TAICS

TAICS TS-0040 v1.0 : 2021

無線寬頻分享器資安標準

Cybersecurity standard 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標準

Cybersecurity standard for wireless broadband routers

出版日期: 2021/08/19

終審日期: 2021/07/26

誌謝

本標準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

此標準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

本標準由國家通訊傳播委員會支持研究制定。

目錄

前言

本標準係依台灣資通產業標準協會(TAICS)之規定，經理事會審定，由協會公布之產業標準。

本標準並未建議所有安全事項，使用本標準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。

本標準之部分內容，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資安標準之制定，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

本標準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。

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

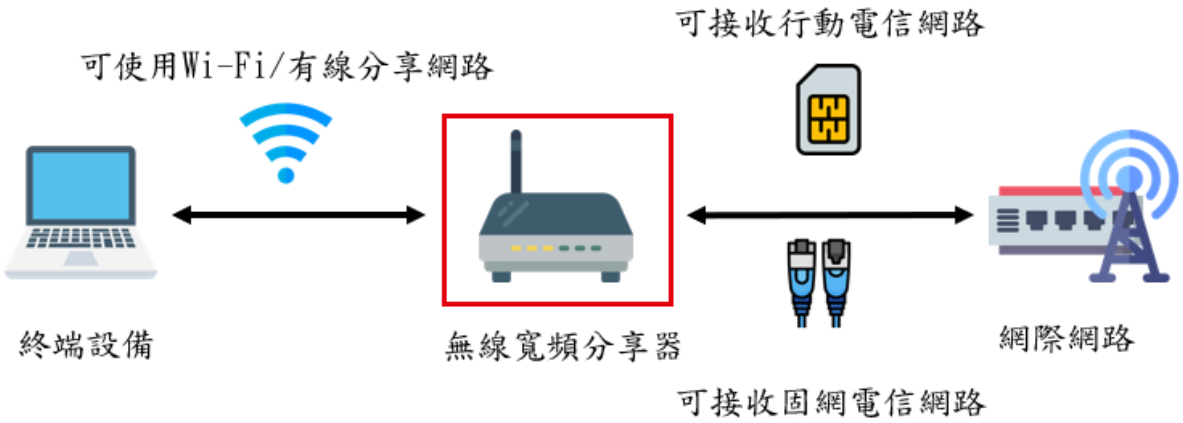

圖 1 適用範圍示意圖

2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。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。

3. 用語及定義

下列用語及定義適用於本標準。

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. 安全等級

安全等級係為降低或消弭產品之資訊安全威脅，透過最適之安全組合，確保產品達到安全之要求。本標準安全等級 1、2、3 分別對應至「無線寬頻分享器資安測試規範」安全等級 1、2、3，各安全等級之安全要求。

4.1 安全等級概述

4.1.1 安全等級說明

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符合的安全要求分項，安全等級越高，其涵蓋範圍與要求也越嚴謹。

4.1.2 安全構面

(a) 可用性：主要包含分享器無線傳輸技術及通訊協定等安全要求，並確保功能服務提供的穩定性。

(b) 身分識別：主要包含分享器對於通行碼設定、登入介面的防護機制與使用權限的安全要求。

(c) 隱私加密：主要包含分享器資料的保護，在傳輸通訊的資料，或是儲存在設備上敏感性資料的加密機制。

(d) 安全功能：主要包含分享器的安全機制，預設的功能設定、本身系統的已知弱點或使用不安全的第三方套件。

4.1.3 安全要求分項

依安全構面所設計對應之安全要求要項，且每一安全要求分項包含一個以上之安全要求，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。本安全等級總表各欄的關連性，須依循下節 5.1 至 5.4 之技術規範內容。

表 1 安全等級總表

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 身分識別安全	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		
	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	

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
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	5.4.5.2	
	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 流量管制功能	5.4.8.1	5.4.8.2	
	5.4.9 行動網路設定	5.4.9.1		

5. 標準規範

本節詳盡載明無線寬頻分享器可用性、身分識別、隱私加密、安全功能應採取的共通方法，所有無線寬頻分享器應符合本節中所有安全要求。

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。

5.1.1.2 分享器更新功能應具有安全防護機制。

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。

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。

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。

5.1.4.2 分享器應具有非正常關機恢復。

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。

5.1.5.2 分享器應能在真實環境產生的流量下穩定運行。

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。

5.2.1.2 分享器初始化時應強制更改預設通行碼。

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。

5.2.2.2 分享器登入介面應有通行碼保密功能。

5.2.2.3 分享器登入介面有效時間。

5.2.3 通行碼

5.2.3.1 分享器通行碼強度規範。

5.2.3.2 分享器應可使用多因子或強驗證進行身分辨識。

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。

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。

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。

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。

5.3.4 後端傳輸

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。

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。

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。

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。

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。

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。

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。

5.4.4 日誌紀錄安全

5.4.4.1 分享器應提供日誌功能。

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。

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。

5.4.5.2 分享器應預設關閉高風險服務。

5.4.6 網頁管理介面常見漏洞

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。

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。

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。

5.4.8.2 分享器應符合所設定區域網路管制之功能。

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。

附錄 A
(參考)
標準規範要求事項與各標準規範對照表

表 A.1 標準規範要求事項與各標準規範對照表

資安脆弱性	本標準要求事項	參考或對應標準規範
缺乏更新機制	5.1.1	● ETSI EN 303 645 ➢ 5.3: Keep Software updated
協定弱點	5.1.2	● 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 ➢ 模糊測試 7.5.4、7.5.5、7.5.6
設備穩定性	5.1.3	● 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 ➢ 流通量 7.2.1
設備穩定性	5.1.4	● 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 ➢ 異常流量 7.3.1
弱密碼	5.2.1	● ETSI EN 303 645 ➢ 5.1 No universal default passwords
弱密碼	5.2.2	● ETSI EN 303 645 ➢ 5.1 No universal default passwords
弱密碼	5.2.3	● CLS Minimum Test Specification ➢ To ensure that the wireless router employs a strong password policy.
權限控管	5.2.4	● 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 ➢ 安全角色 7.1.11
明文儲存	5.3.1	● CLS Minimum Test Specification ➢ To ensure that the device (including the manufacturer's website) shall not allow an attacker

		to retrieve sensitive credentials and contents from its firmware (i.e. secure storage).
不安全通訊埠	5.3.2	● ETSI EN 303 645 ➢ 5.6 Minimize exposed attack surfaces
明文傳輸	5.3.3	● CLS Minimum Test Specification ➢ To ensure that the device communicates in a secure manner with associated cloud services over the internet, configuration portal, and the companion mobile application.
明文傳輸	5.3.4	● 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 ➢ 動態分析 7.5.7
不安全加密協定	5.3.5	● CLS Minimum Test Specification ➢ Default communication settings should be secured. For example, routers should employ WPA2-PSK-AES-CGM on its wireless interface
潛在弱點	5.4.1	● 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 ➢ 共通弱點評估 7.5.1 7.5.2
潛在弱點	5.4.2	● 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 ➢ 惡意程式測試 7.5.3
實體介面	5.4.3	● CLS Minimum Test Specification ➢ To ensure that the device does not have hardware ports such as JTAG or UART
缺乏事件紀錄	5.4.4	● 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 ➢ 事件紀錄產出 7.1.1
不安全配置	5.4.5	● CLS Minimum Test Specification ➢ To ensure that the wireless router disables the following services by default.
網頁弱點	5.4.6	● CLS Minimum Test Specification

		➢ To ensure that the device's configuration portal is not susceptible to command injection attacks.
惡意程式	5.4.7	● 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 ➢ 惡意程式測試 7.5.3
不安全配置	5.4.8	● 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 ➢ 網際網路流量管制功能 7.1.13 ● CLS Minimum Test Specification ➢ To ensure that the Guest WLAN does not allow access to the configuration portal of the device, or to other devices in the main private-WLAN.
不安全配置	5.4.9	● Guide to LTE Security ➢ 5.4 User-Defined Option for Connecting to LTE Networks

附錄 B
(參考)
風險來源分析與資安需求

無線寬頻分享器近年來發生多起資安威脅與攻擊案例，在可用性、身分識別、隱私加密與安全功能構面分析風險來源並提出防護對策，由威脅目標與攻擊技術制定安全等級與標準規範，風險來源分析與資安需求分析表，如表 B.1 所示。

表 B.1 風險來源分析與資安需求分析表

威脅描述	威脅目標	攻擊技術	防護對策	安全構面
明文儲存	敏感性資料	資料探索	加密	隱私加密
	參考來源： OWASP IoT top 10 2018 - Insecure Data Transfer and Storage			
潛在弱點	作業系統	漏洞利用	漏洞修補	安全性
	參考來源： OWASP IoT TOP 10 2014 - Insecure Software/Firmware			
明文傳輸	敏感性資料	中間人攻擊	加密通道	隱私加密
	參考來源： OWASP IoT TOP10 2018 - Insecure Data Transfer and Storage			
弱密碼	敏感性資料、使用者權限	暴力破解	提高複雜度	身分辨識
	參考來源： OWASP IoT top 10 2018 - Weak Guessable, or Hardcoded Passwords			
不安全配置	服務功能	請求偽造	預設關閉	安全性
	參考來源： OWASP IoT top 10 2018 - Insecure Default Settings			
實體介面	敏感性資料、作業系統	資料竄改	身分鑑別	安全性
	參考來源： OWASP IoT top 10 2018 - Lack of Physical Hardening			
網頁弱點	網頁配置	重送攻擊	登出時清除 Cookie	安全性
	參考來源： OWASP IoT top 10 2014 - Insecure Web Interface			
弱密碼	使用者權限	暴力破解	封鎖攻擊 IP	身分辨識
	參考來源： OWASP IoT top 10 2018 - Weak Guessable, or Hardcoded Passwords			
權限控管	使用者權限	竄改設定	確保權限設定	身分辨識
	參考來源： OWASP IoT TOP 10 2014 - Insufficient Authentication/Authorization			

不安全通訊埠	作業系統	暴力破解	關閉不必要通訊埠	隱私加密
	參考來源： OWASP IoT top 10 2018 - Insecure Network Services			
缺乏更新機制	作業系統	漏洞利用	提供更新機制	可用性
	參考來源： OWASP IoT top 10 2018 - Lack of Secure Update Mechanism			
不安全加密協定	傳輸資訊	中間人攻擊	使用更安全的協定	隱私加密
	參考來源： OWASP IoT top 10 2014 - Lack of Transport Encryption			

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 15408，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) IEC 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