TAICS

TAICS TS-0014-2 v1.0 : 2017

影像監控系統資安標準
－網路攝影機

Video Surveillance System Security Standard
- IP Camera

2017/11/26

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

影像監控系統資安標準—網路攝影機

Video Surveillance System Security Standard - IP Camera

出版日期: 2017/11/26

終審日期: 2017/10/26

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：安華聯網科技(股)公司 洪光鈞 總經理

TC 秘書：資訊工業策進會 高傳凱 博士

此標準制定之協會會員參與名單為(以中文名稱順序排列)：

(行)國家中山科學研究院、(財)工業技術研究院、(財)台灣電子檢驗中心、(財)資訊工業策進會、(財)電信技術中心、中華電信(股)公司、友訊科技(股)公司、安華聯網科技(股)公司、宏達國際電子(股)公司、果核數位(股)公司、國立中央大學、晶復科技(股)公司、趨勢科技(股)公司。

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

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，而物聯網科技成功與否，資訊安全是最主要的關鍵，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，包括物聯網通用資安標準、輔助應用程式資安標準、影像監控系統資安標準、工控系統資安標準、車聯網系統資安標準、醫療儀器資安標準及銷售點終端系統資安標準等，全面推升國內資安產業自主研發能量，提供穩定且安全的產業發展環境。

物聯網的盛行，使日常用品皆朝向數位化邁進，網路攝影機也是其中之一，運用範圍包括：視訊通話、遠端監控、直播服務等，相當受到消費者青睞。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「影像監控系統資安標準-網路攝影機」之制定(以下簡安稱本標準)，建立國內在網路攝影機之資安品質的標準，期使設備商或系統服務商在產品研發上有所依據，藉以促進國內產業整體優質化及產品競爭力，並確保消費者在網路攝影機之運用上達到資訊安全的目的。

本標準旨在網路攝影機於產品開發階段，建立產品資訊安全的評估及驗證時所遵循之共同標準，用以鑑別產品之安全等級。本標準係參照國際物聯網相關資安標準/規範，如International Organization for Standardization (ISO) 27001、Underwriters Laboratories (UL) 2900系列標準[1]、Groupe Speciale Mobile Association (GSMA) IoT Security Guideline[2]、Open Web Application Security Project (OWASP) Top IoT Vulnerabilities[3]及日本政府的物聯網安全指導方針[4]等，主要規劃從五個安全構面確保網路攝影機的資訊安全，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、及(5)隱私保護等；並分成三個安全等級，詳盡載明欲實踐每一個安全等級的必要條件，用以界定不同產品須具備之資安要求。

在確保網路攝影機之資安品質的同時，應一併考量整體影像監控系統的資訊安全性，例如:管理網路攝影機的雲服務被駭客入侵、操控網路攝影機的行動應用程式含有軟體漏洞、及數位或網路影像錄影機安全等級不足等因素，這些因素可能對網路攝影

機造成資安威脅，因此建議設置時需採用相同資安等級之相關產品，達到整體網路影像監控系統的安全保證(Security Assurance)。

1. 適用範圍

本標準為確保影像監控系統網路攝影機的資訊安全，依(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)隱私保護等五項安全構面，訂定其產品安全技術要求。本標準適用於影像監控系統中具連網功能之嵌入式網路攝影機(如圖 1)。

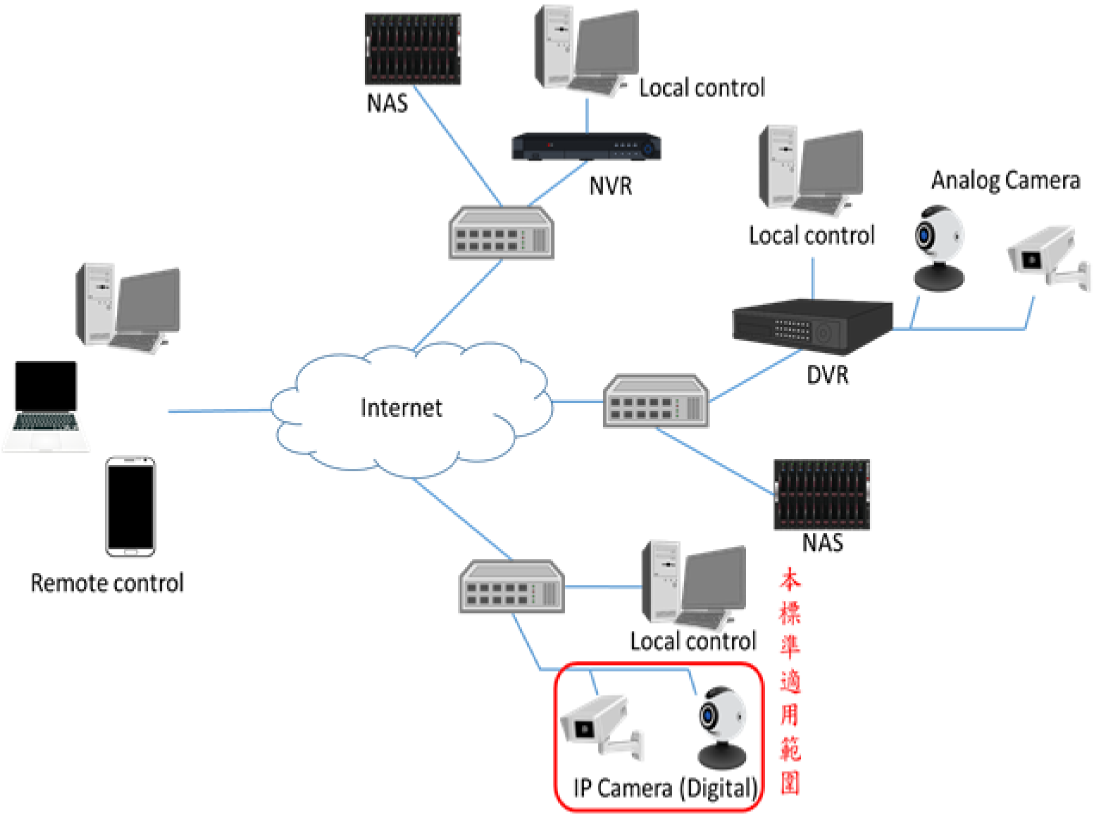

圖 1 適用範圍示意圖

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。

CNS 27001 資訊技術－安全技術－資訊安全管理系統－要求事項

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 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。

3.2 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。

3.3 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。

3.4 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[5]，負責 3.3 常見弱點與漏洞之資料的發布及更新。

3.5 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[6]。

3.6 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。

3.7 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、憑證或地理位置等。

3.8 個人資料 (Personally Identifiable Information)

依「個人資料保護法」[7]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。

3.9 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網路攝影機所錄製之影像及用戶資訊。

3.10 操控程式 (Control Program)

係指用於控制網路攝影機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。

3.11 遠端管理介面 (Remote Control Management, RCM)

係指透過網路自遠端裝置取得網路攝影機作業系統的操控權，如：

(a) 於遠端使用操控程式或透過網頁管理介面執行產品維護、存取網路攝影機 資源、監看畫面或操控鏡頭。

(b) 於遠端使用或透過網頁管理介面進行系統設定，例如：網際網路協定位址(IP)。

3.12 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。大部份網路攝影機皆具備該介面操控端應用程式呼叫，用戶透過超文本傳輸協定(HTTP)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。

3.13 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。

3.14 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。

3.15 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。

3.16 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性通訊層(Secure Sockets Layer, SSL)和傳輸層安全性(Transport Layer Security, TLS)。

3.17 安全區域 (Secure Domain)

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。

3.18 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)[8]，以降低駭客入侵與導致資安事件之疑慮。

3.19 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。

3.20 預設通行碼 (Default Password)

係指產品在用戶初次將其連上網路，且在未更改任何設定的情況下，用以登入網路攝影機之通行碼。

3.21 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。

3.22 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登入系統的嘗試。

3.23 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。

3.24 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。

3.25 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，在無須設定 IP 位址或 DNS 伺服器的情況下，設備即可自行發現彼此。

3.26 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，無須任何繁複的安全性設定。

3.27 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)[9]加密演算法。

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

係指身分鑑別須透過二種以上的鑑別機制後，得以獲得裝置之存取權限。

3.29 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。

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及(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，須依循本節 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	5.1.1.2	-
	5.1.2. 實體異常行為警示	-	5.1.2.1	-
	5.1.3. 實體防護	-	5.1.3.1	5.1.3.2
	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	-	5.2.1.2
	5.2.2. 網路服務連接埠安全	5.2.2.1	-	-
	5.2.3. 更新安全	5.2.3.1	5.2.3.2	-
	5.2.4. 韌體程式安全(選項)	5.2.4.1	-	-
	5.2.5. 敏感性資料儲存安全	-	5.2.5.1	5.2.5.2
	5.2.6. 網頁管理介面安全	5.2.6.1	-	-
	5.2.7. 操控程式之應用程式安全	5.2.7.1	-	-
	5.2.8. 系統日誌檔與警示	5.2.8.1	5.2.8.2	-
通訊安全	5.3.1. 敏感性資料傳輸安全	5.3.1.1	5.3.1.2	-
	5.3.2. 通訊介面的安全設置	5.3.2.1	-	-
	5.3.3. 通訊協定安全	-	5.3.3.1	-
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
	5.4.2. 通行碼鑑別機制	5.4.2.1	-	-
	5.4.3. 權限控管	5.4.3.1	-	-
隱私保護	5.5.1. 隱私資料的存取保護	5.5.1.1	-	-
	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，須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，須確保鑑別與授權相關機制。

(e) 隱私保護：網路攝影機之隱私，包括使用者之資料和影像，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)風險承受度、(2)安全技術深度、(3)產品技術現況、(4)無通用檢測方法及(5)檢測所需時間綜合考量，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必須先滿足較低安全等級要求。

4.2 安全等級詳述

4.2.1 安全第 1 級

係指產品的功能及操作主要以便利性為導向，安全威脅則是次要考量的應用環境，重點是專注於須被保護的敏感資訊及個人資料之管控，為開發商對於用戶提供最基本的安全。

表 2　第 1 級安全技術要求

安全類別	要求分類	安全技術要求
實體安全	實體埠安全管控	5.1.1.1(a) 預設不應透過實體埠存取產品作業系統之除錯模式。
系統安全	作業系統與網路服務不應存在重大風險之常見弱點與漏洞	5.2.1.1(a) 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 嚴重性等級評比為重大。
	僅開啟必要之網路服務	5.2.2.1(a) 產品開啟之網路服務須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，且廠商須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。
	韌體更新機密性保證	5.2.3.1(a) 韌體須具備更新機制。 5.2.3.1(b) 產品支援離線手動更新者，在更新檔案時為確保機密性須具加密保護，其加密方式不應使用列於「附錄 A」公認之弱加密演算法。 5.2.3.1(c) 產品支援線上更新，其更新路徑須通過安全通道，且安全通道版本須符合「附錄 B」的要求，並且預設啟用之加密演算法與訊息完整性校驗須採用 Federal Information Processing Standards (FIPS) 140-2[10]]所核可，以及同時支援前向安全之加密演算法。
	敏感性資料不應出現於裝置韌體程式碼中(選項)	5.2.4.1(a) 產品之身分鑑別因子、加解密用之金鑰(不含非對稱加密用之公鑰)及個人資料，不應出現於韌體之程式碼與安裝檔內其他檔案中。

安全類別	要求分類	安全技術要求
	網頁管理介面不應存在 OWASP web top 10[11]常見網站安全風險	5.2.6.1(a) 產品本機提供之網頁管理介面不應存在 OWASP web top 10 之 Injection 及 Cross-Site Scripting (XSS)攻擊。
	應用程式介面之鑑別機制強度	5.2.7.1(a) 應用程式介面之鑑別機制安全依 5.4.1.1(a)及 4.4.1.1(b)之要求。 5.2.7.1(b) 應用程式介面之通行碼鑑別安全依 5.4.2 該要求項之相關要求。 5.2.7.1(c) 應用程式介面之權限管控依 5.4.3 該要求項之相關要求。
	產品須提供安全事件日誌檔	5.2.8.1(a) 須具備安全事件記錄與顯示功能，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。其內容須包括完整時間戳記、使用者身分及操作行為等，供後續查閱之用。 5.2.8.1(b) 產品之安全事件紀錄須具備權限控管機制，該日誌檔不應允許未經授權的修改。 5.2.8.1(c) 須要求產品之日誌檔留存時間，且符合 NIST SP 800-92[12]中 high impact systems 的日誌資料維護長度。
通訊安全	敏感性資料於傳輸過程中須加密保護	5.3.1.1(a) 敏感性資料之網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[10]，以確保機密性。
	避免錯誤的通訊介面設置	5.3.2.1(a) 產品須提供使用者得自行開/關「網路裝置資訊探詢」功能，例如：通用隨插即用通訊協定、簡單網路管理協定及零配置通訊協定。 5.3.2.1(b) 產品須提供使用者得自行開/關「Wi-Fi 保護設置」之 WPS PIN 功能，而其預設值須為關閉狀態。 5.3.2.1(c) 無線網路傳輸的安全機制預設須採用「Wi-Fi 保護存取 2」。 5.3.2.1(d) 預設不應透過網路連線存取產品作業系統之除錯模式。
身分鑑別與授權機制安全	鑑別機制初階強度要求	5.4.1.1(a) 透過管理介面存取產品資源前，須透過具備防止重送攻擊之身分鑑別機制。 5.4.1.1(b) 鑑別錯誤訊息不應顯露出合法使用者名稱。

安全類別	要求分類	安全技術要求
		5.4.1.1(c) 支援影像監控系統裝置身分鑑別功能，且須具備防止重送攻擊之能力，確保相連裝置之可信度。 5.4.1.1(d) 採用憑證鑑別須確保憑證有效性，例如:發證單位、有效期限、格式錯誤及憑證簽章等。
	通行碼鑑別機制強度	5.4.2.1(a) 通行碼強度原則必須符合政府組態基準之通行碼原則類別，包括最小通行碼長度原則 CCE-33789-9、通行碼必須符合複雜性需求原則 CCE-33777-4、及強制執行通行碼歷程記錄原則 CCE-35219-5。 5.4.2.1(b) 廠商所生產之裝置，其預設通行碼都須相異。 5.4.2.1(c) 首次成功取得產品存取之授權，須強制更改預設通行碼。 5.4.2.1(d) 產品在登入通行碼的設計上須有輸入頻率及次數的限制，即: - 最高五次嘗試登入失敗即鎖定帳戶。 - 帳戶鎖定期間至少一分鐘以上，始可自動解除。 - 帳戶鎖定計數器至少一分鐘以上的時間間隔，始可將失敗的登入嘗試計數器重設為零次。
	資源的存取，須具備權限管控機制	5.4.3.1(a) 產品須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。 5.4.3.1(b) 產品之授權行為，須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，須要求新的鑑別。
隱私保護	隱私資料的權限管控	5.5.1.1(a) 產品所儲存的隱私資料，須被授權的個體始可存取。 5.5.1.1(b) 使用者對其儲存的隱私資料擁有刪除之權限和功能。 5.5.1.1(c) 於每次發生新的存取事件時，產品必須主動發出警示；抑或是須於外殼設置狀態指示燈，顯示監控功能運行中。
	隱私資料傳輸機密性初階要求	5.5.2.1(a) 影像類隱私資料之傳輸不應為明文，非影像類隱私資料之傳輸，須使用 FIPS 140-2 所核可之加密演算法[10]。

4.2.2 安全第 2 級

組織在營運規劃上考量資安的重要性，且欲於良好商業發展活動中，積極發展安全工程技術，具準備付出額外的安全工程之意願，但不須大幅度重新設計開發。

表 3　第 2 級安全技術要求

安全類別	要求分類	安全技術要求
實體安全	產品之外接實體介面	5.1.1.2(a) 外接式儲存媒體使用的插槽須移除。 5.1.1.2(b) 產品須具有實體埠插拔操作記錄功能。
	硬體設計須具備異常狀態之警示機制	5.1.2.1(a) 產品須具備相關警示機制於實體操作發生斷訊、斷電時。
	產品之外殼須具不被輕易拆除的防護機制	5.1.3.1(a) 產品須採用一體成形或防拆螺絲等機殼防拆除保護設計。
系統安全	韌體更新機制強度	5.2.3.2(a) 產品必須具備驗證韌體之正確性及完整性的功能。
	敏感性資料須透過加密儲存	5.2.5.1(a) 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)及個人資料不應明文儲存，而保護資料的加密方式不應使用列於「附錄 A」公認之弱加密演算法。
	產品須提供異常警示功能	5.2.8.2(a) 產品須提供系統警示功能以避免安全事件紀錄無法儲存之狀況發生。
通訊安全	敏感性資料傳輸須採用安全通道	5.3.1.2(a) 敏感性資料之網路傳輸須通過安全通道，且安全通道版本須符合「附錄 B」的要求，且預設啟用之加密演算法與訊息完整性校驗須採用 FIPS 140-2[10]所核可，以及同時支援前向安全之加密演算法。
	產品所使用之關鍵通訊協定，必須通過異常輸入檢測	5.3.3.1(a) 產品之關鍵通訊協定(參考附錄 C)，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。
隱私保護	隱私資料傳輸機密性中階要求	5.5.2.2(a) 隱私資料之網路傳輸須通過安全通道，且安全通道版本須符合「附錄 B」的要求，且預設啟用之加密演算法與訊息完整性校驗須採用 FIPS 140-2 [10]所核可，以及同時支援前向安全之加密演算法。

4.2.3 安全第 3 級

應用環境屬於高風險狀態，認為保護資產之價值使額外付出顯得正當時，以保護高價值資產對抗高風險為最終目的。因此產品須使用高階之安全工程技術，且大幅度的重新設計開發。

表 4 第 3 級安全技術要求

安全類別	要求分類	安全技術要求
實體安全	避免不安全的實體設計	5.1.3.2(a) 晶片上不應存在晶片編號，且電路板上不應存在功能編號。 5.1.3.2(b) 產品外部不應有徒手即可輕易還原預設通行碼的設計。
		5.1.4.1(a) 產品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。
系統安全	作業系統與網路服務不應存在高風險之常見弱點與漏洞	5.2.1.3(a) 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。
	敏感性資料的存放，須從正常作業環境中隔離	5.2.5.2(a) 敏感性資料須存放於產品的安全區域。
身分鑑別與授權機制安全	鑑別機制中階強度要求	5.4.1.2(a) 產品之鑑別機制須採用多因子鑑別。
隱私保護	隱私資料傳輸機密性高階要求	5.5.2.3(a) 確保隱私資料之網路傳輸加密演算法須支援 AES-256[9]。

5. 標準規範

5.1 實體安全

5.1.1 實體埠之安全管控

5.1.1.1 出廠之實體埠必須具備安全管控。

(a) 預設不應透過實體埠存取產品作業系統之除錯模式。

5.1.1.2 產品之外接實體介面。

(a) 外接式儲存媒體使用的插槽須移除。

(b) 產品須具有實體埠插拔操作記錄功能。

5.1.2 實體異常行為警示

5.1.2.1 硬體設計須具備異常狀態之警示機制。

(a) 產品須具備相關警示機制於實體操作發生斷訊、斷電時。

5.1.3 實體防護

5.1.3.1 產品之外殼須具不被輕易拆除的防護機制。

(a) 產品須採用一體成形或防拆螺絲等機殼防拆除保護設計。

5.1.3.2 避免不安全的實體設計。

(a) 晶片上不應存在晶片編號，且電路板上不應存在功能編號。

(b) 產品外部不應有徒手即可輕易還原預設通行碼的設計。

5.1.4 安全啟動

5.1.4.1 產品須提供安全啟動(Secure Boot)功能。

(a) 產品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重大風險之常見弱點與漏洞。

(a) 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 嚴重性等級評比為重大。

5.2.1.2 產品之作業系統與網路服務不應存在高風險之常見弱點與漏洞。

(a) 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。

5.2.2 網路服務連接埠安全

5.2.2.1 產品僅開啟必要之網路服務。

(a) 產品開啟之網路服務須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，且廠商須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。

5.2.3 更新安全

5.2.3.1 韌體更新機密性保證。

(a) 韌體須具備更新機制。

(b) 產品支援離線手動更新者，在更新檔案時為確保機密性須具加密保護，其加密方式不應使用列於「附錄 A」公認之弱加密演算法。

(c) 產品支援線上更新，其更新路徑須通過安全通道，且安全通道版本須符合「附錄 B」的要求，並且預設啟用之加密演算法與訊息完整性校驗須採用 FIPS 140-2[10] 所核可，以及同時支援前向安全之加密演算法。

5.2.3.2 韌體更新機制強度。

(a) 產品必須具備驗證韌體之正確性及完整性的功能。

5.2.4 韌體程式安全 (選項)

5.2.4.1 產品之敏感性資料不應出現於裝置韌體程式碼中。

(a) 產品之身分鑑別因子、加解密用之金鑰(不含非對稱加密用之公鑰)及個人資料，不應出現於韌體之程式碼與安裝檔內其他檔案中。

5.2.5 敏感性資料儲存安全

5.2.5.1 產品所儲存之敏感性資料須透過加密儲存。

(a) 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)及個人資料不應明文儲存，而保護資料的加密方式不應使用列於「附錄 A」公認之弱加密演算法。

5.2.5.2 敏感性資料的存放，須從正常作業環境中隔離。

(a) 敏感性資料須存放於產品的安全區域。

5.2.6 網頁管理介面安全

5.2.6.1 網頁管理介面不應存在 OWASP web top 10[11]常見網站安全風險。

(a) 產品本機提供之網頁管理介面不應存在 OWASP web top 10 之 Injection 及 Cross-Site Scripting (XSS)攻擊。

5.2.7 操控程式之應用程式介面安全

5.2.7.1 應用程式介面之鑑別機制強度。

(a) 應用程式介面之鑑別機制安全依 5.4.1.1(a)及 5.4.1.1(b)之要求。

(b) 應用程式介面之通行碼鑑別安全依 5.4.2 該要求項之相關要求。

(c) 應用程式介面之權限管控依 5.4.3 該要求項之相關要求。

5.2.8 系統日誌檔與警示

5.2.8.1 產品須提供安全事件日誌檔。

(a) 須具備安全事件記錄與顯示功能，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。其內容須包括完整時間戳記、使用者身分及操作行為等，供後續查閱之用。

(b) 產品之安全事件紀錄須具備權限控管機制，該日誌檔不應允許未經授權的修改。

(c) 須要求產品之日誌檔留存時間，且符合 NIST SP 800-92[12]中 high impact systems 的日誌資料維護長度。

5.2.8.2 產品須提供異常警示功能。

(a) 產品須提供系統警示功能以避免安全事件紀錄無法儲存之狀況發生。

5.3 通訊安全要求

5.3.1 敏感性資料傳輸安全

5.3.1.1 敏感性資料於傳輸過程中須加密保護。

(a) 敏感性資料之網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[10]，以確保機密性。

5.3.1.2 敏感性資料傳輸須採用安全通道。

(a) 敏感性資料之網路傳輸須通過安全通道，且安全通道版本須符合「附錄 B」的要求，且預設啟用之加密演算法與訊息完整性校驗須採用 FIPS 140-2[10]所核可，以及同時支援前向安全之加密演算法。

5.3.2 通訊介面的安全設置

5.3.2.1 避免錯誤的通訊介面設置。

(a) 產品須提供使用者得自行開/關「網路裝置資訊探詢」功能，例如：通用隨插即用通訊協定、簡單網路管理協定及零配置通訊協定。

(b) 產品須提供使用者得自行開/關「Wi-Fi 保護設置」之 WPS PIN 功能，而其預設值須為關閉狀態。

(c) 無線網路傳輸的安全機制預設須採用「Wi-Fi 保護存取 2」。

(d) 預設不應透過網路連線存取產品作業系統之除錯模式。

5.3.3 通訊協定安全

5.3.3.1 產品所使用之關鍵通訊協定，必須通過異常輸入檢測。

(a) 產品之關鍵通訊協定(參考附錄 C)，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。

5.4 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 鑑別機制初階強度要求。

(a) 透過管理介面存取產品資源前，須透過具備防止重送攻擊之身分鑑別機制。

(b) 鑑別錯誤訊息不應顯露出合法使用者名稱。

(c) 支援影像監控系統裝置身分鑑別功能，且須具備防止重送攻擊之能力，確保相連裝置之可信度。

(d) 採用憑證鑑別須確保憑證有效性，例如:發證單位、有效期限、格式錯誤及憑證簽章等。

5.4.1.2 鑑別機制中階強度要求。

(a) 產品之鑑別機制須採用多因子鑑別。

5.4.2 通行碼鑑別安全

5.4.2.1 通行碼鑑別機制強度。

(a) 通行碼強度原則必須符合政府組態基準之通行碼原則類別，包括最小通行碼長度原則 CCE-33789-9、通行碼必須符合複雜性需求原則 CCE-33777-4、及強制執行通行碼歷程記錄原則 CCE-35219-5。

(b) 廠商所生產之裝置，其預設通行碼都須相異。

(c) 首次成功取得產品存取之授權，須強制更改預設通行碼。

(d) 產品在登入通行碼的設計上須有輸入頻率及次數的限制，即:

(i) 最高五次嘗試登入失敗即鎖定帳戶。

(ii) 帳戶鎖定期間至少一分鐘以上，始可自動解除。

(iii) 帳戶鎖定計數器至少一分鐘以上的時間間隔，始可將失敗的登入嘗試計數器

重設為零次。

5.4.3 權限管控

5.4.3.1 產品資源的存取，須具備權限管控機制。

(a) 產品須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。

(b) 產品之授權行為，須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，須要求新的鑑別。

5.5 隱私保護要求

5.5.1 隱私資料的存取保護

5.5.1.1 隱私資料的權限管控

(a) 產品所儲存的隱私資料，須被授權的個體始可存取。

(b) 使用者對其儲存的隱私資料擁有刪除之權限和功能。

(c) 於每次發生新的存取事件時，產品必須主動發出警示；抑或是須於外殼設置狀態指示燈，顯示監控功能運行中。

5.5.2 隱私資料的傳輸保護

5.5.2.1 隱私資料傳輸機密性初階要求。

(a) 影像類隱私資料之傳輸不應為明文，非影像類隱私資料之傳輸，須使用 FIPS 140-2 所核可之加密演算法[10]。

5.5.2.2 隱私資料傳輸機密性中階要求。

(a) 隱私資料之網路傳輸須通過安全通道，且安全通道版本須符合「附錄 B」的要求，且預設啟用之加密演算法與訊息完整性校驗須採用 FIPS 140-2 [10]所核可，以及同時支援前向安全之加密演算法。

5.5.2.3 隱私資料傳輸機密性高階要求。

(a) 確保隱私資料之網路傳輸加密演算法須支援 AES-256[9]。

附錄 A
(規定)
公認之弱加密演算法

A.1 BASE 64 Encode and Decode

Base64 是一種能將任意二位元資料，用 64 種字元組合成字串的方法，而這個二位元資料和字串資料彼此之間是可以互相轉換的，此機制的目的是在保證效率的情況下，不讓處理過的資料被輕易識別，因此演算法的複雜度相對也就不能太高。

A.2 Data Encryption Standard, DES

是一種基於使用 56 位元金鑰之對稱式加密演算法，此加密演算法在 1999 年已被公開破解，也有一些分析報告提出了演算法理論上的漏洞。

A.3 Message-Digest Algorithm, MD5

是一種雜湊函式(Hash Function)，可以產生出一個 128 位元的雜湊值(Hash Value)，用於確保傳輸中資料的完整性，此方法在 1996 年已被證實存在漏洞，可以被破解。

A.4 Rivest Cipher 4, RC4

是一種密鑰長度可變的對稱加密演算法，同時也是有線等效加密所採用的加密演算法，在 2015 年被公告已破解，並禁止在所有版本的傳輸層安全性協定中使用。

A.5 Secure Hash Algorithm 1, SHA-1

是一種雜湊函式(hash function)，可以產生出一個 160 位元的雜湊值(Hash Value)，用於確保傳輸中資料的完整性，2005 年 SHA-1 被發現含有理論上漏洞，會造成碰撞攻擊(Collision Attack)。

附錄 B
(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性通訊層協定或傳輸層安全性協定，建立安全通道以保護傳輸中資料不被竊取之技術，然而安全性通訊層協定在 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性通訊層協定，但傳輸層安全性協定 1.0 存在可以降級到安全性通訊層協定 3.0 的功能，使得傳輸層安全性協定 1.0 同樣不被信任，因此目前本標準強烈建議使用的版本為：

傳輸層安全性協定 1.2

附錄 C
(規定)
網路攝影機所使用之通訊協定

C.1 即時傳輸協定 (Real-time Transport Protocol, RTP)：

定義在 RFC 3550 規範中[14]，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。

C.2 即時傳送控制協定 (Real-time Transport Control Protocol, RTCP)：

定義在 RFC 3550 規範中，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)。

C.3 即時串流協定 (Real Time Streaming Protocol, RTSP)：

定義在 RFC 2326 規範中[15]，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。

C.4 超文本傳輸協定 (HyperText Transfer Protocol, HTTP)：

定義在 RFC 7540 規範中[16]，，是目前網際網路上應用最廣泛的一個網路協議（protocol），其主要目的是為了提供網頁的發佈與取得。

C.5 傳輸層安全協定 (The Transport Layer Security, TLS)：

定義在 RFC 5246 規範中[17]，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 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[3]	ONVIF 對應項目[18-19]
5.1.1.1(a)	I10: Poor Physical Security Ensuring USB ports or other external ports can not be used to maliciously access the device.	N/A
5.1.1.2(a) 5.1.1.2(b)	I10: Poor Physical Security Ensuring only required external ports such as USB are required for the product to function.	N/A
5.1.2.1(a) 5.1.2.1(b)	N/A	N/A
5.1.3.1(a)	I10: Poor Physical Security Ensuring data storage medium can not be easily removed. Ensuring device can not be easily disassembled.	N/A
5.1.3.2(a) 5.1.3.2(b)	I2: Insufficient Authentication/Authorization Ensuring that password recovery mechanisms are secure.	N/A
5.1.4.1(a)	I9: Insecure Software/Firmware Implement the secure boot if possible (chain of trust).	N/A
5.2.1.1(a)	N/A	N/A
5.2.1.2(a)	N/A	N/A
5.2.2.1(a)	I3: Insecure Network Services Ensuring only necessary ports are exposed and available.	N/A
5.2.3.1(a) 5.2.3.1(b) 5.2.3.1(c)	I9: Insecure Software/Firmware Ensuring the device has the ability to update (very important, need secure update mechanism). Ensuring the update file is encrypted using accepted encryption methods. Ensuring the update file is transmitted via an encrypted connection.	Core Spec. – Ver. 16.12 4.5.5 Firmware Upgrade
5.2.3.2(a) 5.2.3.2(b)	I9: Insecure Software/Firmware Ensuring the update is signed and verified before allowing the update to be uploaded and applied.	N/A
5.2.4.1(a)	I9: Insecure Software/Firmware Ensuring the update file does not expose sensitive data.	N/A
5.2.4.2(a)	N/A	N/A

技術要求	OWASP 對應項目[3]	ONVIF 對應項目[18-19]
5.2.5.1(a)	N/A	Advanced Security Service Spec. – Ver. 1.3 5.2 Keystore
5.2.5.2(a)	I10: Poor Physical Security Ensuring stored data is encrypted at rest. I8: Insufficient Security Configurability Ensuring the ability to encrypt data at rest or in transit.	Advanced Security Service Spec. – Ver. 1.3 5.2 Keystore
5.2.6.1(a)	I1: Insecure Web Interface Ensuring web interface is not susceptible to XSS, SQLi or CSRF.	N/A
5.2.7.1(a) 5.2.7.1(b) 5.2.7.1(c)	I2: Insufficient Authentication/Authorization Ensuring re-authentication is required for sensitive features. I3: Insecure Network Services The abnormal service request traffic should be detected and blocked on service gateway layer.	N/A
5.2.7.2(a)	N/A	N/A
5.2.8.1(a) 5.2.8.1(b) 5.2.8.1(c)	I8: Insufficient Security Configurability Ensuring the ability to enable logging of security events.	N/A
5.2.8.2(a)	I8: Insufficient Security Configurability Ensuring the ability to notify end users of security events	N/A
5.3.1.1(a)	I1: Insecure Web Interface Ensuring credentials are not exposed in internal or external network traffic. I2: Insufficient Authentication/Authorization Ensuring credentials are properly protected. I4: Lack of Transport Encryption Ensuring only accepted encryption standards are used and avoid using proprietary encryption protocols. I8: Insufficient Security Configurability Ensuring the ability to encrypt data at rest or in transit.	N/A
5.3.1.2(a)	I1: Insecure Web Interface Ensuring credentials are not exposed in internal or external network traffic. I2: Insufficient Authentication/Authorization Ensuring credentials are properly protected. 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.	Core Spec. – Ver. 16.12 5.12.1 Authentication

技術要求	OWASP 對應項目[3]	ONVIF 對應項目[18-19]
	I8: Insufficient Security Configurability Ensuring the ability to encrypt data at rest or in transit.	
4.3.2.1(a) 5.3.2.1(b) 5.3.2.1(c) 5.3.2.1(d)	I3: Insecure Network Services Ensuring network ports or services are not exposed to the internet via UPnP for example.	N/A
5.3.3.1(a)	I3: Insecure Network Services Ensuring services are not vulnerable to buffer overflow and fuzzing attacks. The abnormal service request traffic should be detected and blocked on service gateway layer.	N/A
5.4.1.1(a) 5.4.1.1(b) 5.4.1.1(c)	I1: Insecure Web Interface Ensuring password recovery mechanisms are robust and do not supply an attacker with information indicating a valid account I2: Insufficient Authentication/Authorization Ensuring granular access control is in place when necessary. The device authentication is required. Ensuring that password recovery mechanisms are secure	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(a)	I2: Insufficient Authentication/Authorization Implement two factor authentication where possible	N/A
5.4.2.1(a) 5.4.2.1(b) 5.4.2.1(c) 5.4.2.1(d)	I1: Insecure Web Interface Default passwords and ideally default usernames to be changed during initial setup. 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. I8: Insufficient Security Configurability Ensuring the ability to force strong password policies.	N/A
5.4.3.1(a) 5.4.3.1(b)	I2: Insufficient Authentication/Authorization Reviewing the various interfaces to determine whether the interfaces allow for separation of roles. For example, all features will be accessible to administrators, but users will have a more limited set of features available. I8: Insufficient Security Configurability Ensuring the ability to separate normal users from administrative users.	Core Spec. – Ver. 16.12 5.12.2 User-based access control

技術要求	OWASP 對應項目[3]	ONVIF 對應項目[18-19]
5.5.1.1(a) 5.5.1.1(b) 5.5.1.1(c)	I5: Privacy Concerns Ensuring only authorized individuals have access to collected personal information.	N/A
5.5.2.1(a)	I4: Lack of Transport Encryption Ensuring the message payload encryption. I5: Privacy Concerns Ensuring any data collected is properly protected with encryption.	N/A
5.5.2.2(a)	I4: Lack of Transport Encryption Ensuring the message payload encryption. I5: Privacy Concerns Ensuring any data collected is properly protected with encryption.	N/A
5.5.2.3(a)	I4: Lack of Transport Encryption Ensuring the message payload encryption. I5: Privacy Concerns Ensuring any data collected is properly protected with encryption.	N/A

參考資料

[1] UL 2900-1, Outline of Investigation for Software Cybersecurity for Network Connectable Products, Part 1: General Requirements

[2] GSMA corp., IoT Security Guidelines for Endpoint Ecosystems

[3] OWASP.org, Top IoT Vulnerabilities, https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

[4] 總務省　經濟產業省, IoT セキュリティガイドライン ver 1.0

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

[6] First, Common Vulnerability Scoring System v3.0 Specification, https://www.first.org/cvss/specification-document

[7] 行政院法務部，個人資料保護法, Dec., 2015

[8] 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)

[9] NIST, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", October 2, 2012.

[10] NIST, Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May 10, 2017

[11] OWASP.org, OWASP Top Ten 2017 Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project

[12] NIST, NIST Special Publication 800-92: Guide to Computer Security Log Management, Sep, 2006

[13] 行動應用資安聯盟，行動應用 App 基本資安規範 V1.1

[14] RFC 3550, RTP: A Transport Protocol for Real-Time Applications

[15] RFC 2326, Real Time Streaming Protocol (RTSP)

[16] RFC 7540, Hypertext Transfer Protocol Version 2 (HTTP/2)

[17] RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2

[18] ONVIF, Core Specification Version 16.12, Dec., 2016.

[19] ONVIF, Advanced Security Service Version 1.3, Feb., 2016.

版本修改紀錄

版本	時間	摘要
v1.0	2017/11/26	出版

台灣資通產業標準協會

Taiwan Association of Information and Communication Standards

地　址・台北市中正區重慶南路二段51號8樓之一
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw