財團法人台灣網路資訊中心
「網路安全委員會」第一次會議紀錄

時間：九十年四月十一日(星期三)上午 10 時整
地點：台灣網路資訊中心會議室(羅斯福路二段 9 號 4 樓之二)
主席：陳年興主任委員　　**記錄:** 陳玉萱
出列席人員：
中山大學資管系　陳年興教授　　行政院研考會　何全德副處長
中華民國網路消費學會 林世華理事長　中央警察大學　林宜隆教授
國防部通資局　吳家麒先生代　中正大學資工系　張真誠教授（請假）
交通部電信總局　許錫蘭簡任技正　資訊傳真股份有限公司　辜存信總經理
中研院資訊所　黃世昆研究員　台灣大學電機系　雷欽隆教授
行政院主計處電子資料處理中心 劉勝東副主任
財團法人資訊工業策進會 鄭祥勝顧問
中華綜合科技有限公司 蕭家黎總經理（請假）
成功大學電機系　賴溪松教授（請假）　交通大學資工系　謝續平教授（請假）
行政院 NII 小組　游啟聰主任(方主任代)
本中心　曾憲雄董事長、陳文生執行長、施朝正組長、許乃文組長、楊禎葆先生、陳玉萱小姐

壹、主席致詞(略)
貳、報告事項：
一、TWNIC 網路安全委員會籌備過程及網路安全委員會設置要點報告
報告人：陳年興主任委員（略）

二、NII 我國資通訊安全機制之建置
報告人：NII 方主任
報告摘要：
1. 原 NII 小組從四月份開始改為 NICI 小組（行政院國家資訊通信發展推動組）。
2. 我國通資訊基礎建設計劃：資通安全保護對象有三，國防、政府機構、民間(最重要)。在重點保護的體系最重要的就是維持軍事力量、讓政府正常運作、國家救援體系也能正常運作。
3. 資通安全保護的重點有三：一、如何保護資通安全，不讓人家有機會攻擊。二、在遭受危害之前能事先識別、偵測危害的徵兆。三、造成危害時，有回覆或備援的機制。
4. 目標：(1)建立防衛通知的安全機制、(2)主動偵測、通報的體系、(3)如何使網路安全有回覆的機制
5. 執行要點：
. 計劃發布以後，如何編組人員來推動通資安全的工作？
. 資通安全發生危機時，有沒有一個通報的體系(或預警的體系)？如何彙整發布已發生的通報事件以供各單位參考、運用？

.如何在國家通資基礎上建立主動偵防的能力。
.整個安全機制的規範、回覆的措施以及相關的網路安全有沒有要檢討或修正的
.通資安全的產品有沒有檢驗的機制
.推動學術界對通資安全做研究
.對通資安全的人力能積極培訓
.對全國人民做推廣跟宣導
.對網路上犯罪的行為應如何處理(設立了網路犯罪組)
.建立跨國跟區域性的合作機制

臨時提案：因應電信研究所民營化之角色轉換，建議 TWNIC 加入 NICI（行政院國家資訊通信發展推動小組）技術工作之編組。

主席裁示：列入爾後會議再與有關主題綜合討論。

參、討論及決議事項：

一、網路安全委員會之定位

說明：在 NII 全國通資訊安全之大架構下及電信總局擔負民間通資安全協調角色，本委員會所應扮演之角色為何？

決議：1. TWNIC 之主管單位為交通部，本委員會設置要點條列有八項主要任務， 此主要任務與政府推動通資安全之任務息息相關，建議未來能透過交通部與有關組織相互配合。

2. 本委員會設置要點主要任務[6]之文字建議調整為：
[6] 提供網站安全檢測服務，制定網路安全檢測標準，發布國內網路安全指標調查年報。

3. 建議執行網站安全檢測服務及進行主動偵測以了解國家整體網路安全性情形時，應注意程序上之合法性及合理性。

4. 建議執行主要任務 6.之相關作法可以考慮與民間團體（如 TWCERT 、ISP 聯盟）協商或契約合作。

二、如何確保我國 DNS 主機的安全性，及提高 DNS 服務的穩定性？

說明：根據澳洲一家網路安全顧問公司於 2000 年 6 月的一份分析報告顯示，3/4 的澳洲 DNS 伺服器有漏洞，可能會遭受阻斷式攻擊 (Denial of Service, 簡稱 DoS)，一半左右的伺服器其 root 可能被竊取。因此如何確保我國 DNS 伺服器得到較佳的保障，避免遭受攻擊而導致網路服務中斷；並建立網路安全通報體系，即時協助、處理安全事件，及迅速通知 DNS 階層式系統下之相關伺服器管理者重要安全資訊，以確保 DNS 系統能運作正常不受攻擊。

決議：1. DNS 是一切 Internet 服務的基礎，如何確保我國 DNS 主機的安全性，及提高 DNS 服務的穩定性是 TWNIC 最重視的工作，建議未來有幾個方向的工作能藉重 TWCERT 之專業來合作進行。例如：

. 持續掌握網路安全最新資訊,提升 TWCERT 技術人員之專業知識。

. 透過 TWCERT 專屬網站持續提供網路安全相關技術新知、各種新

版的安全漏洞及攻擊方法之防禦方式。

. 藉由與 TWNIC 合辦相關教育訓練提供給一般業界參與，協助提升全國 DNS 管理人員網路安全方面的技術及知識，導引全國網路使用者提升對網路安全之重視。

. TWNIC 如有需對所屬客戶提供網路安全檢測之服務，建議 TWCERT 提供相關整體的工具、技術及程序。

2. 建議 TWNIC 制定並公告各行業網路安全標準等級之參考規範，對現有客戶主動通知盡告知義務，對新客戶則於申請網域名稱時告知，同時可提供讓客戶依所屬分類等級，選擇網路安全檢測之服務。逐漸形成業者為取信於大眾而主動提升 DNS 安全等級之風氣。

3. 我國第二層 DNS root server 是否穩定、安全，與公共利益有關，建議有必要請 DNS 緊急應變小組所有成員全面提升第二層 DNS 之安全等級。

4. 建議爾後可討論對於執行網路安全檢測之技術核心人員，離開工作崗位後應如何掌握，以提升 TWNIC 執行網路安全檢測服務之公信力。

三、如何整合相關單位之資源及人力，以有效提昇網路之安全？

決議：因為會議時間的關係，此議題將留待下一次會議討論。

四、目前有哪些值得關心與探討的網路安全議題？

決議：

1. 下次會議建議增加下列有關議題：

. ADSL 寬頻使用環境安全議題之探討。

. 討論與網路咖啡廳業者合作舉辦網路安全教育訓練之可行性。

2. 各位委員平時如果有相關議題，建議可隨時提出加入下次討論議題。

五、如何評估網路的安全性，網路安全指標的訂定與規範

說明：企業安全管理規範、防禦工具軟體之認證、
網路安全人員之認證、系統安全之認證

決議：因為會議時間的關係，此議題將留待下一次會議討論。

六、散會

董事長	執行長	簽核人	記錄