IoT-1005-1

消費性網路攝影機資安標準

V1.0

經濟部工業局

中華民國 110 年 6 月

目錄

引言

由於高速網路傳輸與高畫質影像需求的趨勢，加上人口結構的改變，市場上出現了面向居家幼兒照護、老年人居家照顧、寵物關懷等智慧家庭應用中消費性網路攝影機產品。根據 Frost & Sullivan 的調查報告，全球網路攝影機將以平均成長率超過 20% 的速度發展，至 2024 年出貨量達 3.2 億台，其中亞太區域為銷售增長最快的地區。然而，近年來隨著消費性網路攝影機多起個人私密影像外洩的問題，也引發使用者對於個人隱私的疑慮。

經濟部工業局雖於 2017 年制定符合安控需求之影像監控系統資安標準，在安控產業上奠定了資訊與網路安全的重要基礎；然而，上述問題多數來自消費性網路攝影機資安防護不足。此類資安事件造成消費者紛紛向消費者保護單位提出申訴，行政院消費者保護會(簡稱消保會)表達亟需制定消費性網路攝影機產品資安標準之需求，以規範消費性網路攝影機之資訊安全。

影像監控系統的網路攝影機產品的設計與使用者區隔有別於消費性網路攝影機產品(如附錄 B)，在資安防禦基礎上亦有所分別，因此在經濟部工業局與網路攝影機產業的支持下，本標準以 ETSI EN 303 645 Cyber Security for Consumer Internet of Things：Baseline Requirements[1]為基礎，制定我國消費性網路攝影機資安產業標準。本標準制定之目的為提供行政院消保會以確保消費者個人隱私的保護，及政府所屬之各機關院校採購消費性網路攝影機設備時，作為產品資安品質要求之依據，同時協助我國網路攝影機業者提升產品資安防護能力與自主資安檢測能量。

1. 適用範圍

本標準規定消費性網路攝影機之資訊安全要求。消費性網路攝影機係指具聯網功能之網路攝影機，主要之使用對象為一般消費者，該產品設置於消費者欲監看環境中，透過 IP 直接連接網際網路，可將影像與聲音傳送至指定之網路服務平台；消費者透過網際網路在該網路服務平台與欲監看的設備間進行聲音、影像與控制指令傳輸。消費性網路攝影機之適用情境包括但不限於寵物關懷、幼兒照護、長輩照顧和居家安全等應用。

本標準的適用範圍如下圖 1 所示，但不包括下列項目：

(a) 電信網路與消費性網路攝影機網路服務平台間之網路傳輸安全。

(b) 消費性網路攝影機網路服務平台。

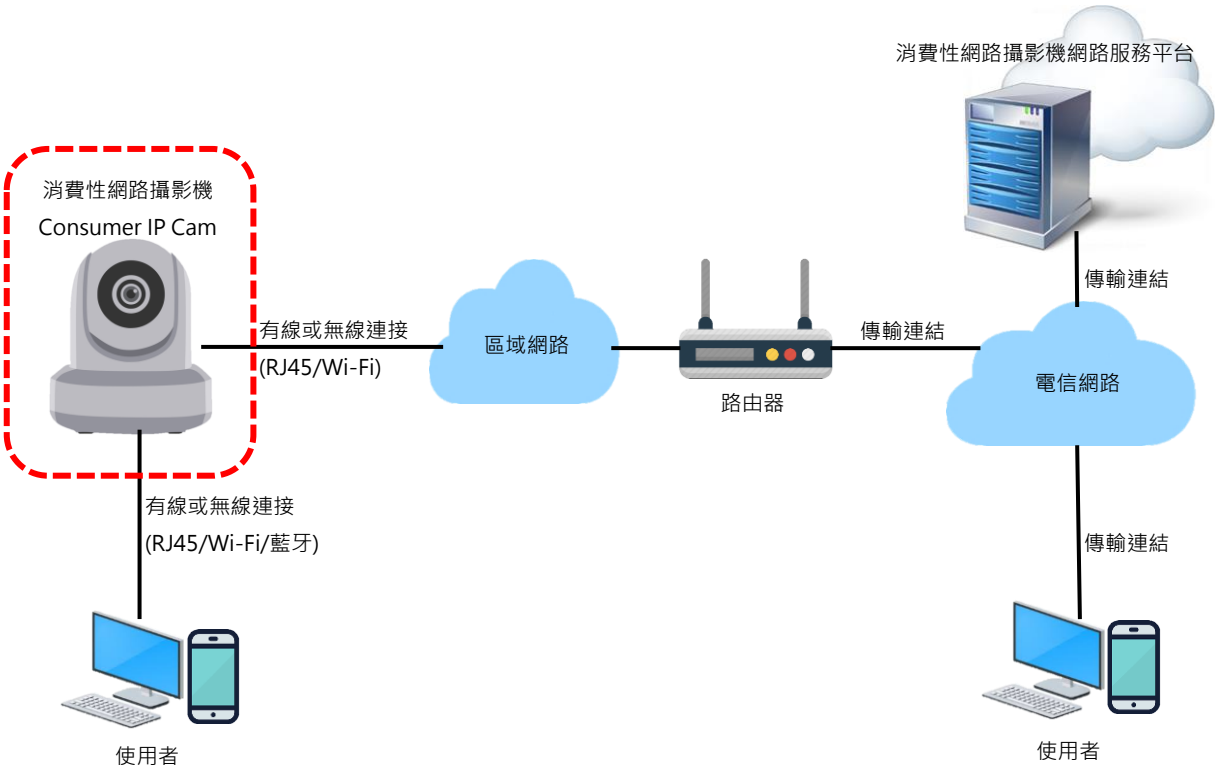


圖 1 適用範圍示意圖

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] ETSI EN 303 645 V2.1.1 (2020-06) Cyber Security for Consumer Internet of Things: Baseline Requirements

[2] IoT-1001-2 v1.0 影像監控系統資安標準-第二部：網路攝影機

3. 用語及定義

下列用語與定義適用於本標準。

3.1 消費性網路攝影機(Consumer IP camera)

指具聯網功能之網路攝影機，一般被消費者設置在欲監看的環境中，提供即時影像和聲音，不經由其它裝置(如:電腦)直接連接網際網路，消費者可以使用網際網路遠端連線監看。

3.2 遙測數據(Telemetry data)

指來自產品的資訊，可以提供廠商用以識別問題或改善產品服務所需之相關的訊息，例如：故障回報、GPS 定位座標、使用習慣紀錄等。

3.3 國家弱點資料庫(National vulnerabilities database)

指美國國家標準技術研究所(National Institute of Standards and Technology, NIST)提供的國家弱點資料庫[5]，負責常見弱點與漏洞(如 3.5 所述)之資料的發布及更新。

3.4 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。

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

由美國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[8]，目前發展至第 3 版，以衡量軟體漏洞的特徵和嚴重性進行評分。

3.6 安全敏感性資料(Secure sensitivity data)

指與設備或服務之安全性相關的資料，例如通行碼、金鑰等系統運行所需之機敏資料。當產品透過 OTA 更新韌體時，如果更新伺服器發送之憑證金鑰遭惡意人士竄改，可能造成更新失敗或安裝了帶有惡意程式之韌體。

3.7 敏感性個人資料(Sensitive personal data)

泛指對於已識別或可識別自然人有關的任何資訊，包括識別個人身分之隱私資料，例如：身分證字號、電話號碼、住址、車牌及生物辨識相關之影像等。

3.8 管理者(Administrator)

具更改產品設定、作業系統、控制介面、功能應用程式之權限人員，如系統管理者。

3.9 通行碼(Password)

指一組能讓消費者使用系統或以識別消費者身分之字元串，包括本機儲存資料加密檔案密碼、自身帳號及密碼、遠端網路服務帳號及密碼。

3.10 預設通行碼(Default password)

指產品出廠預先設定好的通行碼，即消費者在初次將其連上網路，且在未更改任何設定的情況下，用以登入產品之通行碼。

3.11 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讀而達到保密之目的。

3.12 安全事件(Security event)

本標準之安全事件定義為，包括但不限於消費者登入、配置設定之各種可能發生威脅或攻擊事件之活動。

3.13 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(Transport Layer Security, TLS)。

3.14 前向安全(Forward Secrecy, FS)

指萬一通行碼或金鑰在某個時間點不慎洩漏，過往的通訊依然是安全，不會因此而洩漏過去的通信數據。

3.15 無線下載(Over-the-air, OTA)

為一種裝置透過行動網路、Wi-Fi 等無線傳輸，下載更新韌體並自動安裝的技術。

4. 安全構面與要求

本標準為消費性網路攝影機裝置之網路安全要求，所有安全要求項目皆參照 ETSI EN 303 645 消費性物聯網產品之基本要求，因此，為達消費性網路攝影機基本安全要求，則須符合本標準所有之安全要求項目。

4.1 安全構面與要求概述

安全構面與要求總表如表 1 所示，第一欄為安全構面，包括：(1)身分鑑別與權限控管、(2)已知漏洞安全、(3)軟韌體更新、(4)資料機密性與完整性、(5)系統完整性、(6)資源可用性、(7)隱私保護及(8)警示與紀錄；第二欄為安全要求，係依第一欄安全構面設計之對應安全要求；第三欄為安全要求項目，須依循第 5 節之技術規範內容。

表 1 安全構面與要求總表

安全構面	安全要求	安全要求項目
5.1 身分鑑別與權限控管	5.1.1 鑑別機制	5.1.1.1 5.1.1.2 5.1.1.3
	5.1.2 權限控管	5.1.2.1 5.1.2.2
	5.1.3 通行碼鑑別	5.1.3.1
5.2 已知漏洞安全	5.2.1 作業系統與網路服務	5.2.1.1
	5.2.2 網服務連接埠安全	5.2.2.1
	5.2.3 資訊安全管理	5.2.3.1 5.2.3.2 5.2.3.3 5.2.3.4
5.3 軟韌體更新	5.3.1 更新安全	5.3.1.1 5.3.1.2 5.3.1.3 5.3.1.4
5.4 資料機密性與完整性	5.4.1 安全敏感性資料儲存	5.4.1.1 5.4.1.2
	5.4.2 傳輸資料保護	5.4.2.1 5.4.2.2
5.5 系統完整性	5.5.1 實體入侵防護	5.5.1.1
	5.5.2 輸入驗證	5.5.2.1

安全構面	安全要求	安全要求項目
5.6 資源可用性	5.6.1 資源管理	5.6.1.1
5.7 隱私保護	5.7.1 隱私保護能力	5.7.1.1 5.7.1.2
5.8 警示與紀錄	5.8.1 安全事件警示	5.8.1.1

4.1.1 安全構面：

(a) 身分鑑別與權限控管：溝通介面須確保鑑別、授權及權限控管相關機制，包括遠端指令管理介面、通訊協定等，應具備一定防護能力，避免遭受蓄意人士入侵。

(b) 已知漏洞安全：產品之系統、網路服務應防止漏洞及具備即時檢視漏洞之安全機制，及預防與處置機制的資訊安全管理。

(c) 韌體更新：產品之韌體版本更新服務及韌體程式設計等，須具備足夠安全防護。

(d) 資料機密性與完整性：產品傳輸與儲存之資料應具有足夠安全之防護，避免遭受蓄意人士入侵。

(e) 系統完整性：產品測試用連接埠的處置，應具備一定防護能力，視為實體安全要求的標的。

(f) 資源可用性：產品之資源管理應預防造成服務中斷。

(g) 隱私保護：產品須具有敏感性個人資料的保護機制。

(h) 警示與紀錄：產品須有安全事件管理機制，於安全事件發生時須具有警示能力。

4.1.2 安全要求項目：

依安全構面所設計對應之安全要求，其中每一安全要求包含一個或以上之安全要求項目。

5. 標準規範

本節詳盡載明消費性網路攝影機為滿足安全功能應採取的方法，消費性網路攝影機產品應符合本節中所有安全基本要求。

5.1 身分鑑別與權限控管

5.1.1 鑑別機制

5.1.1.1 每個產品應有一組唯一的識別碼。

5.1.1.2 產品應確保每一台金鑰之唯一性。

5.1.1.3 產品需具備身分鑑別機制，且該身分鑑別機制應能防止重送攻擊。

5.1.2 權限管控

5.1.2.1 產品的存取權限須控管，應切割成數個使用者角色，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。

5.1.2.2 產品在登入通行碼的設計須有輸入頻率與次數限制。

5.1.3 通行碼鑑別

5.1.3.1 產品預設通行碼之設定都須相異，或應於產品首次成功取得存取之授權時，要求強制預設通行碼之更改。

5.2 已知漏洞安全

5.2.1 作業系統與網路服務

5.2.1.1 產品之作業系統與網路服務，不應存在國家弱點資料庫所公開的常見弱點與漏洞資料，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為高風險。

5.2.2 網路服務連接埠安全

5.2.2.1 產品啟用之功能與網路服務須為廠商提供必要服務之所需。

5.2.3 資訊安全管理

5.2.3.1 廠商須對所生產之產品提供漏洞揭露與改善措施政策宣告。

5.2.3.2 廠商須提供產品安全開發說明文件。

5.2.3.3 廠商須提供產品設置之安全指南。

5.2.3.4 廠商所生產之產品須清楚顯示產品型號名稱於實體介面。

5.3 軟韌體更新

5.3.1 更新安全

5.3.1.1 產品須具備韌體更新機制，且即使發生更新失敗時，系統能回復正常運作。

5.3.1.2 產品之更新路徑須通過安全通道，以確保韌體之機密性、正確性及完整性，且安全通道版本須符合「附錄 A」的要求，同時金鑰交換協議應支援前向保密 (Forward Secrecy)。

5.3.1.3 產品須定期檢查是否有可用之安全更新，並顯示產品版本更新狀態。

5.3.1.4 廠商須提供產品支援更新之期限。

5.4 資料機密性與完整性

5.4.1 安全敏感性資料儲存

5.4.1.1 韌體檔案不應置於公開存取之位置，韌體須加密保護以確保機密性，且須採用 NIST SP 800-140C[(6)]與 NIST SP 800-131A[(7)]所核可之同等或以上強度的加密演算法；亦或是韌體不應存在未宣告之相連伺服器 IP 和 URL，與明文或可被解密回復之安全敏感性資料。

5.4.1.2 產品所儲存之安全敏感性資料應加密儲存，而保護資料的加密方式須採用 NIST SP 800-140C 與 NIST SP 800-131A 所核可之同等或以上強度的加密演算法。

5.4.2 傳輸資料保護

5.4.2.1 資料傳輸須走安全通道，以確保資料之機密性、正確性及完整性，且安全通道版本須符合「附錄 A」的要求，同時金鑰交換協議應支援前向保密 (Forward Secrecy)。

5.4.2.2 產品之身分鑑別因子應加密傳輸，而保護資料的加密方式須採用 NIST SP 800-140C 所核可之加密演算法。

5.5 系統完整性

5.5.1 實體入侵防護

5.5.1.1 不得經由實體介面存取產品作業系統之除錯模式，或該實體介面之存取須通過身分鑑別。

5.5.2 輸入驗證

5.5.2.1 產品之本地端管理介面應驗證輸入的語法和內容。

5.6 資源可用性

5.6.1 資源管理

5.6.1.1 產品須在服務中斷恢復後，系統能回復正常運作。

5.7 隱私保護

5.7.1 隱私保護能力

5.7.1.1 產品所收集之敏感性個人資料，須為廠商必要之所需，且應提供消費者刪除敏感性個人資料之功能及服務。

5.7.1.2 產品所收集之遙測數據，應取得消費者之同意，且須說明遙測數據之使用目的和使用者(包括供第三方廠商)。

5.8 警示與紀錄

5.8.1 安全事件警示

5.8.1.1 產品之使用者登錄介面發生使用者異常登入安全事件時，須具備主動告警機制，包括回報管理者或推播警示、告警及設備識別碼編號等訊息。

附錄 A
(規定)
安全通道版本使用要求

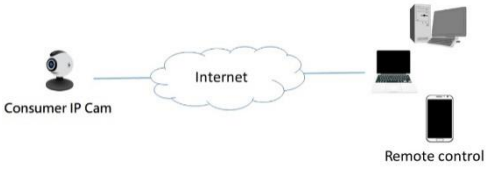
指超文本傳輸協定(HTTP)結合安全套接層協定(SSL)或傳輸層安全性協定(TLS)，建立安全通道以保護傳輸中資料不被竊取之技術；然而安全套接層協定在 2014 年 10 月由 Google 指出其資訊安全漏洞，宣布將全面禁用，所以已經完全由傳輸層安全性協定取代安全套接層協定。但傳輸層安全性協定 1.0 存在可以降級到安全套接層協定 3.0 的功能，使得傳輸層安全性協定 1.0 同樣不被信任，因此目前本標準應使用的版本為：

傳輸層安全性協定 v1.2 同等或以上之版本。

附錄 B
(參考)
網路攝影機之分類

網路攝影機依功能與使用對象可區分為二類，分別為消費性網路攝影機(Consumer IP camera)與影像監控網路攝影機(IP Camera)。由其功能和產品特性，如下表 B.1 所示：

表 B.1 網路攝影機之分類

設備名稱	消費性網路攝影機	影像監控網路攝影機
使用目的與系統組成	由消費者自行安裝之網路攝影機，主要安裝在使用者個人之場所，所攝影之對象及內容，均為較私密之個人隱私，且大部份消費性網路攝影機具有聲音雙向傳輸與遠端鏡頭控制功能，可透過網際網路，於消費性網路攝影機網路服務平台與消費者監看設備間傳輸，可強化日漸需求所增加的消費性網路攝影機之資安防護，以確保消費者個人隱私安全。	影像監控系統，又稱安控系統，目的是監看特定場所以達到維安目的，主要是由影像監控網路攝影機、數位影像錄影機、網路影像錄影機及網路儲存裝置組成。
系統示意圖		
功能/特性	▪ 購買與銷售之主要對象為一般消費者。 ▪ 適用在寵物關懷、幼兒照護、長輩照顧和居家安全...等。 ▪ 具有連網與 Wi-Fi 功能。 ▪ 可透過網路服務平台遠端連線觀看。 ▪ 操作簡單，方便安裝。	▪ 購買與銷售之主要對象為一般企業或需安防之場所，例如：國防單位、金融機構、政府機構、博物館、賭場...等。 ▪ 適用在近端監看特定場所以達到維安目的。 ▪ 具有 ONVIF 功能。 ▪ 支援 PoE 網路供電。 ▪ 需進行設定及規劃安裝配置。

附錄 C
(參考)
消費性網路攝影機安全需求

根據本標準之適用範圍定義消費性網路攝影機資產列表，如下表 C. 1 所示。

表 C. 1 消費性網路攝影機資產列表

資產名稱	敘述
實體	實體為組成產品的各組件，包括主機板、電路板、除錯介面、外接儲存裝置、電源裝置。
韌體	燒錄在消費性網路攝影機硬體模組或控制器之控制晶片中、非屬檔案系統(File System)類型之軟體。
安全敏感性資料	攝影之影像聲音資料、消費性網路攝影機網路服務平台傳送的控制指令或身分驗證。
通訊協定	有線網路(RJ45)或無線網路(Wi-Fi、行動網路、藍牙)。
日誌資料	記錄系統安全事件或是使用者操作的資料。
系統組態檔	定義作業系統及軟體運作方式之重要設定檔，如: 伺服器 IP、FTP 設定等。
作業系統	控制消費性網路攝影機、硬體模組，包含或不包含檔案系統(File System)之核心軟體。
內建應用程式	韌體或作業系統中所包含，提供消費性網路攝影機服務之應用程式(如網路服務，身分識別及授權，語音辨識等)。
使用者介面(UI)	使用者針對裝置進行設定及操作之介面。
應用程式介面(API)	消費性網路攝影機之內建應用程式和外部應用程式(如雲端伺服器、配套應用程式等)進行銜接的特定資訊傳輸格式。

根據上述步驟所識別之消費性網路攝影機之資產項目，經分析定義出其衍生之常見資安威脅，透過下列說明各資產與其資安威脅之關聯。

(a) 實體

(1) 主機板、電路板：主機板、電路板被有心人士加入惡意晶片，透過惡意晶片發動攻擊，透過回傳影像聲音資料功能傳送惡意程式至消費性網路攝影機網路服務平台，以取得平台控制權監控或竊取敏感資料。

(2) 除錯介面：透過實體埠更新偽造韌體或竄改設定資料，導致影像聲音資料傳送至非法伺服器成為公開存取資料。

(3) 外接儲存裝置：透過破壞產品外殼，竊取外接儲存裝置(例如:記憶卡)資料造成儲存影像資料丟失，或產品功能異常。

(4) 電源裝置：破壞電源裝置造成產品關機無法運作。

(b) 韌體、作業系統、內建應用程式

韌體本身可能存在未經修補之已知資安漏洞；韌體遭竄改植入惡意程式，安裝至該品牌型號產品後，可能導致該品牌型號之消費性網路攝影機產品遭駭客控制與監看，或回傳已被植入惡意程式的影像資料，造成消費性網路攝影機網路服務平台受到攻擊。

(c) 安全敏感性資料

消費性網路攝影機與消費性網路攝影機網路服務平台進行身分驗證時，恐遭攔截竄改，或竄改消費性網路攝影機網路服務平台發送之控制指令等，發動 DoS 攻擊，癱瘓系統運作。

(d) 通訊協定

駭客利用已知通訊協定漏洞，潛入傳送通道監聽身分認證和回傳的資料，利用假冒消費性網路攝影機，回傳偽造的影像資料，導致消費者觀看的影像為錯誤資訊，影響民眾出門後無法觀察到家中的狀況。

(e) 使用者介面、應用程式介面

開啟非產品使用之必要服務介面，導致機密或隱私資料外洩，例如遠端監看遙控消費性網路攝影機鏡頭。

根據識別之資產可能遭遇的威脅建立威脅模型，以 ETSI TVRA[(1)]所定義的風險評估方法進行評量。首先，將威脅對於資產的影響嚴重程度，程度分為 Low、Medium 和 High 三級；接著以發動一次攻擊所需的時間(Time)、攻擊者的專業度(Expertise)、對資產熟悉程度(Knowledge)、發動攻擊的機會(Opportunity)、與攻擊所使用的工具專業度(Equipment)進行潛在攻擊的可能性(likelihood of attack)的識別；最後，資產影響程度

(Asset Impact)與發動攻擊的強度(Intensity)進行風險等級劃分。完成的威脅分析結果，如下表 C. 2 所示，其中風險等級定義如下：

(a) Critical: 供應商和用戶的主要利益受到威脅，應最大程度的降低風險。

(b) Major: 對相關資產的威脅可能會發生，儘管其影響不太可能是致命的，但應該確實處理風險，並通過適當緩解對策來將風險最小化。

(c) Minor: 造成較小風險的資安威脅，根本不需要採取緩解對策。

表 C. 2 威脅分析表

威脅	弱點	不良後果	風險等級
Stored data analysis	1. 儲存中敏感資料未加密 2. 日誌存有敏感資料	1.儲存中的密碼未經過 hash 處理，且/或金鑰未經過加密，且權限控管不當，一旦作業系統層被入侵，敏感資料外洩，將遭受更嚴重的攻擊 2.日誌資料中有敏感資料被顯示出來	Critical
	韌體 hardcode 敏感資料	韌體放在公眾可取得，或者是可以從 flash 中萃取出來，該韌體又 hardcode 敏感資料造成敏感資料外洩，將遭受更進一步的駭客攻擊	Critical
Authentication factor leakage	認證因子明文傳輸	認證時，相關身分認證因子，例: 密碼、憑證，會因為傳輸通道沒有加密而導致敏感資料可被有心人士擷取	Critical
Secret stolen	不必要的功能/服務沒有關掉	產品存在不必要功能/服務，導致機密資料外洩，例:偷傳資料回惡意伺服器、回傳敏感區域之監控影像	Critical
	沒有限制收集不必要的敏感性個人資料	導致機密資料或個人隱私外洩	Critical

威脅	弱點	不良後果	風險等級
1. Fabrication of data 2.Replay/MITM control message	1.接收端或通訊 API 沒有驗證資料的完整性及真確性 2.接收端或通訊 API 沒有驗證控制訊息來源的真確性、或未鑑別傳送控制訊息者身分	1.傳送至伺服器的資料被竄改 2.攔截控制指令，重送攻擊或竄改指令	Critical
Masquerade as IoT device	1. 實體/通訊介面沒有支援認證功能 2. 裝置本身沒去驗裝載韌體的完整性及真確性，裝置的實體/遠端通訊介面也沒有身分認證機制	1. 重刷有帶 malware 的韌體，或從實體/遠端通訊介面入侵，取得管理者權限，可以控制該合法機器，執行任意動作 2. 在另一台 IoT 裝置載入合法韌體，複製認證因子，偽造另一台同型機種	Critical
Denial of service	程式設計未對控制代碼及格式加以限制	透過槽糊測試方法造成設備崩潰或找出漏洞	Critical
Firmware eavesdropping	接收端或通訊API沒有驗證資料的完整性及真確性	安裝植入惡意程式的韌體，控制感測器運作，傳送錯誤感測資料或發動 DoS/DDoS 攻擊癱瘓服務	Critical
Software vulnerabilities	設備韌/軟體之漏洞被有心人士利用	設備之軟/韌體 bugs 或設定錯誤而容易攻擊，對網路安全造成風險	Critical
Denial of transmission	無資安事件警示功能	當使用者介面遭遇異常登入時無法立即因應	Major
Power/Network outage	欠缺備援電源/網路	惡意斷電或斷網導致設備關機或無法運作	Major

根據上述步驟，識別消費性網路攝影機的資產與資安威脅，排除非適用範圍所定義之資產衍生的威脅，透過威脅分析衍生出消費性網路攝影機之緩解對策(即資安需求)，詳見表 C. 3。

表 C. 3 安全需求緩解對策表

威脅	緩解對策	風險等級(原)	風險等級(緩解後)
Stored data analysis	5.1.3.1 廠商所生產之產品，其設定預設通行碼都須相異；抑或首次成功取得產品存取之授權，須強制更改預設通行碼。	Critical	Major
Stored data analysis	5.1.2.2 產品在登入通行碼的設計須有輸入頻率與次數的限制。	Critical	Major
Stored data analysis	5.4.1.1 韌體檔案不應置於公開存取之位置，韌體須加密保護以確保機密性，且須採用 NIST SP 800-140C 所核可之同等或以上強度的加密演算法；亦或是韌體不應存在未宣告之相連伺服器 IP 和 URL，與明文或可被解密回復之安全敏感性資料。 5.4.1.2 產品所儲存之安全敏感性資料應加密儲存，而保護資料的加密方式須採用 NIST SP 800-140C 所核可之同等或以上強度的加密演算法。	Critical	Minor
Authentication factor leakage	5.4.2.2 產品之身分鑑別因子應加密傳輸，而保護資料的加密方式須採用 NIST SP 800-140C 所核可之加密演算法。	Critical	Minor
Secret stolen	5.2.2.1 產品啟用之功能與網路服務須為廠商提供必要服務之所需。	Critical	Minor
1. Fabrication of data 2. Replay/MITM control message	5.4.2.1 資料傳輸須走安全通道，以確保資料之機密性、正確性及完整性，且安全通道版本須符合「附錄 A」的要求。	Critical	Minor
Masquerade as IoT	5.1.1.1 每個產品應有一組唯一的識別碼。	Critical	Minor

威脅	緩解對策	風險等級(原)	風險等級(緩解後)
device	5.1.1.2 產品應確保每一台金鑰之唯一性。		
Masquerade as IoT device	5.1.2.1 產品的存取權限須控管包括管理介面、通訊協定、API，應切割成數個使用者角色，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。 5.5.1.1 預設不應透過實體介面存取產品作業系統之除錯模式，或該實體介面之存取須通過身分鑑別。 5.2.1.1 產品之作業系統與網路服務，不應存在國家弱點資料庫所公開的常見弱點與漏洞資料，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為高風險。	Critical	Minor
Denial of service	5.5.2.1 產品之管理介面應驗證任何輸入的語法和內容。	Critical	Minor
Firmware eavesdropping	5.3.1.2 產品之更新路徑須通過安全通道，以確保韌體之機密性、正確性及完整性，且安全通道版本須符合「附錄 A」的要求，同時金鑰交換協議應支援前向保密 (Forward Secrecy) 。	Critical	Minor
Software vulnerabilities	5.3.1.1 產品須具備軟韌體更新機制，且即使發生更新失敗時，系統能回復正常運作。	Critical	Minor
Denial of transmission	5.8.1.1 產品之網頁介面、遠端指令控制介面、應用程式介面、實體介面發生使用者登入系統安全事件時，須具備主動告警機	Major	Minor

威脅	緩解對策	風險等級(原)	風險等級(緩解後)
	制，包括回報管理者或推播警示、告警及設備識別碼編號等訊息。		
Power/Network outage	5.6.1.1 產品須在服務中斷恢復後，系統能回復正常運作。	Major	Minor

附錄 D
(參考)
安全要求事項與各標準規範對照表

本標準與 ETSI EN 303 645 之比對結果，如下表所示：

表 D. 1 安全要求事項與各標準規範對照表

對應標準規範	
本標準要求事項	ETSI EN 303 645
5.1.1.1 每個產品應有一組唯一的識別碼。	5.4 Securely store sensitive security parameters 5.4.2
5.1.1.2 產品應確保每一台金鑰之唯一性。	5.4 Securely store sensitive security parameters 5.4.4
5.1.1.3 產品需具備身分鑑別機制，且該身分鑑別機制應能防止重送攻擊。	5.5 Communicate securely 5.5.4
5.1.2.1 產品的存取權限須控管，應切割成數個使用者角色，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。	5.1 No universal default passwords 5.1.4
5.1.2.2 產品在登入通行碼的設計須有輸入頻率與次數限制。	5.1 No universal default passwords 5.1.5
5.1.3.1 預設通行碼之設定都須相異，或應於產品首次成功取得存取之授權時，要求強制預設通行碼之更改。	5.1 No universal default passwords 5.1.1, 5.1.2, 5.1.3
5.2.1.1 產品之作業系統與網路服務，不應存在國家弱點資料庫所公開的常見弱點與漏洞資料，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為高風險。	5.6 Minimize exposed attack surfaces 5.6.6
5.2.2.1 產品啟用之功能與網路服務須為廠商提供必要服務之所需。	5.6 Minimize exposed attack surfaces 5.6.1, 5.6.2, 5.6.5, 5.6.7
5.2.3.1 廠商須對所生產之產品提供漏洞揭露與改善措施政策宣告。	5.2 Implement a means to manage reports of vulnerabilities 5.2.1, 5.2.2, 5.2.3
5.2.3.2 廠商須提供產品安全開發說明文件。	5.6 Minimize exposed attack surfaces 5.6.9
5.2.3.3 廠商須提供產品設置之安全指南。	5.8 Ensure that personal data is secure 5.8.3 5.12 Make installation and maintenance

對應標準規範	
本標準要求事項	ETSI EN 303 645
	of devices easy 5.12.1, 5.12.2, 5.12.3
5.2.3.4 廠商所生產之產品須清楚顯示產品型號名稱於實體介面。	5.3 Keep software updated 5.3.16
5.3.1.1 產品須具備韌體更新機制，且即使發生更新失敗時，系統能回復正常運作。	5.3 Keep software updated 5.3.1, 5.3.3, 5.3.4, 5.3.8, 5.3.12 5.9 Make systems resilient to outages 5.9.3
5.3.1.2 產品之更新路徑須通過安全通道，以確保韌體之機密性、正確性及完整性，且安全通道版本須符合「附錄 A」的要求，同時金鑰交換協議應支援前向保密 (Forward Secrecy)。	5.3 Keep software updated 5.3.2, 5.3.7, 5.3.10
5.3.1.3 產品須定期檢查是否有可用之安全更新，並顯示產品版本更新狀態。	5.3 Keep software updated 5.3.5, 5.3.6, 5.3.11
5.3.1.4 廠商須提供產品支援更新之期限。	5.3 Keep software updated 5.3.13
5.4.1.1 韌體檔案不應置於公開存取之位置，韌體須加密保護以確保機密性，且須採用 NIST SP 800-140C[6]與 NIST SP 800-131A[7]所核可之同等或以上強度的加密演算法；亦或是韌體不應存在未宣告之相連伺服器 IP 和 URL，與明文或可被解密回復之安全敏感性資料。	5.4 Securely store sensitive security parameters 5.4.1, 5.4.3
5.4.1.2 產品所儲存之安全敏感性資料應加密儲存，而保護資料的加密方式須採用 NIST SP 800-140C 與 NIST SP 800-131A 所核可之同等或以上強度的加密演算法。	5.5 Communicate securely 5.5.3
5.4.2.1 資料傳輸須走安全通道，以確保資料之機密性、正確性及完整性，且安全通道版本須符合「附錄 A」的要求，同時金鑰交換協議應支援前向保密 (Forward Secrecy)。	5.5 Communicate securely 5.5.1, 5.5.2, 5.5.5, 5.5.7 5.8 Ensure that personal data is secure 5.8.1
5.4.2.2 產品之身分鑑別因子應加密傳輸，而保護資料的加密方式須採用 NIST SP 800-140C 所核可之加密演算法。	5.5 Communicate securely 5.5.6, 5.5.8
5.5.1.1 預設不得經由實體介面存取產品作業系統之除錯模式，或該實體介面之存取須通過身分鑑別。	5.6 Minimize exposed attack surfaces 5.6.3, 5.6.4
5.5.2.1 產品之管理介面應驗證任何輸入的語法和內容。	5.13 Validate input data 5.13.1

對應標準規範	
本標準要求事項	ETSI EN 303 645
5.6.1.1 產品須在服務中斷恢復後，系統能回復正常運作。	5.9 Make systems resilient to outages 5.9.1, 5.9.2
5.7.1.1 產品所收集之敏感性個人資料，須為廠商必要之所需，且應提供消費者刪除敏感性個人資料之功能及服務。	5.11 Make it easy for users to delete user data 5.11.1, 5.11.2, 5.11.3, 5.11.4 6 Data protection provisions for consumer IoT 6.3, 6.4
5.7.1.2 產品所收集之遙測數據，應取得消費者之同意，且須說明遙測數據之使用目的和使用者(包括供第三方廠商)。	6 Data protection provisions for consumer IoT 6.1, 6.2, 6.5
5.8.1.1 產品之使用者登錄介面發生使用者異常登入安全事件時，須具備主動告警機制，包括回報管理者或推播警示、告警及設備識別碼編號等訊息。	5.10 Examine system telemetry data 5.10.1

參考資料

(1) ETSI TS 102 165-1 V5.2.3 (2017-10), CYBER; Methods and protocols;Part 1: Method and pro forma for Threat,Vulnerability, Risk Analysis(TVRA)

(2) ETSI TS 103 645 V1.1.1 (2019-02), CYBER; Cyber Security for Consumer Internet of Things.

(3) IEC 62443-4-2-2018 Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components.

(4) NISTIR 8259 Draft (2nd) Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline.

(5) NIST, National Vulnerability Database, https://nvd.nist.gov/vuln/full-listing

(6) National Institute of Standards and Technology, NIST SP 800-140C, CMVP Approved Security Functions, available at URL: https://csrc.nist.gov/projects/cryptographic-module-validation-program

(7) National Institute of Standards and Technology, SP 800-131A Rev. 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths, available at URL: https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final

(8) FIRST, Common Vulnerability Scoring System version 3.1: Specification Document, https://www.first.org/cvss/specification-document