# 財團法人台灣網路資訊中心

# 「TWNIC 網路安全委員會」座談會 記錄

**開會時間：**九十年九月二十一日（星期五）上午 9:30~11:30
**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
**出列席人員：**
中山大學資管系　陳年興教授　　中央警察大學　林宜隆教授
成功大學電機系　賴溪松教授
本中心　曾憲雄董事長、陳文生執行長、許乃文組長、楊禎葆先生、陳玉萱小姐
台灣電腦網路危機處理中心　蕭群祐先生、周守廉先生、梁慧芬小姐
**記錄：梁慧芬**

---

**一、　主席報告**

因適逢美國 911 恐怖攻擊事件，多位委員滯留美國，加上台北 917 水災也有多位委員忙於災後復原的工作，因此出席委員不足，本次委員會議改成座談會。

**二、　報告事項**

1. TWCERT 工作執行報告(略)
2. TWCERT 申請加入 FIRST 進度報告(略)
3. TWNIC 委託 DNS Security 執行報告

**報告人：**TWCERT 蕭群祐
**摘要：**(略)
**主席裁示：**

(1)第二階段剛完成初步的檢測，手動檢測的部分尚未完成，請 TWCERT 儘快完成第二階段的檢測，並提供具體檢測報告。

(2)對於委員提出網際網路是公共財的概念，對於放在網際網路上的 server，應要求必須具備某一水準的安全性，以確保資訊安全。建議以行政命令或立法，以強迫的方式規範網路安全。相對於日本有 online mark 和 privacy mark，我們也可以發展一套網路安全的分級制度。這部份請賴溪松賴教授下次委員會時就技術面提供 security mark 的資訊來討論。也請林宜隆林教授就行政面、法規面的角度提供 certification procedure 的資訊來進一步討論，並訂出具體可行的方案來推動。

4. Code Red 網蟲癱瘓網路正常運作事件處理報告

**報告人：**TWCERT 周守廉

**摘要：**預測新的網蟲 Nimda 有可能造成和 Code Red 一樣嚴重的後果。

**主席裁示：**TWCERT 應扮演類似網路中央氣象局的角色。委員會應有預警的功效，在災害尚未發生前，整理出漏洞發生的原因、如何防治及風險評估，召開記者會引起大眾對這件事情的重視並採取預防措施。請 TWCERT 提供相關資訊，與 TWNIC 的公關配合，安排一個記者會，並請林宜隆林教授擔任記者會主持人，對媒體發布消息、教導民眾以正確的態度及方法來面對可能發生的災害。

## 三、 提案討論事項

**議題一：如何有效防治類似 Code Red 網蟲所造成的危害？**

**結論：**

一、網路節點的流量管理：

應要求各單位網管中心加強網路節點的流量控制，尤其是在主幹網路或重要 subnet 所下放的 ip 分配管理中心，應安裝流量管理軟體，架設入侵偵測系統。一旦發現有某些主機的流量異常增加，應立即通知該主機的使用人員，甚至暫時中斷其網路連線，以避免災情擴大。

二、社會大眾的網路安全教育：

對於一般大眾而言，Windows 2000 較 win9X 與 win ME 系統穩定，因此往往安裝 Windows 2000 當作 win 9X 使用，而忽略了其額外伺服應用程式的安全處理。因此應教育民眾，依據電腦的使用需要，安裝相對應的作業系統；或對於安裝伺服器作業系統的使用者，宣導其注意相關的漏洞通報與安全修補。

三、媒體工作者的宣導：

對於這次的 Code Red 事件，雖然國內的 TW-CERT、GSN-CERT、趨勢科技及鈺松科技等網路安全廠商有發布警告消息，並提供解決的方式，但一般大眾最常接觸的新聞媒體，往往僅提出 Code Red 的警告消息與災情報導，甚少教導社會大眾如何清除網蟲、如何修補漏洞。因此，建議以後可製作宣導帶或以廣告的方式，透過媒體傳播的能力，將警告消息及修補訊息廣為宣傳，以其達到降低災害的目的。

四、區域聯防的相互支援：

Code Red 網蟲還突顯出一個問題，便是各家網路安全廠商、TWCERT 與 GSN-CERT 分別提出了 Code Red 的清除程式與修補方式，各家所提供的解決方式難易有差，且眾多的選擇方式往往造成民眾無所適從。建議政府單位應有效統合這些資源，交由專人進行測試並依操作之難易程度分類，最後由國家資通安全處理機構統一在網頁上發布消息，這樣民眾才有可依循的處理方式。此外，TWCERT 與 GSN-CERT 所發布的通報與災害統計往往是全國性的，

建議可藉由各地的區域聯防中心提供災害情報給中央處理單位，對於受害較為嚴重的地區，加強資訊安全的宣導，或派員協助處理，如此相信更能有效的運用資源，也更能精確的得知災害的程度。

**議題二:作業系統供應商因系統漏洞造成使用者權益的重大損害所應負的責任探討**

主席決議：下次會議討論

**議題三：TWNIC 對全國性 DNS 安全防護之需求與討論**

TWNIC 對全國性 DNS 安全防護提出下列五項需求：

1. 建議匯集提供關於 BIND、Windows DNS Server…..等，各類作業系統平台及版本所有之 DNS 系統漏洞列表、安全資訊及相關升級建議，並將匯集之資訊定期公佈於 Web Site 並隨時即時更新。

2. 建議提供相關規劃、技術及工具，以及對全國第一、二、三層 DNS 作遠端掃描、偵測等之安全檢測工作，並分析結果以了解國內一般使用者 DNS 安全性之情形。對具破壞性及非破壞性之掃描及偵測之工作階分別提供恰當之檢測服務機制及做法。每月提供全國 DNS 掃描、偵測等之安全檢測情形之檔案並於網路安全委員會議中報告。全國第一、二、三層 DNS 安全檢測工作之範圍簡述如下：
   (1)對第一層.tw DNS 之安全檢測工作
   (2)對第二層.com.tw，.org.tw，.net.tw，.edu.tw，.gov.tw，.idv.tw 等 DNS 之安全檢測工作
   (3)對第三層由全國使用者註冊建置之 DNS，目前為數約 50,000~60,000 台 DNS 之安全檢測工作

   對於如何定期完成為數龐大的第三層 DNS 之安全檢測工作，並避免因偵測所造成之類似攻擊行為，建議提供可行之執行方案。

3. 建議根據對全國第一、二、三層 DNS 做遠端掃描、偵測等之安全檢測的結果，規劃出可行的 DNS 安全補強建議方案，對於一般共通性、整體性之補強方案建議定期公告於 Web Site，如屬個別性之資訊則與 TWNIC 配合提供給 DNS 管理者，建議其確實加強 DNS 安全防護工作，以普遍提高全國 DNS 環境的安全性。

4. 建議整體規劃並按月定期舉辦全國有關 DNS 安全防護之專業技術教育訓練、研討會。

5. 建議於 Web Site 提供 DNS 安全防護觀念及相關技術專業資訊之專區，並定期出刊 Newsletter 報導 DNS 安全檢測、防護及技術之最新情形與趨勢。

**討論與決議：**依據各項需求，主席之裁示如下：

1. 將請 TWCERT 在一個月內提供關於 BIND、Windows DNS Server…..等，各類作業系統平台及版本所有之 DNS 系統漏洞列表、安全資訊及相關升級建議，並將匯集之資訊定期公佈於 Web Site 並隨時即時更新。

2. 對於如何完成數量龐大的第三層 DNS 之安全檢測工作，建議可按照賴溪松賴教授所提出的程序，第一個步驟是檢測，第二個步驟是 training，配合 TWCERT 所舉辦的網安課程，要求檢測結果是比較有漏洞的單位來參加 training program；第三個步驟是改善，第四個步驟則是稽核、追蹤。至於要如何執行，則必須要擬一具體之執行方案，包括方法、程序、步驟、時程，並取得區域協助。此一執行方案由 TWCERT 研擬，並在下次委員會議中提出討論。

3. 網路安全委員會應建立專業的 Reputation，使外界得以信賴所提供的資訊並願意配合、落實安全補強建議。此需求與第一項需求配合，一同公告於 web site。

4. 教育訓練與研討會可逐漸朝向收費的制度舉辦或與其他單位合辦。同時，對於參加教育訓練的網管人員，希望將來可做到授與證照，以提昇參加教育訓練的附加價值。

5. 將所有委員加入 TWCERT 的 Newsletter 的 mailing list(每月發布一次)，其他如 advisory 發布的頻率較高，為避免造成資訊超載，請有意願的委員另行上網訂閱。

**議題四：如何提昇各界對網路安全的認知與重視程度？**

**結論：**

1. 對一般使用者而言：

一般民眾對於網路系統安全的認知相當匱乏，建議可製作網路安全教育帶，以廣播電視等媒體的傳播力量，教育社會大眾正確的網路安全觀念。此外，對於各級學校的電腦網路課程，也可加入網路安全方面的教材，從教育著手，才是真正的治本之道。

2. 對網管人員而言：

督促網管人員參加網路安全課程。政府應提供網管的證照制度，證照每定期應重新認證考核，使網管人員的素質維持一定的水平。

3. 對企業網路而言：

企業在架設網路伺服器環境時，除繼有伺服環境的建置外，亦應參考 BS7799(ISO 17799)。此外，政府單位也可參照類似制度，發放相關證照；對於未來申辦網路事業相關的企業團體，亦需通過相關的檢驗之後，才准予發放營利事業證件。

**四、 臨時動議**

**五、 會議總結：**

1. 請 TWCERT 提供新一波網蟲 Nimda 的相關資訊，與 TWNIC 的公關配合，安排一個記者會，並請林宜隆林教授擔任記者會主持人，對媒體發布消息、教導民眾以正確的態度及方法來面對可能發生的災害。
2. 下次委員會請賴教授及林教授分別提供技術面及程序面的網站 mark(網站安全認證等級)的相關資料，以供討論。
3. 一個月內提出執行第三層 DNS Security 檢測的具體方案。
4. 近期之內召開第二次委員會議。
5. 請 TWCERT 儘快完成第二階段的 DNS 安全檢測具體報告、各類作業系統平台及版本所有之 DNS 系統漏洞列表、安全資訊及相關升級建議、規劃可行的 DNS 安全補強建議方案。

**六、 散會**