影像監控系統資安標準草案-網路攝影機 (V0.9.0)

推動單位：

台灣資通產業標準協會(TAICS)

制定單位：

台灣資通產業標準協會之網路與資訊安全技術工作委員會(TC5)

支持單位：

經濟部工業局、財團法人資訊工業策進會

2017-09-25

目錄

前言

本標準係依台灣資通產業標準協會（TAICS）之規定，經技術管理委員會(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，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。

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草案-網路攝影機」之制定(以下簡稱本標準)，建立國內在網路攝影機之資安品質的規範，期使設備商或系統服務商在產品研發上有所依據，促進國內產業整體優質化及產品競爭力，確保消費者在網路攝影機之運用上達到安全的目的。

本標準之制定係參照國際物聯網相關資安標準/規範，如 ISO 27001、UL 2900 系列標準[1]、GSMA IoT Security Guideline[2]、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，包括實體安全、系統安全、通訊安全、身分認證與授權機制安全及隱私保護；並分成三個安全保證等級，詳盡載明欲實踐每一個安全保證等級的必要條件，用以界定不同產品須具備之資安要求。

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安全等級不足的數位/網路影像錄影機等因素，這些因素可能對網路攝影機造成資安威脅，因此建議設置時須參閱所有相關產品之資安標準，達到整體網路影像監控系統的安全保證(Security Assurance)。

1. 適用範圍

泛指應用於影像監控系統的嵌入式攝影機，且凡是攝影機本身具連網功能者皆是網路攝影機的一種，如圖 1 紅框處所示。

本標準為確保網路攝影機資安，訂定其產品之安全技術要求，擬依五個安全構面定義之，包括：實體安全、系統安全、通訊安全、身分認證與授權機制安全、隱私保護。

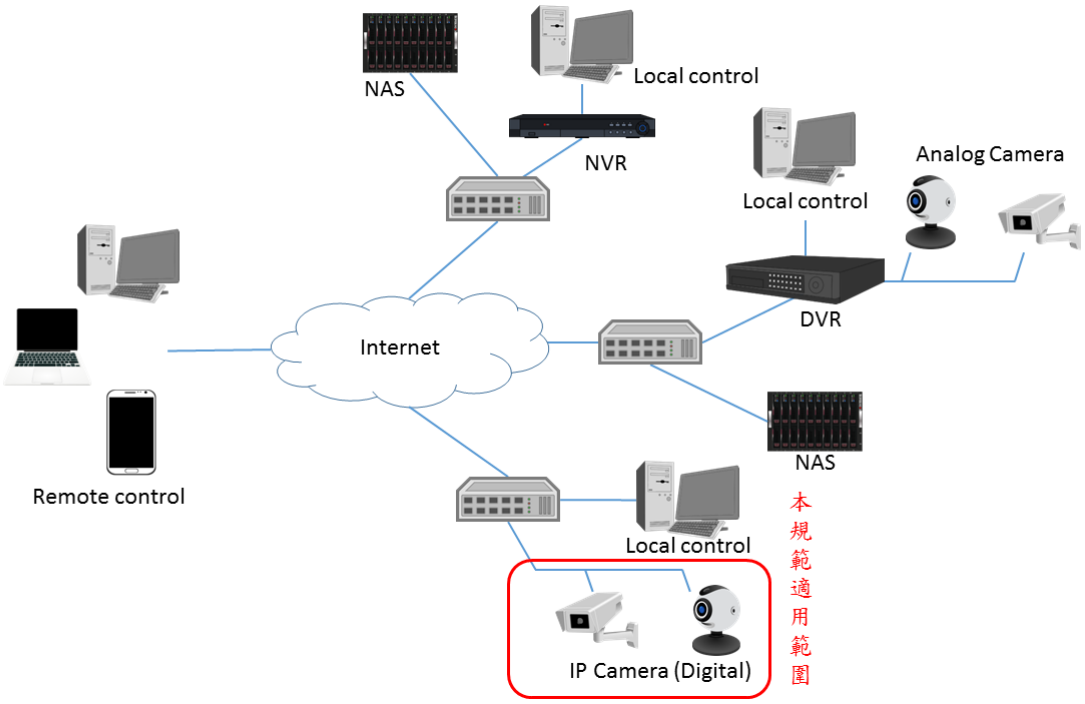

圖 1 適用範圍示意圖

2. 引用標準

下列標準因本標準所引用，成為本標準之一部份。下列引用標準適用最新版(包括補充增修)。

CNS 27001 資訊技術－安全技術－資訊安全管理系統－要求事項

3. 用語及定義

下列用語與定義適用於本標準。

3.1 網路攝影機 (IP Camera)

係指一種主要用於影像監控系統且具連網功能的攝影機，其應用類型包括：網路攝影機(IP camera)、智能家庭攝影機(smart camera)及 3D 攝影機(3D camera)等。

3.2 資訊安全弱點 (Security Vulnerability)

指受測裝置安全方面之缺陷，使得系統或行動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)

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。

3.4 國家弱點資料庫 (National Vulnerabilities Database)

係指美國國家標準技術研究所（NIST）提供的國家弱點資料庫[5]，負責 2.3 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)

一套公開評比企業資訊科技系統的安全性評鑑標準，CVSS 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、攻擊者不當運用該漏洞的難易度，都被列入評比。評分分數從 0 分到 10 分，0 代表沒有弱點，而 10 則代表最高風險。

3.6 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、密碼

或地理位置等。

3.7 個人資料 (Personally Identifiable Information)

指主要依「個人資料保護法」上定義之所有得以直接或間接方式識別該個人之資料，包括自然人之姓名、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。

3.8 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，本標準所指之隱私包括網路攝影機所錄製之影像及用戶資訊。

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

係指透過網路自遠端裝置上取得網路攝影機作業系統層的操控權，作業模式如下列：

(a) 工程師遠端維護產品使用或透過網頁管理介面遠端存取網路攝影機資源，例如：監看畫面、操控鏡頭

(b) 進行系統設定，例如：設定網際協定位址(IP)。

3.10 操控程式 (Control Program)

係指用於控制網路攝影機行為或瀏覽監控內容之應用程式，目前可能的應用程式類型包括行動版及電腦版。

3.11 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提供 API 給操控端之應用程式呼叫，用戶可透過這些 API，撰寫實際實現網路攝影機相關操作(例如：系統資訊擷取、監控影像擷取等)的應用程式。

3.12 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。

3.13 加密 (Encryption)

係指法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。

3.14 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。

3.15 安全通道 (Security Tunnel)

目的是為網際網路通訊的端點與端點(End-to-End)之間，建立一條兼顧資料隱密性及完整性之通道，目前常見之實作通訊協定為安全通訊端層(SSL)和傳輸層安全性(TLS)。

3.16 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，並保存敏感性資料用。

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

規範資通訊終端設備(如：個人電腦) 的一致性安全設定[6] (如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮。

3.18 密碼 (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。

3.19 預設密碼 (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密碼。

3.20 裝置認證 (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，常用之認證方式可能是要求相連裝置提交使用者名稱及密碼，或者是相連裝置之數位憑證來確認裝置之身分。

4. 安全等級

本標準旨在建立網路攝影機於產品發展階段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。

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

安全要求等級總表，如表 1 所示，第一欄為安全構面，包括：實體安全、系統安全、通訊安全、身分認證與授權機制安全、隱私保護；第二欄為安全要求分項，係依第一欄安全構面設計對應之安全要求分項技術規範；第三欄為安全等級，按各安全要求分項規範之驗證結果，作為安全等級評估標準。且本安全要求等級總表中之各欄的關連性，須依循第 4 節之規範內容。

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. 出廠之實體埠必須具備安全管控。	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. 作業系統安全	5.2.1.1	5.2.1.2	5.2.1.3
	5.2.2. 網路服務連接埠	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	5.2.4.1	5.2.4.2	
	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		5.2.6.2
	5.2.7. 操控程式之 API 安全	5.2.7.1		5.2.7.2
	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	
身分認證與授權機制安全	5.4.1. 認證機制安全	5.4.1.1		5.4.1.2
	5.4.2. 密碼認證機制	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：產品是否能輕易被拆解，或產品之儲存與測試除錯用之連接埠的管控，作為建立安全要求的標的。

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

(c) 通訊安全：著重在機敏資料之通訊安全，和探查通訊服務是否存在未知之資安漏洞。

(d) 身分認證與授權機制安全：網路攝影機存在數種不同的溝通介面，包括遠端指令管理介面、網頁管理介面、操控程式等，無論從那一類介面，皆須確保認證與授權機制的落實。

(e) 隱私保護：網路攝影機之隱私，包括使用者之資料和影像、儲存與傳輸的保護及權限管控等，確保隱私資料不外洩。

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，而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)風險承受度綜合考量、(2)安全技術深度、(3)目前尚無通用檢測方法、(4)產品技術現況及(5)檢測所需時間，共為三個等級，分為 1 級、2 級、3 級，與其對應之列代表的安全要求分項，識別一個特定的技術要求，且按等級順序排列，數字越

大表示安全等級越高，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	安全技術要求
實體安全	5.1.1.1(a) - 實體埠預設不得被利用來存取產品之作業系統。
系統安全	5.2.1.1(a) - 受測產品之作業系統與網路服務，不得存在國家弱點資料庫[5]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 9 分以上，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。
	5.2.2.1(a) - 產品開啟之網路服務僅須為廠商提供必要服務之所需，使用最小化網路服務的方式，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明所需啟用及停用之網路服務，避免存在未宣告之網路服務連接埠被開啟。
	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，在更新檔案時為確保機密性須加密保護，且加密方式不得為列於「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，且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，及預設啟用之加密演算法與訊息完整性校驗須採用 FIPS 140-2 所核可之演算法[7]。
	5.2.4.1(a) - 產品之身分認證因子、加解密用之金鑰(不含非對稱加密用之公鑰)及個人資料，不得出現於韌體之程式碼與安裝檔內其他檔案中。
	5.2.6.1(a) - 確保產品本身提供之網頁管理介面不得存在 OWASP top 10 之 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊。
	5.2.7.1(a) - API 之身分認證機制，不得因為重送攻擊(Replay Attack)而使認證被通過。 5.2.7.1(b) - 認證錯誤訊息不能顯露出合法使用者名稱。 5.2.7.1(c) - 密碼強度原則必須符合政府組態基準之密碼原則類別，包括最小密碼長度原則 CCE-33789-9、密碼必須符合複雜性需求原則 CCE-33777-4、或(及)強制執行密碼歷程記錄 CCE-35219-5。 5.2.7.1(d) - API 呼叫之預設授權密碼都須相異廠商所生產之網路攝影機其預設密碼都須相異。 5.2.7.1(e) - 首次成功取得網路攝影機 API 授權，須強制更改預設密碼。 5.2.7.1(f) - 產品在認證密碼的設計上須有輸入頻率及次數的限制。 5.2.7.1(g) - API 的存取，須具備權限管控機制。產品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

	品文件中標明現存角色與其對應的權限，確保產品之角色權限與廠商所宣告的相符。 5.2.7.1(h) - API 呼叫之授權行為，須存在閒置時限功能，一旦連線逾時、遺失或結束，須要求新的認證。
	5.2.8.1(a) - 須具備安全事件日誌檔之顯示功能，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。該日誌檔內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) - 產品須對安全事件日誌檔進行權限控管，該紀錄檔不得允許未經授權的修改，防止被竄改的可能性。 5.2.8.1(c) - 須要求產品之日誌檔留存時間，且須符合 NIST SP 800-92[9] 中 high impact systems 的日誌資料維護長度。
通訊安全	5.3.1.1(a) - 敏感資料之網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[7]，以確保機密性。
	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：UPnP、SNMP 及 Bonjour，且預設值須為關閉狀態。 5.3.2.1(b) - 產品須提供使用者可自行開/關無線網路之 WPS PIN 及 WPS Lock 功能，且預設值為須為關閉。 5.3.2.1(c) - 無線網路傳輸的安全機制預設須採用 WPA2。 5.3.2.1(d) - 網路埠預設不得使用於存取產品之作業系統。

身分認證與授權機制安全	5.4.1.1(a) - 產品之身分認證機制，不得因為重送攻擊而使認證被通過。 5.4.1.1(b) - 認證錯誤訊息不得顯露出合法使用者名稱。
	5.4.2.1(a) - 密碼強度原則必須符合政府組態基準之密碼原則類別，包括最小密碼長度原則 CCE-33789-9、密碼必須符合複雜性需求原則 CCE-33777-4 、或（及）強制執行密碼歷程記錄原則 CCE-35219-5。 5.4.2.1(b) - 產品之預設密碼都須相異廠商所生產之網路攝影機其預設密碼都須相異。 5.4.2.1(c) - 首次登入產品須強制更改預設密碼首次登入產品須強制更改預設密碼。 5.4.2.1(d) - 產品在登入密碼的設計上必須有輸入頻率及次數的限制產品在登入密碼的設計上須有輸入頻率及次數的限制。
	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、特權使用者、與系統管理者等，並於產品文件中標明現存角色與其對應的權限，確保產品之角色權限與廠商所宣告的相符。 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，一旦遠端連線逾時、遺失或結束，須要求新的認證。
隱私保護	5.5.1.1(a) - 產品所儲存的隱私資料，須已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) - 於每次產品發生新的存取事件時，產品必須主動發出警示。警示功能設計如：E- Mail 通知、訊息推播、蜂鳴器等。
	5.5.2.1(a) - 影像類隱私資料之傳輸不得為明文，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[7]。

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	安全技術要求
實體安全	5.1.1.2(a) - 所有不使用的介面應移除，包括外接式儲存媒體使用的插槽、電路板上用於除錯或測試用途之界面，須移除。 5.1.1.2(b) - 外接實體埠的插拔操作須提供日誌記錄。
	5.1.2.1(a) - 產品於實體操作時，出現鏡頭被異物遮敝、鏡頭遭調焦及鏡頭遭轉向之異常現象時，須提供警示機制。 5.1.2.1(b) - 產品於實體操作時，出現實體設備遭受破壞，例如：斷電、斷訊狀況，須提供警示機制。
	5.1.3.1(a) - 產品在實體上要有一定程度的防護機制，可能的做法：使用防

	盜螺絲增加拆解的困難。
系統安全	5.2.1.2(a) - 受測產品之作業系統與網路服務，不得存在國家弱點資料庫[5]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 8 分以上，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。
	5.2.3.2(a) - 韌體更新機制須一律採用線上更新。 5.2.3.2(b) - 產品必須具備驗證韌體之正確性及完整性的功能。
	5.2.4.2(a) - 產品的韌體不得存在 CWE/SANS TOP 25 Most Dangerous Software Errors [11viii]。
	5.2.5.1(a) - 系統所儲存之身分認證因子、加解密用之金鑰(不含非對稱加密用之公鑰)及個人資料不得明文儲存，且保護資料的加密方式不得為列於「附錄 A」公認之弱加密演算法。
	5.2.8.2(a) - 產品須提供當安全事件日誌檔無法儲存時之系統警示功能。
通訊安全	5.3.3.1(a) 經由錯誤處理漏洞的查找，包括檢視訊息長度、訊息 ID 及關鍵協定屬性等欄位，避免關鍵之通訊協定(參考附錄 A)因任意或非法的輸入，造成產品異常行為的發生。
隱私保護	5.5.2.2(a) 隱私資料之傳輸須使用 FIPS 140-2 所核可之加密演算法[7]。

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	安全技術要求
實體安全	5.1.3.2(a) - 晶片與功能編號不得存在於電路板。 5.1.1.2(b) - 產品實體上不得存在未經由任何工具,即可輕易還原回預設密碼的設計。
	5.1.4.1(a) 確保產品於開機時，避免未經授權的韌體、驅動程式及作業系統的執行，待系統的完整性及可信度獲得保證，產品始得開機。
系統安全	5.2.1.3(a) 受測產品之作業系統與網路服務，不得存在國家弱點資料庫[5]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 7 分以上，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。
	5.2.5.2(a) 敏感資料必須存放於產品的安全區域(Secure domain)中。
	5.2.6.2(a) 確保產品本身提供之網頁管理介面不得存在 OWASP top 10 之 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊-人工檢測。
	5.2.7.2(a) 透過錯誤處理漏洞的查找，包括檢視訊息長度、訊息 ID 及關鍵協定屬性等欄位，避免 API 因任意或非法的輸入，造成產品異常行為的發生。
通訊安全	5.3.1.2.(a)確保敏感資料之網路傳輸加密演算法預設必須採用 AES-256。

身分認證與授權機制安全	5.4.1.2(a) 產品之認證機制須採用雙因子認證。
隱私保護	5.5.2.3(a) 確保隱私資料之網路傳輸加密演算法預設必須採用 AES-256。

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) 實體埠預設不得被利用來存取產品之作業系統。

5.1.1.2 產品不得有外接儲存用及除錯測試用之實體介面存在。

(a) 所有不使用的介面應移除，包括外接式儲存媒體使用的插槽、電路板上用於除錯或測試用途之界面，須移除。

(b) 外接實體埠的插拔操作須提供日誌記錄。

5.1.2 實體異常行為警示

5.1.2.1 網路攝影機之硬體設計須具備異常狀態之警示機制。

(a) 產品於實體操作時，出現鏡頭被異物遮敝、鏡頭遭調焦及鏡頭遭轉向之異常現象時，須提供警示機制。

(b) 產品於實體操作時，出現實體設備遭受破壞，例如：斷電、斷訊狀況，須提供警示機制。

上述警示機制設計如：E- Mail 通知、訊息推播、蜂鳴器等。

5.1.3 實體防護

5.1.3.1 產品之外殼須具不被輕易拆除或破壞的防護機制。

(a) 產品在實體上要有一定程度的防護機制，可能的做法：使用防盜螺絲增加拆解的困難。

5.1.3.2 避免不安全的實體設計。

(a) 晶片與功能編號不得存在於電路板。

(b) 產品實體上不得存在未經由任何工具，即可輕易還原回預設密碼的設計。

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) 確保產品於開機時，避免未經授權的韌體、驅動程式及作業系統的執行，待系統的完整性及可信度獲得保證，產品始得開機。

5.2 系統安全技術要求

5.2.1 作業系統安全

5.2.1.1 作業系統與網路服務不得存在 CVSS v3 評分為 9 分以上之資訊安全弱點。

(a) 受測產品之作業系統與網路服務，不得存在國家弱點資料庫[5]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 9 分以上，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

5.2.1.2 作業系統與網路服務不得存在 CVSS v3 評分為 8 分以上之資訊安全弱點。

(a) 受測產品之作業系統與網路服務，不得存在國家弱點資料庫[5]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 8 分以上，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

5.2.1.3 作業系統與網路服務不得存在 CVSS v3 評分為 7 分以上之資訊安全弱點。

(a) 受測產品之作業系統與網路服務，不得存在國家弱點資料庫[5]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 7 分以上，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

5.2.2 網路服務連接埠

5.2.2.1 網路攝影機僅開啟必要之網路服務。

(a) 產品開啟之網路服務僅須為廠商提供必要服務之所需，使用最小化網路服務的方式，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明所需啟用及停用之網路服務，避免存在未宣告之網路服務連接埠被開啟。

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，在更新檔案時為確保機密性須加密保護，且加密方式不得為列於「附錄 A」公認之弱加密演算法。

(c) 產品支援線上更新，且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，及預設啟用之加密演算法與訊息完整性校驗須採用 FIPS 140-2 所核可之演算法[7]。

5.2.3.2 韌體更新機制強度。

(a) 韌體更新機制須一律採用線上更新。

(b) 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

5.2.4.1 產品之敏感性資料不得出現於裝置韌體程式碼中。

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

4.2.4.2 產品的韌體不得存在因程式設計錯誤，而導致程式存在安全性弱點。

(a) 產品的韌體不得存在 CWE/SANS TOP 25 Most Dangerous Software Errors [11viii]。

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) 系統所儲存之身分認證因子、加解密用之金鑰(不含非對稱加密用之公鑰)及個人資料不得明文儲存，且保護資料的加密方式不得為列於「附錄 A」公認之弱加密演算法。

5.2.5.2 敏感資料的存放，須從正常作業環境中隔離。

(a) 敏感資料必須存放於產品的安全區域(Secure domain)中。

5.2.6 網頁管理介面安全

5.2.6.1 網頁管理介面不得存在 OWASP top 10 [8]中所揭露之常見網站安全風險之初階安全要求。

(a) 確保產品本身提供之網頁管理介面不得存在 OWASP top 10 之 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊之初階安全要求。

5.2.6.2 網頁管理介面不得存在 OWASP top 10 [8]中所揭露之常見網站安全風險之中階安全要求。

(a) 確保產品本身提供之網頁管理介面不得存在 OWASP top 10 之 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊之中階安全要求。

5.2.7 操控程式之 API 安全

5.2.7.1 API 之認證機制強度。

(a) API 之認證機制，不得因為重送攻擊(Replay Attack)而使認證被通過。

(b) 認證錯誤訊息不能顯露出合法使用者名稱。

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

(d) API 呼叫之預設授權密碼都須相異。

(e) 首次成功取得網路攝影機 API 授權，須強制更改預設密碼。

(f) 產品在認證密碼的設計上須有輸入頻率及次數的限制。

(g) API 的存取，須具備權限管控機制。產品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，並於產品文件中標明現存角色與其對應的權限，確保產品之角色權限與產品文件所定義的相符。

(h) API 呼叫之授權行為，須存在閒置時限功能，一旦連線逾時、遺失或結束，須要求新的認證。

5.2.7.2 操控程式之 API 必須通過異常輸入檢測，不得發生崩潰(crash)導致服務中止的情形。

(a) 透過錯誤處理漏洞的查找，包括檢視訊息長度、訊息 ID 及關鍵協定屬性等欄位，避免 API 因任意或非法的輸入，造成產品異常行為的發生。

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) 須具備安全事件日誌檔之顯示功能，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。該日誌檔內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) 產品須對安全事件日誌檔進行權限控管，該紀錄檔不得允許未經授權的修改，防止被竄改的可能性。

(c) 須要求產品之日誌檔留存時間，且須符合 NIST SP 800-92[9]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) 產品須提供當安全事件日誌檔無法儲存時之系統警示功能。警示功能設計如：E-Mail 通知、訊息推播、蜂鳴器等。

5.3 通訊安全技術要求

5.3.1 敏感性資料傳輸安全

5.3.1.1 敏感資料於傳輸過程中須加密保護。

(a) 敏感資料之網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[7]，以確保機密性。

5.3.1.2 敏感性資料傳輸須採用較嚴謹之加密演算法。

(a) 確保敏感資料之網路傳輸加密演算法預設必須採用 AES-256。

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：UPnP、SNMP及 Bonjour，且預設值須為關閉狀態。

(b) 產品須提供使用者可自行開/關無線網路之 WPS PIN 及 WPS Lock 功能，且預設值為須為關閉。

(c) 無線網路傳輸的安全機制預設須採用 WPA2。

(d) 網路埠預設不得使用於存取產品之作業系統。

5.3.3 通訊協定安全

5.3.3.1 網路攝影機所使用之關鍵通訊協定，必須通過異常輸入檢測，不得發生崩潰(crash)導致服務中止的情形。

(a) 經由錯誤處理漏洞的查找，包括檢視訊息長度、訊息 ID 及關鍵協定屬性等欄位，避免關鍵之通訊協定(參考附錄 A)因任意或非法的輸入，造成產品異常行為的發生。

5.4 身分認證與授權機制安全技術要求

5.4.1 認證機制安全

5.4.1.1 認證機制強度初階要求。

(a) 透過管理介面存取產品資源前，須先經過身分認證機制，且不得因為重送攻擊而使認證被通過。

(b) 支援影像監控系統裝置認證功能，不得因為重送攻擊而使認證被通過，確保相連裝置之可信度。

(c) 認證錯誤訊息不得顯露出合法使用者名稱。

5.4.1.2 認證機制強度中階要求。

(a) 產品之認證機制須採用雙因子認證。

5.4.2 密碼認證安全

5.4.2.1 密碼認證機制強度。

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

(b) 產品之預設密碼都須相異。

(c) 首次登入產品須強制更改預設密碼。

(d) 產品在登入密碼的設計上必須有輸入頻率及次數的限制。

5.4.3 權限管控

5.4.3.1 網路攝影機資源的存取，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，並於產品文件中標明現存角色與其對應的權限，確保產品之角色權限與產品文件所定義的相符。

(b) 產品之授權行為，須存在閒置時限供使用者設定，一旦遠端連線逾時、遺失或結束，須要求新的認證。

5.5 隱私保護技術要求

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，須已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) 於每次產品發生新的存取事件時，產品必須主動發出警示。警示功能設計如：E-Mail 通知、訊息推播、蜂鳴器等。

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得為明文，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[7]。

5.5.2.2 隱私資料傳輸機密性中階要求。

(a) 隱私資料之傳輸須使用 FIPS 140-2 所核可之加密演算法[7]。

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預設必須採用 AES-256。

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 Binary 資料用 64 種字元組合成字串的方法，而這個 Binary 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，同時也是無線加密協定(WEP)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 TLS 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

HTTPS 是超文本傳輸協定(HTTP)結合 SSL/TLS 安全通道的傳輸中資料保護技術，然而 SSL 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 TLS 取代 SSL，但 TLS 1.0 存在可以降級到 SSL 3.0 的功能，使得 TLS 1.0 同樣不被信任，因此目前本規範強烈建議使用的版本如下：

- Transport Layer Security (TLS) 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[11]，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[12]，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[13]，超文本傳輸協定之全名為 HypertText Transfer Protocol（簡稱為 HTTP），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 HTTPS 加密協定(HyperText Transfer Protocol Secure, HTTPS)：

定義在 RFC 2818 規範中[14]，是一種經由 HTTP 進行通訊傳輸，且傳輸是建立在 SSL/TLS 安全通道之上，以保護傳輸中之資料。HTTPS 的主要應用是對網站伺服器進行身分認證，確保傳輸中資料的隱密性與完整性。

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. 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)
7. NIST, Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May 10, 2017
8. OWASP.org, OWASP Top Ten 2017 Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project
9. NIST, NIST Special Publication 800-92: Guide to Computer Security Log Management, Sep, 2006
10. 行動應用資安聯盟, 行動應用 App 基本資安規範 V1.1
11. RFC 3550, RTP: A Transport Protocol for Real-Time Applications
12. RFC 2326, Real Time Streaming Protocol (RTSP)
13. RFC 7540, Hypertext Transfer Protocol Version 2 (HTTP/2)
14. RFC 2818, HTTP Over TLS