出國報告(出國類別：考察)

「資通設備之安全檢測研究計畫」參訪設備認證機關及檢測實驗室

服務機關：國家通訊傳播委員會
姓名職稱：陳簡任技正春木、韓鎮華科長、
王科員三峰
派赴國家：美國
出國期間：100 年 4 月 9 日至 4 月 18 日
報告日期：100 年 7 月 1 日

摘要

為研擬適合我國的資通設備檢測要求，包括安全檢測技術規範、檢測技術標準、設備採購參考指引等配套措施，並規劃短中長期資通設備安全檢測與國際接軌的策略方向，以期滿足政府機關(構)對於資通設備採購及使用的安全需求，進而促進我國資通產業發展。通傳會於 2011 年 4 月 9 日至 18 日派員至美國，拜會 ICSA 實驗室、國家標準與技術院、新罕布希爾大學互通性實驗室及思科系統公司等 4 個單位，實地觀摩、學習美國如何推動資通設備安全檢測，以為我日後相關施政的參考。其中，產品認證測試分級、建立樣本資料庫及採「真實樣本」測試等作法，均值得參考借鏡。

目次

壹、目的

為推動「國家資通訊安全發展方案」，使我國的資通環境更能面對複雜多變的資通安全威脅，行政院於 2009 年 8 月 18 日至 20 日舉辦『塑造資安文化、推升資安產值』產業科技策略會議（Strategy Review Board，SRB）」。行政院科技顧問組於該策略會議所達成的共識與策略基礎上，協同相關部會規劃完成「行政院『塑造資安文化、推升資安產值』產業科技策略會議關鍵推動方案」，並由各主責部會在施政措施上予以落實。通傳會（NCC；National Communications Commission）依前開方案之行動計畫 3-1（2010 年至 2013 年），負責推動「資通設備之安全檢測研究計畫」，即在兼顧「政府需要」、「產業發展」及「建立檢測能量」原則下，研擬適合我國的資通設備檢測要求，包括安全檢測技術規範、檢測技術標準、設備採購參考指引等配套措施，並規劃短中長期資通設備安全檢測與國際接軌的策略方向，以期滿足政府機關(構)對於資通設備採購及使用的安全需求，進而促進我國資通產業發展。

考量美國向為資通訊設備先驅，且不遺餘力地執行資訊安全政策，為透過有效安全測試、驗證與評估，增加使用者資訊系統與網路的信任等級，推動「共同標準評估與驗證計畫（CCEVS；Common Criteria Evaluation and Validation Scheme）」，以達成下列目標：

1、 符合政府與產業對於資訊產品具成本效益的評估需求

2、 鼓勵商業安全測試實驗室的成立和民間私有安全測試產業的發展

3、 確保資訊產品安全評估能符合一致標準

4、 改善已評估資訊產品的可用性

他山之石可以攻玉，實地觀摩、學習美國如何推動資通設備安全檢測，以作為我日後相關施政的參考，確有其必要性。此次活動，拜會 ICSA Lab、NIST、UNH-IOL 及 CISCO SYSTEM 等 4 個單位。

貳、參訪機關

一、ICSA 實驗室

成立於 1989 年，屬 Verizon 企業公司旗下的獨立部門，位於賓夕法尼亞州的米卡尼克，是一間對於美國網通產業檢驗有極大影響力的實驗室，通過 ISO 17025:2005 及 ISO 9001:2008 認證，主要從事的業務有(1)認證測試(2)客製化測試(3)驗證測試等三項，目前接受送測的產品有 Anti-Spam, Anti-Spyware, Anti-Virus, Custom Testing, Endpoint Security, IPSec, IPv6/USGv6, Network Firewall, Network IPS, Web Application Firewall 等項目 。該實驗室擁有世界頂尖的評測水準，已成為使用者評估產品相容性和可靠性的重要依據。

二、國家標準與技術院（NIST；National Institute of Standards and Technology）

美國政府為了增強商務部國家標準局(the Commerce Department's National Bureau of Standards, NBS)能達成科技協助業界的任務與功能，於 1988 年將其更名為國家標準與技術院，總部設在馬里蘭州的蓋瑟斯堡（Gaithersburg, Maryland），並於 2010 年 10 月將原 10 個實驗室重整為以下六個實驗室：

（1） 工程實驗室（EL；Engineering Laboratory）

（2） 資訊技術實驗室（ITL；Information Technology Laboratory）

（3） 材料測量實驗室（MML；Material Measurement Laboratory）

（4） 物理測量實驗室（PML；Physical Measurement Laboratory）

（5） 奈米科學及技術中心（CNST；Center for Nanoscale Science and Technology）

（6） 中子研究中心（NCNR；NIST Center for Neutron Research）

NIST 一年預算約在美金 9 億元左右，雇用科學家、工程師、技術員、商業分析師及經營管理者約 2900 人，另外客座的研究員、工程師約 1800 人， NIST 在全美各地約與 1400 家製造公司有合作關係。

NIST 和 ISO 類似，是在技術認定標準及研發的機構，不同的是，它服務對

象多以本土工業、企業為主，且商業導向大於學術功能，並在聯邦政府領導電腦系統技術之研究。其中在開放系統環境（open systems environment）推動方面，NIST 有資訊管理指令（Information Management Directions）及應用可攜剖繪（Application Portability Profile）兩個主要成果，指導美國聯邦單位，提升互通性、可攜性、可度量性及標準化資訊架構與系統。

三、新罕布希爾大學互通性實驗室（UNH-IOL；University of New Hampshire InterOperability Laboratory）

1988 年成立，為世界著名的公開測試實驗室。其資金來源完全來自於委託 IOL 測試其產品符合性(Conformance)及互通性(Interoperability)能力的廠商。因有嚴謹的測試步驟、完備之測試環境，深受各界信賴，在北美的網路設備商中擁有非常廣大的會員與影響力。其對於各種技術領域之研發測試都有涉獵，相關領域包含了：xDSL (ADSL, SHDSL, VDSL) 、802.11 wireless (802.11a, 802.11b, and 802.11g) 、Bridging (STP, VLANs, RSTP, 802.1X) 、Ethernet (10, 100, 1000, 10Gig) 、IPv4 Routing (RIP, OSPF, BGP4, Multicast) IPv6 (Base Specifications, RIP, soon to offer OSPF/BGP testing, Moonv6) 等。網路廠商常把 UNH-IOL 當作是自己內部研發及測試實驗室的延伸，以確保在產品正式銷售前，能更完整且有效率的釐清並解決產品問題

四、思科系統公司（CISCO system）

1984 年創立，總公司位於聖荷西，為全球網路設備領導廠商。在全球 67 個國家已有超過 400 個以上的分支據點，約擁有 35,000 名員工。針對「無線（Wireless）」、「語音（Voice）」、「安全（Security）」、「儲存（Storage）」等技術，提供現代化產品，包括 ATM/Frame-Relay 寬頻交換機、超高速交換路由器（Giga Switched Router）、語音訊號處理（Voice Signaling）網路電話（IP-XML）、電話加值服務（Voice value-added services）、數位用戶迴路（DSL）、高速/超高速 LAN 交換機等，並藉由 IOS(Internetwork Operating System)網路通訊軟體完成連通。

參、過程

4 月 09 日	自臺北中正機場啟程
4 月 11 日	拜會 ICSA 實驗室
4 月 12 日	拜會 國家標準和技術院
4 月 13 日	拜會 新罕布希爾大學互通性實驗室
4 月 15 日	拜會 思科系統公司
4 月 18 日	返抵國門

肆、參訪紀要

一、拜會 ICSA Lab

由總經理 George P. Japak 及高級諮詢分析師 Al Potter 負責接待，Al Potter 先簡報該實驗室發展現況，雙方復針對資通訊產品驗證問題進行意見交流，會談內容略整如次：

（1） 在認證測試部分，各項不同的產品依其需求有不同的規範要求，以網路防火牆（Network Firewall）為例，其規範可以分為最基本的（Baseline）、住家的（Residential）、中小企業的(SMB)、公司的（Corporate）四種等級，無論那一等級，皆要符合 Baseline 要求，而 Residential、SMB 或 Corporate 則係在 Baseline 上，對這三種等級進行更精確的要求定義。

（2） 在 ICSA Lab 的測試過程中，經統計 98%的產品在送測的第一次會無法通過，送審廠商需根據問題進行反覆修正，最終約有 82%送測產品通過 ICSA Lab 要求。

（3） 在 ICSA Lab 定義的測試過程中，由於資訊安全強調「真實樣本」測試，所以 ICSA Lab 會實地進行樣本蒐集。以 Anti-Spam 測試為例，該測試過程需使用 E-mail 樣本驗證 Anti-Spam 設備，判斷 Spam 準確率是否符合標準，為使測試結果符合真實情況，測試樣本最好來自真實環境，循此，ICSA Lab 特意蒐集該實驗室 20 年來沒人使用的 E-mail 帳號所收到的 Spam，成為 Anti-Spam 測試樣本。

二、拜會 NIST

由電腦安全處密碼技術組資訊安全專家 Matthew A. Scholl 博士及組長 Ranall J. Easter 等全程接見，並向我方簡報有關 NIST 運作概況、密碼模組確認等方案，

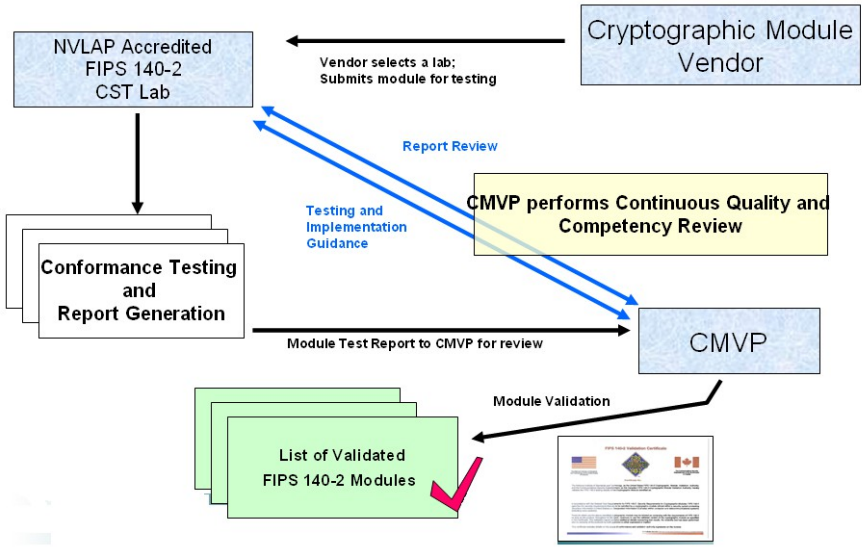
隨後，雙方進行意見交流，會談內容略整如次：

（1） 目前 NIST 電腦鑑識（forensics）工作有二：

1. 提供國際標準參考資料支援調查及研究，即執行國際軟體參考庫(NSRL；National Software Reference Library)計畫，包括業蒐集超過 11,000 套裝軟體 (包括行動通訊應用程式）及超過 7 千萬個可特別辨識出每一檔案的檔案指紋（fingerprint）與資訊，並每季提出參考資料集（RDS；Reference Data Set ）等等。
2. 建立電腦與行動裝置鑑識工具測試（CFTT；Computer and mobile Forensics Tool Testing ）方法論，以增加數位證據的接受度。

（2） 美國聯邦資訊處理標準（FIPS；Federal Information Processing Standard）140-2 僅係提供給美國聯邦政府使用，而非所有各級政府機關均會引用之(如：州政府未必會用)。

（3） 目前並沒有一套檢測標準或技術規範可以涵蓋所有的安全需求，由 NIST 所制訂的 FIPS 140-2 亦是如此。FIPS 140-2 的標準主要是依據聯邦政府的需求及業界的公開標準/業界標準制訂而成，以符合性測試（Conformance Test）概念進行產品檢測。其發證程序如下：



（4） 聯邦政府在採購與「密碼模組」或「密碼演算法」有關資訊設備時，

均需依 FIPS 140-2 技術規範，由設備廠商提供產品檢測證明。另在共同準則的部分，在目前 22 個被要求使用共同準則（CC；Common Criteria）檢測標準的聯邦政府單位中，目前僅有國防部（DoD；Department of Defense）及情報局（Intelligent Agency）有採用 CC 的檢測標準。

（5） CC 的主管機關為美國國家資訊安全保證合作夥伴 (NIAP；National Information Assurance Partnership)，主要是由美國國家安全局（NSA；National Security Agency）負責運作，依據 ISO/IEC 15408 國際標準進行資通訊產品的檢測；NIST 不涉此業務。

（6） ISO 19790 (FIPS 140-2 ISO 版)的第 3 版初稿(working draft)預期將於今年年底前對外公佈，NIST 僅會針對與技術層面有關的規範與業者及進行討論，其他非技術性問題，不在 NIST 負責範圍內。

（7） 不管是 FIPS 140-2 或 CC 標準，均是以最基本的保證（Baseline Assurance）及有限的要求（Limit Requirements）二概念去制訂技術規範，主要目的是協助使用者及設備商能夠有一個清楚的檢測概念，去採購及開發符合資訊安全最低且必要的門檻要求。

（8） 目前經 NIST 認可的密碼安全測試實驗室(CST；Cryptographic Security Testing) Lab 共有 18 間，私人鑑定證明實驗室 (PIV；Personal Identification Verification) Lab 共有 10 間，安全內容自動化協定實驗室 (SCAP； Security Content Automation Protocol) Lab 共有 9 間。取得 SCAP Lab 的實驗室必須先具備 PIV Lab 的資格，取得 PIV Lab 資格的實驗室必須先具備 CST Lab 的資格。

（9） 智慧電網（Smart Grid）部分，要求與 FIPS 140-2 技術規範相同，主要係應用在網路傳輸「傳統電表」所使用的數據及識別資訊上。

三、拜會 UNH-IOL

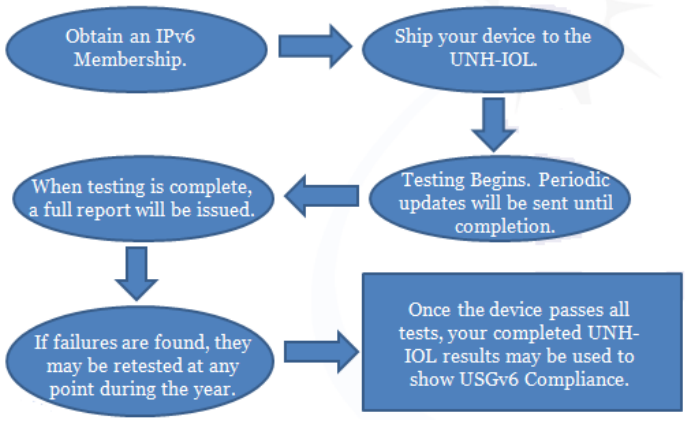
由總經理 Erica Johnson 及軟體工程部經理 Timothy Winters 負責接待，

Timothy Winters 先就該實驗室經營現況做簡報，雙方復對資通訊產品驗證問題進行意見交流，會後參觀該實驗室，會談內容略整如次：

（1） 企業與教育結合是減少驗證成本支出的利器，IOL 雇用新罕布希爾大學研究生作檢測，不僅讓學校能有實務操作之環境，IOL 亦可藉由學校研究的能量，提昇自身測試能量，而不用花太多的錢達到互蒙其利的目的。另由於 IOL 在互通測試上頗負盛名，廠商很願意對其投資網通測試工具，讓 IOL 省去龐大的設備採購成本。

（2） IOL 互通測試僅針對資訊產品，並不包括電信設備，蓋因，電信廠商不認為該等設備須與其他廠牌之電信設備要能互通。

（3） 依 2009 年 12 月 10 日美國發布之聯邦採購規定，政府機關於採購使用網際網路協定之資訊技術需求時，必須參考定義於美國聯邦政府 IPv6 剖繪（USGv6 Profile）之適當技術能力與定義於 USGv6 測試計畫(USGv6 Testing Program)之相關符合性宣告。IOL 為 USGv6 測試實驗室之一，測試流程如下：



每會員資格將允許你測試二個產品(IP stacks)，每個產品測試時間將需要三個星期。但可買多個會員資格，以允許安排超過二個以上 stacks 的測試。

四、拜會 CISCO SYSTEM

由首席工程師 Choa-Li Tarng 博士及專案經理 Hsin-Yi Anna Meng 負責接待 。

Hsin-Yi Anna Meng 就該公司營運情形做簡報，雙方復對資安事故（incident）、產品等實務處理面，進行意見交流，會後參觀該公司最新產品及相關應用，會談內容略整如次：

（1） 為處理產品資安事故，Cisco 成立產品資安事故回應小組（PSIRT； Product Security Incident Response Team），其處理程序如次：

值得一提，Cisco PSIRT 除會向其客戶公佈產品資安事故處理方式外，亦幫助事故報告者（不一定為 Cisco 本身）向第三方協調中心（如 CERT/CC、 CPNI 等）通報產業所揭露之弱點。

（2） 防火牆安全特性之一關鍵，是對 TCP 資訊包序列編號進行隨機化處理，可將該列入功能檢測考量。其因係 IP 位址電子欺騙的方法早已公佈，所以，入侵者已有可能通過這種方法，控制住一個現成的 TCP 連接，然後向內部局域網上的電腦發送它們自己的資訊。況且若每次初始化連接時，大都採用一個相同的編號來啟動會話，入侵者在 TCP/IP 中就很容易猜出正確的序列編號。

（3） 一般網通產品的測試驗證過程所遭遇的最大問題是時間，如何在有限的時間內完成產品品質驗證是一個很大的挑戰，在 Cisco 內部，

以大量的自動化測試環境來取代人力，自動化的好處是可重複繁瑣的動作，比人為更精準且有效率。此外，更可以彈性使用更多的設備進行擴充，而不必面對人力需要訓練以及計畫解散後遣散的問題。

（4） 在測試中最常遇到的問題是客戶端問題重製，雖然 Cisco 利用了大量的自動化測試提昇了測試效率，但產品在送達客戶端時，仍然會有新的問題發生，客戶端遭遇的問題往往不容易重製，而且影響到客戶對於 Cisco 產品的印象。因此我們嘗試解決這個問題，即考量 Cisco 在聖荷西總部的人員夠多，且分布於各棟不同的建築物中，我們建置了 alpha network，來針對產品進行測試。在這個 alpha network，我們放上刻正開發的產品，讓 Cisco 內部員工進行試用，根據過去 alpha network 測試經驗顯示，這樣的測試模式可以發現，許多依照 test case 進行測試，所不能測試到的問題。囿於這些員工在公司的主要任務還是上班，為了避免網路中斷，影響到這些員工的工作效率，我們必須時時監控網路，並且在錯誤發生時，快速的解決，或是即時將無法解決錯誤的產品下線，以避免影響到公司正常運作。

（5） alpha network 目前參與人數約 300 人，建置及管理 alpha network 隨著參與人數及產品問題發生的次數越多，所需付出的成本越高。然而參與人數多寡與產品發生的次數同時也是測試效益指標。以參與人數多寡這項指標而言，當越多人參與，縱使產品最後沒有測試出問題，依舊可提昇我們對於產品的信心，因為產品順利通過了這麼多人使用的考驗。同樣的，產品發生問題的次數越多，顯示我們透過 alpha network 也找到更多一般測試找不到的問題。將兩者相除，可計算出建置 alpha network 的效益數值，雖然這個數值並不

固定，但是根據統計經驗，建置 alpha network 是值得的。

（6） Cisco 網路整合應用技術展示，主要有(1)通話 (2)智慧家庭(3)生醫照護等部分：

1. 在通話應用部分，Cisco 切入 Android/IOS 平台服務軟體的開發。運用 Cisco 在各個平台上提供的軟體，使用者能進行流暢的視訊對話，對話的過程不局限於兩人，可做到三方甚至多方通話，透過網路執行的通話功能，比一般傳統話機所能提供的功能，更為強大與方便。
2. 智慧家庭應用部分，Cisco 提出居家保全整合概念，透過 Cisco 所提供的網路解決方案，使用者透過感測晶片取代鑰匙進出家門，也可隨時監看家中閉路電視攝影機，以了解家中是否異狀發生。
3. 生醫照護應用部分，Cisco 賦予基本醫療設備連網的能力，如脈搏感測器及血糖檢驗器等，都可連接上網際網路，醫師可以透過這些感測設備進行診斷，讓使用者不需長途跋涉就能獲得最完善的照護。

伍、心得與建議

此次交流活動，讓吾等了解到美國在資通設備安全檢測之作法，其中包括樣本資料庫的建置、設備檢測分級的方式、建構模擬實體的採樣環境、資安事故處理模式等，均值得我方借鏡學習。相關建議如下：

（一）制定符合我國需求的資通設備安全驗證等級

由於各國資通設備製造廠商之市場規模、研發與製造能力，並不相同若將某些國家的資通設備安全驗證等級，一味移植於我國，恐造成水土不服，治絲益棼。準此，應先檢視我國現況，了解政府資通設備安全檢測預期目標為何，方去訂定相關驗證等級，以挈其領，達其效。

（二）制定能與國際標準接軌的資通設備檢測規範

目前我國尚待申請加入國際共同準則承認協定(CCRA；Common Criteria Recognition Arrangement)組織，因此，除研提適於我國之短中長期資通安全檢測設備類別、項目及檢測技術規範外，亦須考量將前開內容適當加入與國際接軌之具體作法及對應配套措施，較為妥適。

（三）制定合理可接受的資通設備檢測費用與時程

共同準則(Common Criteria；亦稱 ISO/IEC 15408)雖為國際通用的資安產品驗證標準，但因該驗證時間較長，一般可達 18 個月，且動輒千萬，所費不貲，造成在實務推動上，有其瓶頸，業者接受度不如預期。準此，為利我國發展資安產業得以順遂，得考量免除非必要之檢測項目，縮短驗證時程並降低費用。

（四）制定能篩檢把關的檢測實驗室相關管理辦法

囿於政府人力不足，為使我國資通設備安全能維持一定水平，藉由第三方檢測機構（實驗室）的角色對資通設備產業進行安全檢測的工作，就益顯重要。準此，如何避免實驗室良莠不齊，由實驗室相關管理辦法篩檢

把關，應為可行，即其內容至少須包含實驗室執行之檢測範圍、具備之檢測能力等項，供主管機關據以認可。

陸、照片

照片 1

▲訪問 ICSA

照片 2

▲訪問 NIST

照片 3

▲訪問 UNH-IOL

照片 4

▲訪問 Cisco