IoT-1001-4

影像監控系統資安標準

-第四部：網路儲存裝置

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(數位發展部數位產業署承接)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-1001-4 影像監控系統資安標準-第四部:網路儲存裝置」(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，主要規劃從六個安全構面確保網路儲存裝置的資訊安全，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、(5)隱私保護、(6)應用程式安全，建立國內在網路儲存裝置之資安品質的標準，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網路儲存裝置(如圖 1)。

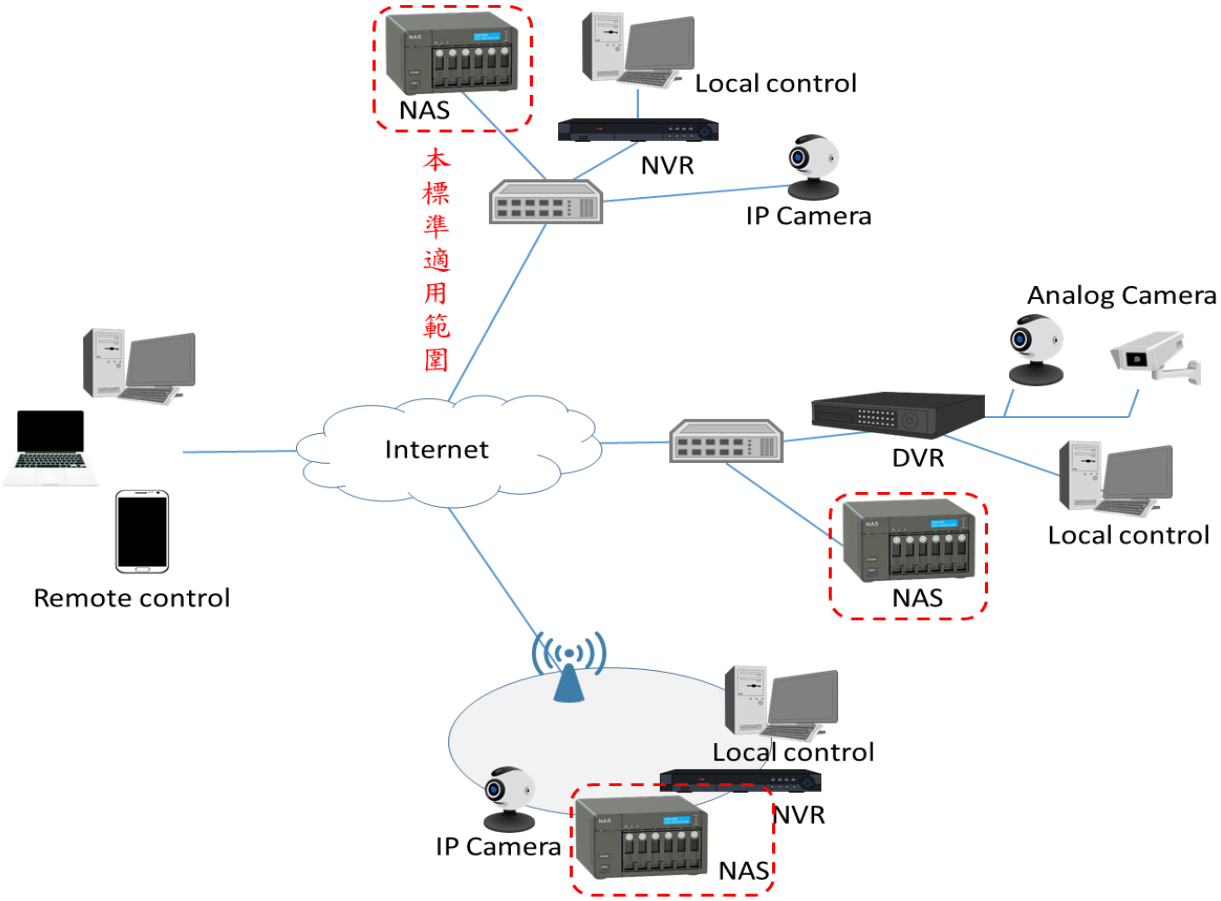

圖 1 適用範圍示意圖

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 v1.0:2021	**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 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與影像檔案寫入之行為。

3.2 外部序列先進技術附件(External Serial Advanced Technology Attachment，eSATA)

一種為外接驅動器而制定的 Serial ATA，用於儲存媒體之間的資料傳輸，外部介面傳輸速度最大為 600Mb/s。

3.3 容錯式磁碟陣列(Redundant Array of Independent Disks，RAID)

一種將多個硬碟組合起來，成為一組硬碟陣列，提升資料整合、容錯功能及處理量。

3.4 熱備援 (Hot Spare)

裝置中某一顆硬碟損壞時，扮演熱備援角色之硬碟將會立即替代該損壞硬碟。

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、(6)應用程式安全；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 5.6 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	-	-	-
	5.1.4. 安全啟動	-	-	-
	5.1.5. 實體備份	5.1.5.1	5.1.5.2	5.1.5.3
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	5.2.7.2	-	-
	5.2.8. 儲存安全	-	5.2.8.1 5.2.8.2	-
	5.2.9. 系統備份安全	5.2.9.1		5.2.9.2
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	-	-	-
	5.3.3. 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	-	-	-
	5.5.2. 隱私資料的傳輸保護	-	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
應用程式安全	5.6.1 應用程式安全	-	5.6.1.1	5.6.1.2

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。

(a) 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。

(b) 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。

(c) 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。

(d) 隱私保護：網路儲存裝置之隱私，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。

(e) 應用程式安全：影像錄影機之出廠預載應用程式，不包含使用者自行下載之非原廠軟體或附加服務，確保其符合現階段資訊安全要求。

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

本節詳盡載明網路儲存裝置為滿足安全功能應採取的方法，網路儲存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 產品支援儲存媒體(例如：硬碟)保護機制，且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。

5.1.4 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。

5.1.5 實體備份

5.1.5.1 確保產品具備外部儲存備份之介面，例如：USB、eSATA 等。

備註：產品宜主動偵測外部儲存備份裝置是否夾帶病毒。

5.1.5.2 確保產品儲存影像資料，支援資料冗餘之能力，例如：RAID 1 等級以上。

5.1.5.3 確保產品儲存備份支援硬碟熱備援之功能，提升容錯能力。

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。

5.2.7.2 安全事件須確實記錄影像檔案寫入行為，內容應包括完整時間戳記、使用者身分及執行結果，供後續查閱用。

5.2.8 儲存安全

5.2.8.1 確保產品具備有效儲存空間設定機制，儲存空間小於設定值時，須發出警示。

5.2.8.2 確保影像檔案支援防竄改之警示機制。

5.2.9 系統備份安全

5.2.9.1 確保產品支援備份影像檔案之能力。

5.2.9.2 備份影像檔案預設須加密保護以確保機密性，且須採用 FIPS 140-2 Annex A [2]所核可之加密演算法。

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。

5.3.3 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。

5.5.2 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。

5.6 應用程式安全要求

5.6.1 應用程式安全

5.6.1.1 未授權或遭竄改之出廠預載應用程式(如：bin 檔、exe 檔、及網頁原始碼)不應被啟動。

5.6.1.2 應用程式須於文件中標明所引用之第三方函式庫，確保引用來源是安全的。

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[3]	ONVIF 對應項目[4-5]
5.1.2.2	I10: Poor Physical Security Ensuring stored data is encrypted at rest.	-
5.1.5.1	-	-
5.1.5.2	-	-
5.1.5.3	-	-
5.2.8.1	-	-
5.2.8.2	-	-
5.2.9.1	-	-
5.2.9.2	-	-
5.6.1.1	-	-
5.6.1.2	-	-

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] National Institute of Standards and Technology(NIST), Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May 10, 2017

[3] 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

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

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