議事項

- A 攻擊與漏洞間的關係應詳加解釋，使非技術人員亦能了解其弱點、漏洞所產生的影響；此外應對統計數據作解釋與建議如何做修補與防護。
- B 相關弱點或漏洞的檢測程式更新，應建立相關程序，在一定時間內新增。
- C 使用 DNS 檢測系統的人數偏少之原因為該系統只剛剛建置上線一年，許多人還不瞭解，建議利用 TWNIC Newsletter 與 DNS 專欄來廣為宣傳，並應該於 TWNIC 的 DNS 訓練時安排專門場次介紹。
- D 建議檢測項目為不收費，開放予以所有用戶使用，而後續對於檢測報告進一步說明及修補防護的顧問服務才收取費用。收費方案待後續規劃題綱討論。

2. TWCERT/CC 網路安全工作執行報告(TWCERT/CC 魏銷志)

(1) 報告摘要：略

(2) 建議事項：

Slammer Worm 與 Deloder Worm 病毒至今仍傳出零星災情，建議網路及系統管理者從帳號控管與網管政策著手，如：訂定強韌的密碼原則、

限制 TCP Port 445、139 存取，及相關修補程式修補政策。

3. 近期發布的重大弱點報告 (TWCERT/CC 陳宗裕)
 - (1) 報告摘要：略
 - (2) 建議事項：

應注意防範漏洞不斷地產生，修補時程縮短，以及被後門程式利用的影響情形及嚴重性。
4. APCERT 成立大會及目前運作現況報告(TWCERT/CC 陳宗裕)
 - (1) 報告摘要：略
 - (2) 建議事項：

原本已經協調國內由 TWCERT/CC 代表參與 APCERT 委員會之選舉，可是因為技服中心臨時也以 TWCIRC 的名義加入提名，投票結果 TWCERT/CC 獲得七票，TWCIRC 獲得三票，造成雙雙落選。建議日後儘量整合我國現有之兩個 CERT 相關組織，於參與 APCERT Steering Committee 推選等活動時，儘量避免類似這次選票分散而未能獲選的情形發生。
5. TWNIC DNS 系統列為影響國家安全、社會安定之重要二十個資安作業系統現況報告 (TWNIC 許乃文組長)
 - (1) 報告摘要：略
 - (2) 建議事項
 - A SOC 部分建議以功能編組方式執行，非建置實體辦公室或設備形式。
 - B ISMS 建議分為兩階段來導入，並以功能相關之導向為範圍來進行會較快，而不是進行全組織的導入。
 - C 人員證照部份，並非一定要求取得 BS7799 稽核認證，其他安全認證應該也可以考慮，例如 TWCERT/CC 所舉辦的網路安全認證。
 - D 應衡量費用與成本並視其情況選擇最適方案。
 - E 進行風險管理，確定 DNS 系統是安全幸無虞才是主要的工作目標。

三、討論提綱

1. 討論 DNS 安全掃描服務收費方案與執行面的議題。
 - (1) 說明：DNS 安全檢測服務辦法草案 (略)，請參閱會議資料。
 - (2) 討論及建議事項：
 - A. DNS 安全檢測服務應為免費之服務，建議檢測時不收取費用，若考慮收費，建議是針對檢測完後，提供檢測報告的進一步說明與修補顧問等服務，才考慮收取相關費用，並可結合業者搭配相關後續服務的方式進行。
 - B. 建議收費草案對個人用戶與企業之收費方案要區分，特別是對於子網域的收費方案應再行細部規劃。
 - C. DNS 安全檢測服務辦法草案有關資料保護的部分建議加入個人資料保護法；智慧財產權的保護部分，建議將「均受中華民國著作權法及國際……」一段修改為「均受中華民國智慧財產權相關法規及國際……」。

- D. 目前 DNS 安全檢測服務為 TWNIC 提供給用戶的免費服務，如有考慮針對檢測完後，提供檢測報告的進一步說明與修補顧問等服務，才考慮收取相關費用。若考慮由 TWNIC 直接向用戶收費的構想，尚需經 TWNIC DN 委員會決議與電信總局的相關程序。
2. 討論國內網路伺服器主機被大量植入後門程式的因應之道？(請 ISP 業者提供相關資料及意見)
- (1) 說明：目前在區網中心發現大量的網路伺服器主機被植入後門程式，情況嚴重，建請各委員提供因應之道。
- (2) 討論及建議事項：
- A. 建議各 ISP 業者考慮組成相關聯盟，如發現網路伺服器主機被植入後門程式，彼此協助共同研商因應之道。
- B. 建議相關業者研究可能之檢測技術等，最後能夠有預警的機制，並能每年定期舉辦網路安全入侵與防衛的聯合研習。
3. 討論各大骨幹網路流量異常監測機制。
- (1) 說明：TWNIC 今年內將徵求一計畫進行骨幹網路流量異常監測機制研究，冀望能夠藉此找出特定的流量之異常 Pattern，早期發現攻擊或是病毒對於網路安全的傷害。
- (2) 討論及建議事項：
- 建議委請寬華網路科技股份有限公司周頌鈞委員與精誠資訊股份有限公司張輝觀委員，提出可行的規劃方案與技術方法建議。請於下一次會議時，提出來供委員們進一步討論出 CFP，然後公告給有興趣的單位以委託計畫的方式來執行。

四、臨時動議

1. 建議預定第九次「TWNIC 網路安全委員會」會議開會時間。
- (1) 說明：下一次網安委員會開會時間建議於 92 年 6 月 6 日。
- (2) 討論及決議事項：經協調各委員，暫先預定於 92 年 6 月 6 日，召開第九次「TWNIC 網路安全委員會」會議。

五、散會