CNS16190

中華民國國家標準 CNS 16190

消費者物聯網之網宇安全：基準要求事項

Cybersecurity for consumer internet of things: Baseline requirements
中華民國112年1月13日制定公布
Date of Promulgation:202313

目錄

節次
前言
簡介

前言

本標準係依標準法之規定，經國家標準審查委員會審定，由主管機關公布之中華民國國家標準。
依標準法第四條之規定，國家標準採自願性方式實施。 但經各該目的事業主管機關引用全部或部分內容為法規者，從其規定。
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，主管機關及標準專責機關不負責任何或所有此類專利權、商標權與著作權之鑑別。

簡介

- 當家庭中更多裝置連接至網際網路時，物聯網 (internet of things, IoT) 之網宇安全 (cyber security) 日益受到關注。人們將其個人資料委託予遞增之線上裝置及服務。傳統上離線之產品及裝置現已連接網路，因而需設計為能抵禦網宇威脅。
- 本標準將網際網路連接式消費裝置安全公認之良好實務作法，彙整成 1 組高層次控制措施。本標準旨在支援參與消費者 Io T 開發及製造的所有各方，並提供有關保護其產品之指引。
- 該等控制措施主要係結果導向，而非規定性，給予組織彈性創新並實作適切其產品之安全解決方案。
- 本標準並非旨在解決與消費者 IoT相關聯之所有安全挑戰。其亦未聚焦於防止長期/複雜之攻擊，且未防止對裝置持續實體接取的攻擊，而焦點係最重要之技術控制措施及組織政策，以因應最重大且最普遍的安全缺陷。總體而言，考量安全之基準層級，旨在防止於基本設計弱點上的初階攻擊(諸如使用易於猜出之通行碼)。

- 本標準提供適用於所有消費者 IoT 裝置之1組基準控制措施。其旨在藉由其他標準加以補充，該等標準係對特定裝置，定義更特定控制措施且完全可測試及/或可查證之要求事項，其將與本標準一起有助於保證方案的制定。
- 許多消費者IoT裝置及其相關聯服務處理並儲存個人資料，本標準協助確保此等裝置符合一般資料保護規則 (general data protection regulation, GDPR) [7]。 於設計即保護安全係本標準所支持之重要原則。
- ETSI TS 103 701 [19] 提供有關如何依本標準中之評鑑，並確保 IoT 產品的指引 。
- 本標準中之控制措施係於審查有關 IoT 安全及隱私所發布的標準、建議及指引之後所制定者，其包括： ETSI TR 103305-3 [1] 、 ETSI TR 103309 [2] 、 ENISA 基準安全建議 [8] 、英國數位文化媒體暨體育部 (DCMS) 安全設計報告 [9]、IoT安全基金會符合性框架 [10] 、 GSMA IoT 安全指引及評鑑 [11] 、 ETSI TR 103533 [12] 、 DIN SPEC 27072[20] ，以OWASP IoT [23]。
    - 備考： IoT 安全標準、建議及指引之對映可查詢ENISA Baseline Security Recommendatio ns for IoT–Interactive Tool [15] 及 Copper Horse Mapping Security & Privacy in the Internet of Things [14] 等網站 。
- 隨著消費者 IoT產品變得越來越安全，預期本標準中目前之建議控制措施，於本標準之未來修訂版將成為必備控制措施。

1. 適用範圍:

本標準針對連接至網路基礎設施 (諸如網際網路或家庭網路) 之消費者 IoT裝置，以及其與相關聯服務的互動，規定高層次安全及資料保護控制措施。相關聯服務非屬本標準適用範圍 。 消費者IoT裝置示例之非窮舉表列包括：

- 所連接之兒童玩具及嬰兒監視器。
- 所連接之煙霧偵測器、門鎖及窗戶感測器。
- 連接多個裝置之 Io T 閘道器、基地臺及集線器 。
- 智慧型相機、電視及揚聲器。
- 穿戴式健康追蹤器。
- 所連接之家庭自動化及告警系統，特別是其閘道器及集線器。
- 所連接之電器，諸如洗衣機及冰箱。

- 智慧型家庭助理。

此外，本標準闡明特定於受限制裝置之安全考量。例：窗戶接觸感測器、淹水感測器及能源開關通常為受限制裝置。
針對參與消費者 IoT 開發及製造之組織，本標準透過示例及解釋文字，提供有關如何實作該等控制措施的基本指引 。 表 B.1 針對讀者提供綱要，以提供有關控制措施實作之資訊。
非屬消費者 IoT裝置之裝置，例：主要用於製造、醫療保健或其他工業應用的裝置，非屬本標準範圍。
本標準主要係為協助保護消費者所制定，然而消費者IoT之其他使用者同樣受益於此處所列控制措施的實作。
本標準納入附錄A (參考)，以提供第4節、第5節及第6節 (規定)之全景。 附錄A包含裝置及參考架構示例，並包括各狀態資料儲存的裝置狀態之示例模型。

2. 引用標準:

本標準無引用標準。

3. 用語及定義、符號及縮寫:

3.1 用語及定義:

下列用語及定義適用於本標準。

3.1.1 管理者 (administrator):

具裝置使用者可能達到之最高等級特殊權限的使用者，此可意指其能變更與預期功能性相關的任何組態。

3.1.2 相關聯服務 (associated service):

與裝置一起成為整體消費者 IoT 產品之一部分的數位服務，通常要求提供該產品之預期功能性。例1.相關聯服務可包括行動應用程式及雲端運算/儲存，以及第三方應用程式介面(API)。例2.裝置傳輸遙測資料至由裝置製造者所選定之第三方服務。此服務係相關聯服務。

3.1.3鑑別機制 (authentication mechanism):

用以證明個體之真確性的方法。
備考：〝個體〞可為使用者抑或機器。
例：鑑別機制可為請求通行碼、掃描行動條碼 (QR code) 或使用生物特徵之指紋掃描器。

3.1.4 鑑別值 (authentication value):

鑑別機制所使用之屬性的個別值。
例： 當鑑別機制請求通行碼時，鑑別值可為字元串。 當鑑別機制為生物特徵指紋辨識時，鑑別值可為左手食指指紋。

3.1.5 最佳實務密碼學 (best practice cryptography):

適合於相對應之使用案例的密碼學，並無以目前可用技術進行可行攻擊的跡象。備考 1. 此不僅意指所使用之密碼式基元 (cryp to grap hic p rimitive) ，且亦包含實作、金鑰產生及金鑰處理。
備考 2.多個組織 (諸如 SDO 及公務機構) 維護可使用之密碼方法的指導及目錄。例： 裝置製造者以IoT 平台提供之通訊協定及密碼程式館，且該密碼程式館及協定已針對可行的攻擊 (諸如重演) 進行評鑑 。

3.1.6 受限制裝置 (constrained device):

由於預期使用之限制，於資料處理能力、資料通訊能力、資料儲存能力，抑或與使用者互動的能力等方面具實體限制之裝置。
備考 1.實體限制可能由於電源、電池壽命、處理能力、實體接觸、有限功能性、有限記憶體或有限網路頻寬。此等限制可要求受限制裝置由另一裝置支援，諸如基地臺或配套裝置。
例1. 使用者無法為窗戶感測器之電池充電或更換之。此係受限制之裝置 。
例2. 由於儲存體限制，裝置無法更新其軟體，導致硬體更換或網路隔離成為管安全脆弱性之唯一選項。
例3. 低耗電裝置使用電池，以使其可部署於某些位置。執行高耗電密碼式運算，將迅速縮短電池壽命，因此其依賴基地臺或集線器執行更新之驗核。
例4. 裝置無顯示幕以驗核藍牙配對之繫結碼 (binding code) 。
例5. 裝置無法輸入 (諸如經由鍵盤) 鑑別資訊 。
考2. 具有線電源且可支援IP式協定，以及此等協定使用之密碼式基元的裝置，不受限制。
例6. 裝置係由主電源供電，且主要使用 TLS (傳送層安全) 通訊 。

3.1.7 消費者 (consumer):

為貿易、營運、工藝或專業外之目的而行事的自然人。
備考：包括任何規模之企業在內的組織使用消費者 IoT。例：智慧型電視經常部署於會議室中，而家庭安全套件可保護小型營運之場所。

3.1.8 消費者 IoT 裝置 (consumer IoT device):

與相關聯服務有關係之連網(可連網)裝置，且通常由消費者於家中使用或作為電子穿戴的裝置。
備考 1.消費者 IoT 裝置通常亦用於營運全景。 此等裝置仍歸類為消費者IoT裝置。
備考 2.消費者 IoT 裝置通常可供消費者於零售環境中購買。 消費者IoT裝置亦可專業使用及/或安裝 。

3.1.9 關鍵安全參數 (critical security parameter):

與安全相關之秘密資訊，遭揭露或修改，可能危及安全模組的安全。
例：秘密密碼金鑰、鑑別值 (諸如通行碼、 PIN) 、憑證之私密組件 。

3.1.10 除錯介面 (debug interface):

製造者於開發期間與裝置通訊，或執行裝置問題檢修所使用之實體介面，不用於消費者導向的功能之一部分。
例：測試點、 UART 、 SWD 、 JTAG 。

3.1.10 定義之支援期間 (defined support period):

製造者將提供安全更新之最短時間長度，以期間或結束日期表示之。
備考：此定義聚焦於安全層面，而非與產品支援相關之其他層面，諸如保固。

3.1.11 裝置製造者 (device manufacturer):

建立所組裝最終消費者 Io T 產品之個體，其可能包含許多其他供應者的產品及組件。

3.1.12 原廠預設 (factory default):

原廠重置或最終生產 / 組裝之後裝置之狀態 。
備考：此包括組裝後呈現之實體裝置及軟體 (包括韌體) 。

3.1.13 初始化 (initialization):

對使用者或網路接取之操作及選項設定鑑別特徵，啟動裝置的網路連接性之過程。

3.1.14 初始化狀態 (initialized state):

裝置初始化後之狀態。

3.1.15 IoT 產品 (IoT product):

消費者 Io T 裝置及其相關聯服務 。

3.1.16 可隔離 (isolable):

能由其所連接之網路中移除，其中所導致的任何功能性喪失僅與該連接性相關，與其主要功能性無關；或者，若且唯若能確保該環境內裝置之完整性，則能與其他裝置一起置於自給自足 (self-contained) 的環境中。
例：智慧型冰箱具觸控螢幕介面，可連接網路。此介面可於不停止冰箱保持內容物冷藏之情況下移除。

3.1.17 邏輯介面 (logical interface):

利用網路介面經由通道或埠，透過網路通訊之軟體實作。

3.1.18 製造者 (manufacturer):

供應鏈中之相關經濟營運者(包括裝置製造者)。
備考：此定義認可消費者IoT生態系統中所涉及之行為者的多樣性，以及其可分擔責任之複雜方式。除裝置製造者外，此等個體亦可為例如：取決於遞交之特定情況：進口商、經銷商、整合者、組件及平台提供者、軟體提供者、IT及電信服務提供者、受管理服務提供者，以及相關聯服務提供者。

3.1.19 網路介面 (network interface):

可用以經由網路存取消費者IoT功能性之實體介面 。

3.1.20 擁有者 (owner):

擁有或購買裝置之使用者。

3.1.21 個人資料 (personal data):

與已識別或可識別之自然人有關的所有資訊。
備考：此用語係用以與眾所周知之術語保持一致，但於本標準中不具法律意義。

3.1.22 實體介面 (physical interface):

用以於實體層與裝置通訊之實體埠或空中介面(諸如無線電、音訊或光學)。
例：無線電、乙太網路埠、 USB 等串列介面，以及用以除錯之介面 。

3.1.23 公開安全參數 (public security parameter):

與安全相關之公開資訊，遭修改可能危及安全模組的安全。
例1.用以查證軟體更新之真確性 / 完整性的公鑰 。
例2.憑證之公開組件 。

3.1.24 可遠端接取 (remotely accessible):

旨在由本地網路外部接取。

3.1.25 安全模組 (security module):

實作安全功能之硬體、軟體及 / 或韌體的集合 。
例：裝置包含硬體式信任根、於受信任執行環境內運作的密碼軟體程式館，以及於作業系統內實施安全性之軟體，諸如使用者區隔及更新機制。 所有此等構成安全模組。

3.1.26 安全更新 (security update):

因應由製造者所發現或報告予製造者之安全脆弱性的軟體更新。
備考：若脆弱性之嚴重性要求更高優先序修復，則軟體更新可為單純安全更新。

3.1.27 敏感性安全參數 (sensitive security parameter):

關鍵安全參數及公開安全參數。

3.1.28 軟體服務 (softw are service):

用以支援功能性之裝置軟體組件。
備考：裝置軟體內所使用之程式設計語言的運行時間，或暴露該裝置軟體所使API之常駐程式(daemon)，例：密碼模組API。

3.1.29 遙測 (telemetry):

源自裝置之資料，其可提供資訊以協助製造者識別與裝置使用相關的問題或資訊。
例：消費者IoT裝置向製造者報告軟體故障，使其可識別並糾正原因 。

3.1.30 每裝置唯一 (unique perdevice):

對所給定產品類別或型式之各個別裝置係唯一者。

3.1.31 使用者 (user):

自然人或組織。

3.2 符號

空白。

3.3 縮寫

下列縮寫適用於本標準：

- API 應用程式介面 (appication programming interface)
- ASLR 位址空間布局隨機化 (address space layout randomization)
- CVD 協調脆弱性揭露 (coordinated vulnerability disclosure)
- CVRF 通用脆弱性報告框架 (common vulnerability reporting framework)
- DDoS 分散式阻絕服務 (distributed denial of service)
- DSC 專用安全組件 (dedicated security component)
- ENISA歐盟網路及資訊安全署 (European Union Aagency for Network and Information Security)
- EU 歐盟 (European Union)
- GDPR 一般資料保護規則 (General Data Protection Regulation)
- GSM全球行動通訊系統 (global system for mobile communication)
- GSMA GSM 協會 (GSM association)
- IEEE電機電子工程師學會 (Institute of Electrical and Electronics Engineers)
- IoT(internet o f things)
- IP 網際網路協定 (Internet protocol)
- ISO國際標準化組織 (International Organization for Standardization)
- JTAG 聯合測試行動組 (joint testaction group)

4. 縮寫報告實作

本標準中控制措施之實作，係藉由風險評鑑及威脅建模(諸如CNS27005[27]及STRIDE威脅模型[28])所告知；此係由裝置製造者及/或其他相關個體所執行，但非屬本標準範圍。
對某些使用案例及下列風險評鑑，可適切應用額外控制措施及本標準內之控制措施。
本標準設定安全基準；然而，由於消費者IoT之廣闊前景，控制措施的適用性取決於各裝置。本標準透過使用非必備宜使用控制措施(建議) ，提供一定程度之彈性。

控制措施 4-1：對本標準中視為不適用或消費者 IoT 裝置未滿足之各項建議，應記錄衡量理由。

B.1 提供以結構化方式記錄此等衡量理由之綱要。此係容許其他利害相關者(例：保證評鑑者、供應鏈成員、安全研究者或零售商)判定是否正確且適切適用控制措施。
例1. 製造者於其網站上與產品說明一起發布表 B.1 之完整版本。
例2. 製造者填寫表 B.1 以保存內部紀錄。一段時間後，外部保證組織依本標準評鑑產品，並請求提供與產品安全設計相關之資訊。 製造者可易於提供此等資訊，因其包含於表B.1中。

- 消費者 IoT裝置不適用或未執行控制措施之情況包括：
  當裝置係受限制裝置時，某些安全措施之實作，對已識別風險（安全或隱私）係可能或不適切。
- 未納入控制措施中所描述之功能性（例：僅提供資料而未要求鑑別的裝置）。

例3. 電池壽命有限之窗戶感測器於觸發時，經由遠端相關聯服務發送警示，並經集線器控制。因相較於其他消費者IoT裝置，其電池壽命及處理能力有限，故其為受限制裝置。此外，由於使用者經由集線器控制裝置，使用者無需使用通行碼或其他鑑別機制直接鑑別裝置。

5. 消費者 IoT 裝置之網宇安全控制措施

5.1 禁止使用通用預設通行碼

- 控制措施 5.1.1：使用通行碼且處於原廠預設值外之任何狀態時，所有消費者IoT 裝置通行碼應為每裝置唯一或由使用者所定義 。
  - 備考：有許多用以執行鑑別之機制，且通行碼並非用於對裝置鑑別使用者的唯一機制。然而若使用，則建議依 NIST Special Publication 800-63B [3]，依循通行碼之最佳實務作法。對機器對機器之鑑別，使用通行碼通常不適切。

- 許多消費者IoT裝置於銷售時，具通用預設使用者名稱及通行碼(諸如"admin, admin")，用於使用者介面直至網路協定。繼續使用通用預設值係IoT中許多安全問題之根源[17]，需停止該實務作法。上述控制措施可藉由使用每裝置唯一之預先安裝通行碼及/或藉由要求使用者選擇，依循最佳實務作法的通行碼作為初始化之一部分，或藉由其他不使用通行碼的方法實作。
  例1. 於初始化期間，裝置產生憑證，其係用於經由相關聯服務 (如行動應用程式) 裝置使用者鑑別。提高安全性，可使用多因子鑑別(諸如使用通行碼及 OTP程序)，更佳保護裝置或相關聯服務。藉由具唯一且不可變之識別資訊，可進一步加強裝置安全性。

- 控制措施 5.1.1：若使用預先安裝之每裝置唯一通行碼，則應以機制產生此等通碼，以降低對某類別或型式裝置的自動化攻擊之風險。
  - 例1. 預先安裝之通行碼係充分隨機化 。
  - 反例為：具遞增計數之通行碼 (諸如"password1"、"password2"等) 易於猜出。此外，使用以明顯方式與公開資訊(經由空中或於網路內發送)相關之通行碼，諸如MAC位址或Wi-Fi SSID，可考量使用自動化方式檢索通行碼。
- 控制措施 5.1.3：用以對裝置鑑別使用者之鑑別機制，應使用對技術、風險及使用的性質適切之最佳實務密碼學。
- 控制措施 5.1.4：當使用者可對裝置鑑別時，裝置應向使用者或管理者提供簡單機制，以變更所使用之鑑別值。
  - 例3.對生物特徵鑑別值，裝置製造者容許透過對新生物特徵之重新訓練變更鑑別值。
  - 例4.家庭中之父母於裝置上為其子女建立帳戶，選擇並管理子女所使用的PIN 或通行碼。父母係裝置管理者，可限制子女變更PIN 或通行碼。
  - 例5. 為讓使用者易於變更通行碼，製造者以要求最少步驟之方式，設計通行碼變更過程。製造者於使用者手冊及教學影片中解釋該過程。
  - 用以鑑別使用者之鑑別機制，無論其為指紋、通行碼或其他符記，其值需可更改。當此機制係裝置正常使用流程之一部分時，將較容易。
- 控制措施 5.1.5：當裝置係非受限制時，其應具可用之機制，使得經由網路介面力攻擊鑑別機制為不切實際。
  - 例6.裝置於一定時間區間內限制鑑別嘗試之次數，亦使用增加嘗試間之時間間隔。

- 例7.客戶端應用程式能於鑑別嘗試不成功之限定次數後，鎖住帳戶或延遲後續鑑別嘗試。
- 此控制措施因應執行"信符填充 (credential stuffing)"或窮舉整個金鑰空間之攻擊。重要的是，消費者IoT裝置可偵測出此等型式之攻擊並加以防禦，同時防範相關的"資源耗盡"威脅及阻絕服務(denial of service)攻擊。

5.2 實作管理脆弱性報告之方式

- 控制措施 5.2.1：製造者應使脆弱性揭露政策公開可用。此政策至少應包括：
  - 對問題報告之聯繫資訊。
  - 對下列項目之時程資訊： (a)接收報告之初次認可。(b)直至解決所報告問題之狀態更新。

  弱性揭露政策明確規定安全研究者及其他人能報告問題之過程。必要時可更新此種政策，以進一步確保製造者與安全研究者往來之透明度及清晰度，反之亦然。
  協調脆弱性揭露 (CVD) 係1組用以處理有關潛在安全脆弱性之揭露，並支援修復此等脆弱性的過程 。 CVD 係由國際標準化組織 (ISO) 於 ISO/IEC 29147 [4]中關於脆弱性揭露之標準化，且已於全球某些大型軟體公司中證明成功。
  於 IoT 產業中，CVD 目前尚未成熟 [16]，因某些公司不願與安全研究者往來。於此， CVD 為公司提供框架以管理此過程。此係安全研究者對公司通報安全問題之途徑，使公司領先於惡意利用的威脅，並給予公司於公開揭露前回應，並解決脆弱性之機會。

- 控制措施 5.2.2：對已揭露之脆弱性宜以及時方式採取行動 。

  對脆弱性採取行動之"及時方式"差異甚大，且為事故特定；然而通常情況下，對軟體解決方案，脆弱性處理過程係於90天內完成，包括修補程式之可用性及問題通知。以解決硬體修復可能需比軟體修復較長時間。此外，與伺服器軟體修復相比，須部署至裝置之修復可能需較長時間實施。

- 控制措施 5.2.3：製造者宜於所定義支援期間內，對其銷售及生產，以及所生產之產品及運作的服務，持續監視、識別及矯正安全脆弱性。

  備考 1.預期製造者將實施適當維護產品中使用之所有軟體及硬體，此包括適當維護及提供相關聯服務所選定的第三方，以支援產品功能。

  軟體解決方案通常包含開放原始碼及第三方軟體組件。 建立並維護所有軟體組件及其子組件之列表，係能監視產品脆弱性的先決條件。 存在各種工具用以掃描原始碼及二進碼，並構建所謂軟體組成清單 (SB OM)，其可識別第三方組件及產品中所使用

的版本。 然後，此資訊用以監視各已識別軟體組件之相關聯安全及使用授權的風險。

預期脆弱性將於第一時間直接報告受影響之利害相關者。若不可能，可將脆弱性報告主管機關。亦 鼓勵製造者與諸如 GSMA及IoT安全基金會等權責產業機構共享資訊。協調脆弱性揭露之指引，可查詢參引 ISO/IEC 29147 [4]之IoT安全基金[22]。

預期於其所定義支援期間內，對裝置執行此運作。 然而製造者可於該期間外繼續執行此運作並發布安全更新，以矯正脆弱性。

提供IoT產品之製造者有責任維護，可能因未備妥 CVD 計畫而受傷害的消費者及第三方。 此外，透過產業機構共享此資訊之公司，可協助其他可能遭受相同問題的困擾者。依情況而定，揭露可包括不同作法：

- 與單一產品或服務相關之脆弱性：預期問題將直接報告受影響的利害相關者(通常為裝置製造者、 IoT服務提供者或行動應用程式開發者)。此等報告之來源可為安全研究者或產業同儕。
- 系統性脆弱性：利害相關者(諸如裝置製造者)可發現潛在系統性問題。雖於裝置製造者自己之產品中對其修復至關重要，然共享此等資訊對產業及消費者有重大利益。同樣，安全研究者亦可尋求報告此種系統性脆弱性。對系統性脆弱性，相關之權責產業機構可協調更廣泛的回應。

備考2. 通用脆弱性報告框架 (CVRF)[5]用以交換有關安全脆弱性之資訊亦屬有用。網宇安全威脅資訊共享可依 ETSI TR 103 331[6]於開發及生產安全產品中支援組織。

5.3 保持軟體為最新

- 及時開發並部署安全更新，係製造者可採取的最重要動作之一，以保護其客戶及更廣泛的技術生態系統。
- 所有軟體保持更新並維護良好係屬良好實務作法。 由5.3-3 至5.3-1 2 之各控制措施取決於所實作的更新機制，依控制措施5.3.1或5.3.2。
- 控制措施 5.3.1：消費者IoT裝置中之所有軟體組件宜為可安全更新 。
    - 備考1. 成功管理軟體更新，通常依裝置與製造者間之軟體組件的版本資訊之通訊。

    並非裝置上之所有軟體皆為可更新。
    - 例1.裝置上第1階段啟動載入器一旦寫入裝置儲存體後，即為不可變 。

- 例2.於具數個微控制器（例：其一用於通訊，另一用於應用）之裝置上，其中某些可能無法更新。

- 控制措施 5.3.2：當裝置係非受限制時，其應具用於更新之安全安裝的更新機制。
  - 備考2. 於某些情況下，即使控制措施 5.3-2不適用，亦適用控制措施 5.3-1。
  - "可安全更新"及"安全安裝"意指具防止攻擊者錯誤使用更新機制之適切措施。
  - 例3.措施可包括使用真實之軟體更新伺服器、完整性保護的通訊通道、查證軟體更新之真確性及完整性。 軟體更新機制與〝安裝〞之構成存在很大差異係屬公認。
  - 例4.依版本核對之防轉返政策，可用以防止降級攻擊。更新機制之範圍可由裝置直接由遠端伺服器下載更新、由行動應用程式傳輸或透過 USB 或其他實體介面傳送。若攻擊者破解此種機制，則容許於裝置上安裝惡意版本之軟體。

- 控制措施 5.3.3：供使用者使用之更新應簡單。

  簡單程度依裝置之設計及預期用途而定。 使用簡單之更新，將自動套用，使用相關聯服務（諸如行動應用程式）或經由裝置上的網頁介面啟動 。 若更新難以套用，則將增加使用者一再延後更新裝置之機會，從而使其處於脆弱狀態。

- 控制措施 5.3.4：軟體更新，宜使用自動化機制。

  若自動更新不成功，則於某些情況下，使用者不能再使用裝置 。 偵測機制(諸如監看器)及雙區塊 (dual-bank) 快閃記憶體或復原分區之使用，能確保裝置返回已知的良好版本或原廠狀態。

  能以預防方式提供裝置安全更新，作為自動更新之一部分，其能於安全脆弱性遭利用前移除。 管理此點可能複雜，尤其是需平行處理相關聯服務更新、裝置更新及其他服務更新之情況下。因此，清晰之管理及部署計畫係有利於製造者，對消費者關於更新支援的目前狀態之透通性亦然。

  於許多情況下，發布軟體更新涉及對其他組織之多重相依性，諸如生產子組件的製造者；然而此非拒絕更新之理由。 製造者於安全更新之開發及部署中，考量整個軟體供應鏈可能有用。

  通常建議勿將安全更新與更複雜之軟體更新（諸如功能性更新）繫結 。 導入新功能之功能性更新，可能觸發額外要求事項，並延遲對裝置更新的交付。

  - 例5.依歐盟產品法規，功能性更新可能變更裝置之預期用途，從而將其轉變為新產品，要求進行新的符合性評鑑。 然而衝擊有限之軟體更新，可視為未要求新符

合性評鑑的維護更新。有關歐盟產品法規全景下，軟體更新衝擊之更多資訊，參照 Blue Guide [13]。

- 控制措施 5.3.5 ： 裝置宜於初始化後核對，再定期核對是否有可用之安全更新 。
  - 例6.可經由裝置之初始化介面，對使用者顯示存在更新 。
  - 例7.裝置每天於隨機時間核對可用更新 。

  對某些產品，執行此種核對可能較適切於相關聯服務而非裝置。
- 控制措施 5.3.6：若裝置支援自動更新及/或更新通知，則其宜於初始化狀態下啟用並可組態設定，以便使用者可啟用、停用或延後安裝安全更新及/或更新通知 。

  就消費者權利及擁有權觀點而言，重要的是使用者可控制其是否收到更新。 使用者可能有充分理由選擇不更新，包括安全。 此外，若部署更新且隨後發現導致問題，則製造者可要求使用者不升級其軟體，以使此等裝置不受影響。
- 控制措施 5.3.7：裝置應使用最佳實務密碼學，以有助於安全更新機制 。
- 控制措施 5.3.8：安全更新應及時 。

  安全更新全景中之〝及時〞可能有所不同，取決於特定問題及修復，以及其他因素，諸如接觸裝置的能力或受限制裝置考量事項。 重要的是，製造者以適切之優先序處置修復關鍵脆弱性 (亦即具大規模潛在不利影響的脆弱性) 之安全更新 。 由於現代軟體之複雜結構及無所不在的通訊平台，安全更新可能涉及多個利害相關者。
  - 例8.特定軟體更新涉及軟體程式館之第三方廠商、IoT裝置製造者，以及IoT服務平台營運者。此等利害相關者間之協作可確保軟體更新的適切及時性。
- 控制措施 5.3.9：裝置宜查證軟體更新之真確性及完整性。

  確認更新有效之共同作法為查證其完整性及真確性。此可於裝置上完成；然而受限制裝置可能具功率限制，此使得執行密碼運算之成本甚高。於此種情況下，可由受信任執行此查證之另一裝置執行查證。然後，經查證之更新將經由安全通道發送至裝置。於集線器上且然後於裝置上執行更新之查證，可降低破解的風險。裝置於偵測出無效及潛在惡意更新時，採取行動係屬良好實務作法。 除拒絕更新外，其亦可將事故報告適切之服務及 / 或通知使用者。此外，可備妥減緩控制措施，以防止攻擊者繞過或錯誤使用更新機制。 作為更新機制之一部分，對攻擊者提供儘可能少的資訊將降低其利用之能力。
  - 例9.當裝置偵測出無法成功交付或適用更新時 (藉由不成功之完整性或鑑別核對)，裝置可藉由不對更新過程發起者提供有關不成功之任何資訊以減輕資訊洩漏。 然而，裝置可產生日誌資料項，並經由安全通道，將日誌資料項之通知傳遞

予受信任的對等方（例：裝置管理者），以便知悉發生事故，且裝置之擁有者或管理者可做出適切回應。

- 控制措施 5.3.10：於經由網路介面傳遞更新時，裝置應經由信任關係查證各更新之真確性及完整性。
    - 備考3.有效之信任關係包括：經鑑別的通訊通道、存在於要求裝置擁有關鍵安全參數或通行碼方能加入之網路上、數位簽章式更新查證或使用者確認。
    - 備考4.信任關係之驗核對確保未經授權個體（例：裝置管理平台或裝置）無法安裝惡意程式碼至關重要。
- 控制措施 5.3.11：製造者宜以可辨識且明顯之方式通知使用者，要求安全更新連同關於藉由該更新所減輕風險的資訊。
    - 例10. 製造者經由使用者介面上之通知或經由電子郵件，通知使用者要求更新。
- 控制措施 5.3.12：當套用軟體更新，將中斷裝置之基本功能時，裝置宜通知使用者。
    - 備考5.若通知係由相關聯服務所為，則此係非必要。

    此通知可包含額外細節，諸如裝置將離線之大致預期持續時間。
    - 例11.通知包括有關緊迫性及大致預期停機時間之持續時間的資訊。

    裝置於更新期間繼續運作對使用者至關重要。 此係為何上述控制措施建議於更新可能中斷功能性時通知使用者。 特別是，滿足人身設備安全相關功能之裝置預期於更新情況下不完全關閉。 某些最小系統功能性係所預期者。 若未正確考量或管理，則功能中斷可能成為某些型式裝置及系統之關鍵安全問題。
    - 例12.於更新期間，手錶將繼續顯示時間、家用恆溫器將繼續保持合理溫度及智型門鎖將繼續鎖住及解鎖門。
- 控制措施 5.3.13：製造者應以對使用者清晰透通之可存取方式，公布所定義的支援期間。

    於購買產品時，消費者預期釐清此期間之軟體更新支援。
- 控制措施 5.3.14：對無法更新其軟體之受限制裝置，製造者宜以對使用者清晰透通的可存取方式，公布未更新軟體之理由闡述、硬體更換支援的期間及方法，以及定義之支援期間。
- 控制措施 5.3.15：對無法更新軟體之受限制裝置，產品宜為可隔離且硬體可更換。

於某些情況下，裝置無法修補程式。 對受限制裝置，需備妥更換計畫並清楚傳達予消費者。此計畫通常詳細說明何時需更換技術，以及適用時，何時結束對硬體及軟體之支援等的排程。

- 控制措施 5.3.16：消費者 IoT 裝置之型號名稱應藉由於裝置上加標籤，或經由實體介面可清晰辨識。

  此通常經由邏輯介面與裝置通訊所執行，但其亦可為UI之一部分。

  - 例13.裝置具報告型號名稱之HTTP(或適切時為HTTPS) API (於使用者鑑別後)。通常要求瞭解裝置之特定名稱，以核對定義的軟體更新支援期間或軟體更新的可用性。

5.4 安全儲存敏感性安全參數

- 控制措施 5.4.1：持久性儲存體中之敏感性安全參數應由裝置安全儲存。

  安全儲存機制可用以保護敏感性安全參數。 適切之機制包括由受信任執行環境 (TEE) 所提供的機制，以及與硬體、安全元件 (SE) 或專用安全組件 (DSC) 相關聯之加密儲存，並於 UICC(依 ETSI TR 121905 [29]、 ETSI TS 102221 [25]) 上 / 於嵌入式 UICC(依GSMA SGP.22 Technical Specification v2.2.1 [26]) 上運行的軟體之處理能力。

  備考：此控制措施適用於持久性儲存體，但製造者亦可對記憶體中之敏感性安全參數實作類似作法。

  - 例1.授權及接取許可之無線電頻率(例：LTE-m 細胞式接取)所涉及的根金鑰儲存於UICC中。
  - 例2.使用受信任執行環境(TEE)儲存並存取敏感性安全參數之遠端控制門鎖。
  - 例3.無線恆溫器將無線網路之信符儲存於防竄改微控制器中，而非於外部快閃儲存體中。

- 控制措施 5.4.2：對安全目的，於裝置中使用硬編碼唯一之每裝置識別資訊時，應以防止藉由實體、電氣或軟體等方式竄改的方式實作。

  - 例4.用於網路接取對裝置唯一之主金鑰儲存於遵循相關 ET SI 標準的 UICC 中 (例：參照 ETSI TS 102221 [25])。

- 控制措施 5.4.3：不應使用裝置軟體原始碼中硬編碼之關鍵安全參數。

裝置及應用程式之逆向工程，能輕易發現軟體中硬編碼的使用者名稱及通行碼等信符。 此等信符亦可為容許於遠端服務中，使用安全敏感功能性之 API 金鑰，或為裝置用以通訊的協定安全中所使用之私鑰。 此種信符通常可於原始碼內發現，此係公認之不良實務作法。 用以隱藏或加密此硬編碼資訊之簡單混淆方法亦能輕易破解。

- 控制措施 5.4.4：用於軟體更新之完整性及真確性的核對，以及用於保護與裝置軟體中相關聯服務之通訊的任何關鍵安全參數，應為每裝置唯一，並應以降低對各類別裝置自動化攻擊的機制產生。
    - 例5.於同一產品類別之各裝置上部署不同的對稱金鑰，用以產生並查證軟體更新之訊息鑑別碼。
    - 例6.裝置使用製造者之公鑰查證軟體更新。此並非關鍵安全參數，且無需為每裝置唯一者。

  為裝置提供唯一之關鍵安全參數，有助於保護軟體更新的完整性及真確性，以及裝置與相關聯服務之通訊。 若使用全域關鍵安全參數，則其揭露可能導致對其他 Io T 裝置之大規模攻擊，諸如建立殭屍網路 。

5.5 安全通訊

- 控制措施 5.5.1：消費者 IoT 裝置應使用最佳實務密碼學安全通訊。安 全控制措施之適切性及最佳實務密碼學的使用，取決於許多因素，包括使用全景。 隨著安全不斷演進，很難提供關於密碼學或其他安全措施之規定性建議，而無此種建議很快過時的風險。
- 控制措施 5.5.2：消費者 IoT 裝置宜使用經審查或經評估之實作，交付網路功能性及安全功能性，特別是密碼學領域。
    - 審查及評估可能涉及獨立之內部或外部個體。
    - 例1.開發及測試社群中散佈之軟體程式館、經驗證軟體模組，以及硬體設備加密服務提供者(諸如安全元件及受信任執行環境)係全部經審查或評估。
- 控制措施 5.5.3：密碼演算法及基元宜為可更新。
    - 備考1.此亦稱為"密碼敏捷性"。
    - 對無法更新之裝置，重要的是裝置之預期壽命不超過裝置所使用密碼演算法的建議使用壽命(包括金鑰長度)。
- 控制措施 5.5.4：宜僅於鑑別介面後，方可經由網路介面於初始化狀態存取裝置功能性。

    - 備考2.於使用案例上功能性可能差異很大，且可能包含某些內容，包括存取個人資料及裝置致動器。
    - 有些裝置可提供公開之開放資料，例：於 Web of Things [18]中。此等裝置無需鑑別即可存取，從而對所有人開放存取。
    - 裝置可經由網路服務中之脆弱性遭受危害。適切之鑑別機制可防止未經授權的存取，且有助於裝置中之縱深防禦。
- 控制措施 5.5.5：容許經由網路介面於組態中之安全相關變更的裝置功能性，僅應於鑑別後存取。裝置所依賴之網路服務協定不需鑑別，且製造者無法保證裝置運作所要求的組態亦不需鑑別。
    - 備考3.例外協定包括 ARP、DHCP、DNS、ICMP及NTP 。
    - 例2.安全相關之變更包括許可管理、網路金鑰組態及通行碼變更。
- 控制措施 5.5.6：傳輸中之關鍵安全參數宜以適切的技術、風險及使用性質之方式加密。
- 控制措施 5.5.7：消費者 IoT 裝置經由可遠端接取之網路介面進行通訊，應保護關鍵安全參數的機密性。
    - 存在許多不同之註冊及鑑別方法。某些鑑別值係由帶外(out -of-band)鑑別機制所提供，諸如 QR碼，而某些鑑別值係人類可讀，諸如通行碼。
    - 若鑑別機制於每個鑑別運作中使用唯一值 (例：於詰問回應(challenge - response)機制中或使用單次通行碼作為第2個因子時)，則回應並非鑑別值本身。然而對該等值套用機密性保護仍屬良好實務作法。
    - 可使用加密通訊通道或酬載加密達成機密性保護。此通常使用至少與所傳輸之金鑰資料一樣強度的協定或演算法完成之，但亦可使用其他減緩措施，諸如需近距離接觸。
- 控制措施 5.5.8：製造者應依循與裝置相關之關鍵安全參數的安全管理過程。
    - 強烈鼓勵對關鍵安全參數(通常稱為"金鑰管理") 使用經同儕審查之開放標準。

5.6 最小化暴露之攻擊面

"最小特殊權限原則"係良好安全工程之基石，適用於IoT及任何其他應用領域。

- 控制措施 5.6.1：應停用所有未使用之網路介面及邏輯介面。

    - 例1. 管理用 UI 預設由 LAN 存取，不能由WAN存取 。
    - 例2. 經由Bluetooth低功率暴露之直接韌體更新(DFU)服務係用於開發，但未預期用於生產，於最終產品中停用。
- 控制措施 5.6.2：於初始化狀態下，裝置之網路介面應最小化未經鑑別的安全相關資訊揭露。
    - 作為初始化過程之一部分，可經由網路介面暴露與安全相關的資訊。 當裝置於建立連接共享與安全相關之資訊時，攻擊者可能用以識別脆弱裝置。
    - 例3. 當於整個 I P 位址空間中查找 (find ing) 脆弱裝置時，與安全相關之資訊可能為關於裝置組態、內核 (kernel) 版本或軟體版本的資訊 。
- 控制措施 5.6.3：裝置硬體不宜將實體介面非必要暴露於攻擊。
    - 攻擊者可能使用實體介面破壞裝置上之韌體或記憶體。 〝非必要〞係指製造者對開啟用於使用者功能性或除錯目的之介面的利益之評量。
    - 例4. 旨在僅用於為裝置供電之 micro - USB 埠，於實體上組態設定為亦不容許執命令或除錯。
- 控制措施 5.6.4：若除錯介面係可實體存取，則應於軟體中停用。
    - 例5. 透過裝置上之啟動載入器軟體，停用 UART 串列介面。 由於此停用，將無登入提示及互動式選單。
- 控制措施 5.6.5：對裝置之預期用途或運作，製造者宜僅啟用其所使用或所要求的軟體服務。
    - 例6. 對預期用途，製造者不提供裝置未要求之任何背景過程、內核延伸、命令、程式或工具。
- 控制措施 5.6.6：程式碼宜最小化服務/裝置運作所必要之功能性。
    - 例7. 移除"失效"或未使用之程式碼，其不視為良性程式碼 。
- 控制措施 5.6.7：軟體宜以最小必要特殊權限運行，同時考量安全及功能性。
    - 例8. 以"根"特殊權限運行最少常駐程式/過程。特別是使用網路介面之過程要求非特殊權限使用者而要求非〝根〞使用者。
    - 例9.對各組件或服務，於納入多使用者作業系統 (例： Linux ®) 之裝置上運行的應用程式，使用不同之使用者。

- 透過諸如堆疊跳動、位址空間布局隨機化 (ASLR) 等機制，能減緩意圖破壞記憶體之裝置上軟體攻擊。 製造者可使用可用之平台安全功能性協助進一步降低風險。降低其運行之特殊權限並最小化程式碼，亦有助於降低此種風險。

- 控制措施 5.6.8：裝置宜納入用於記憶體之硬體層級存取控制機制。
  - 軟體脆弱性利用經常利用記憶體中缺乏存取控制，執行惡意程式碼。 存取控制機制限制裝置記憶體中之資料是否可執行。適切之機制包括諸如MMU或MPU、可執行空間保護(例：NX位元)、記憶體加標籤及受信任執行環境等技術 。

- 控制措施 5.6.9：製造者宜依循安全開發過程，部署於裝置上之軟體。 安全開發過程，包括使用版本控制或啟用與安全相關之編譯器選項 (例：堆疊保護)，能協助確保軟體產出更安全 。 製造者於使用支援之工具鏈時，可使用此等選項。

5.7 確保軟體完整性

- 控制措施 5.7.1：消費者 IoT裝置宜使用安全啟動機制查證其軟體。

  作為安全啟動機制之一部分，硬體式信任根係提供強力證明之 1 種方式 。 硬體式信任根為系統組件，所有其他組件皆由該組件導出其〝信任〞 — 亦即該系統內密碼信任之來源。 為滿足其功能性，當無機制可判定組件是否已失效或遭變更時，硬體式信任根係屬可靠，且可抵抗實體及邏輯竄改。 藉由利用硬體式信任根，裝置可信任密碼功能性之結果，諸如用於安全啟動者。 硬體式信任根可藉由用於信符的安全儲存之機制提供支持，亦或藉由提供與給定裝置所要求的安全層級成正比之安全保證基準層級的其他替代方案提供支持。

- 控制措施 5.7.2：若偵測出對軟體之未經授權的變更，則裝置宜對使用者及/或管理者發出警示，且不宜連接至比執行警示功能所必要之網路更廣的網路。

  由未經授權之變更中遠端復原的能力，可依賴於已知之良好狀態，諸如本地儲存已知良好的版本，以啟用裝置之安全復原及更新。 此將避免阻絕服務及昂貴之召回或維護接取，同時管理攻擊者破壞更新或其他網路通訊機制可能接管裝置的風險。

  若消費者IoT裝置偵測出對其軟體之未經授權的變更，其將能通知正確之利害相關者。於某些情況下，裝置能具處於管理模式下之能力。
  - 例：房間中之恆溫器可具使用者模式；此模式防止變更其他設定值。 若偵測出對軟體之未經授權的變更，則對管理者發出警示係屬適切，因管理者能對警示採取行動(而使用者則不能)。
  - 備考：若裝置無法成功執行此操作或攻擊者能重複造成此影響，則強制裝置回復至已知良好狀態之攻擊可能引入DoS風險。

5.8 確保個人資料安全

- 控制措施 5.8.1：宜使用最佳實務密碼學保護於裝置與服務間傳輸之個人資料的機密性，特別是相關聯服務。
- 控制措施 5.8.2：應保護於裝置與相關聯服務間通訊之敏感性個人資料的機密性，並採用適合之技術性及用途的密碼學。
    - 備考1.於本控制措施之全景中，"敏感性個人資料"係指其揭露極可能對個人造成傷害的資料。 視為"敏感性個人資料"之內容隨產品及使用案例而異，例：家庭安全攝影機的視訊串流、支付資訊、通訊資料內容及加時戳之定位資料。 執行安全及資料保護衝擊評鑑可協助製造者做出適切選擇。
    - 備考2.此全景中之相關聯服務通常為雲端服務。 此外，此等服務受製造者所控制或影響。 此等服務通常非由使用者操作。
    - 備考3.機密性保護通常包括依最佳實務密碼學之完整性保護。
- 控制措施 控制措施 5.8.3：裝置之所有外部感測能力應以對使用者清晰透通的可存取方式記錄。
    - 例：外部感測能力可為光學或聲學感測器 。 本標準第6節包含特定於保護個人資料之控制措施。

5.9 使系統對中斷具韌性

本節之各控制措施旨在確保隨著消費者生活之各層面（包括與人身設備安全相關的功能）採用 Io T 裝置日增， IoT 服務保持正常運行 。 重要的是需注意能適用安全相關之法規，但關鍵為避免使中斷成為對使用者產生影響的原因，並設計能於對此等挑戰有一定程度韌性之產品及服務。

- 控制措施 5.9.1：宜於消費者 IoT 裝置與服務中建立韌性，考量資料網路與電源中斷之可能性。
- 控制措施 5.9.2：消費者 IoT 裝置於失去網路接取權之情況下，宜保持運作及本地功能性，且宜於斷電復原的情況下澈底復原。
    - 備考：“澈底復原"通常涉及以相同或改善之狀態復原連接性及功能性。
- 控制措施 5.9.3：消費者 IoT 裝置宜以預期可操作且穩定之狀態，並以有秩序的方式連接至網路，同時考量基礎設施之能力。

- 例1.智慧家庭於停電後失去對網際網路之連接。當網路連接回復時，家中之裝置於隨機延遲後重新連接，以最小化網路利用率。
- 例2.於提供更新後，製造者分批通知裝置，以防止其同時下載更新。

消費者依賴 IoT系統及裝置處理日趨重要之使用案例，此等使用案例可能與人身設備安全相關或衝擊生命。 若網路中斷，則保持服務於本地運行係提高韌性的措施之一。 其他措施可包括於相關聯服務中建構備援，以及減緩分散式阻絕服務(DDoS)攻擊或信令風暴，其可能係由中斷後裝置之大規模重新連接所引起 。 預期必要之韌性水準係成正比，且由使用情況所判定，以及考量依賴系統、服務或裝置之其他者，因中斷可能產生較預期更廣的影響。

有秩序重新連接意指採取明確步驟之方式，以避免源自大量IoT裝置的同時請求，諸如軟體更新或重新連接。 此種明確步驟可包括依遞增後退機制，於重新連接嘗試前引入隨機延遲。

5.10 檢查系統遙測資料

- 控制措施 5.10.1：若蒐集由消費者 IoT 裝置及服務蒐集遙測資料 (諸如使用及量測資料) ，則宜檢查安全是否異常 。
  - 例1.安全異常可藉由裝置正常行為的偏差表示之，依監視指示符所表示者，例：不成功登入嘗試的異常增加。
  - 例2.源自多個裝置之遙測，容許製造者注意由於無效的軟體更新真確性核對而導致更新不成功。

對安全評估，檢查遙測資料 (包括日誌資料) 係屬有用，且考量及早識別並處理異常情況，從而極小化安全風險且迅速化解問題。
第6節包含當蒐集遙測資料時，特定於保護個人資料之控制措施。

5.11 使用者容易刪除使用者資料

- 控制措施 5.11.1：應為使用者提供功能性，以便能以簡單方式由裝置中抹除使用者資料。
  - 備考1.此全景中之使用者資料意指儲存於 Io T 裝置上的所有個人資料，包括個資、使用者組態及密碼資料，諸如使用者通行碼或金鑰。
- 控制措施 5.11.2：宜向消費者提供裝置上之功能性，以便能以簡單方式由相關聯服務中移除個人資料。

此種功能性係適用於擁有權轉移、消費者希望刪除個人資料、消費者希望由裝置中移除服務及/或消費者希望汰除裝置等情況。預期此種功能性遵循適用之資料保護法，包括GDPR[7] 。

"容易"移除個人資料意指完成該動作所要求之最少步驟，各步驟涉及最小複雜性。此種功能性可潛在呈現攻擊向量。

- 控制措施 5.11.3：宜對使用者明確說明如何刪除其個人資料。
- 控制措施 5.11.4：宜對使用者清楚確認個人資料已由服務、裝置及應用程式中刪除。

  消費者IoT裝置經常更換擁有權，最終將回收或汰除。可提供容許消費者保持控制，並由服務、裝置及應用程式中刪除個人資料之機制。當消費者希望完全移除其個人資料時，其亦希望追溯備份複本之刪除。
  由裝置或服務中刪除個人資料，通常無法簡單藉由將裝置重置為其原廠預設狀態達成。 於許多使用案例中，消費者並非裝置之擁有者，但希望由裝置及所有相關聯服務 (諸如雲端服務或行動應用程式) 中刪除其自有個人資料 。

  - 例：使用者可於所租賃之公寓內臨時使用消費者IoT產品。執行產品之原廠重置可能移除組態設定值或停用裝置，從而損害公寓擁有者及未來使用者的利益 。 原廠重置 (由IoT裝置中刪除所有資料) 並非於諸如此種共用使用全景中刪除單一使用者個人資料之適切方式。
  - 備考 2.　本標準附錄 A 包含裝置狀態之示例模型，包括各狀態的資料儲存。

5.12 使裝置容易安裝及維護

- 控制措施 5.12.1：消費者IoT裝置之安裝及維護宜由使用者做最少決定，且宜依循有關可用性的安全最佳實務作法。
  - 例：使用者使用精靈設置裝置，其中組態選項之子集以已規定的共同預設值，以及預設已開啟之適切安全選項呈現。
- 控制措施 5.12.2：製造者宜提供使用者有關如何安全設置其裝置之指引。然而理想之過程為涉及最少人工介入，並自動達成安全組態。
- 控制措施 5.12.3：製造者宜提供使用者有關如何核對其裝置是否安全設置之指引。

  藉由適切因應使用者介面之複雜性及不良設計，可減少甚至消除由消費者混淆或錯誤組態設定所引起的安全問題。為使用者提供有關如何安全組態設定裝置之明確指引，亦可減少其暴露於威脅之下。

於一般情況下，安全設置裝置之平均額外負擔高於核對裝置是否安全設置的平均額外負擔。 就過程而言，安全設置之核對很大程度上可由製造者透過與裝置遠端通訊的自動化過程承擔。此種自動化過程之一部分可能包括驗核裝置建立安全通訊通道的能力。

5.13 驗核輸入資料

- 控制措施 5.13.1 ： 消費者 IoT 裝置軟體應驗核經由使用者介面輸入，或經由應用程式介面 (API) 或於服務中網路與裝置間傳送之資料 。
  跨不同型式介面傳送之格式化不正確的資料或程式碼可能破壞系統。攻擊者或測試者可使用諸如模糊器之自動化工具，利用因未驗核資料而出現的可能間隙及弱點。
  - 例1. 裝置接收非屬預期型式之資料，例：可執行程式碼而非使用者輸入的文字。裝置上之軟體已編寫，使得輸入為參數化或〝逸出〞，從而防止運行此程式碼。
  - 例2. 溫度感測器接收超出範圍之資料，不嘗試處理此輸入，而識別為超出可能的範圍並丟棄，且事件於遙測中擷取。

6.消費者 IoT 裝置之資料保護控制措施

許多消費者IoT裝置處理個人資料。預期製造者於消費者IoT裝置內提供支援保護此種個人資料之功能性。此外，亦存在與消費者IoT裝置中個人資料保護相關之法規(例： GDPR [7])。本標準旨在協助消費者IoT裝置製造者，由嚴格技術角度提供許多保護個人資料之功能性。

- 控制措施 6-1： 製造者應對各裝置及服務，向消費者提供清晰且透通之資訊，包括處理哪些個人資料、如何使用、由誰使用及用於何種目的。 此亦適用於可能涉及之第三方，包括廣告商。
- 控制措施 6-2： 處理個人資料之依據係消費者的同意，應以有效方式取得此同意。
  "以有效方式"取得同意通常涉及使消費者自由、明顯且明確選擇是否可將其個人資料用於特定目的。
- 控制措施 6-3：同意處理其個人資料之消費者，有權隨時撤銷同意。
  消費者期望能藉由適切之組態設定IoT裝置及服務功能性保護其隱私 。
- 控制措施 6-4：若由消費者 IoT 裝置及服務蒐集遙測資料，則宜將個人資料之處理保持於預期功能性所必要的最低限度。

- 控制措施 6-5：若由消費者 IoT 裝置及服務中蒐集遙測資料，應向消費者提供有關蒐集哪些遙測資料、如何利用、利用對象及利用目的之資訊。

附錄 A（參考）基本概念及模型

A.1 架構

消費者 IoT裝置係硬體與軟體組件之彙集，通常具實體介面，亦可為網路介面 。通用示例及特定〝智慧型揚聲器〞複雜示例，如圖 A.1 中所示。此等架構係屬參考性，不預期繪出裝置之所有或部分組件。

圖A.1 裝置之一般架構及智慧型揚聲器的架構示例

部署於家庭中之消費者IoT裝置通常由各種受限制及非受限制裝置組成，此等裝置將直接透過IP連接性 (諸如經由乙太網路或 Wi-Fi) 連接至 LAN，或間接經由閘道器或集線器連接至LAN。 此對LAN之間接連接通常使用非 I P 連接性（例：基於 IEEE 802.15.4的協定[24]）。 然後，路由器將 LAN 連接至 WAN（亦即網際網路）。然而，於某些情況下，家庭中之裝置可經由其他非 I P 或 I P 連接（諸如 GSM 或Lo RaWAN) 直接連接至WAN 。

家庭中之消費者 IoT 裝置將通常對外連接（或將藉以連接進）線上或本地服務。於本標準中，由製造者所納入者（例：遙測或配套行動應用程式），或須作為初始化之一部分所安裝者被歸類為相關聯服務－ 於使用者選擇安裝服務的情況下，或存取外部內容者則不被當作相關聯服務。 例：下列某些情境：

- 經由裝置之瀏覽器所接取的網站可能非屬相關聯服務，因其係使用者決定接取，而非裝置軟體的開發者。
- 於裝置上運行之軟體應用程式（諸如可能被安裝於智慧型電視上的〝ap p〞）。 若其係預設安裝者，則其通常歸類為相關聯服務。 然而若其係透過使用者選擇之商店所安裝，則其將非屬相關聯。
- 連接至遙測平台將屬相關聯服務，因此通常由裝置製造者預先組態設定。

圖A.2 提供此部署模型之架構示例 。 〝家庭〞邊界表示本標準所定義範圍之大致範圍－包括對相關聯服務的通訊。

圖A.2 家庭環境中消費者 Io T 裝置部署之參考架構示例

圖A.3 顯示家庭中消費者 Io T 之實際部署示例 。 下列各使用案例圖示如何使用此設置，並釐清定義中將涵蓋及不涵蓋之內容：

- 智慧型電視與 2 個外部服務通訊 。 其一為裝置遙測服務（相關聯服務）；於使用者許可之情況下，擷取自電視之資訊（諸如當機日誌及關於使用的資料），以使開發人員能修復軟體缺陷並優先開發新功能性。智慧型電視亦透過使用者於初始化後所下載之應用程式連接至視訊共享服務。此視訊共享服務讓使用者能經由第三方應用程式觀看娛樂節目，該應用可安裝於電視使用之作業系統中。 此串流媒體服務將非屬相關聯服務。
- 閘道器提供對各種受限制裝置之接取，包括用以監視並管理家庭的 IEEE 802.15.4 [24] 網狀網路及光線感測器。其連接至雲端存取服務，讓使用者能遠端控制其智慧型門鎖並查看源自感測器之資料。 此係相關聯服務。
- 智慧型電冰箱安裝網路瀏覽器；此容許使用者就近查看新聞網站之標題。新聞網站將非屬相關聯服務。
- 使用者使用氣候感測器核對戶外溫度。由於其於實體上遠離家庭本身，因此無法連接至LAN 。 反之，其經由 GSM 直接與 WAN 通訊。氣候感測器所連接之服務係屬相關聯服務。

圖A.3 消費者 IoT 裝置部署架構示例

A.2 裝置狀態

除役裝置非屬本標準範圍內。除役裝置係處於不存在敏感性資料之狀態。裝置（由製造至除役）將於幾個狀態之間轉換。此等轉換如圖A.4中所示，以明確所定義之狀態如何於裝置中使用。 於此模型中，除役裝置將處於原廠預設狀態，因原廠重設過程似乎用以刪除所有使用者資料及組態之過程。例：除役時，裝置可回收、轉售或銷毀。

圖A.4消費者IoT裝置狀態之狀態圖
於此等狀態下，對哪些資料將儲存於任意裝置中，圖 A . 5 顯示模型示例 。 對各種情況，預期將不相同。

圖 A . 5　以狀態裝置儲存之模型示例

附錄 B(參考) 實作符合性聲明一覽表

- 儘管存在與本標準文字相關之著作權節次的控制措施，ET SI 允許本標準使用者可自由複製本附錄中之一覽表，以便將其用於預期目的，並可進一步發布包括表 B . 1 的完整附錄。
- 對本標準使用者 (預期其將為參與消費者 Io T 裝置開發或製造之個體)，表 B . 1 可提供機制，以提供有關本標準中控制措施的實作資訊。參引欄引用本標準中之控制措施。
- 狀態欄指示控制措施之狀態。 使用下列記法：
  - M: 該控制措施係必備要求。
  - R: 該控制措施係建議。
  - MC: 該控制措施係必備要求及條件式。
  - RC: 該控制措施係建議及條件式。
    備考： 於使用條件式記法之情況下，此係取決於該控制措施的文字。表格底部提供條件，並為相關控制措施提供參考以協助釐清。
- 支援欄可由本標準使用者填寫。使用下列記法：
  - Y: 實作支援。
  - N: 實作不支援。
  - N/A: 控制措施不適用 (僅當控制措施於狀態欄中指示為條件式並已判定該條件不適用於相關產品時容許)。
  -
- 本標準使用者可填寫細節欄：
  - 若某控制措施係實作支援，則細節欄中之資料項將包含有關為達成支援而實作的措施之資訊。
  - 若實作不支援某控制措施，則細節欄中之資料項將包含有關實作不可能或不適切的原因之資訊。

- 若某控制措施不適用，則細節欄中之資料項將包含此判定的理由。

表 B . 1　消費者 Io T 裝置安全控制措施之實作 (續)
節次及標題
條件：
(1) 使用通行碼。
(2) 使用預先安裝之通行碼。
(3) 軟體組件不可更新。
(4) 裝置受限制。
(5) 裝置不受限制。
(6) 正蒐集之遙測資料。
(7) 於消費者同意之基礎上處理個人資料。
(8) 容許使用者鑑別之裝置。
(9) 裝置支援自動更新及 / 或更新通知。
(1 0)　　對安全目的，使用每裝置識別資訊之唯一硬編碼。
(1 1) 更新係經由網路介面遞送。
(1 2)　　實作更新機制。
(1 3)　　除錯介面係實體可接取。

參考資料
[1]　ETSI TR　103305-3:" CYBER;Critical Security　Controls for Effective　　Cyber Defence; Part 3 : Service Sector Implementations" .
[2]　ETSI TR 103309 : " CYBER; Secure by Default - platform security technolo gy" .
[3]　NIST Special Publication 800-63B : "Digital Id entity Guidelines - Authentication and Lifecycle Management" .
備考：可查詢網址 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf。
[4]　ISO/IEC 29147 : "Info rmatio n techno lo gy - Security techniq ues - Vulnerab ility Disclosure" .
備 考：可查詢網址https://www.iso.org/standard/45170.html 。
[5]　OASIS: "CSAF Common Vulnerability Reporting Framework (CVRF)" .
備考：可查詢網址。
備 考：可查詢網址 。
[10] IoT Security Foundation: " IoT Security Compliance Framework" , Release 2 December 2018.備考：可查詢網址。

[11] GSMA: " GSMA IoT Security Guidelines and Assessment" .
備考：可查詢網址。

[17] F-Secure: " IoT threats: Explosion of 'smart' devices filling up ho mes leads to increasing risks" .。
[22] Io T Security Foundation: " Vulnerability Disclosure - Best Practice Guidelines" .
備考：可查詢網址。
[23] OWASP Internet o f Things (IoT) Top 10 2018.
備考：可查詢網址

[24] IEEE 802.15.4 - 2015 : "IEEE Stand ard for Low - Rate Wireless Netwo rks" .
備考：可查詢網址。
[25] ETSI TS 102221 : " Smart Card s; UICC - Terminal interface; Physical and logical characteristics" .
[26] GSMA: " SGP. 2 2 Technical Sp ecificatio n v2.2. 1 " .
[27] CNS 27005:2018 : " Information technology - Security techniques - Info rmation security risk management" .
備 考：可查詢網址 。
[28] Microsoft Corporatio n: " The STRIDE Threat Model" .
備考：可查詢網址
。
[29] ETSI TR121905 : " Digital cellular telecommunications system (Phase 2 +) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Vocabulary for 3 GPP Specifications (3 GPPTR 21.905)" .
[30] ETSI EN 303645:2020 " CYBER ； Cyber Security for Concumer Internet of Things:Baseline Requirements " .
備考：可查詢網址
。

名詞對照

- A -
  administrator: 管理者
  ap plication programming interface, API: 應用程式介面
  associated service: 相關聯服務
  authentication mechanism: 鑑別機制

authentication value: 鑑別值
authenticity: 真確性

- B -
  base station: 基地臺
  baseline provision: 基準控制措施
  best practice cryptography: 最佳實務密碼學
  boot loader: 啟動載入器

- C -
  certificate: 憑證
  common vulnerability reporting framework, CVRF: 通用脆弱性報告框架
  communication protocol: 通訊協定
  competent industry body: 權責產業機構
  configuration: 組態
  constrained device: 受限制裝置
  consumer:消費者
  consumer IoT device:消費者 IoT裝置
  controls:控制措施
  coordinated vulnerability disclosure, CVD credential stuffing:協調脆弱性揭露
  critical stuffing:信符填充
  critical security parameter:關鍵安全參數
  crypto graphic operation:密碼式運算
  crypto graphic primitive:密碼式基元
  cyber security:網宇安全

- D -
  daemon: 常駐程式
  debug interface: 除錯介面
  denial of service, DoS: 阻絕服務
  device manufacturer:裝置製造者
  distributed denial of service, DDoS:分散式阻絕服務

- F -
  factory default: 原廠預設
  factory state: 原廠狀態
  functionality: 功能性

- G -
  gateway 閘道器
  General Data Protection Regulation, GDPR: 一般資料保護規則
- H -
  hub 集線器
- I -
  identity:識別資訊；身分
  incremental back - off:遞增後退
  initializatio:初始化
  initialized state:初始化狀態
  internet of things, IoT:IoT
- L -
  log entry:日誌資料項
- M -
  model designation:型號名稱
- O -
  open source: 開放原始碼
  owner: 擁有者
- P -
  password: 通行碼
  patch: 修補程式
  personal data:個人資料
  physical interface:實體介面
  public security parameter: 公開安全參數
- R -
  requirements:要求事項
- S -
  security by design:於設計即保護安全
  security module:安全模組
  security update:安全更新
  sensitive security parameter:敏感性安全參數
  sensor:感測器

software bill of materials, SBOM:軟體組成清單
source code:原始碼
stakeholder:利害相關者

- T -
  telemetry data: 遙測資料
  trusted execution environment, TEE: 受信任執行環境
- V -
  vulnerability: 脆弱性