TAICS

TAICS TS-0041 v1.0 : 2021

無線寬頻分享器資安測試規範

Cybersecurity test specification for wireless broadband routers

2021 / 08 / 19

社團法人台灣資通產業標準協會
Taiwan Association of Informationand Communication Standards

無線寬頻分享器資安測試規範

Cybersecurity test specification for wireless broadband routers

出版日期: 2021/08/19

終審日期: 2021/06/18

誌謝

本規範由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC5 主席：神盾股份有限公司 張心玲 副總經理

TC5 副主席：財團法人資訊工業策進會 毛敬豪 資安鑄造廠總經理

TC5 副主席：財團法人電信技術中心 林炫佑 副執行長

TC5 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC5 物聯網資安工作組組長：財團法人資訊工業策進會 高傳凱 副主任

TC5 秘書：財團法人資訊工業策進會 秦燕君

技術編輯：財團法人電信技術中心 王慶豐 副主任、許博堯 副理、吳宗恩 工程師

此規範制定之協會會員參與名單為(以中文名稱順序排列)：

合勤科技股份有限公司、宏碁股份有限公司、亞太電信股份有限公司、神盾股份有限公司、財團法人資訊工業策進會、財團法人電信技術中心、華碩電腦股份有限公司

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

友訊科技股份有限公司、居易科技股份有限公司、訊舟科技股份有限公司

本規範由國家通訊傳播委員會支持研究制定。

目錄

前言

本規範係依台灣資通產業標準協會(TAICS)之規定，經技術管理委員會審定，由協會公布之產業規範。

本規範並未建議所有安全事項，使用本規範前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本規範之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

引言

現今社會的發展，對於網路的需求越來越大，隨著物聯網發展，許多設備擁有 Wi-Fi 連網功能，因此不管在哪種環境下，皆須具備 Wi-Fi 接取及路由器功能的無線寬頻分享器(以下簡稱分享器)來連接各個連網設備，在網路環境中擔任著核心角色。

然而分享器也潛藏不同資安風險，過去曾發生多起資安事件，例如在 2019 年，有網路犯罪組織侵入家庭路由器，利用路由器韌體安全漏洞，竄改域名系統(Domain Name System, DNS) 伺服器設定，將網路連線導向假的 DNS 伺服器，誘使使用者連結假網站輸入帳號密碼或其他個人資料。又如 2020 年國外資安廠商 Palo Alto 的資安研究團隊公布多項家用路由器的資安漏洞，如出廠設備所提供之網頁管理介面有命令輸入與跨站請求偽造的安全漏洞，或是其加密機制不夠完善，容易被分析破解，甚至是使用明文傳輸與儲存資料等威脅。

基於此，國家通訊傳播委員會(National Communications Commission, NCC)為確保無線寬頻分享器之安全性，委託財團法人電信技術中心(Telecom Technology Center, TTC)參考國際標準、規範與指引，在台灣資通產業標準協會(TAICS)聚集產、官、學、研，依產業標準制定程序，進行無線寬頻分享器檢測規範之制定，後續並將建立產品認驗證制度，推動無線寬頻分享器符合標準規範，以保障消費者的使用安全並協助產業提升資安能力及產品競爭力，進一步接軌國際。

1. 適用範圍

本規範規定無線寬頻分享器之資訊安全要求；其中無線寬頻分享器主要為提供網際網路和區域網路存取的服務，且具備無線射頻功能分享或接收網路之設備。

本規範適用範圍如圖 1 所示。但僅能透過有線線路分享接收網路的寬頻分享器，則不在本規範之範圍。

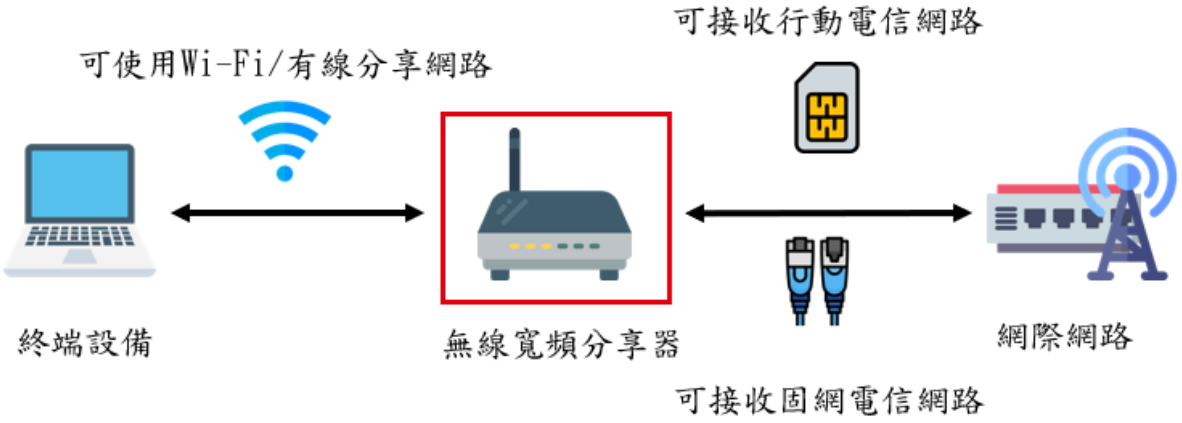

圖 1 適用範圍示意圖

2. 引用標準

下列標準因本規範所引用，成為本規範之一部分。有加註年份者，適用該年份之版次，不適用於其後之修訂版(包括補充增修)。無加註年份者，適用該最新版(包括補充增修)。

[1] Cyber Security Agency of Singapore，Cybersecurity Labelling Scheme (CLS) Minimum - Test Specifications and Methodology for Tier 4_v1.0：2020。

[2] European Telecommunications Standards Institute (ETSI)，EN 303 645 Cyber Security for Consumer Internet of Things：Baseline Requirements_v2.1.0：2020。

[3] Groupe Speciale Mobile Association (GSMA)，IoT Security Guidelines Overview Document_v2.2：2020。

[4] International Electrotechnical Commission (IEC)，62443-4-2 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components：2019。

[5] 國家通訊傳播委員會，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：2018。(本測試規範以此指引為基準，並加入近年相關的國際標準與測試規範進行修訂)

3. 用語及定義

下列用語及定義適用於本規範。

3.1 加密 (Encryption)

指明文資訊透過加密數學演算法進行改變，使改變後的資料不具可讀性，而接收端用相對應的解密數學演算法可以恢復明文資訊而達到保密的目的。

3.2 通訊埠 (Port)

通訊埠，又稱為網路埠或連接埠，內建軟體因服務需求開啟，作為連網裝置與外部傳送/接收通訊資料。

3.3 敏感性資料 (Sensitive Data)

指洩漏時導致使用者造成損害之資料，包括但不限於個人資料、通行碼、金鑰或地理位置等。此等資料依使用者行為或應用程式之運作，於裝置及其附屬儲存媒體建立、儲存或傳輸。

3.4 通行碼 (Password)

指一組字元串，能使系統辨識使用者身分，並進一步控管使用者存取系統之權限。

3.5 美國國家弱點資料庫(US National Vulnerabilities Database, NVD)

指美國國家標準暨技術研究院(US National Institute of Standards and Technology, NIST)提供的國家弱點資料庫，負責常見脆弱性與漏洞之資料的發布及更新。

3.6 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同編號。

3.7 常見漏洞評鑑系統 (Common Vulnerability Scoring System, CVSS)

指一套漏洞評鑑系統的判定標準，包括威脅所造成損害的嚴重性、資安脆弱性的可利用程度與攻擊者不當運用該脆弱性的難易度，都被列入計分。自 0 分至 10 分，0 代表無風險，而 10 則代表最高風險。

3.8 無線傳輸技術 (Wireless Transmission Technology)

指透過無線通訊標準的連接，讓分享器透過網路或點對點等連線方式來傳輸資料，分享器使用的無線傳輸技術如 Wi-Fi(Wireless Fidelity)、無線區域網路、行動通訊網路等。

3.9 無線區域網路 (Wireless Local Area Network, WLAN)

指透過無線電波、雷射光或紅外線作為傳輸資料的媒介與網路連線，其功能與有線區域網路相同。

3.10 傳輸層安全性協定 (Transport Layer Security, TLS)

指一種安全協定，為網際網路通訊提供安全及資料完整性保障。1999 年公布第一版 TLS 標準檔案。在瀏覽器、電子郵件、即時通訊、網路電話(Voice over Internet Protocol，VoIP)、網路傳真等應用程式中，廣泛支援這個協定。

3.11 機密性 (Confidentiality)

指資訊不提供或不揭露予未獲授權之個人、實體或過程的性質。

3.12 完整性 (Integrity)

指資料不會被未經授權改變或破壞的特性。

3.13 安全等級 (Security Level)

指因應產品面臨不同程度之資安威脅，針對產品所需的安全功能要求提供不同強度之分級。

3.14 HTTPS (Hypertext Transfer Protocol Secure)

指利用 SSL/TLS 加密方式，提供網頁瀏覽器安全及使用者身分鑑別之加密通訊協定。

3.15 韌體 (Firmware)

指嵌入在硬體裝置中的軟體。主要是將程式碼或資料寫入在唯讀記憶體內。

3.16 流通量 (Throughput)

指設備在固定時間內封包能成功傳遞的平均資料量，單位通常以 Mbps 或 Gbps 表示。

3.17 多因子鑑別 (Multi-Factor Authentication, MFA)

指採用 2 種以上因子的鑑別機制，以獲得裝置之存取權限。多因子鑑別依據 4 個因子，包括所知之事(something you know)、所持之物(something you have)、所具之形(something you are)、所具之行為(something you behave)，於不同階段對同一裝置進行鑑別。

3.18 強驗證 (Strong Authentication)

指使用者在登入過程中，要求使用者針對登入詢問輸入獨一無二的單次回應，或輸入由驗證伺服器提供的特殊代碼，現今驗證協議有 FIDO (Fast IDentity Online)：通用認證框架(Universal Authentication Framework, UAF)、通用第二因素框架(Universal Second Framework, U2F)與 FIDO2/WebAuthn。

3.19 負載測試 (Load Testing)

指透過模擬多個使用者連接至系統進行互動，讓系統長時間待在此條件下，查看是否能夠達到預期水準，無發生異常狀態。

4. 測試項目分級

本節依據 TAICS TS-0040 v1.0「無線寬頻分享器資安標準」制定相對應之安全測試項目與測試方法。

實機測試標準等級總表，如表 1 所示，第一欄為安全構面，包括：(1)可用性、(2)身分識別、(3)隱私加密、(4)安全功能；第二欄為安全要求分項，係依各安全構面設計對應之安全要求；第三欄為安全等級，按各安全要求分項之驗證結果，作為安全等級評估標準。

安全等級依據(1)相關資安風險高低、(2)技術實現複雜度，區分 1 級、2 級、3 級三個等級，資安風險高低指資安事件所造成的損失程度，而技術實現複雜度指攻擊實現與資安檢測的難易度。1 級安全要求所對應連網設備常見的安全問題，2 級安全要求所對應為需要工具或一定的技術能力來達成惡意攻擊，3 級安全要求所對應的資安風險屬於需要長時間布置或大量設備，造成極高的資安風險。其對應之列即其所應通過的安全要求分項，安全等級越高，其涵蓋範圍與要求也越嚴謹。

表 1 實機測試標準等級總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
5.1 可用性	5.1.1 韌體更新	5.1.1.1	5.1.1.2	
	5.1.2 Wi-Fi 模糊測試	5.1.2.1		
	5.1.3 壓力測試		5.1.3.1	
	5.1.4 堅實測試			5.1.4.1 5.1.4.2
	5.1.5 穩定測試		5.1.5.1	5.1.5.2
5.2 身分識別	5.2.1 預設通行碼	5.2.1.1	5.2.1.2	
	5.2.2 登入限制	5.2.2.1 5.2.2.2 5.2.2.3		

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
5.2 身分識別	5.2.3 通行碼	5.2.3.1	5.2.3.2	
	5.2.4 安全角色		5.2.4.1	
5.3 隱私加密	5.3.1 韌體敏感性資料	5.3.1.1		
	5.3.2 最小化通訊埠	5.3.2.1		
	5.3.3 網頁管理介面傳輸	5.3.3.1		
	5.3.4 後端傳輸			5.3.4.1
	5.3.5 Wi-Fi 傳輸		5.3.5.1	
5.4 安全功能	5.4.1 作業系統常見漏洞	5.4.1.1	5.4.1.2	
	5.4.2 韌體常見漏洞	5.4.2.1	5.4.2.2	
	5.4.3 實體埠安全			5.4.3.1
	5.4.4 日誌紀錄安全	5.4.4.1	5.4.4.2	
	5.4.5 組態設置安全	5.4.5.1	5.4.5.1	
	5.4.6 網頁管理介面常見漏洞	5.4.6.1		
	5.4.7 惡意程式測試		5.4.7.1	
	5.4.8 網路管制功能	5.4.8.1	5.4.8.2	
	5.4.9 行動網路設定	5.4.9.1		

5. 資安測試規範

檢視無線寬頻分享器之裝置設備、系統功能與傳輸通訊安全測試需求是否通過廠商送審之書面送審資料，韌體版本應於測試期間更新為最新版本，以維持服務正常使用、新增功能或安全性，測試布局如下。並依下列各測試項目進行實機測試。

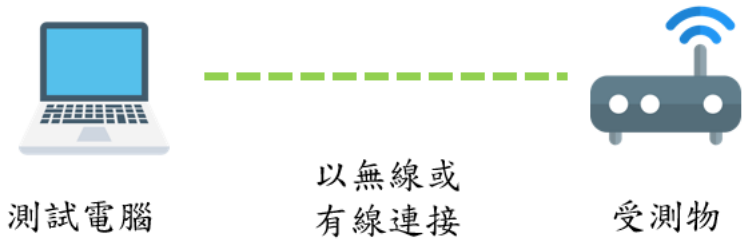

圖 2 測試布局一

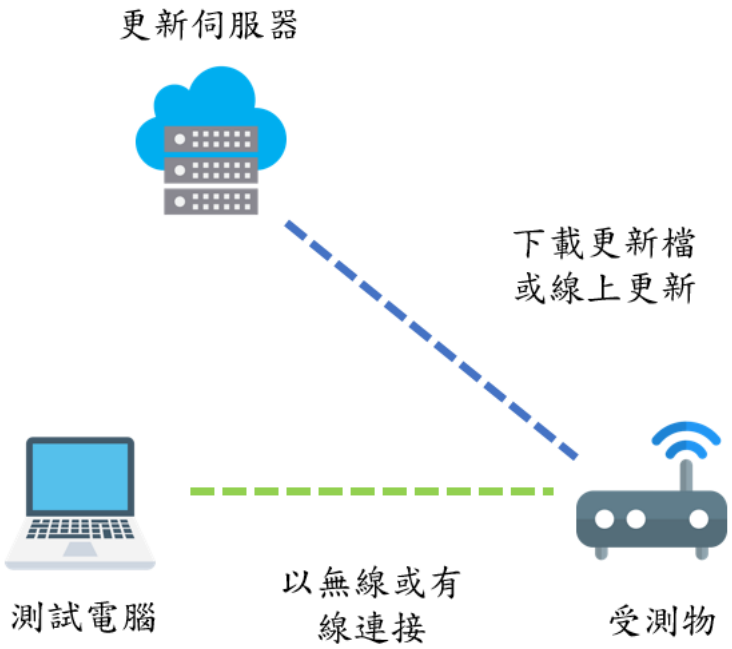

圖 3 測試布局二

圖 4 測試布局三

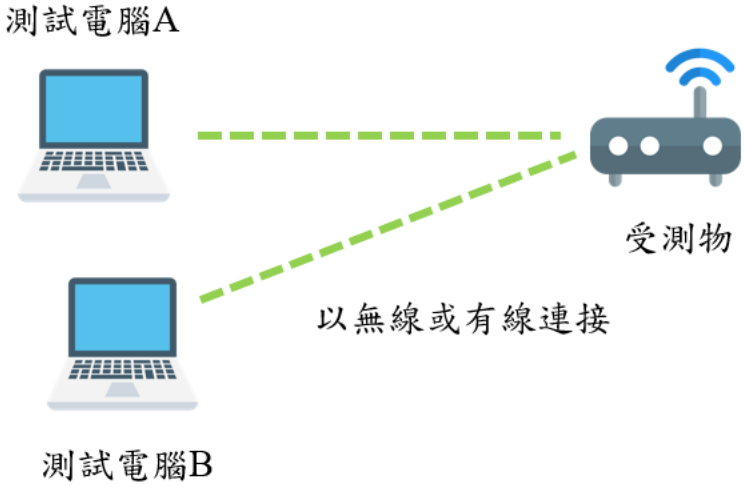

圖 5 測試布局四

5.1 可用性

5.1.1 韌體更新

5.1.1.1 韌體檔案應具有安全取得機制。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.1.1.1 節。

(b) 測試目的：

驗證線上更新或手動更新下載的韌體，取得來源是否安全或韌體完整未遭竄改。

(c) 檢測條件：

受測物具備更新功能。

(d) 測試佈局：

如
圖 3。

(e) 測試方法：

(1) 透過工具抓取線上更新封包，檢測其傳輸通道加密方式與憑證期限。

(2) 透過網站下載取得韌體，檢測是否提供相關機制來驗證韌體本身的完整性。

(f) 測試結果：

(1) 通過：測試方法(1)更新採用 TLS1.2 以上加密並憑證未過期；測試方法(2)提供的更新檔具有數位簽章。

(2) 不通過：無使用安全傳輸或憑證過期；無法驗證檔案完整性。

(3) 不適用：未具備更新功能。

5.1.1.2 分享器更新功能應具有安全防護機制。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.1.1.2 節。

(b) 測試目的：

驗證受測物更新韌體時，應檢查並拒絕更新遭受竄改的韌體或較為低版本的韌體。

(c) 檢測條件：

受測物具備手動更新功能。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 使用受測物提供之更新機制進行測試。

(2) 將舊版韌體上傳至受測物嘗試降級更新。

(3) 修改更新韌體之內容並上傳至受測物嘗試更新。

(f) 測試結果：

(1) 通過：受測物經測試方法(1)、(2)更新結果皆失敗。

(2) 不通過：受測物更新成功。

(3) 不適用：採用線上更新、未具備更新功能。

5.1.2 Wi-Fi 模糊測試

5.1.2.1 分享器 Wi-Fi 傳輸應具有抗干擾的保護機制。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.1.2.1 節。

(b) 測試目的：

驗證 Wi-Fi 傳輸接受測試樣本時，不應影響或中斷受測物服務的運行。

(c) 檢測條件：

受測物具備 Wi-Fi 熱點功能。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 使用模糊測試工具對受測物 Wi-Fi 熱點進行測試。

(2) 傳輸 1,000,000 筆隨機樣本測試，或是連續傳輸樣本測試八小時。

(f) 測試結果：

(1) 通過：受測物無中斷服務或重新啟動。

(2) 不通過：受測物中斷服務或重新啟動。

(3) 不適用：未具備 Wi-Fi 熱點功能。

5.1.3 壓力測試

5.1.3.1 分享器應能在廠商宣告的流通量定值下穩定運行。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.1.3.1 節。

(b) 測試目的：

驗證受測物的流通量達到定值時，不應影響或中斷受測物服務的運行。

(c) 檢測條件：

受測物具備 Wi-Fi 熱點功能。

(d) 測試佈局：

如圖 4。

(e) 測試方法：

(1) 使用工具對受測物傳送依 57%、7%、16%及 20%之比例混合之 64、570、594 及 1,518 位元組網路封包，並持續傳送混合後之網路封包 60 秒。

(f) 測試結果：

(1) 通過：當受測物所負荷的流通量達「附錄 A-廠商自我宣告表」中宣告的流通量定值時，應能正常運作。

(2) 不通過：受測物無任何反應或重新啟動。

(3) 不適用：未具備 Wi-Fi 熱點功能。

5.1.4 堅實測試

5.1.4.1 分享器應具有防護異常流量機制。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.1.4.1 節。

(b) 測試目的：

驗證受測物接收異常流量測試時，不應影響或中斷受測物服務的運行。

(c) 檢測條件：

受測物具備 Wi-Fi 熱點功能。

(d) 測試佈局：

如圖 4。

(e) 測試方法：

(1) 使用工具對受測物傳送以下不同類型的異常流量，持續 120 秒。

i. 802.11 鑑別氾濫式攻擊 802.11 Authenticate Flood 。

ii. 802.1x EAP-Start 氾濫式攻擊(802.1x EAP-Start Flood)。

iii. 802.1x EAP-of-Death 攻擊(802.1x EAP-of-Death)。

iv. 802.1x EAP 長度攻擊(802.1x EAP Length Attacks)。

v. 異常 Frame-Assoc 請求(Malformed Frame Associates Request)。

vi. 異常 Frame-Auth Malformed Frame Authentication)。

(f) 測試結果：

(1) 通過：當受測物所負荷的流通量達「附錄 A-廠商自我宣告表」中宣告的流通量定值時，應能正常運作。

(2) 不通過：受測物無任何反應或重新啟動。

(3) 不適用：未具備 Wi-Fi 熱點功能。

5.1.4.2 分享器應具有非正常關機恢復。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.1.4.2 節。

(b) 測試目的：

驗證受測物遭非正常關機時，是否保存原有設定。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 進入受測物網頁管理介面，觸發日誌產生事件，更改功能設定。

(2) 記錄並儲存受測物當前狀態。

(3) 受測物連線時將電源中斷，並於 1 分鐘後接上電源，重新啟動受測物。

(f) 測試結果：

(1) 通過：受測物應保留斷電前的系統設定、日誌紀錄，並恢復至正常狀態。

(2) 不通過：還原至預設設定、日誌紀錄清除，或無法正常開機使用。

(3) 不適用：無。

5.1.5 穩定測試

5.1.5.1 分享器應符合廠商宣告的 IP 資源最大配額。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.1.5.1 節。

(b) 測試目的：

驗證受測物是否符合廠商宣告可分配區域網路 IP 位址數量或範圍功能設定。

(c) 檢測條件：

受測物具備 DHCP 功能。

(d) 測試佈局：圖 4。

(e) 測試方法：

(1) 進入受測物網頁管理介面，並設定分配「附錄 A-廠商自我宣告表」中宣告的可分配區域網路使用之 IP 位址數量 X。

(2) 向受測物請求 X 個 IP 位址分配，並以網頁管理介面確認 IP 分配狀況。

(3) 向受測物請求 X+1 個 IP 位址分配，並以網頁管理介面確認 IP 分配狀況。

(4) 向受測物請求 X-1 個 IP 位址分配，並以網頁管理介面確認 IP 分配狀況。

(f) 測試結果：

(1) 通過：受測物 IP 位址分配與設置符合。

(2) 不通過：受測物 IP 位址分配與設置不符合。。

(3) 不適用：無 DHCP 功能。

5.1.5.2 分享器應能在真實環境產生的流量下穩定運行。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.1.5.2 節。

(b) 測試目的：

驗證受測物是否能穩定持續接取真實環境產生的網際網路服務之流量。

(c) 檢測條件：

受測物具備 Wi-Fi 熱點功能。

(d) 測試佈局：

如圖 4。

(e) 測試方法：

(1) 對受測物以 Wi-Fi 方式傳輸真實流量並至少持續 240 小時。

(2) 對受測物傳送真實網路之流量，網路流量樣本須符合以下要求。

i. 至少 100 組 IP 位址同時接取網際網路服務之流量。

ii. 測試流量應達受測物最大流通量 50%以上。

iii. 流量內容須涵蓋 Chat、E-Mail、File Transfer、Game、P2P、Remote Access、Streaming、Web、Network Infrastructure Services 等 9 種(含)以上類型，且每種類型應由 3 項(含)以上之應用程式或服務所組成。

(f) 測試結果：

(1) 通過：受測物在測試過程中能正常運作。

(2) 不通過：受測物傳輸中斷，或重新啟動。

(3) 不適用：未具備 Wi-Fi 熱點功能。

5.2 身分識別

5.2.1 預設通行碼

5.2.1.1 分享器不應使用通用預設通行碼。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.2.1.1 節。

(b) 測試目的：

驗證受測物提供的預設通行碼是否為通用的或是可被猜測的。

(c) 檢測條件：

受測物提供預設通行碼。

(d) 測試佈局：無。

(e) 測試方法：

(1) 檢視「附錄 A-廠商自我宣告表」提供的預設密碼，是否屬於計數型、設備資訊有關聯或使用通用常見的單字進行設計。

(f) 測試結果：

(1) 通過：預設通行碼設計模式，具有足夠隨機化。

(2) 不通過：使用特定名詞，或是可推演的預設密碼。

(3) 不適用：無預設通行碼。

5.2.1.2 分享器初始化時應強制更改預設通行碼。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.2.1.2 節。

(b) 測試目的：

驗證受測物是否初始化時強制使用者更改預設通行碼，並符合 5.2.3.1 的強度規範。

(c) 檢測條件：

受測物提供預設通行碼。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 將受測物進行初始化，並檢視其初始化流程是否強制使用者更改通行碼。

(2) 檢測更改通行碼是否符合 5.2.3.1 的強度規範。

(f) 測試結果：

(1) 通過：強制使用者更改預設通行碼，且不可跳過，並通過 5.2.3.1 規定。

(2) 不通過：未強制使用者更改預設通行碼、可跳過預設通行碼更改步驟或是不符合 5.2.3.1 規定。

(3) 不適用：無。

5.2.2 登入限制

5.2.2.1 分享器登入介面應有通行碼猜測防護機制。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.2.2.1 節。

(b) 測試目的：

驗證受測物登入介面遭受字典攻擊或暴力破解等行為時，是否具備防護機制。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 檢視「附錄 A-廠商自我宣告表」中設備登入方式。

(2) 連接登入介面(如；SSH，網頁)，並測試連續輸入錯誤的通行碼。

(f) 測試結果：

(1) 通過：登入介面具有「附錄 A-廠商自我宣告表」中宣告之登入介面防護機制。

(2) 不通過：可無限制輸入通行碼。

(3) 不適用：無。

5.2.2.2 分享器登入介面應有通行碼保密功能。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.2.2.2 節。

(b) 測試目的：

驗證受測物登入介面時，應以特殊字元遮蔽輸入之通行碼。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 檢視「附錄 A-廠商自我宣告表」中設備登入方式。

(2) 連接登入介面(如；SSH，網頁)，並檢視輸入之通行碼。

(f) 測試結果：

(1) 通過：輸入之通行碼以特殊字元遮蔽。

(2) 不通過：輸入之通行碼以明文顯示。

(3) 不適用：無。

5.2.2.3 分享器登入介面有效時間。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.2.2.3 節。

(b) 測試目的：

驗證受測物在使用者無進行任何操作時，是否靜止一段時間後，會自動進行登出動作。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 檢視「附錄 A-廠商自我宣告表」中設備登入方式。

(2) 連接登入介面(如；SSH，網頁)，並閒置超過自動鎖定或自動登出設定時間。

(f) 測試結果：

(1) 通過：受測物超過「附錄 A-廠商自我宣告表」中宣告登入介面有效時間後，應返回至登入畫面或斷開連結。

(2) 不通過：無限制登入時間。

(3) 不適用：無。

5.2.3 通行碼

5.2.3.1 分享器通行碼強度規範。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.2.3.1 節。

(b) 測試目的：

驗證通行碼長度最少應使用 10 碼，且包含特殊符號、大小寫英文或數字四種選三種字元組成。

(c) 檢測條件：

受測物使用通行碼作為身份驗證機制。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 使用受測物密碼更改功能，並輸入簡易密碼(如；1234)，進行通行碼更改。

(f) 測試結果：

(1) 通過：受測物密碼更改失敗。

(2) 不通過：受測物密碼更改成功。

(3) 不適用：不使用通行碼作為身份驗證機制。

5.2.3.2 分享器應可使用多因子或強驗證進行身分辨識。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.2.3.2 節。

(b) 測試目的：

驗證受測物是否使用多因子或強驗證機制進行使用者身份辨識。

(c) 檢測條件：

受測物具備多因子驗證、硬體或軟體 Token、公開金鑰驗證、FIDO UAF 或 U2F、FIDO2/WebAuthn 等驗證機制。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 連接至網頁管理介面，檢查受測物是否使用「附錄 A-廠商自我宣告表」中宣告之多因子或強驗證機制。

(f) 測試結果：

(1) 通過：受測物提供使用者多因子驗證之機制。

(2) 不通過：無使用多因子機制且不通過測項 5.2.3.1。

(3) 不適用：未具備多因子驗證之機制。

5.2.4 安全角色

5.2.4.1 分享器授權之角色應符合其設置權限。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.2.4.1 節。

(b) 測試目的：

驗證授權之角色應符合其權限設置，不應使用超出權限之功能。

(c) 檢測條件：

受測物具備設定相異功能及授權角色之功能。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 在受測物上建立 2 組(含)以上，具相異功能及授權之角色，如管理者、維護者。

(2) 分別登入建立之角色進行授權及非授權功能操作。

(f) 測試結果：

(1) 通過：建立之角色登入後，受測物僅能提供符合之權限功能。

(2) 不通過：受測物提供未授權之功能。

(3) 不適用：未具備建立安全角色之功能。

5.3 隱私加密

5.3.1 韌體敏感性資料

5.3.1.1 韌體不應以明文方式儲存敏感性資料。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.3.1.1 節。

(b) 測試目的：

驗證韌體不以明文方式儲存之敏感性資料，例如：通行碼、金鑰...等。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 在官網下載或請廠商提供韌體檔案。
(2) 使用韌體拆解工具，對受測物之韌體檔案進行拆解。
(3) 使用檢索工具或指令，針對敏感性資料之關鍵字詞進行搜尋，確認是否有明文之敏感性資料。

(f) 測試結果：

(1) 通過：韌體檔案無法遭工具拆解，或是無搜尋出敏感性資料。
(2) 不通過：搜尋出敏感性資料。
(3) 不適用：無。

5.3.2 最小化通訊埠

5.3.2.1 分享器應最小化開啟的通訊埠。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.3.2.1 節。

(b) 測試目的：

驗證受測物是否預設開啟不必要或未知的通訊埠。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 分別在 WAN 與 LAN 環境下使用檢測工具對通訊埠進行掃描。

(f) 測試結果：

(1) 通過：掃描結果與「附錄 A-廠商自我宣告表」中宣告的預設開啟之通訊埠一致，且在 WAN 下不得開啟遠端連線等服務。

(2) 不通過：發現開啟未知不必要的通訊埠，在 WAN 下開啟遠端連線等服務。

(3) 不適用：無。

5.3.3 網頁管理介面傳輸

5.3.3.1 分享器之網頁管理介面應強制使用 HTTPS 傳輸。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.3.3.1 節。

(b) 測試目的：

驗證受測物網頁管理介面是否強制使用 HTTPS 傳輸，且加密、解密及簽章演算法應通過金鑰演算法標準。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 使用封包側錄工具，擷取受測物使用之通訊封包，確認其於傳輸過程中使用之通道設定。

(f) 測試結果：

(1) 通過：傳輸使用 TLS 1.2 同等或以上之安全通訊協定，並符合「附錄 B–安全通道建議使用之密碼套件」中所列密碼套件。

(2) 不通過：無使用 HTTPS 傳輸或不符合核准之加密編譯演算法。

(3) 不適用：無。

5.3.4 後端通訊傳輸

5.3.4.1 分享器後端網路通訊時不應傳給廠商未宣告的 IP。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.3.4.1 節。

(b) 測試目的：

驗證傳輸給後端平台時，是否使用加密通訊協定傳輸資料，且無傳輸資料給廠商未宣告的 IP 位址。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 受測物使用 SIM 卡為網路來源，並抓取封包。

(2) 如未具備 SIM 卡為網路來源，則使用實體線路進行測試。

(3) 持續分析受測物收發之網路封包 144 小時，並分析該網路封包連接之網站或 IP 位址與傳輸的資訊。

(f) 測試結果：

(1) 通過：未發現除「附錄 A-廠商自我宣告表」中宣告允許主動連線之網站或 IP 位址外，採用加密傳輸或明文傳輸中未出現相關敏感性資料(如：IMEI、IMSI、APN 等)。

(2) 不通過：發現傳輸給未知的第三方 IP 位址或明文傳輸相關敏感性資料。

(3) 不適用：無。

5.3.5 Wi-Fi 傳輸

5.3.5.1 分享器 Wi-Fi 傳輸資料時應只使用 WPA2 AES 以上加密通訊協定傳輸資料。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.3.5.1 節。

(b) 測試目的：

驗證 Wi-Fi 傳輸應只使用 WPA2 AES 以上加密通訊協定傳輸資料。

(c) 檢測條件：

受測物具備 Wi-Fi 熱點功能。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 使用封包分析工具，檢測是否有使用 WPA2 AES 以上加密通訊協定傳輸資料。

(f) 測試結果：

(1) 通過：使用 WPA2 AES 以上加密通訊協定傳輸資料。

(2) 不通過：未使用 WPA2 AES 以上加密通訊協定傳輸資料。

(3) 不適用：未具備 Wi-Fi 熱點功能。

5.4 安全功能

5.4.1 作業系統常見漏洞

5.4.1.1 分享器作業系統不應存有 CVSS v3 9.0 分以上的已知漏洞。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.1.1 節。

(b) 測試目的：

驗證作業系統不應存有 CVSS v3 9.0 分以上的已知漏洞。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 使用弱點掃描工具對作業系統進行檢測。

(f) 測試結果：

(1) 通過：無發現 CVSS v3 評分為 9.0 以上的已知漏洞。

(2) 不通過：發現 CVSS v3 評分為 9.0 以上的已知漏洞。

(3) 不適用：無。

5.4.1.2 分享器作業系統不應存有 CVSS v3 7.0 分以上的已知漏洞。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.1.2 節。

(b) 測試目的：

驗證作業系統不應存有 CVSS v3 7.0 分以上的已知漏洞。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 使用弱點掃描工具對作業系統進行檢測。

(f) 測試結果：

(1) 通過：無發現 CVSS v3 評分為 7.0 以上的已知漏洞。

(2) 不通過：發現 CVSS v3 評分為 7.0 以上的已知漏洞。

(3) 不適用：無。

5.4.2 韌體常見漏洞

5.4.2.1 分享器韌體不應存有 CVSS v3 9.0 分以上的已知漏洞。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.2.1 節。

(b) 測試目的：

驗證韌體不應存有 CVSS v3 9.0 分以上的已知漏洞。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 在官網下載或請廠商提供韌體檔案。

(2) 使用弱點掃描工具對韌體進行檢測。

(f) 測試結果：

(1) 通過：無發現 CVSS v3 評分為 9.0 以上的已知漏洞。

(2) 不通過：發現 CVSS v3 評分為 9.0 以上的已知漏洞。

(3) 不適用：無。

5.4.2.2 分享器韌體不應存有 CVSS v3 7.0 分以上的已知漏洞。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.2.2 節。

(b) 測試目的：

驗證韌體不應存有 CVSS v3 7.0 分以上的已知漏洞。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 在官網下載或請廠商提供韌體檔案。

(2) 使用弱點掃描工具對韌體進行檢測。

(f) 測試結果：

(1) 通過：無發現 CVSS v3 評分為 7.0 以上的已知漏洞。

(2) 不通過：發現 CVSS v3 評分為 7.0 以上的已知漏洞。

(3) 不適用：無。

5.4.3 實體埠安全

5.4.3.1 分享器不得透過 UART / JTAG 介面直接進入作業系統之除錯模式。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.3.1 節。

(b) 測試目的：

驗證受測物是否可在未經授權下透過 UART / JTAG 介面進入系統除錯模式。

(c) 檢測條件：

受測物具備 UART / JTAG 介面。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 檢視「附錄 A-廠商自我宣告表」中是否使用 UART / JTAG 介面進入除錯模式。

(2) 測試電腦連接受測物之 UART / JTAG 介面。

(3) 確認是否透過 UART / JTAG 介面進入系統除錯模式。

(f) 測試結果：

(1) 通過：連接 UART / JTAG 介面無任何資訊回饋，或需進行身分驗證才可進入。

(2) 不通過：可直接進入系統除錯模式。

(3) 不適用：無使用 UART / JTAG 介面作為進入除錯模式。

5.4.4 日誌紀錄安全

5.4.4.1 分享器應提供日誌功能。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.4.1 節。

(b) 測試目的：

驗證受測物是否有提供日誌紀錄，讓使用者查詢。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 試電腦連接受測物，並進行登入動作或更改設定參數值。

(2) 觸發安全事件，檢視該筆安全事件是否被保留。

(3) 檢查是否出現敏感性資料。

(f) 測試結果：

(1) 通過：提供日誌紀錄，且無顯示敏感性資料。

(2) 不通過：無提供日誌紀錄，或顯示敏感性資料。

(3) 不適用：無。

5.4.4.2 分享器日誌紀錄之儲存空間應充足，並具備保護機制，且不應提供刪除修改功能。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.4.2 節。

(b) 測試目的：

驗證受測物應提供日誌紀錄具備容量不足的保護機制，且不應提供刪除修改功能。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 觸發事件，測試記憶容量是否因為超出而導致服務中斷。

(2) 檢測是否能對日誌紀錄進行修改或刪除。

(f) 測試結果：

(1) 通過：使用「附錄 A-廠商自我宣告表」中宣告的日誌空間儲存機制，且不可更改或刪除日誌。

(2) 不通過：無容量防護機制，或可對日誌進行更改刪除動作。

(3) 不適用：無。

5.4.5 組態設置安全

5.4.5.1 分享器應提供手動關閉服務之功能。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.5.1 節。

(b) 測試目的：

驗證受測物是否提供使用者開關服務之功能。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 進入受測物網頁管理介面查看是否提供 WPS、UPnP、HNAP、NAT-PMP 或遠端連線等服務開關功能。

(f) 測試結果：

(1) 通過：提供開關功能。

(2) 不通過：無提供開關功能。

(3) 不適用：無。

5.4.5.2 分享器應預設關閉高風險服務。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.5.2 節。

(b) 測試目的：

驗證受測物應預設關閉高風險服務。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 使用工具掃描受測物是否開啟 WPS、UPnP、HNAP、NAT-PMP 或遠端連線等服務。

(f) 測試結果：

(1) 通過：無開啟服務。

(2) 不通過：無預設關閉服務。

(3) 不適用：無。

5.4.6 網頁常見漏洞

5.4.6.1 分享器網頁管理介面不應存有已知 OWASP TOP 10 弱點或其它高危險弱點。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.6.1 節。

(b) 測試目的：

驗證網頁管理介面是否存有重大已知漏洞。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：。

(1) 使用弱點掃描工具對受測物網頁管理介面進行檢測。

(f) 測試結果：

(1) 通過：網頁管理介面不存在 OWASP TOP 10 弱點或其它高危險弱點。

(2) 不通過：網頁管理介面存在 OWASP TOP 10 弱點或其它高危險弱點。

(3) 不適用：無。

5.4.7 惡意程式測試

5.4.7.1 分享器韌體不應存有惡意程式。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.7.1 節。

(b) 測試目的：

驗證受測物韌體是否存有惡意程式。

(c) 檢測條件：

無。

(d) 測試佈局：

如圖 2。

(e) 測試方法：。

(1) 在官網下載或請廠商提供韌體檔案。

(2) 使用一套(含)以上防毒軟體完整掃描韌體，掃描前應更新至最新病毒碼，且必須符合以下要求。

i. 資安測試機構 AV-Test 最近一年測試結果，防護分數達 5.5 分以上。

ii. 資安測試機構 AV-Comparatives 最近一年測試結果，Malware Protection Tests 取的 Advanced+(三星)等級。

(f) 測試結果：

(1) 通過：韌體不存在惡意程式(如：病毒、蠕蟲、特洛伊病毒、邏輯炸彈、間諜軟體、廣告程式及後門程式等)。

(2) 不通過：韌體存在惡意程式。

(3) 不適用：無。

5.4.8 網路管制功能

5.4.8.1 分享器應符合所設定網際網路管制之功能。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.8.1 節。

(b) 測試目的：

驗證受測物是否具備網際網路管制功能，限制 IP 連接至網際網路。

(c) 檢測條件：

受測物具備路由功能。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 登入受測物之網頁管理介面，開啟受測物網際網路管制功能(如:家長管理)。

(2) 設定連接設備無法連線至網際網路。

(f) 測試結果：

(1) 通過：連接設備無法連線至網際網路。

(2) 不通過：連接設備可連線至網際網路。

(3) 不適用：未具備路由功能。

5.4.8.2 分享器應符合所設定區域網路管制之功能。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.8.2 節。

(b) 測試目的：

驗證受測物是否具備區域網路管制功能，分隔多個區域網路。

(c) 檢測條件：

受測物具備路由功能。

(d) 測試佈局：

如圖 2。

(e) 測試方法：。

(1) 登入受測物之網頁管理介面，開啟受測物區域網路管制功能(如:訪客網路)。

(2) 設定連接設備無法連線至主區域網路。

(f) 測試結果：

(1) 通過：連接設備無法連線至主區域網路，無法登入管理介面。

(2) 不通過：接設備可連線至主區域網路，可登入管理介面。

(3) 不適用：未具備路由功能。

5.4.9 行動網路設定

5.4.9.1 分享器應提供限制接取行動網路類型之功能。

(a) 測試依據：

TAICS TS-0040 v1.0「無線寬頻分享器資安標準」第 5.4.9.1 節。

(b) 測試目的：

驗證受測物是否提供限制接取行動網路之功能，防止接取 3G 以下之行動網路。

(c) 檢測條件：

受測物具備行動網路設定功能。

(d) 測試佈局：

如圖 4。

(e) 測試方法：

(1) 登入受測物之網頁管理介面，更改接取的行動網路類型。

(2) 使用工具提供 2G/3G 行動網路，讓受測物連接。

(f) 測試結果：

(1) 通過：受測物無法連接至 2G/3G 行動網路。

(2) 不通過：受測物可連接至 2G/3G 行動網路。

(3) 不適用：無提供行動網路設定功能。

附錄 A
(參考)
廠商自我宣告表

設備識別		
設備名稱		
廠牌		
型號		
申請者 (公司、商號名稱)	製造商 ☐ 進口商 ☐ 經銷商 ☐	
製造商		
韌體版本		
預設開啟之通訊埠		
允許主動連線之網站或 IP 位址		
流通量額定值		
可分配區域網路使用之 IP 位址數量與範圍		

安全功能需求	
日誌空間容量	請提供可儲存之容量大小或筆數
日誌空間儲存機制	請提供使用何種方式以確保日誌紀錄儲存功能。
韌體更新方式	請列出有幾種方式可以進行韌體更新。
登入介面防護機制	請提供使用何種方式來防護暴力攻擊。
登入介面有效時間	請提供預設多長時間會斷開登入。(網頁管理介面或遠端登入)
預設通行碼	請說明預設通行碼產生的方式，並提供範例至少十組。
多因子或強驗證身分辨識	請提供使用的多因子或強驗證身分辨識。
除錯模式	請列出進入除錯模式的方法。
設備登入方式	請列出連接設備的方式，如遠端、網頁管理介面，以及其驗證機制。
設備是否有隱藏帳號	請說明是否有除錯或預設帳號，並說明其通行碼強度是否符合本規範要求。
問題回報	請列出可與廠商回報問題的連絡方式。
設備型號標籤	請說明設備外觀上何處可以取得此資訊。
設備支援日期	請說明可在何處讓使用者知道設備支援日期。
設備漏洞更新的機制	請說明如何讓使用者知道漏洞，且說明更新機制。
資料回傳	請說明是否回傳網路資料或遙測資料以及其用途，列出對應回傳的網址與 IP。
通訊加密	請列出所使用有關通訊的加密技術、演算法。

附錄 B
(參考)
安全通道建議使用之密碼套件

安全通道(TLS)所選用的密碼套件應遵循下述幾項要求：

- TLSv1.2
  - TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
  - TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES256_SHA384
  - TLS_ECDHE_RSA_WITH_AES256_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES128_SHA256
  - TLS_ECDHE_RSA_WITH_AES128_SHA256

- TLSv1.3
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_SHA256
  - TLS_AES_128_CCM_8_SHA256

參考資料

(1) NIST，Special Publication 800-187 Guide to LTE Security。
(2) RFC 5246，The Transport Layer Security (TLS) Protocol Version 1.2。
(3) NIST FIPS PUB 140-2，Security Requirements For Cryptographic Modules：2001。
(4) ETSI，Cyber Security for Consumer Internet of Things TS 103 645 Version 1.1.1：2019。
(5) ISO/IEC 1540，共同準則(Common Criteria for Information Technology Security Evaluation, CC)。
(6) ENISA，Recommended cryptographic measures-Securing personal data。
(7) SANS，Security Guidelines for Wireless LAN Implementation。
(8) CSA，Cybersecurity Labelling Scheme (CLS) Minimum - Pub 2 Scheme Specifications v1:2020。
(9) CSA，Cybersecurity Labelling Scheme (CLS) Minimum - Pub 1 Overview of CLS v1：2020。
(10) OWASP，Internet of Things TOP 10：2018。
(11) OWASP，Internet of Things TOP 10：2014。
(12) NIAP，Collaborative Protection Profile for Network Devices_v2.0：2017。
(13) UL，2900-1 Standard for Software Cybersecurity for Network-Connectable Products Part 1: General Requirements。
(14) ENISA，Cybersecurity Certification: EUCC Candidate Scheme v1：2020。
(15) EU，General Data Protection Regulation：2016。
(16) I EC 62443-4-1 Security for industrial automation and control systems –Part 4-1: Secure product development lifecycle requirements：2018。
(17) ISO/IEC 17025，General requirements for the competence of testing and calibration laboratories：2017

版本修改紀錄

版本	時間	摘要
v1.0	2021/08/19	出版

地　址・台北市中正區北平東路30-2號6樓
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw