IoT-1001-2

影像監控系統資安標準

-第二部：網路攝影機

V1.0

行動應用資安聯盟

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，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，制定「IoT-1001-2 影像監控系統資安標準-第二部：網路攝影機」(以下簡稱本標準)，並結合 IoT-1001-1 影像監控系統資安標準-第一部：一般要求[1]之使用，即本標準之資訊安全要求包括第五節與 IoT-1001-1，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，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。

1. 適用範圍

本標準適用於影像監控系統中具連網功能的嵌入式攝影機(如圖 1)。

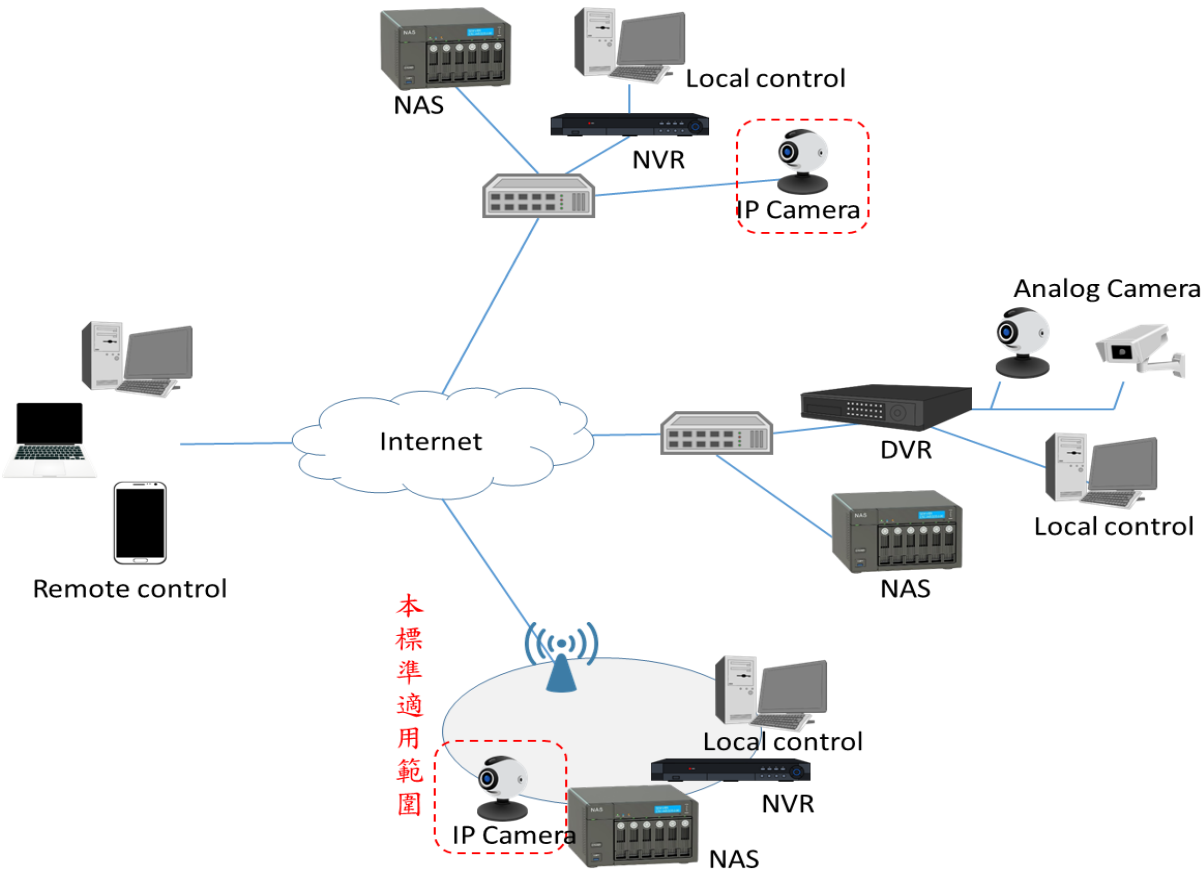

圖 1 適用範圍示意圖

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。

ANSI/CAN/UL 2900-1	**Software Cybersecurity for Network-Connectable Products, Part 1： General Requirements**
CNS 27001：2013	**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**
IoT-1001-1 v1.0	**影像監控系統資安標準-第一部：一般要求**

3. 用語及定義

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」所述及下列用語及定義適用於本標準。

3.1 一體成型

係指產品的外殼不是由零件組合而成，而是整體不分割地直接製成。

3.2 防拆螺絲

係指在螺絲設計上採用各種特殊頭型及沖針設計等，一般十字與一字板手無法拆卸。

3.3 隱私遮罩

係指網路攝影機所監控範圍內的影像，若存在不欲顯示的影像區塊，當用戶存取時，設定隱私遮罩的區塊不會顯示在畫面上。

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	-	5.1.1.2	-
	5.1.2. 實體異常行為警示	-	-	-
	5.1.3. 實體防護	-	5.1.3.2	-
	5.1.4. 安全啟動	-	-	-
系統安全	5.2.1. 作業系統與網路服務安全	-	-	-
	5.2.2. 網路服務連接埠安全	-	-	-
	5.2.3. 更新安全	-	-	-
	5.2.4. 敏感性資料儲存安全	-	-	-
	5.2.5. 網頁管理介面安全	-	-	-
	5.2.6. 操控程式之應用程式安全	-	-	-
	5.2.7. 日誌檔與警示	-	-	-
通訊安全	5.3.1. 敏感性資料傳輸安全	-	-	-
	5.3.2. 通訊介面的安全設置	-	-	5.3.2.2
	5.3.3. 通訊協定安全	-	-	-
身分鑑別與授權機制安全	5.4.1. 鑑別機制安全	-	-	-
	5.4.2. 通行碼鑑別機制	-	-	-
	5.4.3. 權限控管	-	-	-
隱私保護	5.5.1. 隱私資料的存取保護	-	5.5.1.2	-
	5.5.2. 隱私資料的傳輸保護	-	-	-

4.1.1 安全構面：

IoT-1001-1 之第 4.1.1 節之規定適用於本標準。

4.1.2 安全要求分項：

IoT-1001-1 之第 4.1.2 節之規定適用於本標準。

4.1.3 安全等級：

IoT-1001-1 之第 4.1.3 節之規定適用於本標準。

5. 一般要求

本節詳盡載明網路攝影機為滿足安全功能應採取的方法，網路攝影機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 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求第 5.1.1 節之要求。

5.1.1.2 卸除式儲存媒體使用的插槽須移除；抑或卸除式儲存媒體支援儲存媒體保護機制，即產品之儲存媒體不應在本機以外的機器被存取。

5.1.2 實體異常行為警示

5.1.2.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.1.2 節之要求。

5.1.3 實體防護

5.1.3.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.1.3 節之要求。

5.1.3.2 產品須採用一體成形或防拆螺絲等機殼防拆除保護設計。

5.1.4 安全啟動

5.1.4.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.1.4 節之要求。

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 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.2.1 節之要求。

5.2.2 網路服務連接埠安全

5.2.2.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.2.2 節之要求。

5.2.3 更新安全

5.2.3.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.2.3 節之要求。

5.2.4 敏感性資料儲存安全

5.2.4.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.2.4 節之要求。

5.2.5 網頁管理介面安全

5.2.5.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.2.5 節之要求。

5.2.6 操控程式之應用程式介面(API)安全

5.2.6.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.2.6 節之要求。

5.2.7 日誌檔與警示

5.2.7.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.2.7 節之要求。

5.3 通訊安全要求

5.3.1 敏感性資料傳輸安全

5.3.1.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.3.1 節之要求。

5.3.2 通訊協定與設置安全

5.3.2.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.3.2 節之要求。

5.3.2.2 產品所提供之自行開/關「網路裝置資訊探詢」功能，預設須為關閉，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)。

5.3.3 Wi-Fi 通訊安全

5.3.3.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.3.3 節之要求。

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 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.4.1 節之要求。

5.4.2 通行碼鑑別安全

5.4.2.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.4.2 節之要求。

5.4.3 權限管控

5.4.3.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.4.3 節之要求。

5.5 隱私保護要求

5.5.1 隱私資料的存取保護

5.5.1.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.5.1 節之要求。

5.5.1.2 產品應支援隱私遮罩，避免正常作業引發之隱私外洩風險。

備註：產品宜於外殼設置狀態指示燈，告知監控功能運行中，避免隱私影像外洩。

5.5.2 隱私資料的傳輸保護

5.5.2.1 產品須依循 IoT-1001-1 影像監控系統資安標準-第一部：一般要求，第 5.5.2 節之要求。

附錄 A

(參考)

技術要求事項與各標準規範對照表

表 A.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[2]	ONVIF 對應項目[3-4]
5.1.1.2	I10： Poor Physical Security Ensuring USB ports or other external ports can not be used to maliciously access the device.	-
5.1.3.2	-	-
5.3.2.2	-	-
5.5.1.2	-	-

參考資料

[1] IoT-1001-1 v1.0：影像監控系統資安標準-第一部：一般要求

[2] 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

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

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