IoT-1001-1

影像監控系統資安標準

-第一部：一般要求

V1.0

經濟部工業局

中華民國 110 年 6 月

目錄

引言

物聯網科技是全世界發展最快速的產業，相關應用不斷推陳出新，不可否認，資訊安全是物聯網科技成功與否最主要的關鍵，因此經濟部工業局率先提出制定物聯網資安環境標準的目標，包括影像監控系統資安標準、車聯網系統資安標準、物聯網通用資安標準、輔助應用程式資安標準、工控系統資安標準、醫療儀器資安標準及銷售點終端系統資安標準等，促進國內產業整體優質化及產品競爭力，並確保消費者在影像監控裝置之運用上達到資訊安全的目的。

物聯網的盛行，使日常用品皆朝向數位化邁進，影像監控設備也是其中之一，運用範圍包括：車聯網、家聯網、醫聯網、社區聯網等，應用範圍十分廣泛。但隨之而來的問題是網路攻擊事件，從 2014 年起網路資安事件日益頻繁，攻擊事件規模越來越大，2016 年底以 Mirai 為名的惡意程式，藉由網路攝影機為跳板，製造出前所未聞之網路攻擊的手法。

有鑑於此，藉由參照國際物聯網相關資安標準/規範，如 CNS 27001(1)、ANSI/CAN/UL 2900-1：2017 標準(2)、Groupe Speciale Mobile Association (GSMA) IoT Security Guideline(3)、Open Web Application Security Project (OWASP) Top IoT Vulnerabilities(4)及日本政府的物聯網安全指導方針(5)等，建立國內在影像監控系統上資安品質的標準，包含 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、及 5.隱私保護，從此五大安全構面針對影像監控裝置詳盡載明應採取的共通方法。

IoT-1001 系列標準為影像監控系統相關，包括網路攝影機、影像錄影機及網路儲存裝置(統稱影像監控裝置)，IoT-2001 系列為驗證產品符合 IoT-1001 系列標準之測試方法及基準，「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」(以下簡稱本標準)，為其它 IoT-1001 系列標準的參照，包括「IoT-1001-2 影像監控系統資安標準-第二部：網路攝影機」(6)、「IoT-1001-3 影像監控系統資安標準-第三部：影像錄影機」(7)，及「IoT-1001-4 影像監控系統資安標準-第四部：網路儲存裝置」(8)，所有影像監控裝置應符合本標準中關於它的安全相關規定。

網路攝影機資安認驗證制定實際運行了 3 年，期間收集更多的產品使用情境及實驗室測試情境，此版本則根據上述情境運行心得進一步優化標準需求及測試方法，包括：

1. 資安需求更針對安防監控應用：相對於個人用之消費型網路攝影機著重在隱私的確保，安防用之網路攝影機目的以穩定提供服務為主，並確保監控設備及影像能正確執行其功能，依此調整相關安全需求。

2. 測試方法優化：納入更多的測試情境及案例，優化測試方法並增進測試一致性。

1. 適用範圍

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，由網路攝影機、數位影像錄影機、網路影像錄影機及網路儲存裝置組成，除此之外，監控所有攝影機畫面的監控中心，包括本地端或遠端電腦設備、行動裝置及雲端伺服器，及連接監控設備之網路環境，包括 Wi-Fi 存取點、路由器及交換機等，構成整個影像監控系統。

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] ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1： General Requirements

[2] CNS 27001：2013 資訊技術－安全技術－資訊安全管理系統－要求事項

[3] NIST SP 800-92 Guide to Computer Security Log Management

3. 用語及定義

下列用語及定義適用於本標準。

3.1 影像監控系統 (Video surveillance system)

又稱安控系統，目的是監看特定場所以達到維安目的，其應用常見於出入口人員監看、車庫或停車場等重要場所之監視，為確保維安目的能確實，該系統主要由以下幾種設備組成，包括：網路攝影機、影像錄影機及網路儲存裝置。

3.2 網路攝影機 (IP camera)

係指運用於影像監控系統且具連網功能的嵌入式攝影機，其類型包括：網路攝影機(IP camera)、智能攝影機(smart camera)及 3D 攝影機(3D camera)等。

3.3 影像錄影機 (Video recorder)

係指一種主要用於影像監控系統且具連網功能的影像錄影機，其應用類型包括：數位影像錄影機(Digital Video Recorder，DVR)與網路影像錄影機(Network Video Recorder， NVR)等。

(a) 數位影像錄影機(DVR)：為一種封閉式架構之影像儲存管理設備，支援 NTSC、PAL 等影像格式，並支援有線(例如：同軸電纜)之前端攝影機，其影像儲存支援內建儲存媒體。

(b) 網路影像錄影機(NVR)：為一種開放式架構之影像儲存管理設備，支援 H.264、AVI 等影像格式，並支援有線(例如：網路線)及無線(例如：WiFi)之前端攝影機，其影像儲存支援本地端或遠端之儲存媒體。

3.4 網路儲存裝置 (Network attached atorage)

係指於網路上專門提供資料儲存的裝置，運行資料存取等相關管理功能，並支援多種檔案傳輸協定，使不同作業系統或執行不同協定的電腦皆可存取網路儲存裝置。

3.5 嵌入式 (Embedded)

係指基於微處理器具有專一功能和計算效能的電腦系統，通常會嵌入在一個數位硬體和機械部件的完整裝置中。

3.6 資訊安全弱點 (Security vulnerability)

指裝置安全之缺陷，使得系統或應用程式資料之保密性、完整性及可用性面臨威脅。

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

係指美國國土安全部贊助之弱點管理計畫，該計畫針對每一弱點項目賦予其全球認可唯一共通編號。

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

係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(9)，負責 3.3 常見弱點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)

為一套漏洞評鑑系統的判定標準，包括威脅所造成損害的嚴重性、資安漏洞的可利用程度與攻擊者不當運用該漏洞的難易度，都被列入評比。評比從 0 分到 10 分，0 代表沒有弱點，而 10 則代表最高風險(10)。

3.10 嚴重性等級 (Severity rating)

係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 敏感性資料 (Sensitivity data)

指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介建立、儲存或傳輸之資訊，而該資訊之洩漏可能對使用者造成損害之虞，包括但不限於個人資料、通行碼、金鑰或地理位置等。

3.12 個人資料 (Personally identifiable information)

依「個人資料保護法」(11)第一章第二條第一項定義為自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

3.13 隱私 (Privacy)

係指私人資訊，此一資訊的全部或部份不可被公開，且所有人有權利去保護的部分，本文所指之隱私包括影像監控裝置所錄製之影像及用戶資訊。

3.14 操控程式 (Control program)

係指用於控制影像監控裝置動態或瀏覽監控內容之應用程式，包括行動版及電腦版應用程式。

3.15 管理介面 (Management Interface)

係指透過本地端或遠端網路取得裝置作業系統的操控權，如：

(a) 於操控程式、網頁管理介面或指令介面執行產品維護、存取裝置資源、監看畫面或操控鏡頭。

(b) 於操控程式、網頁管理介面或指令介面進行系統設定，例如：網際網路協定位址(IP)。

3.16 應用程式介面 (Application Program Interface, API)

係指軟體系統不同組成部分銜接的約定。目前影像監控裝置最普遍使用的是Open Network Video Interface Forum (ONVIF)應用程式介面，用戶透過超文本傳輸協定(HTTP)傳遞 ONVIF 應用程式介面，實現網路攝影機相關操作應用程式，例如：系統資訊擷取、監控影像擷取等。

3.17 第三方函式庫 (3rd party library)

係指系統程式設計者為加速開發，引用其他組織所製作具備某特定功能之函式庫，以滿足裝置所需提供的服務。

3.18 加密 (Encryption)

係指明文資訊透過數學演算法進行改變，使原來的資料不可讀而達到保密的目的。

3.19 數位簽章 (Digital signature)

係指簽署人以私鑰簽名經由數學演算法處理過後產生一定長度之電子文件，形成電子簽章，並得以公開金鑰進行驗證，不僅可確保該文件的完整性，同時驗證文件作者的不可否認性。

3.20 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，如：目前常見之實作通訊協定為安全套接層(Secure Sockets Layer, SSL)和傳輸層安全性(Transport Layer Security, TLS)。

3.21 安全區域 (Secure domain, Secure world)

係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，如：加解密、金鑰管理、完整性檢查，並供敏感性資料保存用。

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

資通訊終端設備(如：個人電腦) 一致性安全設定規範(如：通行碼長度、更新期限等)(12)，以降低駭客入侵與導致資安事件之疑慮。

3.23 通行碼 (Password)

係指一組字元串能讓系統辨識用戶身分，並可進一步控管用戶存取系統之權限。

3.24 預設通行碼 (Default password)

係指產品出廠預先設定好的通行碼，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，用以登入影像監控裝置之通行碼。

3.25 裝置鑑別 (Device authentication)

係指受測物為驗證相連裝置之身分，以確保傳輸對象身分是否可信賴，常用之鑑別方式可能是要求相連裝置提交使用者名稱及通行碼，或者是相連裝置之數位憑證來確認裝置之身分。

3.26 安全事件日誌 (Security event log)

係指記錄每個稽核規則所定義的活動，用以察覺威脅或攻擊事件的發生，本文之安全事件即是指用戶登入系統之行為。

3.27 通用隨插即用通訊協定 (Universal Plug and Play, UPnP)

在區域網路環境下(例如：家庭網路或公司網路等)，使各種裝置能夠直接互相連線，同時自行設定組態以進行資料分享。

3.28 簡單網路管理協定 (Simple Network Management Protocol, SNMP)

將網路設備區分為管理器(Manager)及代理器(Agent)二個角色。代理器以變數呈現本身所收集之網域的網路狀態資料；而管理器透過 GET 等指令收集代理器所傳回的資訊。

3.29 零配置通訊協定 (Bonjour)

在區域網路環境下(例如：家庭網路或公司網路等)，提供自動搜尋網路設備的服務。Bonjour 使用 IP 通訊協定，在無應設定 IP 位址或 DNS 伺服器的情況下，設備即可自行發現彼此。

3.30 Wi-Fi 保護設置 (Wi-Fi Protected Setup, WPS)

由 Wi- Fi 聯盟推出的一個通訊協定，得以簡化使用者在無線安全性方面的設定，假如無線接入點啟動 WPS 模式之後，使用者僅需要在用戶端(Client)按下按鈕便即可連線，無應任何繁複的安全性設定。WPS 分二種連線方式，一種是以 PIN 碼連線，另一種 PBC 模式(Push-Button Connection)是透過按按鍥的方式，啟動連線。

3.31 Wi-Fi 保護存取 (Wi-Fi Protected Access, WPA)

用以保護網路傳輸安全之加密方式，分成 WPA 與 WPA2 兩個標準，改善有線等效加密(WEP)所存在的網路弱點。WPA 採用 Michael 訊息認證碼與 RC4 加密演算法；而 WPA2 採用的是 CCMP 訊息認證碼與 AES(Advanced Encryption Standard)(13)加密演算法。

3.32 多因子鑑別 (Multi-factor authentication, MFA)

係指身分鑑別應透過二種以上因素的鑑別機制後，得以獲得裝置之存取權限。多因子鑑別主要依據密碼學身分鑑別的三個因素，包括所知之事(something you know)、所持之物(something you have)、所具之形(something you are)，於不同階段對同一裝置進行身分鑑別。

3.33 前向安全 (Forward Secrecy, FS)

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

3.34 除錯模式 (Debug mode)

又稱工程模式(Engineer Mode)，一般於開發或修補階段，產品會處在此模式中，此模式可存取之系統資源不會受限，且還會顯示錯誤訊息提供工程人員除錯用。

3.35 遙測資料(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。

4. 安全等級

安全等級係為降低或消弭產品之資訊安全威脅，透過最適之安全組合，確保產品達到安全之要求。

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；第二欄為安全要求分項，係依各安全構面設計對應之安全要求分項；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，應依循本節 5.1 至 5.5 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	-	-
	5.1.2. 實體異常行為警示	-	5.1.2.1 5.1.2.2	-
	5.1.3. 實體防護	5.1.3.1	-	-
	5.1.4. 安全啟動	-	-	5.1.4.1
系統安全	5.2.1. 作業系統與網路服務安全	5.2.1.1	5.2.1.1	5.2.1.2
	5.2.2. 最小化網路與服務安全	5.2.2.1 5.2.2.2	-	-
	5.2.3. 更新安全	5.2.3.1 5.2.3.2 5.2.3.3 5.2.3.4 5.2.3.5	-	-
	5.2.4. 敏感性資料儲存安全	5.2.4.1 5.2.4.2	5.2.4.3	5.2.4.4
	5.2.5. 網頁管理介面安全	5.2.5.1	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
	5.2.6. 操控程式之應用程式安全	5.2.6.1 5.2.6.2 5.2.6.3	-	-
	5.2.7. 安全事件日誌檔與警示	5.2.7.1 5.2.7.2 5.2.7.3	-	-
通訊安全	5.3.1. 敏感性資料傳輸安全	5.3.1.1	5.3.1.2	5.3.1.3
	5.3.2. 通訊協定與設置安全	5.3.2.1 5.3.2.2	5.3.2.3	-
	5.3.3. Wi-Fi 通訊安全	5.3.3.1 5.3.3.2	5.3.3.3	5.3.3.4
身分鑑別與授權機制安全	5.4.1. 鑑別機制安全	5.4.1.1 5.4.1.2	5.4.1.3 5.4.1.4	5.4.1.5 5.4.1.6
	5.4.2. 通行碼鑑別機制	5.4.2.1 5.4.2.2 5.4.2.3 5.4.2.4	-	5.4.2.5 5.4.2.6
	5.4.3. 權限控管	5.4.3.1 5.4.3.2	-	-
隱私保護	5.5.1. 隱私資料的存取保護	5.5.1.1 5.5.1.2	-	-
	5.5.2. 隱私資料的傳輸保護	5.5.2.1	5.5.2.2	5.5.2.3

4.1.1 **安全構面：**

(a) 實體安全：產品輕易被拆解與否，或產品資料存儲與測試用連接埠的處置，應視為實體安全要求的標的。

(b) 系統安全：產品之作業系統、網路服務、更新服務及韌體程式設計等，應具備足夠之安全防護。

(c) 通訊安全：敏感性資料之通訊安全，和通訊服務存在未知之資安漏洞與否。

(d) 身分鑑別與授權機制安全：溝通介面，包括遠端指令管理介面、網頁管理介面、操控程式等，應確保鑑別與授權相關機制。

(e) 隱私保護：影像監控裝置之隱私，包括使用者之影像資料，於存取與傳輸的保護及權限管控等，確保隱私資料不應外洩。

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，且每一安全要求分項包含一個以上之安全要求。

4.1.3 安全等級：

安全等級依(1)相關資安風險高低、(2)技術實現複雜度綜合考量，分為 1 級、2 級、3 級三個等級。其對應之列即其所應符合的安全要求分項，安全等級級數的大小代表安全等級的高低，欲符合較高等級之安全要求應先滿足較低安全等級要求。

5. 一般要求

本節詳盡載明影像監控裝置為滿足安全功能應採取的共通方法，所有影像監控裝置應符合本節中所有安全要求。

5.1 實體安全要求

5.1.1 實體埠之安全管控

5.1.1.1 產品預設不應透過實體介面存取產品作業系統之除錯模式。 若需經實體介面存取，則應通過身分鑑別作業始得執行。

5.1.2 實體異常行為警示

5.1.2.1 產品應具有實體埠插拔操作記錄功能。

5.1.2.2 產品應具備相關警示功能於實體操作發生斷訊時。

5.1.3 實體防護

5.1.3.1 產品外部不應有徒手即可還原預設通行碼的功能。

5.1.4 安全啟動

5.1.4.1 產品應支援安全啟動(Secure Boot)功能，不應以未經授權的韌體、驅動程式及作業系統執行開機，以確保系統的完整性及可信度。

5.2 系統安全要求

5.2.1 作業系統與網路服務安全

5.2.1.1 產品之作業系統與網路服務，不應存在美國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 嚴重性等級評比為重大。

5.2.1.2 產品之作業系統與網路服務，不應存在美國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。

5.2.2 最小化網路與服務安全

5.2.2.1 產品開啟之網路服務應為廠商提供必要服務之所需，防止產品因啟用網路介面而被侵入的可能性，且廠商應於產品文件中標註得啟用之網路服務，避免未宣告之網路服務被開啟。

5.2.2.2 產品所收集之遙測資料應告知使用者，且未告知之遙測資料不應被收集。

5.2.3 更新安全

5.2.3.1 韌體應具備更新機制。

5.2.3.2 產品若支援離線手動更新，則更新檔案應加密保護以確保機密性，且應採用 NIST SP 800-140C, CMVP Approved Security Functions(14)所核可之同等或以上加密演算法；抑或是產品韌體之程式碼與安裝檔內其它檔案中，不應存在明文或甚至可被解密回復之敏感性資料。

5.2.3.3 產品若支援線上更新，其更新路徑應通過安全通道，且安全通道版本應符合「附錄 A」的要求，同時金鑰交換協議應支援前向安全功能(Forward Secrecy)，其中於身分鑑別過程應驗證憑證合法性，以及有效性(如：發證機構、有效期限、憑證格式及憑證簽章等)。

5.2.3.4 產品應具備驗證韌體之完整性及真確性的功能。

5.2.3.5 產品應具備備援更新功能，即發生更新失敗時，系統能回復至更新前之狀態。

5.2.4 敏感性資料儲存安全

5.2.4.1 產品所儲存的敏感性資料，應僅由獲授權個體存取。

5.2.4.2 產品所儲存之身分鑑別因子、加解密用之金鑰(不含非對稱加密用之公鑰)不應明文儲存，而保護資料的方式應採用 NIST SP 800-140C, CMVP Approved Security Functions 所核可之安全功能。

5.2.4.3 產品應提出金鑰管理程序，以確保金鑰管理的品質。

5.2.4.4 敏感性資料應存放於產品的安全區域(Security Domain)，與正常作業環境隔離。

5.2.5 網頁管理介面安全

5.2.5.1 產品之網頁管理介面不應存在引發 Injection 及 Cross-Site Scripting (XSS)攻擊之漏洞。

5.2.6 .ONVIF (Open Network Video Interface Forum)應用程式介面(API)安全

5.2.6.1 ONVIF 應用程式介面，應具備身分鑑別機制，且其鑑別機制安全依 5.4.1.1 及 5.4.1.2 之要求。

5.2.6.2 ONVIF 應用程式介面，其通行碼鑑別安全依 5.4.2 該要求項之所有要求。

5.2.6.3 ONVIF 應用程式介面，其權限管控依 5.4.3 該要求項之所有要求。

5.2.7 安全事件日誌檔與警示

5.2.7.1 應具備安全事件日誌與顯示功能，確實記錄使用者的存取行為，得以查核未授權或異常的登入操作。其內容應包括完整時間戳記、使用者身分及執行結果，供後續查閱之用。

5.2.7.2 產品之安全事件日誌應具備權限控管機制，該日誌檔不應允許未經授權的存取。

5.2.7.3 產品之安全事件日誌檔應具備日誌滾動(log rotate)機制。

5.3 通訊安全要求

5.3.1 敏感性資料傳輸安全

5.3.1.1 敏感性資料之網路傳輸預設應通過安全通道，且安全通道版本應符合「附錄 A」的要求，同時金鑰交換協議應支援前向安全功能(Forward Secrecy)。

5.3.1.2 接收敏感性資料傳輸之安全通道，其中於身分鑑別過程應驗證憑證真確性及有效性，如：發證機構、有效期限、憑證格式及憑證簽章等。

5.3.1.3 傳輸敏感性資料之安全通道，應支援 AES-256 同等或以上加密強度的演算法。

5.3.2 通訊協定與設置安全

5.3.2.1 產品應提供使用者得自行開/關「網路裝置資訊探詢」功能，包括：通用隨插即用通訊協定 (UPnP)、簡單網路管理協定 (SNMP) 及零配置通訊協定 (Bonjour)。

5.3.2.2 預設不應透過網路連線存取產品作業系統之除錯模式。

5.3.2.3 產品之關鍵通訊協定(見附錄 B)，不應存在錯誤處理漏洞，包括訊息長度、訊息識別碼及關鍵協定屬性等欄位，導致產品因發生崩潰而服務中止的情形。

5.3.3 Wi-Fi 通訊安全

5.3.3.1 產品應提供使用者得自行開/關「Wi-Fi 保護設置 (WPS)」之 WPS PIN 功能，而其預設值應為關閉狀態。

5.3.3.2 Wi-Fi 的安全機制預設應採用「Wi-Fi 保護存取 (WPA)」，且 Wi-Fi 保護存取之版本應符合「附錄 C」的要求。

5.3.3.3 產品支援 Wi-Fi 協定，則不應存在錯誤處理漏洞，包括檢視訊息長度、訊息識別碼及關鍵協定屬性等欄位，導致產品因發生崩潰而服務中止的情形。

5.3.3.4 Wi-Fi 認證安全機制應支援 802.1X 基於埠的網路存取控制(Port-Based Networks Access Control)。

5.4 身分鑑別與授權機制安全要求

5.4.1 鑑別機制安全

5.4.1.1 存取產品資源前，應透過具備防止重送攻擊之身分鑑別機制。

5.4.1.2 鑑別錯誤訊息不應顯露出合法使用者名稱。

5.4.1.3 產品應具備置換憑證之功能，以增加憑證鑑別機制之可信度。

5.4.1.4 產品每次還原出廠設定時，憑證之金鑰(包括 SSH 及 TLS)都應改變，確保每台產品金鑰之唯一性，及降低金鑰外洩可能引發之資安風險。

5.4.1.5 產品之鑑別機制應採用 PKI 或多因子鑑別(例: token, FIDO)等強鑑別機制。

5.4.1.6 相連之影像監控產品應支援雙向鑑別，確保相連裝置之可信度。

5.4.2 通行碼鑑別安全

5.4.2.1 廠商所生產之裝置，其預設通行碼都應相異；抑或首次成功取得產品存取之授權，應強制更改預設通行碼。

5.4.2.2 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼長度至少大於 8 個字元；抑或警示使用者其採用之通行碼強度不足。

5.4.2.3 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼中之字元應符合下列四種字元中的三種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.10 進位數字 (0 到 9)；4.非英文字母字元 (例如： !、$、#、%)；抑或警示使用者其採用之通行碼強度不足。

5.4.2.4 產品在登入通行碼的設計上應有輸入頻率及次數的限制，即：

(a) 最高五次嘗試登入失敗即鎖定帳戶或 IP。

(b) 在一定時間內應鎖定帳戶或 IP。

(c) 至少經過一定時間，始可將失敗的登入嘗試計數器重設為零次。

5.4.2.5 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼含使用者帳戶名稱全名中，不能包含 3 個以上之連續字元。

5.4.2.6 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼應執行歷程記錄。

備考：本節之通行碼鑑別安全原則，基於全世界對其規格各有其定義，送測廠商可提供符合國際標準要求，包括但不限於 NIST SP 800-63B, ENISA's ten security awareness good practices，或具公認資安產業慣例之規格(例：FBI: Building a Digital Defense with Passwords)來滿足此節要求。

5.4.3 權限管控

5.4.3.1 產品應將使用者角色切割成數個使用者環境，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。

5.4.3.2 產品之授權行為，應存在閒置時限供使用者設定，假如遠端連線逾時、遺失或結束，應要求新的鑑別

5.5 隱私保護要求

5.5.1 隱私資料的存取保護

5.5.1.1 產品所儲存的隱私資料，應被授權的個體始可存取。

5.5.1.2 每次發生新的隱私存取事件時，產品應主動發出警示。

5.5.2 隱私資料的傳輸保護

5.5.2.1 隱私資料之網路傳輸預設應通過安全通道，且安全通道版本應符合「附錄 A」的要求，同時金鑰交換協議應支援前向安全功能(Forward Secrecy)。

5.5.2.2 接收隱私資料傳輸之安全通道，其中於身分鑑別過程應驗證憑證真確性及有效性(如：發證機構、有效期限、憑證格式及憑證簽章等。

5.5.2.3 傳輸隱私資料之安全通道，應支援 AES-256 同等或以上加密強度的演算法。

附錄 A

(規定)

安全通道版本使用要求

係指超文本傳輸協定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

(規定)

影像監控裝置所使用之通訊協定

B.1 即時傳輸協定 (Real-time Transport Protocol, RTP) & 即時傳送控制協定 (Real-time Transport Control Protocol, RTCP)：

定義在 RFC 3550 規範中(16)，常應用於影音串流(Video Streaming)系統、視訊會議及一鍵通(Push to Talk)系統，其定義了在網際網路上傳遞音訊和影片的標準封包格式，而 RTCP 並不用於資料傳輸，而是支援 RTP 將多媒體資料封裝並發送，RTCP 會週期性地在一個 RTP 會議連線上以帶外(Out-of-Band)的方式提供統計及傳輸控制資訊，此協定之主要功能是為 RTP 提供服務品質(Quality of Service)的反饋(Feedback)。

B.2 即時串流協定 (Real Time Streaming Protocol, RTSP)：

定義在 RFC 2326 規範中(17)，用來控制具有即時性需求的資料，如影音多媒體資料的播放、錄製及暫停，可達到用戶端到媒體伺服器之間的即時影音控制。

B.3 傳輸層安全協定 (The Transport Layer Security, TLS)：

定義在 RFC 5246 規範中(18)，在兩個應用程式之間透過網路建立起安全通道，於交換資料時可防止遭受到竊聽及篡改。

附錄 C

(規定)

影像監控裝置所使用之 Wi-Fi 保護設置版本

Wi-Fi 保護設置版本，是一種保護 Wi-Fi 傳輸安全的機制。它實作 IEEE 802.11i 以取代有線等效加密安全性不足所引發的資安問題，然而 Wi-Fi 保護設置 v1 已經被破解了。目前本標準應使用的版本為：

Wi-Fi 保護設置 v2 同等或以上之版本

附錄 D

(參考)

技術要求事項與各標準規範對照表

表 D.1　技術要求事項與各標準規範對照表

技術要求	OWASP 對應項目(4)	ANSI/UL 2900-1 對應項目	ONVIF 對應項目(19-20)
5.1.1.1	I10： Poor Physical Security Ensuring only required external ports such as USB are required for the product to function. Ensuring the product has the ability to limit administrative capabilities.		-
5.1.2.1 5.1.2.2	-		-
5.1.3.1	I2 ： Insufficient Authentication/Authorization Ensuring that password recovery mechanisms are secure.		-
5.1.4.1	I9： Insecure Software/Firmware Implement the secure boot if possible (chain of trust).		-
5.2.1.1 5.2.1.2	-	13.1 13.2	-
5.2.2.1	I3： Insecure Network Services Ensuring only necessary ports are exposed and available.		-
5.2.3.1	I9： Insecure Software/Firmware Ensuring the device has the ability to update (very important, need secure update mechanism).	11.1 11.2	Core Spec. – Ver. 16.12 4.5.5 Firmware Upgrade

	Ensuring the update file is encrypted using accepted encryption methods. Ensuring the update file is transmitted via an encrypted connection. Ensuring the update file does not expose sensitive data.		
5.2.3.2	I9： Insecure Software/Firmware Ensuring the update is signed and verified before allowing the update to be uploaded and applied.	11.1 11.2 11.6	-
5.2.3.3	N/A	11.1	-
5.2.4.1	I8： Insufficient Security Configurability Ensuring the ability to separate normal users from administrative users.	8.4(a)(b) 10.1	-
5.2.4.2	I8： Insufficient Security Configurability Ensuring the ability to encrypt data at rest or in transit.	8.3(a) 10.1 10.3	-
5.2.4.3	N/A	10.1	-
5.2.4.4	I8： Insufficient Security Configurability Ensuring the ability to encrypt data at rest or in transit. I2 Insufficient Authentication/Authorization Ensuring credentials are properly protected.	10.1	-
5.2.5.1	I1： Insecure Web Interface Ensuring web interface is not susceptible to XSS, SQLi or CSRF.		-
5.2.6.1 5.2.6.2	I2 ： Insufficient Authentication/Authorization Ensuring that the strong passwords are required The app authentication is required.	8.3(b) 8.3(c) 8.3(d) 8.8 8.9	-

5.2.6.3	I2 ： Insufficient Authentication/Authorization Ensuring granular access control is in place when necessary. I8： Insufficient Security Configurability Jump to: navigation, search Ensuring the ability to separate normal users from administrative users.		-
5.2.7.1	I8： Insufficient Security Configurability Ensuring the ability to enable logging of security events.		-
5.2.7.2	-		-
5.2.7.3	-		-
5.2.7.4	I8： Insufficient Security Configurability Ensuring the ability to notify end users of security events		-
5.3.1.1 5.3.1.2	I4： Lack of Transport Encryption Ensuring data is encrypted using protocols such as SSL and TLS while transiting networks. Ensuring only accepted encryption standards are used and avoid using proprietary encryption protocols. Ensuring the message payload encryption. Ensuring the secure encryption key handshaking. Ensuring received data integrity verification. I8： Insufficient Security Configurability Ensuring the ability to encrypt data at rest or in transit.	8.3(a) 9.1 10.1 10.3	-
5.3.2.1	I3： Insecure Network Services		-

	Ensuring network ports or services are not exposed to the internet via UPnP for example.		
5.3.2.2	I10： Poor Physical Security Ensuring the product has the ability to limit administrative capabilities		-
5.3.2.3	I3： Insecure Network Services Ensuring services are not vulnerable to buffer overflow and fuzzing attacks.	15	-
5.3.3.1 5.3.3.2	I8： Insufficient Security Configurability Ensuring the ability to encrypt data at rest or in transit.		-
5.3.3.3	I3： Insecure Network Services Ensuring services are not vulnerable to buffer overflow and fuzzing attacks.		-
5.3.3.4	-		-
5.4.1.1	I2 ： Insufficient Authentication/Authorization The app authentication is required.	8.8 8.9	Core Spec. – Ver. 16.12 5.12.1 Authentication 5.12.3 Username token profile Advanced Security Service Spec. – Ver. 1.3 4.2 Certificate-based Client Authentication
5.4.1.2	I7： Insecure Mobile Interface	8.3(b)	-

	Ensuring user accounts can not be enumerated using functionality such as password reset mechanisms		
5.4.1.3 5.4.1.4	-		-
5.4.1.5	I2 : Insufficient Authentication/Authorization Implement two factor authentication where possible. I7： Insecure Mobile Interface Implementing two factor authentication if possible.		-
5.4.1.6	I2 : Insufficient Authentication/Authorization The device authentication is required.		-
5.4.2.1	I1： Insecure Web Interface Default passwords and ideally default usernames to be changed during initial setup. I7： Insecure Mobile Interface Default passwords and ideally default usernames to be changed during initial setup.	8.3(e)	
5.4.2.2 5.4.2.3 5.4.2.4 5.4.2.5 5.4.2.6	I1： Insecure Web Interface Ensuring weak passwords are not allowed. Ensuring account lockout after 3 -5 failed login attempts. I2 : Insufficient Authentication/Authorization Ensuring that the strong passwords are required. Ensuring options are available for configuring password controls.	8.3(b) 8.3(c)	-

	I7： Insecure Mobile Interface Ensuring account lockout after an 3 - 5 failed login attempts. I8： Insufficient Security Configurability Ensuring the ability to force strong password policies.		
5.4.3.1 5.4.3.2	I2 ： Insufficient Authentication/Authorization Ensuring granular access control is in place when necessary. I8： Insufficient Security Configurability Ensuring the ability to separate normal users from administrative users.	8.2 8.4(a)(b)	Core Spec. – Ver. 16.12 5.12.2 User-based access control
5.5.1.1 5.5.1.2	I5： Privacy Concerns Ensuring only authorized individuals have access to collected personal information.	8.4(a)(b) 11.5	-
5.5.1.3	I8： Insufficient Security Configurability Ensuring the ability to notify end users of security events		-
5.5.2.1 5.5.2.2	I4： Lack of Transport Encryption Ensuring the message payload encryption. I5： Privacy Concerns Ensuring any data collected is properly protected with encryption.	9.1 10.3	-

參考資料

(1) CNS 27001 資訊技術－安全技術－資訊安全管理系統－要求事項

(2) ANSI/CAN/UL 2900-1：2017 Software Cybersecurity for Network Connectable Products, Part 1： General Requirements

(3) GSMA corp., IoT Security Guidelines for Endpoint Ecosystems

(4) Open Web Application Security Project (OWASP) org., Top IoT Vulnerabilities [viewed 2018-05-16]. Available at https：//www.owasp.org/index.php/Top_IoT_Vulnerabilities

(5) 總務省, 經濟產業省, IoT セキュリティガイドライン ver 1.0

(6) IoT-1001-2 v10：影像監控系統資安標準-第二部：網路攝影機

(7) IoT-1001-3 v1.0：影像監控系統資安標準-第三部：影像錄影機

(8) IoT-1001-4 v1.0：影像監控系統資安標準-第四部：網路儲存裝置

(9) National Institute of Standards and Technology(NIST), National Vulnerability Database, https：//nvd.nist.gov/vuln/full-listing

(10) First, Common Vulnerability Scoring System v3.0 Specification, https：//www.first.org/cvss/specification-document

(11) 行政院法務部, 個人資料保護法, Dec., 2015

(12) 行政院國家資通安全會報技術服務中心, 政府組態基準 Microsoft Windows 8.1 (V1.3)

(13) National Institute of Standards and Technology(NIST), "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", October 2, 2012.

(14) National Institute of Standards and Technology, NIST SP 800-140C, CMVP Approved Security Functions, available at URL: http://www.nist.gov/cmvp.

(15) Open Web Application Security Project (OWASP) org., OWASP Top Ten 2017 Project [viewed 2018-05-16]. Available at https：//www.owasp.org/index.php/Category：OWASP_Top_Ten_2017_Project

(16) RFC 3550, RTP： A Transport Protocol for Real-Time Applications

(17) RFC 2326, Real Time Streaming Protocol (RTSP)

(18) RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2

(19) Open Network Video Interface Forum(ONVIF), Core Specification Version 16.12, Dec., 2016.

(20) Open Network Video Interface Forum(ONVIF), Advanced Security Service Version 1.3, Feb., 2016.