IoT-2001-3

影像監控系統資安測試規範

-第三部：影像錄影機

V1.0

經濟部工業局

中華民國 110 年 6 月

目錄

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改善其資安品質，計劃制定一系列影像監控系統相關之資安標準，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-2001-3 影像監控系統資安測試規範-第三部:影像錄影機」(以下簡稱本測試規範)，依據「IoT-1001-3 影像監控系統資安標準-第三部:影像錄影機」[1]所訂定，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」，俾利影像錄影機製造商、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之固定式影像錄影機(如圖 1)。

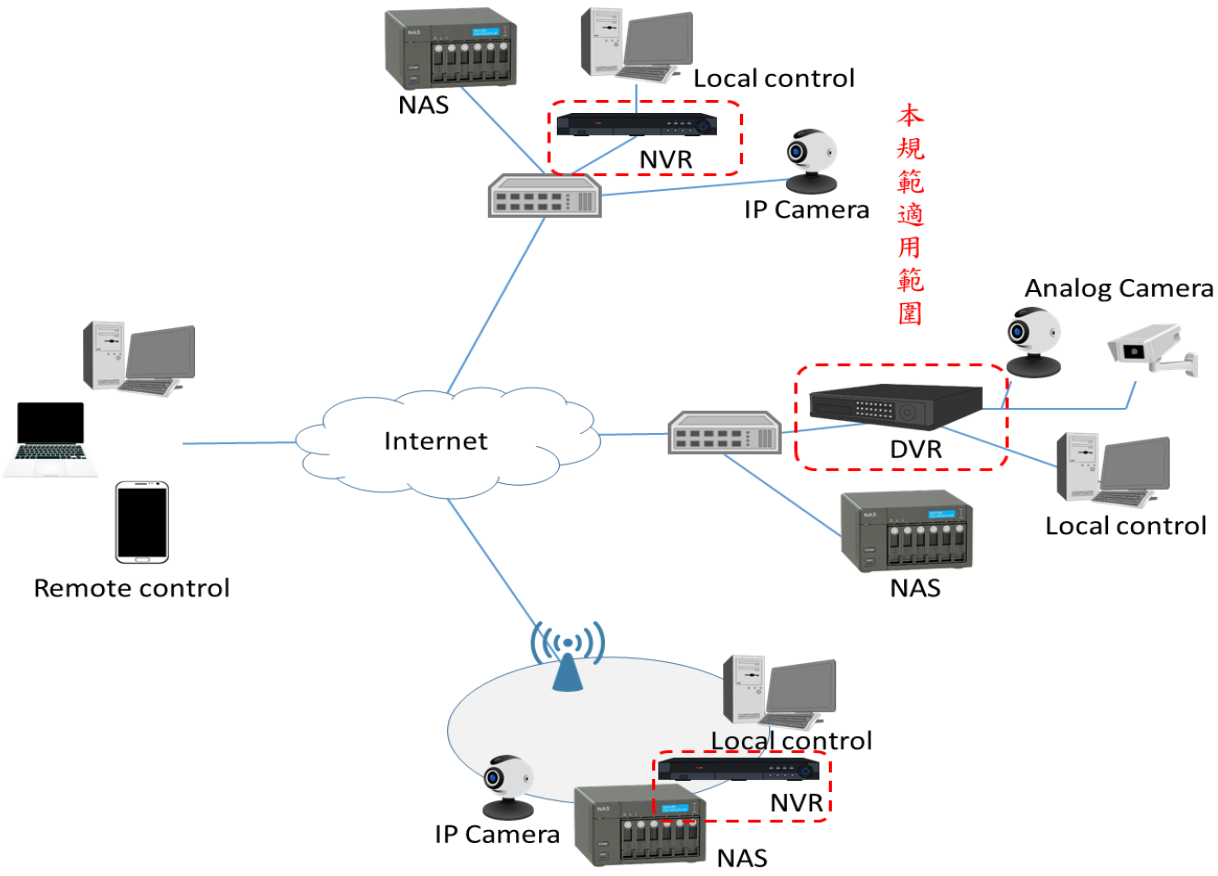

圖 1 適用範圍示意圖

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。

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-2001-1 v1.0	**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-1001-3 影像監控系統資安標準-第三部:影像錄影機」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-1001-3 影像監控系統資安標準-第三部:影像錄影機制定相對應之安全測試項目與測試方法。

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、及應用程式安全；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，產品須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	-	-	-
	5.1.2. 實體異常行為警示測試	-	5.1.2.2	-
	5.1.3. 實體防護測試	-	-	-
	5.1.4. 安全啟動測試	-	-	-
	5.1.5. 實體備份測試	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	5.2.7.2	-	-
	5.2.8. 儲存安全測試	-	5.2.8.1 5.2.8.2	-
	5.2.9. 系統備份安全測試	5.2.9.1	-	5.2.9.2
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	-	-	-
	5.3.3. 通訊協定安全測試	-	-	-
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	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
	5.5.2. 隱私資料的傳輸保護測試	-	-	-
應用程式安全	5.6.1 應用程式安全	-	5.6.1.1	5.6.1.2

5. 資安測試規範

5.1 實體安全測試

檢視影像錄影機之實體安全測試需求是否符合書面送審資料，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 儲存媒體保護機制測試

(a) 測試依據：

(1) IoT-1001-3「影像監控系統資安標準-第三部:影像錄影機」之 5.1.1.2。

(b) 測試目的：

(1) 驗證產品之儲存媒體（例如：硬碟機），是否可在本機以外的機器被存取。

(c) 樣品條件：

(1) 無。

(d) 測試佈局：

(1) 無。

(e) 測試方法：

(1) 將儲存媒體從產品取出，並透過測試電腦讀取該儲存媒體中影像資料。

(2) 檢視在未經授權的情況下，儲存媒體內之影像資料是否可讀取。

(f) 預期結果：

(1) 儲存媒體內之影像資料不可讀取。

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。

5.1.4 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。

5.1.5 實體備份測試

5.1.5.1 儲存備份機制初階安全測試

(a) 測試依據：

(1) IoT-1001-3「影像監控系統資安標準-第三部:影像錄影機」之 5.1.5.1。

(b) 測試目的：

(1) 確保受測產品具備有外部儲存備份之介面。

(c) 樣品條件：

(1) 無。

(d) 測試佈局：

(1) 無。

(e) 測試方法：

(1) 目視產品外觀是否具備外部儲存備份之裝置與連接介面。

(f) 預期結果：

(1) 產品外觀具備外部儲存備份之裝置與連接介面。

5.1.5.2 儲存備份機制中階安全測試

(a) 測試依據：

(1) IoT-1001-3「影像監控系統資安標準-第三部:影像錄影機」之 5.1.5.2。

(b) 測試目的：

(1) 確保產品所儲存之影像，支援資料冗餘之能力，例如：RAID 1 等級以上。

(c) 樣品條件：

(1) 無。

(d) 測試佈局：

(1) 見圖 2。

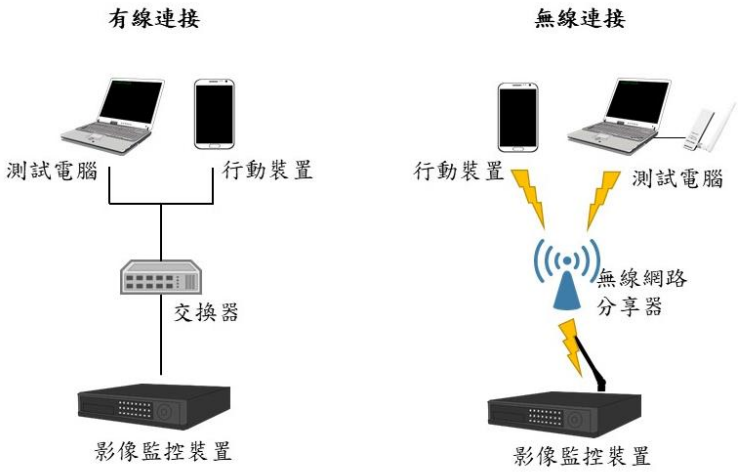

圖 2 測試示意圖

(e) 測試方法：

(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) 於產品啟動狀況下，將其中一顆儲存媒體卸載，檢視產品是否仍可正常運行。

(f) 預期結果：

(1) 影像監控相關功能正常運行。

5.1.5.3 儲存備份機制高階安全測試

(a) 測試依據：

(1) IoT-1001-3「影像監控系統資安標準-第三部:影像錄影機」之 5.1.5.3。

(b) 測試目的：

(1) 確保產品支援硬碟熱備援之功能，提升容錯能力。

(c) 樣品條件：

(1) 產品須提供熱備援機制功能之使用說明。

(d) 測試佈局：

(1) 無。

(e) 測試方法：

(1) 於產品運行狀況下，直接拔掉其中一顆 raid 硬碟。

(2) 檢查產品是否正常運行、效能是否下降、功能是否完整。

(f) 預期結果：

(1) 產品正常運行，且效能不變、功能依舊完整。

5.2 系統安全測試

檢視影像錄影機之系統安全需求是否符合書面送審資料，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 影像監控系統資安標試規範-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。

5.2.7.2 影像檔案寫入日誌測試

(a) 測試依據：

(1) IoT-1001-3「影像監控系統資安標準-第三部:影像錄影機」之 5.2.7.2。

(b) 測試目的：

(1) 驗證產品是否具有影像檔案寫入事件之紀錄供查詢。

(c) 樣品條件：

(1) 無。

(d) 測試佈局：

(1) 見圖 3。

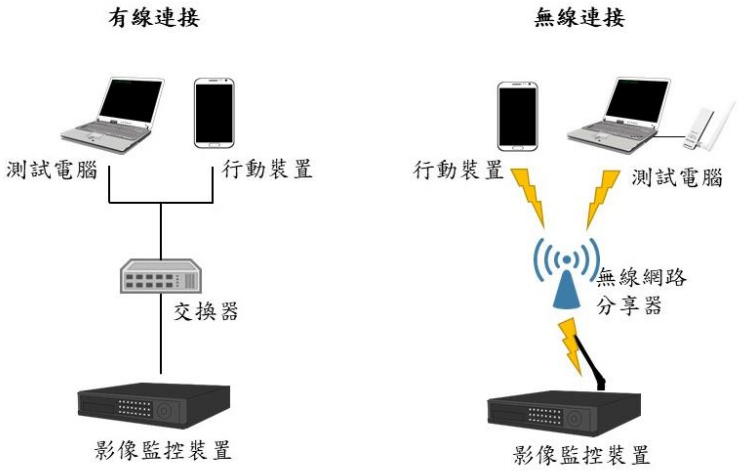

圖 3 測試示意圖

(e) 測試方法：

(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，瀏覽安全事件日誌。

(3) 觸發影像檔案寫入事件。

(4) 檢視日誌內容是否記載影像檔案寫入事件。

(5) 檢視該日誌之登入紀錄是否提供正確時間、使用者身分及執行結果。

(6) 將產品重新開機。

(7) 檢視重開機前之日誌資料是否仍然可視。

(f) 預期結果：

(1) 產品具有可供使用者檢視影像檔案寫入事件之安全事件日誌功能。

(2) 安全事件日誌的資料包含正確時間(包括年、月、日、時、分、秒)、使用者身分及執行結果。

(3) 重開機前之安全事件紀錄仍可查詢。

5.2.8 儲存安全測試

5.2.8.1 有效儲存空間設定機制測試

(a) 測試依據：

(1) IoT-1001-3「影像監控系統資安標準-第三部:影像錄影機」之 5.2.8.1。

(b) 測試目的：

(1) 確保產品儲存空間小於設定值時，提供警告機制。

(c) 樣品條件：

(1) 產品須提供當儲存空間不足時，此異常警示如何運作之說明文件。

(d) 測試佈局：

(1) 見圖 4。

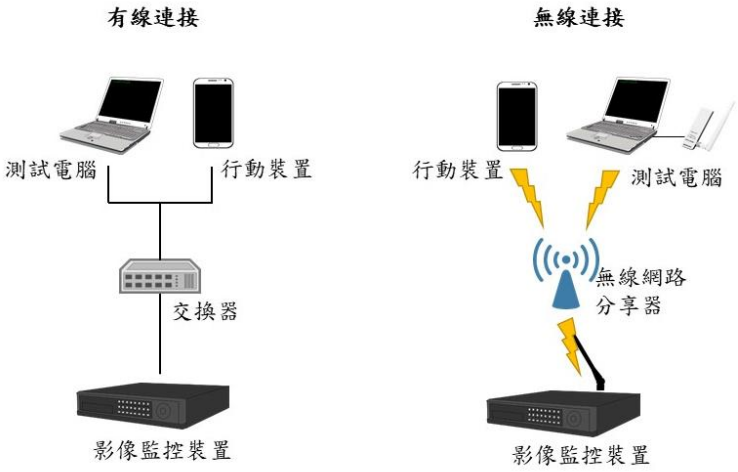

圖 4 測試示意圖

(e) 測試方法：

(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) 將產品之儲存空間填滿，導致可用空間小於設定值時。

(4) 檢視產品是否發出異常警示。

(f) 預期結果：

(1) 產品發出儲存空間不足之相關警示。

5.2.8.2 儲存資料防竄改機制測試

(a) 測試依據：

(1) IoT-1001-3「影像監控系統資安標準-第三部:影像錄影機」之 5.2.8.2。

(b) 測試目的：

(1) 確保產品支援影像檔案防竄改之警示機制。

(c) 樣品條件：

(1) 產品須提供系統管理者權限供使用者。

(d) 測試佈局：

(1) 見圖 5。

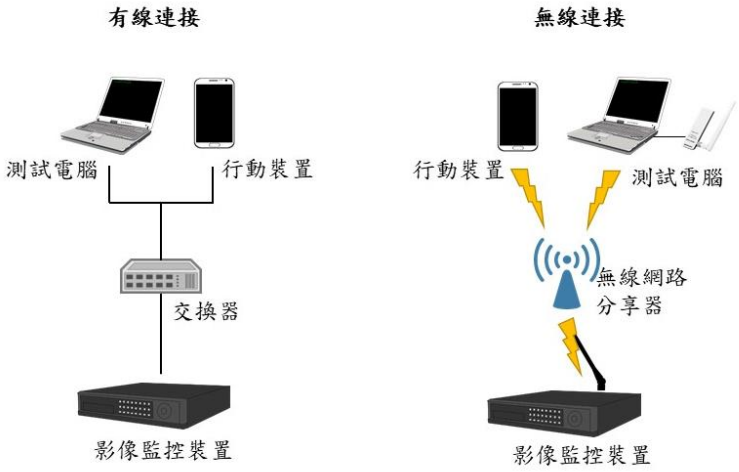

圖 5 測試示意圖

(e) 測試方法：

(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) 竄改產品所錄制之影像檔案。

(4) 檢視產品是否發出異常警示。

(f) 預期結果：

(1) 產品發出影像檔案遭竄改之相關警示。

5.2.9 系統備份安全測試

5.2.9.1 影像備份能力測試

(a) 測試依據：

(1) IoT-1001-3「影像監控系統資安標準-第三部:影像錄影機」之 5.2.9.1。

(b) 測試目的：

(1) 確保產品支援影像檔案備份功能。

(c) 樣品條件：

(1) 產品須提供備份功能之使用說明。

(d) 測試佈局：

(1) 見圖 6。

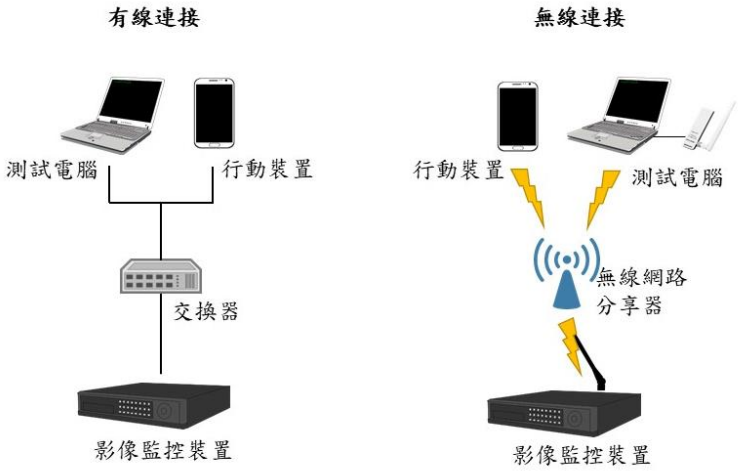

圖 6 測試示意圖

(e) 測試方法：

(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) 啟動備份功能，檢視功能是否正常運行。

(f) 預期結果：

(1) 備份功能正常運行。

5.2.9.2 影像備份保護測試

(a) 測試依據：

(1) IoT-1001-3「影像監控系統資安標準-第三部:影像錄影機」之 5.2.9.2。

(b) 測試目的：

(1) 確保產品之影像備份檔案之儲存機密性。

(c) 樣品條件：

(1) 產品須提供敏感性資料儲存保護之演算法書面資料作為審查依據。

(d) 測試佈局：

(1) 無。

(e) 測試方法：

(1) 審閱能證明符合此安全要求之書面資料。

(2) 檢視備份加密所採用之演算法。

(f) 預期結果：

(1) 備份加密採用 FIPS 140-2 Annex A [2]所核可之加密演算法。

5.3 通訊安全測試

檢視影像錄影機之通訊安全需求是否符合書面送審資料，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。

5.3.3 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

檢視影像錄影機之身分鑑別與授權機制測試需求是否符合書面送審資料，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

檢視影像錄影機之隱私保護需求是否符合書面送審資料，並依下列各測試項目進行實機測試。在本測試規範中，隱私資料泛指從影像錄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：

(1) IoT-1001-3「影像監控系統資安標準-第三部:影像錄影機」之 5.5.1.2。

(b) 測試目的：

(1) 驗證產品是否具備選定監控範圍內不予以顯示的影像區塊。

(c) 樣品條件：

(1) 產品須支援數位影像錄影機(DVR)功能，否則此測項不適用。

(d) 測試佈局：

(1) 見圖 7。

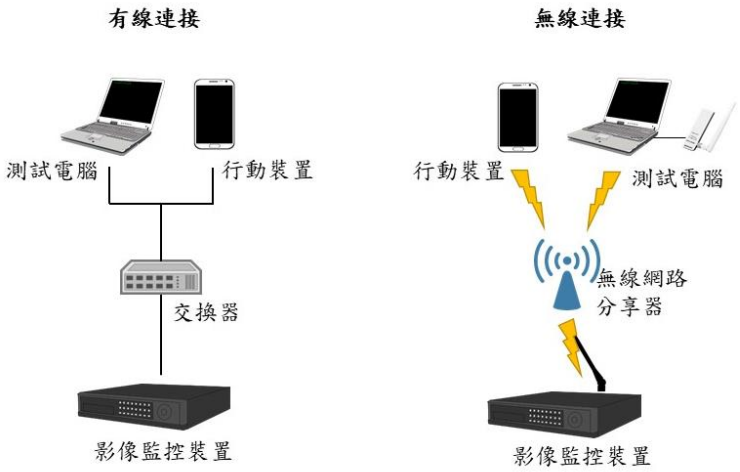

圖 7 測試示意圖

(e) 測試方法：

(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) 預期結果：

(1) 隱私遮罩所圈選的圖像區塊不可視。

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。

5.6 應用程式安全測試

檢視影像錄影機之應用程式安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.6.1 應用程式安全測試

5.6.1.1 應用程式防竄改測試

(a) 測試依據：

(1) IoT-1001-3「影像監控系統資安標準-第三部:影像錄影機」之 5.6.1.1。

(b) 測試目的：

(1) 驗證產品預載之應用程式是否具備遭竄改之啟動防護。

(c) 樣品條件：

(1) 無。

(d) 測試佈局：

(1) 產品須提供系統管理者權限供測試。

(e) 測試方法：

(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) 替換應用程式執行檔，檢視替換過後的應用程式可否被啟動。

(4) 替換網頁原始碼，檢視替換過後的網頁原始碼可否被啟動。

(f) 預期結果：

(1) 遭替換之應用程式不可被啟動。

(2) 遭替換之網頁原始碼不可被啟動。

5.6.1.2 應用程式防竄改測試

(a) 測試依據：

(1) IoT-1001-3「影像監控系統資安標準-第三部:影像錄影機」之 5.6.1.2。

(b) 測試目的：

(1) 檢視產品所引用網路相關之第三方函式庫來源。

(c) 樣品條件：

(1) 產品須提供所引用網路相關之第三方函式庫清單(包括函式庫名稱與版本號)。

(d) 測試佈局：

(1) 無。

(e) 測試方法：

(1) 審閱第三方函式庫清單。

(2) 根據該版本函式庫所可能潛藏 CVSS v3 評分為 9.0 分以上之資安漏洞，實際驗證是否確實存在。

(f) 預期結果：

(1) 經實測後未發現 CVSS v3 評分為 9.0 分以上之資安漏洞。

附錄 A
(規定)
安全功能規格說明(範例)

送測之產品應提供下表供測試實驗室參閱：

表一、安全功能規格表

項目	說明	申請者填寫內容
1.備份功能	一步步描述執行備份功能的方法，或提供佐證文件。 *範例：* *1. 登入管理介面。* *2. 點選「設定」。* *3. 點選「備份」。* *4. ...。*	
2.熱備援功能	一步步描述執行熱備援功能的方法，或提供佐證文件。 *範例：* *1. 登入管理介面。* *2. 點選「設定」。* *3. 點選「熱備援」。* *4. ...。*	
3.第三方函式庫清單	條列所使用之第三方函式庫。 *範例：* *1. openssl ver. 1.1.1。*	

參考資料

[1] IoT-1001-3 v1.0 影像監控系統資安標準-第三部:影像錄影機

[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