具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引總說明

考量現行家戶為接收多媒體隨選視訊服務或有線電視服務時，訂戶端須加裝數位機上盒始得收視，而隨著物聯網及創新應用服務蓬勃發展，愈來愈多數位機上盒亦具備連接網際網路之功能，若此類數位機上盒無完善的資通安全防護機制，極可能衍生個人隱私安全及相關應用服務之損害，爰參考 NIST、UL、CableLabs、OWASP 等國際組織訂定之標準研訂本指引，期帶動相關產品之自主性資安檢測及驗證，以保護消費者權益並協助業者強化產品之安全。其重點說明如下：

一、前言。（第一點）

二、適用範圍。（第二點）

三、引用標準。（第三點）

四、用語釋義。（第四點）

五、檢測方式及安全等級。（第五點）

六、書面審查合格標準。（第六點）

七、實機測試合格標準。（第七點）

具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引

規定	說明
1. 前言 為確保連接固定通信多媒體內容傳輸平臺、有線廣播電視系統之數位機上盒（Set Top Box，STB）網際網路連線功能資安品質，爰訂定本指引。	本指引之訂定目的。
2. 適用範圍 本指引適用具接收並解調固定通信多媒體內容傳輸平臺、有線廣播電視系統頭端傳送之訊號，以供訂戶端接收影像、聲音或資訊，且可連接網際網路之終端設備。	本指引適用之設備。
3. 引用標準 本指引參考標準如下，測試項目與相關國際標準對照詳附錄一及附錄二。 3.1 CableLabs® Requirements CPE Security，Common Security Requirements for IP-Based MSO-Provided CPE，V01，2013/03，CableLabs。 3.2. Recommendation for Cryptographic Key Generation, NIST Computer Security Division，V01，201212，NIST。 3.3. CableLabs Specifications Security Criteria for Service Delivery Network，V01，2009/07，CableLabs。 3.4. Collaborative Protection Profile for Network Devices，Version 2.0， 2017/05，NIAP。 3.5. Network Device Collaborative Protection Profile（NDcPP） Extended Package-Wireless Local Area Network （WLAN） Access Systems， Version 1.0，2015/05，NIAP。 3.6. Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations，Revision 4，2013/04，NIST。 3.7. Standard for Software Cybersecurity for Network-Connectable Products, Part 1:	本指引內容參考來源。

General Requirements，Version 1.0，2017/07，UL 2900-1。 3.8. Standard for ONVIF™ Core Specification，Version 2.1，June, 2011，ONVIF™。 3.9. IoT Security Guidance，Version 1.0，2017/02，OWASP。 3.10. ITU-T H.721 IPTV terminal devices: Basic model，2016/10，ITU-T。 3.11. 無線區域網路接取設備及路由設備資通安全檢測技術指引（ISG011），2018/10，國家通訊傳播委員會。 3.12. 智慧型手機系統內建應用程式資通安全檢測技術規範，2017/03，國家通訊傳播委員會。 3.13. 行動應用App基本資安檢測基準，V3.0，2017/08，經濟部工業局。 3.14. 影像監控系統資安標準—第一部：一般要求（TAICS TS-0014-1），Version 1.0，2018/06，台灣資通產業標準協會。 3.15. 影像監控系統資安標準—第二部：網路攝影機（TAICS TS-0014-2），Version 2.0，2018/06，台灣資通產業標準協會。	
4.用語釋義 4.1 共同準則（Common Criteria，CC） 指國際資通安全產品評估及驗證之標準（ISO/IEC 15408），用以評估及驗證資通安全產品之安全等級與功能性，其評估保證等級（Evaluation Assurance Level，下稱EAL）分為7個等級，最低等級為EAL 1，最高等級為EAL 7。 4.2 安全標的（Security Target, ST） 指待測物符合保護剖繪或特定安全功能需求之規格文件。 4.3 保護剖繪（Protection Profile, PP） 指待測物應具備之安全基本需求文件。 4.4 安全功能（TOE Security Functions, TSF） 指待測物實現安全標的（ST）所列安全規格之功能。 4.5 安全功能需求（Security Functional Requirement, SFR）	本指引之用語釋義。

指依「共同準則第二部：安全功能需求」所列TSF相關規定，陳述評估標的應具備之安全功能。 4.6 評估標的（Target of Evaluation，TOE） 指待測物。 4.7 安全功能介面（TOE Security Functions Interface, TSFI） 指待測物實現安全功能需求對外溝通之介面。 4.8 安全領域（Security Domain） 指待測物為實現安全功能需求，分配不同權限使用者之資源。 4.9 自我保護（Self-Protection） 指防護安全功能不被無關之程式碼或外力破壞之機制。 4.10 常見弱點與漏洞 （Common Vulnerabilities and Exposures, CVE） 指美國國土安全部贊助之弱點管理計畫，該計畫針對每一弱點項目賦予其全球認可唯一共通編號。 4.11 漏洞評鑑系統 （Common Vulnerability Scoring System, CVSS） 指包括威脅所造成損害的嚴重性、資安漏洞的可利用程度與攻擊者不當運用該漏洞的難易度等判定標準之評鑑系統。評比從0分到10分，0代表沒有弱點，而10則代表最高風險。 4.12. 敏感性資料（Sensitive Data） 指內容遭外洩或竄改將可能導致個人或資料擁有者的權益受損之相關資訊，如個人資料保護法所稱個人資料、帳號密碼、電話號碼、信用卡資訊等。 4.13. 通用非同步收發傳輸器（Universal Asynchronous Receiver /Transmitter，UART） 指一種異步收發傳輸器，屬電腦硬體的一部分，將資料由串行通信與並行通信間作傳輸轉換，可作為連接外部設備的接口。 4.14. 埠鏡像（port mirroring） 指將某一通訊埠上之流量複製到另一通訊埠上，以達流量監控、除錯等目的。	

5.檢測方式及安全等級 5.1 檢測方式分為書面審查及實機測試。 5.1.1 書面審查之檢測項目包括設備概述、安全架構、安全功能規格、安全指引及設計安全性。 5.1.2 實機測試之檢測項目包括實體安全、系統安全、Wi-Fi功能及其他功能。 5.2 安全等級依書面審查及實機測試之檢測項目之差異，分為初階、中階與高階三級。 5.3 檢測項目、檢測細項所對應之安全等級與適用設備如表一至表二，申請者應依待測物申請之安全等級檢附表一所列文件。	明定本指引之檢測方式、檢測項目、檢測細項及相對應之安全等級。
6.書面審查合格標準 6.1 設備概述 設備概述說明（如表三）應載明下列事項： （1）設備名稱、廠牌、型號、產地。 （2）申請者名稱（製造商或代理商）。 （3）製造商名稱。 （4）軟體、韌體版本及產地。 （5）通訊協定（含版本）。 （6）通訊介面。 （7）Wi-Fi傳輸安全機制，申請高階安全等級且具Wi-Fi AP功能之待測物應提供WPA2等級以上（含）之保密機制，且金鑰強度至少為128位元（含）。 （8）進入作業系統除錯模式之方法。 （9）預設開啟之網路通訊埠。 （10）軟、韌體更新方式。 （11）工程模式密碼。 （12）使用敏感性資料之內建應用程式清單及其使用之敏感性資料類型。 （13）外觀：檢附待測物4x6吋以上之彩色照片或圖片彩色照片，其廠牌及型號須清晰可辨讀，並包含樣品之頂視圖、底視圖、左視圖、右視圖、正視圖及背視圖。 6.2 安全架構 安全架構描述表(如表四)應載明下列事項: （1）因執行安全功能所區隔之安全領域。 （2）安全功能的安全初始程序。	明定書面審查之合格標準，本點係參考ISO/IEC 15408 訂定，以瞭解產品在設計開發的階段是否納入資安考量。

（3）安全功能的自我保護機制。 （4）安全功能執行如何避免被繞道。 6.3 安全功能規格 安全功能介面表(如表五)應載明下列事項: （1）安全功能介面名稱。 （2）目的。 （3）可實現的安全功能需求。 （4）操作方式。 （5）參數。 （6）執行的動作。 （7）錯誤訊息。 6.4 設計安全性 子系統描述與分類表（如表七）應說明如何以子系統組成安全功能規格之安全功能介面，並載明下列事項： （1）子系統名稱。 （2）目的。 （3）子系統隸屬之安全功能介面。 （4）子系統行為說明。	
7. 實機測試合格標準 7.1 實體安全 7.1.1 實體介面安全管控 （1）測試環境 A.測試設備：以有線（如USB、UART等）方式連接待測物之設備。 B.測試設備及待測物連接方式如圖一。 （2）測試方法 以USB埠、UART埠及其他實體介面方式進入作業系統之除錯模式。 （3）判定標準 待測物具USB埠、UART埠或其他實體介面者，應通過身分鑑別，始得以該等介面進入作業系統之除錯模式，但無法經由該等介面進入除錯模式者，不在此限。 7.1.2 外殼實體防護 （1）測試環境 無。 （2）測試方法	參考 NIST、UL、CableLabs、OWASP 等國際組織訂定之標準，明定實機測試之合格標準。

檢視待測物外殼是否具備防拆設計（如一體成型、防拆螺絲等）。 （3）判定標準 待測物應符合下列情形之一： A.待測物外殼應具備防拆設計。 B.待測物外部不應有徒手即可還原預設通行碼之設計。 7.2. 系統安全 7.2.1. 網路通訊埠安全 （1）測試環境 A.測試設備：以無線（如Wi-Fi）或有線(如乙太網路)方式連接待測物之設備，並且具備網路通訊埠掃描功能。 B.測試設備及待測物連接方式如圖二。 （2）測試方法 掃描待測物於原廠設定狀態下開啟之網路通訊埠。 （3）判定標準 A.待測物開啟之網路通訊埠，應與申請者檢附之表三相符。 B.待測物應關閉FTP及Telnet使用之網路通訊埠，但以明確之方式宣告(如載明於說明書）前述網路通訊埠開啟者，不在此限。 7.2.3. 軟韌體更新 （1）測試環境 待測物透過有線（如乙太網路或同軸電纜）方式連接至可更新軟韌體之伺服器，連接方式如圖三。 （2）測試方法 依據表三之軟韌體更新方式執行待測物更新。 （3）判定標準 待測物應完成更新，且用戶設定應與更新前相符，例如：親子鎖密碼。 7.2.3. 登入保密功能 （1）測試環境 待測物透過有線（如乙太網路或同軸	

電纜)方式連接至服務提供者,連接方式如圖四。 （2）測試方法 開啟待測物之工程模式及親子鎖，並輸入密碼進行登入。 （3）判定標準 A.登入過程中，待測物之工程模式登入介面應以特殊符號(如：＊)遮蔽輸入之明文密碼字元。 B.登入過程中，待測物之親子鎖登入介面應以特殊符號(如：＊)遮蔽輸入之明文密碼字元。 7.2.4. 工程模式鑑別 （1）測試環境 待測物連接顯示器，並透過遙控器進行操作，連接方式如圖五。 （2）測試方法 A.連續輸入3次（含）以上錯誤之密碼嘗試登入待測物之工程模式。 B.輸入正確之密碼登入待測物之工程模式。 （3）判定標準 A.輸入錯誤密碼應無法登入待測物之工程模式。 B.輸入正確密碼始可登入待測物之工程模式。 C.工程模式密碼長度至少應為8位數字。 7.2.5. 影音傳輸保護（僅適用固定通信多媒體內容傳輸平臺機上盒） （1）測試環境 A.測試設備：以有線(如乙太網路)方式連接交換器與服務提供者，並透過交換器連接待測物及檢測平台，且交換器應具埠鏡像功能。 B.測試設備及待測物連接方式如圖六。 （2）測試方法 開啟交換器之埠鏡像功能，使用遙控器執行待測物之收視功能（如隨選視	

訊或頻道切換等）並側錄封包。 （3）判定標準 A.待測物與服務提供者的資料傳輸，採用加密傳輸，金鑰強度至少為128位元（含）。 B.側錄封包之憑證資訊，應由公正第三方單位發行且憑證應在有效期限內。 7.3. Wi-Fi通訊安全 第7.3.測試規定適用具Wi-Fi功能之待測物。 7.3.1. Wi-Fi功能登入保密 （1）測試環境 同7.2.4之測試環境。 （2）測試方法 開啟待測物之Wi-Fi功能設定介面，並輸入密碼進行登入。 （3）判定標準 A.登入過程中，待測物之Wi-Fi功能設定介面應以特殊符號（如：＊）遮蔽輸入之明文密碼字元。 B.密碼由英文大小寫、數字或特殊字元所組成。 密碼長度可由管理人員設定，且需支援8字元以上之密碼。 7.3.2. Wi-Fi功能網頁管理介面安全 （1）測試環境 A.測試設備：以無線（如Wi-Fi等）或有線（如乙太網路線等）方式連接待測物之設備，並且具備網頁管理介面弱點掃瞄工具。 B.測試設備及待測物連接方式如圖二。 （2）測試方法 A.更新測試設備之網頁管理介面弱點掃瞄工具至最新版本。 B.對待測物設定Wi-Fi功能之網頁管理介面進行Injection 及Cross-Site Scripting （XSS）弱點掃描。 （3）判定標準	

待測物提供網頁管理介面以設定Wi-Fi功能者，待測物不得檢出Injection及Cross-Site Scripting （XSS）之資安攻擊風險。 7.3.3. 共通弱點評估初階測試與中階測試 （1）測試環境 A.測試設備：以Wi-Fi方式連接待測物之設備。 B.測試設備、待測物及稽核伺服器連接方式如圖七。 （2）測試方法 A.更新測試設備弱點偵測功能之CVE弱點資料庫，該資料庫應包含NIST發布之CVE弱點，及採用NIST發布之弱點評估方式。 B.掃描待測物通訊或管理介面之CVE弱點。 （3）判定標準 待測物不得檢出弱點評鑑系統（CVSS）嚴重性等級評比為重大（Critical，即9分以上）之弱點。 7.3.4. 共通弱點評估高階測試 待測物不得檢出弱點評鑑系統（CVSS)嚴重性等級評比為高(High，即7分以上）之弱點；測試環境、測試方法依7.5.1規定為之。 7.3.5. 模糊測試初階測試 （1）測試環境 同7.3.3之測試環境。 （2）測試方法 使用模糊測試工具(參考附錄三)進行5,000筆隨機樣本之測試，並將結果儲存在測試設備。前述隨機樣本至少應包含IEEE 802.11i標準下產生變異樣本。 （3）判定標準 測試過程中待測物應正常運作，且不得重新開機。 7.3.6. 模糊測試中階測試 除測試方法之測試樣本筆數增加至	

7,000筆之外，測試環境、測試方法及判定標準依7.3.5之規定為之。 7.3.7. 模糊測試高階測試 除測試方法之測試樣本筆數增加至10,000筆之外，測試環境、測試方法及判定標準依7.3.5之規定為之。 7.4. 其他功能 7.4.1. 付費機制控管 （1）測試環境 同7.2.3之測試環境。 （2）測試方法 A.使用遙控器執行待測物之付費功能（如選購隨選視訊或付費頻道等），選擇拒絕（或取消）付費選項，並查詢付費紀錄。 B.使用遙控器執行待測物之付費功能，選擇確認付費選項，並查詢付費紀錄之時間及金額。 （3）判定標準 待測物具備付費功能者，應符合下列要求： A.待測物提供付費確認及拒絕（或取消）選項。 B.測試方法A執行後，無付費紀錄或顯示交易未成功。 C. 測試方法B執行後，付費紀錄之時間及金額與選購行為相符，且選購之服務可正常使用。 7.4.2. 敏感性資料之存取 （1）測試環境 同7.2.3之測試環境。 （2）測試方法 A.檢查申請者檢附之表三所列使用敏感性資料之內建應用程式的隱私權政策或使用聲明。 B.執行受測應用程式。 （3）判定標準 申請者檢附之表三所列使用敏感性資料之內建應用程式，應符合下列情形之一：	

A.步驟A中，隱私權政策或使用聲明應提供應用程式存取敏感性資料之相對應說明及使用者同意機制。 B.步驟B中，應用程式存取敏感性資料時，應提供相對應之使用者同意機制。	

表一、書面審查之檢測項目及對應之安全等級與適用設備

檢測項目	應檢附文件	安全等級		
		初階	中階	高階
設備概述	設備概述說明　（如表三）	6.1	6.1	6.1
安全架構	安全架構描述表　（如表四）	--	--	6.2
安全功能規格	安全功能介面表　（如表五）	--	--	6.3
設計安全性	子系統描述與分類表（如表六）	--	--	6.4

表二、實機測試之檢測項目及對應之安全等級與適用設備

檢測項目	檢測細項	安全等級		
		初階	中階	高階
實體安全	實體介面安全管控	7.1.1	7.1.1	7.1.1
	外殼實體防護	--	7.1.2	7.1.2
系統安全	網路通訊埠安全	7.2.1	7.2.1	7.2.1
	軟韌體更新	7.2.2	7.2.2	7.2.2
	登入保密功能	--	7.2.3	7.2.3
	工程模式鑑別	7.2.4	7.2.4	7.2.4
	影音傳輸保護	7.2.5	7.2.5	7.2.5
Wi-Fi 通訊安全	Wi-Fi 功能登入保密	7.3.1	7.3.1	7.3.1
	Wi-Fi 功能網頁管理介面安全	7.3.2	7.3.2	7.3.2
	共通弱點評估	7.3.3	7.3.3	7.3.4
	模糊測試	7.3.5	7.3.6	7.3.7
其他功能	付費機制控管	--	7.4.1	7.4.1
	敏感性資料之存取	7.4.2	7.4.2	7.4.2

表三、設備概述說明

設備名稱		
廠牌		
型號		
產地		
申請者 （公司、商號名稱）	□ 製造商 □ 代理商 □ 其　他	
製造商		
軟體、韌體 版本及產地		
通訊協定 （含版本）		
通訊介面		
Wi-Fi 傳輸安全機制		
進入作業系統 除錯模式之方法		
預設開啟之 網路通訊埠		
軟體、韌體 更新方式		
工程模式密碼		
使用敏感性資料之 內建應用程式清單	使用敏感性資料之 內建應用程式	使用之敏感性資料類型
		□個人資料保護法所稱個人資料 □帳號密碼　□電話號碼 □信用卡資訊　□其他
		□個人資料保護法所稱個人資料 □帳號密碼　□電話號碼 □信用卡資訊　□其他
外觀		

表四、安全架構描述表

項目	說明	申請者填寫內容
1.安全領域	列出各安全功能介面對應之安全領域名稱，並在安全功能操作環境及內部執行限制下，如何區隔所需保護的資料。 *範例：TSFI_GUI:* *Domain_SecureLogAudit* *Domain_SecureConnection* *透過 TSFI_GUI 來執行管理功能時，該 TSFI 同一時間只能有單一遠端連線，並只能執行單一稽核資料處理請求。*	
2.初始程序	操作待測物的相關元件/環境 *範例：待測物網路連接程序* 提供安全啟動待測物之相關元件起始步驟及安裝程序。 *範例：* *1. 從端口標記為 0/0（ethernet0/0 接口）連接一個 RJ-45 電纜到交換機或路由器 Trust 安全區。* *2. 從端口標記為 0/1（ethernet0/1 接口）連接一個 RJ-45 電纜到交換機或路由器中的 DMZ 安全區。*	
3.自我保護機制	1.自我保護功能 列出各安全功能介面對應之自我保護機制 *範例：TSFI_WEB* *自我保護 1:身分驗證* *自我保護 2:遠端連線加密* 2. 與外部設備之關係 說明安全功能及其介面與外部設備之資料交換動作 *範例：遠端以瀏覽器連線待測物進行管理功能時，以 TSFI_WEB GUI 介面進行身分認驗證* 3.自我保護機制說明 安全功能介面提供實體上或邏輯上的自我保護機制 *範例：*	

項目	說明	申請者填寫內容
	（1）應輸入密碼才能進入介面。 *（2）資料傳輸機制：TLS/SSL。* *（3）特殊執行方式：指紋辨識。* *（4）特殊設備需求：指紋辨識器。*	
4.防止繞道	1. 列出各安全功能對應之防止繞道機制 *範例：TSF_Authentication 身分驗證功能* 2. 列舉可能繞道之手法 *範例：可能直接以維護介面不經身分鑑別操控待測物。* 3. 說明防範作法，包含進入安全功能的介面如何被保護、執行階段的資料處理如何保護、是否存有其他對外通道及相關防範非法進入之機制等。 *範例：防範作法為以實體封鎖方式，防止利用維護介面繞道身分鑑別程序。*	

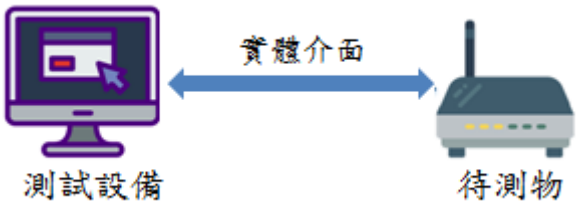
表五、安全功能介面表

項目	項目說明	申請者填寫內容
1.安全功能介面名稱	列出所有安全功能介面。 *範例：TSFI_CLI*	
2.目的	說明各安全功能介面之安全功能目的。 *範例：提供命令列模式操作介面*	
3.可實現的安全功能需求	說明各安全功能介面如何實現表二所列之實機測試檢測項目。 *範例：SFR_安全管理：提供安全管理功能*	
4.操作方式	說明如何使用各安全功能介面。 *範例：以 ssh 連接待測物，即提供命令列模式操作介面*	
5.參數	說明各安全功能介面所有參數及其意義。 *範例：ID & password*	
6.執行動作	說明各安全功能介面如何運作及其執行細節。 *範例：可下達管理命令操作待測物*	
7.錯誤訊息	說明執行各安全功能介面產生之錯誤訊息，包含其意義及產生條件。 *範例：連接失敗、鑑別失敗*	

表六、子系統描述與分類表

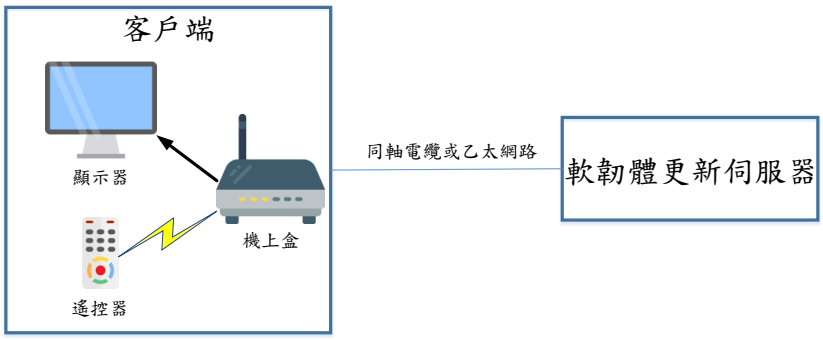
項目	項目說明	申請者填寫內容
1.子系統名稱	列出各安全功能介面之子系統。 *範例：Subsystem_ssh*	
2.目的	說明各子系統之安全功能目的。 *範例：提供 ssh 服務*	
3.子系統隸屬之安全功能介面	說明各子系統隸屬於表五所列之安全功能介面。 *範例：TSFI_CLI*	
4.子系統行為說明	說明各子系統行為如下： 1. 如何實現安全功能介面的功能。 *範例：提供 TSFI_CLI 命令列模式操作介面* 2. 與其他子系統間互動之資訊，包含不同子系統間的溝通以及傳遞資料的特性。 *範例：與其他子系統之互動：* *（1）Subsystem_auth: 傳遞鑑別資訊給 Subsystem_auth，並由回覆訊息確認鑑別是否成功* *（2）Subsystem_terminal: ...*	

圖一、實體介面安全管控測試環境示意圖

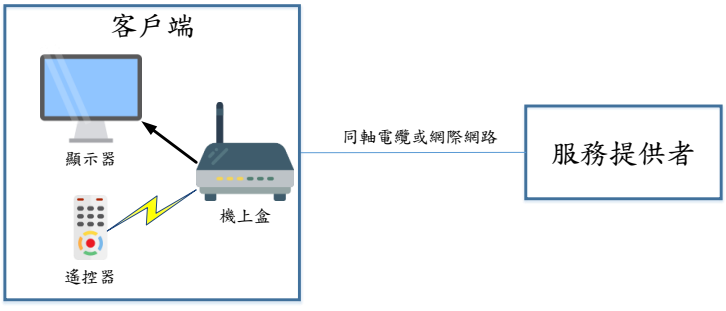


圖二、網路通訊埠安全測試環境示意圖

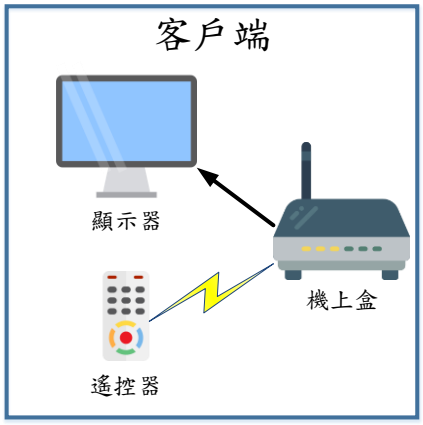
圖三、軟韌體更新測試環境示意圖



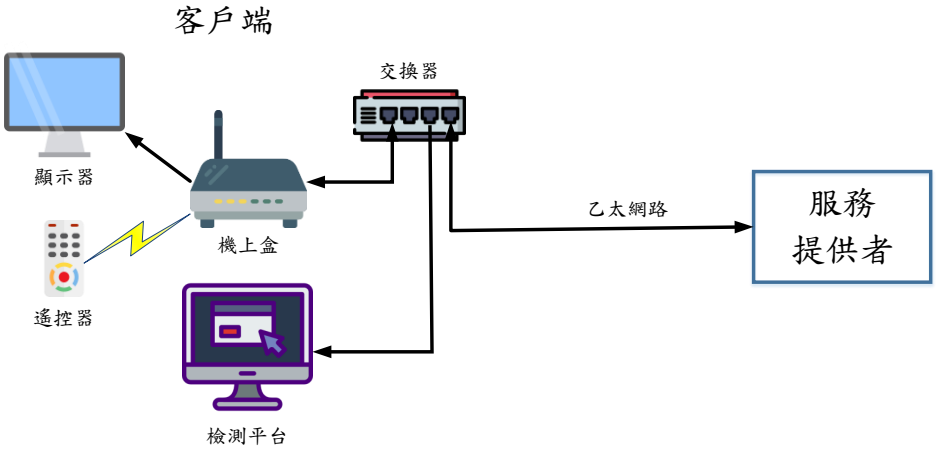
圖四、登入保密功能測試環境示意圖



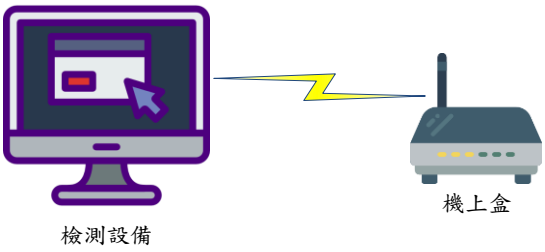
圖五、工程模式鑑別測試環境示意圖



圖六、影音傳輸保護測試環境示意圖



圖七、共通弱點評估測試環境示意圖



附錄一、實機測試項目與國際標準對照表

檢測項目	檢測細項	審查標準	參考來源	參考內容
實體安全	實體介面安全管控	本指引 7.1.1	CableLabs® Requirements CPE Security	6.1 Hardware Requirements
			影像監控系統資安標準—第一部：一般要求	5.1.1. 實體埠之安全管控
			影像監控系統資安標準—第二部：網路攝影機	5.1.1. 實體埠之安全管控
	外殼實體防護	本指引 7.1.2	Developer IoT Security Guidance	10: Poor Physical Security
			影像監控系統資安標準—第一部：一般要求	5.1.3. 實體防護
			影像監控系統資安標準—第二部：網路攝影機	5.1.3. 實體防護
系統安全	網路通訊埠安全	本指引 7.2.1	OWASP IoT Security Guidance	I3: Insecure Network Services
			影像監控系統資安標準—第一部：一般要求	5.2.2. 網路服務連接埠安全
	軟韌體更新	本指引 7.2.2	OWASP IoT Security Guidance	I9: Insecure Software/Firmware
			ONVIF Core Spec	4.5.5 Firmware Upgrade
			影像監控系統資安標準—第一部：一般要求	5.2.3.更新安全
	登入保密功能	本指引 7.2.3	Collaborative Protection Profile for Network Devices	FIA_UAU.7.1
			影像監控系統資安標準—第一部：一般要求	5.2.6. 操控程式之應用程式安全
	工程模式鑑別	本指引 7.2.4	CableLabs® Requirements CPE Security	6.4.2 Administrative Accounts/Logins
	影音傳輸保護	本指引 7.2.5	ITU-T H.721 IPTV terminal devices: Basic model	7.1.4 Interactive services
			影像監控系統資安標準—第一部：一般要求	5.5.2.1 隱私資料的傳輸機密性初階保護
Wi-Fi 通訊安全	Wi-Fi 功能登入保密	本指引 7.3.1	Collaborative Protection Profile for Network Devices	FIA_UAU.7 Protected Authentication Feedback
	Wi-Fi 功能網頁管理介面安全	本指引 7.3.2	OWASP IoT Security Guidance	I1: Insecure Web Interface
			影像監控系統資安標準—第一部：一般要求	5.2.5. 網頁管理介面安全
	共通弱點評估	本指引 7.3.3 及 7.3.4	NIST Special Publication 800-53	RA-5 VULNERABILITY SCANNING
			Collaborative Protection Profile for Network Devices	7.6 Class AVA: Vulnerability Assessment
	模糊測試	本指引 7.3.5、7.3.6 及 7.3.7	NIST Special Publication 800-53	SA-11 DEVELOPER SECURITY TESTING AND EVALUATION

檢測項目	檢測細項	審查標準	參考來源	參考內容
				(8) DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	15 Malformed Input Testing
			OWASP IoT Security Guidance	I3: Insecure Network Services
			影像監控系統資安標準—第一部：一般要求	5.3.3. Wi-Fi 通訊安全
其他功能	付費機制控管	本指引 7.4.1	行動應用 App 基本資安檢測基準	4.1.3. 交易資源控管安全
	頻道密碼管理	本指引 7.4.2	OWASP IoT Security Guidance	I2: Insufficient Authentication/Authorization
			影像監控系統資安標準—第一部：一般要求	5.4.1. 鑑別機制安全 5.4.2. 通行碼鑑別機制
			ONVIF Core Spec.	5.12.1 Authentication
	敏感性資料之存取	本指引 7.4.3	智慧型手機系統內建軟體資通安全檢測技術規範	D.1.1.B 手機系統內建軟體於存取敏感性資料前，應取得使用者同意。

附錄二、測試工具應備功能及要求說明表

檢測項目	檢測細項	測試工具	
		工具名稱	具備功能
實體安全	實體介面安全管控	USB 連接線、UART 連接線與作業系統除錯模式軟體	作業系統除錯模式軟體，透過 USB 或 UART 連接線，連接到待測物。
	外殼實體防護	不適用。	不適用。
系統安全	網路通訊埠安全	網路掃描與探測工具。	具備掃描整個子網域或主機通訊埠功能。
	軟韌體更新	不適用。	不適用。
	登入保密功能	不適用。	不適用。
	工程模式鑑別	不適用。	不適用。
	影音傳輸保護	交換器。 封包分析工具。	具備埠鏡像功能交換器。 網路封包分析軟體的功能是截取網路封包，並顯示詳細的網路封包資料功能。
Wi-Fi 通訊安全	Wi-Fi 功能登入保密	不適用。	不適用。
	Wi-Fi 功能網頁管理介面安全	網頁管理介面弱點掃瞄工具。	應至少包含 Injection 與 XSS 弱點檢測能力。
	共通弱點評估	共通弱點評估工具	至少包含 NIST 發布之 CVE 漏洞資料庫。
	模糊測試	模糊測試工具	IEEE 802.11i 標準下產生變異樣本。
其他功能	付費機制控管	不適用。	不適用。
	頻道密碼管理	不適用。	不適用。
	敏感性資料之存取	不適用。	不適用。