IoT-2001-2

影像監控系統資安測試規範

-第二部：網路攝影機

V2.0

行動應用資安聯盟

中華民國 110 年 6 月

目錄

勘誤與修正對照表

文件版本：v2.0　　對照表發布日期：111 年 4 月 1 日

更正日期：111 年 5 月 26 日　　更正後版本：v2.0（版本維持不變）

章節名稱	修正內容	現行內容	說　　明
5.5.1.2 影像隱私外洩防護測試	(f)測試結果 (1) 通過:隱私遮罩所選定的圖像區塊不可視。 (2) 不通過:隱私遮罩所選定的圖像區塊**可視，或無隱私遮罩功能**。	(f)測試結果 (1) 通過:隱私遮罩所選定的圖像區塊不可視。 (2) 不通過:隱私遮罩所選定的圖像區塊不可視。	(f)測試結果之(2)文字，因誤植而與(1)相同，進行勘誤。修正(f)測試結果之(2)不通過條件內容文字將「不可視」改為「可視，或無隱私遮罩功能」，其餘文字不變。

引言

鑑於近幾年影像監控系統資安事件頻傳，經濟部工業局為全面提升其資安品質，計劃制定一系列影像監控裝置相關之資安標準，並參考現行國際間物聯網資安相關標準與規範，協助台灣產業接軌國際，提升研發技術及保證產品質量。

「IoT-2001-2 影像監控系統資安測試規範-第二部：網路攝影機」(以下簡稱本測試規範)，依據「IoT-1001-2 影像監控系統資安標準-第二部：網路攝影機(1)」訂定，同時參照「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」俾利影像監控系統裝置製造商、系統整合商及物聯網資安檢測實驗室等作為相關產品檢測技術的參考藍本。本測試規範中具體明列資安檢測之測試項目、測試條件、測試方法及測試標準等事項。

1. 適用範圍

本規範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)。

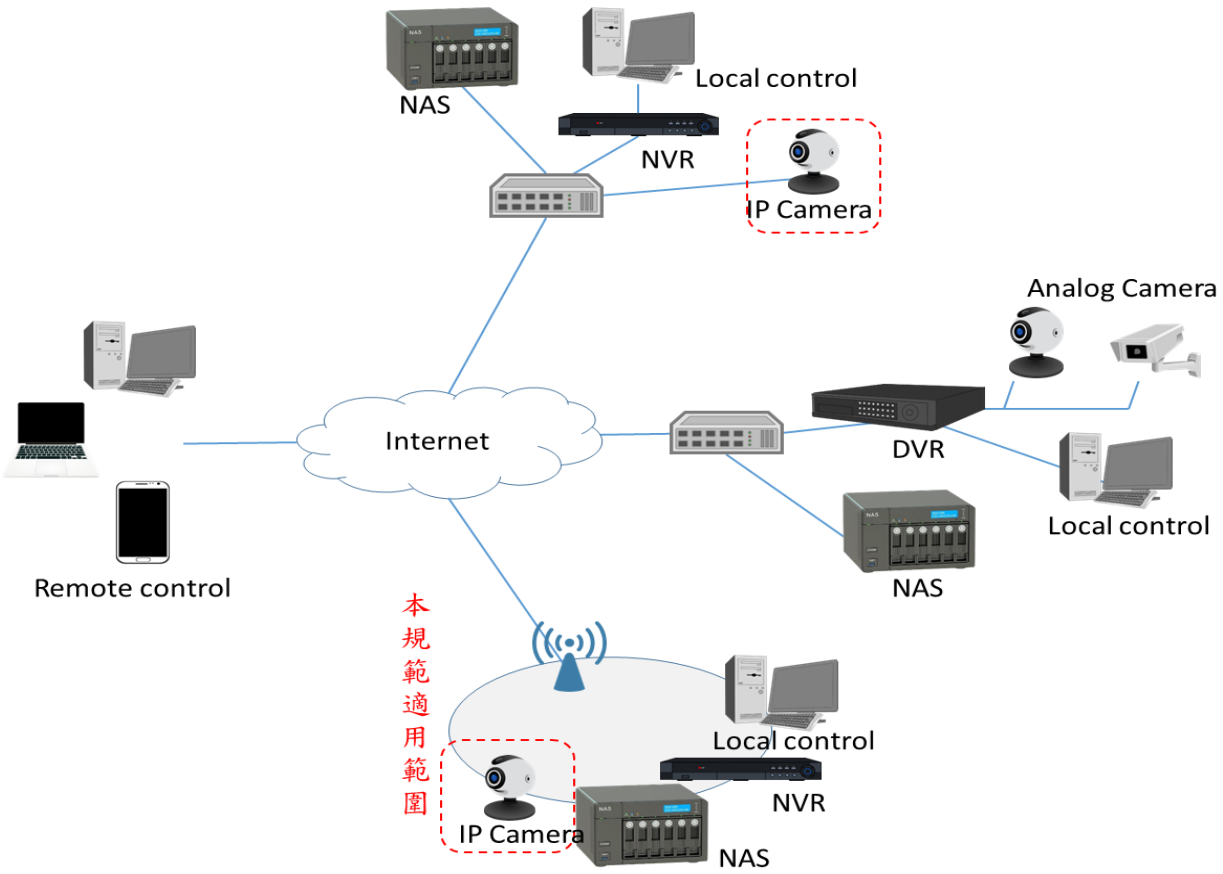

圖 1 適用範圍示意圖

2. 引用標準

下列法規、標準或文件因本規範所引用，成為本規範之一部分。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

[4] IoT-2001-1 v2.0 影像監控系統資安測試規範-第一部：一般要求

3. 用語及定義

「IoT-1001-2 影像監控系統資安標準-第二部：網路攝影機」所規定之用語及定義適用於本規範。

4. 測試項目分級

本節依據「IoT-1001-2 影像監控系統資安標準-第二部：網路攝影機」制定相對應之安全測試項目及測試方法。

實機測試標準等級總表，如表 1 所示，第一欄為安全測試構面，包括：實體安全、系統安全、通訊安全、身分鑑別與授權機制安全、隱私保護；第二欄為安全測試項目，係依第一欄安全測試構面設計對應之安全測試項目；第三欄為安全等級之測試標準，按各安全測試項目所做之測試標準，評估安全等級。

安全等級依(1)相關資安風險高低、(2)安全技術實現複雜度，分為 1 級、2 級、3 級三個等級，產品應先通過較低安全等級之測試，始可進行進階等級之測試。

表 1 實機測試標準等級總表

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

5. 資安測試規範

5.1 實體安全測試

檢視產品有關實體安全部分之送審資料是否符合 IoT-1001-2 之安全要求，並依下列各測試項目進行實機測試。

5.1.1 實體埠之安全管控測試

5.1.1.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.1.1 節。**

5.1.1.2 **最小實體介面測試**

(a) 測試依據：

「IoT-1001-2 影像監控系統資安標準-第二部：網路攝影機」之 5.1.1.2。

(b) 測試目的：

查驗是否可徒手從產品外部取得儲存媒體。

(c) 前置條件：

無。

(d) 測試佈局：

無。

(e) 測試步驟：

(1) 情境 1：

(i) 目視產品外觀(不包括設計上應緊靠牆壁該面)，是否存在記憶卡(SD card)插槽。

(ii) 目視產品外觀(不包括設計上應緊靠牆壁該面)，是否存在通用序列匯流排(USB)插槽。

(2) 情境 2：

(i) 將記憶卡從產品取出，並透過測試電腦讀取該記憶卡中影像資料。

(ii) 檢視在未經授權的情況下，記憶卡內之影像資料是否可讀取。

(iii) 將透過通用序列匯流排接取之儲存裝置卸除，並透過測試電腦讀取該儲存裝置中影像資料。

(iv) 檢視在未經授權的情況下，儲存裝置內之影像資料是否可讀取。

(f) 測試結果：

(1) 情境 1：

(i) 產品不存在卸除式儲存媒體使用的記憶卡插槽。

(ii) 產品不存在卸除式儲存媒體使用的通用序列匯流排插槽。

(iii) 通過：(i)(ii)項皆通過。

(iv) 不通過：(i)(ii)任一項不通過。

(v) 不適用：無。

(2) 情境 2：

(i) 在未經授權的情況下，記憶卡內之影像資料不可被讀取。

(ii) 在未經授權的情況下，透過通用序列匯流排接取之儲存裝置，其中之影像資料不可被讀取。

(iii) 通過：(i)(ii)二項皆通過。

(iv) 不通過：(i)(ii)任一項不通過。

(v) 不適用：無。

5.1.2 實體異常行為警示測試

5.1.2.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.1.2 節。**

5.1.3 實體防護測試

5.1.3.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.1.3 節。**

5.1.3.2 **實體保護測試**

(a) 測試依據：

「IoT-1001-2 影像監控系統資安標準-第二部：網路攝影機」之 5.1.3.2。

(b) 測試目的：

查驗產品是否建立外殼拆除障礙。

(c) 前置條件：

若產品之外殼拆除障礙，是透過現場佈建時，額外於產品外殼再裝上支架或防護罩外殼來加以保護，廠商應在產品之使用說明書或資安指引中註明產品於現場佈建時應額外加裝支架或防護罩外殼，並說明建議加裝的類型，且該文件應公告在廠商官網上。

(d) 測試佈局：

無

(e) 測試步驟：

(1) 目視產品之外殼是一體成型。

(2) 目視產品之外殼經防拆螺絲鎖住。

(f) 測試結果：

(1) 產品採用一體成形或防拆螺絲等機殼防拆除保護設計。

(2) 當產品應額外加裝支架或防護罩外殼，產品之使用說明書或資安指引中註明產品於現場布建時應額外加裝支架或防護罩外殼，並說明建議加裝的類型，且該文件公告在廠商官網上。

(3) 通過：(1)(2)項任一條件符合。

(4) 不通過：(1)(2)項皆不符合。

(5) 不適用：無。

5.1.4 安全啟動測試

5.1.4.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.1.4 節。**

5.2 系統安全測試

檢視產品有關系統安全部分之送審資料是否符合 IoT-1001-2 之安全要求，並依下列各測試項目進行實機測試。

5.2.1 作業系統安全與網路服務安全測試

5.2.1.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.2.1 節。**

5.2.2 網路服務連接埠管控測試

5.2.2.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.2.2 節。**

5.2.3 更新安全測試

5.2.3.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.2.3 節。**

5.2.4 敏感性資料儲存安全測試

5.2.4.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.2.4 節。**

5.2.5 網頁管理介面安全測試

5.2.5.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.2.5 節。**

5.2.6 操控程式之應用程式介面安全測試

5.2.6.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.2.6 節。**

5.2.7 日誌檔與警示測試

5.2.7.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.2.7 節。**

5.3 通訊安全測試

檢視產品有關通訊安全部分之送審資料是否符合 IoT-1001-2 之安全要求，並依下列各測試項目進行實機測試。

5.3.1 資料傳輸安全測試

5.3.1.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.3.1 節。**

5.3.2 通訊協定與設置安全

5.3.2.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.3.2 節。**

5.3.2.2 **網路裝置資訊探詢功能測試**

(a) 測試依據：

「IoT-1001-2 影像監控系統資安標準-第二部：網路攝影機」之 5.3.2.2。

(b) 測試目的：

查驗產品是否運行在具安全風險的網路設定。

(c) 前置條件：

(1) 產品應支援通用隨插即用通訊協定、簡單網路管理協定、零配置通訊協定之任一個網路服務，否則本測項不適用。

(2) 產品應保持出廠預設環境狀態。

(3) 產品應提供所支援網路服務之說明文件。

(d) 測試佈局：

見圖 2。

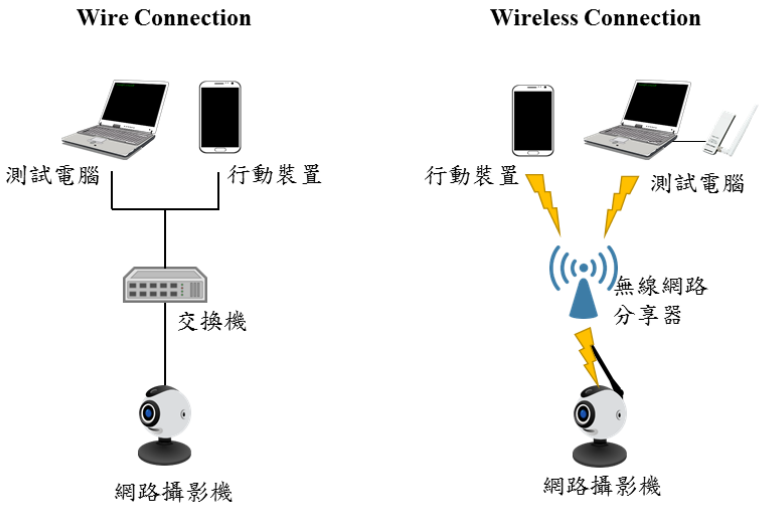

圖 2 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 根據產品使用說明，開啟相應之管理介面連接工具。

(3) 透過具通用隨插即用通訊協定掃描功能之工具以確認產品是否支援通用隨插即用通訊協定服務，且預設為關閉。

(4) 透過具簡單網路管理協定掃描功能之工具以確認產品是否支援簡單網路管理協定服務，且預設為關閉。

(5) 透過具零配置通訊協定掃描功能之工具以確認產品是否支援零配置通訊協定服務，且預設為關閉。

(f) 測試結果：

(1) 若產品支援通用隨插即用通訊協定服務，出廠即預設為關閉狀態。

(2) 若產品支援簡單網路管理協定服務，出廠即預設為關閉狀態。

(3) 若產品支援零配置通訊協定服務，出廠即預設為關閉狀態。

(4) 通過：(1)~(3)項皆符合。

(5) 不通過：(1)~(3)項任一不符合。

不適用：不支援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。

5.3.3 Wi-Fi 通訊安全

5.3.3.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.3.3 節。**

5.4 身分鑑別與授權機制安全測試

檢視產品有關身分鑑別與授權機制部分之送審資料是否符合 IoT-1001-2 之安全要求，並依下列各測試項目進行實機測試。

5.4.1 鑑別機制安全測試

5.4.1.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.4.1 節。**

5.4.2 通行碼鑑別機制

5.4.2.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.4.2 節。**

5.4.3 權限管控測試

5.4.3.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.4.3 節。**

5.5 隱私保護測試

檢視產品有關隱私保護部分之送審資料是否符合 IoT-1001-2 之安全要求，並依下列各測試項目進行實機測試。在本測試規範中，隱私資料泛指從網路攝影機端所收集到的影音資料。

5.5.1 隱私資料的存取保護測試

5.5.1.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.5.1 節。**

5.5.1.2 **影像隱私外洩防護測試**

(a) 測試依據：

「IoT-1001-2 影像監控系統資安標準-第二部：網路攝影機」之 5.5.1.2。

(b) 測試目的：

查驗產品是否具備選定監控範圍內不予以顯示的影像區塊。

(c) 前置條件：

無。

(d) 測試佈局：

見圖 3。

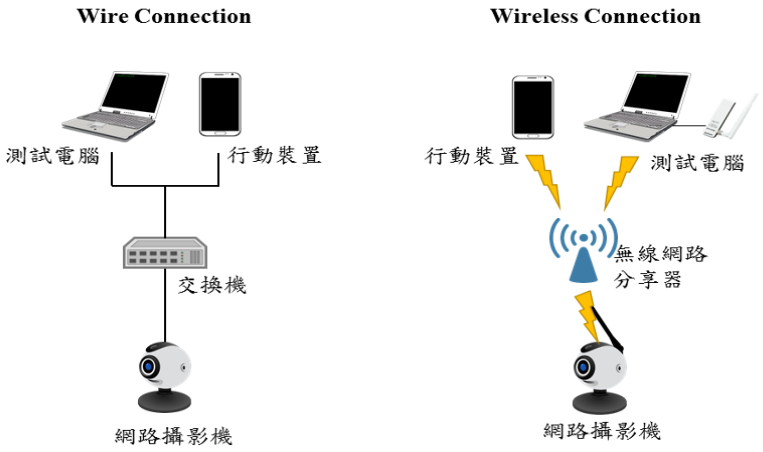

圖 3 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 根據產品使用說明，開啟相應之管理介面連接工具。

(3) 目視產品之操控程式或網頁管理介面，是否存在供使用者設定隱私遮罩的操作介面。

(4) 執行隱私遮罩功能後，檢視產品所監控之影像是否某些區塊是不可視的。

(f) 測試結果：

(1) 通過：隱私遮罩所選定的圖像區塊不可視。

(2) 不通過：隱私遮罩所選定的圖像區塊可視，**或無隱私遮罩功能**。

(3) 不適用：無。

5.5.2 隱私資料的傳輸保護測試

5.5.2.1 **測試依循「IoT-2001-1 影像監控系統資安測試規範-第一部：一般要求」第 5.5.2 節。**

參考資料

(1) IoT-1001-2 v1.0: 影像監控系統資安標準-第二部：網路攝影機