103 年委託研究報告

103 年資通設備之安全檢測規範增修訂及推廣計畫委託研究案期末報告書

計畫委託單位：國家通訊傳播委員會

中華民國 104 年 4 月 15 日

103 年委託研究報告
PG10306-0183

103 年資通設備之安全檢測規範增修訂及推廣計畫委託研究案期末報告書

受委託單位

中華民國資訊軟體協會

計畫主持人

喻維貞

協同主持人

詹麗淑

研究人員

楊蕙如、力信恩、王井強、陳鍠洲、林敏凡、姚人鳳

中華民國 104 年 4 月

目　次

四、 附件四 進階持續性威脅防禦設備(APT Defense System)資通安全採購參考指引草案(初稿)

五、 附件五 行動無線寬頻分享器(Mobile Wi-Fi Hotspot 資通安全檢測技術規範草案(初稿)

六、 附件六 行動無線寬頻分享器(Mobile Wi-Fi Hotspot)採購參考指引草案(初稿)

七、 附件七 虛擬私人網路閘道器(VPN Gateway)資通安全檢測技術規範草案(初稿)

八、 附件八 虛擬私人網路閘道器(VPN Gateway)採購參考指引草案(初稿)

九、 附件九 103 年資通設備試測報告

十、 附件十　現有規範檢討與修正

十一、 附件十一　座談會會議記錄及簽到表

十二、 附件十二　7 場次推廣說明會簽到表

十三、 附件十三　性別相關統計比例

十四、 附件十四　各品項產品彙整

表　次

圖　次

提要

關鍵詞：資通設備、安全、檢測規範、採購參考

一、研究緣起

為持續強化政府機關(構)使用之資通設備安全性，並促進我國資通環境安全，茲擬定新增資通設備安全檢測規範，並進行推廣，以利各級政府機關了解並得以應用。

二、研究方法及過程

本會將計畫工作項目分為三類重點執行，計畫研究方式與整體架構如下：

(一)「制定檢測規範」

持續提升我國資通設備安全性與一致標準，針對現行資通設備使用狀況，在短、中、長期檢測技術規範發展策略框架下，綜合考量國內資通安全產業供需環境與國際檢測規範內容，研提 4 項適合我國之資通設備安全檢測規範。並藉由座談會，了解各政府機關對於既有規範於執行面之看法。

(二)「檢討檢測規範」

針對國家通訊傳播委員會於 100、101 年所完成之 10 份技術規範進行檢討，藉由會議之辦理，了解各界代表對於既有技術規範實際執行狀況，檢討技術規範之適切性，研提修正建議使規範更符合國內環境需求。

(三)「推動安全檢測」

為推動國內政府機關採用、資通設備廠商參與檢測，將撰擬政府機關(構)資通設備採購參考指引及推動建議，並辦理座談會及推廣說明會，除可了解現行各政府機構資安人員組成與背景，亦能藉

由推廣會議推廣資通設備安全測試觀念及做法之普及。

本計畫研究範圍如下：

1.研提 4 項資通產品檢測技術規範，包括書面審查與實機檢測，實機檢測包含功能面、效能面、穩定面以及堅實面。

2.檢討 10 項現行資通安全設備檢測規範並提出修正建議。

3.提出資通安全設備檢測規範推動建議，並辦理相關推廣活動。

三、重要發現 research detection

(一)研提 4 項資通設備之安全檢測規範草案

1.本年度建議撰擬之 4 項資通產品分別為：資料庫安全稽核設備(Database Activity Monitor, DAM)、進階持續性威脅防禦設備(Advanced Persistent Threat Defense System, APTDS)、行動無線寬頻分享器(Mobile Wi-Fi Hotspot)、虛擬私人網路閘道器(VPN Gateway)。

2.規範草案書面審查部分以產品出廠後，最主要且直接影響產品安全功能及品質的項目進行審查，規範另有安全功能測試、壓力測試、堅實測試及穩定測試等四個的實機檢測項目，並納入基礎型與進階型之檢測分類內容請參考附件一、三、五、七。

(二)研提 4 項資通設備採購參考指引草案

1.為協助政府機關熟悉資通設備產品，以及其佈署之規劃、設定、檢查與更新資訊，撰擬資通設備採購參考指引，提供檢測項目功能之說明。

2.參考指引將可促使機關了解檢測分級保障範圍及效益，以利機關將來選擇採購產品時之參考。詳細內容請參閱附件二、四、六、八。

(三)邀集資安設備廠商試測新增訂之資通設備安全檢測技術規範

1.書面審查部分以產品出廠後，最主要且直接影響產品安全功能及品質的項目進行審查。

2.本規範設計了安全功能測試、壓力測試、堅實測試及穩定測試等四個主要的實機檢測項目來彌補書面審查的不足及盲點，新增 4 項檢測技術規範已分別邀請廠商進行試測，並依據試測結果進一步調整規範內容，詳細內容請參閱附件九。

(四)檢討現行資通設備安全檢測技術規範

依據 100~103 年資通安全設備檢測結果，以通傳會公告之資通設備安全檢測技術規範為基礎，檢討現行 10 種現行安全檢測技術規範並修正之。

(五)對新增訂及現行資通設備安全檢測規範廣徵修正意見

1.針對新增訂資通安全檢測技術規範之品項擇定、新增訂技術規範內容及現行資通設備安全檢測規範之意見，計辦理 3 場座談會。

2.邀集產官學代表共同研析討論，會議結論皆為各規範之依循方向。

(六)推動政府機關選用符合本會安全檢測規範之資通設備

為推動資通設備安全檢測技術規範，於全國北中南東及離島地區辦理 7 場次推廣說明會，向政府機關說明規範內容與通過審驗之優點。

(七)提出本案與性別相關之統計及分析

經統計瞭解與本案相關之資訊、採購人員性別、學歷比例等差異性。

四、主要建議事項

(一)立即可行之建議

1.逐年進行規範編撰，逐步提升資安產業自我研發能量，健全資安整體環境。

2.輔導業者通過檢測技術規範或提供檢測補助，提高廠商參與意願。

3.積極推動規範納入共同供應契約

4.推動示範性機關使用通過檢測設備

(二)中長期性建議

1.通過檢測設備廠商與機關使用經驗分享，強化檢測品質與優勢

2.長期建立法源依據，強化整體國家資訊安全

Abstract

Keyword: Information and Communications Devices、Security、Testing Guide、Purchase Guideline

1. The origin of Research

   To strengthen the security of using information and communications devices in the government agencies, and promote the safety of domestic information and communications environment, this project compile 4 new security testing guides, and promote the security testing guides. Therefore the government agencies can select in line with the security testing guides for information and communications devices from NCC.

2. Research Methods and Process

   This project's main work is divided into three categories, the research methods and process are as follows:

   - Security testing guides for information and communications devices

     According to the usage of the government agencies, the 4 kinds of new security testing guides, which are considered in the development strategy framework of the compile security testing guides, could make the the standards of the security of using information and communications devices accordant. By the symposiums, this project could ensure that the security testing guides in this project can meet the demands of government agencies.

   - Review security testing guides for information and communications devices

     According to the preliminary results of security testing for information and communications devices in 2011-2012, we review 10 kinds of existing security testing guides. Hold symposiums to ensure that the security testing guides in this project can meet the demands of the domestic market of information and communications devices and the

government agencies.

- Promote security testing

  To promote the government be familiar with security testing guides for information and communications devices, let the manufacturers go testing the security guides, we hold the promotion sessions and guides symposium to explain the content and the benefits of certification to the government agencies. Through these promotion sessions, we can comprehend the government information security agencies, and popularized the testing of the information and communications devices.

The scope of the study are as follows:

- 4 kinds of security testing guides for information and communications devices(draft), include the documentation review and device evaluation, the device evaluation includes security function evaluation, stress test, robustness test and stability test.
- Review and revised 10 kinds of security testing guides for information and communications devices.
- promote security testing guides for information and communications devices, hold the promotion sessions to explain the content and the benefits of certification to the government agencies.

3. Research detection

- 4 kinds of purchase guidelines for information and communications devices(draft).

  Threr’re 4 kinds of new purchase guidelines (draft) for information and communications devices : Database Activity Monitor (DAM), Advanced Persistent Threat Defense System (APTDS), Mobile Wi-Fi Hotspot, VPN Gateway.

  The document review inspects the items that affect the security function and quality most after the devices are released. Moreover, the guide

includes four device testing items, security function testing, stress testing, robustness testing and stability testing. The items are also divided into basic and advanced items. To learn more about the information, please check Appendix 1, 3, 5 and 7.

- 4 kinds of purchase guidelines for information and communications devices(draft).

  To help the government be familiar with information and communications devices, including the deployment plan, setting and examination and update information, there are guidelines for the purchase, including the explanation of testing items.

  The government can understand the protection scopes of examination classification and benefits. The guidelines can be a great reference for the government in purchasing products in the future. To learn more about the information, please check Appendix 2, 4, 6 and 8.

- Invite the manufacturers of new information and communications devices testing guides.

  The document review inspects the items that affect the security function and quality most after the devices are released.

  The guide includes four device testing items, security function testing, stress testing, robustness testing and stability testing to complement the insufficiency of document review. There’re 4 manufacturers testing the new draft purchase guidelines for information and communications devices. To learn more about the information, please check Appendix 9.

- Review and revised 10 security testing guides for information and communications devices.

  According to the preliminary results of security testing for information and communications devices during 2011 – 2014, based on the security testing guides for information and communications devices from NCC,

review and revised 10 security testing guides for information and communications devices.

- Ask for the revision opinion of the security testing guides for information and communications devices.

  Hold 3 symposiums to selects the item of the new ecurity testing guides for information and communications devices, to ensure the content of the new security testing guides in this project.

  Bring the representatives of industry, government and science together to discuss the research analysis. This project will follow the conclusions of the symposiums.

- To promote the government agencies to select in line with the security testing guides for information and communications devices from NCC

  To promote security testing guides for information and communications devices, hold 7 promotion sessions to explain the content and the benefits of certification to the government agencies.

- Gender statistics and analysis

  Statistics and analysis the proportion of gender, education of the I.T.,Procurement staff.

4. Recommendations

- Immediately feasible recommendations
  - Yearly guideline revision to enhance the R & D capabilities of the information security industry, strengthen the environment of the information security industry.
  - Counseling the manufacturers of information and communications devices pass the testing or provide the testing grants to increase the manufacturers' willingness to participate.
  - Promote the security testing guides into the supply contracts.
  - Promote the exemplary government agencies to select in line with

the security testing guides for information and communications devices.

- Long-term recommendations
  - By detecting equipment manufacturers and agencies to share the experiences, strengthen the benefits and the certification of the security testing guides for information and communications devices to the government agencies.
  - Establish the law of the security for information and communications devices, strengthen National Information Security.

壹、緒論

一、專案名稱

「103 年資通設備之安全檢測規範增修訂及推廣計畫」委託研究案

二、專案目標

為持續強化政府機關(構)使用之資通設備安全性，並促進我國資通環境安全，本專案之計畫目標如下：

(一)增加政府機關選用符合通傳會安全檢測規範之資通設備

通傳會至 101 年底已制定 10 項資通設備安全檢測技術規範，為滿足政府採購資通安全設備的安全保障，及因應資安攻擊技術的日新月異，應持續新增資通設備安全檢測技術規範品項，讓政府機關可採購通過驗測之設備。

(二)邀集資安設備廠商試測，完善新增訂之安全檢測技術規範

為使今年度新增訂之資通設備安全檢測技術規範於實務上達到產品資安防護水準，將邀集資安設備廠商進行試測，期望藉由實機試測結果讓廠商了解測試項目及作業方式，並以試測結果調整新增訂之資通設備安全檢測技術規範，確認規範之可用性。

(三)檢討現行資通設備安全檢測技術規範，以更符合產業實際所需

由通傳會認可之資通設備安全檢測實驗室依據過往檢測經驗，就現行安全檢測技術規範進行檢討，並邀請業者、機關代表針對規範提供修正意見，讓設備檢測規範內容更符合機關及產業需求。

(四)推廣符合通傳會安全檢測規範之資通設備

藉由檢測技術規範的推廣，可使通過通傳會檢測之產品品項，更容易為政府機關所採購使用，讓機關使用者對通傳會所擬之檢測

技術規範更具信心，以建立買方市場規模，逐步將供需雙方之資安品質要求向上提升，進而健全國內資安環境。

三、專案研究範圍

(一)研提 4 項資通產品檢測技術規範，包括書面審查與實機檢測，實機檢測包含功能面、效能面、穩定面以及堅實面。

(二)檢討 10 項現行資通安全設備檢測規範並提出修正建議。

(三)提出資通安全設備檢測規範推動建議，並辦理相關推廣活動。

四、交付項目

自契約生效次工作日起至 104 年 2 月 11 日前提出期末報告中文版本 14 份，期末報告書包含下列項目，本會已完成並列於對照頁內：

表1　交付項目對照表

項次	內容	已完成	對照頁
1	4 項新增之資通設備安全檢測規範項目。	已完成擇定 4 項新增之資通設備安全檢測規範項目。	P5-11
2	4 項新增加之資通設備安全檢測技術規範草案(初稿)。	已完成 4 項新增加之資通設備安全檢測技術規範草案(初稿)。	P11-23 附件一、三、五、七
3	4 項新增加資通設備採購參考指引草案(初稿)。	已完成 4 項新增加資通設備採購參考指引草案(初稿)。	P23-26 附件二、四、六、八
4	資通設備試測作業	已完成資通設備試測作業	P26-38 附件九
5	10 項現行資通設備安全檢測規範修正意見。	已完成 10 項現行資通設備安全檢測規範修正。	P39-515 附件十
6	已辦理之座談會活動紀錄。	已完成辦理 3 場座談會	P51-55 附件十一

項次	內容	已完成	對照頁
7	7 場次推廣說明會辦理	已完成辦理 7 場次推廣說明會	P56-65

貳、研究發現

一、本年度資通設備之安全檢測規範項目

本會於 100、101 年「資通設備之安全檢測研究計畫」中，已依據國際檢測項目及國內產業發展狀況、政府採購設備需求等，並依循短、中、長期檢測技術規範發展策略，研提 10 項安全檢測規範與採購參考指引，10 項安全檢測規範之檢測產品如下：

1.網路型防火牆(Firewall)

2.入侵偵測防禦系統(IDP)

3.防毒閘道設備(Anti-Virus)

4.網路型垃圾郵件過濾設備(Anti-Spam)

5.網頁應用防火牆(WAF)

6.應用軟體控管系統(AC)

7.乙太網路交換器(L2 Switch)

8.路由交換器(L3 Switch)

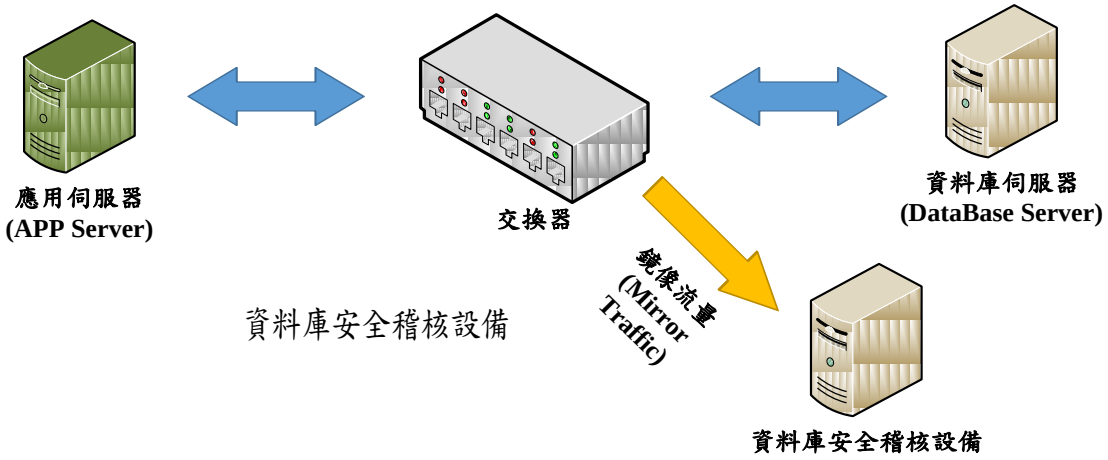
9.無線接取設備(Thin AP+控制器或 Fat AP)

10.無線區域網路路由器(Wireless Router)

本年度建議撰擬之 4 項資通產品如下：

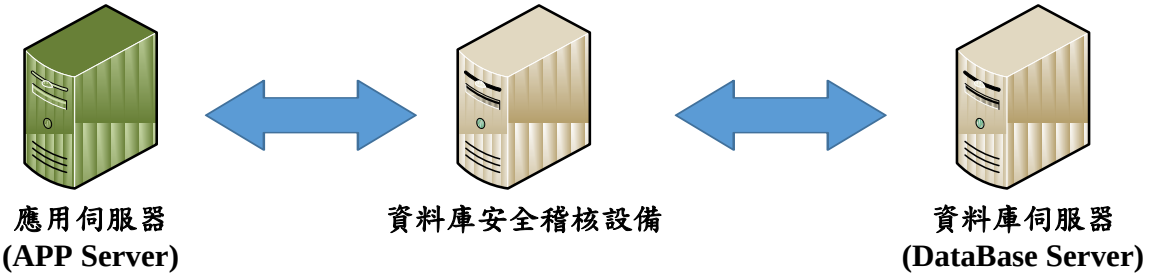
(一)「資料庫安全稽核設備(DAM)」[1]

資料庫安全稽核設備 (Database Activity Monitor, DAM)是一種資料庫安全技術，用來監視及分析資料庫活動，DAM 是獨立運作於資料庫管理系統之外，以應用程式面來偵測異常資料庫讀取和更新活動，進而改善資料庫的安全性。資料庫安全稽核設備並需提供持續性及即時性的監控運作，對違反稽核政策的行為或未經授權的活動提供告警機制。



資料來源：本計畫自行整理

圖1　資料庫安全稽核設備示意圖(1)



資料來源：本計畫自行整理

圖2　資料庫安全稽核設備示意圖(2)

[1] 本項產品名稱於本計畫第一次專家學者座談會時建議為：「資料庫監控設備(DBAM)」，然經相關資料參考，改引用財團法人**電信**技術中心(TTC)用所使用之名稱：「資料庫安全稽核設備(DAM)」，以利使用者了解。

(二)「進階持續性威脅防禦設備(APT Defense System)」[2]

進階持續性威脅防禦設備(Advanced Persistent Threat Defense System, APTDS)透過對可疑程式碼的深層分析及惡意通訊的辨認，偵測進階持續威脅(Advanced Persistent Threat, APT)對特定用戶端（如具備較大權限或可存取機敏資料之用戶）之特定應用漏洞進行之攻擊，攻擊模式的生命週期可分為：

1.初步的入侵：利用一些釣魚網站或電子郵件來做為入侵的媒介。

2.建立立足點：植入 Rootkit 等惡意程式以掌握使用者系統。

3.取得官理權限：利用破解密碼等方式取得該電腦管理者權限。

4.內部偵查與平行擴散：找尋該主機附近的其它主機或伺服器，並伺機取得期內部資料庫儲存之機密資料。

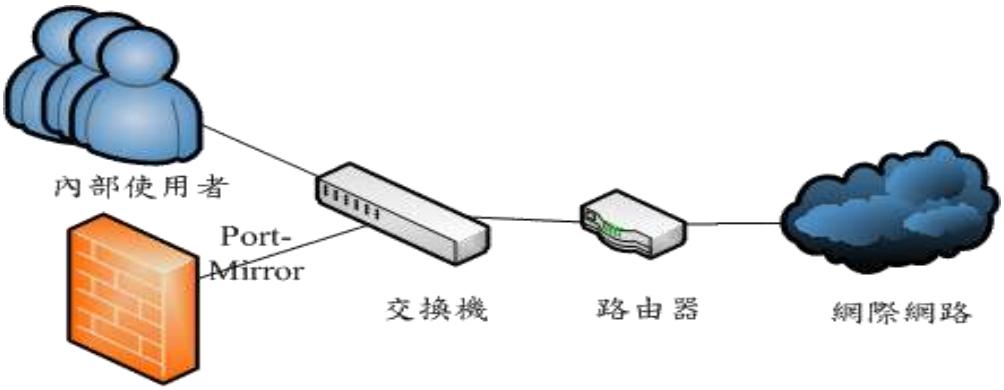
5.持續監控並完成任務：持續掌控資料庫伺服器或是主機，並將資料匯出達到竊取機密的目的。

攻擊內容則包括進階惡意程式(Advanced Malware)與零時漏洞攻擊(Zero-Day Exploit)，或是長時間且持續性的潛伏及監控，這些攻擊模式可能繞過傳統偵測機制，包括應用層防火牆(Application Firewall)、網站應用程式防火牆(Web Application Firewall)、入侵偵測防禦系統(Intrusion Detection and Prevention Systems)、防毒軟體(Anti-Virus)與端點防護系統(Endpoint Protection)等，而 APTDS 的價值就在無特徵碼比對的情況下，可以透過觀察受防護主機的異常行為模式（例如：連線至特定中繼站、開啟特定連接埠等）早

[2]本項產品名稱於本計畫第一次專家學者座談會時建議為：「APT 防護設備(APT Protection)」，然經相關資料參考，改引用財團法人電信技術中心(TTC)用所使用之名稱：「進階持續性威脅防禦設備(APT Defense System)」，以利使用者了解。

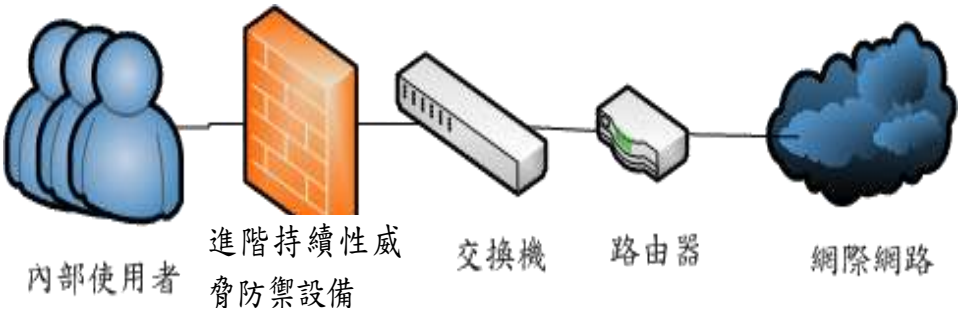
期發掘攻擊的存在，進而採取應變措施。

此種類設備有兩種運作模式，包含監聽模式 (Monitor Mode)與線上模式 (In-Line Mode)，示意如下：



資料來源：本計畫自行整理

圖3　Monitor Mode 示意圖



資料來源：本計畫自行整理

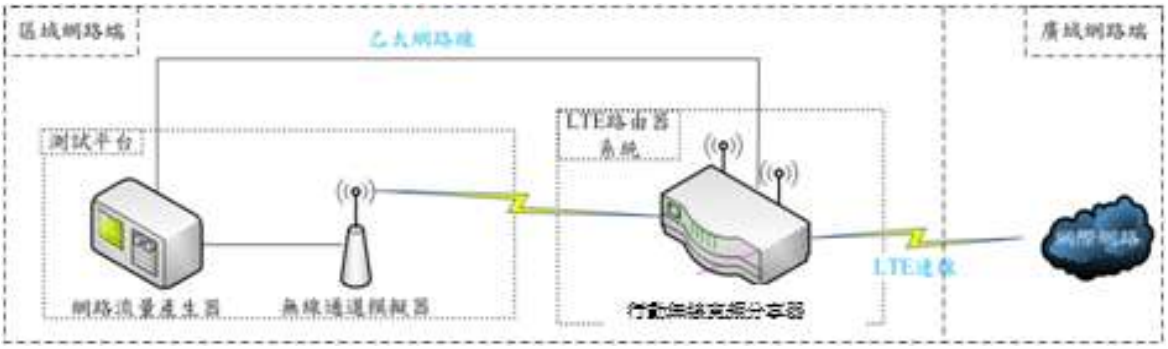
圖4　In-Line Mode 示意圖

(三)「行動無線寬頻分享器」[3]

行動無線寬頻分享器可讓使用者在進入組織/單位後透過此設備以

[3]本項產品名稱於本計畫第一次專家學者座談會時建議為：「無線寬頻分享器」，然經相關資料參考，改引用財團法人**電信**技術中心(TTC)用所使用之名稱：行動無線寬頻分享器」，以利使用者了解。

行動上網方式對外連線上網，並且對內以無線方式分享給更多其他用戶經由該設備上網。由於透過此管道上網時資料傳輸過程將不受組織/單位管控，因此該設備對外連線是否安全將成為資料傳輸安全的關鍵。

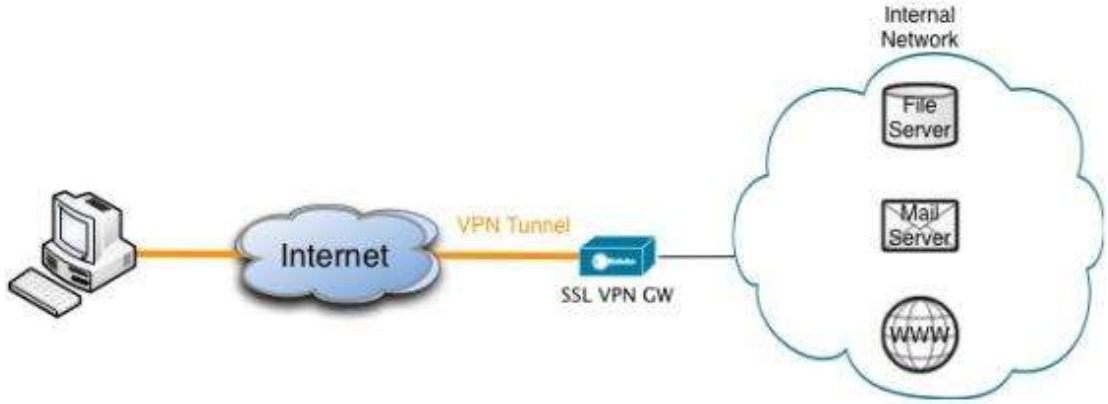


資料來源：本計畫自行整理

圖5　行動無線寬頻分享器示意圖

(四)「虛擬私人網路閘道器(VPN Gateway)」

虛擬私人網路閘道器(Virtual Private Network Gateway, VPN Gateway)可藉由加密網路封包提升網路傳輸的安全性，虛擬私人網路閘道器通常有遠端存取(Remote Access)及點對點(Site to Site)兩種不同的應用模式，可以透過 RFC 2246 SSL(Secure Sockets Layer)及 RFC 2401 IPSec(Internet Protocol Security)兩種技術標準來達成。使用點對點模式，組織可以直接利用網際網路串連兩個私人網路而不犧牲傳輸過程中的安全性，省去佈建專用實體線路的硬體成本。而使用遠端存取模式可以在保證資訊安全的狀況下，讓使用者透過公開的網際網路存取私人網路中的資源，更有彈性地的提供資訊服務。



資料來源：本計畫自行整理

圖6　虛擬私人網路閘道器示意圖

資通設備本身之資安顧慮愈高，就愈需以檢測來區分及保障設備安全等級，因此優先性亦愈高。近來資安攻擊事件中主要可進行偵測、預防之品項，其資安顧慮與所面臨之威脅如下分析：

表2　資通安全設備之資安顧慮

設備	資安顧慮
資料庫安全稽核設備	組態設定頁面可能被任意存取，亦可能遭受阻斷式攻擊，資料庫存取紀錄及防止紀錄被盜取及竄改
進階持續性威脅防禦設備	組態設定頁面可能被任意存取，且無支援樣本分析機制，受阻斷式攻擊亦無法有反制機制
行動無線寬頻分享器	使用無線傳輸，須具備驗證其資料保護功能(e.g. NAS)，以維護使用者資料傳輸時的隱密性
虛擬私人網路閘道器	封包重播攻擊、資料完整性檢查。已知軟體漏洞的利用，如 heartbleed：取得 ssl private key、 session cookie、帳密等資訊。組態設定頁面可能被任意存取，亦可能遭受阻斷式攻擊

資料來源：本計畫自行整理

表3　資通安全設備之所面臨威脅分析

項目設備	共同威脅			額外威脅		
資料庫安全稽核設備	遭入侵並竄改設定參數	遭受阻斷服務式攻擊	未經授權的使用者存取服務	Pattern update (特徵碼更新)	url obfuscation (URL 混淆)	
進階持續性威脅防禦設備				Anti-Detection 機制(反偵測機制)	檔案加密/封裝規避	特徵碼更新
行動無線寬頻分享器				資料傳送時遭竊聽	NAT 功能失效	
虛擬私人網路閘道器				資料傳送時的遺漏或不完整 (Data integrity)	重播攻擊 (Replay attack)	

資料來源：本計畫自行整理

國際資通訊市場競爭激烈，我國雖為全球通訊用戶終端設備重要的研發與生產重鎮，唯國際大廠以產品通過國際組織 CC(Common Criteria)驗證通過之優勢，進入我國政府及民間大廠市場，為協助我國資通訊設備廠商發展，將選擇國內具自主研發能量，且有與國際大廠競爭、外銷實力之產品，期望透過資通設備安全檢測技術規範之實作，讓業者提高產品品質，預做國際檢測之準備。茲將 4 項資通產品與其對應廠商統計如下：

表4　4 項資通產品與其對應廠商

設備	代表業者
資料庫安全稽核設備	玄力科技(Chalet Tech)、庫柏資訊(Cobrasonic)、希比思系統(CPS Systems)、GSI 全球系統整合、利基

設備	代表業者
	公司(L7-Networks)
進階持續性威脅防禦設備	艾斯酷博、台灣威瑞特、趨勢（Trend Micro）、阿碼證點、數位資安(iSecurity)
行動無線寬頻分享器	中磊(Sercomm)、智易(Arcadyan)、盟創(MitraStar)、明泰(Alpha Networks)、正文(Gemtek)、亞旭(ASKEY)、智捷(Z-Com)、達創(Delta Networks)、合勤(ZyXEL)、友訊(D-Link)
虛擬私人網路閘道器	合勤(ZyXEL)、桓基(hgiga)、俠諾(QNO)、星通資訊、居易、友訊(D-Link)、友旺(AboCom)、o2security、盛達電業(Billion)

資料來源：本計畫自行整理

上述4項產品已於評選會議時經委員同意，並於7月2日第一次專家學者座談會，經專家學者與各業者認同。

二、本年度安全檢測技術規範

本年度新增訂之安全檢設測技術規範將參考過往以驗證可行之規範架構執行，同時參考美國國家標準與技術研究院(National Institute of Standards and Technology，NIST)、共同準則承認協定之國際組織(Common Criteria Recognition Arrangement，CCRA)、測試資安產品功能實驗室(ICSA及NSS)、測試網通產品實驗室(UNH-IOL)、制定IEEE 802.11規格之無線網通產品之國際組織(WiFi Alliance) 相關文獻等資料，並依據過去檢測技術規範將檢測項目分為書面審查及實機檢測兩部分，並納入基礎型與進階型之檢測分類，詳細檢測技術規範請參閱附件一、三、五、七。

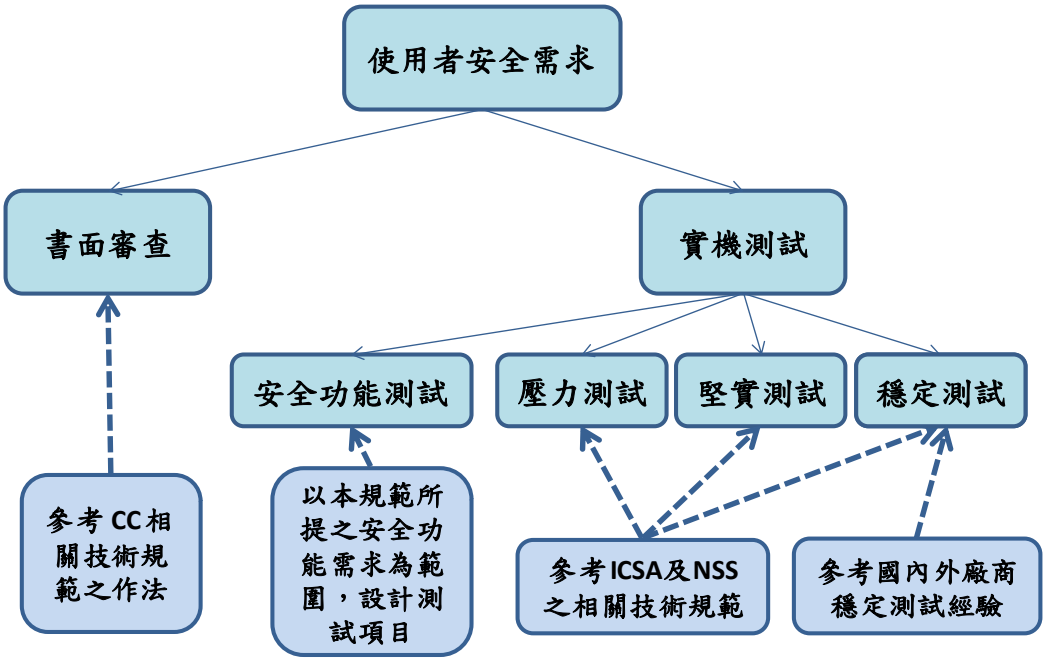


圖7　檢測技術規範架構

資料來源：本專案自行整理

(一)書面審查

書面審查包含安全標的、安全功能設計等，其中安全功能設計包含安全功能規格、設計安全性、安全架構、安全指引、安全功能測試等。基礎型於設計安全性可免進行書審，進階型則需全部進行審查。

表5　書面審查類別(以進階持續性威脅防禦設備為例)

類別	項目	基礎型	進階型
安全標的	設備規格	✓	✓
	安全功能需求	✓	✓
安全功能設計	安全功能規格	✓	✓
	設計安全性		✓
	安全架構	✓	✓
	安全指引	✓	✓

表6　安全功能需求(書審附表 1-2)對照表

△: 基礎&進階適用 ✓: 僅進階適用

類別/項目	子項目	資料庫安全稽核設備	進階持續威脅防禦設備	行動無線寬頻分享器	虛擬私人網路閘道器
安全標的/安全功能需求	稽核資料產生	△			
	使用者身分關聯	△			
	稽核審查	△			
	受限制之稽核	△			
	受保護之稽核存底儲存	△			
	稽核資料可能遺失時之作為	△			
	密碼金鑰產生	△			
	密碼金鑰分配	△			
	密碼金鑰銷毀	△			
	密碼操作	△			
	使用者屬性定義	△	△		
	鑑別時序	△	△		
	識別時序	△			
	安全功能行為之管理	△	△	△	△
	安全功能資料管理	△	△		
	安全功能資料輸出之可用性		△		

類別/項目	子項目	資料庫安全稽核設備	進階持續威脅防禦設備	行動無線寬頻分享器	虛擬私人網路閘道器
	安全功能資料輸出之機密性		△		
	安全功能資料輸出之完整性		△		
	管理功能之標準	△			
	管理功能規格			△	△
	安全角色	△	△	△	△
	安全功能資料傳輸保護	△			
	鑑別失敗處理	✓	△	△	△
	可選擇之稽核審查	✓			
	資源利用	✓			
	可信賴之時戳		△	△	△
	可信賴更新			△	△
	稽核紀錄		△	△	△
	稽核紀錄之查詢		△		
	稽核紀錄可用性之保證		△		
	外部稽核紀錄存取				△
	系統資料蒐集		△		
	系統資料分析功能		△		

類別/項目	子項目	資料庫安全稽核設備	進階持續威脅防禦設備	行動無線寬頻分享器	虛擬私人網路閘道器
	系統資料回應功能		△		
	受限制的系統資料審查		△		
	系統資料可用性之保證		△		
	系統資料漏失之預防		△		
	密碼操作		✓		
	管理功能之標準		✓		
	可信賴路徑		✓	✓	△
	可信賴通道			✓	△
	密碼金鑰管理			△	△
	密碼操作			△	△
	殘餘資訊保護			△	△
	亂數產生器			✓	
	通行碼管理			△	
	鑑別機制			△	△
	失效保全			△	✓
	重送攻擊偵測			△	
	管理者通行碼保護			△	△
	安全功能自我測試			△	✓
	最大資源配置			△	

類別/項目	子項目	資料庫安全稽核設備	進階持續威脅防禦設備	行動無線寬頻分享器	虛擬私人網路閘道器
	登入連線之鎖定			△	△
	登入連線之終止			△	△
	待測物存取預設標語			△	△
	待測物交談建立				△
	資料流控制			✓	△
	安全屬性初始值			✓	

(二)實機測試

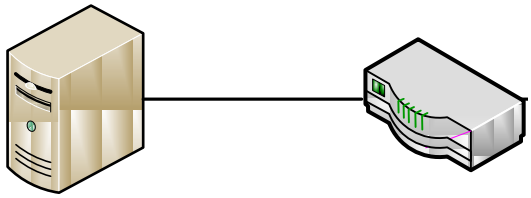
實機測試包括功能面、效能面、堅實面以及穩定面四大層面的測試項目，內容規劃如下。

1.安全功能測試(Security Functionality Test)

檢視待測物之安全功能需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

(1)先進惡意程式與零時漏洞攻擊偵測率(漏擋與誤擋)

(2)測試環境



測試平台　　待測物

資料來源：本計畫自行整理

圖8　安全功能測試(基本功能驗證)：封包過濾測試接續示意圖

A.測試平台：可產生網路封包之測試儀器或程式。

B.網路連接線：乙太網路線或光纖纜線。

C.連接測試平台、待測物如圖 8。

D.開啟待測物之先進惡意程式與零時漏洞攻擊偵測功能。

(3)偵測測試樣本

常用之樣本依型態可分為檔案及 URL 兩大類，檔案至少須包含可執行檔、壓縮檔等格式；URL 至少須包含已知的惡意網頁。基礎型待測物必須支援至少 300 種樣本用於偵測；進階型待測物必須支援至少 1000 種樣本用於偵測。

(4)測試方法及標準

A.以偵測測試樣本數量之 10% 對待測物進行測試 (基礎型測試樣本抽測數量至多 30 項，進階型測試樣本抽測數量至多 100 項)，待測物必須分析並阻擋認為是先進惡意程式或零時偵測攻擊的樣本。

B.將其所測之樣本拿至 VirusTotal 進行分析並參考其結果，若 VirusTotal 中有些產品會阻擋，但待測物並沒有阻擋，則稱為漏擋，若 VirusTotal 中沒有產品會阻擋，但待測物阻擋此樣本，則稱為誤擋。

2.壓力測試(Stress Test)

(1)吞吐量測試

A.測試環境

a.測試平台：可產生測試樣本之測試儀器或程式。

b.網路連接線：乙太網路線或光纖纜線。

c.連接測試平台及待測物如圖 8。

d.開啟待測物之安全功能。

e.測試平台產生各種樣本並不斷使待測物端之設備下載樣本或打開 URL，時間至少 60 秒。

B.測試方法及標準

測試平台傳送不同種的樣本供待測物偵測。當待測物所負荷的吞吐量達到其規格說明之最大值時，待測物安全功能應正常運作。

(2)偵測延遲與儲存容量擴充性

A.測試環境

同上方安全功能測試

B.測試方法及標準

測試平台產生一定量的樣本讓待測物進行偵測，並記錄其總偵測時間，以此來得到平均偵測延遲時間。

3.堅實測試(Robustness Test)

- 阻斷式攻擊

A.測試環境

a.測試平台：可產生大量網路流量之測試儀器或程式。

b.網路連接線：乙太網路線或光纖纜線。

c.連接測試平台及待測物如圖 8。

d.開啟待測物之安全功能。

e.測試平台針對待測物的服務連接埠，發動阻斷式攻擊。

B.測試方法及標準

測試平台送出大量的網路流量，持續 600 秒攻擊待測物開啟的連接埠，並阻斷其服務。當攻擊流量低於或等於待測物規格說明之吞吐量最大值時，安全功能應正常運作。

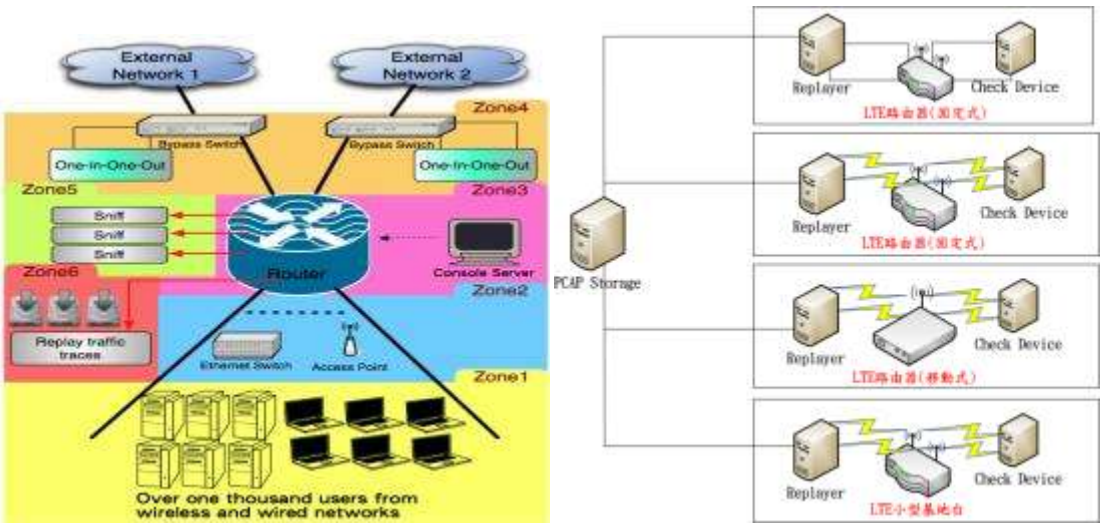
4.穩定測試(Stability Test)

(1)測試環境：建立真實流量重播測試環境。

(2)測試樣本必須滿足以下要求：應從真實網路環境錄製。具備至少 100 位使用者所下載的檔案及 URL，應為該待測物送測前 2 周內所蒐集之樣本。

(3)測試方式：以重播工具將流量重播至待測物，持續進行一定週期的穩定測試。

(4)測試結果：檢查待測物在長時間且大量真實流量的環境中，是否發生當機、重開機、斷線或處理速度變慢等情況。



資料來源：本計畫自行整理

圖9　穩定測試：行動無線寬頻分享器測試示意圖

茲將各資通設備之實機檢測內容彙整如下表 7：

表7　實機測試對照表

△: 基礎&進階適用 ✓: 僅進階適用

類別	項目	資料庫安全稽核設備	進階持續威脅防禦設備	行動無線寬頻分享器	虛擬私人網路閘道器
安全功能測試	安全管理	△			△
	安全稽核功能	△			
	資料庫型態偵測	△			
	線上更新	△			
	先進惡意程式與零時漏洞攻擊偵測率(漏擋與誤擋)		△		
	安全事件記錄		△		△
	反應機制(通知、隔離、斷線、診斷)		△		

類別	項目	資料庫安全稽核設備	進階持續威脅防禦設備	行動無線寬頻分享器	虛擬私人網路閘道器
	稽核資料產出			△	
	鑑別功能			△	
	使用者識別及授權功能			△	
	使用者身分保密性			△	
	通道流量統計				△
	通道控制				△
	流量控管功能				✓
壓力測試	最大同時連線數	✓			
	最大連線建立速率	✓			
	吞吐量		△	✓	
	站對站(Site-to-Site)吞吐量測試				△
	站對站(Site-to-Site)通道數量測試				✓
	遠端訪問(Remote Access)吞吐量測試				△
	遠端訪問(Remote Access)通道數量測試				✓
堅實測試	阻斷式攻擊	△	△		△
	遠端管理異常流量	✓	✓		✓
	非正常關機復原	△	△	△	△
	異常流量測試			✓	
穩定測試	真實流量測試	△	△	--	△

資料來源：本計畫自行整理

表8　實機測試項目(以進階持續性威脅防禦設備為例)

類別	項目	判定標準	基礎	進階
安全功能測試	先進惡意程式與零時漏洞攻擊偵測率(漏擋與誤擋)	1. 依 6.4.1.1.3.(1) 進行測試，得到待測物對該群樣本的偵測結果。 2. 依 6.4.1.1.3.(2) 進行測試其所測之樣本拿至 VirusTotal 進行分析並參考其結果，並依其結果算出其待測物的漏擋跟誤擋率。	✓	✓
	安全事件記錄	依 6.4.1.3.3. 進行測試，待測物的偵測分析報告應正確記錄樣本類型名稱、危害程度及內容。	✓	✓
	反應機制(通知、隔離、斷線、診斷)	依 6.4.1.4.2. 進行測試，在偵測到後應具備相關的反應機制(通知、隔離、斷線、診斷)	✓	✓
	備援管理	依 6.4.1.5.2. 進行測試，備援待測物應於規定時間內接替失效之待測物。		✓
壓力測試	吞吐量	依 6.4.2.1.2. 進行測試，當待測物所負荷的吞吐量達到其規格說明之最大值時，待測物安全功能應正常運作。	✓	✓
堅實測試	阻斷式攻擊	依 6.4.3.1.2. 進行測試，當攻擊流量低於或等於待測物規格說明之吞吐量最大值時，安全功能應正常運作。	✓	✓
	遠端管理異常流量	依 6.4.3.2.3. 進行測試，待測物遠端管理介面對服務/協定異常流量應保持正常運作。		✓
	非正常關	依 6.4.3.3.1. 進行測試，待測物應可復原	✓	✓

類別	項目	判定標準	基礎	進階
	機復原	到非正常關閉電源前的最後狀態。		
穩定測試	真實流量	依 6.4.4.1.3. 進行測試，待測物應可持續 168 小時穩定運作。	✓	
		依 6.4.4.1.3. 進行測試，應可持續 336 小時穩定運作。		✓

檢測技術規範之詳細內容請參考附件一、三、五、七。

三、本年度政府機關(構)資通設備採購參考指引草案

為協助政府機關熟悉資通設備產品，以及其佈署之規劃、設定、檢查與更新資訊，將撰擬資通設備採購參考指引，提供檢測項目功能之說明，使機關了解檢測分級保障範圍及效益，以利機關將來選擇採購產品時之參考。

本年度將參考去年計畫所撰擬之綱要，包含下列項目：

表9　資通設備採購參考指引綱要(以進階持續性威脅防禦設備為例)

章節	標題	內容大綱
前言	目的	旨在說明採購進階持續性威脅防禦設備須注意之功能面及效能面考量。政府機關 (構) 得參考本指引進行採購，以強化網路之安全管理。本指引係屬建議性質，單位進行設備採購時仍需符合單位資安管理規範之要求。資料庫安全稽核設備之目的在於提供政府機關 (構) 人員資料安全管理之能力，建構安全之網路管理及異常通報機制，強化機敏資料保護。
	適用對象	本文件適用於政府機關 (構) 運用資訊科技從事「業務維運」之所有人員。為便於閱讀與使用，

章節	標題	內容大綱
		特將適用對象區分為「一般主管」、「資訊人員」及「一般使用者」。一般主管及資訊人員可考慮閱讀整份文件，一般使用者則可略過第二章的部份。
設備介紹	進階持續性威脅防禦設備簡介	進階持續性威脅防禦設備是指具備在線或離線的方式監控進階持續性威脅攻擊內容的設備，雖然進階持續性威脅並不是一個特性的攻擊方法或模式，而且其軌跡多屬隱性的方式在進行相關的工作，不過無論攻擊者手法如何縝密仍然會在各式網路行為中留下蛛絲馬跡，而進階持續性威脅防禦設備的功能就在於記錄這些「證據」(evidence)，攻擊者為了發動攻擊，會利用各式手法將惡意程式植入到電腦之中，並進行複製資料與傳送至外部的行為，系統內部或網路流量一定會記錄下相關的活動內容，進階持續性威脅防禦設備必須在此活動內容中找到異常的行為及流量內容，確保對軟體內容標記符合內部的使用政策，自動化的檢查機制與程式內容比對將有利於查找相對應的攻擊內容。
	系統架構	進階持續性威脅防禦設備屬高階且重要具機敏資料之產品，一般此種設備至少具備數個乙太網路介面，當在線模式啟動時，產品可以利用透通(transparent)的方式讓所有的網路流量經過此設備進行過濾，因此佈署於此區域內的流量將完全受到進階持續性威脅防禦設備的管制，可以達到最多的限制及管制；如果使用離線模式，則產品將透過交換器等設備利用鏡像的方式將流量導

章節	標題	內容大綱
		入到進階持續性威脅防禦設備中，但是此時只可做為分析及告警之用。
	運作原理	進階持續性威脅防禦設備透過各技術判讀不同的惡意程式內容，常用的技術包含殭屍網路、沙盒、社交工程等面向。(詳細內容請參考附件四)
資安需求	如何評估	在採購進階持續性威脅防禦設備時，必須考量效能、安全功能、穩定性等
	防護措施	有鑑於進階持續性威脅防禦設備可能帶來的資安風險，採購單位在選購相關產品時，應注意：安全功能、效能、穩定性。 此外，採購單位應優先採購經過檢測技術規範認證的產品，可有效避免產品潛在瑕疵所帶來的不便和危害。
採購認證設備	降低資安風險	根據「資通設備安全檢測技術規範」針對「進階持續性威脅防禦設備」所規範的檢測方式，就資料庫安全稽核設備在使用上的主要風險，可透過安全功能測試、堅實測試、壓力測試及穩定測試進行檢測。檢測技術規範裡定義「基礎等級」以及「進階等級」二種不同程度的標準，所要求符合的測試項目也有所差異，以進階等級的要求的通過標準較為嚴格。
	有效資安健檢	「資通設備安全檢測技術規範」針對設備基本存取和使用安全做完整的功能測試。包括：稽核資料產出、安全管理功能。 唯有嚴格且縝密的測試，方能確保產品於使用過程中，符合各使用單位之安全及效能需求。

檢測技術規範之詳細內容請參考附件二、四、六、八。

四、新增加資通設備試測作業

本計畫於 11 月上旬逐步進行 4 項新增產品之試測，試測作業將由合格之檢測試驗室進行，藉以了解新增之檢測技術規範之可行性，藉以做為規範檢討參考依據。檢測單位於試測作業中亦將協助廠商瞭解檢測技術規範與檢測流程，待整體試測完成後即可針對試測結果進一步調整規範內容，詳細規劃報告請參考附件九。

表10 4 項資通產品與其對應試測廠商

設備	試測業者
資料庫安全稽核設備	庫柏資訊
進階持續性威脅防禦設備	艾斯酷博(台灣威瑞特)
行動無線寬頻分享器	盟創科技
虛擬私人網路閘道器	居易科技

資料來源：本計畫自行整理

(一)試測受理期間

自 103 年 10 月 20 日至 103 年 10 月 31 日止。

(二)試測期間

自 103 年 10 月 20 日至 103 年 12 月 30 日止。

(三)申請時應繳交項目

1.申請書。

2.設備樣品。

3.中文或英文之使用手冊或說明書。

4.中文或英文之規格資料。

5.安全檢測技術規範要求之相關資料。

6.光碟片一份，含 1~5 資料。

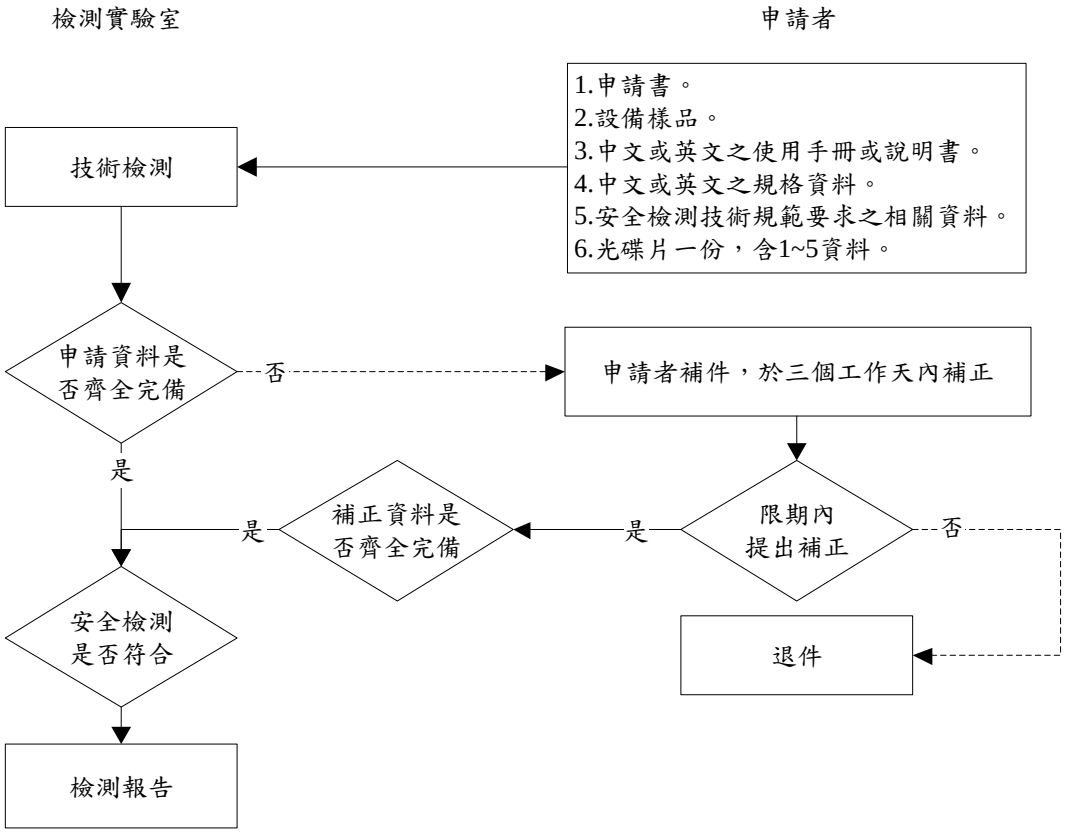


圖10 試測流程圖

資料來源：本計畫自行整理

(四)測試項目

表11 試測項目彙整表

項目	資料庫安全稽核設備	進階持續性威脅防禦設備	行動無線寬頻分享器	虛擬私人網路閘道器
書面審查	1. 設備規格 2. 安全功能規格			

項目	資料庫安全稽核設備	進階持續性威脅防禦設備	行動無線寬頻分享器	虛擬私人網路閘道器
	3. 安全架構 4. 安全功能需求 5. 設計安全性 6. 安全指引			
實機測試	1. 封包過濾 2. 安全事件紀錄 3. 備援管理 4. 吞吐量 5. 最大建立連線速率 6. 異常流量 7. 真實流量測試 8. 流量內容統計 9. 安全管理 10. 規則控管 11. 最大同時連線數 12. 阻斷式攻擊 13. 非正常關機復原	1. 漏判/誤判測試 2. 安全管理 3. 線上更新 4. 具備 IPv6 封包檢測 5. 最大同時連線數 6. 阻斷式攻擊 7. 非正常關機復原 8. 躲避攻擊 9. 異常/攻擊事件紀錄 10. 使用者自訂安全規則 11. 吞吐量 12. 最大建立連線速率 13. 異常流量 14. 真實流量測試	1. 安全事件紀錄 2. 吞吐量 3. 最大建立連線速率 4. 異常流量 5. 真實流量測試 6. 線上更新 7. 流量內容統計 8. 安全管理 9. 規則控管 10. 最大同時連線數 11. 非正常關機復原	1. 安全管理 2. 線上更新 3. 最大同時連線數 4. 阻斷式攻擊 5. 非正常關機復原 6. 異常/攻擊事件紀錄 7. 使用者自訂安全規則 8. 吞吐量 9. 最大建立連線速率 10. 異常流量 11. 真實流量測試

(五)測試報告

目前資料庫安全稽核設備、進階持續性威脅防禦設備、行動無線寬頻分享器設備、虛擬私人網路閘道器設備之試測已陸續完成，透過試測作業將可進一步比對目前研擬之檢測規範草案內容是否有需要調整之處，以下為各品項之測試報告概要：

表12 資料庫安全稽核設備試測結果概要

類別	項目	測試結果	規範可行性	測試結果分析/規範調整建議
安全功能測試	安全管理	Fail	Yes	不支援嘗試輸入錯誤通行碼的偵測及提供鎖定的機制。驗證方式，連續輸入超過三次失敗的登入嘗試後接著輸入正確的帳密，成功登入，故判斷不合格。
	異常/攻擊事件紀錄	Fail	Partial	待測物並無主動提供或是預設有提供 SQLInjection 的特徵碼/防護，故判定不合格。
堅實測試	阻斷式攻擊	Pass	Yes	在測試設備產生最大速率之阻式斷流量送往待測物提供的各類通訊協定時，其管理界面基本功能仍正常運作，且待測物的可用性仍高於 80%，故判定合格。
	遠端管理 異常流量	Pass	Yes	針對測試設備送出的各類協定變型流量，都無法導致待測物提供的通訊協定異常或是找到存在的漏洞，故判定合格
	非正常關機恢復	Pass	Yes	經比對待測物在非正常關機的前後設定檔、log、report 的設定內容一致，待測物可保留非正常關機前的最後狀態，故判定合格。
壓力	最大同時連線數	N/T	Partial	該測項不適用於此類型 offline 設備，故不測試。

類別	項目	測試結果	規範可行性	測試結果分析/規範調整建議
測試	最大連線建立速率	N/A	Partial	由於送測廠商所提供的規格書裡，並不提供最大連線速率的數據，因此該測項僅以得出一個數據供參考，如果雙方對該數據無疑慮的話，該結果即為合格。測試結果為 SQLTransactionrate：30000/sec
穩定測試	真實流量	Fail	Yes	僅能 a 偵測 postgresql、mysql 及 mssql 的流量。db2 與 oracle 的 db 流量都無法正確辨識，故判定不合格。

表13 進階持續性威脅防禦設備試測結果概要

類別	項目	測試結果	規範可行性	測試結果分析/規範調整建議
安全功能測試	先進惡意程式與零時漏洞攻擊偵測率	Pass	Yes	漏擋率(42%)低於標準(50%)且誤擋率(0%)低於標準(30%)，所以判定為合格。
	安全事件記錄	Pass	Yes	當違反安全事件被觸發，待測物將違反事件的相關資訊紀錄下來，且事件記錄提供的資訊格式符合規範要求的欄位記錄故判定合格。
	反應機制(通知、隔離、斷線、診斷)	Pass	Yes	當待測物在偵測到後應具備相關的反應機制，也就是隔離，故判定合格。
	備援管理	Fail	Yes	待測物本身並不支援該功能，故判定為不合格。
堅實測試	阻斷式攻擊	Fail	Yes	在測試設備產生最大速率之阻斷流量送往待測物提供的各類通訊協定時，可用性不及 30%，故判定不合格。

類別	項目	測試結果	規範可行性	測試結果分析/規範調整建議
	遠端管理異常流量	Fail	Yes	針對測試設備送出的各類協定變型流量，針對 smtp 存在數個潛在的風險，故判定不合格。
	非正常關機復原	Pass	Yes	經比對待測物在非正常關機的前後設定檔、log、report 的設定內容一致，待測物可保留非正常關機前的最後狀態，故判定合格。
壓力測試	吞吐量測試	N/A	Yes	當待測物在有背景流量的情況下，待測物仍可正常運作。
穩定測試	真實流量	N/T	Yes	不適用

表14 行動無線寬頻分享器設備試測結果概要

類別	項目	測試結果	規範可行性	測試結果分析/規範調整建議
安全功能測試	稽核資料產出	Pass	Yes	產出之稽核資訊符合相關規定，故判定合格。
	鑑別功能	Pass	Yes	LTE 端鑑別(EPS-AKA 鑑別及 NAS 鑑別)符合相關規定，故判定合格。
	使用者識別及授權功能	Pass	Yes	輸入正確 PIN 碼才能登入待測物並取得 IMSI 資訊及使用權。開啟待測物於輸入正確 PIN 碼後方能存取服務並進行後續操作。符合相關規定，故判定合格。
	使用者身分保密性	Pass	Yes	接入網路過程使用暫時身分識別碼或是加密過之永久身分識別碼。符合相關規定，故判定合格。
堅實	阻斷式攻擊	Pass	Yes	對於遠端管理介面產生服務/協定異或攻

類別	項目	測試結果	規範可行性	測試結果分析/規範調整建議
測試				擊流量可保持正常運作，故判定合格。
	非正常關機復原	Pass	Yes	經比對待測物在非正常關機的前後設定檔的設定內容一致，待測物可保留非正常關機前的最後狀態，故判定合格。
壓力測試	吞吐量	N/A	Partial	需評估測試工具(需支援無線介面之流量產生器)，若無適合測試工具建議範移除此測項目。
穩定測試	真實流量	N/A	Partial	行動裝置使用模式並非長時間啟用並且受制於電源待機時間，另一方面考量測試儀器支援程度(需支援無線介面之流量重播技術)，故建議規範移除此測項目。

表15 虛擬私人網路閘道器設備試測結果概要

類別	項目	測試結果	規範可行性	測試結果分析/規範調整建議
安全功能測試	通道流量統計	Fail	Yes	待測物的流量統計資訊，不包含通道的傳輸量資訊，故判定不合格。
	通道控制	Pass	Yes	針對欲進行阻擋過濾/放行之流量與測試樣本，均能有效可控地處理與反應，故判定合格。
	安全事件紀錄	Pass	Yes	當違反安全事件被觸發，待測物將違反事件的相關資訊紀錄下來，且事件記錄提供的資訊格式符合規範要求的欄位記錄故判定合格。
	安全管理	Fail	Yes	登入待測物需輸入使用者密碼。 待測物有支援最大錯誤次數設定及指定封鎖時間，在啟動該功能後，登入錯誤達指

類別	項目	測試結果	規範可行性	測試結果分析/規範調整建議
				定次數後會封鎖管理界面至指定的秒數。支援管理者與非管理者角色定義與權限控管，故判定不合格。
	流量控管	Fail	Yes	待測物不具備規則描述以外區域的存取控制能力，故判定為不合格。
堅實測試	阻斷式攻擊	Pass	Yes	待測物於測試期間未發生當機、重開或通道中斷之情況。當攻擊結束後，安全功能正常運作，故判定合格。
	遠端管理異常流量	Pass	Yes	當遠端管理異常流量經過待測物時流量內容可被正常處理。
	非正常關機恢復	Fail	Yes	重開機後的系統日誌，系統時間被重設，而且沒有保留舊日誌，故判定不合格。
壓力測試	站對站(Site-to-Site)吞吐量測試	Fail	Yes	實測結果與廠商提供的規格資訊有落差，故判定不合格。
	站對站(Site-to-Site)通道數量測試	Fail	Yes	無法全數建立站對站通道。
	遠端訪問(RemoteAccess)吞吐量測試	N/T	Partial	因目前檢測工具不支援特定 frame size 故不適用，已調整檢測項目指定為最大 frame size。
	遠端訪問(RemoteAccess)通道數量測試	N/T	Partial	不適用，已取消該檢測項目。
穩定測試	站對站吞吐量測試	Pass	Partial	待測物測試結果為通過，唯測試過程中需確認真實流量有在兩台待測務所建立通道上執行。

整體而言規範內容僅有少數測項需進行調整，調整因素例如調整文字敘述讓讀者更容易理解、調整參數設定以符合現有檢測工具等，至於對通過標準之要求則無調整，對於原先所參考之國際標準之要求保持一致。相關內容彙整如下：

表16 檢測技術規範建議調整彙整.

類別	產品	項目	原因	對應規範章節
建議調整	資料庫安全稽核設備	阻斷式攻擊	建議規範註明此測項對於 offlinemode 產品的作法。	附件一-20
		遠端管理異常流量	建議規範可調整成最多取幾項，最少則以待測物所支援的上限。	附件一-21
		最大同時連線數	建議規範還需評估測試工具。	此項目不適合此產品故取消此測項
		最大連線建立速率	建議規範還需評估測試工具。	附件一-20
	虛擬私人網路閘道器	非正常關機復原	建議規範項目 2 日誌保留部份的要求也納入 syslog。 建議規範項目 3 的要求建議可以調整成與項目 1 合併。	附件七-27
		站對站吞吐量測試	建議規範指定 tunnel 是採用何種加密演算法、hashfunction 的參數。	附件七-23 不進行調整，因為規範內容為通用不針對特定的功能進行描述

類別	產品	項目	原因	對應規範章節
	行動無線寬頻分享器	吞吐量	建議規範還需評估測試工具。	附件五-33
建議移除	行動無線寬頻分享器	真實流量	行動裝置使用模式並非長時間啟用並且受制於電源待機時間，另一方面考量測試儀器支援程度，建議規範移除此測項目。	已移除
	虛擬私人網路閘道器	遠端訪問(RemoteAccess)吞吐量測試	不適用，不列為檢測項目	已移除
		遠端訪問(RemoteAccess)通道數量測試	不適用，不列為檢測項目	已移除

整體而言，一方面對於試測結果中 Fail 項目進行分析，分析該項目 Fail 是否因規範可用性所造成或是產品設計實作上尚未加以考量，另一方面依據實際狀況調整規範提高可用性，例如調整文字敘述讓讀者更容易理解、調整參數設定以符合現有檢測工具等，至於對通過標準之要求則無調整，對於原先所參考之國際標準之要求保持一致，以確保規範品質。

在資料庫安全稽核設備試測方面，分析 Fail 項目包括安全管理、異常/攻擊事件紀錄與真實流量，以安全管理為例產品不支援嘗試輸入錯誤通行碼的偵測及提供鎖定的機制。驗證方式，連續輸入超過三次失敗的登入嘗試後接著輸入正確的帳密，成功登入，故判斷不合格。整體而言 Fail 原因在於產品設計實作上尚未加以考量，規範可用性無虞。

在進階持續性威脅防禦設備試測方面，分析 Fail 項目包括備援管理、阻斷式攻擊以及遠端管理異常流量，以遠端管理異常流量為例產品針對測試設備送出的各類協定變型流量，針對 smtp 存在數個潛在的風險，故判定不合格。整體而言 Fail 原因在於產品設計實作上尚未加以考量，規範可用性無虞。

在行動無線寬頻分享器設備試測方面，產品並無 Fail 項目。此外由於行動裝置使用模式並非長時間啟用並且受制於電源待機時間，另一方面考量測試儀器支援程度(需支援無線介面之流量重播技術)，故移除此測項目。整體而言規範可用性無虞。

在虛擬私人網路閘道器設備試測方面，分析 Fail 項目包括通道流量統計、安全管理、流量控管、非正常關機恢復、站對站(Site-to-Site)吞吐量測試以及站對站(Site-to-Site)通道數量測試、，以通道流量統計為例產品的流量統計資訊，不包含通道的傳輸量資訊，故判定不合格。整體而言 Fail 原因在於產品設計實作上尚未加以考量，規範可用性無虞。

書面審查所需時程與費用如表 17，實機測試所需時程與費用如表 18，各產品所需經費如表 19。

表17 檢測技術規範-書面審查建議時程及費用

時程/成本 產品	基礎型		進階型	
	時程(天)	成本(NTD)	時程(天)	成本(NTD)
資料庫安全稽核設備	31	$122,468	34	$135,212
進階持續性威脅防禦設備	34	$134,876	38	$151,756
行動無線寬頻分享器	35	$138,676	43	$170,756

時程/成本 產品	基礎型		進階型	
	時程(天)	成本(NTD)	時程(天)	成本(NTD)
虛擬私人網路閘道器	35	$138,676	40	$159,356

資料來源：通傳會審驗核可實驗室

表18 檢測技術規範-實機檢測建議時程及費用

時程/成本 產品	基礎型		進階型	
	時程(天)	成本(NTD)	時程(天)	成本(NTD)
資料庫安全稽核設備	13.5	$143,820	24.5	$207,420
進階持續性威脅防禦設備	14.5	$145,320	25.5	$219,320
行動無線寬頻分享器	14.5	$144,570	23.5	$194,570
虛擬私人網路閘道器	7.5	$86,960	10.5	$135,210

資料來源：通傳會審驗核可實驗室

表19 檢測技術規範-建議時程及費用

時程/成本 產品	基礎型		進階型	
	時程(天)	成本(NTD)	時程(天)	成本(NTD)
資料庫安全稽核設備	44.5	$266,288	58.5	$342,632
進階持續性威脅防禦設備	48.5	$280,196	63.5	$371,076

時程/成本 產品	基礎型		進階型	
	時程(天)	成本(NTD)	時程(天)	成本(NTD)
行動無線寬頻分享器	49.5	$283,246	66.5	$365,326
虛擬私人網路閘道器	42.5	$225,636	50.5	$294,566

資料來源：本計畫自行整理

五、10 項現行資通設備安全檢測規範修正意見

國家通訊傳播委員會分別於 100、101 年完成網路型防火牆(Firewall)、入侵偵測防禦系統(IDP)、防毒閘道設備(Anti-Virus)、網路型垃圾郵件過濾設備(Anti-Spam)、網頁應用防火牆(WAF)、應用軟體控管系統(AC)、乙太網路交換器(L2 Switch)、路由交換器(L3 Switch)、無線接取設備(Thin AP+控制器或 Fat AP)、無線區域網路路由器(Wireless Router)等 10 項資通設備安全檢測技術規範。時至今日已逾 3 年，相關產品之製造技術與功能皆現行需求改變有所調整，考量實際檢測過程中反映與回饋建議，希望藉由現行檢測規範的修訂，完善整體檢測規範。

茲將過去 10 項檢測技術規範之檢測內容統整如下表，提供參考：

表20 10 項檢測技術規範之檢測內容統整

△表示基礎/進階適用、✓表示僅進階適用

類別	項目	網路型防火牆(Firewall)	入侵偵測防禦系統(IDP)	防毒閘道設備(Anti-Virus)	網路型垃圾郵件過濾設備	網頁應用防火牆(WAF)	應用軟體控管系統(AC)	乙太網路交換器(L2 Switch)	路由交換器(L3 Switch)	無線接取設備(Thin AP+控制器或Fat AP)	無線區域網路路由器(Wireless Router)
安全功能測試	封包過濾	△							△		
	逃脫技巧偵測					△					
	異常/攻擊偵測		△			△					
	異常/攻擊事件紀錄		△								
	躲避攻擊		△								
	病毒偵測			△							
	流量內容統計	△					△				
	流量控管規則	✓									
	安全事件紀錄	△		△	△	△	△				

類別	項目	網路型防火牆(Firewall)	入侵偵測防禦系統(IDP)	防毒閘道設備(Anti-Virus)	網路型垃圾郵件過濾設備	網頁應用防火牆(WAF)	應用軟體控管系統(AC)	乙太網路交換器(L2 Switch)	路由交換器(L3 Switch)	無線接取設備(Thin AP+控制器或Fat AP)	無線區域網路路由器(Wireless Router)
	安全管理	△	△	△	△	△	△	△	△	△	△
	線上更新		△	△							
	備援管理	✓				△	△		✓		
	組態備援管理							✓	✓		
	具備 IPv6 封包檢測		✓								
	運作模式切換			✓							
	惡意網址過濾			✓							
	郵件內容反釣魚網址過濾				✓						
	網路偵測與預防機制								✓		
	網路用戶認證機制								✓		
	即時流量內容監控						△				

類別	項目	網路型防火牆(Firewall)	入侵偵測防禦系統(IDP)	防毒閘道設備(Anti-Virus)	網路型垃圾郵件過濾設備	網頁應用防火牆(WAF)	應用軟體控管系統(AC)	乙太網路交換器(L2 Switch)	路由交換器(L3 Switch)	無線接取設備(Thin AP+控制器或Fat AP)	無線區域網路路由器(Wireless Router)
	安全稽核功能							△			
	資料流控制							△			
	可靠時戳							△			
	密碼支援功能										
	使用者識別與鑑別功能							△			
	虛擬區網(VLAN)保護功能							✓			
	自動登出功能								△		
	路由認證保護								△		
	路由被動介面								△		
	稽核資料產出									△	△
	與稽核伺服器失去連線後的									△	△

類別	項目	網路型防火牆(Firewall)	入侵偵測防禦系統(IDP)	防毒閘道設備(Anti-Virus)	網路型垃圾郵件過濾設備	網頁應用防火牆(WAF)	應用軟體控管系統(AC)	乙太網路交換器(L2 Switch)	路由交換器(L3 Switch)	無線接取設備(Thin AP+控制器或Fat AP)	無線區域網路路由器(Wireless Router)
	應變措施										
	重播偵測										△
	重送攻擊偵測									△	
	待測物的安全功能自測									△	
	認證失敗控制功能									△	
	使用者識別及授權功能									△	△
	通行碼逾期功能									△	△
	更新通行碼重新認證功能									△	△
	登入畫面保密功能									△	
	802.1X 使用者識別及認證功能									△	△

類別	項目	網路型防火牆(Firewall)	入侵偵測防禦系統(IDP)	防毒閘道設備(Anti-Virus)	網路型垃圾郵件過濾設備	網頁應用防火牆(WAF)	應用軟體控管系統(AC)	乙太網路交換器(L2 Switch)	路由交換器(L3 Switch)	無線接取設備(Thin AP+控制器或Fat AP)	無線區域網路路由器(Wireless Router)
	資源最大配額									△	△
	安全功能初始會談鎖定									△	△
	使用者初始階段中斷									△	△
	鑑別失敗控制功能										△
	安全功能自測										△
	安全角色										△
	金鑰保護										✓
	資料流控制										✓
	安全屬性初始值										✓
壓力測試	吞吐量	△	△	△	△	△	△	△	✓	✓	✓
	最大同時連線數	✓	✓	✓	✓	✓	✓				

類別	項目	網路型防火牆(Firewall)	入侵偵測防禦系統(IDP)	防毒閘道設備(Anti-Virus)	網路型垃圾郵件過濾設備	網頁應用防火牆(WAF)	應用軟體控管系統(AC)	乙太網路交換器(L2 Switch)	路由交換器(L3 Switch)	無線接取設備(Thin AP+控制器或Fat AP)	無線區域網路路由器(Wireless Router)
	最大建立連線速率	✓	✓	✓	✓	✓	✓				
	最大虛擬(VLAN)容量							✓			
	最大 MAC 容量							✓			
堅實測試	阻斷式攻擊	△	△	△	△	△	△	△	△		
	遠端管理異常流量	✓	✓	✓	✓		✓	✓	✓		
	異常流量測試									△	△
	惡意流量					✓					
	非正常關機復原	△	△	△	△	△	△	△	△	✓	✓
穩定測試	真實流量測試	△	△	△	△	△	△	△	△	△	△

有關現行資通設備安全檢測規範修正內容，可區分為以下方面：

1.依據資通設備現行新增功能，調整規範要求：

據現行資通安全需求調整調整檢測規格，如：通行碼長度最少支援 8 位以上字元(後因應期中審查委員意見改為 13 位字元)、攻擊方式。

2.根據過往執行情況，調整規範要求避免誤解：

依照過往測試經驗，將文字說明明確定義，如：送出大量的網路流量最大吞吐量 300%的 HTTP 封包，避免送驗廠商誤解延遲正式驗測時間。

3.依據實際測試之有效性，調整規範內容。

依照過往測試經驗，強化測試結果之有效性，如：測試平台針對待測物提供之每項服務皆產生 10 種異常流量作為測試樣本。

10 項規範修正方向如下：

表21 現行安全檢測規範預定修改內容

項目	章節	建議修改內容
網頁應用防火牆(WAF)	6.4.2.1.1	(9)測試平台產生大小為 64、570、594 及 1518 位元組之網路封包， 並依 IMIX 之比例 57%、7%、16%及 20%混合，**時間為 60 秒。**
	6.4.3.1.2	測試平台產生待測物規格說明之**最大吞吐量 300%的 HTTP 封包，**持續 600 秒攻擊待測物開啟的連接埠以阻斷其服務，待測物不能發生當機、重開或斷線之情況。當攻擊結束後，安全功能應正常運作。
	6.4.3.2.2.	以測試平台**針對待測物提供之每項服務皆產**

項目	章節	建議修改內容
		生 10 種異常流量作為測試樣本。
	6.4.3.3.2	待測物運作期間不正常關閉電源時，經重新啟動後，應復原到非正常關閉電源前的狀態且**須符合下列要求(1)應保留最後設定的系統組態。(2)應保留斷電時間點前最後 5 分鐘的日誌檔案 (含系統日誌及安全事件日誌)。(3)能以最後設定的系統組態正常開機。**
	6.4.4.1.2	(4)流量之**平均速率**在測試期間**應維持待測物規格說明處理能力最大值之 50%。**
	6.4.1.2.2	新增**(13)上述 12 種方法的任意組合**
	6.4.1.3.3	(1)由測試平台產生**違反**安全事件的流量通過待測物，待測物的流量統計資訊應正確記錄~~**違反安全規則之**~~事件名稱、**成功與失敗**、時間、來源 IP、**來源 Port**、目的 IP、**目的 Port** 及內容。 **(2)管理者登入管理介面成功與失敗的認證紀錄。** **(3)管理者修改 WAF 規則時亦應產生對應的事件紀錄。**
	6.4.1.4.2	(3)**通行碼長度最少支援 13 位以上字元**
無線區域網路路由器(Wireless Router)	6.4.1.1.2	E.事件的日期、時間**(精確度應紀錄至秒)** 、類別、主題識別碼及結果（成功或失敗）。
	6.4.1.3.2	在安裝更新前須通過待測物之電子簽章機制驗證，如驗證失敗，應拒絕執行該次更新操作**並產生對應稽核紀錄。**
	6.4.1.5.2	**新增(3)通行碼長度最少支援 13 位以上字元**
	6.4.1.7.2	(2) 完成登入程序後立即更換通行碼，**更換**

項目	章節	建議修改內容
		通行碼時，需要驗證正確原始通行碼後始得更換通行碼。
	6.4.1.13.2	新增**(5)指派之 IP 位址個數達到最大值而無法建立連線時，應於連線介面顯示對應之錯誤訊息。**
網路型防火牆(Firewall)	6.4.1.4.2.	**(3)通行碼長度最少支援 13 位以上字元**
入侵偵測防禦系統(IDP)	6.4.1.3.2.	**(3)通行碼長度最少支援 13 位以上字元**
	6.4.1.4.2.	由測試平台產生~~違反~~安全事件的流量通過待測物，待測物的流量統計資訊應正確記錄~~違反安全規則之~~事件名稱、**成功與失敗**、時間、來源 IP、**來源 Port**、目的 IP、**目的 Port** 及內容。
	6.4.1.2.2.	開啟待測物預設之安全規則，使用測試平台自 A 埠各式躲避攻擊 (Evasion Attacks) 之流量，如：IP Packet Fragmentation、TCP Stream Segmentation 、URL Obfuscation 、FTP Evasion 及 RPC Fragmentation 或混合**以上技巧**躲避攻擊之流量，確認無法從 B 埠收到躲避攻擊之封包。
防毒閘道設備 Anti-Virus	6.4.2.1.1.	(9)測試平台產生大小為 64、570、594 及 1518 位元組之網路封包， 並依 IMIX 之比例 57%、7%、16%及 20%混合，**時間為 60 秒**。
	6.4.3.1.2.	測試平台產生待測物規格說明之**最大吞吐量 300%的 HTTP 封包**，持續 600 秒攻擊待測物開啟的連接埠以阻斷其服務，待測物不能發生當機、重開或斷線之情況。當攻擊結束

項目	章節	建議修改內容
		後，安全功能應正常運作。
	6.4.4.2.2.	以測試平台**針對待測物提供之每項服務皆產生 10 種異常流量**作為測試樣本。
	6.4.3.3.2.	待測物運作期間不正常關閉電源時，經重新啟動後，應復原到非正常關閉電源前的狀態且**須符合下列要求(1)應保留最後設定的系統組態。(2)應保留斷電時間點前最後 5 分鐘的日誌檔案 (含系統日誌及安全事件日誌)。(3)能以最後設定的系統組態正常開機**。
	6.4.4.1.2.	(4)流量之**平均速率**在測試期間**應維持**待測物規格說明處理能力**最大值之 50%。**
	6.4.1.4.2.	**(3)通行碼長度最少支援 13 位以上字元**
網路型垃圾郵件過濾設備(Anti-Spam)	6.4.2.1.1.	(9)測試平台產生大小為 64、570、594 及 1518 位元組之網路封包， 並依 IMIX 之比例 57%、7%、16%及 20%混合，**時間為 60 秒**。
	6.4.3.1.2.	測試平台產生待測物規格說明之**最大吞吐量 300%的 HTTP 封包**，持續 600 秒攻擊待測物開啟的連接埠以阻斷其服務，待測物不能發生當機、重開或斷線之情況。當攻擊結束後，安全功能應正常運作。
	6.4.3.2.2.	以測試平台**針對待測物提供之每項服務皆產生 10 種異常流量**作為測試樣本。
應用軟體控管系統(AC)	6.4.1.3.3.	由測試平台產生**違反**安全事件的流量通過待測物，待測物的流量統計資訊應正確記錄**違反安全規則之**事件名稱、**成功與失敗**、時間、來源 IP、**來源 Port**、目的 IP、**目的 Port** 及

項目	章節	建議修改內容
		內容。
	6.4.1.4.2.	**(3)通行碼長度最少支援 13 位以上字元**
	6.4.2.1.1	(9)測試平台產生大小為 64、570、594 及 1518 位元組之網路封包， 並依 IMIX 之比例 57%、7%、16%及 20%混合，**時間為 60 秒**。
	6.4.3.1.2.	測試平台產生待測物規格說明之**最大吞吐量 300%的 HTTP 封包**，持續 600 秒攻擊待測物開啟的連接埠以阻斷其服務，待測物不能發生當機、重開或斷線之情況。當攻擊結束後，安全功能應正常運作。
	6.4.3.3.1.	待測物運作期間不正常關閉電源時，經重新啟動後，應復原到非正常關閉電源前的狀態**且須符合下列要求(1)應保留最後設定的系統組態。(2)應保留斷電時間點前最後 5 分鐘的日誌檔案 (含系統日誌及安全事件日誌)。(3)能以最後設定的系統組態正常開機**。
	6.4.4.1.2.	(4)流量之**平均速率**在測試期間**應維持**待測物規格說明處理能力**最大值之 50%。**
乙太網路路由交換器 L2 Switch 路由交換器 L3-Switch	6.4.2.1.1	(9)測試平台產生大小為 64、570、594 及 1518 位元組之網路封包， 並依 IMIX 之比例 57%、7%、16%及 20%混合，**時間為 60 秒**。
	6.4.3.1.2.	測試平台產生待測物規格說明之**最大吞吐量 300%的 HTTP 封包**，持續 600 秒攻擊待測物開啟的連接埠以阻斷其服務，待測物不能發生當機、重開或斷線之情況。當攻擊結束後，安全功能應正常運作。

項目	章節	建議修改內容
	6.4.4.1.2.	(4)流量之**平均速率**在測試期間**應維持**待測物規格說明處理能力**最大值之 50%。**
無線接取設備 Thin AP+控制器或 Fat AP	6.4.1.1.2.	E.事件的日期、時間(**精確度應紀錄至秒**) 、類別、主題識別碼及結果（成功或失敗）。
	6.4.1.3.2.	在安裝更新前須通過待測物之電子簽章機制驗證，如驗證失敗，應拒絕執行該次更新操作**並產生對應稽核紀錄。**
	6.4.1.5.2.	**(3)通行碼長度最少支援 13 位以上字元**
	6.4.1.9.2.	(2) 完成登入程序後立即更換通行碼，**更換通行碼時，需要驗證正確原始通行碼後始得更換通行碼。**
	6.4.1.13.2.	**(5)指派之 IP 位址個數達到最大值而無法建立連線時，應於連線介面顯示對應之錯誤訊息。**

本計畫已於 103 年 9 月 2 日針對過去 10 項檢測規範辦理修正討論座談會議，相關意見可參考本報告座談會辦理(第二場座談會)之會議紀錄。

六、專家學者座談會

配合本專案各項工作項目需辦理 3 場座談會，座談會邀請政府機關、專家學者以及廠商代表，針對新增訂之資通設備檢測項目、過去 10 項資通設備檢測規範等議題進行討論，以使本專案擇出之資通設備及各設備安全檢測技術規範符合國內市場之需求。

(一)第一次專家學者座談會

1.時　　間：103 年 07 月 02 日(星期三) 15:00~17:30

2.地　　點：中華民國資訊軟體協會

3.主　　席：計畫主持人喻維貞副秘書長

4.與會人員：

出席代表	單位	職稱
專家學者	中華電信研究院	研究員
	財團法人資訊工業策進會	組長
	文化大學資訊工程學系	教授
政府機關	經濟部工業局資訊室	主任
	國家發展委員會資訊處	處長
	台北市政府資訊處	主任秘書 (書審)
廠商代表	趨勢科技股份有限公司	協理
	台灣威瑞特系統科技 股份有限公司	總經理
	庫柏資訊軟體股份有限公司	經理
	智易科技股份有限公司	副理

5.報告事項

由計畫協同主持人陳一瑋報告專案內容及預訂新增安全檢測技術規範之 4 項產品，並以進階持續性威脅防禦設備檢測技術規範草稿為例說明。

6.會議決議

(1)同意今年度新增資通設備安全檢測規範 4 品項為：「資料庫監

控設備(DBAM)」、「APT 防護設備(APT Protection)」、「無線寬頻分享器」、「虛擬私人網路閘道器(VPN Gateway)」，詳細各品項中英文名稱將由執行單位研擬後確定。[4]

(2)相關檢測技術規範內容撰擬方向將參考以下專家意見交流建議內容。

7.詳細會議紀錄請參考附件十一。

(二)第二次專家學者座談會

1.時　　間：103 年 09 月 09 日(星期三) 15:00~17:00

2.地　　點：中華民國資訊軟體協會

3.主　　席：計畫主持人喻維貞副秘書長

4.與會人員：

出席代表	單位	姓名
專家學者	財團法人資訊工業策進會	組長
	文化大學資訊工程學系	教授
	國立台灣科技大學資訊管理系	教授
政府機關	行政院公共工程委員會	專門委員
	經濟部工業局資訊室	主任(書審)
	檔案管理局	組長
廠商代表	友旺科技股份有限公司	資深經理
	趨勢科技股份有限公司	專案經理

4 本次會議決議之產品名，後於本計畫規範撰擬時，參考財團法人電信 技術中心(TTC)之用語，原：「資料庫監控設備(DBAM)」改為「資料庫安全稽核設備(DAM)」、原「APT 防護設備」改為「進階持續性威脅防禦設備(APT Defense System)」、原「無線寬頻分享器」改為「行動無線寬頻分享器」。

出席代表	單位	姓名
	桓基科技股份有限公司	副理
	世騰電子科技股份有限公司	專案經理

5.報告事項

由計畫專案顧問許郡泓報告現行已公告之 10 項安全檢測規範檢討與修正方向，並以網頁應用防火牆、無線區域網路路由器舉例說明修正內容。

6.會議決議

(1)同意 10 項安全檢測規範依據最新參考依據之版本進行調整，並加入目前資訊安全之重要議題，完善檢測規範。

(2)相關檢測技術規範內容修正方向，將參考與會專家建議並提請本計畫主辦單位確認後調整於規範內容中。

7.詳細會議紀錄請參考附件十一。

(三)第三次專家學者座談會

1.時　　間：103 年 12 月 17 日(星期三) 15:00~17:00

2.地　　點：中華民國資訊軟體協會

3.主　　席：計畫主持人喻維貞副秘書長

4.與會人員：

出席代表	單位	姓名
專家學者	文化大學資訊工程學系	教授
	中華電信研究院	經理
	中央大學資訊工程學系	教授(書審)
政府機關	經濟部資訊中心	主任

出席代表	單位	姓名
	行政院公共工程委員會	專門委員
	經濟部工業局資訊室	主任
	內政部警政署資訊室	主任
廠商代表	友旺科技股份有限公司	資深經理
	庫柏資訊軟體股份有限公司	經理
	台灣威瑞特系統科技 股份有限公司	總經理
	合勤科技股份有限公司	經理

5.報告事項

由計畫協同主持人報告 103 年度新增 4 項安全檢測規範草案(初稿)內容，並就試測作業進行說明，提出草案修正方案。

6.會議決議

(1)同意 4 項安全檢測規範依據試測結果進行調整，同時未避免閱讀誤解，請與通傳會就採購參考指引內「專用型」、「複合型」，以及安全檢測技術規範之「基礎型」、「進階型」加註說明。

(2)部分規範文字呈現盡量精準說明，避免讀者錯誤聯想。

(3)建議行動無線寬頻分享器應加註 LTE，與現行無線寬頻分享器設備區分。

7.詳細會議紀錄請參考附件十一。

七、推廣說明會

為使全台各級政府機關單位進一步認識與了解安全檢測之重要性，今年度特別辦理北、中、南、東及離島地區總計 7 場次推廣說明會，共計 355 人報名，345 人與會，比例為 97.18%。

本次推廣說明會主要針對檢測技術規範內容與通過審驗之效益向政府機關進行推廣說明，各場次資訊如表 22，相關人員詳參附件十二。部分與會機關代表於座談問答時段亦提出相關詢問，針對未來安全檢測規範如何應用在採購設備上提問。

表22 推廣說明會場次資訊

編號	場次	參與人數	時間	地點
1	金門	10	103 年 12 月 5 日 13:30~16:00	金門縣文化局 3 樓會議室(金門縣金城鎮環島北路 66 號)
2	高雄	48	103 年 12 月 8 日 13:30~16:00	蓮潭會館 101 會議室(高雄市左營區崇德路 801 號)
3	臺中 (第一場)	36	103 年 12 月 9 日 09:30~12:00	中國文化大學台中教育中心 319 教室(臺中市西屯區臺灣大道三段 658 號 3 樓)
4	臺中 (第二場)	48	103 年 12 月 9 日 13:30~16:00	中國文化大學台中教育中心 319 教室(臺中市西屯區臺灣大道三段 658 號 3 樓)
5	臺北 (第一場)	90	103 年 12 月 11 日 09:30~12:00	中國文化大學大新館 B2 樓圓形演講廳(臺北市延平南路 127 號)
6	臺北 (第二場)	88	103 年 12 月 11 日 13:30~16:00	中國文化大學大新館 B2 樓圓形演講廳(臺北市延平南路 127 號)
7	花蓮	25	103 年 12 月 12 日 13:30~16:00	花蓮洄瀾親子館階梯教室(花蓮市文苑路 12 號)
合計		345		

金門場

高雄場

台中場

台北場 1

台北場 2

花蓮場

資料來源：本計畫自行整理

圖11 推廣說明會實況

本計畫於推廣說明會報名期間同步進行性別與相關資料統計，因本次推廣會議題，分別有「資訊人員」、「採購人員」參加，資訊人員佔 89%，採購人員佔 11%，比例如圖 12：

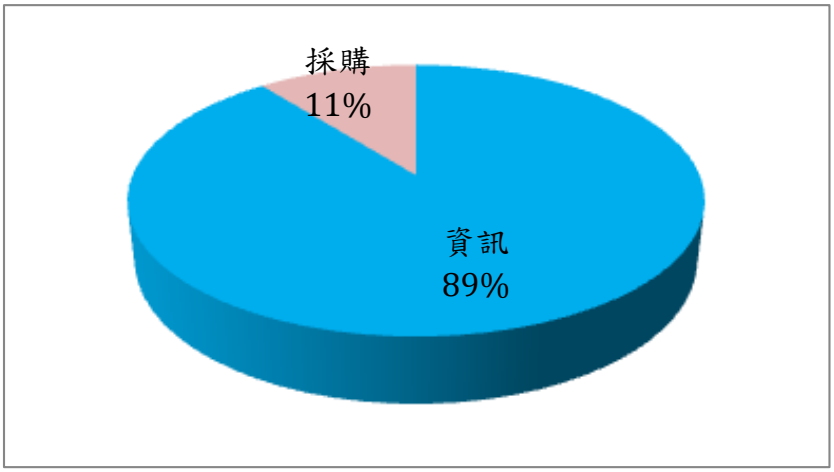


圖12 「資訊人員」、「採購人員」比例

報名人員性別比，資訊人員男女比為 81%：19%；採購人員男女比為 76%:24%，整體比例為：資訊(男)73%、資訊(女)17%、採購(男)8%、採購(女)2%，圖示如下：

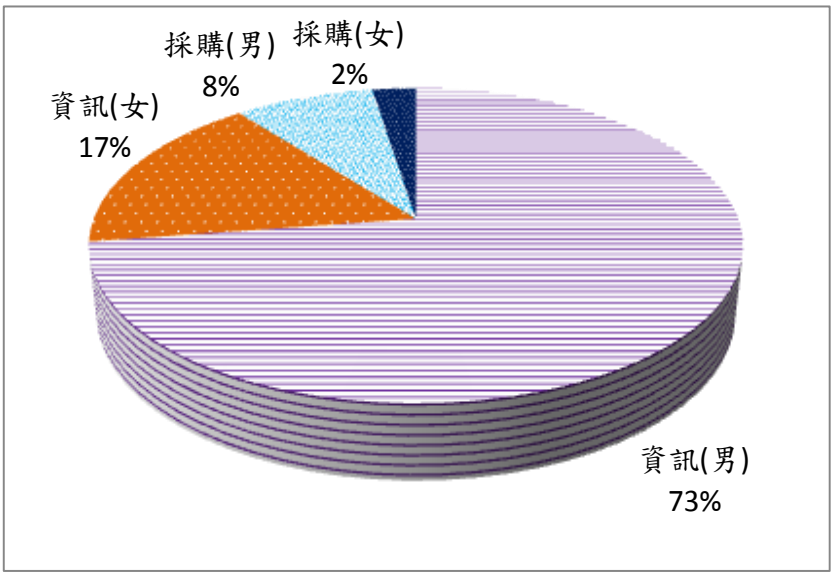


圖13 「資訊人員」、「採購人員」性別比例

因本次議題主要以資通設備檢測為主，故主要參與對象仍以資訊人

員為主，採購人員主要是因為議程後段安排有共同供應契約說明而報名參加。本次報名人員中，學歷比例如圖 14，主要仍是以學士與碩士為主(相關性別統計則請參考附件十三)：

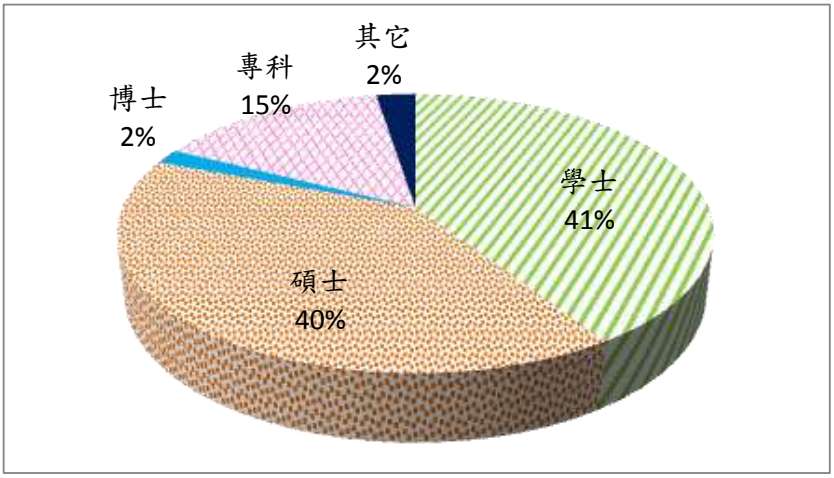


圖14 與會人員學歷比例

本次統計資訊中，超過半數以上的機關在近 3 年中皆已採購資安設備(294 個機關)，其它 61 個機關代表表示未曾購買或不清楚，比例為 17.18%。

本次推廣說明會於報名時針對各機關報名人員就「有關資通設備採購時，會有哪些考量因素影響判斷」進行調查，本會以「規格、功能、有效性、便利、其它」等因素進行統計，統計分析後，機關人員於購買資通設備產品主要考量因素如下(以複選統計)：

表23 機關人員購買資通設備主要考量因素

	功能	有效	規格	便利
佔比(%)	60.06	33.24	26.48	25.63

對於資訊人員而言，資通設備的購買主要以功能為考量主因，此部分在說明會現場 QA 時段，亦能充分反映。總結本次推廣說明會可歸納以下意見，做為後續參考：

1.資通設備安全檢測規範若能協助各級機關人員採購相關資通設

備時可參考、援引注意之規範，建議可將相關檢測規範納入法規並且明確列入共同供應契約，以便各級機關人員有所遵循依據。

2.建議未來可持續提供相關資訊予各級政府機關資訊、採購人員參考，以利資訊、採購人員能即時了解目前中央政府資通安全需求，於採購時能購得符合自身需求之設備。

八、後續推廣建議

(一)背景說明

網際網路為人類帶來便利與快捷，然而伴隨網路普及化與消費者行為改變，引發的網路犯罪及個資保護等課題，已逐漸成為影響國家安全、社會安定的隱憂，全球正面臨嚴峻的資安威脅。

近年各主要國家、區域均積極推動新資安政策，包含：將資安議題提升至國家安全層次、重視國民相關權益與個資保護議題、逐漸重視雲端運算相關安全議題、重視政府與民間或產學合作、與國際合作交流等。

圖15　國家資通訊安全執行策略與行動方案圖

資料來源：國家資通訊安全發展方案(102-105 年)

依據 102-105 年國家資通訊安全發展方案中，透過「推展資安基礎環境安全設定」、「加強資安防護管理二線監控機制及情蒐」、「強化資安應變功能及復原能力」及「建構資安專案管理(SPMO)機制」等行動方案，達成「強化國家資安政策，建立安全資安環境」、「完備資安防護管理，分享多元資安情報」、「奠基資安技術能量，整合科技實務應用」及「擴大資安人才培育，加強國際資安交流」4大策略目標。

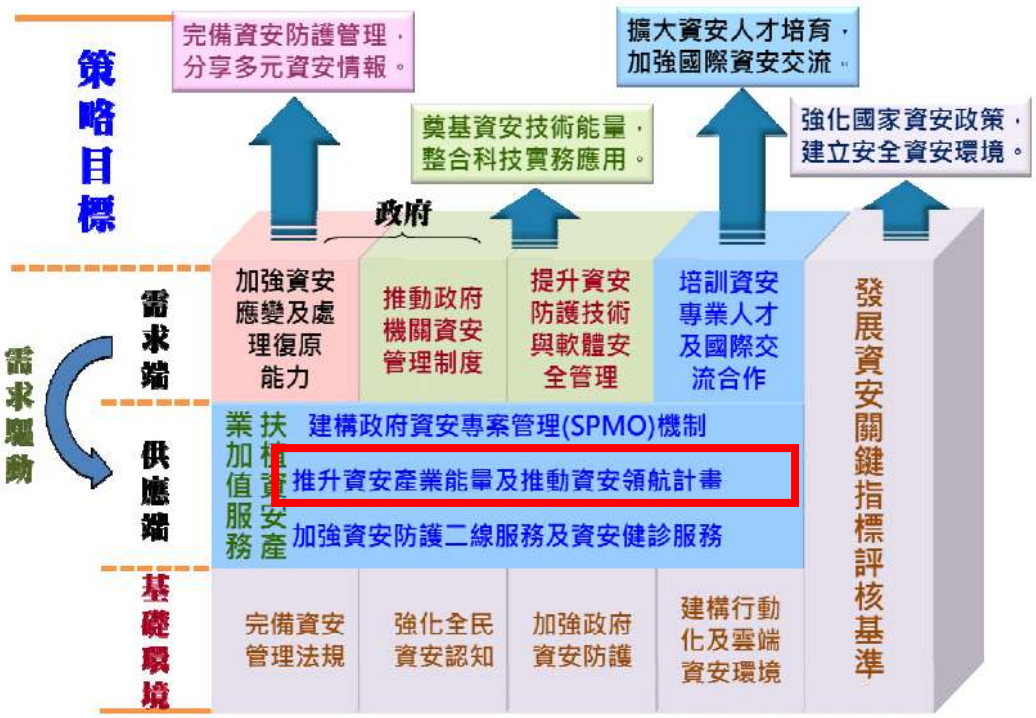


圖16　資通安全政策發展藍圖

資料來源：國家資通訊安全發展方案(102-105 年)

(二)現階段執行現況說明

推動資通訊設備安全檢測為確保政府機關所使用之資通設備具備安全性，國家通訊傳播委員會推動政府機關採購經資安驗證合格之設備。具體作法包含研析國內廠商資通設備之市場規模及研發能力，據以研訂適合我國短中長期資通設備安全檢測適用設備類別、項目及安全防護等級，並訂出各項技術標準、與資通安全設

備採購參考指引，上述內容截至本年度已完成 14 項產品規範。

茲將相關上述完成之資通安全設備檢測技術規範與代表廠商對應參照如下表。

表24 短、中期資通設備檢測技術規範與共同供應契約對應參照

產品	代表廠商列舉
防火牆(Firewall)	友訊、桓基、威播、合勤
入侵偵測防禦設備(IDP)	趨勢、新軟、友旺、眾至
防毒閘道器設備(Anti-Virus)	友訊、文佳、合勤、全景
垃圾郵件過濾設備(Anti-Spam)	綠色運算、友旺、碩琦、中華數位
網頁應用防火牆(WAF)	阿碼、安穩特、文佳
應用軟體控管系統(AC)	利基、威播、文佳
乙太網路交換器(L2 Switch)	友訊、合勤、華碩、明泰
路由交換器(L3 Switch)	華碩、明泰、智邦、友訊、合勤
無線接取設備(AP)	普聯、訊舟、華碩、友勁、美商防特網
無線寬頻路由器設備(WiFi-Router)	正文、明泰、智邦、永洋、居易、台達電子
資料庫安全稽核設備(DAM)	玄力、庫柏、希比思系統、利基
進階持續性威脅防禦設備(APTDS)	趨勢、美商阿碼證點、數位資安
行動無線寬頻路由器(Mobile Wi-Fi Hotspot)	中磊、智易、明泰、亞旭、合勤、友訊
虛擬私人網路閘道器(VPN Gateway)	合勤、友訊、桓基、俠諾、居易、友旺

(三)後續推廣建議

資通安全設備本身之安全性攸關使用者安全防護之效益，對安全防護環境之維護極為重要，若設備本身不能發揮應有之作用，甚至有資安漏洞或被植入木馬等重大疏失，對使用者之影響將即為嚴重，尤其使用者為政府機關時，甚至將影響國家安全。國家通訊傳播委員會主責技術規範內容，然推動資通設備檢測技術規範之落實，並非訂出檢測規範後即可，仍需從整體推動面進行。

1.逐年進行規範編撰

(1)至 103 年底制定完成 14 項檢測技術規範

本計畫已於 100 年度計畫中完成 8 項檢測技術規範，包含：網路型防火牆(Firewall)、入侵偵測防禦系統(IDP)、防毒閘道設備(AntiVirus)、網路型垃圾郵件過濾設備(AntiSpam)、網頁應用防火牆(WAF)、應用軟體控管系統(ApplicationControl)、乙太網路交換器(L2Switch)、路由交換器(L3Switch)等。於 101 年度計畫中完成無線接取設備(Thin AP+控制器或 Fat AP)、無線區域網路路由器(Wireless Router)二項。並於今(103)年完成資料庫安全稽核設備(DAM)、進階持續性威脅防禦設備(APTDS)、行動無線寬頻路由器(Mobile Wi-Fi Hotspot)、虛擬私人網路閘道器(VPN Gateway)等四項資通設備檢測技術規範。

(2)依據供需雙方需求逐年增加檢測技術規範，健全資安整體環境面

通傳會已制定 14 項檢測技術規範，應逐年依據供需雙方需求編列預算進行規範之編撰過規範編撰，並藉由產品檢測技術規範之編撰逐步提升資安產業自我研發能量，進一步推動使政府機關採購之資通設備產品納入檢測範圍中，藉以強化我

國整體資訊安全。

2.規範檢測與機關導入推廣作業

(1)輔導業者通過檢測技術規範或提供檢測補助，提高廠商參與意願

國內資安業者營運不易，資安問題亦層出不窮急需各業者投入資源研發，建議可輔導業者通過檢測技術規範，或由主責部會提供檢測補助，提高廠商參與意願。

(2)積極推動規範納入共同供應契約

目前台銀共同供應契約已停辦資通安全設備項目採購作業，相形之下資通設備檢測技術規範納入於現階段無法納入共同供應契約，然而各機關同仁對於資通安全設備透過共同供應契約採購之需求若渴，希可於未來確認該類之共同供應契約承接機關後，推動檢測技術規範納入共同供應契約，對於業者提高產品之附加價值確有一定程度之助益。

(3)推動示範性機關使用通過檢測設備

資通設備廠商送驗產品不外乎希望能提高產品附加價值，並有更多消費者願意採購檢測通過之產品，因此建議短期以各級政府機關宣導為主，期望透過各機關單位於新增購資通設備時納入安全檢測通過證明，有效推廣安全檢測技術規範。於未來可持續進行規範推廣活動，並建議通傳會與國發會合作推動示範性機關採購通過檢測規範之產品。

(4)通過檢測設備廠商與機關使用經驗分享，強化檢測品質與優勢

透過通過檢測之設備廠商對於提升產品優勢與競爭力之經驗

分享，與示範性機關採購通過檢測之資通設備後所獲得之助益，供需雙方之經驗分享擴散，強化通過檢測之產品品質與優勢，有助於吸引更多資安業者加入檢測行列，共同研發更安全、優質之資通設備產品。

(5)長期建立法源依據，強化整體國家資訊安全

希望能有相關法源明確規定資通設備具通過安全檢測，取得通過證明，俾利各機關於採購規格研提時有參考依據，當資通安全設備皆通過審驗標準，對整體國家資訊安全定有莫大助益。

參、附件

一、附件一 資料庫安全稽核設備(DAM)資通安全檢測技術規範草案(初稿)

二、附件二 資料庫安全稽核設備(DAM)資通安全採購參考指引草案(初稿)

三、附件三 進階持續性威脅防禦設備(APT Defense System)資通安全檢測技術規範草案(初稿)

四、附件四 進階持續性威脅防禦設備(APT Defense System)資通安全採購參考指引草案(初稿)

五、附件五 行動無線寬頻分享器(Mobile Wi-Fi Hotspot 資通安全檢測技術規範草案(初稿)

六、附件六 行動無線寬頻分享器(Mobile Wi-Fi Hotspot)採購參考指引草案(初稿)

七、附件七 虛擬私人網路閘道器(VPN Gateway)資通安全檢測技術規範草案(初稿)

八、附件八 虛擬私人網路閘道器(VPN Gateway)採購參考指引草案(初稿)

九、附件九 103 年資通設備試測報告

十、附件十 現有規範檢討與修正

十一、附件十一 座談會會議記錄及簽到表

十二、附件十二 7 場次推廣說明會簽到表

十三、附件十三 性別相關統計比例

十四、附件十四 各品項產品彙整

附件一

資料庫安全稽核設備(DAM)

資通安全檢測技術規範草案(初稿)

附件二

資料庫安全稽核設備(DAM)

資通安全採購參考指引草案(初稿)

附件三

進階持續性威脅防禦設備(APT Defense System)
資通安全檢測技術規範草案(初稿)

附件四

進階持續性威脅防禦設備(APT Defense System)
資通安全採購參考指引草案(初稿)

附件五

行動無線寬頻分享器(Mobile Wi-Fi Hotspot)資通安全檢測技術規範

附件六

行動無線寬頻分享器(Mobile Wi-Fi Hotspot)

採購參考指引草案(初稿)

附件七

虛擬私人網路閘道器(VPN Gateway)

資通安全檢測技術規範草案(初稿)

附件八

虛擬私人網路閘道器(VPN Gateway)

採購參考指引草案(初稿)

附件九

103 年資通設備試測報告

附件十

現有規範檢討與修正

附件十一

座談會會議記錄及簽到表

附件十二

7 場次推廣說明會簽到表

附件十三

性別相關統計比例

附件十四

各品項產品彙整