TAICS

TAICS TS-0031 v1.0 : 2020

智慧音箱資安標準

Cybersecurity standard for smart speakers

2020 / 09 / 18

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

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。

TC 主席：神盾股份有限公司 張心玲 副總經理

TC 副主席：財團法人資訊工業策進會 毛敬豪 所長

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 博士

TC 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 吳勁僑 工程師、許博堯 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)：

中華電信股份有限公司、台灣德國萊因技術監護顧問股份有限公司、安華聯網科技股份有限公司、行動檢測服務股份有限公司、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、國立交通大學、國家儀器股份有限公司、華碩電腦股份有限公司、勤業眾信聯合會計師事務所、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)：

台灣小米通訊有限公司、中華資安國際股份有限公司、台灣獵豹移動股份有限公司、美商蘋果亞洲股份有限公司、英華達股份有限公司、國立台灣科技大學、國立雲林科技大學、經濟部標準檢驗局。

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

近年來網路相關應用呈現爆炸性發展，各種五花八門的連網硬體與軟體服務一一出現，智慧音箱便是其中一款硬體結合軟體服務的物聯網設備。不同於以往傳統的藍牙喇叭，智慧音箱具備人工智慧語音處理功能，能夠通過喚醒詞、語音輸入、語音辨識、語意理解、語音合成等技術與用戶互動，並獲取來自網路的內容播放；但由於具備網路連接功能，相關的安全性問題也隨之而來：病毒攻擊、個人隱私資料外洩、硬體及韌體漏洞相繼成為智慧音箱的安全隱患。此外，智慧音箱透過 Wi-Fi、藍牙等無線通訊技術與其他智慧家電串聯，若缺乏足夠的網路安全機制，將容易遭入侵並嚴重影響用戶隱私安全與服務使用安全。

除了一般物聯網設備所關切的資安風險，智慧音箱的最大隱憂仍在於個人隱私(資料保護)。歐盟資料保護監督機關(European Data Protection Supervisor, EDPS)於 2019 年提出一份報告(6)，指出智慧音箱資料保護的八大議題；經濟合作暨發展組織(Organization for Economic Co-operation and Development, OECD)於 2013 年所公布之 OECD Privacy Guidelines [9] 也曾針對相關隱私議題提出指引。隨著智慧音箱應用更加多元，包含購物、家電控制等服務不斷推陳出新，另一方面對應的資安防護與隱私宣告、防護等技術仍參差不齊，產業實有其必要制定一個可齊平遵循的資安標準。為此，國家通訊傳播委員會(National Communications Commission, NCC)為確保智慧音箱使用上之安全性，於 2019 年 7 月委由財團法人電信技術中心(Telecom Technology Center, TTC)訂定智慧音箱資安標準，並於台灣資通產業標準協會辦理產業標準制定工作。

TAICS TS-0031 「智慧音箱資安標準」(以下簡稱本標準)引用國際物聯網相關標準與規範[1-10]，並參考相關資料(1-6)，依實體安全、系統安全、通訊安全、身分鑑別與授權機制安全、隱私保護、行動應用程式安全等安全構面，訂定產品安全要求，以協助相關產業確保智慧音箱之資安防護。

1. 適用範圍

本標準規定智慧音箱之資訊安全要求；其中，智慧音箱指具備連網、語音輸入與內建人工智慧語音助理功能之音箱。

本標準適用於智慧音箱本體、產品應用程式、音箱對外之通訊傳輸網路；雲端伺服器與不具喇叭外觀之音箱(如具音箱功能之智慧冰箱等)，則不在本標準規範之範圍。本標準適用範圍如圖 1 所示。

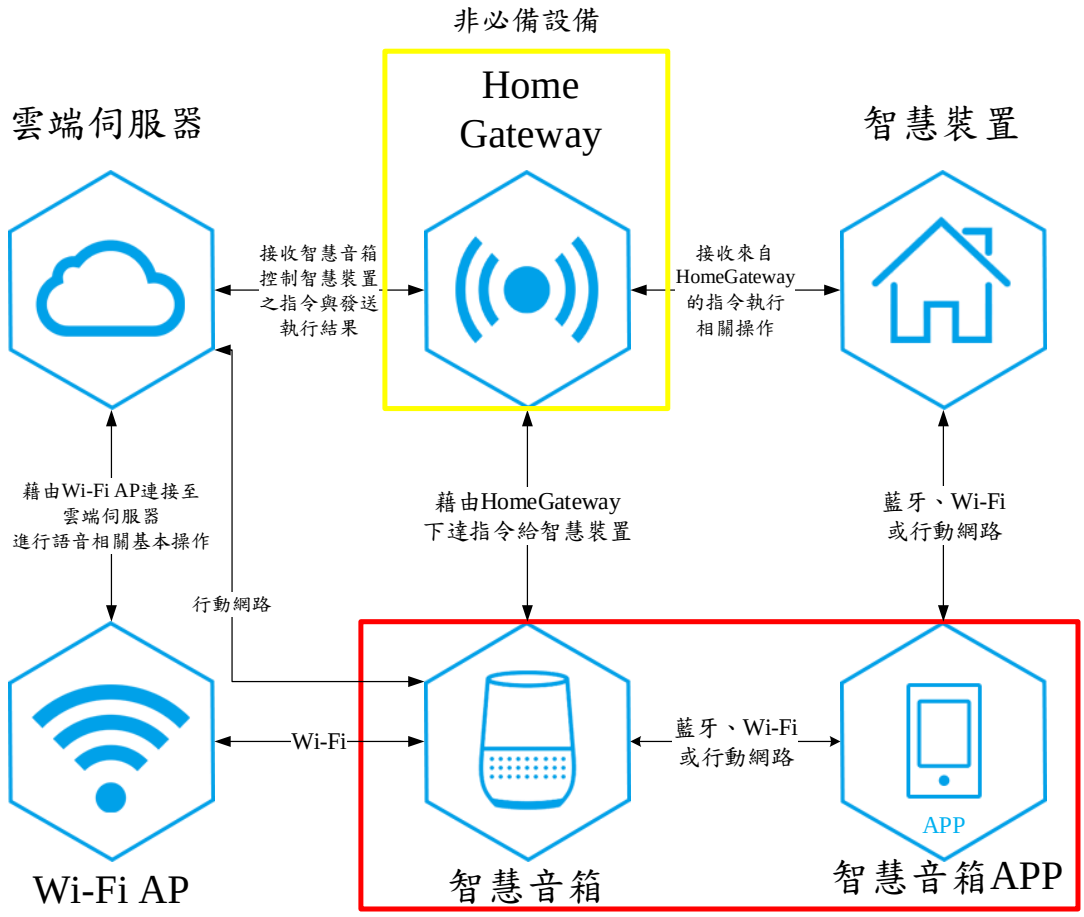

圖 1 適用範圍示意圖

2. 引用標準

以下引用標準係本標準必要參考文件。如所列標準標示年版者，則僅該年版標準予以引用。未標示年版者，則依其最新版本(含補充增修)適用之。

[1] NIST FIPS 140-2 Security Requirements for Cryptographic Module, Annex A: Approved Security Functions, 2019/06
[2] ETSI TS 103 645 CYBER; Cyber Security for Consumer Internet of ThingsV1.1.1. 2019/02
[3] ISO/IEC 27030 Information technology - Security techniques - Guidelines for security and privacy in Internet of Things (IoT), 2018/01
[4] ISO/IEC 15408-1: 2014 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model, 2014/01
[5] IEC 62443-4-2:2019 Security for industrial automation and control systems –Part 4-2: Technical security requirements for IACS components, 2019/02
[6] IEEE Standard Association, P2413.1 Standard for a Reference Architecture for Smart City (RASC), 2018/06
[7] NIST, Guide to Bluetooth Security, SP 800-121 Revision 2, 2017/05
[8] FIRST.org, Common Vulnerability Scoring System v3.1, 2019/11
[9] OECD Privacy Guidelines, 2013/03
[10] 行動應用資安聯盟，行動應用 App 基本資安檢測基準 V3.1, 2019/09

3. 用語及定義

下列用語及定義適用於本標準。

3.1 歐盟資料保護監督機關(European Data Protection Supervisor, EDPS)

歐盟資料保護監督機關為一獨立的監督機構，其主要目的是確保歐洲機構與機構間在處理個人數據和制訂新政策時尊重隱私權和數據保護權。

3.2 除錯模式(Debug Mode)

指產品處於開發或修補階段之模式。於此模式中系統資源之存取可不受限，且亦顯示錯誤訊息以提供除錯使用，又稱工程模式(Engineering Mode)。

3.3 前向安全(Forward Secrecy, FS)

指通行碼或金鑰在某個時間點不慎洩露時，過往的通訊依然是安全，不會因此而洩露過去的通信資料。

3.4 敏感性資料(Sensitive Data)

指洩漏時可能對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。

3.5 隱私資料(Privacy Data)

指私人資訊，此一資訊之洩露會使個人生活私密領域受他人侵擾，本標準所指隱私包括，但不限於裝置經緯度、使用者辨識資訊、麥克風錄音、語音對話訊息等。

3.6 通行碼(Password)

指一組字元串，能使系統辨識用戶身分，並進一步控管用戶存取系統之權限[6]。

3.7 預設通行碼(Default Password)

指產品出廠預先設定之通行碼，即在用戶初次將其連上網路，且在未更改任何設定的情況下，用以登入系統之通行碼。

3.8 美國國家脆弱性資料庫(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)提供的國家脆弱性資料庫，負責常見脆弱性與漏洞之資料的發布及更新。

3.9 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[8]，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。

3.10 嚴重性評等(Severity Rating)

指漏洞評鑑系統之評比分數皆有其對應之嚴重性等級，分別是 0 分為無(none)嚴重性、0.1-3.9 分為低(low)嚴重性、4.0-6.9 分為中(medium)嚴重性、7.0-8.9 分高(high)嚴重性及 9.0-10.0 為重大(critical)嚴重性。

3.11 安全區域(Secure Zone)

指與正常作業環境隔離出的區域，僅用於執行安全性相關操作，例：加解密、金鑰管理、完整性檢查，並提供敏感性資料儲存。

3.12 中間人攻擊(Man-in-The-Middle attack, MITM attack)

指攻擊者與通訊的兩端分別建立獨立的連線，並交換所收到的資料，使通訊兩端認為他們正在通過一個私密的連線與對方直接對話，但事實上整個對談都被攻擊者完全控制。在中間人攻擊中，攻擊者可以攔截通訊雙方的通話，並插入新的內容。

3.13 Wi-Fi 保護存取協定 2(Wi-Fi Protected Access 2, WPA2)

指一種保護無線網路(Wi-Fi)存取安全的技術標準，WPA2 所採用的加密方式由 2 個部份組成，一個是鑑別訊息之完整性及來源，另一個是保護傳送中之資料不被窺視之加密演算法。

3.14 政府組態基準(Government Configuration Baseline, GCB)

資通訊終端設備(例：個人電腦)一致性安全設定規範(例：通行碼長度、更新期限等)，以降低駭客入侵與導致資安事件之疑慮(5)。

3.15 安全通道(Security Tunnel)

為網際網路通訊端點與端點(End-to-End)間，兼顧資料隱密性及完整性所建立之通道。

3.16 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。

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，透過最適合之安全組合，確保產品達到安全之要求。

4.1 安全等級概述

安全等級總表，如表 1 所示，第一欄為安全構面，包括：(1)實體安全、(2)系統安全、(3)通訊安全、(4)身分鑑別與授權機制安全、(5)隱私保護、(6)行動應用程式安全；第二欄為安全要求分項，係依第一欄各安全構面設計對應之安全要求項目；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，需依循下節 5.1 至 5.6 之技術規範內容。

表 1 安全要求等級總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
實體安全	5.1.1 實體埠之安全管控	-	5.1.1.1	-
系統安全	5.2.1 韌體更新功能	5.2.1.1	-	-
	5.2.2 韌體更新檔之完整性及合法性	-	5.2.2.1	-
	5.2.3 韌體檔案加密	-	5.2.3.1	-
	5.2.4 作業系統與網路服務安全	5.2.4.1	-	-
	5.2.5 敏感性資料之儲存加密	-	5.2.5.1	5.2.5.2
	5.2.6 通訊協定安全	-	5.2.6.1 5.2.6.2	-
通訊安全	5.3.1 HTTP 傳輸安全	5.3.1.1	-	-
	5.3.2 最小化網路服務連接埠	5.3.2.1	-	-
	5.3.3 憑證認證應具 MITM 防護	5.3.3.1	-	-
	5.3.4 敏感性資料之 Wi-Fi 傳輸安全	-	5.3.4.1	-
	5.3.5 藍牙傳輸安全	-	5.3.5.1	-
身分鑑別與授權機制安全	5.4.1 預設通行碼安全	5.4.1.1	-	-
	5.4.2 網頁管理頁面之身分鑑別機制	5.4.2.1	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
		5.4.2.2		
	5.4.3 敏感性功能之身分鑑別機制	-	5.4.3.1	5.4.3.2
隱私保護	5.5.1 隱私保護條款與機制	5.5.1.1 ~ 5.5.1.12	-	5.5.1.13
行動應用程式安全	5.6.1 行動應用 App 基本資安認證		5.6.1.1	5.6.1.2

4.1.1 安全構面

(a) 實體安全：係指運用音箱實體通訊埠之安全。

(b) 系統安全：係指智慧音箱之作業系統、網路服務、更新服務及韌體程式設計等安全需求。

(c) 通訊安全：係指智慧音箱通訊協定與系統之安全需求，如 HTTP、Wi-Fi、Bluetooth 等。

(d) 身分鑑別與授權機制安全：係指智慧音箱使用者透過各種人機介面，存取設備功能之安全需求。

(e) 隱私保護：係指智慧音箱所儲存個人隱私資料之安全需求，包括使用者之身分和語音資料。

(f) 行動應用程式安全：係指提供使用者用於與智慧音箱溝通之手機 APP 的安全需求。

4.1.2 安全要求分項

依安全構面所設計對應之安全要求要項目，且每一安全要求分項包含一個以上之安全要求項目。

4.1.3 安全等級

安全等級考慮(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 級安全要求所對應資安事件較容易發生且造成損失較高，2 級安全要求所對應資安事件的發生機率與造成損失為一般，3 級安全要求所對應資安事件較不容易發生且造成損失也較低。其對應之列即其所應符合的安全要求分項，安全等級越高代表安全性越佳，欲符合較高等級之安全要求必須先滿足較低安全等級要求。

5. 標準規範

本節詳盡載明智慧音箱為符合安全功能驗證應採取的共通方法，所有智慧音箱應符合本節中所有安全要求。

5.1 實體安全

5.1.1 實體埠之安全管控

5.1.1.1 產品提供使用者透過實體埠存取系統功能，須具備身分鑑別機制。

5.2 系統安全

5.2.1 韌體更新功能

5.2.1.1 產品需具備韌體更新功能。

5.2.2 韌體更新檔之完整性及合法性

5.2.2.1 產品需具備自我驗證韌體完整性及合法性之功能，且需具備可追蹤韌體更新紀錄之管理功能。

5.2.3 韌體檔案加密

5.2.3.1 韌體內之設定檔或資料庫檔案，不得包含未加密之敏感性資料或可識別之隱私資料。

5.2.4 作業系統與網路服務安全

5.2.4.1 產品之作業系統與網路服務，不得有美國國家弱點資料庫所公布及更新的常見弱點與漏洞資料，且 CVSS 評分為 9.0 以上。

5.2.5 敏感性資料之儲存加密

5.2.5.1 產品所儲存之敏感性資料不得明文儲存，而保護資料的加密方式需採用 FIPS 140-2 Annex A 核准之加密演算法。

5.2.5.2 敏感性資料需存放於產品的安全區域(Secure Zone)，與正常作業環境中隔離。

5.2.6 通訊協定安全

5.2.6.1 產品之 Wi-Fi 通訊協定，不得有錯誤處理漏洞，包括檢視訊息長度、訊息識別碼及關鍵協定屬性等欄位，導致產品因發生異常而服務中斷的情形。

5.2.6.2 產品之藍牙通訊協定，不得有錯誤處理漏洞，包括檢視訊息長度、訊息識別碼及關鍵協定屬性等欄位，導致產品因發生異常而服務中斷的情形。

5.3 通訊安全

5.3.1 HTTP 傳輸安全

5.3.1.1 網路傳輸預設需通過安全通道之驗證，且安全通道版本需使用 TLS 1.2 同等或以上之安全通訊協定，同時金鑰交換協議應支援前向安全功能(Forward Secrecy)。

5.3.2 最小化網路服務連接埠

5.3.2.1 產品出廠所開啟之網路通訊埠，應為設備商提供必要服務之所需，並載明於產品文件中，以防止產品因網路介面設定不當而被侵入。

5.3.3 憑證認證應具 MITM 防護

5.3.3.1 產品憑證應具備有效鑑別性，在遭受竄改或置換憑證時，能有效阻擋連線。

5.3.4 敏感性資料之 Wi-Fi 傳輸安全

5.3.4.1 無線網路傳輸的安全機制預設需採用 WPA2(含)以上之加密機制。

5.3.5 藍牙傳輸安全

5.3.5.1 藍牙傳輸須採用 AES128 以上之加密演算法。

5.4 身分鑑別與授權機制安全

5.4.1 預設通行碼安全

5.4.1.1 設備商所生產之裝置，若以通行碼作為身分鑑別與授權機制，其預設通行碼不可相同；或者首次成功取得產品存取之授權，需強制更改預設通行碼。

5.4.2 網頁管理頁面之身分鑑別機制

5.4.2.1 網頁管理介面需具備身分鑑別機制並具備抵抗重送攻擊的能力。

5.4.2.2 若以通行碼作為網頁管理頁面之身分鑑別機制，通行碼強度需符合政府組態基準(5)原則，包括最小通行碼長度原則(CCE-33789-9)、複雜性需求原則(CCE-33777-4)及強制執行通行碼歷程記錄原則(CCE-35219-5)。

5.4.3 敏感性功能之身分鑑別機制

5.4.3.1 觸發智慧音箱之金流交易功能(如：語音購物等)時，需經過身分鑑別機制。

5.4.3.2 觸發智慧音箱之人身安全功能(如：家用安防設備等)時，需經過多因子鑑別機制鑑別。

5.5 隱私保護

5.5.1 隱私保護條款與機制

5.5.1.1 符合國家個人資料保護法及經濟合作暨發展組織 (Organization for Economic Co-operation and Development, OECD)[9]公布之限制蒐集原則，於蒐集個人資料時，確認有合法、公正、通知當事人並獲得使用者同意。

5.5.1.2 符合國家個人資料保護法及 OECD 公布之目的明確原則，於隱私權聲明內需聲明個人資料之蒐集目的，最遲應於蒐集時提醒。

5.5.1.3 符合國家個人資料保護法及 OECD 公布之利用限制原則，於隱私權聲明內需聲明個人資料除得當事人同意或法律另有規定者外，不得為蒐集目的外之揭露或利用。

5.5.1.4 符合國家個人資料保護法及 OECD 公布之安全措施原則，於隱私權聲明內需聲明個人資料應予以合理的安全措施加以保護，以防止個人資料被竊取、竄改、毀損、滅失或洩漏等危險。

5.5.1.5 符合國家個人資料保護法及 OECD 公布之公開原則，於確認隱私權聲明內需聲明有關個人資料之蒐集、處理、或利用及政策之制定，對社會大眾為公開。

5.5.1.6 符合國家個人資料保護法及 OECD 公布之個人參與原則，於隱私權聲明內需包含同意使用者關於自己的資料得享有得於合理期間內管理有關於自己的資料，可要求資料控制者對於資料加以刪除、修改、完整及補充。

5.5.1.7 符合國家個人資料保護法及 OECD 公布之責任原則，於聲明書內聲明負責提供使用者之個人資料管理之責任。

5.5.1.8 符合國家個人資料保護法及 OECD 公布之資料品質原則，於聲明書內容，需由使用者確認個人資料之正確、完整及保持全新狀態。

5.5.1.9 智慧音箱應有不同提示，顯示設備處於服務偵測狀態或服務狀態。

5.5.1.10 智慧音箱應有實體麥克風關閉功能，且於麥克風關閉狀態時，不得有任何收音及上傳之行為。

5.5.1.11 智慧音箱在服務偵測狀態，未偵測到喚醒詞前，不得有任何資料上傳行為。

5.5.1.12 智慧音箱應聲明在偵測到喚醒詞，進入服務狀態後，收集語音資料時間長度與資料上傳機制。

5.5.1.13 智慧音箱對外傳輸資料時，應有適當提醒告知之機制。

5.6 行動應用程式安全

5.6.1 行動應用 App 基本資安認證

5.6.1.1 智慧音箱搭配之手機 APP 需通過行動應用資安聯盟所推出之行動應用 App 基本資安檢測基準 V3.1[10]L2 之認證。

5.6.1.2 智慧音箱搭配之手機 APP 需通過行動應用資安聯盟所推出之行動應用 App 基本資安檢測基準 V3.1 L3 之認證。

附錄 A
(參考)
安全要求分項與各標準規範對照表

表 A.1　技術要求事項與各標準規範對照表

安全構面	安全要求分項	判定標準	參考來源	參考內容
實體安全	實體埠之安全管控	本標準 5.1.1.1	OWASP IoT Top Ten(3)	10：Lack of Physical Hardening
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements (4)	15. Malformed Input Testing
系統安全	韌體更新功能	本標準 5.2.1.1	OWASP IoT Top Ten	4：Lack of Secure Update Mechanism
			IEC 62443-4-2 [5]	FR 3 - System integrity
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	11. Product Management
	韌體更新檔之完整性及合法性	本標準 5.2.2.1	OWASP IoT Top Ten	4：Lack of Secure Update Mechanism
			IEC 62443-4-2	FR 3 - System integrity
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	11. Product Management
	韌體檔案加密	本標準 5.2.3.1	OWASP IoT Top Ten	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 4 - Data confidentiality
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	10. Cryptography
	作業系統與網路服務安全	本標準 5.2.4.1	OWASP IoT Top Ten	2：Insecure Network Services 5：Use of Insecure or Outdated Components
			IEC 62443-4-2	FR 3 - System integrity

安全構面	安全要求分項	判定標準	參考來源	參考內容
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	12. Vendor Product Risk Management Process
	敏感性資料之儲存加密	本標準 5.2.5.1	OWASP IoT Top Ten	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 4 - Data confidentiality
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	10. Cryptography
		本標準 5.2.5.2	IEC 62443-4-2	FR 1 - Identification and authentication control
	通訊協定安全	本標準 5.2.6.1	UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	12. Vendor Product Risk Management Process
		本標準 5.2.6.2	UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	12. Vendor Product Risk Management Process
通訊安全	HTTP 傳輸安全	本標準 5.3.1.1	OWASP IoT Top Ten	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 3 - System integrity
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	9. Remote Communication
	最小化網路服務連接埠	本標準 5.3.2.1	OWASP IoT Top Ten	2：Insecure Network Services
			IEC 62443-4-2	FR 7 - Resource availability
	憑證認證應具 MITM 防護	本標準 5.3.3.1	OWASP IoT Top Ten	3：Insecure Ecosystem Interfaces
			IEC 62443-4-2	FR 1 - Identification and authentication control
			UL 2900-1 Standard for Software Cybersecurity	9. Remote Communication

安全構面	安全要求分項	判定標準	參考來源	參考內容
			for Network-Connectable Products, Part 1: General Requirements	
	敏感性資料之 Wi-Fi 傳輸安全	本標準 5.3.4.1	OWASP IoT Top Ten	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 3 - System integrity
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	9. Remote Communication
	藍牙傳輸安全	本標準 5.3.5.1	OWASP IoT Top Ten	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 3 - System integrity
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	9. Remote Communication
身分鑑別與授權機制安全	預設通行碼安全	本標準 5.4.1.1	OWASP IoT Top Ten	1：Weak, Guessable, or Hardcoded Passwords
			IEC 62443-4-2	FR 1 - Identification and authentication control
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	8. Access Control, User Authentication and User Authorization
	網頁管理頁面之身分鑑別機制	本標準 5.4.2.1	OWASP IoT Top Ten	3：Insecure Ecosystem Interfaces
			IEC 62443-4-2	FR 1 - Identification and authentication control
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	8. Access Control, User Authentication and User Authorization
		本標準 5.4.2.2	OWASP IoT Top Ten	1：Weak, Guessable, or Hardcoded Passwords
			IEC 62443-4-2	FR 1 - Identification and authentication control

安全構面	安全要求分項	判定標準	參考來源	參考內容
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	8. Access Control, User Authentication and User Authorization
	敏感性功能之身分鑑別機制	本標準 5.4.3.1	OWASP IoT Top Ten	3：Insecure Ecosystem Interfaces
			IEC 62443-4-2	FR 1 - Identification and authentication control
			UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	8. Access Control, User Authentication and User Authorization
			IEC 62443-4-2	FR 1 - Identification and authentication control
隱私保護	隱私保護條款與機制	本標準 5.5.1.1 ~ 本標準 5.5.1.13	OECD Privacy Guidelines[9]	Collection Limitation Data Quality Individual Participation Purpose Specification Use Limitation Security Safeguards Openness Accountability
行動應用程式安全	行動應用 App 基本資安認證	本標準 5.6.1.1、5.6.1.2	行動應用 App 基本資安檢測基準 V3.1 [10]	ALL

附錄 B
(參考)
風險來源分析與資安需求表

針對目前已知威脅，依照威脅描述、威脅目標、攻擊技術、防護對策、參考資料與安全構面歸類於表 B-1。

表 B-1 風險來源分析與資安需求表

威脅描述	威脅目標	攻擊技術	防護對策	安全構面
除錯模式無身分鑑別	系統存取權 敏感性資料	藉由 JTAG、UART 等除錯介面取得系統存取權	移除除錯介面 加上身分鑑別	實體安全
	參考來源:DEF CON 26 Breaking Smart Speaker - Exploit Amazon Echo https://github.com/tencentbladeteam/Exploit-Amazon-Echo			
韌體無更新機制	系統存取權 敏感性資料	藉由各組件漏洞取得系統存取權	更新組件到最新版	系統安全
	參考來源:ENISA Baseline Security Recommendations for IoT https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot			
韌體無正確性與完整性檢查機制	系統存取權 敏感性資料	竄改韌體取得系統存取權	防止韌體遭到竄改	系統安全
	參考來源:Trend Micro, The Sound of a Targeted Attack https://documents.trendmicro.com/assets/pdf/The-Sound-of-a-Targeted-Attack.pdf			
韌體無加密機制	系統存取權 敏感性資料	反組譯韌體取得系統存取權	韌體加密	系統安全
	參考來源:Trend Micro, The Sound of a Targeted Attack https://documents.trendmicro.com/assets/pdf/The-Sound-of-a-Targeted-Attack.pdf			
通訊協定無輸入判斷機制	系統正常性	藉由輸入錯誤的資料導致相關服務當機無法正常使用	加入防止異常輸入判斷機制	系統安全
	參考來源:ENISA Baseline Security Recommendations for IoT https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot			
通訊無加密或加密強度不足	敏感性資料	通訊無加密或加密強度不足遭破解取得敏感性資料	採用足夠強度之通訊加密技術	通訊安全

	參考來源:Trend Micro, The Sound of a Targeted Attack https://documents.trendmicro.com/assets/pdf/The-Sound-of-a-Targeted-Attack.pdf			
開啟不必要網路服務	系統存取權敏感性資料	設備開啟不必要之網路服務(Telnet、SSH、FTP等)導致被破解入侵	服務最小化 只開啟必備服務	系統安全
	參考來源:Trend Micro, The Sound of a Targeted Attack https://documents.trendmicro.com/assets/pdf/The-Sound-of-a-Targeted-Attack.pdf			
中間人攻擊(MITM)	敏感性資料	無使用憑證綁定或憑證為無效憑證，導致遭置換憑證遭受中間人攻擊	使用有效憑證認證	通訊安全
	參考來源:Trend Micro, Infosec Guide: Defending Against Man-in-the-Middle Attacks https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/infosec-guide-defending-against-man-in-the-middle-attacks			
Wi-Fi 連線無加密或加密強度不足	敏感性資料	Wi-Fi 無加密或加密強度不足遭破解取得敏感性資料	採用足夠強度之Wi-Fi 加密技術	通訊安全
	參考來源:Trend Micro, Vulnerabilities in WPA2 Reportedly Expose Wi-Fi-Enabled Devices to Eavesdropping https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/vulnerabilities-in-wpa2-reportedly-expose-wi-fi-enabled-devices-to-eavesdropping			
藍牙傳輸無加密	敏感性資料	藍牙無加密或加密強度不足遭破解取得敏感性資料	採用足夠強度之藍牙加密技術	通訊安全
	參考來源:Trend Micro, Bluetooth Vulnerabilities Expose Billions of Devices to Hacking https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/blueborne-bluetooth-vulnerabilities-expose-billions-of-devices-to-hacking			
內建簡單預設通行碼	系統存取權敏感性資料	內建簡單預設通行碼且初次使用無強制更改導致遭破解	採用不同預設通行碼或初次使用需更改預設通行碼	身分鑑別與授權機制

	參考來源:Trend Micro, The Sound of a Targeted Attack https://documents.trendmicro.com/assets/pdf/The-Sound-of-a-Targeted-Attack.pdf			
登入機制無防止重送	系統存取權敏感性資料	登入機制無防止重送攻擊機制，遭強力破解	加入防止重送機制	身分鑑別與授權機制
	參考來源:Cyber Security Community, Cookie Hijacking https://www.securitycommunity.tcs.com/infosecsoapbox/articles/2017/01/05/cookie-hijacking-learning-through-replay-attack-examples			
通行碼強度與複雜度不足	系統存取權敏感性資料	通行碼強度與複雜度不足，遭強力破解	通行碼需大於 8 碼，並包含英文大小寫、特殊符號	身分鑑別與授權機制
	參考來源:Trend Micro, The Sound of a Targeted Attack https://documents.trendmicro.com/assets/pdf/The-Sound-of-a-Targeted-Attack.pdf			
隱私政策不足	敏感性資料	隱私政策不明，導致使用者隱私資料洩漏與不正當使用	說明隱私資料使用範圍與相關規定	隱私安全
	參考來源:iThome, 傳 Amazon 以數千員工聽取 Echo 用戶對話來訓練 Alexa https://www.ithome.com.tw/news/129934			
音箱 APP 缺乏安全	系統存取權敏感性資料	智慧音箱大多需搭配APP使用，應用程式安全性不足也會一併影響到音箱安全	APP 通過基本資安檢測	行動應用程式安全
	參考來源:DEF CON 26 Breaking Smart Speaker - Exploit Amazon Echo https://github.com/tencentbladeteam/Exploit-Amazon-Echo			
缺乏個資使用透明度	敏感性資料	隱私政策不明，導致使用者隱私資料洩漏與不正當使用	說明隱私資料使用範圍與相關聲明	隱私安全
	參考來源:European Data Protection Supervisor - TechDispatch #1: Smart Speakers and Virtual Assistants			
個資數據保留過久	敏感性資料	隱私政策不明，導致使用者隱私資料洩漏與不正當使用	說明隱私資料保存時間相關聲明	隱私安全
	參考來源:European Data Protection Supervisor - TechDispatch #1: Smart Speakers and Virtual Assistants			
缺乏適當的同意管理機制	敏感性資料	隱私政策不明，導致使用者隱私	說明隱私資料使用範圍與相關聲明	隱私安全

		資料洩漏與不正當使用		
	參考來源:European Data Protection Supervisor - TechDispatch #1: Smart Speakers and Virtual Assistants			
未經同意就執行處理	敏感性資料	隱私政策不明，導致使用者隱私資料洩漏與不正當使用	說明隱私資料使用範圍與相關聲明	隱私安全
	參考來源:European Data Protection Supervisor - TechDispatch #1: Smart Speakers and Virtual Assistants			
重新利用個資數據	敏感性資料	隱私政策不明，導致使用者隱私資料洩漏與不正當使用	說明隱私資料使用範圍與相關聲明	隱私安全
	參考來源:European Data Protection Supervisor - TechDispatch #1: Smart Speakers and Virtual Assistants			
個人資料的安全	敏感性資料	隱私政策不明，導致使用者隱私資料洩漏與不正當使用	說明隱私資料使用範圍與相關聲明	隱私安全
	參考來源:European Data Protection Supervisor - TechDispatch #1: Smart Speakers and Virtual Assistants			
可能遭大規模監視	敏感性資料	隱私政策不明，導致使用者隱私資料洩漏與不正當使用	說明隱私資料使用範圍與相關聲明	隱私安全
	參考來源:European Data Protection Supervisor - TechDispatch #1: Smart Speakers and Virtual Assistants			
資料數據的保護源自於設計	敏感性資料	隱私政策不明，導致使用者隱私資料洩漏與不正當使用	說明隱私資料使用範圍與相關聲明	隱私安全
	參考來源:European Data Protection Supervisor - TechDispatch #1: Smart Speakers and Virtual Assistants			

參考資料

(1) NIST, Cybersecurity Framework, Version 1.1, 2018/04

(2) U.S. Department of Homeland Security, Strategic Principles for Securing the Internet of Things (IoT), Version 1.0, 2016/11

(3) OWASP, OWASP Internet of Things Project, 2018/03

(4) UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, 2017/07

(5) 政府組態基準 GCB_帳戶原則與精細密碼原則設定說明(V1.0), 2017/01

(6) EUROPEAN DATA PROTECTION SUPERVISOR, TechDispatch #1: Smart Speakers and Virtual Assistants, 2019/07
https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-1-smart-speakers-and-virtual_en

版本修改紀錄

版本	時間	摘要
v1.0	2020/09/18	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