TAICS

TAICS TS-0050 v1.0 : 2022

數據機資安測試規範

Cybersecurity test specification for modem

2022/09/15

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

數據機資安測試規範

Cybersecurity test specification for modem

出版日期: 2022/09/15

終審日期: 2022/06/17

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。

TC 主席：神盾股份有限公司 張心玲 副總經理

TC 副主席：財團法人電信技術中心 林炫佑 副執行長

TC 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC 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

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、張彥威 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)：

中華資安國際股份有限公司、中華電信股份有限公司、合勤科技股份有限公司、安華聯網科技股份有限公司、亞旭電腦股份有限公司、神盾股份有限公司、財團法人工業技術研究院、財團法人台灣商品檢測驗證中心、財團法人資訊工業策進會、財團法人電信技術中心、國立陽明交通大學、智邦科技股份有限公司、智易科技股份有限公司、遠傳電信股份有限公司

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

國立雲林科技大學、凱擘股份有限公司

本規範由國家通訊傳播委員會支持研究制定

目錄

前言

本規範依據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

數據機(Modem) 泛指對通信設備所傳輸訊號進行調變或解調的設備，能於傳送時將資料處理設備相容的資料形式調變為與傳輸設備相容的資料形式，且於接收時進行反向的解調轉換。常見的數據機包含固網數據機(xDSL、撥接上網等方式)、行動連網裝置(4G/5G/Wi-Fi 等方式)等等，可將無線電波、光纖網路/電纜線脈衝訊號，經由 modem 轉化為數位訊號，提供與數據機串接的路由器、閘道、行動裝置等連網裝置，連接成彼此能互相通信的網路。

數據機也成為常見的惡意網路攻擊媒介與破口，駭客除了對數據機發動攻擊或攔截訊號以外，也會盜取或側錄與數據機串接的內網連網裝置關鍵資料及參數，造成對數據機本身架構安全性，甚至是數據機與連網裝置持有者隱私的衝擊，例如 CVE-2019-13411 便發現數據機在 3097 埠可以遠端執行任意指令，CVE-2019-13412 則可以利用來讀取任意文件，CVE-2019-15064 則可以讓攻擊者無需任何身分驗證即可登錄設備，CVE-2019-15065 則可以允許攻擊者在 6998 埠上執行特定命令來讀取內容。

本規範制定之目的為增進數據機安全功能，並導入資安防護設計概念與技術，保障數據機運作安全性與資料完整性。

1. 適用範圍

本規範規定數據機之資訊安全要求。數據機(modem)為連接使用者終端設備至 ISP 業者間之提供上網功能設備，如圖 1 所示。本規範之適用範圍為數據機本體，包括硬體、韌體、輸出入介面、傳輸協定等，與圖 2 所示。

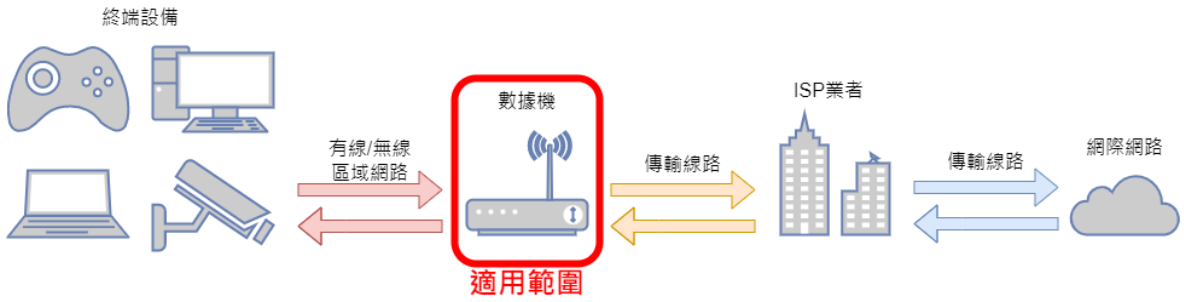

圖 1 適用範圍示意圖

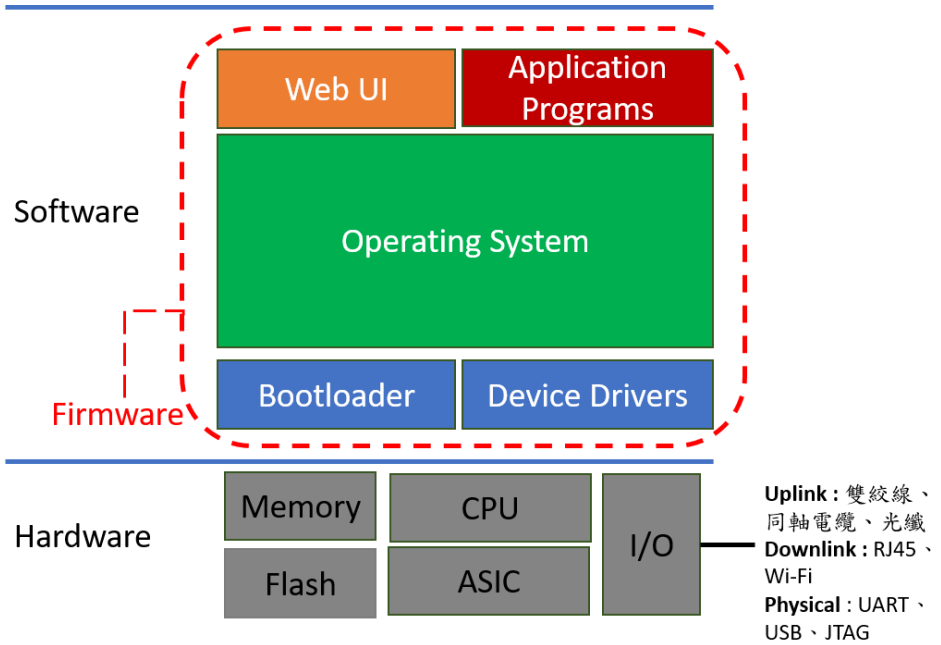

圖 2 數據機架構示意圖

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] TAICS TS-0049 v1.0 數據機資安標準

[2] NIST SP 800-140C, CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759

[3] NIST Special Publication 800-92, Guide to Computer Security Log Management

[4] TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範

3. 用語及定義

下列用語與定義適用於本規範。

3.1 數據機

數據機為 Modulator（調變器）與 Demodulator（解調器）的簡稱，對通信設備所傳輸訊號進行調變或解調的設備，能將與資料處理設備相容的資料形式轉換為與傳輸設備相容的資料形式，或進行相反的轉換。

3.2 安全事件

安全事件泛指與系統操作以及系統異常之事件紀錄，包括管理介面及系統之登入、登出、修改通行碼及設定、異常狀況等。

3.3 日誌輪替(Log Rotate)

日誌輪替是指系統管理中一個自動化歸檔過期日誌文件的過程，其中包含日誌的分割與轉存，每當產生新的事件紀錄時，將會以其設計之時間、空間、存取位置及輪轉條件參數進行日誌文件管理，如日誌紀錄新增過程達到時間或空間參數條件時，將進行日誌分割，舊日誌文件名後面的數字即會增加，並依據存取位置進行儲存，若已滿足輪轉條件時，日誌可依據其設計方式進行刪除或者轉存到他處來釋放儲存空間以達成一次日誌輪替。日誌輪替提供了一個有效的方法來限制日誌文件的大小，同時保留近期的日誌用於分析。

3.4 國家弱點資料庫(National Vulnerabilities Database, NVD)

指美國國家標準技術研究所(National Institute of Standards and Technology, NIST)提供的美國國家弱點資料庫，負責常見弱點與漏洞(如 3.5 所述)之資料的發布及更新。

3.5 常見弱點與漏洞(Common Vulnerabilities and Exposures, CVE)

由美國國土安全部贊助之弱點管理計畫，針對每一弱點項目給予全球認可之唯一共通編號。

3.6 通用漏洞評分系統(Common Vulnerability Scoring System, CVSS)

由資安事件應變小組論壇(Forum of Incident Response and Security Teams, FIRST) 提供的漏洞評分系統，以衡量軟體漏洞的特徵和嚴重性進行評分。

3.7 管理者(Administrator)

具更改作業系統、控制介面、功能應用程式之權限人員，如維修人員、設備管理者。

3.8 加密(Encryption)

指為了避免資訊的洩漏，明文資訊透過數學演算法進行改變，使原來的明文資訊變成不可直接識別其原始之資訊，從而達到保密之目的。

3.9 安全通道(Security Tunnel)

為網際網路通訊端點與端點(End-to-End)間，並達到資料隱密性及完整性所建立之通道，如：目前常見之實作安全套接層協定 (Secure Sockets Layer, SSL)和傳輸層安全性協定(Transport Layer Security, TLS)。

3.10 敏感性資料(Sensitive Data)

指洩漏時可能對使用者造成損害之資料，不限但至少包含個人資料、通行碼、金鑰或地理位置等。此等資料依使用者行為或行動應用程式之運作，於裝置及其附屬儲存媒體建立、儲存或傳輸。

3.11 遠端連線(Remote Control)

提供使用者可透過網路連線的方式，在網路另一端連接到提供服務的軟體或硬體設備。

3.12 身分鑑別(User Authentication)

一種電腦存取控制之方法，允許軟體與設備用以鑑別使用者身分之機制，並可防止未經授權之用戶存取敏感性資料之關鍵步驟。藉由通行碼、生物特徵、智慧卡…等身分鑑別機制可用以判別使用者是否為合法使用者。

3.13 通用平台枚舉(Common Platform Enumeration, CPE)

CPE 是資訊系統、軟體和軟體套件的結構化命名方式。基於統一資源標識符(URI) 的通用語法，CPE 包括正式名稱格式、用於根據系統檢查名稱的方法以及用於將文本和測試綁定到名稱的描述格式，並由美國國家弱點資料庫(NVD)平台提供已紀錄之 CPE 字典檔案及基本查詢服務。

3.14 軟體物料清單(Software Bill of Materials, SBOM)

軟體物料清單（SBOM）為軟體組件成分列表，透過提高軟體透明度，以進行軟體安全和軟體供應鏈風險管理。

3.15 通行碼

通行碼為密碼、暗號、通行字，是一種用於身分驗證的保密字符串，以達到保護隱私及防止未經授權的操作。

4. 測試項目分級

本節依據 TAICS TS-0049 v1.0 數據機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，第一欄為安全測試構面，包括：(1)實體安全、(2)韌體安全及更新、(3)系統安全、(4)傳輸通訊安全、(5)身分鑑別機制安全、(6)網頁服務安全、(7)日誌紀錄安全；第二欄為安全測試項目，係依第一欄安全測試構面設計對應之安全測試項目；第三欄為安全等級之測試標準，按各安全測試項目所做之測試標準，評估安全等級。

安全等級依相關資安風險高低，分為 1 級、2 級、3 級三個等級。1 級適用於供消費者使用之受測物；2 級適用於企業或工廠使用之受測物；3 級適用於政府單位或關鍵基礎設施使用之受測物。受測物須先通過初階安全等級之測試，始可進行高階等級之測試。

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 實體安全	5.1.1 實體埠安全管控	5.1.1.1*	-	-
5.2 韌體安全及更新	5.2.1 韌體更新	5.2.1.1*	5.2.1.2	-
	5.2.2 韌體更新檔之真確性與完整性	5.2.2.1*	-	-
	5.2.3 韌體傾印(Dump)之敏感性資料	-	-	5.2.3.1
5.3 系統安全	5.3.1 作業系統與網路服務重大資安風險之漏洞	5.3.1.1	5.3.1.2	5.3.1.3
	5.3.2 最小化網路服務連接埠	5.3.2.1*	-	-
	5.3.3 敏感性資料之儲存加密	5.3.3.1*	-	-
	5.3.4 安全晶片之儲存保護聲明	-	-	5.3.4.1*
	5.3.5 遠端連線服務安全性	5.3.5.1*	-	-
5.4 傳輸通訊安全	5.4.1 網頁管理介面之傳輸安全	5.4.1.1*	-	-
	5.4.2 儲存媒體共用模式之傳輸安全	5.4.2.1	-	-
	5.4.3 Wi-Fi 傳輸安全	5.4.3.1*	-	-
	5.4.4 安全的 Wi-Fi 組態設置	5.4.4.1	-	-
	5.4.5 安全的數據機組態設置	5.4.5.1	-	5.4.5.2
5.5 身分鑑別機制安全	5.5.1 會話安全性	5.5.1.1	-	-
	5.5.2 檔案共享功能之權限控管機制	5.5.2.1	-	-
	5.5.3 預設通行碼安全性	5.5.3.1*	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
	5.5.4 通行碼鑑別機制強度	5.5.4.1	-	-
	5.5.5 通行碼的輸入頻率及次數限制	5.5.5.1*	-	-
5.6 網頁服務安全	5.6.1 管理者登入會話有效時間	5.6.1.1	-	-
	5.6.2 網頁管理介面重大資安風險之漏洞	5.6.2.1	5.6.2.2	5.6.2.3
	5.6.3 應用程式重送攻擊安全測試	-	-	5.6.3.1*
	5.6.4 設備設定檔內容之敏感性資料與權限管理	5.6.4.1*	-	-
5.7 日誌紀錄安全	5.7.1 安全事件日誌	5.7.1.1	5.7.1.2	-
	5.7.2 日誌內容之敏感性資料	5.7.2.1	-	-
	5.7.3 日誌輪替功能	5.7.3.1	5.7.3.2	5.7.3.3

註：以上項目編號標示*字樣者，為參考 TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範。

5. 資安測試規範

5.1 實體安全

檢視數據機之實體安全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。

5.1.1 實體埠安全管控

5.1.1.1 實體埠之安全管控測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.1.1.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.1.1.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.2.2.4

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物是否可透過受測物實體連接介面，直接存取作業系統之除錯模式。

(e) 測試條件：

(1) 受測物須保持出廠預設環境狀態。

(2) 受測物須於文件中說明所有進入作業系統除錯模式之方法。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 根據廠商設備自我宣告表(附錄 B)所提供進入作業系統除錯模式之方法，開啟相應之管理介面連接工具。

(2) 測試電腦連接受測物之 USB / UART / JTAG 介面。

(3) 確認可否透過 USB / UART / JTAG 埠存取作業系統之除錯模式。

(4) 若存取前須經通行碼鑑別程序，則檢視通行碼鑑別是否符合 5.5.4 通行碼鑑別機制須具備之複雜度及強度測試的要求。

(h) 判定標準：

(1) 受測物無法透過 USB/UART/JTAG 介面存取作業系統之除錯模式。

(2) 受測物存取除錯模式須經過身分鑑別，且通行碼鑑別符合 5.5.4 通行碼鑑別機制須具備之複雜度及強度測試的要求。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)兩項結果符合其中一項。

(2) 不通過：判定標準(1)、(2)兩項結果皆不符合。

(3) 不適用：無。

5.2 韌體安全及更新

檢視數據機之韌體安全及更新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。

5.2.1 韌體更新

5.2.1.1 韌體更新測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.2.1.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.3.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物韌體是否具備更新機制。

(e) 測試條件：

(1) 廠商須提供韌體更新方法的說明。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 依據廠商使用說明文件中所提供之韌體安全性更新方法進行更新，或請廠商觸發更新。

(2) 檢視受測物是否能進行更新。

(h) 判定標準：

(1) 受測物之韌體可更新。

(i) 判定結果：

(1) 通過：判定標準(1)結果符合。

(2) 不通過：判定標準(1)結果不符合。

(3) 不適用：無。

5.2.1.2 韌體更新失敗復原測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.2.1.2

(b) 安全等級：

2 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗產品韌體更新失敗時，產品具備系統能回復更新前正常運作之能力。

(e) 測試條件：

(1) 廠商須提供韌體更新方法的說明。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 依據廠商使用說明文件中所提供之韌體安全性更新方法，或請廠商觸發更新。

(2) 檢視受測物是否能進行更新。

(3) 於更新過程中(非檔案下載階段)，觸發更新中斷，檢視受測物是否回復至更新前之狀態。

(h) 判定標準：

(1) 受測物若更新失敗，仍可回復至更新版本前之狀態。

(i) 判定結果：

(1) 通過：判定標準(1)結果符合。

(2) 不通過：判定標準(1)結果不符合。

(3) 不適用：無。

5.2.2 韌體更新檔之真確性與完整性

5.2.2.1 韌體真確性與完整性測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.2.2.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.3.1.9

(b) 安全等級：

1 級。

(c) 測試資料：

韌體更新檔。

(d) 測試目的：

查驗受測物是否具備確認韌體有無被置換之能力。

(e) 測試條件：

(1) 受測物須提供更新所使用之韌體檔案。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 當受測物之韌體更新機制為手動更新，根據廠商所提供韌體檔案數位簽章之方法，使用自簽憑證對韌體更新檔重新簽章並上傳至受測物。

(2) 執行受測物手動更新，並檢視步驟(1)更新是否成功。

(3) 當受測物之韌體更新機制為手動更新，根據廠商所提供已合法簽章之韌體檔案，並上傳至受測物。

(4) 執行受測物手動更新，並檢視步驟(3)更新是否成功。

(h) 判定標準：

(1) 置換或修改韌體檔案後，更新受測物韌體失敗。

(2) 使用合法簽章韌體檔案，更新受測物韌體成功。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)結果皆符合。

(2) 不通過：判定標準(1)、(2)結果不符合其中一項，或韌體不具備更新功能。

(3) 不適用：無。

5.2.3 韌體傾印(Dump)之敏感性資料

5.2.3.1 韌體傾印(Dump)之敏感性資料測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.2.3.1

(b) 安全等級：

3 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物韌體是否具備防止敏感性資料暴露之能力。

(e) 測試條件：

廠商須提供韌體 Dump 方法(如：提供治具或接腳定義、除錯線等)。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 啟動設備並進行正常操作。

(2) 依廠商提供之方法，嘗試傾印(Dump)韌體檔案。

(3) 使用具韌體分析功能之工具，對受測物之韌體進行分析。

(4) 使用檢索工具或系統指令如 strings, grep, find 等，針對敏感性資料之關鍵字詞(如：password, pwd, private key, config, conf.…等)進行作業系統或 MCU（Micro Control Unit）韌體掃描，確認是否有未加密之敏感性資料。若有加密之敏感性資料，加密方式須採用 NIST SP 800-140C 所核可之加密演算法。

(5) 檢視韌體內之設定檔或資料庫檔案，是否存在未加密之敏感性資料或可識別之隱私資料。

(h) 判定標準：

(1) 受測物韌體無法傾印(Dump)，如晶片有設定防讀取機制。

(2) 受測物韌體內之敏感性資料已加密，且加密方式須採用 NIST SP 800-140C 所核可之加密演算法。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)兩項結果符合其中一項。

(2) 不通過：判定標準(1)、(2)兩項結果皆不符合。

(3) 不適用：無。

5.3 系統安全

檢視數據機之系統安全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。

5.3.1 作業系統與網路服務重大資安風險之漏洞

5.3.1.1 作業系統與網路服務重大資安風險之漏洞 1 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.3.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物之作業系統與網路服務是否存在安全漏洞。

(e) 測試條件：

廠商須提供作業系統層最高權限登入之方法。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 測試電腦連接受測物，以最高權限登入受測物之作業系統。

(2) 使用弱點掃描工具掃描。

(3) 確認作業系統與網路服務是否存在安全漏洞。

(4) 以最新版本之 CVSS 版本為主，若無 CVSS v3.x 版本之分數，則以 CVSS v2 評分為基準。

(h) 判定標準：

(1) 受測物之作業系統與網路服務不存在美國國家弱點資料庫(NVD)所評分 CVSS 基本風險計量為 9.0 以上之資安弱點與漏洞。

(i) 判定結果：

(1) 通過：判定標準(1)結果符合。

(2) 不通過：判定標準(1)結果不符合。

(3) 不適用：無。

5.3.1.2 作業系統與網路服務重大資安風險之漏洞 2 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.3.1.2

(b) 安全等級：

2 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物之作業系統與網路服務是否存在安全漏洞。

(e) 測試條件：

廠商須提供作業系統層最高權限登入之方法。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 測試電腦連接受測物，以最高權限登入受測物之作業系統。

(2) 使用弱點掃描工具掃描。

(3) 確認作業系統與網路服務是否存在安全漏洞。

(4) 以最新版本之 CVSS 版本為主，若無 CVSS v3.x 版本之分數，則以 CVSS v2 評分為基準。

(h) 判定標準：

(1) 受測物之作業系統與網路服務不存在美國國家弱點資料庫(NVD)所評分 CVSS 基本風險計量為 7.0 以上之資安弱點與漏洞。

(i) 判定結果：

(1) 通過：判定標準(1)結果符合。

(2) 不通過：判定標準(1)結果不符合。

(3) 不適用：無。

5.3.1.3 作業系統與網路服務重大資安風險之漏洞 3 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.3.1.3

(b) 安全等級：

3 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物之作業系統與網路服務是否存在安全漏洞。

(e) 測試條件：

廠商須提供作業系統層最高權限登入之方法，並提供 SBOM 清單。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 測試電腦連接受測物，以最高權限登入作業系統。

(2) 使用弱點掃描工具掃描。

(3) 確認作業系統與網路服務是否存在安全漏洞。

(4) 以最新版本之 CVSS 版本為主，若無 CVSS v3.x 版本之分數，則以 CVSS v2 評分為基準。

(5) 檢視 SBOM 清單，並透過 NIST NVD 所提供最新之 CPE 資料進行比對。

(h) 判定標準：

(1) 受測物之作業系統與網路服務不存在美國國家弱點資料庫(NVD)所評分 CVSS 基本風險計量為 4.0 以上之資安弱點與漏洞。

(2) 受測物之作業系統與網路服務之 SBOM 清單比對 CPE 資料結果不存在美國國家弱點資料庫(NVD)所評分 CVSS 基本風險計量為 HIGH 以上之資安弱點與漏洞。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)兩項結果皆符合。

(2) 不通過：判定標準(1)、(2)兩項結果不符合其中一項。

(3) 不適用：無。

5.3.2 最小化網路服務連接

5.3.2.1 最小化網路服務連接測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.3.2.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.2.2.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物是否存在未宣告之網路通訊埠。

(e) 測試條件：

廠商須提供使用之網路通訊服務與宣告之通訊埠資料。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 檢視廠商設備自我宣告表(附錄 A)，提供受測物使用之網路通訊服務與宣告之網路通訊埠資料。

(2) 以測試電腦連接受測物。

(3) 使用網路通訊埠掃描軟體進行埠掃描。

(4) 確認是否存在未宣告之網路通訊埠。

(5) 確認每個網路通訊埠是否同附錄 A 所註明必須開啟。

(h) 判定標準：

(1) 受測物所開啟之網路通訊埠與廠商自我宣告一致(附錄 A)。

(2) 受測物所開啟之網路通訊埠皆為必須開啟。

(3) 不可開啟常見高風險傳輸服務(如 ftp、telnet)。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)、(2)三項結果皆符合。

(2) 不通過：判定標準(1)、(2)、(3)三項結果不符合其中一項。

(3) 不適用：無。

5.3.3 敏感性資料之儲存加密

5.3.3.1 敏感性資料之儲存加密測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.3.3.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.4.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物作業系統內之敏感性資料是否加密儲存。

(e) 測試條件：

廠商須提供作業系統層最高權限登入之方法與相關加密佐證紀錄資訊。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 透過廠商提供資訊登入受測物系統之作業系統層並檢視廠商提供之相關敏感性資料使用之加密佐證紀錄資訊。

(2) 使用檢索工具或系統指令如 strings, grep, find 等，針對敏感性資料之關鍵字詞(如：password, pwd, private key, config, conf.…等)進行查看或作業系統掃描，確認是否有未加密之敏感性資料。

(3) 檢視作業系統內之設定檔或資料庫檔案，是否存在未加密之敏感性資料或可識別之隱私資料。

(h) 判定標準：

(1) 可透過廠商提供資訊成功進入受測物作業系統，提供相關敏感性資料使用之加密佐證紀錄資訊採用 NIST SP 800-140C 所核可之安全功能。

(2) 受測物不存在存取作業系統之介面，提供相關敏感性資料使用之加密佐證紀錄資訊採用 NIST SP 800-140C 所核可之安全功能。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)兩項結果符合其中一項。

(2) 不通過：判定標準(1)、(2)兩項結果皆不符合。

(3) 不適用：無。

5.3.4 安全晶片之儲存保護聲明

5.3.4.1 安全晶片之儲存保護聲明

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.3.4.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.4.1.1

(b) 安全等級：

3 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物是否使用安全晶片保護敏感性資料。

(e) 測試條件：

廠商須提供安全晶片之使用證明文件。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 檢視廠商提供書面審查安全晶片(如：TrustZone、TPM…等)之使用證明文件。

(h) 判定標準：

(1) 受測物使用安全晶片保護敏感性資料。

(i) 判定結果

(1) 通過：判定標準(1)結果符合。

(2) 不通過：判定標準(1)結果不符合。

(3) 不適用：無。

5.3.5 遠端連線服務安全性

5.3.5.1 遠端連線服務安全性測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.3.5.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.2.2.2

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.2.2.5

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物遠端連線服務之安全性。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 受測物還原至出廠設定。

(2) 透過網路連接受測物之系統，使用通訊埠掃描軟體進行埠掃描，確認遠端連線服務(如：adb、telnet、ssh 等)為關閉狀態。

(3) 啟用遠端連線服務，確認是否提示警語訊息(如：開啟該服務有資安風險等)。

(4) 須經過通行碼鑑別以存取遠端連線服務進入存取作業系統時，檢視通行碼鑑別，是否符合 5.5.4 通行碼鑑別機制須具備複雜度及強度測試的要求。

(h) 判定標準：

(1) 受測物通訊埠不具備遠端連線服務 (如：adb、telnet、ssh 等)。

(2) 受測物預設關閉遠端連線服務 (如：adb、telnet、ssh 等)。

(3) 受測物啟用遠端連線服務時提示警語訊息。

(4) 受測物存取遠端連線服務時須經過身分鑑別，且符合 5.5.4 通行碼鑑別機制須具備複雜度及強度測試的要求。

(i) 判定結果：

(1) 通過：判定標準(1)結果符合或判定標準(2)、(3)、(4)三項結果皆符合。

(2) 不通過：判定標準(1)結果不符合及判定標準(2)、(3)、(4)三項結果其中一項不符合。

(3) 不適用：無。

5.4 傳輸通訊安全

檢視數據機之傳輸通訊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。

5.4.1 網頁管理介面之傳輸安全

5.4.1.1 網頁管理介面之傳輸安全測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.4.1.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.4.2.7

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物網頁管理介面預設傳輸是否使用 TLS 1.2 同等或以上之安全通訊協定。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 將測試電腦或行動裝置連接受測物之管理介面。

(2) 使用安全通道掃描工具，確認網頁管理頁面所使用之安全通道版本。

(3) 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。

(h) 判定標準：

(1) 受測物預設傳輸使用 TLS 1.2 同等或以上之安全通訊協定。

(i) 判定結果：

(1) 通過：判定標準(1)結果符合。

(2) 不通過：判定標準(1)結果不符合。

(3) 不適用：無。

5.4.2 儲存媒體共用模式之傳輸安全

5.4.2.1 儲存媒體共用模式身分驗證測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.4.2.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物儲存媒體共用模式之傳輸是否經過身分驗證。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 使受測物處於檔案共用模式，於相應之介面提供相應之身分驗證因子，以進行資料讀取寫入。

(2) 當經由通行碼鑑別以存取共用檔案，檢視通行碼鑑別，是否符合 5.5.4 通行碼鑑別機制須具備複雜度及強度測試的要求。

(3) 當非經由通行碼鑑別存取共用檔案時，依廠商宣告足以鑑別使用者身分之機制方法進行驗證。

(h) 判定標準：

(1) 當受測物檔案共用模式採用通行碼鑑別方式，符合 5.5.4 通行碼鑑別機制須具備複雜度及強度之要求。

(2) 當受測物檔案共用模式採用非通行碼鑑別方式，符合足以鑑別使用者身分之機制驗證。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)兩項結果符合其中一項。

(2) 不通過：判定標準(1)、(2)兩項結果皆不符合。

(3) 不適用：受測物沒有儲存媒體共用模式。

5.4.3 Wi-Fi 傳輸安全

5.4.3.1 Wi-Fi 傳輸安全測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.4.3.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.7.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物 Wi-Fi 是否使用 WPA2 同等或以上版本之保護設置。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 使用 Wi-Fi 掃描工具，確認受測物所使用之 Wi-Fi 通道設定。

(h) 判定標準：

(1) 受測物 Wi-Fi 使用 WPA2 同等或以上之 Wi-Fi 安全通道。

(i) 判定結果：

(1) 通過：判定標準(1)結果符合。

(2) 不通過：判定標準(1)結果不符合。

(3) 不適用：受測物 Wi-Fi 不具備 Wi-Fi 傳輸功能。

5.4.4 安全的 Wi-Fi 組態設置

5.4.4.1 安全的 Wi-Fi 組態設置測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.4.4.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物是否存在具有安全風險的 Wi-Fi 設定。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 將測試電腦或行動裝置連接受測物。

(2) 根據受測物使用說明，開啟相應之管理介面連接工具。

(3) 檢視受測物網頁管理介面，「WPS PIN」與「WPS PBC」功能是否存在供使用者操作的開/關介面，並確認 WPS 功能是否皆為關閉狀態。

(h) 判定標準：

(1) 受測物有提供使用者操作「WPS PIN」與「WPS PBC」操作的開/關介面。

(2) 受測物 WPS 功能預設皆須為關閉狀態。

(i) 判定結果：

(1) 通過：判定標準(1)、判定標準(2)兩項結果皆符合。

(2) 不通過：判定標準(1)、判定標準(2)兩項結果不符合其中一項。

(3) 不適用：受測物不具備 WPS 功能。

5.4.5 安全的數據機組態設置

5.4.5.1 安全的數據機組態設置 1 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.4.5.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物是否存在不安全的組態設定。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 將測試電腦或行動裝置連接受測物。

(2) 根據受測物使用說明，開啟相應之管理介面連接工具。

(3) 檢視受測物網頁管理介面，UPnP 是否存在供使用者操作的開/關介面，並確認 UPnP 功能啟用時是否提示警語訊息(如：開啟該服務有資安風險等)。

(h) 判定標準：

(1) 受測物提供使用者操作 UPnP 操作的開/關介面。

(2) 受測物 UPnP 功能啟用時提示警語訊息。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)兩項結果皆符合。

(2) 不通過：判定標準(1)、(2)兩項結果不符合其中一項。

(3) 不適用：產品未具備 UPnP 功能。

5.4.5.2 安全的數據機組態設置 3 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.4.5.1

TAICS TS-0049 v1.0 數據機資安標準 5.4.5.2

(b) 安全等級：

3 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物是否存在不安全的組態設定。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 將測試電腦或行動裝置連接受測物。

(2) 根據受測物使用說明，開啟相應之管理介面連接工具。

(3) 檢視受測物網頁管理介面，確認 UPnP 功能是否預設為關閉。

(h) 判定標準：

(1) 受測物符合 5.4.5.1 之要求。

(2) 受測物 UPnP 功能預設為關閉狀態。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)兩項結果皆符合。

(2) 不通過：判定標準(1)、(2)兩項結果不符合其中一項。

(3) 不適用：產品未具備 UPnP 功能。

5.5 身分鑑別機制安全

檢視數據機之身分鑑別機制安全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。

5.5.1 會話安全性

5.5.1.1 管理者會話安全性測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.5.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗產品僅允許單一管理者同時只有一個有效會話。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 根據受測物之使用說明文件，開啟相應之管理介面進行管理者身分鑑別並完成連接受測物。

(2) 於另一台測試電腦或不同瀏覽器開啟相應之管理介面進行同一管理者身分鑑別嘗試連接及控制受測物。

(h) 判定標準：

(1) 受測物網頁管理介面具備身分鑑別機制。

(2) 受測物於另一台測試電腦或不同瀏覽器開啟相應之管理介面，無法進行同一身分鑑別連接及控制受測物。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)兩項結果皆符合。

(2) 不通過：判定標準(1)、(2)兩項結果不符合其中一項。

(3) 不適用：無。

5.5.2 檔案共享功能之權限控管機制

5.5.2.1 檔案共享功能之權限控管機制測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.5.2.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物檔案共享功能是否具備權限區分管控之能力。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 根據受測物之使用說明文件，開啟相應之管理介面。

(2) 於管理介面新增一般使用者功能，新增一位一般使用者帳密。

(3) 以管理者權限，進入檔案共享介面。

(4) 存取受測物共享檔案，檢視該帳號之身分類型與其對應之權限，是否與廠商自我宣告權限相符。

(5) 以一般使用者帳密登入，進入檔案共享介面。

(6) 存取受測物共享檔案，檢視該帳號之身分類型與其對應之權限，是否與廠商自我宣告相符。

(7) 嘗試存取他人共享檔案，檢視該帳號之身分類型與其對應之權限，是否與廠商自我宣告相符。

(h) 判定標準：

(1) 受測物共享檔案的存取權限，其身分授權與廠商自我宣告一致。

(i) 判定結果：

(1) 通過：判定標準(1)結果符合。

(2) 不通過：判定標準(1)結果不符合。

(3) 不適用：受測物不具備檔案共享功能。

5.5.3 預設通行碼安全性

5.5.3.1 預設通行碼安全性之測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.5.3.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.1.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物不應使用共通的預設通行碼。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 初次連接受測物(或先還原出廠設定再連接受測物)。

(2) 根據受測物之使用說明文件，開啟相應之管理介面連接工具並輸入預設通行碼後登入。

(3) 檢視系統是否強制修改管理者通行碼後，方可運行。

(h) 判定標準：

(1) 受測物初次登入，系統強制修改管理者通行碼。

(2) 受測物預設通行碼每台不同。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)兩項結果符合其中一項。

(2) 不通過：判定標準(1)、(2)兩項結果皆不符合。

(3) 不適用：無。

5.5.4 通行碼鑑別機制強度

5.5.4.1 通行碼鑑別機制強度測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.5.4.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物通行碼是否符合政府組態基準(Government Configuration Baseline, GCB)或國際標準之強度要求。

(e) 測試條件：

提供參照之通行碼強度要求資訊(如 GCB、國際標準或本測試規範方法)。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 情境一(8 個字元以上加複雜度)：

(i) 根據受測物之使用說明文件，連接所有相應之登入介面，包括但不限於網頁管理介面、無線網路連線介面等。

(ii) 輸入小於 8 個字元長度之通行碼，檢查通行碼是否能成功建立或變更。

(iii) 輸入同時含下述四種字元中的兩種或以下：(1)英文大寫字元(A 到 Z)；(2)英文小寫字元(a 到 z)；(3)十進位數字(0 到 9)；(4)非英文字母字元(例如：!、$、#、%)，檢查通行碼是否能成功建立或變更。

(iv) 輸入同時含下述四種字元中的三種或以上，並包含重複或連續字符（例如包含'aaaa'、'1234'、'abcd'等字符）之通行碼：(1)英文大寫字元(A 到 Z)；(2)英文小寫字元(a 到 z)；(3)十進位數字(0 到 9)；(4)非英文字母字元(例如：!、$、#、%)，檢查通行碼是否能成功建立或變更。

(v) 輸入同時含下述四種字元中的三種或以上，不具有重複或連續字符（例如包含'aaaa'、'1234'、'abcd'等字符）之通行碼：(1)英文大寫字元(A 到 Z)；(2)英文小寫字元(a 到 z)；(3)十進位數字(0 到 9)；(4)非英文字母字元(例如：!、$、#、%)，檢查通行碼是否能成功建立或變更。

(vi) 確認建立或變更通行碼時是否出現通行碼規則提示訊息。

(2) 情境二(15 個字元以上)：

(i) 根據受測物之使用說明文件，連接所有相應之登入介面，包括但不限於網頁管理介面、無線網路連線介面等。

(ii) 輸入小於 15 個字元長度之通行碼，檢查通行碼是否能成功建立或變更。

(iii) 輸入大於等於 15 個字元長度，並包含重複或連續字符（例如包含'aaaa'、'1234'、'abcd'等字符）之通行碼，檢查通行碼是否能成功建立或變更。

(iv) 輸入大於等於 15 個字元長度，不具有重複或連續字符（例如包含'aaaa'、'1234'、'abcd'等字符）之通行碼，檢查通行碼是否能成功建立或變更。

(v) 確認建立或變更通行碼時是否出現通行碼規則提示訊息。

(3) 情境三(其他情況)：

(i) 根據受測物之使用說明文件，連接所有相應之登入介面，包括但不限於網頁管理介面、無線網路連線介面等。

(ii) 輸入符合其他標準或規範許可之通行碼，檢查通行碼是否能成功建立或變更。

(h) 判定標準：

(1) 受測物通行碼長度不得小於 8 個字元，且通行碼複雜度須包含規定四種字元(英文大寫字元、英文小寫字元、十進位數字、特殊符號)中的三種或以上，且不得為重複或連續字符（例如包含'aaaa'、'1234'、'abcd'等字符），並具有通行碼規則訊息提示。

(2) 受測物通行碼長度不得小於 15 個字元，且不得為重複或連續字符（例如包含'aaaa'、'1234'、'abcd'等字符），並具有通行碼規則訊息提示。

(3) 受測物通行碼符合情境三之要求。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)、(3)三項結果符合其中一項。

(2) 不通過：判定標準(1)、(2)、(3)三項結果皆不符合。

(3) 不適用：無。

5.5.5 通行碼的輸入頻率及次數限制

5.5.5.1 通行碼的輸入頻率及次數限制測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.5.5.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.1.2.2

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物身分查驗機制是否具備防止暴力破解的能力。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 將測試電腦或行動裝置連接受測物。

(2) 根據受測物使用說明，開啟相應之管理介面連接工具以執行身分鑑別。

(3) 不斷輸入錯誤的通行碼。

(4) 檢視受測物是否如廠商宣告之機制會鎖定帳戶。

(5) 帳戶鎖定後，於鎖定期間內持續輸入相異且錯誤的通行碼，比對廠商宣告帳戶鎖定時限內，檢視帳戶是否解除鎖定，預設帳戶鎖定時限依各廠商及使用情境自行設定合理時限。

(6) 同一帳戶任一次登入失敗後，於廠商宣告計數器重設時限內，重新輸入錯誤且相異的通行碼，檢視輸入失敗次數是否有重新計算。

(h) 判定標準：

(1) 受測物輸入錯誤通行碼的次數如廠商宣告，會鎖定帳戶。

(2) 受測物於廠商宣告之帳戶鎖定時限內，帳戶未解除鎖定。

(3) 受測物於廠商宣告計數器重設時限內，失敗次數未重新計算。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)、(3)三項結果皆符合。

(2) 不通過：判定標準(1)、(2)、(3)三項結果不符合其中一項。

(3) 不適用：無。

5.6 網頁服務安全

檢視數據機之網頁服務安全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。

5.6.1 管理者登入會話有效時間

5.6.1.1 管理者登入會話有效時間測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.6.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物是否具備登入權限有效時間之限制。

(e) 測試條件：

(1) 廠商須提供書面資料說明閒置時限設定值。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 將測試電腦或行動裝置連接受測物。

(2) 根據受測物之使用說明文件，開啟相應之管理介面進行身分鑑別並完成連接受測物。

(3) 閒置受測物直到超過閒置時限值。

(4) 檢視是否需要重新鑑別方可存取受測物。

(h) 判定標準：

(1) 受測物存在閒置時限機制。

(2) 受測物連線閒置逾時，須重新經過身分鑑別方可存取。

(i) 判定結果：

(1) 通過:判定標準(1)、(2)兩項結果皆符合。

(2) 不通過:判定標準(1)、(2)兩項結果不符合其中一項。

(3) 不適用: 無。

5.6.2 網頁管理介面重大資安風險之漏洞

5.6.2.1 網頁管理介面重大資安風險之漏洞 1 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.6.2.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物之網頁管理介面是否存在安全漏洞。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 將測試電腦連接受測物。

(2) 啟動具備網頁弱點掃描功能之工具，對受測物網頁介面執行弱點掃描。

(3) 檢視該弱點掃描工具所產生之報告，是否存在資安弱點與漏洞。

(4) 以最新版本之 CVSS 版本為主，若無 CVSS v3.x 版本之分數，則以 CVSS v2 評分為基準。

(h) 判定標準：

(1) 受測物之網頁管理介面，不存在美國國家弱點資料庫(NVD)所評分 CVSS 為 9.0 以上之資安弱點與漏洞。

(i) 判定結果：

(1) 通過：判定標準(1)結果符合。

(2) 不通過：判定標準(1)結果不符合。

(3) 不適用：無。

5.6.2.2 網頁管理介面重大資安風險之漏洞 2 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.6.2.2

(b) 安全等級：

2 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物之網頁管理介面是否存在安全漏洞。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 將測試電腦連接受測物。

(2) 啟動具備網頁弱點掃描功能之工具，對受測物網頁介面執行弱點掃描。

(3) 檢視該弱點掃描工具所產生之報告，是否存在資安弱點與漏洞。

(4) 以最新版本之 CVSS 版本為主，若無 CVSS v3.x 版本之分數，則以 CVSS v2 評分為基準。

(h) 判定標準：

(1) 受測物之網頁管理介面，不存在美國國家弱點資料庫(NVD)所評分 CVSS 為 7.0 以上之資安弱點與漏洞。

(i) 判定結果：

(1) 通過：判定標準(1)結果符合。

(2) 不通過：判定標準(1)結果不符合。

(3) 不適用：無。

5.6.2.3 網頁管理介面重大資安風險之漏洞 3 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.6.2.3

(b) 安全等級：

3 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物之網頁管理介面是否存在安全漏洞。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 將測試電腦連接受測物。

(2) 啟動具備網頁弱點掃描功能之工具，對受測物網頁介面執行弱點掃描。

(3) 檢視該弱點掃描工具所產生之報告，是否存在資安弱點與漏洞。

(4) 以最新版本之 CVSS 版本為主，若無 CVSS v3.x 版本之分數，則以 CVSS v2 評分為基準。

(h) 判定標準：

(1) 受測物之網頁管理介面，不存在美國國家弱點資料庫(NVD)所評分 CVSS 為 4.0 以上之資安弱點與漏洞。

(i) 判定結果：

(1) 通過：判定標準(1)結果符合。

(2) 不通過：判定標準(1)結果不符合。

(3) 不適用：無。

5.6.3 應用程式重送攻擊安全測試

5.6.3.1 應用程式重送攻擊安全測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.6.3.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.1.2.3

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物應用程式重送攻擊之安全測試。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 連接測試電腦與受測物。

(2) 根據受測物使用說明，至可觸發存取受測物身分的網站功能或服務之介面。

(3) 透過程式與受測物建立連線，同時側錄連線。

(4) 執行相關操作，檢視側錄結果是否要求身分鑑別，並當採用通行碼鑑別時，須符合 5.5.4 通行碼鑑別機制須具備複雜度及強度測試的要求。

(5) 當受測物要求身分鑑別，將側錄到的身分鑑別資訊，重新發送至受測物。

(6) 檢視鑑別結果是否成功。

(7) 執行受測物登出並再次登入，檢視身分鑑別功能是否正常執行。

(h) 判定標準：

(1) 受測物身分鑑別機制具備抵抗重送攻擊的能力。

(2) 當受測物採用通行碼鑑別方式，符合 5.5.4 通行碼鑑別機制須具備複雜度及強度測試之要求。

(3) 登出後確實須再次登入，方可存取受測物。

(i) 判定結果：

(1) 通過:判定標準(1)、(2)、(3)三項結果皆符合。

(2) 不通過:判定標準(1)、(2)、(3)三項結果不符合其一。

(3) 不適用：無。

5.6.4 設備設定檔內容之敏感性資料與權限管理

5.6.4.1 設備設定檔內容之敏感性資料與權限管理測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.6.4.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.4.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗產品設備設定檔之匯入與匯出功能須具有管理權限要求，並且其輸出之內容不應存在明文顯示之敏感性資料，應用加密方式來儲存敏感性資料，其加密方式採用 NIST SP 800-140C 所核可之加密演算法。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 依據廠商使用說明文件中所提供之匯入與匯出設定檔之方法，分別透過一般權限帳號、管理權限帳號、以及無效帳號進行操作測試。

(2) 測試是否存有匯出受測物設定檔功能。

(3) 檢視設定檔是否洩漏敏感性資料。

(h) 判定標準：

(1) 確認匯入與匯出設定檔功能具有管理權限要求。

(2) 受測物之設定檔內容無洩漏敏感性資料。

(3) 存在加密敏感性資料時，廠商宣告使用之加密方法須符合 NIST SP 800-140C 之要求。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)兩項結果皆符合或判定標準(1)、(3)兩項結果皆符合。

(2) 不通過：判定標準(1)、(3)兩項結果其中一項不符合。

(3) 不適用：受測物不具備設定檔匯入與匯出功能。

5.7 日誌紀錄安全

檢視數據機之日誌紀錄安全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。

5.7.1 安全事件日誌

5.7.1.1 安全事件日誌 1 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.7.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物是否具備安全事件紀錄可供追溯。

(e) 測試條件：

受測物是否具備安全事件紀錄並為啟用狀態。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 依據廠商提供之書面說明，檢視受測物是否有安全事件日誌。

(2) 若有安全事件日誌，確認其時間戳記格式是否包含年月日、時分秒等資訊。

(3) 檢視安全日誌包括管理介面及系統之登入、登出、修改通行碼、設定及異常狀況。

(h) 判定標準：

(1) 受測物提供安全事件日誌供查詢。

(2) 受測物安全事件日誌的時間戳記包含年月日、時分秒等資訊。

(3) 受測物安全事件日誌包括管理介面及系統之登入、登出、修改通行碼、設定及異常狀況。

(i) 判定結果：

(1) 通過:判定標準(1)、(2)、(3)三項結果皆符合。

(2) 不通過: 判定標準(1)、(2)、(3)三項結果不符合其中一項。

(3) 不適用：無。

5.7.1.2 安全事件日誌供 2 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.7.1.2

(b) 安全等級：

2 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物是否具備安全事件紀錄可供追溯，且具備將日誌記錄至外部儲存空間或 Log 伺服器之功能。

(e) 測試條件：

無。

(f) 測試佈局：

一台 Log Server。

(g) 測試方法：

(1) 啟用一台 Log Server 並將日誌記錄儲存設定至該 Server 位置。

(2) 檢視 Log Server 紀錄，是否成功接收該日誌內容。

(h) 判定標準：

(1) Log Server 紀錄成功接收該日誌內容。

(i) 判定結果：

(1) 通過:判定標準(1)結果符合。

(2) 不通過: 判定標準(1)結果不符合。

(3) 不適用：無。

5.7.2 日誌內容之敏感性資料

5.7.2.1 日誌內容之敏感性資料測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.7.2.1

TAICS TS-0046 v1.0 消費性物聯網產品資安測試規範 5.4.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物日誌內容是否洩漏敏感性資料。

(e) 測試條件：

廠商需提供日誌記錄觸發方式。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 日誌與安全事件日誌記錄(如：Service Log、System Log 等)若儲存於裝置內，依據廠商提供觸發日誌記錄之方法進行操作，觸發日誌記錄。

(2) 除廠商提供之日誌記錄觸發方法外，盡可能對受測物之所有功能進行正常操作，確保觸發廠商宣告以外可能產生之日誌紀錄。

(3) 檢視日誌紀錄是否洩漏敏感性資料。

(h) 判定標準：

(1) 受測物之日誌記錄無敏感性資料。

(i) 判定結果：

(1) 通過：判定標準(1)結果符合。

(2) 不通過：判定標準(1)結果不符合。

(3) 不適用：無。

5.7.3 日誌輪替功能

5.7.3.1 日誌輪替功能 1 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.7.3.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物是否具備日誌輪替機制處理日誌儲存空間不足之狀況，以及產品設備是否提供足夠容納測試方法範例最低日誌保留天數總計所需以上的日誌儲存容量。

(e) 測試條件：

(1) 廠商需提供日誌觸發方式與日誌輪替機制。

(2) 廠商需提供可快速填滿日誌儲存空間方法。

(3) 若日誌存放後台則提供相關資訊書面審查。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 日誌與安全事件日誌記錄(如：Service Log、System Log 等)若儲存於裝置內，依據廠商提供之方法觸發日誌紀錄，並塞滿日誌儲存空間。

(2) 持續觸發日誌紀錄，檢視受測物是否會發生儲存空間不足的現象，導致無法正常記錄事件。

(3) 受測物須根據 NIST SP 800-92 Table 4-1 「Examples of Logging Configuration Settings」所呈現的日誌組態設定範例之 Low Impact Systems 類別，並確認產品設備是否提供足夠容納該範例計算每日預估基本日誌產生容量及相應所需儲存日誌天數之總計以上的日誌儲存容量。

(h) 判定標準：

(1) 受測物具有日誌記錄檔輪替機制。

(2) 受測物之日誌儲存容量，符合 NIST SP 800-92 Table 4-1 「Examples of Logging Configuration Settings」所呈現的日誌組態設定範例之 Low Impact Systems 類別要求。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)兩項結果皆符合。

(2) 不通過：判定標準(1)、(2)兩項結果不符合其中一項。

(3) 不適用：無。

5.7.3.2 日誌輪替功能 2 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.7.3.2

(b) 安全等級：

2 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物是否具備日誌輪替機制處理日誌儲存空間不足之狀況，以及產品設備是否提供足夠容納測試方法範例最低日誌保留天數總計所需以上的日誌儲存容量。

(e) 測試條件：

(1) 廠商需提供日誌觸發方式與日誌輪替機制。

(2) 廠商需提供可快速填滿日誌儲存空間方法。

(3) 若日誌存放後台則提供相關資訊書面審查。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 日誌與安全事件日誌記錄(如：Service Log、System Log 等)若儲存於裝置內，依據廠商提供之方法觸發日誌紀錄，並塞滿日誌儲存空間。

(2) 持續觸發日誌紀錄，檢視受測物是否會發生儲存空間不足的現象，導致無法正常記錄事件。

(3) 受測物須根據 NIST SP 800-92 Table 4-1 「Examples of Logging Configuration Settings」所呈現的日誌組態設定範例之 Moderate Impact Systems 類別，並確認產品設備是否提供足夠容納該範例計算每日預估基本日誌產生容量及相應所需儲存日誌天數之總計以上的日誌儲存容量。

(h) 判定標準：

(1) 受測物具有日誌記錄檔輪替機制。

(2) 受測物之日誌儲存容量，符合 NIST SP 800-92 Table 4-1 「Examples of Logging Configuration Settings」所呈現的日誌組態設定範例之 Moderate Impact Systems 類別要求。

(i) 判定結果：

(1) 通過：判定標準(1)、(2)兩項結果皆符合。

(2) 不通過：判定標準(1)、(2)兩項結果不符合其中一項。

(3) 不適用：無。

5.7.3.3 日誌輪替功能 3 級測試

(a) 測試依據：

TAICS TS-0049 v1.0 數據機資安標準 5.7.3.3

(b) 安全等級：

3 級。

(c) 測試資料：

無。

(d) 測試目的：

查驗受測物是否具備日誌輪替機制處理日誌儲存空間不足之狀況，以及產品設備是否提供足夠容納測試方法範例最低日誌保留天數總計所需以上的日誌儲存容量。

(e) 測試條件：

(1) 廠商需提供日誌觸發方式與日誌輪替機制。

(2) 廠商需提供可快速填滿日誌儲存空間方法。

(3) 若日誌存放後台則提供相關資訊書面審查。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 日誌與安全事件日誌記錄(如：Service Log、System Log 等)若儲存於裝置內，依據廠商提供之方法觸發日誌紀錄，並塞滿日誌儲存空間。

(2) 持續觸發日誌紀錄，檢視受測物是否會發生儲存空間不足的現象，導致無法正常記錄事件。

(3) 受測物須根據 NIST SP 800-92 Table 4-1 「Examples of Logging Configuration Settings」所呈現的日誌組態設定範例之 High Impact Systems

類別，並確認產品設備是否提供足夠容納該範例計算每日預估基本日誌產生容量及相應所需儲存日誌天數之總計以上的日誌儲存容量。

(h) 判定標準：

(1) 受測物具有日誌記錄檔輪替機制。

(2) 受測物之日誌儲存容量，符合 NIST SP 800-92 Table 4-1 「Examples of Logging Configuration Settings」所呈現的日誌組態設定範例之 High Impact Systems 類別要求。

(i) 判定結果：

(1) 通過：判定標準(1)、判定標準(2)兩項結果皆符合。

(2) 不通過：判定標準(1)、判定標準(2)兩項結果不符合其中一項。

(3) 不適用：無。

附錄 A
(參考)
設備自我宣告

表 A.1 設備自我宣告表

受測物須檢附設備自我宣告表，以供測試實驗室參閱：

設 備 自 我 宣 告 表		
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 (含雜湊資訊)		
預設啟用之 TCP/UDP 網路通訊埠與對應服務		
採用加密演算法聲明		
進入作業系統除錯模式之方法		
日誌記錄觸發方法與日誌輪替觸發機制		
日誌紀錄預估每日儲存容量		
檔案共享權限聲明		
韌體 Dump 方法 (例如：提供製具、接腳定義、除錯線或工程版本等)		
所有帳號及對應權限聲明(包含系統、除錯模式鑑別、工程帳號...等)		
預設通行碼及通行碼強度參照聲明		
通行碼錯誤鎖定機制		
(欄位可自行增加)		

附錄 B
(參考)
測試項目與國際標準對照

表 B.1 測試項目與國際標準對照表

安全構面	測試項目	判定標準	參考來源	參考內容
實體安全	實體埠安全管控測試	本規範 5.1.1	OWASP IoT Top Ten 2018	10：Lack of Physical Hardening
韌體安全及更新	韌體更新測試	本規範 5.2.1	OWASP IoT Top Ten 2018	4：Lack of Secure Update Mechanism
			IEC 62443-4-2	FR 3 - System integrity
	韌體更新檔之真確性及完整性測試	本規範 5.2.2	OWASP IoT Top Ten 2018	4：Lack of Secure Update Mechanism
			IEC 62443-4-2	FR 3 - System integrity
	韌體傾印(Dump)之敏感性資料測試	本規範 5.2.3	OWASP IoT Top Ten 2018	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 4 - Data confidentiality
系統安全	作業系統與網路服務重大資安風險之漏洞測試	本規範 5.3.1	OWASP IoT Top Ten 2018	2：Insecure Network Services 5：Use of Insecure or Outdated Components
			IEC 62443-4-2	FR 3 - System integrity
	最小化網路服務連接埠測試	本規範 5.3.2	OWASP IoT Top Ten 2018	2：Insecure Network Services
			IEC 62443-4-2	FR 7 - Resource availability
	敏感性資料之儲存加密測試	本規範 5.3.3	OWASP IoT Top Ten 2018	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 4 - Data confidentiality

安全構面	測試項目	判定標準	參考來源	參考內容
	安全晶片之儲存保護聲明測試	本規範 5.3.4	IEC 62443-4-2	FR 1 - Identification and authentication control
	遠端連線服務安全性測試	本規範 5.3.5	OWASP IoT Top Ten 2018	2：Insecure Network Services
			IEC 62443-4-2	FR 1 - Identification and authentication control
傳輸通訊安全	網頁管理介面之傳輸安全測試	本規範 5.4.1	OWASP IoT Top Ten 2018	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 3 - System integrity
	儲存媒體共用模式之傳輸安全測試	本規範 5.4.2	OWASP IoT Top Ten 2018	3：Insecure Ecosystem Interfaces
			IEC 62443-4-2	FR 3 - System integrity
	Wi-Fi 傳輸安全測試	本規範 5.4.3	OWASP IoT Top Ten 2018	9：Insecure Default Settings
			IEC 62443-4-2	FR 3 - System integrity
	安全的 Wi-Fi 組態設置測試	本規範 5.4.4	OWASP IoT Top Ten 2018	3：Insecure Ecosystem Interfaces 9：Insecure Default Settings
			IEC 62443-4-2	FR 2 - Use control
	安全的數據機組態設置測試	本規範 5.4.5	OWASP IoT Top Ten 2018	3：Insecure Ecosystem Interfaces 9：Insecure Default Settings
			IEC 62443-4-2	FR 2 - Use control
身分辨識安全機制	會話安全性測試	本規範 5.5.1	OWASP IoT Top Ten 2018	9：Insecure Default Settings
			IEC 62443-4-2	FR 1 - Identification and authentication control

安全構面	測試項目	判定標準	參考來源	參考內容
	檔案共享功能之權限控管機制測試	本規範 5.5.2	IEC 62443-4-2	FR 2 - Use control
	預設通行碼測試	本規範 5.5.3	OWASP IoT Top Ten 2018	3：Insecure Ecosystem Interfaces
			IEC 62443-4-2	FR 1 - Identification and authentication control
	通行碼鑑別機制強度測試	本規範 5.5.4	OWASP IoT Top Ten 2018	1：Weak, Guessable, or Hardcoded Passwords
			IEC 62443-4-2	FR 1 - Identification and authentication control
	通行碼的輸入頻率及次數限制測試	本規範 5.5.5	OWASP IoT Top Ten 2018	9：Insecure Default Settings
			IEC 62443-4-2	FR 1 - Identification and authentication control
網頁服務安全	管理者登入會話有效時間測試	本規範 5.6.1	OWASP IoT Top Ten 2018	3：Insecure Ecosystem Interfaces
	網頁管理介面重大資安風險之漏洞測試	本規範 5.6.2	OWASP IoT Top Ten 2018	5：Use of Insecure or Outdated Components
			IEC 62443-4-2	FR 3 - System integrity
	應用程式重送攻擊安全測試	本規範 5.6.3	OWASP IoT Top Ten 2018	3：Insecure Ecosystem Interfaces
			IEC 62443-4-2	FR 3 - System integrity
	設備設定檔內容之敏感性資料與權限管理測試	本規範 5.6.4	OWASP IoT Top Ten 2018	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 4 - Data confidentiality
日誌	安全事件日	本規範 5.7.1	IEC 62443-4-2	FR 2 - Use control

安全構面	測試項目	判定標準	參考來源	參考內容
紀錄安全	誌測試			
	日誌內容之敏感性資料測試	本規範 5.7.2	OWASP IoT Top Ten 2018	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 4 - Data confidentiality
	日誌檔之輪替功能測試	本規範 5.7.3	IEC 62443-4-2	FR 2 - Use control
			NIST SP 800-92	Table 4-1. Examples of Logging Configuration Settings

參考資料

(1) FIPS 140-2 Annex A: National Institute of Standards and Technology (NIST),Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Module, May 10, 2017.
(2) Cybersecurity Framework, Version 1.1. 2018/04/16
(3) U.S. Department of Homeland Security, Strategic Principles for Securing the Internet of Things (IoT), Version 1.0, 2016-11-15
(4) SB-327 Information privacy: connected devices. 2017
(5) European Commission Cybersecurity Act. 2017/11/19
(6) European Parliament, The Directive on security of network and information systems (NIS Directive), EUR-Lex - 32016L1148 - EN, 2016/7/6
(7) European Parliament, Regulation on Privacy and Electronic Communications, EUR-Lex - 52017PC0010 – EN
(8) International Organization for Standardization, Are we safe in the Internet of Things? https://www.iso.org/news/2016/09/Ref2113.html
(9) ISO/IEC 27030 (Information technology - Security techniques - Guidelines for security and privacy in Internet of Things (IoT))
(10) ISO/IEC 15408-1: 2009 (Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.)
(11) International Electro technical Commission, About IEC https://www.iec.ch/about/
(12) IEC 62443-4-1:2018 (Security for industrial automation and control systems –Part 4-1: Secure product development lifecycle requirements)
(13) SAE-J 3061:2016 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)
(14) IEEE Standard Association, P2413.1 (Standard for a Reference Architecture for Smart City (RASC))
(15) ENISA, Baseline Security Recommendations for IoT. 2017/11/20
(16) ENISA, Good Practices for Security of Internet of Things in the context of Smart Manufacturing, 2018/11/19
(17) UL 2900-1 (Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements), 2017/7/5

(18) UL2900-2-2 (Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems), 2016/3/30
(19) ETSI, Cyber Security for Consumer Internet of Things, TS 103 645, Version 1.1.1, 2019/2/19
(20) NIST SP 800-92 Guide to Computer Security Log Management Table 4-1
(21) https://nvd.nist.gov/products/cpe

版本修改紀錄

版本	時間	摘要
v1.0	2022/09/15	出版

台灣資通產業標準協會

Taiwan Association of Information and Communication Standards

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