

# 財團法人台灣網路資訊中心 網路安全委員會會議紀錄

## ■第三次網路安全委員會會議紀錄

開會時間：九十一年一月十六日（星期三）上午10:00~12:00

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：

中研院資訊所 黃世昆研究員

中央警察大學 林宜隆教授

國防部通資局 秦雄飛副處長

台灣大學電機系 雷欽隆教授

成功大學電機系 賴溪松教授

中山大學資管系 陳年興教授

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 楊楨葆先生 陳玉萱小姐

台灣微軟解決方案行銷部 劉念臻經理

台灣微軟行銷處 王嘉玲經理

台灣電腦網路危機處理中心

陳嘉玫組長 鄭進興組長 蕭群祐先生

王柔婷小姐

紀錄 王柔婷

**壹、主席致詞：略**

**貳、報告事項：**

1. TW-CERT 90年度工作成果報告

報告人：鄭進興教授

參考文件：

<TWCERT 九十年度工作成果\_鄭進興老師.ppt>

## 報告摘要：

- (1) 處理國內外網路安全事件：IR成長相當迅速截至目前國內外IR各有500多件，值得大家高度重視。
- (2) 舉辦網路安全教育訓練：我們總共舉辦了六場研討會其中有與TWNIC合辦，效果相當不錯。
- (3) 協辦網路安全教育訓練：協辦四個研討會。
- (4) 全國DNS安全防護檢測：由TWNIC委託針對第一層、第二層DNS做檢測，分為三步驟：1.網路安全架構檢測；2.區域內所有主機安全檢測 3.DNS服務檢測。以上檢測已完成。91年度將針對第三層DNS進一步檢測。
- (5) 校園網路安全檢測：每一大學都有相當大的網路頻寬，我們針對中山大學做檢測。檢測結果顯示，校園網路安全值得大家重視。
- (6) 全國Web Server安全檢測：總共檢測5萬多台web server，在比例上顯示19.6%的web server有漏洞，也就是說在100台Web Server中約有20台有漏洞。依據三年統計顯示，Web Server 與經濟發展有關，就漏洞的百分比而言，去年跟今年都是19%左右，漏洞的改進與修補值得我們注意。
- (7) 特別時期緊急應變小組：中美駭客資訊戰監控，520政府網站安全檢測及監控，對總統府、立法院等政府機關進行監控；雙十國慶政府網站安全的檢測及監控，持續監控Code Red、Nimda所造成的影響，並及時提出解決方案，找出受感染主機清除餘毒，減少威脅。
- (8) AusCERT參訪。
- (9) 成為FIRST會員。

## 主席：

過去一年來，TWCERT還有協助技服中心網頁的監控管理，並在今年十月正式加入FIRST拿到PGP key，成為台灣網路安全的對外窗口，可以拿到FIRST所有第一手資料，與其他相關資訊。另外，還有協助主計處辦理資通安全外部稽核，成果卓著。目前TWCERT定期將資訊report給交通部電信總局以及NICI，如何提供最好的服務給社會大眾，是我們關心的一大重點，也是接下來的工作目標。

## 2. TWCERT 91年度工作計劃

報告人：陳嘉玫教授

參考文件：<TWCERT 91年度工作計劃\_陳嘉玫老師.ppt>

## 報告摘要：

TWCERT 91年度的工作目標有三個方向：

- (1) 推廣會員制度，並使我們的服務做的更好。
- (2) 工作計劃延續去年的成果，並加強功能。

(3) 推動區域聯防的觀念。

依據以上三個工作目標所擬定之工作項目為：

- (1) 執行第三層DNS安全檢測。
- (2) DNS security資源網站之維護與DNS安全資訊收集：以第一、二層為主。
- (3) 建置自我安全檢測系統(Self-Auditing System)。
- (4) 維護及強化TWCERT服務：提供自動檢測系統、提供中文化建議書、新弱點及修補程式。
- (5) 推廣會員制度，提供更好的服務。
- (6) 全國網站安全性調查。
- (7) 弱點資料庫：可為會員提供查詢及分析服務。
- (8) 積極與國際交流。
- (9) 推動區域聯防體系。

### 3. 網站安全認證制度之技術面報告

報告人：賴溪松教授

參考資料：<網站安全認證制度之技術面報告\_賴溪松教授.ppt>

報告摘要：

網站印記的現況：

**privacy mark**：企業電子化，經過適當的評估後，資料在此有相當程度的管控，只要有此印記的網站，表示是可信賴、可靠的商家。目前已正式開放申請且正式在運作。

**Online Mark**：逛到一網站時，要如何知道這個網站是合法的、可信賴的？網路上的虛擬商店，應有一實體的商店存在。商店有營利登記證後再申請虛擬商店，一些交易有可能產生的相關問題、爭議在經過認證後，可以降低許多。

**Security Mark**：為前者的再延伸，這標誌表示消費者可以完全信任的在此網站消費，可以建立起消費者的信心。

而Mark放在網頁上，很容易被copy，如何知道Mark的真假，則需要有第三公正單位來提供認證。

認證系統的特色：希望能跨平台，較有安全性，技術由我們自行發展，較無其他問題。認證機制則可由政府公權力或透過TWCERT會員制建立，會員經過掃描、report，然後取得認證，在管制之下受管理，是屬於較安全、較無庸置疑的。

結論：

使用者在進入一網站時，如何確認他所看到的網站確實是真的，不是偽造的？若進入偽造的網站而輸入重要資訊，可能會對使用者造成鉅大的損失。針對此問題，目

前仍無解決的方案，倘若國內打算推行，仍須討論如何建立此機制。建議先從技術面提供解決方案，而整體機制(包含法規面、程序面)則可再進一步研究。

#### 4. 網站安全認證制度之程序面、法規面報告

報告人：林宜隆教授

報告摘要：

- (1) 整個網站就像是CAS及消防局等產品認證，但要如何運行仍須技術面相關法律配合。
- (2) 目前希望在通資的安全上能有幾重點：產品本身、產品品管、驗證分級等。
- (3) 法律面及技術面包括四點：驗證分級制度、檢測技術層面、驗證方法，如ISO、自動認證程序。
- (4) 在經濟部商業司下，有一國家認證委員會，被該委員會委託做安全認證的機關，會對網站之安全性做認證。
- (5) 依據專業的角度：網路犯罪的查緝不易，所以必須要求(強迫)使用者留下資料，以作為辦案需要之證據。但事實上，電腦資料的辨識至今仍有問題，高明一點的駭客在入侵之後，還可刪除系統之log、湮滅犯罪的證據。

結論：

- (1) 強迫使用者留下資料：A.透過政府公權力，例如：A.B計劃、B.透過民間，例如：銀行。
- (2) 關於資料的認證，先做技術面的機制，這部分委託賴教授先將資料整理出來，技術面的機制成熟之後，可由委員會主導，推動後續的工作。
- (3) 委員會亦可提出相關計劃案，以委託計劃之方式，研究認證的機制。

#### 5. 微軟全球性的資訊安全策略性技術保護計劃 (STPP, Strategic Technology Protection Program)

報告人：劉念臻經理、王嘉玲經理

參考資料：

<011601 Microsoft Security.ppt>

報告摘要：請參閱參考資料

結論：

- (1) 期望與有關單位合作，推動區域聯防機制。
- (2) 希望與TWCERT共同推動網路安全，透過網管人員的配合，將此計畫推廣。
- (3) 目前在各地皆有Service Center，政府單位也願意與之配合。

#### 參、提案討論

議題一：

### TWCERT會員收費方式討論與建議

說明：

爲了加速TWCERT運作經費朝向自給自足的目標，交通部電信總局希望TWCERT明年度開始收取會員會費及服務費，請就收費辦法草案提出建議。

參考資料：<收費辦法.doc>

摘要：

- (1) 對於TWCERT發布的漏洞，有些網站管理者並未做到檢測與修補的工作，以至於舊有的漏洞一直存在，而系統也一直處於容易被攻擊的狀態。爲了提高漏洞修補率，TWCERT未來在發布的advisory中，會提供一URL，讓使用者連回我們所研發的漏洞自動檢測系統，方便使用者檢測他們的系統是否有該漏洞，並立即提供修補程式。希望在TWCERT的大力推廣之下，漏洞修補率能提高。
- (2) 除了會員制外，也可以針對使用者的request收費，即使用者有需要服務時，才對他們收費，兩種方式各有利弊，不過on request的overhead較高。
- (3) 可朝向網路保全公司的觀念來做，對於會員，提供他們網路安全的保障，那麼應可吸引很多會員。
- (4) 若TWCERT以網路保全公司的身分吸引會員，就必須對會員的電腦安全負起相當大的責任，這樣的方式執行起來也頗爲困難，建議以俱樂部的方式，吸引使用者成爲俱樂部的會員，成爲會員的使用者可以彼此交流、享有TWCERT所提供的服務，這種方式較爲簡單，所需負擔的責任也相對的較小。
- (5) 收費種類太多，建議不超過三種。
- (6) 可以說明收費制是以何者爲導向？何種類型？定位在哪裡？定義可明確一點。

結論：

此收費方式爲草案，請TWCERT參考委員們的意見、修正後，下回再提案討論。

議題二：

### 第三層DNS安全檢測之具體實行方案

說明：

第三層由全國使用者註冊建置之DNS，目前數量約50,000~60,000台。應如何實行才能完成這數量龐大的安全檢測工作，並避免因偵測所造成之類似攻擊行爲？

參考資料：

<第三層DNS Security 檢測方案\_鄭進興老師.doc>

摘要：請參閱參考資料

結論：

由TWCERT與TWNIC進一步討論及執行。

議題三：

如何建立重要服務網站安全認證

說明：

網路安全認證制度逐漸受到重視，如何建立使用者信賴的網站安全認證制度，將是一個重要議題。

參考資料：

網站安全認證制度之技術面報告\_賴溪松教授.ppt

摘要：略

結論：

請賴委員提計劃，並於下次會議討論及審議。

議題四：

如何針對台灣的mail server有open relay的做一全面性的清查？

參考資料：<附件--MailRelay.doc>

摘要：

- (1) 可與DNS survey做類似的檢測。
- (2) 透過以價制量管理策略，即以mail使用量收費。
- (3) 規定在同一時間，寄發超出標準量信件者罰錢。
- (4) 禁止不當標題及標題不符合內容之信件的傳送。
- (5) 針對不當的收集email address者停權。
- (6) 提防因公佈mail server而被利用來犯罪。
- (7) 架設一中文網站，由管理者收集、過濾網頁。

結論：

請TWCERT建立一機制，有效的遏止濫寄廣告信件的情形。仿照國外網站的做法，建立資料提供參考。

#### **肆、臨時動議**

為提昇委員會的功能，並加強委員之間的意見交流，委員會將以一個半月開一次會為原則。

#### **伍、散會**