資通設備之安全檢測研究計畫

期末報告書

執行單位：中華民國資訊軟體協會

中華民國100年11月

目　次

圖　目　次

表　目　次

壹、專案概述與期末交付項目說明

一、專案名稱

資通設備之安全檢測研究計畫

二、專案目標

為強化政府機關(構)使用之資通設備安全性，並促進我國資通環境安全，本專案之研究目的如下：

(一)確保政府使用資通設備之安全性

我國資通設備安全檢測實驗室可依據本專案產出之資通設備安全檢測技術規範，檢測資通設備之安全性，增加政府採購資通安全設備來源，滿足政府對於資通設備安全需求。

(二)建構我國資通設備發展環境

本專案之推動，將透過政府機關(構)率先採用經檢測實驗室檢測合格之資通設備，增加我國資通設備廠商投入研發之意願，提升我國資通設備廠商全球市場競爭力。由於政府機關(構)重視資通設備安全性，將可提升民間企業使用資通安全設備意願，有助於建構我國資通設備發展環境。

三、期末交付項目

期末報告應於契約生效次日起 300 日內，即 100 年 10 月 11 日前，繳交完整期末報告初稿 14 份。期末報告應包含下列

(一)至少 8 種資通設備之安全檢測技術規範草案(含期中之 4 種資通設備之安全檢測技術規範草案)

(二)至少 8 種資通設備項目之資通設備採購參考指引草案(含期中之 4 種資通設備之資通設備採購參考指引草案)

(三)出國參訪心得分享(日本)

(四)國際接軌之 SWOT 態勢分析結果報告

(五)國際接軌之具體作法及配套措施建議

(六)資通設備之安全檢測之合理費用與時程

(七)3 場座談會(含期中 2 場座談會)及 1 場成果發表會之會議紀錄

貳、期末報告

一、至少 8 種資通設備之安全檢測技術規範草案

技術規範草案內容包含產品適用範圍、用語釋義、技術要求等，規範係參考共同準則、ICSA 實驗室(http://www.icsalabs.com)、NSS 實驗室(http://www.nsslabs.com/)以及其他國際技術標準訂定。為考量我國資通訊設備安全檢測技術規範與國際技術標準之一致性，規範所定之測試項目、判定標準及測試方法，遵循技術標準最新版本相關規定。

目前資通設備之安全檢測技術規範草案，期末共須交付 8 種資通設備項目：

(一)防火牆(Firewall)

(二)入侵偵測防禦設備(IDP)

(三)防毒閘道設備(Anti-Virus)

(四)垃圾郵件過濾設備(Anti-Spam)

(五)網頁應用防火牆(WAF)

(六)應用軟體控管系統(AC)

(七)乙太網路交換器(L2 Switch)

(八)路由交換器(L3 Switch)

上述資通設備項目名稱，依據第三次與第四次專家學者座談會決議，將將網頁過濾管控設備修改名稱為網頁應用防火牆(WAF)，網路安全監控設備修改為應用軟體控管系統(AC)，交換器修改名稱為乙太網路交換器(L2 Switch)，路由器修改為路由交換器(L3 Switch)，較可廣納較多品項或與目前市面上產品名稱較為接近。

上述 8 項之檢測規範乃根據使用者需求所訂定，技術要求部分則包括書面審查及實機測試。書面審查標準主要參考共同準則規範，實機測試標準主要參考 ICSA 與 NSS 等國際實驗室測試標準。

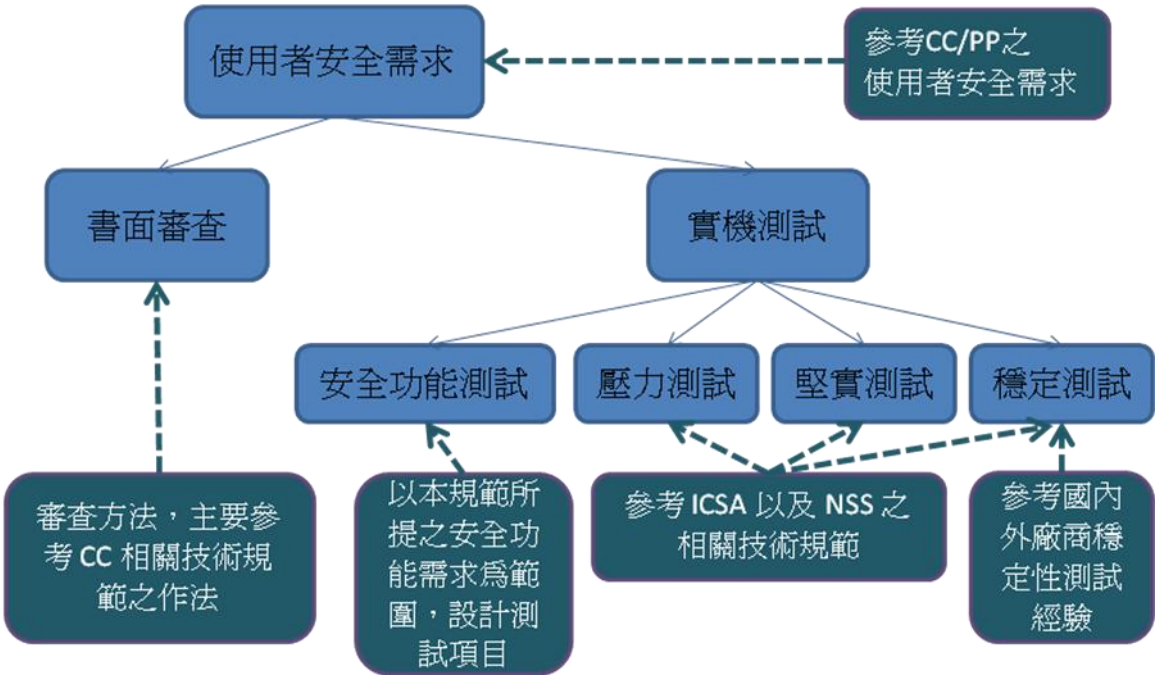


圖1　資通設備之安全檢測技術規範-架構

書面審查包括安全標的及安全功能設計審查類別，如表 1；實機測試包含安全功能測試、效能測試、堅實測試、穩定測試，如表 2。

表1　書面審查類別

項次	類別	內容描述
1.	安全標的	檢測產品驗證範圍定義及安全功能(TSF)概述。
2.	安全功能設計	產品安全功能(TSF)之安全功能規格、安全設計、安全架構、安全指引、安全功能測試等說明。

表2　實機測試類別

項次	類別	內容描述
1.	安全功能測試	測試產品本身所具有的安全防護相關功能。
2.	效能測試	測試產品在尖峰網路使用時期安全功能是否有受影響。
3.	堅實測試	測試產品本身在開啟服務或協定的情況下是否能夠處

項次	類別	內容描述
		理不正常連線行為，依舊保持正常運作而不受影響。
4.	穩定測試	將資通設備置於真實網路流量下運作測試，了解設備在真實的網路流量下是否有不穩定的狀況發生。

詳細資通設備之安全檢測技術規範草案內容，請參閱附件一~八。

8 項產品實機檢測之內容表列如下：

表3　實機檢測測項彙整

類別	項目	Fire-wall	IDP	Anti-Virus	Anti-Spam	WAF	AC	L2 Switch	L3 Switch
安全功能測試	封包過濾	O							
	異常/攻擊偵測		O			O			
	躲避攻擊		O			O			
	病毒偵測			O					
	流量內容統計	O							
	安全事件紀錄	O		O	O	O	O		
	安全管理	O	O	O	O	O	O	O	O
	異常/攻擊事件紀錄		O						
	線上更新		O	O					
	使用者自訂安全規則		V						
	備援管理	V				O			V
	組態備援管理							V	V
	規則控管	V							
	具備 IPv6 封包檢測		V						
	IPv6 認證保護								O
	運作模式切換			V					
	惡意網址過濾			V					
	郵件過濾				O				
	TLS/SSLsupport					V			
	即時流量內容監控						O		
	應用程式行為管理						V		

類別	項目	Fire -wall	IDP	Anti -Virus	Anti -Spam	WAF	AC	L2 Switch	L3 Switch
	安全稽核功能							O	
	密碼支援功能							O	
	使用者資料保護功能							O	
	使用者識別與鑑別功能							O	
	安全功能保護功能							O	
	虛擬區網(VLAN)保護功能							V	
	虛擬路由器保護功能								
	障礙與效能監控功能							V	
	自動登出功能								O
	Multicast 認證保護								O
	路由認證保護								O
	路由被動介面								O
	Port Security 存取控制								O
壓力測試	吞吐量	O	O	O	O	O	O	O	O
	最大同時連線數	V	V	V	V	V	V		
	最大建立連線速率	V	V	V	V	V	V		
	最大虛擬(VLAN)容量							V	
	最大 MAC 容量							V	
堅實測試	阻斷式攻擊	O	O	O	O	O	O	O	O
	惡意流量	V	V	V	V	V	V	V	V
	非正常關機復原	O	O	O	O	O	O	O	O
穩定測試	真實流量測試	O	O	O	O	O	O	O	O
O 表示基礎型與進階型皆須檢測之項目 V 表示僅進階型須檢測之項目									
資料來源：本計畫自行整理									

資通設備安全檢測規範草案中將檢測等級分為基礎型與進階型，採購單位及廠商可根據本身需求來決定適用等級，也可讓政府單位依機敏程度來決定適用等級，分級僅代表安全檢測強度的不同，並非產品功能規格的不同，基礎型與進階型之差異如下：

1.測試項目上的差異

於測試項目部分，進階型須有較多的測試項目。EX：壓力測試中，基礎型僅需測試吞吐量，然進階型則須測試最大同時連線數或其他測項。

2.通過標準上的差異

例如進階型於穩定測試中須通過較長時間之正常運作測試。

3.檢測費用上的差異

由於基礎型與進階型之測項不同，故所需花費之人力物力亦不相同，故檢測費用上亦會有所差距。

二、至少 8 種資通設備項目之資通設備採購參考指引草案

為讓採購單位可以建構安全的資通產品使用環境，除採購時可選擇有通過檢測規範的產品之外，而指引內容重點在於從採購單位的角度出發，一方面提供各類產品的系統架構、運作原理等，讓採購單位可以了解以便挑選到最合適的產品，另一方面也要讓採購單位了解各類產品的安全檢測，對於產品使用過程會有怎麼樣的幫助、降低了哪些安全性的風險以及相較於沒有進行安全檢測的產品之間的差異。

目前資通設備採購參考指引草案，期末共須交付 8 種資通設備項目：

(一)防火牆(Firewall)

(二)入侵偵測防禦設備(IDP)

(三)防毒閘道設備(Anti-Virus)

(四)垃圾郵件過濾設備(Anti-Spam)

(五)網頁應用防火牆(WAF)

(六)應用軟體控管系統(AC)

(七)乙太網路交換器(L2 Switch)

(八)路由交換器(L3 Switch)

表4　資通設備採購參考指引內容架構概要

項目	內容	說明
1	前言	說明目的與適用對象
2	設備介紹	內容包含簡介、系統架構、運作原理、常見安裝方式...等
3	資安需求	內容包含衍生風險、防護措施...等
4	採購認證設備	內容包含如何降低資安風險、有效資安健檢...等

詳細資通設備採購參考指引草案，請參閱附件九~十六。

三、出國參訪心得分享—日本

為了制訂並推動合宜與國際化之資通設備之安全檢測技術規範，此專案執行團隊成員前往日本拜訪了擔任主管機關角色的獨立行政法人情報處理推進機構(IPA)及擔任檢測實驗室角色的資訊技術安全中心(ITSC)兩個單位，希望從這些不同類型組織身上學習到在不同角度下是如何看待安全檢測技術規範的趨勢方向、內容制訂以及推動策略。這

趟參訪交流中發現日本 Common Criteria 認證業務需求主要來自於日本國內事務機(Multi-Function Printer；MFP)廠商的外銷需求，MFP 認證占所有產品認證比例大約 67%，由此了解到認證推動應盡量滿足產業發展的需求。

(一)獨立行政法人情報處理推進機構（Information-technology Promotion Agency；IPA）參訪交流

前稱「情報處理振興事業協會」，係 1970 年 10 月 1 日基於「情報處理推動」相關法律（1970 年 5 月 22 日制定，第 90 號法律）設立之社團法人，復依 2002 年 12 月 11 日通過修正頒布之第 144 號法律，於 2004 年 1 月 5 日改組，成為具有管理功能的機構，目前有 10 個部門及中心，包括 IT 安全中心（約有 100 名研究員及職員）、軟體工程中心等，是日本經濟產業省的外圍組織，負責推展與 IT 有關的國家戰略。其主要業務包括 IT 安全、軟體工程、IT 人才培育及開放軟體等，並受理信息病毒、不當存取及脆弱性關聯情報等申報，與 JPCERT/CC 合作，公開這些情報調查、研究及緊急對策等訊息。每年會在全國 10 個地方實施情報安全研討會。

由理事 仲田 雄作、センター長 矢島 秀浩及主任 村田 松寿等人全程接見，村田 松寿向我方簡報有關 IPA 運作概況，隨後，雙方進行意見交流，會談內容略整如次：

1. 日本中央部會於 2001 年 3 月協議「對於政府採購 IT 產品及系統，建議採用經 CC 評估與驗證者」，該國於 2003 年加入 CCRA，成為授與證書會員國(Certificate Authorizing Participant；CAP)。其發證程序如下：

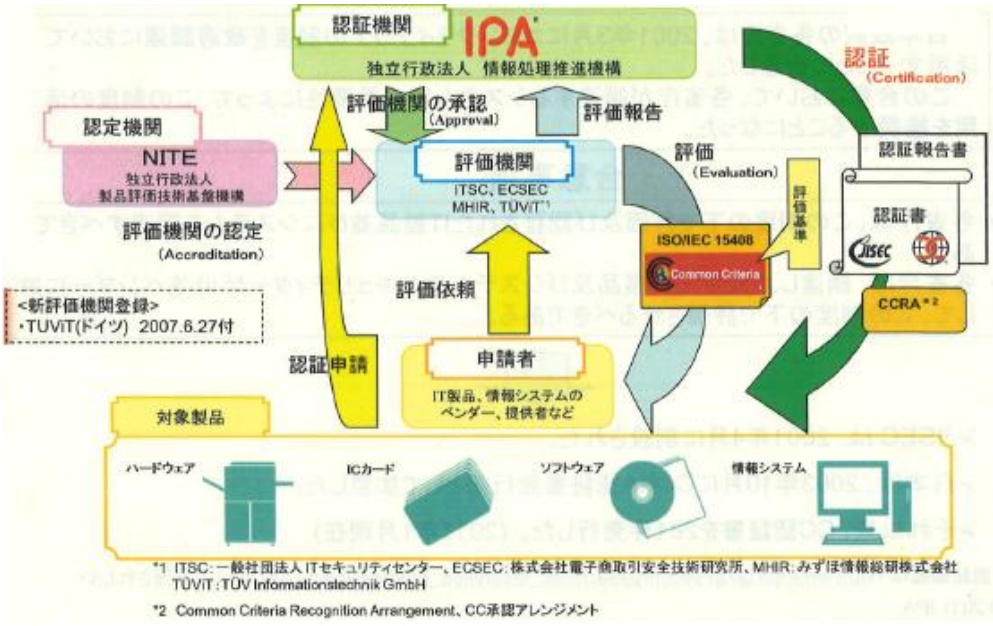


圖2　IPA 發證程序

註：CC 驗證報告書若不公開，該證書之 logo 只能使用「 」而不具「 」。

2. 日本認證產品以事務機（Multi-Function Printer；MFP）為最大量（約占 67%），產品驗證等級則以 EAL3 為大宗（約占 59%）。

3. 日本對近 50 個軟體發展具重要安全須求之政府系統（諸如，貿易統計系統、護照申請檢查系統等）完成安全標的（ST）之評估與確認。

4. 2011 年 4 月 11 日，基於政府採購安全政策，日方公告 IT 安全測量標準產品目錄表，內容包括智慧卡、防火牆、伺服器 OS、事務機、IDS/IPS 及 DATABASE（DBMS）之一般安全功能、認證等級等要求。

統一基準における製品分野リスト　平成23年4月21日 経済産業省

製品分野名	スマートカード（ICカード）	ファイアウォール	OS（サーバOSに限る）	デジタル複合機（MFP）	不正侵入検知／防止システム(IDS/IPS)	データベース管理システム(DBMS)
製品分野定義	プラスチック製カード等にICチップを埋め込み、情報を記録できるようにした製品	インターネットと内部ネットワークの境界に配置され、パケットの内容と事前に定義されたルールに基づきパケット通過を制御する製品	コンピュータのハードウェア制御・操作のために用いられる基本ソフトウェア	プリンタ機能を標準で有し、スキャナ、FAX、コピーのいずれか2つ以上の機能を標準で装備している製品	ネットワークやシステムの稼働状況を監視し、組織内のコンピューターネットワークへの外部からの侵入を報告、防御する製品	共有データとしてのデータベースを管理し、データに対するアクセス要求にこたえる製品
利用用途	住民基本台帳カードやIC旅券等、広く国民に配布され身分確認に利用される。または国民の情報アクセスの認証のために利用される	不正アクセスから保護すべき重要度の高い情報を扱う情報システムを保護する	保護すべき重要度の高い情報を扱う情報システムの基盤として稼動するOS	保護すべき重要度の高い情報の複写やデジタルデータ化、送信等に利用される	ネットワーク上の通信を監視するなどにより、インターネットからの不正アクセスを検知し防止する	国民の個人情報等保護すべき重要度の高い情報をデータベースとして保管するために利用される（サーバOS環境下で稼動するものに限る）
準拠すべき規格・制度	ISO/IEC 15408 Common Criteria	ISO/IEC 15408 Common Criteria	ISO/IEC 15408 Common Criteria	ISO/IEC 15408 Common Criteria	ISO/IEC 15408 Common Criteria	ISO/IEC 15408 Common Criteria
一般的に必要となるセキュリティ機能	セキュリティ監査、送受信の否認不可、暗号化サポート機能、アクセス制御、データ認証、送出データ保護、情報フロー制御、入力データ保護、内部伝送データ保護、残存情報保護、ロールバック、蓄積データ完全性、転送データ機密性、転送データ完全性、識別・認証、セキュリティ管理、プライバシー保護、セキュリティ機能保護、資源利用管理、TOEアクセス制御、高信頼パス／チャネル の各セキュリティ機能について、調達者のニーズに応じて選択。個別製品ごとにどのセキュリティ機能が認証されているかについては、IPAポータルサイトを参照のこと					
評価保証レベル	EAL4+ 以上	EAL4 以上	EAL3 以上	EAL3 以上	EAL3 以上	EAL2 以上

圖3　各類產品須通過之標準等級

5.日本政府為鼓勵業者加速引進 IT 產品認證，提供減稅優惠，方式有二：經認證之產品其稅可減 7%或以全部營收之 7 成繳稅；2010 至 2011 年該國重點輔導對象為中小企業（SMB）。

6.由於日本與大陸貿易非常密切，對大陸進口的電信設備，並無特別有安全限制上之處理。

7.日方完成資訊安全措施（Information Security Measures；ISM）自我評估工具，產業可藉由問答方式（共 25 題，主要出自 ISO/IEC 27001：2005 所定義之安全控制項目），了解自身於 ISM Benchmark 相對應之強弱位置，以改善其企業之資安管理。

圖4　ISM Benchmark 之結果

8.日本 CC 實驗室或驗證機構相關收費規定

申請型態		費用（含稅）
驗證	PP	399,000 円
	EAL1	514,500 円
	EAL2	672,000 円
	EAL3	787,500 円
	EAL4	997,500 円
	EAL5	1,081,500 円
	EAL6 以上	須個案洽談費用
	ST 確認	378,000 円
保證持續		3,700 円
驗證英文版		3,700 円
變更驗證或確認資訊		3,700 円
補發驗證報告書或確認報告書		3,300 円
變更驗證報告書或確認報告書記載事項		3,300 円

日方邀請我方參加今年 11 月預訂在印度舉辦之「亞洲 IT 安全評估與驗證論壇（Asian IT Security Evaluation and Certification Forum）」，除可合作、交換有關 IT 安全評估與驗證資訊外，並可增加我國成為 CCRA 會員之機會。

圖5　IPA 參訪交流

(二)資訊技術安全中心（Information Technology Security Center；ITSC）參訪交流

1987 年即開始研究以共同準則(Common Criteria；CC）為主之評估技術，是 CCRA 在日本第一個正式認可之評估實驗室（2002 年），目前有 15 位評估員，隸屬日本電子情報技術產業協會（Japan Electronics and Information Technology Industries Association；JEITA）成員，並於 2009 年被認可為 FIPS 測試實驗室。業務範圍包括 IT 產品之 EAL1~EAL4 及 PP 安全評估、提供密碼模組與演算測試服務。

由部長代理 北澤 直人、副部長 倉本 康史及理事 宇賀村 直紀負責接待，倉本 康史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，會談內容略整如次：

1.ITSC 做 CC 評估驗證之量為全日之冠（約占 47%）。

2.由於產品驗證時間長、價格不菲，中小企業（SMB）申請認證比例不高，通常上市公司才會提出產品認證。

3.廠商送驗產品若通不過檢測時，廠商可提出相關修正；成功修正耗時最長者，達 2 年。

4.金融海嘯發生時，幾僅剩日本強項－事務機（MFP）提出驗證，目前其他產品驗證有漸增加之態勢。

5.當驗證有疑義時，IPA 會指示、評估到完全一致。

6.每一驗證 case 通常以 3 人一組（1 主驗 2 幫手）來做檢測，該頗有傳承之意味。其訓練評估員之方式有三：

(1)電子學習課程

(2)在工作中學習

(3)技術會議交流

7.ITSC 所做驗證等級只到 EAL4，EAL5 以上雖可試行，但不能發證。除晶片外，EAL5 以上產品均具機敏性。

圖6　ITSC 參訪交流

(三)結論

1.制定符合我國使用者與產業發展需求的資通設備安全驗證等級

由於各國資通環境使用方式不同，設備製造廠商之市場規模、研發與製造能力亦不相同，若將某些國家的資通設備安全驗證機制，一味移植於我國，恐造成水土不服。為了符合我國使用者與產業發展需求，舉例來說，測試樣本必須有一部份要從國內使用環境進行收集，並使用這些收集到的樣本進行檢測，如此一來通過檢測的設備才較能滿足使用者的環境需求，另一好處是促進我國產業發展，因為國內廠商對於國內使用者環境的客製化能力較國外廠商有優勢，也就是說國內廠商對於國內收集之測試樣本的因應能力較佳。

2.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。國際接軌模式包括測報相互承認、授權檢測實驗室以及 pretest 等等，整體來說，短期目標應該以 pretest 為重點，建立起 pretest 所需之檢測環境，而此 pretest 檢測環境又以建立測試樣本資料庫為關鍵，過去台灣廠商到國外測試時經常因為無法偵測某些樣本而被判失敗，廠商為了要能通過必須以每件樣本數萬元美金的價格向其它單位購買，若我國可建立起測試樣本資料庫將十分有助於我國廠商。

3.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。此外廠商設備通常會有一系列型號，同系列每個型號送測的整體費用相當可觀，因此對於系列認證的收費方式必須加以斟酌，經與廠商多次討論後目前申請系列產品檢測之設備，其檢測費用為全項檢測費用乘以重新檢測項目數占全部檢測項目數之比例計算；需重新檢測之項目，由申請者提出並由檢測實驗室認定之。

四、國際接軌之 SWOT 態勢分析結果報告

(一)國際接軌方向

雖然目前本專案所制訂的檢測技術規範未來的實施對象僅為我國政府機關(構)，不過若能與國際接軌則可讓此檢測技術規範發揮更大效益，讓其效益不僅是提升我國政府機關(構)對於資通設備採購及使用之安全性，更有助於我國廠商輸出產品到國際市場。

目前世界各國市場上較受認同的資通設備安全檢測技術規範主要為 CCRA、ICSA 及 NSS 這三個組織所制訂出之規範(其中 CCRA 的規範即為 Common Criteria(CC))，因此我們在制訂規範時主要也是參考這三個來源的資料，自然地對於國際接軌的方向我們也就是朝著與這三個組織接軌的方向前進，期望未來對於歷練過本專案檢測技術規範的廠商，其於檢測過程中所累積的經驗與知識將可有助於它通過上述三個組織的檢測技術規範。

(二)國際接軌模式

國際接軌模式包括測報相互承認、授權檢測實驗室以及 pretest 等，表 5 是分析目前與 CCRA、ICSA 及 NSS 在各種接軌模式的可行性。

表5　接軌模式可行性分析

項目	CCRA	ICSA	NSS
測報相互承認	層級為國與國，CCRA 目前有 26 個會員國，我國亦有提出申請會員國然一直無法通過。可行性低。	層級為檢測實驗室對檢測實驗室，ICSA 目前並無此規劃。可行性低。	層級為檢測實驗室對檢測實驗室，NSS 目前並無此規劃。可行性低。
授權檢測實驗室	CCRA 體制架構中，CCRA 授權檢測實驗室必須為會員國。可行性低。	ICSA 目前正在規劃授權機制。可行性中。	NSS 目前尚無授權其它實驗室的想法。可行性低。
Pretest	目前我國已有 CCRA 技術規範之檢測能量。pretest 可行性高	目前我國已有 pretest 的經驗與能量。pretest 可行性高。	目前我國已有 pretest 的經驗與能量。pretest 可行性高。

綜合來說，我們的策略應朝 pretest 接軌模式努力，同時持續與 ICSA 洽談授權檢測實驗室的接軌。

然而對於單純與 CCRA 技術規範接軌來說，有另一種特別的接軌模式，雖然 TTC 測試報告無法被 CCRA 所承認，然由於 TTC 具有實質的檢測技術，其可接受另一 CCRA 授權檢測實驗室的工作外包，替其執行檢測然後透過該授權檢測實驗室出測報，這樣的業務需求通常是來自中文語系國家廠商，該廠商需要拿到 CC 認證而 TTC 占有語言及地理位置的優勢。另有一接軌模式是將本專案檢測技術規範提供給沒有規範的國家參考(例如東南亞國家)，讓東南亞國家接受台灣的規範將設備送交台灣檢測實驗室檢測，進一步可以把台灣產品銷售到東南亞，拓展廠商的銷售據點。

整體來說，短期目標應該以 pretest 為重點，建立起 pretest 所需之檢測環境，而此 pretest 檢測環境又以建立測試樣本資料庫為關鍵，過去台灣廠商到國外測試時經常因為無法偵測某些樣本而被判失敗，為了要能通過廠商必須以每件樣本數萬元美金的價格向其它單位購買，若我國可建立起測試樣本資料庫將十分有助於我國廠商，因此我們後續便以建立測試樣本資料庫為目標來進行 SWOT 分析。

(三)建立測試樣本資料庫 SWOT 態勢分析

表6　建立測試樣本資料庫 SWOT 態勢分析

優勢 (Strengths) 1. 我國資通使用環境發達，使用行為多樣化，蘊藏豐富之測試樣本(例如病毒樣本、攻擊樣本、垃圾郵件樣本等)。 2. NBL 與國內業者已建立起不錯的信賴程度，易整合業者既有的測試樣本。 3. 測試樣本的搜集與分析技術我國早已投入不少資源研發，具備不錯的技術。	***劣勢 (Weaknesses)*** 1. 政府有些部門亦有在搜集樣本如技服中心、國網中心等等，然目前較難與這些單位進行整合。
機會（Opportunities） 1. 趁本專案的熱度，一舉整合不同單位的測試樣本，以建立我國之測試樣本資料庫。	***威脅 (Threats)*** 1. 本專案的後續落實問題 (1) 台銀共同供應契約配合 (2) 檢測實驗室書面審查技術人員流失 (3) 檢測實驗室實機測試申請資格

五、國際接軌之具體作法及配套措施建議

(一)建立測試樣本資料庫

1.由第三方單位進行搜集樣本、分析網路流量的工作

- 建置立樣本管控中心，提供 NCC 認證檢測實驗室作為統一之

標準

- 進一步加入 WildList.org 以取得 WildList

2.政府必須 fund 此建立測試樣本資料庫專案

- 需要人力進行搜集與維護樣本的工作
- 初期需要政府資金協助第三方單位建立此樣本管控平台
- 後期由此樣本管控平台自己自足，經費來源例如當 NCC 認證檢測實驗室向其拿測試樣本時可酌收費用

(二)惡意程式之收集方式

採用被動與主動兩種方式並行來針對網路常見之惡意程式，包含 virus, botnet, worms, attack traffic 以及 attack programs 等進行偵測與收集。被動式的收集主要是引誘 virus 或是 bot 進入或是攻擊某一個特殊的系統以取得該惡意程式的相關資訊。反之，主動式惡意程式的收集會主動地連結或是開啟惡意 URL 或檔案來取得惡意程式的相關資訊。當使用者透過 URL 或是其他途徑存取或連結惡意程式時，惡意程式即可能攻擊或是感染被害者的系統。與被動式的收集方法比較，主動式的收集方法將有較高的機率去收集到尚未被資安設備所定義之新惡意程式，所以理論上能夠收集更多且不同型態的惡意程式。

在被動收集的部分將透過與國網中心之合作，利用其所建置之蜜罐 (Honeypot) 技術及監控點進行收集，但被動收集仍有其限制且效率較差，所以我們須研發更有效率之主動式惡意程式偵測與收集技術，來彌補被動收集方式之不足。本計畫將以交大 NBL 現有之 PCAP Lib 技術為基礎 (PCAP Lib 之架構如圖 7 所示)，來建置主動式惡意程式收集系統。PCAPLib 主要是從交大建置之 Beatsite 擷取宿舍網路之可疑之流量 (Traffic)，再利用重播 (Replay) 之技術將

流量餵給七臺不同廠牌之入侵偵測系統 (IDS)，之後透過多數決 (Majority Voting) 的方式來辨別是否是入侵之流量。由於這種鑑別方式取決於 IDS 內建之 Signature 之完整度與鑑別度，自動比對之正確率並不是非常理想，經常須以人工的方式協助判斷，因此，本計畫擬發展一個全自動化的惡意軟體偵測系統，可快速且大量地從網路流量中收集我們需要的特定樣本。我們將建置一個主動式惡意程式收集系統，其架構如圖 8 所示。目前存在的 Client Honeypot 技術大都採用 Email 或是 URL 為惡意程式的收集來源，而我們的方法將增加使用 P2P 軟體作為惡意程式收集之來源。此外，現有的 Client Honeypot 只針對惡意程式在主機端的行為資訊，利用常見的分析工具 (Snort or CWSandbox) 來進行分析，而我們的方法將同時分析惡意程式在主機端和網路的行為，與現有的分析機制做比較，我們的方法可更容易地根據惡意程式的行為來修改或擴充分析模組之演算法。

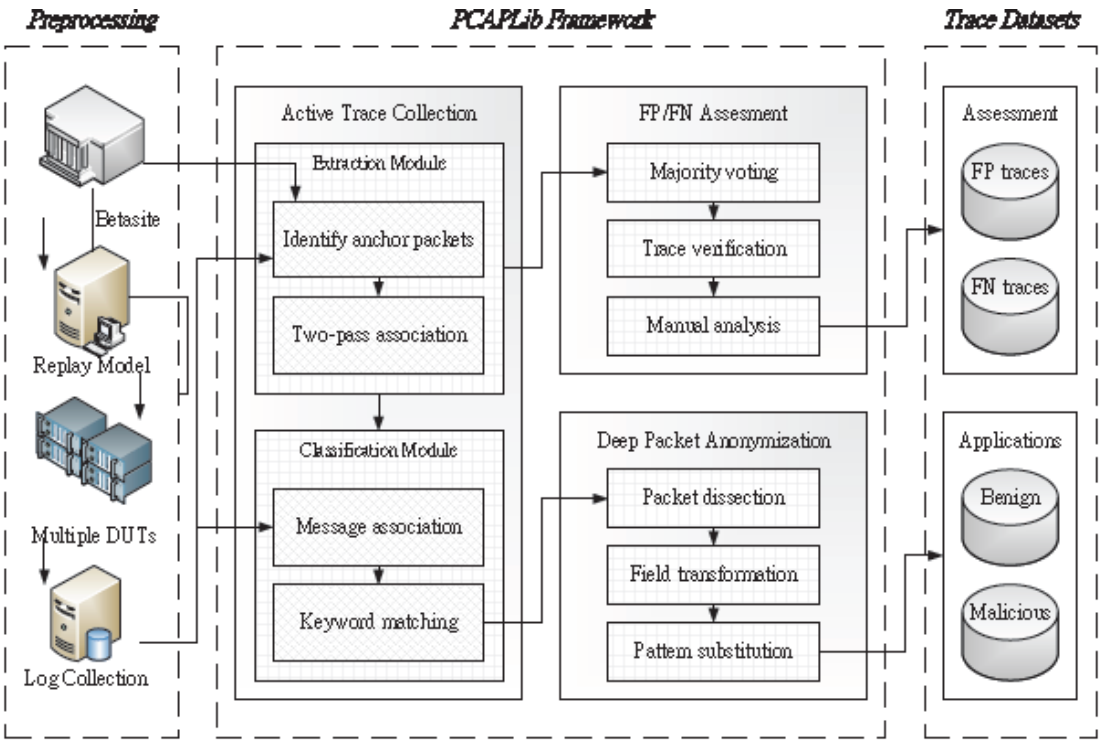


圖7　PCAPLib 系統架構圖

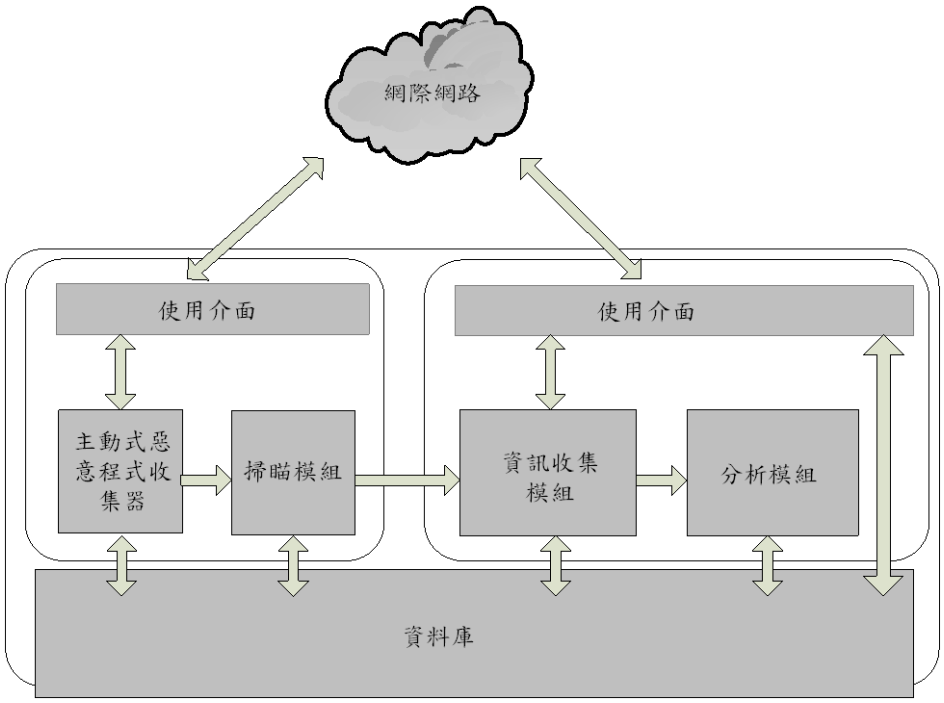


圖8　主動式惡意程式收集系統之架構

(三)惡意程式之行為分析

由於現今大部分的資安軟硬體設備都採用 Signature-based 的方式來進行惡意程式的偵測，然而採用 Signature-based 來偵測有其存在之缺點，例如：無法偵測尚未被發現 (0-day) 的攻擊行為或惡意程式，若圖 2 中分析模組採多數決的方式來鑑別可疑程式，則可能增加其漏判 (FN) 的機率。此外，每個惡意程式樣本都必須建立一個相對的 Signature，如此一來將導致 Signature 的數量過於龐大。相對於採用 Signature 的方式，另一種則是以 Behavior-Based 的方式來進行偵測，即使是尚未被發現的新型態攻擊或惡意程式，只要被分析模組觀察到有不正常的行為，仍然能夠被偵測出來。此種分析方式之優點是不需要針對每個不同的個體而建立其對應之 Signature，所以維護上相對容易。但透過行為分析的方法同樣存在一些缺點，相較於產生惡意程式檢測用之 Signature，當系統要增加一個新的行為分析模型時，將有其困難度，且行為分析模型若設計不當，則誤判

(FP) 的機率通常會高於傳統採用 Signature 之方法。本計畫擬採用以信用值為基礎之權重式投票 (Creditability-based Weighted Voting) 機制來改進傳統採用多數決的缺點，以期提高惡意軟體之偵測正確率，另外，可再配合惡意軟體之主機行為 (Host Behavior) 與網路行為 (Network Behavior) 之分析來提升對於新型態惡意軟體之辨識率。

(四)惡意程式之分類

由於本專案制定之資通安全技術檢測規範中，對於功能或定位不同（基本型或進階型）之資通設備，實機安全檢測時有難易度不同之樣本。我們從真實流量中所擷取之可疑程式，透過行為分析模組進行分析後，可依其辨識之難易度將其分成四大類：

1.容易辨認的正常程式。例如：此程式有原始碼，可詳細地分析並確認此程式無惡意的行為。

2.容易被資安設備辨認的惡意程式。例如：此程式一旦被執行，便會修改系統的檔案或是將系統內部重要的資訊散播出去。

3.容易被誤認為惡意的程式，其本質卻是正常的程式。例如：此程式會建立新的檔案或產生特權的系統呼叫，但對系統而言卻是無害的。

4.容易被誤認為正常的程式，但其本質卻是惡意的程式。例如：此程式在大部份的時間內無任何不正常之行為，在某一個事件發生時，才會觸發該程式進行危害系統之行為。

惡意程式以上述之方式分類後，即可作為實機檢測所需之樣本，最終即可建置一個國內最具代表性與完整性之惡意程式樣本資料庫供各界使用。

六、資通設備之安全檢測之合理費用與時程

(一)檢測費用訂定原則

1.設備檢測費用應分為基礎型與進階型檢測費用。

2.通過基礎型檢測合格之設備，自檢測合格日起三個月內，申請同一設備之進階型檢測者，其檢測費用只須補足基礎型與進階型費用之差額。

3.通過檢測合格之設備，當版本更新或是申請系列認證，得針對有變更之檢測項目進行重新檢測，檢測費用皆為全項檢測費用乘以重新檢測項目數占全部檢測項目數之比例計算。

4.申請設備檢測者被通知設備檢測未符合規定之日起一個月內，得向檢測實驗室提出設備修正，每一送測設備得做兩次修正，無須另外收費。

(二)書面審查費用估算

類別	項目	基礎等級 (人天)	進階等級 (人天)
安全標的	設備類型	3	3
	安全功能需求(SFR)	5	5
安全功能設計	安全功能規格	5	5
	設計安全性		5
	安全架構	3	3
	安全指引	3	3
共計		19	24

(三)實機測試費用估算

1.人力工時

測試大項	測試細項	基礎等級		
		工時 (人天)	小計 (人天)	合計 (人天)
安全功能測試	封包過濾	1	4	23
	流量內容統計	1		
	安全事件記錄	1		
	安全管理	1		
	備援管理			
	規則控管			
壓力測試	吞吐量	2	2	
	最大同時連線數			
	最大建立連線速率			
堅實測試	阻斷式攻擊	2	4	
	惡意流量			
	非正常關機復原	2		
穩定測試	真實流量測試	10	10	
其他	報表整理	3	3	

註: 失敗測項複驗(提供兩次複驗機會，此部份未算入。)

測試大項	測試細項	進階等級		
		工時 (人天)	小計 (人天)	合計 (人天)
安全功能測試	封包過濾	1	6	38
	流量內容統計	1		

測試大項	測試細項	進階等級		
		工時 (人天)	小計 (人天)	合計 (人天)
	安全事件記錄	1		
	安全管理	1		
	備援管理	1		
	規則控管	1		
壓力測試	吞吐量	2	6	
	最大同時連線數	2		
	最大建立連線速率	2		
堅實測試	阻斷式攻擊	2	6	
	惡意流量	2		
	非正常關機復原	2		
穩定測試	真實流量測試	17	17	
其他	報表整理	3	3	

註: 失敗測項複驗(提供兩次複驗機會，此部份未算入。)

2.測試環境/儀器設備

使用儀器	採購價格(NTD)	使用測項	提列年限
Spirent Test Center	600 萬	壓力測試	5 年
Spirent Avalanche	300 萬	壓力測試	5 年
Mu Dynamics	500 萬	堅實測試	5 年
Codenomicon	1000 萬	堅實測試	5 年
測試程式執行平台	100 萬	功能測試	3 年
Betasite 建置	700 萬	穩定測試	5 年
合計	3200 萬		

3.場地租用

	價格	使用測項	
實驗室場地租用(50 坪辦公室)	暫未預估	所有測試	

(四)影響檢測費用之重要變數

項次	變數	說明
1	每月送測件數	送測件數越多，平均成本越低(規模經濟)
2	驗證失敗可重驗次數	可提供重驗次數越多，成本越高(機會成本)
3	實驗室同時收件數量	影響租用場地大小，聘用人員多寡

(五)整體費用與時程

整體時程(每個案件) 單位: 人天

測試項目	基礎等級	進階等級
書面審查	19	24
實機測試	23	38
合計 (可併行測試)	23	38

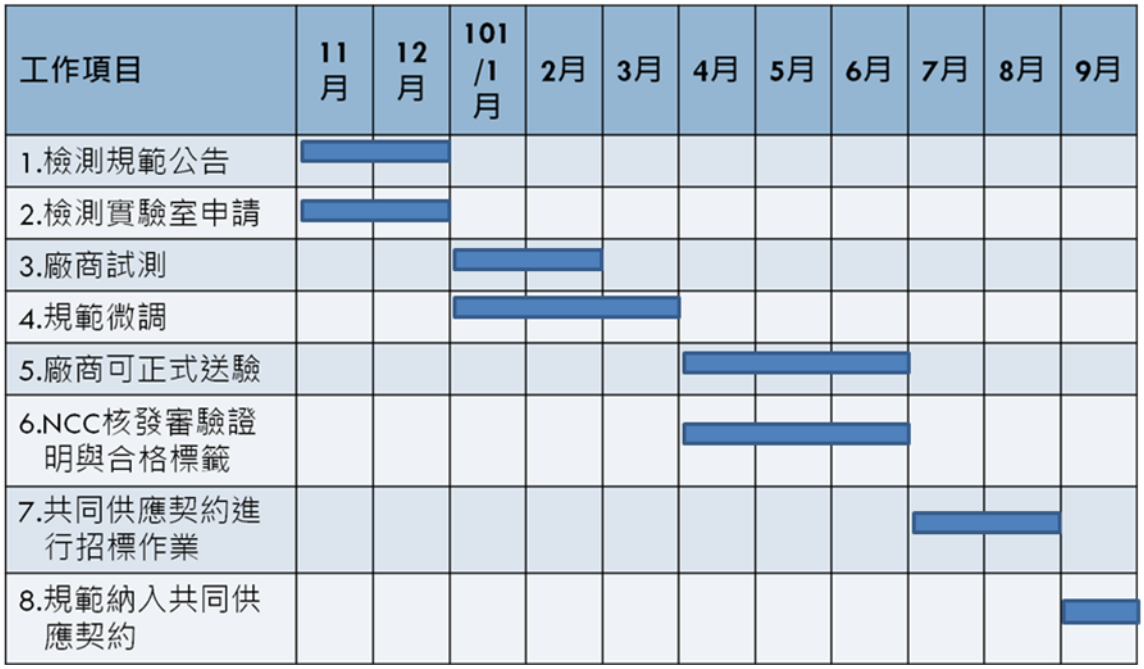
整體費用(每個案件) 單位: 仟元

項目	基礎等級	進階等級
人事費	800(年薪;含勞健保、勞退) x (23+19)(基礎型)/250(一年工作天數) = 134.4	800 x (24+38)/250 = 198.4
設備費	32,000/5(年) = 6,400/年，64,00/50(每年案件數) = 128 /案件	同基礎型。
成本小計	262.4	326.4
管 理 費 (10%)	29.1	36.2
成本合計	291.5	362.6

註 1: 目前成本只是概估，尚未估到空間租金、設備每年維護費用、每個案件兩次重測的費用。

註 2: 目前假設每年有 50 個案件。

(六)未來檢測機制推動時程建議



七、舉辦 3 場座談會(含期中 2 場座談會)及 1 場成果發表會

為使各項設備安全檢測技術規範、相關法規、採購參考指引、費用與時程符合國內市場之需求，期末前應辦理 3 場座談會及 1 場成果發表會，每場次邀請產官學研各界專家學者參加，二次專家學者座談會概述如下表：

表7　專家學者座談會概述

場次	時間	議題
第一次專家學者座談會	100/3/7(一)	議題一 專案簡介以說明本專案的目標及方法，進一步說明資通設備安全檢測現況。 議題二

場次	時間	議題
		以 Firewall 為例說明檢測技術規範的內容。 議題三 資通設備之安全檢測之設備項目清單，包括短中長期適用之設備項目。
第二次專家學者座談會	100/5/30(一) [註 1]	議題一 「資通設備之安全檢測研究計畫」專案執行狀況說明 議題二 防火牆技術規範全文與採購參考指引大綱
第三次專家學者座談會	100/8/30(三) [註 2]	議題： 檢測技術規範內容討論—網頁過濾管控設備(WAF)、網路安全監控設備(IM、P2P、社群網站等應用程式控管)
第四次專家學者座談會	100/9/1(四) [註 2]	議題 檢測技術規範內容討論—交換器、路由器
成果發表會	100/10/3(一) [註 3]	計畫成果與未來執行規劃說明 座談會-我國資通設備安全機制未來發展趨勢

[註 1]原應於 100/4/15 前辦理第二次專家學者座談會依據通傳技字第 10043008150 號來函，因相關人員 4/9-4/18 出國參訪，故延後辦理。

[註 2]原應於 100/8/12 前辦理第三次專家學者座談會，考量第三次專家學者座談會所提出之文件內容須符合第二次期中審查會議之審查委員意見，故通傳技字第 10000386090 號來函同意第三次專家學者座談會延後至 100/9/10 前辦理。

[註 3]原應於 100/9/23 前辦理成果發表會，為使委託研究之檢測規範內容更完備，近期已增加安排與多位相關領域專家、廠商代表進行個別訪談，並依據各界提出之建議修調規範文件內容，考量計畫成果於成果發表會上完整呈現。故通傳技字第 10000448590 號來函同意成果發表會由 100/9/23 前辦理延後至 100/10/7 前辦理。

(一)第一次專家學者座談會會議記錄

時間：中華民國 100 年 03 月 07 日(星期一) 14:30~16:45

地點：中華民國資訊軟體協會 (台北市承德路二段 239 號 6 樓)

主席：計畫主持人張國鴻秘書長

記錄：鍾如郁

1.報告事項

【報告一】計畫簡介與議題說明

【說　明】由協同計畫主持人陳一瑋報告專案內容與進度

【決　議】

(1)資通設備安全檢測技術規範-文件標準格式同意通過，提供電子檔案給予與會專家，後有任何意見可另行提出。

(2)同意目前整合 CC、ICSA、NSS 及真實環境的檢測技術規範項目。並強化國內實驗室檢測之強項(例如 NBL 的真實流量測試)，樹立國內標準的獨特優勢。

2.討論案

【說　明】99 年度列入檢測之 8 項資通設備，提請討論。

【決　議】

(1)以目前列入共同供應契約之資通安全設備優先。

(2)對承辦單位所提出 8 項資通設備，包括：防火牆設備、入侵偵測防禦設備、防毒閘道器設備、垃圾郵件過濾設備、網頁過濾管控設備、網路安全監控設備、乙太網路交換器、路由器，無異議。

(3)8 項資通設備中以防火牆設備、入侵偵測防禦設備、防毒閘道器設備、垃圾郵件過濾設備等四項，優先撰擬檢測技術規範與

標準。

3.其他建議

【說　明】針對本計畫相關內容邀請與會專家學者提供具體建議

【建　議】

(1)實驗室知名度與檢測能量是檢測制度能否成功與國際接軌的關鍵之一，建議應多扶植國內檢測實驗室使具國際知名度。

(2)建議檢測實施後，應規定國外產品也必須通過檢測才得以列入政府採購項目中。中長期則可考量 Smart Card 與 PKI 等項目。

(3)資料外洩防護(DLP)與資料庫稽核因應個資法需求大增，建議列入下一期檢測項目。

(4)根據採購法規定，檢測驗證標準必須為 CNS 國家標準或 ISO 國際標準，才可納入政府採購 RFP 規定中，且無法限制只有國內廠商可參與投標。在相關標準成為國際標準或國家標準前，無法限制外國廠商一定要取得認證。擬採環保標章模式推廣，希望機關優先採購是屬於政策面而非法規面的決定。

(5)希協助向國內使用者推廣：通過檢測之資通設備，安全性與可靠性都相對提高，使國內各機關單位放心採用。

(6)目前規劃 2 個月內、50 萬元可完成的檢測制度，整體推廣與政策協助下，外商公司應可接受國內認證。

(7)建議國內實驗室建立國際實驗室樣本資料庫，以利國際接軌。並可考量公布檢測活體，提供給廠商，可協助廠商快速通過檢測。

4.散會：下午 16 時 45 分

(二)第二次專家學者座談會會議記錄

時間：中華民國 100 年 05 月 30 日(星期一) 14:30~16:45

地點：中華民國資訊軟體協會 (台北市承德路二段 239 號 6 樓)

主席：計畫主持人張國鴻秘書長

記錄：李曉欣

1.報告事項

【報告一】計畫簡介與議題說明

【說　明】由協同計畫主持人陳一瑋報告專案內容與進度。

2.議題討論

【說　明】網路型防火牆資通安全檢測規範(草案)，提請專家學者提供建議。

【決　議】請依下列專家學者意見調整本規範(草案)

(1)P3 表 6 名稱誤植為 IPS 請調整之。

(2)規範中分為基礎與進階，建議進階功能以深度為主且其安全需求應有更明確定義。

(3)防火牆規範 P.12 可選取之稽核審查依 P.9 的定義，應非使用在稽核記錄之「搜尋」及「排序」的功能，而是效能考慮可將某些稽核記錄開啟或關閉。

(4)P14 進階等級防火牆需由廠商自行定義，建議應提出明確內容由廠商提供，避免模糊地帶。

(5)P.20 與 P.21 之「密碼」建議改為「通行碼」較為妥適，另備註欄建議避免特定實驗室之字眼。

3.意見交流

Q1. 基礎與進階有些項目差異性沒有很大的區分,是否有費用的差異性?

A1. 將於審驗辦法中設定不同的驗證費用，並經由 NCC 確認後才得以通過。

Q2. CNS15408，後續是否持續使用，有否相互承認？
國外有通過 CC 或 ICSA 之認證，是否有否對應或交互認可關係？

A2. CNS15408 乃國家標準與目前所撰擬之技術規範並不衝突，本技術規範撰寫時乃參照國外相關認證之規範,目前尚無法有交互認可關係。

Q3. 建議考量檢測重新申請的費用標準？

A3. 依據國際慣例重新申請是有其收費標準,但國內考量會將費用盡量降低,可考量將相關標準加入資通設備安全檢測實驗室管理作業要點中。

Q4. 針對單一產品項次，是否有送測項目的限制？例：單一產品只能送幾個項目或無限制。

A4. 目前針對單一產品項次並未進行送測項目之限制,但送測項目越多將會依據送測項目標準收取費用。

Q5. 目前整體規範與中國大陸是否接軌,是否能與大陸建立共通驗證？爭取大陸市場？

A5. 目前我國與中國大陸之規範源頭皆參考 CC 或其他國際實驗室之規範，故規範源頭大致相同，然建立共通驗證部分涉及廣泛無法與本次會議中進行討論。

4.其他建議

【說　明】針對本計畫相關內容邀請與會專家學者提供具體建議

【建　議】

(1)資通安全設備審驗作業要點應可規範產品測試版本，應參考國際標準定義，新的產品等級建議可於一定規範下直接通過認證。

(2)技術規範公開詳細的程度應取現行參考之國際或國外標準的最大值即可，若撰寫過於詳細則容易失去彈性，建議可分規範標準與參照方式分別處理。

(3)採購指引建議可參考資訊系統分類分級鑑別機制之要求。

(4)建議測試規範中，不同產品的功能面測試，應以該產品主訴求功能為主，避免不同產品類別、測試的功能面重疊，造成用戶混淆。此換言之，就是一個產品可通過不同類別規範，但避免不同規範互相重疊。

(5)測試項目建議增加 UDP 效能測試及 NAT/Transparent 功能測試項目。

5.散會：下午 16 時 45 分

(三)第三次專家學者座談會會議記錄

時間：中華民國 100 年 08 月 31 日(星期三) 14:30~16:45

地點：中華民國資訊軟體協會 (台北市承德路二段 239 號 6 樓)

主席：協同計畫主持人喻維貞資深處長

記錄：陳鐶洲

1.報告事項

【報告一】計畫簡介與檢測技術規範說明

【說　明】由協同計畫主持人陳一瑋報告計畫簡介與網頁過濾管控設備、網路安全監控設備檢測規範。

2.議題討論

【說　明】網頁過濾管控設備與網路安全監控設備檢測規範(草案)，提請專家學者提供建議。

【決　議】請依下列專家學者意見調整本規範(草案)

(1)依據目前現階段產品，建議將網頁過濾管控設備修改名稱為網頁應用防火牆、網路安全監控設備修改為應用軟體控管系統，則可廣納較多產品品項加入檢測規範。

3.意見交流

Q1. 國內都是中小型企業基本上應不太需要支援 IPv6？

A1. 目前有許多應用正透過 IPv6 閃躲偵測且目前共同供應契約上將 IPv6 建議為標準採購項目，此項將會取得業界共識後才進行。

Q2. 軟體可以搭配任意硬體販售，請問是否適用規範？

A2. 目前軟體不在規範規定的範圍中。

Q3. 測試團隊技術能力是否足夠？NCC 如何證明測試團隊之測試能力?

A3. 已於檢測實驗室管理作業要點中載明檢測實驗室比須通過 ISO17025 之實驗室規範標準，才得以申請成為本規範之檢測實驗室，此部分將由 NCC 進行管控要求。

4.其他建議

【說　明】針對本計畫相關內容邀請與會專家學者提供具體建議

【建　議】

(1)若相同樣本有足夠深度，則可使用相同樣本進行基礎與進階認證。但依據使用者立場來說應以不同樣本檢測基礎與進階等級較佳。

(2)針對功能面測試越多，越容易限制產品成為相同類型，造成產

品無差異化。軟體廠商也會根據通過檢測的設備來選擇硬體，最終可能造成硬體皆相同之情形。建議功能檢測的重點放在有沒有後門，服務有沒有漏洞等議題上。

(3)同一系列之產品或同產品重測，建議其費用部分採測試項目計收，以真實反映成本減輕廠商負擔。

(4)建議於共同供應契約中將此規範列為必要條件，可增加廠商受測意願，若非必要條件，廠商若無可預期銷售便不願意花時間與經費在檢測上，則枉費此次計畫之立意良善。

(5)部分設備過濾垃圾郵件時並非使用垃圾信關鍵字，而是使用垃圾郵件來源，若目前檢測方式可能無法通過，建議考量不同檢測方式。

(6)建議除了校園測試流量外，應嘗試拿到企業界樣本，並加上正體中文樣本，以強化整體測試樣本。

(7)共同供應契約為價格決標，無法提升產品的毛利率。建議驗證應以保障最基本的安全功能為目標，基本等級由政府付費，若進階等級可藉此提升廠商毛利率，則可由廠商付費。

(8)檢測設備即使可有兩次的修正機會，但若無法取得樣本，二次檢測的通過機會不高，建議可於不通過的時候提供部分樣本給受驗廠商，以利產品進行修調。

(9)建議檢測規範實行前應有試測與緩衝期，或可於試測緩衝期間免費提供廠商進行檢測，以利整體規範推動。

(10)就國家的角度而言制定一個檢測規範有其一定的效力，會比沒有來的有保障，但建議不應該給業者太多負擔。

(11)以政府單位立場，若規範正式上路後，將可告知各單位優先

採購通過 NCC 認證之產品。

(12)建議規範中功能面部分，應盡可能符合業界與使用者之間的共識。

(四)第四次專家學者座談會會議記錄

時間：中華民國 100 年 09 月 01 日(星期四) 14:30~16:45

地點：中華民國資訊軟體協會 (台北市承德路二段 239 號 6 樓)

主席：協同計畫主持人喻維貞資深處長

記錄：陳鐿洲

1.報告事項

【報告一】計畫簡介與檢測技術規範說明

【說　明】由協同計畫主持人陳一瑋報告計畫簡介與交換器、路由器設備檢測規範。

2.議題討論

【說　明】交換器、路由器設備檢測規範(草案)，提請專家學者提供建議。

【決　議】請依下列專家學者意見調整本規範(草案)

(1)依據目前現階段產品，建議將交換器修改名稱為乙太網路交換器、路由器修改為路由交換器，則與目前市面上產品名稱較為接近。

3.意見交流

Q1. Page 28, L3 Switch 安全管理功能，鎖定的功能實作後，可能會造成其他正常 session 產生斷斷續續的問題。是否可以使用其他功能如 VLAN 的方式取代。

A1. 此建議將由技術團隊進行討論，若會影響到其他功能，將會修正此測項。

Q2. Page 35, L3 Switch CHAP 加密，為何要加入這項測試項目？

A2. 由於共同供應契約中，路由交換器分為三類，目前規劃為涵蓋 LAN and WAN Switch 兩大類，因此包含這個項目。未來如涵蓋類別有變動，測項將會一併修調。

Q3. 書面審查的測試項目，判定通過的標準為何？是否能更加詳細的說明通過標準？

A3. 以防火牆規範做為說明，要求的資訊在規範內皆有詳實描述。

Q4. 通過檢測後的標準是否會對應到 EAL 等級?

A4. 目前檢測標準分成基礎與進階兩個等級，並不會與 EAL 對應。

Q5. 測試時間兩個月內，測試費用 50 萬以內，相較於國外 EAL 的測試時間來說短很多，請說明檢測結果的可信度？

A5. EAL 是 CC 的標準，但 CC 審驗的成本高，世界各國政府(含美國及日本)採用的比例並不高，另外 CC 審驗時間冗長的問題也不易跟隨上最新的資安漏洞及攻擊手法。因此我們這分規範使用去蕪存菁的方式，保留 CC 適用於我國的部分後加以套用，且容易加入最新的資安漏洞及攻擊手法相信有助於強化檢測結果可信度。

Q6. 設備不僅是單一功能，若為複合功能設備，在壓力測試部分如何進行？

A6. 目前壓力測試是採用待測物的預設值來進行。

Q7. 檢測過程中的兩次修正機會如何計算？

A7. 目前的計算方式為書面+實機兩次以內。未來或許可考量調整為書面及實機各兩次修正機會藉以放寬標準。

Q8. 規範實際推動的時程為何？

A8. 以台銀共同供應契約來說，下次更新時間為明(101)年八月，

此實施時機點離目前尚有一段準備時間,可逐步進行規範之推動。

Q9. 若取得 CC 的某個等級，是否可以承認部分測項，以加快測試速度？

A9. 書面審查的項目可考量是否直接通過,但國內與國外測試目前並無相互承認，故目前傾向不承認國外測試。

Q10. 建議可將安全功能中鑑別失敗處理之判定標準改為鎖定非法登入者的 IP 或 MAC 位址。

A10. 此部分仍有討論空間，若改為鎖定非法登入者的 IP 或 MAC 位址，非法登入者則可採用不斷更換 IP 或 MAC 位址的方式重覆攻擊，則無法對此進行鎖定，恐有安全上之疑慮。

4.其他建議

【說　明】針對本計畫相關內容邀請與會專家學者提供具體建議

【建　議】

(1)穩定測試建議改以 session 數管制，而非以 user 數進行測試。

(2)安全管理功能中，當管理者離開管理介面時的 timeout 機制可以考慮成為測試項目之一。

(五)成果發表會會議記錄

時間：中華民國 100 年 10 月 03 日(星期一) 14:30~16:45

地點：中國文化大學推廣教育部大夏館 國際會議廳

(台北市建國南路二段 231 號 B1)

主席：計畫主持人張國鴻秘書長

記錄：陳鐶洲

1.報告事項

【報告一】計畫成果說明

【說　明】由協同計畫主持人陳一瑋報告計畫成果

2.座談會討論

(1)本計畫 8 項產品的檢測技術規範的主要目的是要幫政府部門做資通訊設備產品的安全把關，並制定出在時程及經費上符合國內業者需求的測試內容；讓業者在能負擔的情況下檢測出產品是否符合資安規格，並提供政府單位在採購時參考。

(2)CNS 國家標準並非強制性，多數是國外標準轉為中文版。目前共同供應契約上已有 CC 之規範，但若僅有 CC 標準列入規範中，對國內廠商而言有所不公。未來規劃希望於明年 9 月可列入共同供應契約中，讓政府單位在採購的時可以選擇是否採用；並建議列為強制性條件。

(3)目前所訂出的檢測技術規範等內容仍為草案，歡迎各界參考並提供寶貴的意見做為參考，以將規範修改的更完善。建議可由 NCC 成立溝通平台，讓廠商、檢測實驗室、NCC 驗證單位及使用者能有個交流平台，持續的改善此驗證機制的相關辦法。

(4)對機關採購而言，以鼓勵取代強制，循序漸進之方式鼓勵機關採購；對廠商則是可以提供更廣大的市場。

(5)日前台銀共同供應契約不但資格訂定需要國際認證，價格又不合理的砍價，對國內廠商相當不公平。

(6)國外驗證有費用上之考量，國內驗證可當作至國外驗證之前哨站，並可協助國內廠商進軍國際，最終目標乃是以通過國內認證即可獲得國內及國際二張證照。

(7)希望可將此規範列為國內 CNS 國家標準，讓政府機關可依採購

法直接適用。以政策面而言，將來應將規範列入共同供應契約之中，以推廣此項認證；實務面則是由做中學，朝向更完善的制度及能力；而技術面則是由驗證實驗室來協助加強。

(8)此規範的制訂不僅可以增加資安業者的需求量，對於民眾的信心提升更有顯著的影響；重點不只是降低成本，更重要的是提升資安產品的品質。

(9)未來規範也要考慮用何種方式與國際接軌，讓業者通過此規範也能朝國際市場邁進。

(10)檢測實驗室規範之保密內容,經濟部規定應通過 TAF 認證，建議 NCC 可依此為標準考量。目前檢測實驗室要通過必須有 ISO 17025 的認證，且將由 NCC 與相關專家評鑑檢測實驗室是否符合資格，另應考量認證實驗室是否可完全保密，建議應有機制進行控管，並建立相關罰則。

(11)樣本資料庫不容易分享出來，所有單位皆缺乏樣本資料庫，要所有單位皆貢獻出來，會有其差異性。希望檢測樣本資料庫可請研考會提供相關資源，以獲得更多的檢測樣本。

(12) 此計畫短期來看會增加驗證成本，似乎是對廠商有其障礙；但就長期而言，可藉此提升廠商之資安產品之品質，增加銷售量。

(13) 如何讓改變可以轉換成商機是很重要的，日前台銀所提出的採購條件中列出了須要通過國際認證則是對國內廠商很不公平，若可將此國內之認證取代採購條件，則是眾所樂見。

(14) 建議認證初期都有免費或優惠辦法來促進業者認證。

(15) 有關檢測費用制訂會再與業者溝通出合理價格，並且會有優惠方式，但內容仍須再討論。