IoT-2001-1

影像監控系統資安測試規範

-第一部：一般要求

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
5.2.4.3 金鑰管理程序測試	(f)測試結果 (1)通過:產品有制定金鑰生成、交換、儲存、使用、銷毀及更換之程序，且該程序應達到監督、保證及證明金鑰得到妥善管理。 (2)不通過:產品**無**制定金鑰生成、交換、儲存、使用、銷毀及更換之程序，**或**該程序**未**達到監督、保證及證明金鑰得到妥善管理。	(f)測試結果 (1)通過:產品有制定金鑰生成、交換、儲存、使用、銷毀及更換之程序，且該程序應達到監督、保證及證明金鑰得到妥善管理。 (2)不通過:產品**有**制定金鑰生成、交換、儲存、使用、銷毀及更換之程序，**且**該程序**應**達到監督、保證及證明金鑰得到妥善管理。	(f)測試結果之(2)文字，因誤植而與(1)相同，進行勘誤。 修正測試結果之(2)不通過條件內容文字「有」改為「無」、「且」改為「或」、「應」改為「未」，其餘文字不變。
5.4.2.2 通行碼長度	(f)測試結果： (1)無法建立或變更小於 8 個字元長度之通行碼或產品發出通行碼強度不足警示。 (2)採用之通行碼強度原則出自國際標準或符合公認資安產業慣例。 (3)通過：(1)(2)項**任一**結果符合。 (4)不通過：(1)(2)項結果**皆**不符合。	(f)測試結果： (1)無法建立或變更小於 8 個字元長度之通行碼或產品發出通行碼強度不足警示。 (2)採用之通行碼強度原則出自國際標準或符合公認資安產業慣例。 (3)通過：(1)(2)項結果**皆**符合。 (4)不通過：(1)(2)項**任一**結果不符合。	修正(f)測試結果之(3)通過條件由「皆符合」改為「任一結果符合」。 修正(f)測試結果之(4)不通過條件由「任一結果不符合」改為「皆不符合」。
5.4.2.3 通行碼複雜度	(f)測試結果： (1)**依測試步驟(3)執行，**無法建立或變更通行碼，或產品發出通行碼強度不足警示。 (2)採用之通行碼強度原則出自國際標準	(f)測試結果： (1)無法建立或變更通行碼，或產品發出通行碼強度不足警示。 (2)採用之通行碼強度原則出自國際標準或符合公認資安產	修正(f)測試結果之(1)增加「依測試步驟(3)執行，」。 (3)通過條件由「皆符合」改為「任一結果符合」。 修正(f)測試結果之(4)不通過條件由

章節名稱	修正內容	現行內容	說　　明
	或符合公認資安產業慣例。 (3)通過：(1)(2)項**任一**結果符合。 (4)不通過：(1)(2)項結果**皆**不符合。	業慣例。 (3)通過：(1)(2)項結果**皆**符合。 (4)不通過：(1)(2)項**任一**結果不符合。	「任一結果不符合」改為「皆不符合」，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改善其資安品質，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-2001-1 影像監控系統資安標準測試規範-第一部：一般要求」(以下簡稱本測試規範)，依據「IoT-1001-1 影像監控系統資安標準-第一部：一般要求(1)」訂定，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

影像監控系統，又稱安控系統，目的是監看特定場所以達到維安目的，主要是由網路攝影機、數位影像錄影機、網路影像錄影機及網路儲存裝置組成，除此之外，監控所有攝影機畫面的監控中心，包括本地端或遠端電腦設備、行動裝置及雲端伺服器，及連接監控設備之網路環境，包括 Wi-Fi 存取點、路由器及交換機等，構成整個影像監控系統。

2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。有加註年份者，適用該年份之版次，不適用於其後之修訂版(包括補充增修)。無加註年份者，適用該最新版(包括補充增修)。

[1] CNS 27001: 2013 資訊技術－安全技術－資訊安全管理系統－要求事項

[2] NIST SP 800-92 Guide to Computer Security Log Management

[3] ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

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」所規定及下列用語及定義適用於本規範。

3.1. 密碼套件 (Cipher suite)

係指使用於安全通道(Secure sockets layer/ transport layer security, SSL/TLS)上用以協商安全設定之一系列安全機制，包括：身分驗證、加密、訊息鑑別碼(Message authentication code, MAC)和金鑰交換演算法。

3.2 網路埠掃描 (Port scan)

網路埠，又稱為通訊埠或者連接埠，作為連網裝置與外部來源之間傳送/接收通訊資料，一般駭客使用網路埠掃描來偵測電腦有開啟哪些網路埠或網路服務，進一步探尋其漏洞，藉此找到未經授權的存取點。

4. 測試項目分級

本節依據「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」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；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	5.1.1.1	-	-
	5.1.2. 實體異常行為警示測試	-	5.1.2.1 5.1.2.2	-
	5.1.3. 實體防護測試	5.1.3.1	-	-
	5.1.4. 安全啟動測試	-	-	5.1.4.1
系統安全	5.2.1. 作業系統與網路服務安全測試	5.2.1.1(a)	5.2.1.1(b)	5.2.1.2
	5.2.2. 最小化網路與服務連接埠管控測試	5.2.2.1 5.2.2.2	-	-
	5.2.3. 更新安全測試	5.2.3.1 5.2.3.2 5.2.3.3 5.2.3.4 5.2.3.5	-	-
	5.2.4. 敏感性資料儲存安全測試	5.2.4.1 5.2.4.2	5.2.4.3	5.2.4.4
	5.2.5. 網頁管理介面安全測試	5.2.5.1	-	-
	5.2.6. 操控程式之應用程式介面安全測試	5.2.6.1 5.2.6.2 5.2.6.3	-	-
	5.2.7. 安全事件日誌檔與警示測試	5.2.7.1 5.2.7.2 5.2.7.3	-	-
通訊安全	5.3.1. 敏感性資料傳輸安全測試	5.3.1.1	5.3.1.2	5.3.1.3
	5.3.2. 通訊協定與設置安全	5.3.2.1 5.3.2.2	5.3.2.3	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
	5.3.3. Wi-Fi 通訊安全	5.3.3.1 5.3.3.2	5.3.3.3	5.3.3.4
身分鑑別與授權機制安全	5.4.1. 鑑別機制安全測試	5.4.1.1 5.4.1.2	5.4.1.3 5.4.1.4	5.4.1.5 5.4.1.6
	5.4.2. 通行碼鑑別機制安全測試	5.4.2.1 5.4.2.2 5.4.2.3 5.4.2.4	-	5.4.2.5 5.4.2.6
	5.4.3. 權限管控測試	5.4.3.1 5.4.3.2	-	-
隱私保護	5.5.1. 隱私資料的存取保護測試	5.5.1.1 5.5.1.2	-	-
	5.5.2. 隱私資料的傳輸保護測試	5.5.2.1	5.5.2.2	5.5.2.3

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-1001-1 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 實體介面安全管控測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.1.1.1。

(b) 測試目的：

查驗不能透過產品之實體介面或應透過身分鑑別，存取作業系統之除錯模式。

(c) 前置條件：

(1) 產品應保持出廠預設組態。

(2) 產品若存在作業系統除錯介面，應於文件中說明進入作業系統除錯模式之方法。

(d) 測試布局：

無。

(e) 測試步驟：

(1) 檢視產品文件是否存在可進入作業系統除錯模式之實體介面。

(2) 根據文件所述進入作業系統除錯模式之方法，開啟相應之管理介面連接工具。

(3) 測試電腦連接產品之 USB 埠。

(4) 確認可否透過 USB 埠存取作業系統之除錯模式。

(5) 若存取前應經通行碼鑑別程序，則依照 5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4 測試通行碼鑑別機制之安全性。

(6) 測試電腦連接產品之 UART/JTAG 埠。

(7) 確認可否透過 UART/JTAG 埠存取作業系統之除錯模式。

(8) 若存取前應經通行碼鑑別程序，則依照 5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4 測試通行碼鑑別機制之安全性。

(f) 測試結果：

(1) 產品不存在進入作業系統除錯模式之介面。

(2) 產品透過 USB、UART 及 JTAG 存取作業系統之除錯模式時，產品要求通行碼鑑別，且符合 5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4 之測試結果。

(3) 通過：(1)(2)項結果符合其一。

(4) 不通過：(1)(2)項結果皆不符合。

(5) 不適用：無。

5.1.2 實體異常行為警示測試

5.1.2.1 實體埠插拔操作記錄功能

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.1.2.1。

(b) 測試目的：

查驗產品之實體埠有插拔紀錄。

(c) 前置條件：

應提供產品之實體埠插拔紀錄的操作說明

(d) 測試布局：

無。

(e) 測試步驟：

(1) 將測試電腦(或行動裝置)連接產品。

(2) 依產品送審資料，開啟相對應之管理介面連接工具。

(3) 若產品存在 USB 埠，插拔 USB 埠，由連接之電腦(或行動裝置)檢視插拔操作紀錄。

(4) 若產品存在 RJ45 埠，插拔 RJ45 埠，由連接之電腦(或行動裝置)檢視插拔操作紀錄。

(f)測試結果：

(1) 當產品具有 USB 埠，具有 USB 埠插拔操作紀錄功能。

(2) 當產品具有 RJ45 埠，具有 RJ45 埠插拔操作紀錄功能。

(3) 插拔操作紀錄包含正確時間格式(包括年、月、日、時、分、秒)、使用者身分及執行結果。

(4) 通過：(1)~(3)項結果皆符合。

(5) 不通過：(1)~(3)項結果不符合其一。

(6) 不適用：無。

5.1.2.2 實體異常狀態警示機制

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.1.2.2。

(b) 測試目的：

查驗產品之網路服務遭受實體層阻絕時，有相應之警示機制。

(c) 前置條件：

應提供產品之異常警示機制功能說明

(d) 測試布局：

無。

(e) 測試步驟：

(1) 若產品具有 RJ-45 埠，透過 RJ-45 埠連上網後，將網路線拔除，使主機因訊號中斷而無法連接上網路。

(2) 檢視產品是否依照異常警示機制功能說明達到警示效果。

(3) 若產品具有天線，透過天線連上網後，將天線遮罩，使主機因訊號中斷而無法連接上網路。

(4) 檢視產品是否依照異常警示機制功能說明達到警示效果。

(f)測試結果：

(1) 當產品具有 RJ-45 埠，透過 RJ-45 埠連線後發生斷訊狀況時，產品發出警示(例：電子郵件、推播、閃光、音效等)。

(2) 當產品具有天線，透過天線連線後發生斷訊狀況時，產品發出警示(例：電子郵件、推播、閃光、音效等)。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)(2)項結果不符合其一。

(5) 不適用：無。

5.1.3 實體防護測試

5.1.3.1 還原出廠預設通行碼之實體設計安全測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.1.3.1。

(b) 測試目的：

查驗產品實體層的預設通行碼還原設計，具備安全防護機制。

(c) 前置條件：

應提供產品之還原出廠設定操作說明。

(d) 測試布局：

無。

(e) 測試步驟：

(1) 檢視產品外觀(不包括設計上應鎖定於牆壁該面)，是否存在徒手即可輕易還原預設通行碼之機制。

(2) 若存在，則測試其還原至出廠設定之功能。

(f) 測試結果：

(1) 通過：產品外觀不存在徒手即可輕易還原回預設通行碼的機制。

(2) 不通過：產品外觀具備徒手即可輕易還原回預設通行碼的機制。

(3) 不適用：無。

5.1.4 安全啟動測試

5.1.4.1 測試產品是否支援安全啟動(secure boot)功能

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.1.4.1。

(b) 測試目的：

驗證產品於開機階段是否能確保產品之完整性及合法性。

(c) 前置條件：

產品應提供安全啟動功能之設計文件。

(d) 測試布局：

無。

(e) 測試步驟：

(1) 審閱具備安全啟動功能證明之書面資料。

(2) 確認產品在開機過程中是否驗證韌體與作業系統的簽章。

(f) 測試結果：

(1) 安全啟動功能僅能透過安全區域執行開機啟動。

(2) 書面資料證實產品在開機過程中驗證韌體與作業系統的簽章。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)(2)項結果不符合其一。

(5) 不適用：無。

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-1001-1 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 (a) 測試作業系統是否存在 CVSS v3.0 評分為 9.0 分以上之常見資安弱點與漏洞初階測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.1.1。

(b) 測試目的：

查驗產品之作業系統與網路服務不能含有已知 CVSS v3.0(或更新版本)評分為 9.0 分以上之資安風險漏洞。

(c) 前置條件：

應保持出廠預設組態。

(d) 測試布局：

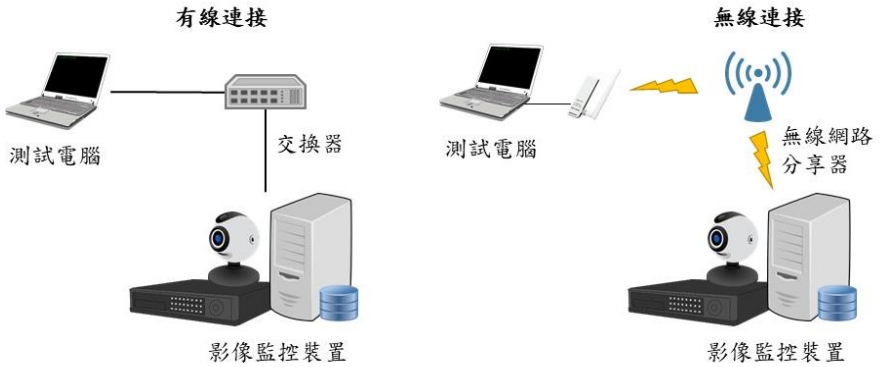

圖 1 測試示意圖

(e) 測試步驟：

(1) 將測試電腦連接產品。

(2) 啟動具作業系統與網路服務弱點掃描功能之工具，對產品執行弱點掃描。

(3) 檢視該弱點掃描工具所產生之報告，確認作業系統與網路服務是否存在 CVSS v3.0 評分為 9.0 分以上之資安風險漏洞。

(f) 測試結果：

(1) 作業系統與網路服務不存在 CVSS v3.0(或更新版本)評分為 9.0 分以上之資安風險漏洞。

(2) 當檢測出之資安風險漏洞不具有 CVSS v3.0(或更新版本)評分時，以 CVSS v2 評分為依據。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)(2)項結果不符合其一。

(5) 不適用：無。

5.2.1.1 (b) 測試作業系統是否存在 CVSS v3.0 評分為 9.0 分以上之常見資安弱點與漏洞中階測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.1.1。

(b) 測試目的：

深入作業系統，查驗產品之作業系統與網路服務不能含有已知 CVSS v3.0(或更新版本)評分為 9.0 分以上之資安風險漏洞。

(c) 前置條件：

(1) 應保持出廠預設組態。

(2) 送測廠商應提供系統最高管理(root)權限之帳戶，供實驗室測試用。

(d) 測試布局：

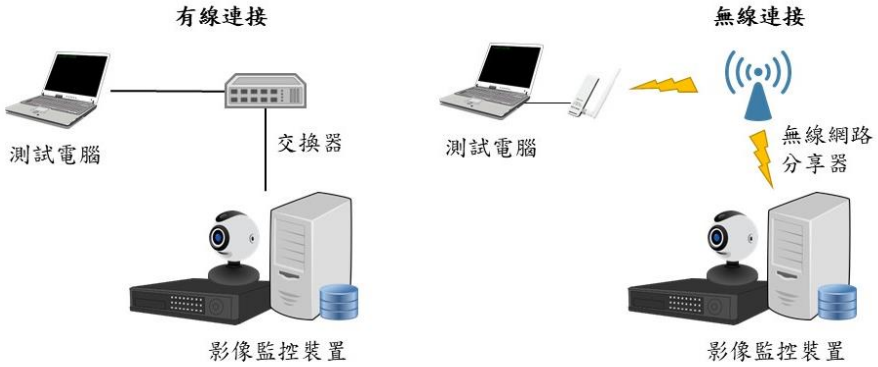

圖 2 測試示意圖

(e) 測試步驟：

(1) 將測試電腦連接產品。

(2) 啟動具作業系統與網路服務弱點掃描功能之工具，使用最高管理(root)權限之帳戶對產品執行弱點掃描。

(3) 檢視該弱點掃描工具所產生之報告，確認作業系統與網路服務是否存在 CVSS v3.0 評分為 9.0 分以上之資安風險漏洞。

(f) 測試結果：

(1) 作業系統與網路服務不存在 CVSS v3.0(或更新版本)評分為 9.0 分以上之資安風險漏洞。

(2) 當檢測出之資安風險漏洞不具有 CVSS v3.0(或更新版本)評分時，以 CVSS v2 評分為依據。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)(2)項結果不符合其一。

(5) 不適用：無。

5.2.1.2 測試作業系統與網路服務是否存在 CVSS v3.0 評分為 7.0 分以上之常見資安弱點與漏洞

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.1.2。

(b) 測試目的：

深入作業系統，查驗產品之作業系統與網路服務不能含有已知 CVSS v3.0(或更新版本)評分為 7.0 分以上之資安風險漏洞。

(c) 前置條件：

(1) 應保持出廠預設組態。

(2) 送測廠商應提供系統最高管理權限之帳戶，供實驗室測試用。

(d) 測試布局：

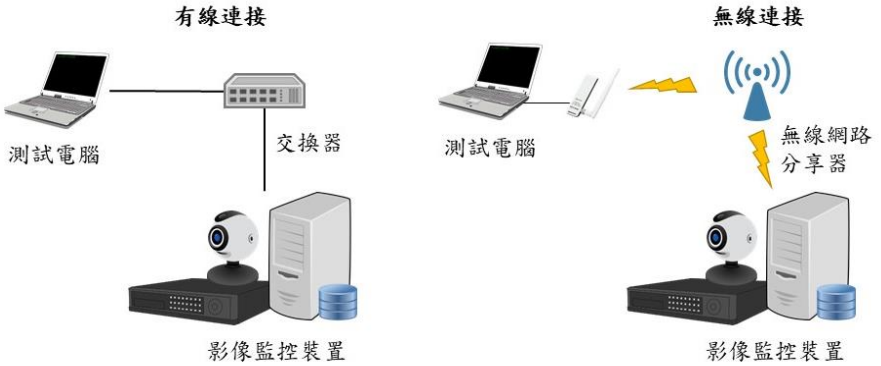

圖 3 測試示意圖

(e) 測試步驟：

(1) 將測試電腦連接產品。

(2) 啟動具作業系統與網路服務弱點掃描功能之工具，使用最高管理(root)權限之帳戶對產品執行弱點掃描。

(3) 檢視該弱點掃描工具所產生之報告，確認作業系統與網路服務是否存在 CVSS v3.0 評分為 7.0 分以上之資安風險漏洞。

(f) 測試結果：

(1) 作業系統與網路服務不存在 CVSS v3.0(或更新版本)評分為 7.0 分以上之資安風險漏洞。

(2) 當檢測出之資安風險漏洞不具有 CVSS v3.0(或更新版本)評分時，以 CVSS v2 評分為依據。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)(2)項結果不符合其一。

(5) 不適用：無。

5.2.2 最小化網路與服務連接埠管控測試

5.2.2.1 網路服務最小化測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.2.1。

(b) 測試目的：

查證產品不能存在預期以外之網路埠。

(c) 前置條件：

書面送審文件應包含產品啟用之網路服務與埠號的對應。

(d) 測試布局：

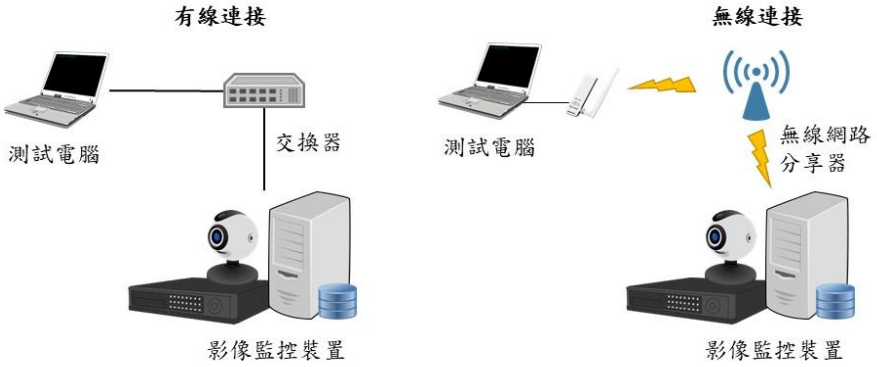

圖 4 測試示意圖

(e) 測試步驟：

(1) 將測試電腦連接產品，啟用廠商所宣告之網路服務。

(2) 啟動具網路埠掃描功能之工具，對產品執行 TCP 與 UDP 埠 0～65535 之掃描。

(3) 核對掃描結果所呈現之網路服務與對應埠。

(4) 比對產品送審資料中所聲明之網路服務與對應埠。

(f) 測試結果：

(1) 通過：產品所開啟之網路服務與對應埠，與送審資料之內容相符

(2) 不通過：產品所開啟之網路服務與對應埠，與送審資料之內容不符。

(3) 不適用：無。

5.2.2.2 遙測資料收集測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.2.2。

(b) 測試目的：

查驗產品不存在預期以外之遙測資料收集。

(c) 測試條件：

(1) 廠商應提供產品之遙測資料收集與利用宣告作為審查依據(包括但不限於產品使用手冊、包裝說明、本地端管理介面、網頁等介面)。

(2) 廠商應提供收集遙測資料的伺服器 IP 及/或 URL。

(d) 測試佈局：

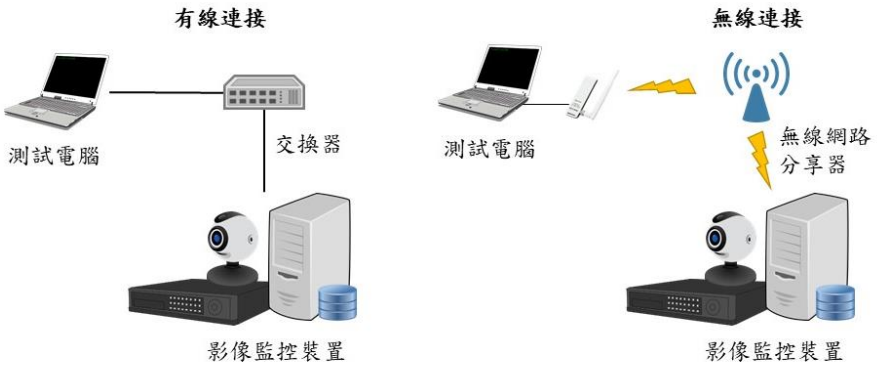

圖 5 測試示意圖

(e) 測試方法：

(1) 將測試電腦連接產品，啟用廠商所宣告之網路服務。

(2) 將產品連接網際網路，使用封包側錄工具，將受測物於連網狀態下持續側錄至少 24 小時。

(3) 檢視側錄結果是否存在產品所宣告之相連伺服器外之 IP 及/或 URL 資料。

(4) 審閱遙測數據收集與利用之說明。

(f) 檢測結果：

(1) 遙測數據收集與利用宣告中應詳細說明收集哪些資訊、使用目的、提供哪些廠商以外的第三方單位使用。

(2) 側錄結果與產品所宣告之相連伺服器之 IP 及/或 URL 資料一致。

(3) 通過：(1)(2)二項結果皆符合。

(4) 不通過：(1)(2)二項結果不符合其一。

(5) 不適用：無。

5.2.3 更新安全測試

5.2.3.1 軟/韌體更新功能測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.3.1。

(b) 測試目的：

查驗產品具軟/韌體更新功能。

(c) 前置條件：

無。

(d) 測試布局：

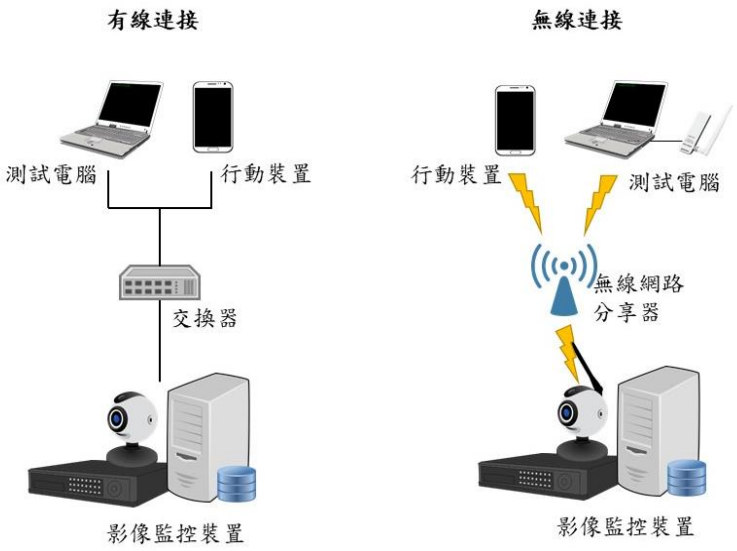

圖 6 測試示意圖

(e) 測試步驟：

(1) 將測試電腦連接產品。

(2) 根據文件所述執行軟/韌體更新。

(f) 測試結果：

(1) 通過：產品具軟/韌體更新功能。

(2) 不通過：產品不具軟/韌體更新功能。

(3) 不適用：無。

5.2.3.2 軟/韌體檔案安全測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.3.2。

(b) 測試目的：

查驗產品之軟/韌體有經過加密保護。

(c) 前置條件：

(1) 產品不具備更新能力則不通過。

(2) 產品應支援離線更新，否則不適用此測試項。

(3) 應提供產品所使用之完整軟/韌體。

(4) 應提供產品所使用之加密演算法書面資料作為審查依據。

(5) 若軟/韌體經過加密處理，則廠商應提供解密工具。

(6) 應提供產品所有相連伺服器之宣告。

(d) 測試布局：

無。

(e) 測試步驟：

(1) 使用具軟/韌體拆解功能之工具，對產品之軟韌體進行拆解。

(2) 檢視該軟/韌體更新檔是否可被解析出檔案系統目錄。

(3) 若軟/韌體更新檔無法被解析出檔案系統目錄，審閱可證明所使用加密演算法之書面資料。

(4) 若軟/韌體更新檔未加密，確認系統通行碼資料的保密機制是否採用 NIST SP 800-140C, CMVP Approved Security Functions(2)所核可之安全功能。

(5) 若軟/韌體更新檔未加密，確認是否存在金鑰。

(6) 若軟/韌體更新檔未加密，確認是否存在非公開之 email 資料。

(7) 若軟/韌體更新檔未加密，確認是否存在所宣告相連伺服器外之 IP 資料。

(8) 若軟/韌體更新檔未加密，確認是否存在所宣告相連伺服器外之 URL 資料。

(f) 測試結果：

(1) 軟/韌體具備更新功能。

(2) 軟/韌體更新檔案無法被解析出檔案系統目錄，且加密演算法採用 NIST SP 800-140C, CMVP Approved Security Functions 所核可之安全功能。

(3) 軟/韌體之程式碼與安裝檔內其他檔案，無檢出通行碼資料。

(4) 軟/韌體之程式碼與安裝檔內其他檔案，無檢出加解密演算法之金鑰，或加解密金鑰不能被解密回復。

(5) 軟/韌體之程式碼與安裝檔內其他檔案，不存在非公開 email 資料。

(6) 軟/韌體之程式碼與安裝檔內其他檔案，不存在所宣告相連伺服器外之 IP 資料。

(7) 軟/韌體之程式碼與安裝檔內其他檔案，不存在所宣告相連伺服器外之 URL 資料。

(8) 通過：(1)(2)項結果符合，或(1)(3)~(7)項結果皆符合。

(9) 不通過：不滿足(8)的測試結果。

(10) 不適用：產品具更新功能但不支援離線更新。

5.2.3.3 軟/韌體更新路徑的保護

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.3.3。

(b) 測試目的：

查驗產品之軟/韌體線上更新採用安全通道，同時能鑑別安全通道所使用憑證之真確性及有效性。

(c) 前置條件：

(1) 產品應支援線上更新，否則不適用此測試項。

(2) 應宣告更新伺服器之 IP。

(3) 送測廠商應協助觸發產品軟/韌體之線上更新。

(4) 產品應設定為出廠預設組態。

(d) 測試布局：

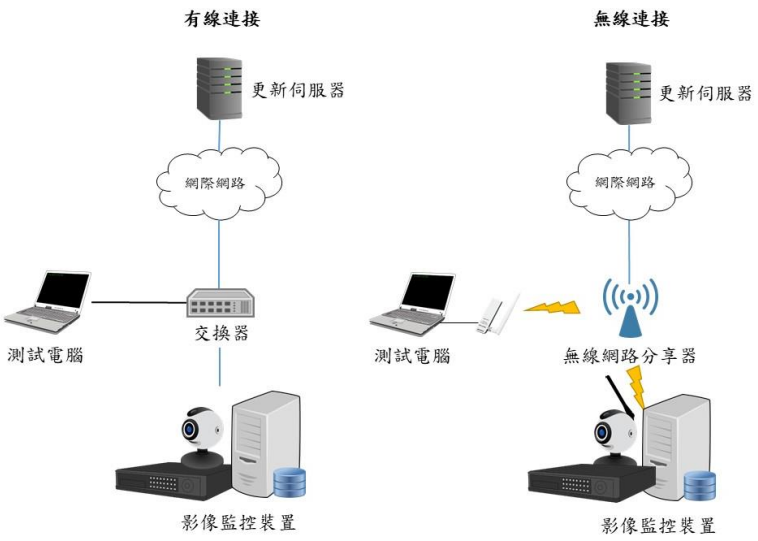

圖 7 測試示意圖

(e) 測試步驟：

(1) 啟動安全通道掃描工具，對更新伺服器進行掃描。

(2) 比對掃描結果，檢視伺服器所支援的密碼套件，是否符合附錄 A 之要求。

(3) 將測試電腦(或行動裝置)連接產品，並啟動更新。

(4) 側錄更新伺服器與產品間之封包，檢視所側錄之封包是否採用安全通道。

(5) 再次啟動更新。

(6) 於更新伺服器發送憑證予產品期間，攔截更新伺服器憑證，並置換憑證公鑰或憑證資訊，包括發證單位、有效期限、格式及憑證簽章。

(7) 發送已竄改之憑證予產品，於安全通道建立的交握過程中側錄封包，檢視產品是否接受此憑證。

(f) 測試結果：

(1) 軟/韌體具備更新功能。

(2) 產品之線上更新路徑通過安全通道，且安全通道僅支援附錄 A 中所建議之密碼套件。

(3) 若更新伺服器之憑證公鑰或憑證資訊被竄改，安全通道建立不成功。

(4) 通過：(1)~(3)項結果符合。

(5) 不通過：(1)~(3)項結果不符合其一。

(6) 不適用：產品具更新功能但不支援線上更新。

5.2.3.4 軟/韌體更新檔之完整性及真確性測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.3.4。

(b) 測試目的：

查驗產品具備驗證軟/韌體更新檔完整性及真確性之能力。

(c) 前置條件：

若選擇測試方法 1 應提供產品之數位簽章使用機制。應提供產品所使用之軟/韌體。

(d) 測試布局：

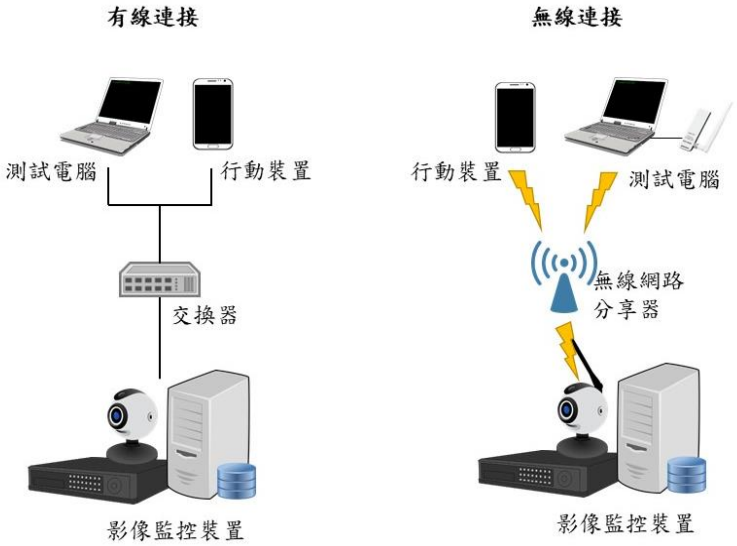

圖 8 測試示意圖

(e) 測試步驟：

方法 1 (廠商提供測試用私鑰予實驗室)：

(1) 廠商提供原始軟/韌體並提供簽章方法，實驗室使用自簽私鑰簽署該軟/韌體。

(2) 實驗室執行軟/韌體更新，檢視更新結果。

方法 2 (實驗室提供自簽公私鑰予廠商)：

(1) 實驗室提供自簽公私鑰予送測廠商，廠商利用該私鑰簽署軟/韌體，並將公鑰植入於產品。

(2) 實驗室執行軟/韌體更新，檢視更新結果。

(3) 受測廠商將實驗室所提供之測試私鑰加入受測物之受信任私鑰列表。

(4) 實驗室執行軟/韌體更新，檢視更新結果。

(f) 測試結果：

(1) 若採用測試方法 1，實驗室使用自簽私鑰簽署軟/韌體，軟/韌體更新失敗

(2) 若採用測試方法 2，廠商使用實驗室提供之自簽公私鑰，軟/韌體更新成功。

(3) 通過：(1)(2)項任一結果符合。

(4) 不通過：(1)(2)項皆不符合。

5.2.3.5 備援更新功能測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.3.5。

(b) 測試目的：

查驗當更新作業異常中斷時，產品仍可恢復正常運作狀態。

(c) 前置條件：

(1) 產品不具備更新機制，則不適用此測項。

(2) 當產品採用 windows 作業系統時，可提出補償措施於使用說明或安全指引中。

(d) 測試布局：

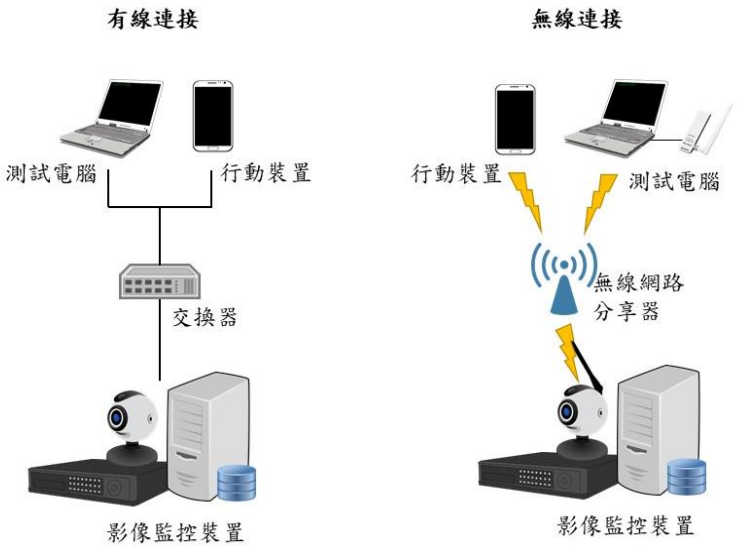

圖 9 測試示意圖

(e) 測試步驟：

(1) 將測試電腦連接產品。

(2) 於軟/韌體安裝期間中斷更新。

(3) 檢視軟/韌體更新結果。

(f) 測試結果：

(1) 更新中斷後，系統仍可回復正常運作狀態。

(2) 當產品採用 windows 作業系統時，產品之使用說明或安全指引敍明針對備援更新功能的補償措施。

(3) 通過：(1)(2)項任一符合。

(4) 不通過：(1)(2)項皆不符合。

(5) 不適用：產品不具備更新機制。

5.2.4 敏感性資料儲存安全測試

5.2.4.1 敏感性資料權限管控測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.4.1。

(b) 測試目的：

查驗產品所儲存之敏感性資料於作業系統存取具有權限管控機制。

(c) 前置條件：

(1) 產品不存在作業系統的存取介面，則不適用此測項。

(2) 應提供產品所儲存之敏感性資料存取權限宣告作為審查依據。

(3) 若存在作業系統的存取介面，應提供能進入產品作業系統的方法。

(4) 應提供產品之系統管理者權限。

(d) 測試布局：

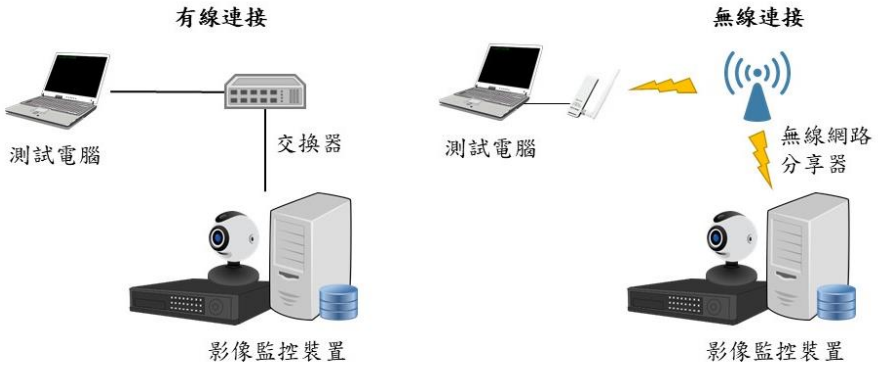

圖 10 測試示意圖

(e) 測試步驟：

(1) 將測試電腦連接產品。

(2) 依據送測廠商所提供之進入作業系統方法，存取產品作業系統。

(3) 檢視產品所儲存之通行碼存取權限。

(4) 檢視產品所儲存之加解密金鑰存取權限。

(f) 測試結果：

(1) 通過：產品通行碼及加解密金鑰之存取權限，與敏感性資料存取權限宣告相符。

(2) 不通過：產品通行碼及加解密金鑰之存取權限，與敏感性資料存取權限宣告不符。

(3) 不適用：產品不存在作業系統的存取介面。

5.2.4.2 敏感性資料加密儲存測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.4.2。

(b) 測試目的：

查驗產品之敏感性資料於儲存狀態下具有加密保護功能。

(c) 前置條件：

(1) 應提供產品所儲存之敏感性資料加密保護演算法作為審查依據。

(2) 應提供能進入產品作業系統的方法，及敏感性資料之存放位置。

(3) 應提供產品之系統管理者權限。

(4) 若產品具日誌功能，應提供檢視產品日誌之方法。

(5) 產品之根金鑰(root key)不適用此測項。

(d) 測試布局：

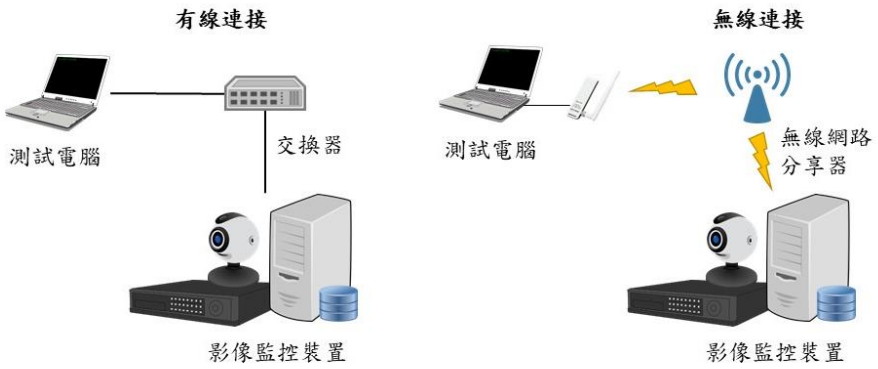

圖 11 測試示意圖

(e) 測試步驟：

(1) 審閱能證明符合此安全要求之書面資料。

(2) 將測試電腦連接產品。

(3) 依據送測廠商所提供之進入作業系統方法，及敏感性資料存放位置宣告，存取敏感性資料。

(4) 檢視產品所儲存之通行碼及加解密用金鑰是否加密保護。

(5) 若產品具日誌功能，檢視產品之日誌存在明文可識別之敏感性資料，例：密碼。

(f) 測試結果：

(1) 通行碼及加解密金鑰採用 NIST SP 800-140C, CMVP Approved Security Functions 所核可之安全功能，或 NTLMv2。

(2) 產品日誌不存在明文可識別之敏感性資料。

(3) 滿足 5.2.4.4 的測試結果。

(4) 通過 1：(1)(2)項皆符合。

(5) 通過 2：(3)項符合

(6) 不通過：(1)(2)項任一不符合。

(7) 不適用：產品不會儲存通行碼及加解密金鑰，或產品所儲存之根金鑰。

5.2.4.3 金鑰管理程序測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.4.3。

(b) 測試目的：

查驗產品之金鑰管理具備可靠的管控程序。

(c) 前置條件：

應提供產品之金鑰管理程序之說明文件。

(d) 測試布局：

無。

(e) 測試步驟：

審閱具備此程序說明之書面資料。

(f) 測試結果：

(1) 通過：產品有制定金鑰生成、交換、儲存、使用、銷毀及更換之程序，且該程序應達到監督、保證及證明金鑰得到妥善管理。

(2) 不通過：產品無制定金鑰生成、交換、儲存、使用、銷毀及更換之程序，或該程序未達到監督、保證及證明金鑰得到妥善管理。

(3) 不適用：產品不會使用到金鑰。

5.2.4.4 敏感性資料隔離保護測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.4.4。

(b) 測試目的：

查驗產品之敏感性資料之存放與正常作業系統隔離。

(c) 前置條件：

(1) 應提供產品之敏感性資料儲存方式之書面資料作為審查依據。

(2) 應聲明產品具備哪些資安功能使用到安全區域之書面資料作為審查依據。

(d) 測試布局：

無。

(e) 測試步驟：

審閱具備此功能證明之書面資料。

(f) 測試結果：

(1) 通過：書面資料證實產品之敏感性資料存放於安全區域。

(2) 不通過：書面資料無法證實產品之敏感性資料存放於安全區域。

(3) 不適用：產品不會儲存通行碼及加解密金鑰。

5.2.5 網頁管理介面安全測試

5.2.5.1 網頁管理介面常見資安風險測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.5.1。

(b) 測試目的：

查驗產品之網頁管理介面不存在 Injection 及 XSS 資安風險漏洞。

(c) 前置條件：

應提供產品網頁管理介面之系統管理者權限。

(d) 測試布局：

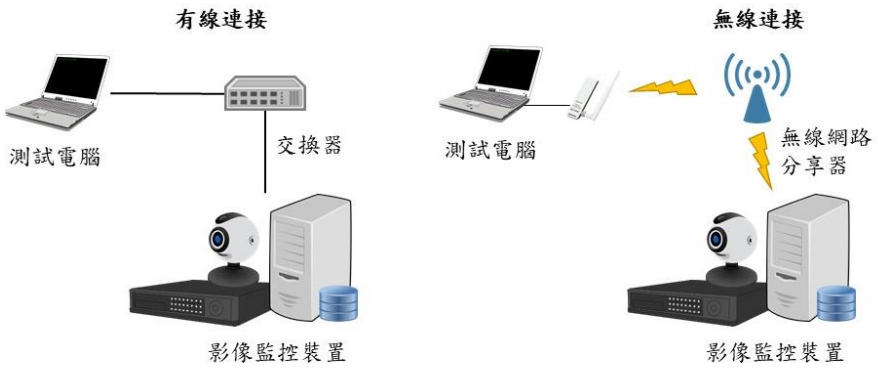

圖 12 測試示意圖

(e) 測試步驟：

(1) 將測試電腦連接產品。

(2) 開啟網頁管理介面。

(3) 啟動具備網頁弱點掃描功能之工具，對產品網頁介面執行弱點掃描。

(4) 檢視該弱點掃描工具所產生之報告，是否存在引發 Injection 及 Cross-Site Scripting (XSS)之資安攻擊風險。

(f) 測試結果：

(1) 通過：產品之網頁管理介面，不存在引發 Injection 及 XSS 資安攻擊風險。

(2) 不通過：產品之網頁管理介面，存在引發 Injection 及 XSS 資安攻擊風險。

(3) 不適用：產品無網頁管理介面。

5.2.6 ONVIF (Open Network Video Interface Forum)應用程式介面(API)安全測試

5.2.6.1 ONVIF 應用程式介面之鑑別機制測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.6.1。

(b) 測試目的：

查驗產品之 ONVIF 應用程式介面呼叫應經過鑑別程序，且該鑑別程序具備重送攻擊抵抗能力，並鑑別錯誤訊息未揭露敏感性資料。

(c) 前置條件：

(1) 產品未啟用 ONVIF profile S，則不適用此測項。

(2) 產品啟用 ONVIF profile Q，則此測試項結果為不適用。但是應在產品之使用說明書或資安指引中註明：「產品於出廠預設組態(factory default state)下，不建議連接網際網路。」，且該文件應公告在廠商官網上。

(3) 產品 ONVIF 應用程式介面之使用者帳戶已建立。

(d) 測試布局：

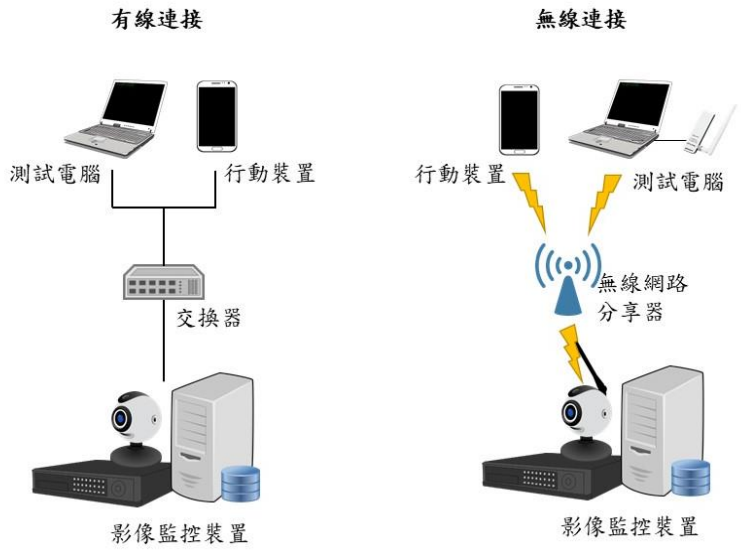

圖 14 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 開啟電腦或行動裝置之 ONVIF 操控程式。

(3) 執行影像監控相關操作，並執行封包側錄。

(4) 輸入已存在之使用者帳戶搭配錯誤的通行碼，檢視鑑別錯誤訊息。

(5) 輸入不存在之使用者帳戶，檢視鑑別錯誤訊息。

(6) 透過操控程式與產品建立連線，同時側錄封包。

(7) 執行影像監控相關操作，檢視封包側錄結果是否要求身分鑑別。

(8) 若產品要求身分鑑別，將側錄到的身分鑑別封包，再另一次身分鑑別操作時，重新發送至受測產品。

(9) 檢視鑑別結果是否成功。

(10) 若產品啟用 ONVIF profile Q，則審閱使用說明或資安指引之相關聲明。

(f) 測試結果：

(1) 透過 ONVIF 應用程式介面存取產品時有要求身分鑑別，且重送攻擊對該身分鑑別無效。

(2) 該身分鑑別錯誤訊息無法推斷出合法使用者帳戶或通行碼。

(3) 產品啟用 ONVIF profile Q，產品之使用說明書或資安指引有註明：「產品於出廠預設組態(factory default state)下，不建議連接網際網路。」，且該文件公告在廠商官網上。

(4) 通過：(1)(2)項結果符合，或(3)項結果符合。

(5) 不通過：不滿足(4)的測試結果。

(6) 不適用：產品未啟用 ONVIF profile S。

5.2.6.2 ONVIF 應用程式介面之通行碼鑑別強度機制測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.6.2。

(b) 測試目的：

查驗產品之 ONVIF 應用程式介面的通行碼鑑別機制強度應足夠。

(c) 前置條件：

(1) 產品之 ONVIF 應用程式介面未支援通行碼鑑別機制，則不適用此測項。

(2) 應提供產品 ONVIF 應用程式介面之之帳戶鎖定機制之設計說明。

(d) 測試布局：

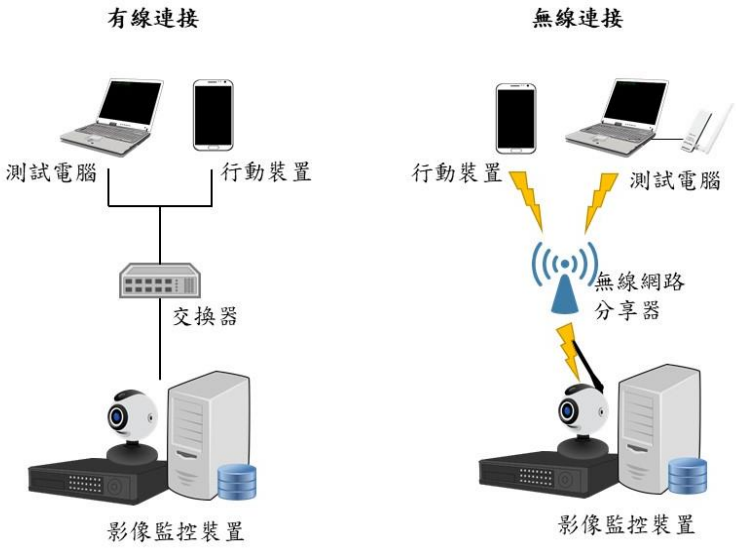

圖 16 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 側錄 ONVIF 之通行碼鑑別封包。

(3) 檢視側錄之封包是否符合 5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4 通行碼鑑別機制之安全性。

(f) 測試結果：

通行碼鑑別機制符合 5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4 之測試預期結果。

5.2.6.3 ONVIF 應用程式介面之權限管控機制測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.6.3。

(b) 測試目的：

查驗產品之 ONVIF 應用程式介面應存在權限管控。

(c) 前置條件：

(1) 產品未啟用 ONVIF profile S，則不適用此測項。

(2) 應提供產品 ONVIF 應用程式介面之角色存取權限之宣告。

(d) 測試布局：

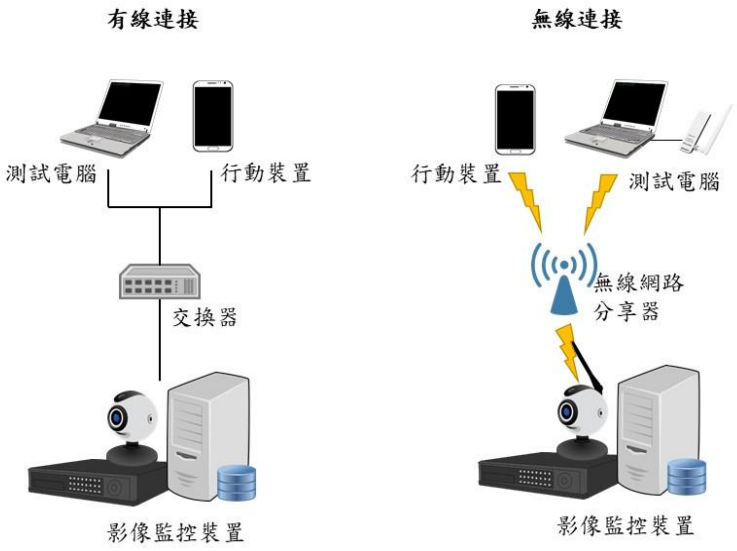

圖 13 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 開啟電腦或行動裝置之 ONVIF 操控程式。

(3) 分別以不同角色使用具 ONVIF API 功能之應用程式存取產品。

(4) 同時檢視該帳戶之身分類型與其對應之權限是否與產品的自我宣告內容相符。

(f) 測試結果：

(1) 各角色 ONVIF API 的權限管控與產品自我宣告相符。

(2) 至少具 2 個以上不同權限的角色。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)(2)項結果不符合其一。

(5) 不適用：產品未啟用 ONVIF profile S。

5.2.7 安全事件日誌與警示測試

5.2.7.1 安全事件日誌測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.7.1。

(b) 測試目的：

查驗產品有安全事件日誌供查詢。

(c) 前置條件：

(1) 應提供安全事件日誌之查詢方法。

(2) 若產品之安全事件日誌由後台伺服器記錄，則應提供可對接之後台伺服器進行測試。

(3) 若產品之安全事件日誌由後台伺服器記錄，則應提供使用說明或資安指引供審。

(d) 測試布局：

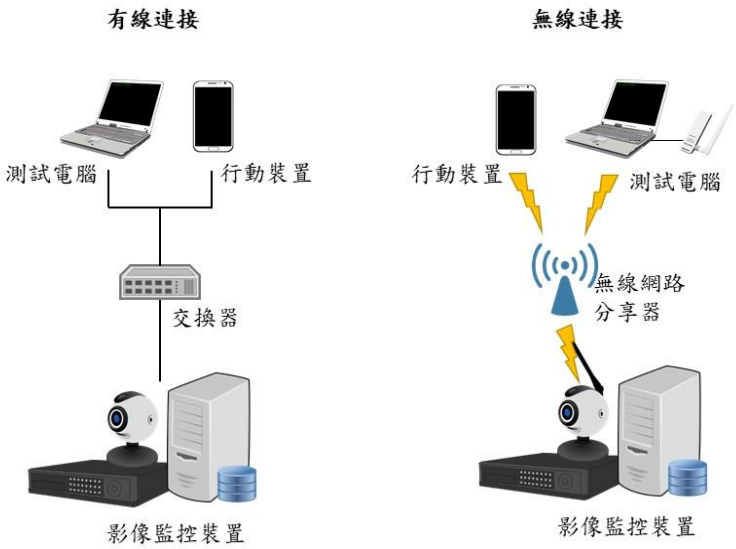

圖 17 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 依產品使用說明，開啟相對應之管理介面連接工具，瀏覽安全事件日誌。

(3) 檢視日誌內容是否記載使用者的登入紀錄，包括時間(含年、月、日、時、分、秒)、登入後之使用者身分及登入成功與否。

(4) 將產品重新開機。

(5) 檢視重開機前之安全事件日誌資料是否存在。

(6) 若產品之安全事件日誌皆記錄於後台伺服器中，則側錄送往後台之安全事件日誌封包。

(7) 審閱使用說明或資安指引之相關安全日誌聲明。

(f) 測試結果：

(1) 產品具有可供使用者檢視之安全事件日誌功能。

(2) 產品之安全事件日誌資料，包含時間、登入後之使用者身分及登入成功與否。

(3) 重開機前之安全事件日誌仍可查詢。

(4) 若產品之安全事件日誌由後台伺服器記錄，則產品送往後台之安全事件日誌封包的資料，至少包含時間、登入後之使用者身分及登入成功與否。

(5) 若產品之安全事件日誌由後台伺服器記錄，則應於使用說明書或資安指引中聲明此情境，且該文件公告在廠商官網上。

(6) 通過：(1)~(3)項結果符合，或(4)(5)項結果皆符合。

(7) 不通過：不滿足(6)的測試結果。

(8) 不適用：無。

5.2.7.2 安全事件日誌檔存取權限管控測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.7.2。

(b) 測試目的：

(c) 查驗產品之安全事件日誌具權限控管。

(d) 前置條件：

(1) 產品之安全事件日誌皆記錄於後台伺服器中，則不適用此測項。

(2) 產品之使用者帳戶及相關鑑別因子(例：通行碼)已建立，並存在系統管理者及一般使用者二類帳戶。

(3) 應提供產品之安全事件日誌存取權限之聲明。

(e) 測試布局：

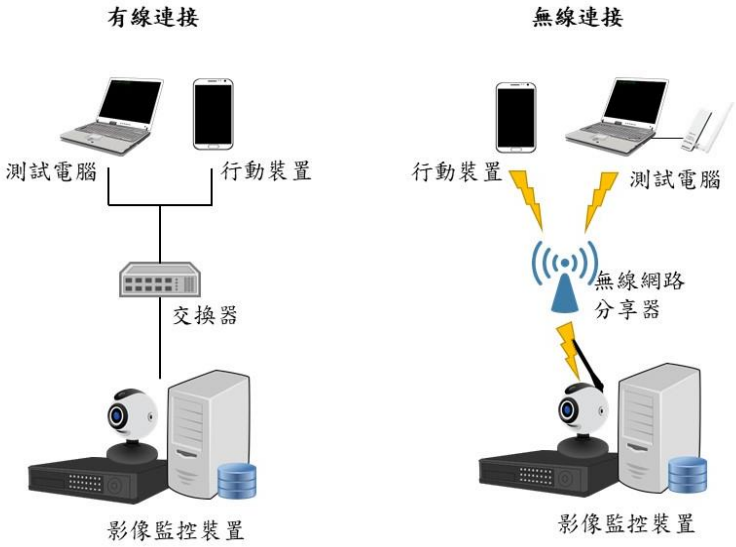

圖 18 測試示意圖

(f) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 依產品使用說明，開啟相對應之管理介面連接工具，瀏覽安全事件日誌。

(3) 檢視帳戶之身分類型對安全事件日誌的存取權限是否與產品自我宣告相符。

(g) 測試結果：

(1) 安全事件日誌的身分授權與產品之自我宣告內容相符。

(2) 至少有 2 個以上不同權限的角色。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)(2)項結果不符合其一。

(5) 不適用：產品之安全事件日誌皆記錄於後台伺服器中。

5.2.7.3 安全事件日誌檔之日誌滾動功能測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.2.7.3。

(b) 測試目的：

查驗產品具處理日誌儲存空間不足之異常狀況的能力。

(c) 前置條件：

(1) 產品之安全事件日誌皆記錄於後台伺服器中，則不適用此測項。

(2) 應提供產品之系統管理者權限。

(d) 測試布局：

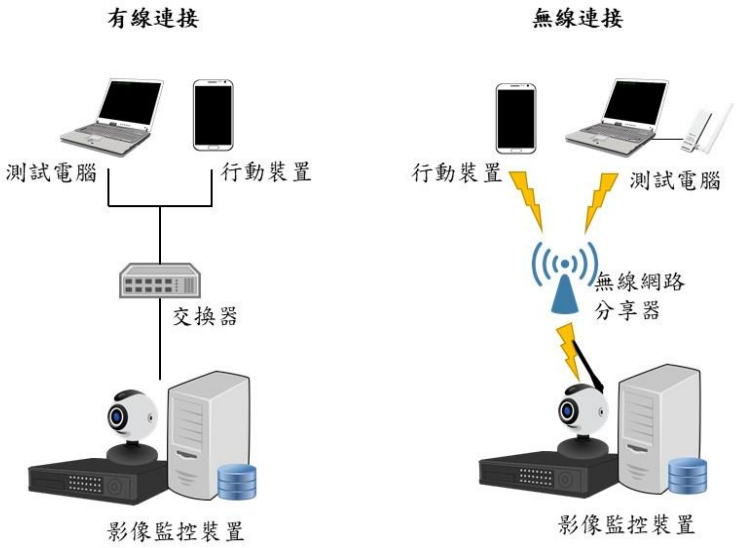

圖 19 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 不斷觸發安全事件日誌，以填充安全事件紀錄儲存空間，直到發生日誌儲存空間循環使用。

(3) 檢視產品是否無法正常記錄安全事件。

(f) 測試結果：

(1) 通過：產品仍可正常記錄安全事件。

(2) 不通過：產品發生儲存空間不足的現象。

(3) 不適用：產品之安全事件日誌皆記錄於後台伺服器中。

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-1001-1 之安全要求，並依下列各測試項目進行實機測試。

5.3.1 敏感性資料傳輸安全測試

5.3.1.1 敏感性資料之傳輸保護初階測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.3.1.1。

(b) 測試目的：

查驗產品敏感性資料之傳輸，預設採用強度足夠之安全通道。

(c) 前置條件：

產品應保持出廠預設組態。

(d) 測試布局：

圖 20 測試示意圖

(e) 測試步驟：

(1) 掃描產品使用之安全通道。

(2) 比對掃描結果是否為附錄 A 中所包含之密碼套件。

(3) 將測試電腦及行動裝置連接產品。

(4) 登入相對應之管理介面，同時側錄封包。

(5) 檢視所側錄之封包是否採用安全通道傳輸。

(f) 測試結果：

(1) 安全通道僅採用附錄 A 中所建議之密碼套件。

(2) 與測試電腦之間的帳戶通行碼資訊傳輸，預設採用安全通道。

(3) 與行動裝置之間的帳戶通行碼資訊傳輸，預設採用安全通道。

(4) 通過：(1)~(3)項結果皆符合。

(5) 不通過：(1)~(3)項結果不符合其一。

(6) 不適用：產品不存在敏感性資料。

5.3.1.2 敏感性資料之傳輸保護中階測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.3.1.2。

(b) 測試目的：

確認產品具備查驗此安全通道憑證有效性及真確性之能力。

(c) 前置條件：

(1) 應提供可與產品相連之影像監控裝置。

(2) 若與產品相連之影像監控裝置採用自簽發憑證，則應提供可匯入根憑證或中繼憑證(immediate certificate)之介面。

(d) 測試布局：

圖 21 測試示意圖

(e) 測試步驟：

(1) 載入可驗證對連影像監控裝置之根憑證或中繼憑證(immediate certificate)至產品中。

(2) 將產品與其他影像監控裝置連接，並啟動安全通道之建立程序。

(3) 當其他影像監控裝置發送憑證予產品時，攔截其憑證，並置換憑證公鑰及憑證資訊(包括發證單位、有效期限、格式及憑證簽章)。

(4) 發送已竄改之憑證予產品，於安全通道建立的交握過程中側錄封包，檢視產品是否接受此憑證。

(f) 測試結果：

(1) 通過：已竄改敏感性資料傳輸用之安全通道憑證未通過產品鑑別。

(2) 不通過：已竄改敏感性資料傳輸用之安全通道憑證通過產品鑑別。

(3) 不適用：產品不存在敏感性資料。

5.3.1.3 敏感性資料之傳輸保護高階測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.3.1.3。

(b) 測試目的：

查驗產品之敏感性資料傳輸，支援強加密演算法。

(c) 前置條件：

產品應具備安全通道功能。

(d) 測試布局：

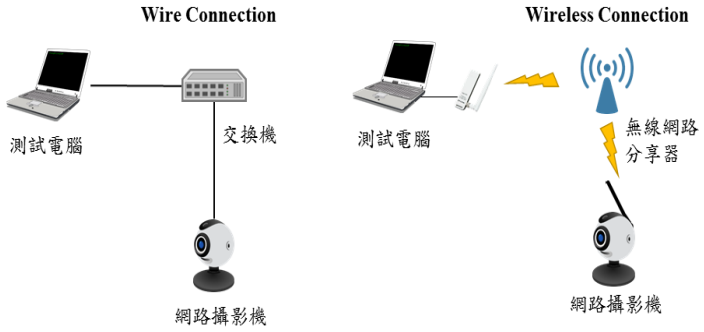

圖 22 測試示意圖

(e) 測試步驟：

(1) 將測試電腦及行動裝置連接產品。

(2) 掃描產品使用之安全通道。

(3) 比對掃描結果是否為附錄 A 中所包含之密碼套件，且支援 AES-256 同等或以上加密強度的演算法。

(f) 測試結果：

(1) 通過：該安全通道支援 AES-256 同等或以上加密強度的演算法。

(2) 不通過：該安全通道不支援 AES-256 同等或以上加密強度的演算法。

(3) 不適用：產品不具備安全通道功能。

5.3.2 通訊協定與設置安全測試

5.3.2.1 網路裝置資訊探詢功能測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.3.2.1。

(b) 測試目的：

查驗產品未運行在具安全風險的網路探詢協定。

(c) 前置條件：

(1) 產品應支援通用隨插即用通訊協定(UPnP)、簡單網路管理協定(SNMP)、零配置通訊協定(Bonjour)之任一網路服務，否則本測試項不適用。

(2) 產品應保持出廠預設組態。

(3) 產品應提供產品所支援網路服務之說明文件。

(d) 測試布局：

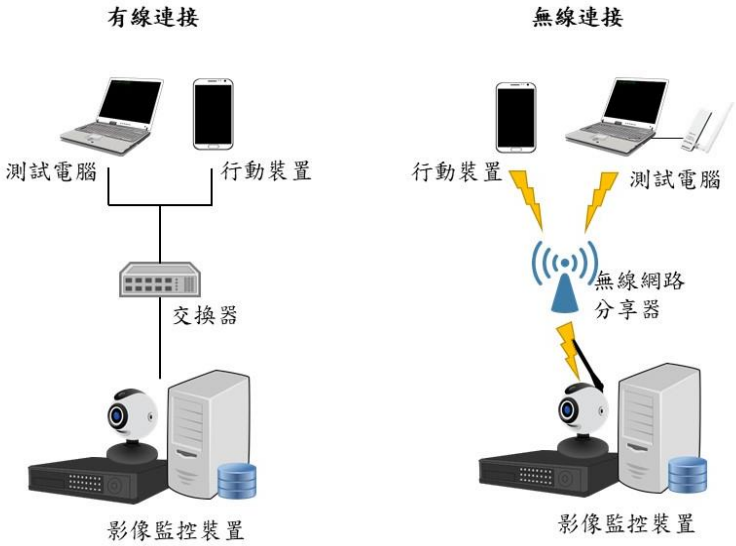

圖 23 測試示意圖

(e) 測試步驟：

(1) 將測試電腦及行動裝置連接產品。

(2) 依產品使用說明，開啟相對應之管理介面連接工具。

(3) 若產品支援 UPnP，目視產品之操控程式或網頁管理介面，UPnP 是否存在供使用者操作的開/關介面。

(4) 透過具 UPnP 掃描功能之工具，以查驗產品是否支援 UPnP 服務，同時查驗使用者是否可自行開/關 UPnP 服務。

(5) 若產品支援 SNMP，目視產品之操控程式或網頁管理介面，SNMP 是否存在供使用者操作的開/關介面。

(6) 透過具 SNMP 掃描功能之工具，以查驗產品是否支援 SNMP 服務，同時查驗使用者是否可自行開/關 SNMP 服務。

(7) 若產品支援零配置通訊協定，目視產品之操控程式或網頁管理介面，零配置通訊協定是否存在供使用者操作的開/關介面。

(8) 透過具零配置通訊協定掃描功能之工具，以查驗產品是否支援零配置通訊協定服務，同時查驗使用者是否可自行開/關零配置通訊協定服務。

(f) 測試結果：

(1) 若產品支援 UPnP 服務，該服務提供使用者可自行開/關功能之設置。

(2) 若產品支援 SNMP 服務，該服務提供使用者可自行開/關功能之設置。

(3) 若產品支援零配置通訊協定服務，該服務提供使用者可自行開/關功能之設置。

(4) 通過：(1)~(3)項結果皆符合。

(5) 不通過：(1)~(3)項結果不符合其一。

(6) 不適用：產品不支援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)之網路服務。

5.3.2.2 網路介面存取設置測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.3.2.2。

(b) 測試目的：

查驗產品之遠端存取除錯模式的方法是具管控的。

(c) 前置條件：

(1) 產品應保持出廠預設組態。

(2) 產品若存在遠端進入除錯模式之介面，應提供進入之方法。

(d) 測試布局：

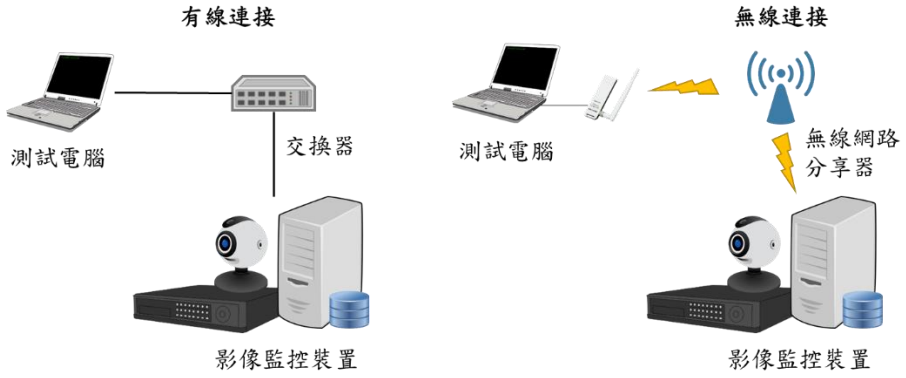

圖 24 測試示意圖

(e) 測試步驟：

(1) 將測試電腦及行動裝置連接產品。

(2) 依產品使用說明，開啟相對應之管理介面連接工具。

(3) 查驗可否透過網路連線存取除錯模式。

(4) 若存取前應經通行碼鑑別程序，則依照 5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4 測試通行碼鑑別機制之安全性。

(f) 測試結果：

(1) 不存在進入作業系統除錯模式之介面。

(2) 若存在進入作業系統除錯模式之介面，產品要求鑑別。

(3) 若存在進入作業系統除錯模式之介面，且要求通行碼鑑別，通行碼鑑別機制符合 5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4 之測試預期結果。

(4) 通過：(1)項結果符合，或(2)(3)項結果皆符合。

(5) 不通過：不滿足(4)的測試結果。

(6) 不適用：無。

5.3.2.3 通訊協定異常輸入測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.3.2.3。

(b) 測試目的：

查驗產品影像傳輸相關之通訊協定是否存在未知之資安風險漏洞。

(c) 前置條件：

產品應支援附錄 B 中任一通訊協定。

(d) 測試布局：

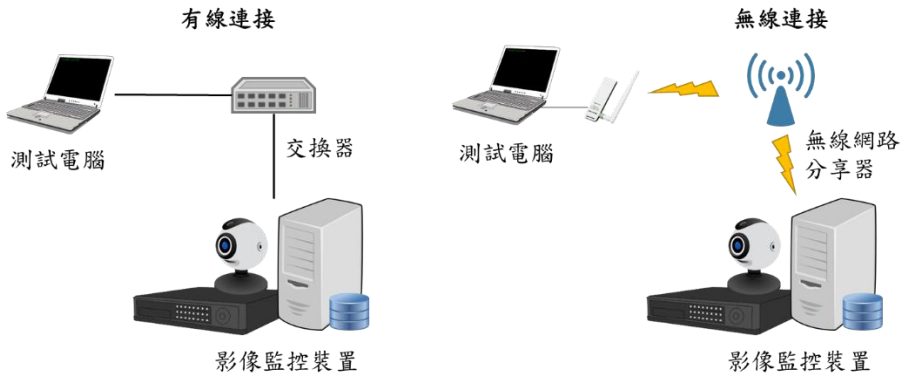

圖 25 測試示意圖

(e) 測試步驟：

(1) 將測試電腦及行動裝置連接產品。

(2) 啟動具模糊測試功能之工具。

(3) 執行對附錄 B 中各種類(例：B1、 B2、B3)之通訊協定所有欄位至少 10 萬筆唯一且獨立之測試項，或者最少 8 小時的異常輸入測試。

(4) 確保同時間只能進行單一測試案例。

(5) 對產品執行影像監控之操作，檢查產品是否仍正常運作。

(f) 測試結果：

(1) 通過：產品於測試過程中不會因為某一特定異常封包而發生程序崩潰(crash)。

(2) 不通過：產品於測試過程中因為某一特定異常封包而發生程序崩潰。

(3) 不適用：無。

5.3.3 Wi-Fi 通訊安全測試

本子節的測試項目參照國家通訊傳播委員會出版之「無線網路攝影機資通安全檢測技術指引」(4)。

5.3.3.1 安全的 Wi-Fi 組態設置測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.3.3.1。

(b) 測試目的：

查驗產品不存在錯誤的 Wi-Fi 設定。

(c) 前置條件：

(1) 產品應支援 Wi-Fi 保護設定功能，否則此測試項不適用。

(2) 產品應保持出廠預設組態。

(d) 測試布局：

圖 26 測試示意圖

(e) 測試步驟：

(1) 將測試電腦及行動裝置連接產品。

(2) 依產品使用說明，開啟相對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，WPS PIN 是否存在供使用者操作的開/關介面，且此開/關功能是否有效。

(f) 測試結果：

(1) 有提供使用者 WPS PIN 開/關之功能。

(2) WPS PIN 功能預設為關閉。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)(2)項結果不符合其一

(5) 不適用：產品不支援 Wi-Fi 保護設定功能。

5.3.3.2 無線網路傳輸安全機制設置測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.3.3.2。

(b) 測試目的：

查驗產品具有安全的 Wi-Fi 通道保護設定。

(c) 前置條件：

(1) 產品應支援 Wi-Fi 保護設定功能，否則此測試項不適用。

(2) 產品應保持出廠預設組態。

(d) 測試布局：

圖 27 測試示意圖

(e) 測試步驟：

(1) 將測試電腦及行動裝置連接產品。

(2) 依產品使用說明，開啟相對應之管理介面連接工具。

(3) 與產品建立連線，同時側錄傳輸封包。

(4) 依側錄結果查驗傳輸係採用〝Wi-Fi 保護設置 v2 同等或以上之版本〞加密方式。

(f) 測試結果：

(1) 通過：Wi-Fi 預設加密模式為〝Wi-Fi 保護設置 v2 同等或以上之版本〞。

(2) 不通過：Wi-Fi 預設加密模式不為〝Wi-Fi 保護設置 v2 同等或以上之版本〞

(3) 不適用：產品不支援 Wi-Fi 功能。

5.3.3.3 Wi-Fi 通訊協定異常輸入測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.3.3.3。

(b) 測試目的：

查驗產品支援之 Wi-Fi 通訊協定不存在其他資安漏洞。

(c) 前置條件：

產品應支援 Wi-Fi 功能。

(d) 測試布局：

圖 28 測試示意圖

(e) 測試步驟：

(1) 將產品以 Wi-Fi 連線至測試電腦所模擬的 Wi-Fi 存取點(AP)。

(2) 啟動具模糊測試功能之工具。

(3) 執行對 IEEE 802.11x 通訊協定所有欄位至少 10 萬筆唯一且獨立之測試項，或者至少 8 小時的異常輸入測試。

(4) 確保同時間只能進行 1 個測試案例。

(5) 對產品執行影像監控之操作，查驗產品仍正常運作。

(f) 測試結果：

(1) 通過：產品於測試過程中不會因為某一特定異常封包而發生程序崩潰。

(2) 不通過：產品於測試過程中因為某一特定異常封包而發生程序崩潰。

(3) 不適用：產品不支援 Wi-Fi 功能。

5.3.3.4 Wi-Fi 認證安全機制設置測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.3.3.4。

(b) 測試目的：

查驗產品支援 IEEE 802.1X 身分鑑別。

(c) 前置條件：

應提供產品建立 IEEE 802.1X 身分鑑別的操作說明。

(d) 測試布局：

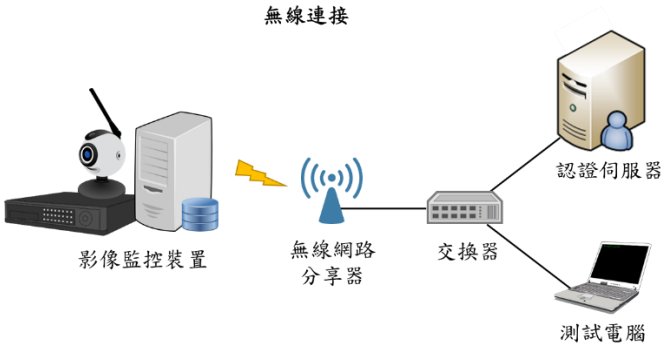

圖 29 測試示意圖

(e) 測試步驟：

(1) 將產品之 IEEE 802.1X 功能開啟。

(2) 連接已啟用 IEEE 802.1X 功能之 Wi-Fi AP。

(f) 測試結果：

(1) 通過：產品可透過 IEEE 802.1X 建立 Wi-Fi 連線。

(2) 不通過：產品無法透過 IEEE 802.1X 建立 Wi-Fi 連線。

(3) 不適用：無。

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-1001-1 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 鑑別機制強度測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.1.1。

(b) 測試目的：

查驗產品具備安全之身分鑑別機制。

(c) 前置條件：

無。

(d) 測試布局：

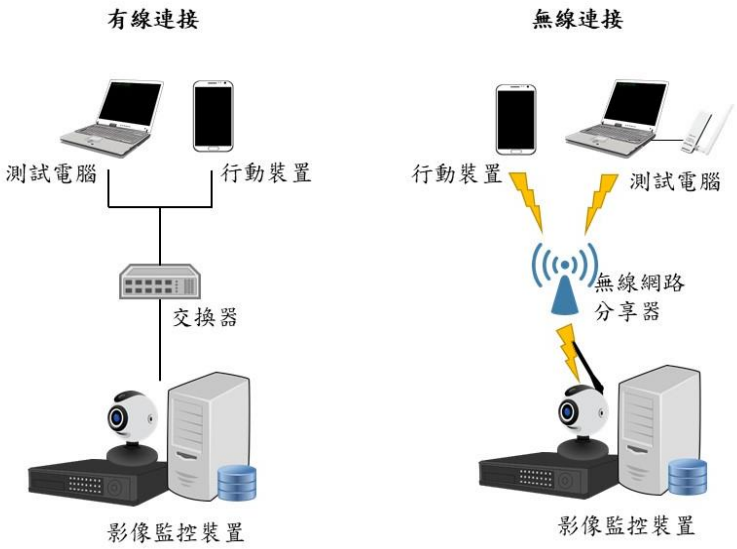

圖 30 測試示意圖

(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，開啟相對應之管理介面連接工具。

(3) 當產品具網頁管理介面，嘗試在未登入情況下，存取錄影監控頁面。

(4) 執行身分鑑別操作，同時側錄封包。

(5) 將側錄到的身分鑑別封包，於另一次身分鑑別操作時，重送至受測產品。

(6) 檢視鑑別結果。

(7) 從產品登出後，嘗試存取需登入時的操作是否仍可成功存取。

(f) 測試結果：

(1) 產品具備身分鑑別機制且身分鑑別功能不能被關閉，同時鑑別機制具備抵抗重送攻擊的能力。

(2) 產品登出後應再次登入，方可存取。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)(2)項結果不符合其一。

(5) 不適用：無。

5.4.1.2 身分鑑別錯誤訊息測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.1.2。

(b) 測試目的：

查驗產品鑑別錯誤訊息未揭露敏感性資料。

(c) 前置條件：

產品不支援身分別機制，則不適用此測項。

(d) 測試布局：

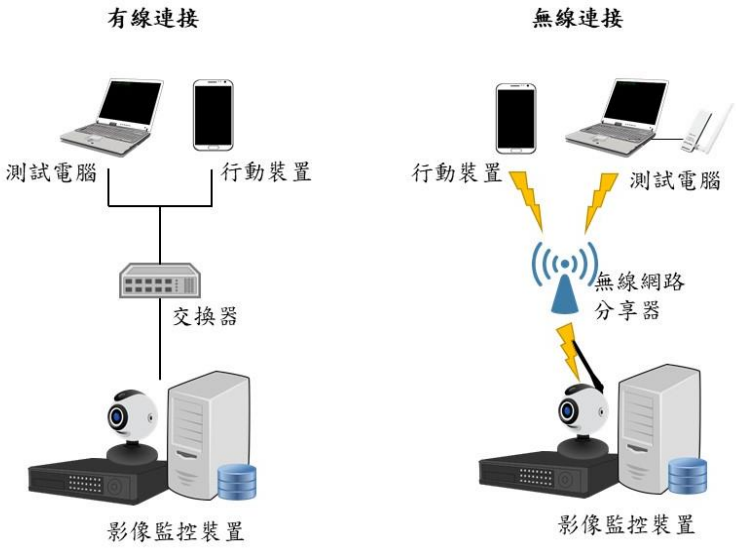

圖 31 測試示意圖

(e) 測試步驟：

(1) 分別將測試電腦及行動裝置連接產品。

(2) 依產品使用說明，開啟相對應之管理介面連接工具以執行身分鑑別。

(3) 輸入已存在之使用者帳戶搭配錯誤的通行碼，檢視鑑別錯誤訊息。

(4) 輸入不存在之使用者帳戶，檢視鑑別錯誤訊息。

(f) 測試結果：

(1) 通過：身分鑑別錯誤訊息無法推斷出合法使用者帳戶或通行碼。

(2) 不通過：身分鑑別錯誤訊息洩露出合法使用者帳戶或通行碼。

(3) 不適用：產品不支援身分鑑別機制。

5.4.1.3 憑證更換功能測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.1.3。

(b) 測試目的：

查驗產品具備憑證更換之功能。

(c) 前置條件：

(1) 產品不存在憑證鑑別之功能，則此測項不適用。

(2) 應提供產品憑證更換之操作說明。

(d) 測試布局：

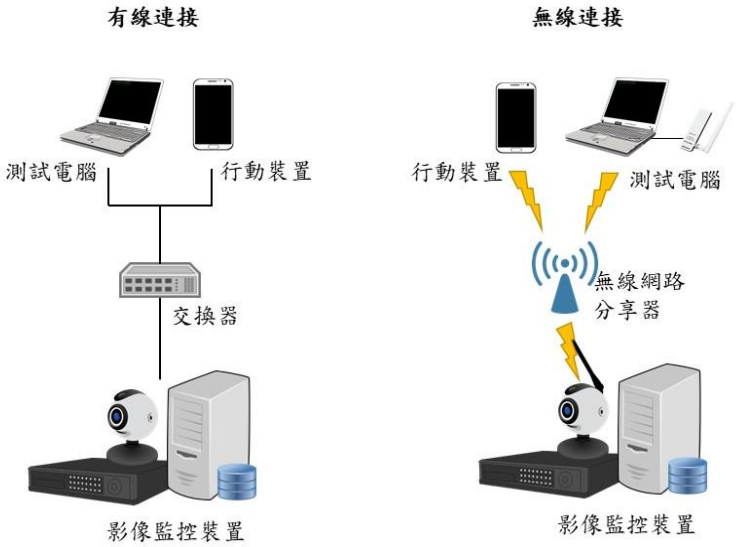

圖 32 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 依產品使用說明，開啟相對應之管理介面連接工具以執行憑證上傳。

(3) 重新連接產品之網頁介面，檢視憑證是否成功更換。

(f) 測試結果：

(1) 通過：憑證成功更換。

(2) 不通過：憑證未成功更換。

(3) 不適用：產品不存在憑證鑑別之功能。

5.4.1.4 金鑰唯一性測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.1.4。

(b) 測試目的：

查驗產品之金鑰係唯一。

(c) 前置條件：

無。

(d) 測試布局：

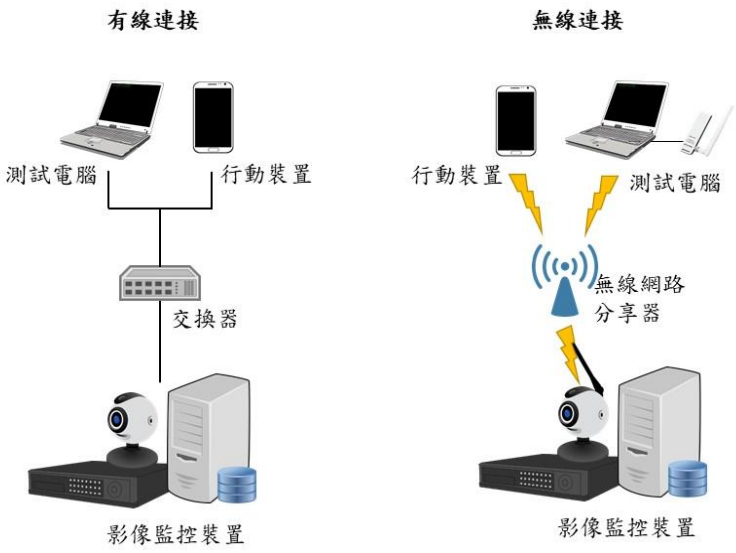

圖 33 測試示意圖

(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，開啟相對應之管理介面連接工具以執行鑑別。

(3) 側錄封包並擷取產品之憑證，檢視其憑證指紋碼(fingerprint)。

(4) 重置產品至出廠預設組態。

(5) 重複步驟 1～3。

(f) 測試結果：

(1) 若測試裝置透過圖形化管理介面連接產品，重置出廠預設組態前後，憑證指紋碼是相異的。

(2) 若測試裝置透過安全外殼協定(SSH)連接產品，重置出廠預設組態前後，憑證指紋碼是相異的。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)(2)項結果不符合其一。

(5) 不適用：無。

5.4.1.5 多因子鑑別機制測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.1.5。

(b) 測試目的：

查驗產品之支援多因子鑑別之強身分鑑別機制。

(c) 前置條件：

(1) 產品之使用者帳戶及相關鑑別因子(例：通行碼)已建立，且多因子鑑別功能已啟用。

(2) 應提供具多因子鑑別操作之說明文件。

(d) 測試布局：

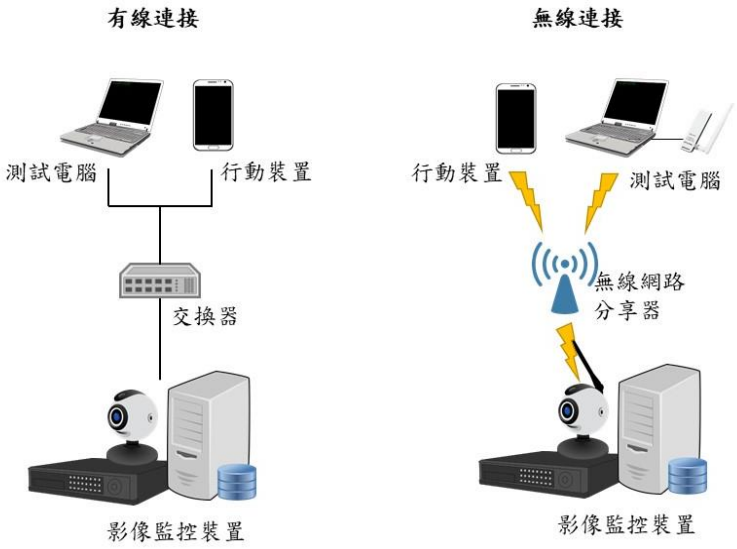

圖 34 測試示意圖

(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，開啟相對應之管理介面連接工具以執行鑑別。

(3) 執行多因子鑑別操作，查驗每次的鑑別均採用不同種類之鑑別因子。

(4) 查驗鑑別過程中未採用簡訊服務(short message service, SMS)獲取驗證碼。

(5) 查驗鑑別過程中，使用行動裝置作為所持物(something you have)之鑑別因子時，查驗僅可在 1 台行動裝置上獲取鑑別因子。

(f) 測試結果：

(1) 網頁管理介面與產品之間的鑑別，透過多因子鑑別。

(2) 每一階段鑑別皆採用不同鑑別因子。

(3) 當使用鑑別因子時，未採用簡訊服務獲取驗證碼。

(4) 當行動裝置作為所持物之鑑別因子時，僅可在 1 台行動裝置上獲取鑑別因子。

(5) 通過：(1)~(4)項結果皆符合。

(6) 不通過：(1)~(4)項結果不符合其一。

(7) 不適用：無。

5.4.1.6 裝置鑑別測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.1.6。

(b) 測試目的：

查驗產品可鑑別相連之影像監控系統裝置身分，且其裝置鑑別機制具備抵抗重送攻擊的能力。

(c) 前置條件：

應提供可與產品相連之影像監控裝置。

(d) 測試布局：

圖 35 測試示意圖

(e) 測試步驟：

(1) 將產品與其他影像監控裝置建立連線。

(2) 將測試電腦或行動裝置連接其他影像監控裝置。

(3) 查驗對相連裝置之鑑別。

(4) 執行鑑別操作，同時側錄封包。

(5) 將側錄到的鑑別封包，於另一次鑑別操作時，重送至產品。

(6) 檢視鑑別結果。

(f) 測試結果：

(1) 通過：其他影像監控裝置與產品建立連線時，產品會鑑別其他影像監控裝置之身分，且該機制能抵抗重送攻擊。

(2) 不通過：其他影像監控裝置與產品建立連線時，產品無鑑別其他影像監控裝置之身分。

(3) 不適用：無。

5.4.2 通行碼鑑別安全測試

5.4.2.1 預設通行碼安全

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.2.1。

(b) 測試目的：

查驗產品沒有相同的預設通行碼或預設通行碼會於首次上線後強制要求更改。

(c) 前置條件：

(1) 產品未支援通行碼鑑別機制，則不適用此測項。

(2) 產品應保持出廠預設組態。

(3) 若產品存在預設通行碼，應提供產品預設通行碼之設計文件。

(d) 測試布局：

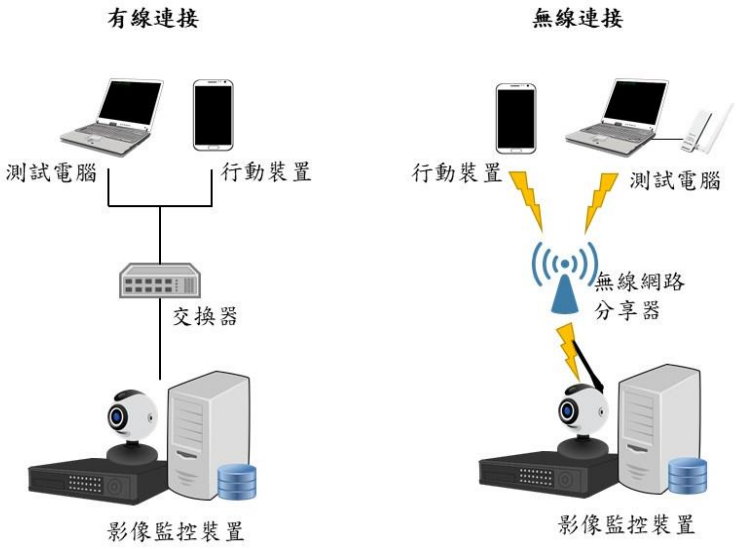

圖 36 測試示意圖

(e) 測試步驟：

(1) 審閱產品之預設通行碼設計文件，檢視產品是否存在相同之預設通行碼。

(2) 將測試電腦或行動裝置連接產品。

(3) 從網頁管理介面或操控程式輸入通行碼。

(4) 確認在未設定新通行碼的情況下，不可存取產品。

(f) 測試結果：

(1) 產品之預設通行碼為全球唯一。

(2) 未經設定新通行碼前無法存取。

(3) 通過：(1)(2)項任一結果符合。

(4) 不通過：(1)(2)項皆不符合。

(5) 不適用：產品未支援通行碼鑑別機制。

5.4.2.2 通行碼長度

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.2.2。

(b) 測試目的：

查驗產品之最小通行碼長度是否足夠。

(c) 前置條件：

產品未支援通行碼鑑別機制，則不適用此測項。

(d) 測試布局：

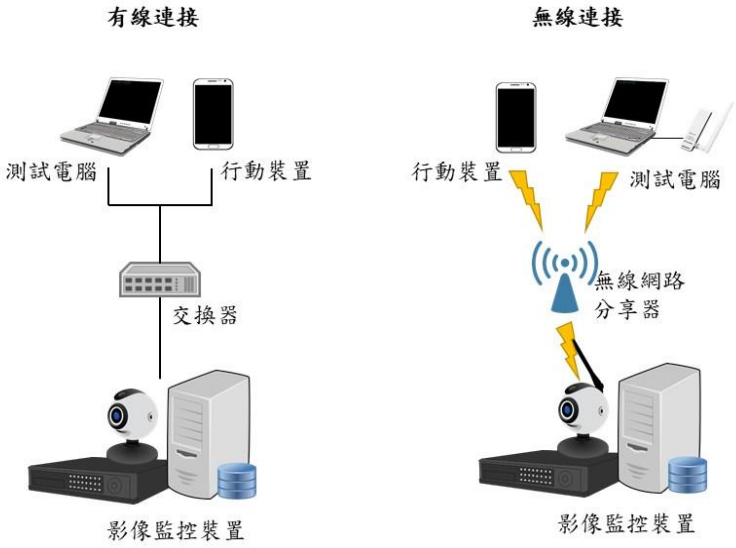

圖 37 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 從網頁管理介面或操控程式，建立或變更通行碼。

(3) 輸入小於 8 個字元長度之通行碼，檢查通行碼未能成功建立或變更，或產品發出通行碼強度不足警示。

(4) 若產品採用的通行碼強度原則是國際標準要求或公認之資安產業慣例之規格，檢視其來源與安全強度是否足夠信任。

(f) 測試結果：

(1) 無法建立或變更小於 8 個字元長度之通行碼或產品發出通行碼強度不足警示。

(2) 採用之通行碼強度原則出自國際標準或符合公認資安產業慣例。

(3) 通過：(1)(2)項任一結果符合。

(4) 不通過：(1)(2)項結果皆不符合。

(5) 不適用：產品未支援通行碼鑑別機制。

5.4.2.3 通行碼複雜度

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.2.3。

(b) 測試目的：

查驗產品之通行碼複雜度是否足夠。

(c) 前置條件：

產品未支援通行碼鑑別機制，則不適用此測項。

(d) 測試布局：

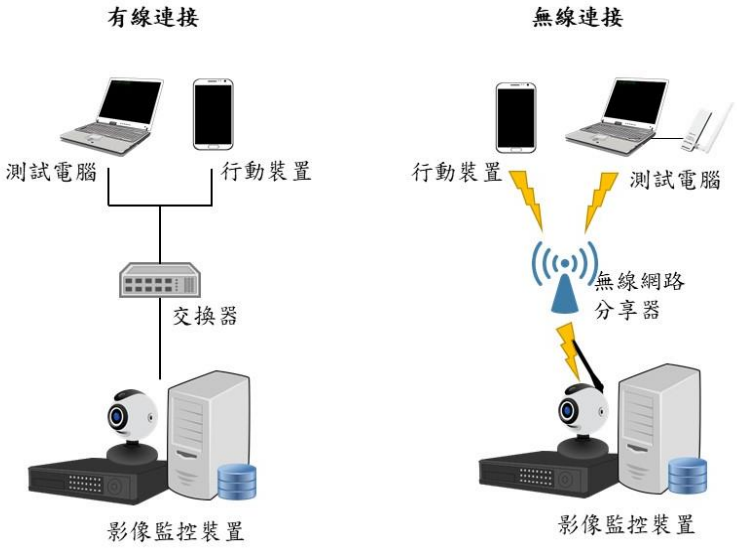

圖 38 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 從網頁管理介面或操控程式，建立或變更通行碼。

(3) 輸入僅同時含下述 4 種字元中的 1 種或 2 種，檢查通行碼無法成功建立或變更：

(i) 英文大寫字元(A 至 Z)。

(ii) 英文小寫字元(a 至 z)。

(iii) 10 進位數字(0 至 9)。

(iv) 非英文字母字元(例：!、$、#、%)。

(4) 若產品採用的通行碼強度原則是國際標準要求或公認之資安產業慣例之規格，檢視其來源與安全強度是否足夠信任。

(f) 測試結果：

(1) 依測試步驟(3)執行，無法建立或變更通行碼，或產品發出通行碼強度不足警示。

(2) 採用之通行碼強度原則出自國際標準或符合公認資安產業慣例。

(3) 通過：(1)(2)項任一結果符合。

(4) 不通過：(1)(2)項結果皆不符合。

(5) 不適用：產品未支援通行碼鑑別機制。

5.4.2.4 通行碼的輸入頻率及次數限制

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.2.4。

(b) 測試目的：

查驗產品之通行碼鑑別機制具防止暴力破解之能力。

(c) 前置條件：

(1) 產品未支援通行碼鑑別機制，則不適用此測項。

(2) 產品之使用者帳戶及相關鑑別因子(例：通行碼)已建立。

(3) 應提供產品之帳戶鎖定機制之設計說明。

(d) 測試布局：

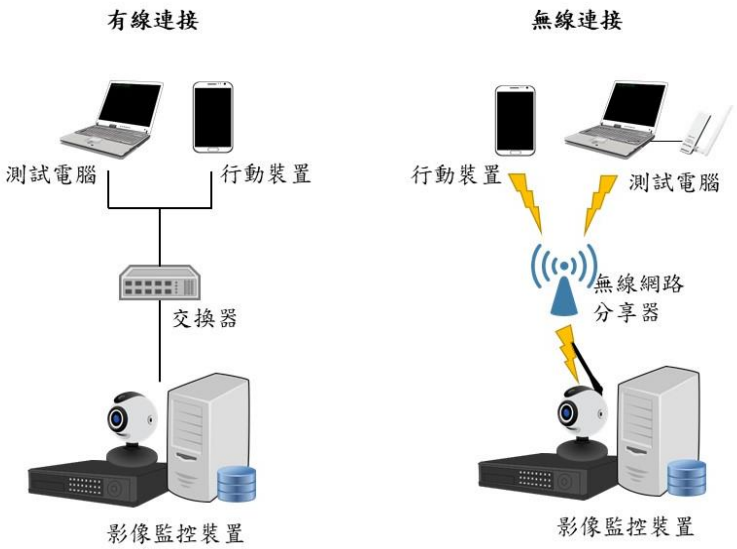

圖 39 測試示意圖

(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，開啟相對應之管理介面連接工具以執行鑑別。

(3) 不斷輸入錯誤且相異的通行碼。

(4) 檢視產品於帳戶或 IP 鎖住計數器重設為 0 前，廠商宣告計數器重設時限內連續登入不成功次數 5 次以內，會鎖住帳戶或 IP。

(5) 鎖住帳戶或 IP 後，於鎖住期間內持續輸入相異且錯誤的通行碼，比對廠商宣告帳戶或 IP 鎖住時限內，檢視帳戶或 IP 是否解鎖。

(6) 同一帳戶或 IP 任一次登入不成功後，於廠商宣告計數器重設時限內，重新輸入錯誤且相異的通行碼，檢視輸入不成功次數是否重新計算。

(7) 若產品採用的通行碼強度原則是國際標準要求或公認之資安產業慣例之規格，檢視其來源與安全強度是否足夠信任。

(f) 測試結果：

(1) 輸入次數 5 次以內，會鎖住帳戶或 IP。

(2) 於廠商宣告之帳戶或 IP 鎖住時限內，帳戶或 IP 未解鎖。

(3) 於廠商宣告計數器重設時限內，不成功次數未重新計算。

(4) 產品採用鎖住 IP 來防止暴力破解，則產品同時應具備可限制被連結 IP 之功能。

(5) 採用之通行碼強度原則出自國際標準或符合公認資安產業慣例。

(6) 通過：(1)~(4)項皆符合，或(5)項符合。

(7) 不通過：不滿足(6)的測試結果。

(8) 不適用：產品未支援通行碼鑑別機制。

5.4.2.5 通行碼連續字元之避免

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.2.5。

(b) 測試目的：

查驗產品之通行碼不含使用者的帳戶名稱中 3 個以上的連續字元。

(c) 前置條件：

產品未支援通行碼鑑別機制，則不適用此測項。

(d) 測試布局：

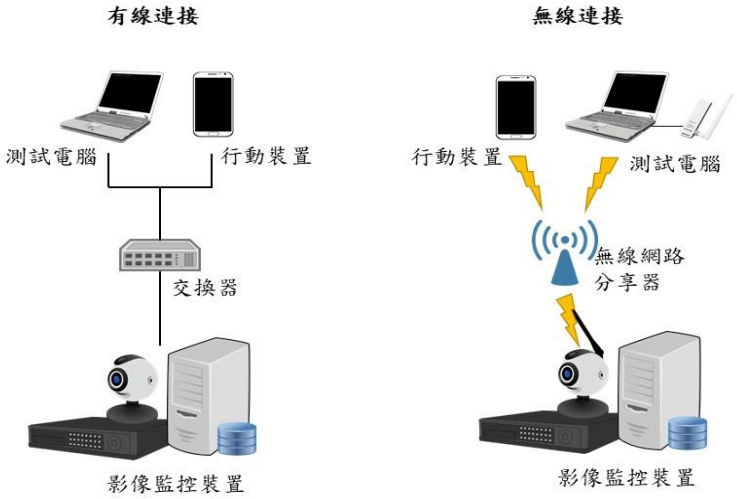

圖 40 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 從網頁管理介面或操控程式，建立或變更通行碼。

(3) 輸入含使用者之帳戶名稱中 3 個以上的連續字元，查驗通行碼能否成功建立或變更。

(4) 若產品採用的通行碼強度原則是國際標準要求或公認之資安產業慣例之規格，檢視其來源與安全強度是否足夠信任。

(f) 測試結果：

(1) 無法建立或變更通行碼。

(2) 採用之通行碼強度原則出自國際標準或符合公認資安產業慣例。

(3) 通過：(1)(2)項任一結果符合。

(4) 不通過：(1)(2)項結果皆不符合。

(5) 不適用：產品未支援通行碼鑑別機制。

5.4.2.6 通行碼歷程記錄

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.2.6。

(b) 測試目的：

查驗產品具備通行碼歷程記錄功能，以確保其強度。

(c) 前置條件：

產品未支援通行碼鑑別機制，則不適用此測項。

(d) 測試布局：

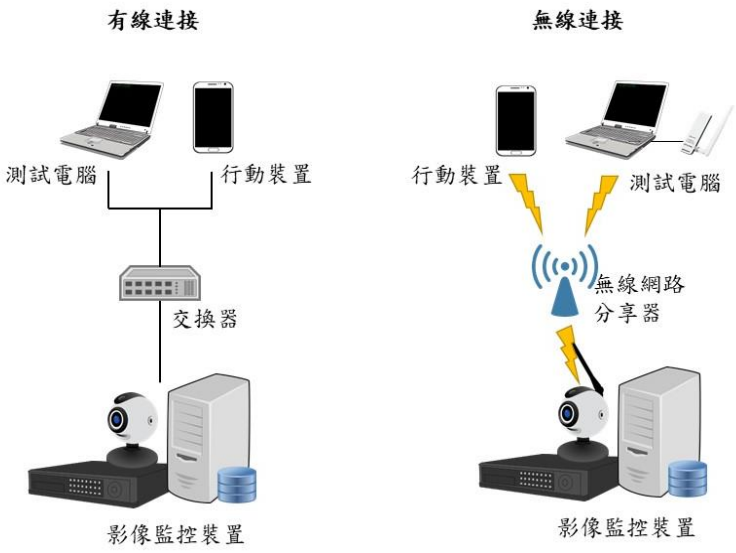

圖 41 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 從網頁管理介面或操控程式，變更通行碼。

(3) 輸入產品曾經使用過之最近三組通行碼。

(4) 若產品採用的通行碼強度原則是國際標準要求或公認之資安產業慣例之規格，檢視其來源與安全強度是否足夠信任。

(f) 測試結果：

(1) 無法變更通行碼。

(2) 採用之通行碼強度原則出自國際標準或符合公認資安產業慣例。

(3) 通過：(1)(2)項任一結果符合。

(4) 不通過：(1)(2)項結果皆不符合。

(5) 不適用：產品未支援通行碼鑑別機制。

5.4.3 權限管控測試

5.4.3.1 權限管控機制

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.3.1。

(b) 測試目的：

查驗產品之資源存取具有權限管控機制。

(c) 前置條件：

(1) 產品之使用者帳戶及相關鑑別因子(例：通行碼)已建立，並存在系統管理者及一般使用者二類帳戶。

(2) 應提供產品之角色存取權限宣告。

(d) 測試布局：

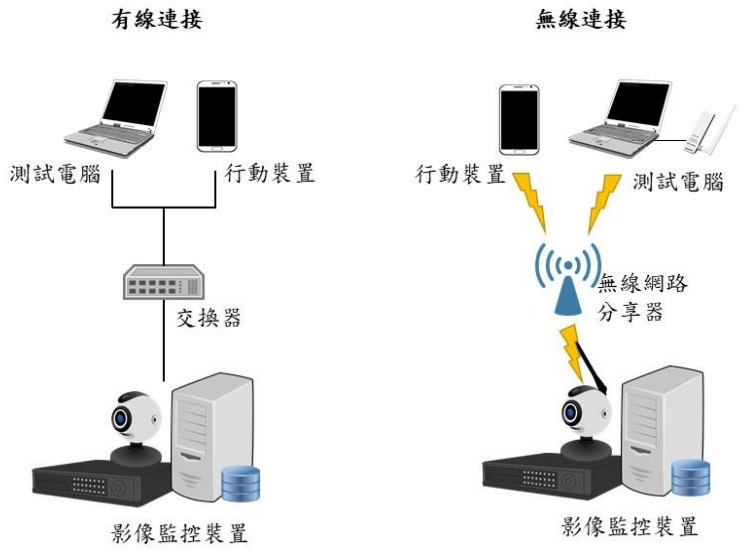

圖 42 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 從網頁管理介面，分別以不同角色登入產品。

(3) 存取產品資源，同時檢視該帳戶之角色與其對應之權限與產品自我宣告相符。

(4) 若為網頁管理介面，則嘗試以同一頁面讓不同權限的角色存取。

(f) 測試結果：

(1) 使用者的身分授權與產品之自我宣告相符。

(2) 至少有 2 個以上不同權限的角色，若此功能會對營運產生不利影響，產品之宣告應提出相關之說明，則產品可具備單一權限角色即可。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)(2)項結果任一不符合。

(5) 不適用：無。

5.4.3.2 權限有效時間

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.4.3.2。

(b) 測試目的：

查驗產品存在有限的授權期限。

(c) 前置條件：

(1) 產品之使用者帳戶及相關鑑別因子(例：通行碼)已建立。

(2) 產品之使用情境必須為常時間使用不間斷(例：大樓監視器)，則廠商應於文件中聲明，並在使用指南或安全指引中註明建議補償做法。

(d) 測試布局：

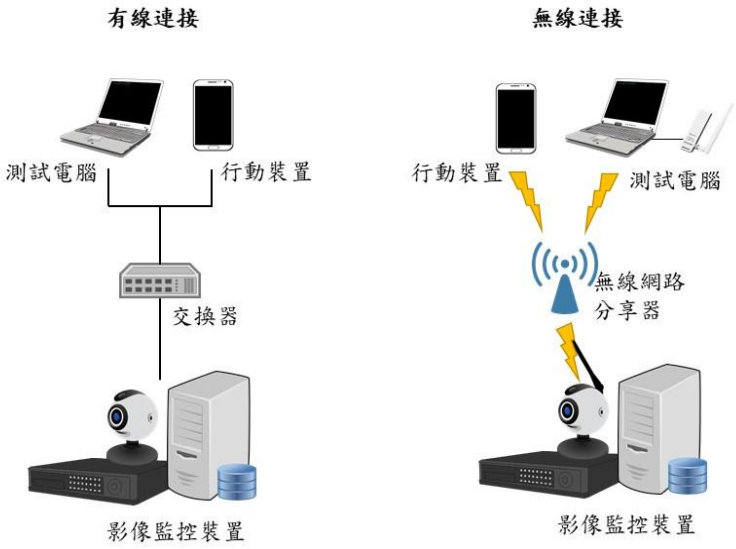

圖 43 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 檢視產品之網頁管理介面，存在供使用者設定的閒置時限操作介面。

(3) 閒置產品直到超過閒置時限值。

(4) 檢視需重新鑑別方可存取產品。

(f) 測試結果：

(1) 產品之授權行為，存在閒置時限供使用者設定。

(2) 遠端連線閒置逾時，應經過鑑別方可存取產品。

(3) 產品之使用情境必須為常時間使用不間斷，則廠商於產品使用指南或安全指引中，聲明建議安全的補償做法。

(4) 通過 1：(1)(2)項結果皆符合。

(5) 通過 2：(3)項結果符合。

(6) 不通過：「通過 1」及「通過 2」皆不符合。

(7) 不適用：無。

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-1001-1 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，隱私資料泛指從影像監控裝置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 隱私資料的存取控制測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.5.1.1。

(b) 測試目的：

查驗產品之隱私權具有存取控制機制。

(c) 前置條件：

(1) 應提供產品之隱私存取權限宣告。

(2) 產品應能建立 2 個以上的帳戶，否則此測試項不適用。

(d) 測試布局：

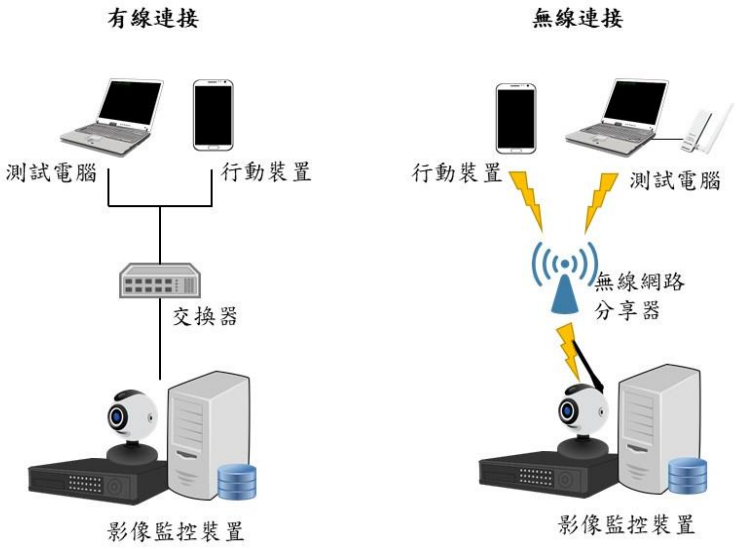

圖 44 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 從網頁管理介面，分別以不同角色登入產品。

(3) 存取影像資料，同時檢視該帳戶之角色與其對應之隱私存取權限與廠商宣告相符。

(4) 當產品提供網頁管理介面且已經有帳戶登入的情況下，檢視無需透過帳戶切換，即可存取該帳戶權限之外的隱私資料。

(f) 測試結果：

(1) 通過：使用者的隱私存取授權與廠商宣告相符。

(2) 不通過：使用者的隱私存取授權與廠商宣告不符。

(3) 不適用：無。

5.5.1.2 隱私外洩警示功能測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.5.1.2。

(b) 測試目的：

查驗產品具有防止隱私外洩之功能。

(c) 前置條件：

(1) 應提供產品之隱私外洩警示功能說明。

(2) 若登入警示應搭配後台伺服器運行，則應提供可對接之後台伺服器進行測試。

(3) 若登入警示應搭配後台伺服器運行，則應提供使用說明或資安指引供審。

(d) 測試布局：

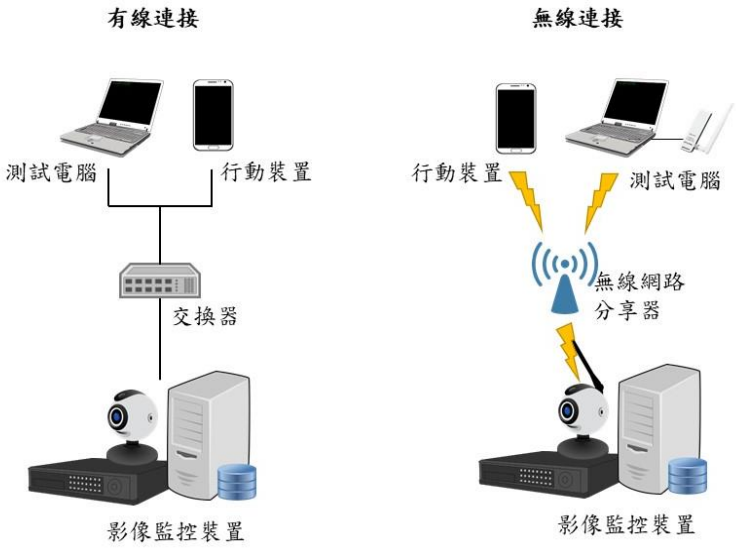

圖 45 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 透過網頁管理介面或操控程式，以不同角色登入產品。

(3) 存取影像資料。

(4) 確認系統管理者或已登入使用者是否接收到警示。

(5) 若產品之發入警示由後台伺服器執行，則側錄送往後台之發入警示相關之封包。

(6) 若產品之發入警示由後台伺服器執行，則審閱使用說明或資安指引之相關登入警示聲明。

(f) 測試結果：

(1) 每次發生新的使用者登入或登入以存取影像事件時，產品發出警示。

(2) 若產品之發入警示由後台伺服器執行，則應於使用說明書或資安指引中聲明此情境，且該文件公告在廠商官網上。

(3) 通過：(1)(2)項任一符合。

(4) 不通過：(1)(2)項皆不符合。

(5) 不適用：無。

5.5.2 隱私資料的傳輸保護測試

5.5.2.1 隱私資料之傳輸保護初階測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.5.2.1。

(b) 測試目的：

查驗產品影像資料之傳輸，預設採用強度足夠之安全通道。

(c) 前置條件：

產品應保持出廠預設組態。

(d) 測試布局：

圖 46 測試示意圖

(e) 測試步驟：

(1) 掃描產品使用之安全通道。

(2) 比對掃描結果是否為附錄 A 中所包含之密碼套件。

(3) 將測試電腦及行動裝置連接產品。

(4) 於相應之管理介面啟動影像監控功能，同時側錄封包。

(5) 檢視所側錄之封包是否採用安全通道傳輸。

(f) 測試結果：

(1) 安全通道僅採用附錄 A 中所建議之密碼套件。

(2) 與測試電腦之間的影像資料傳輸，預設採用安全通道。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)(2)項結果不符合其一。

(5) 不適用：無。

5.5.2.2 隱私資料之傳輸保護中階測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.5.2.2。

(b) 測試目的：

確認產品具備查驗此安全通道憑證有效性及真確性之能力。

(c) 前置條件：

(1) 應提供可與產品相連之影像監控裝置。

(2) 若與產品相連之影像監控裝置採用自簽發憑證，則應提供可匯入根憑證或中繼憑證(immediate certificate)之介面。

(d) 測試布局：

圖 47 測試示意圖

(e) 測試步驟：

(1) 載入可驗證對連影像監控裝置之根憑證或中繼憑證(immediate certificate)至產品中。

(2) 將產品與其他影像監控裝置連接，並啟動安全通道之建立程序。

(3) 當其他影像監控裝置發送憑證予產品時，攔截其憑證，並置換憑證公鑰及憑證資訊(包括發證單位、有效期限、格式及憑證簽章)。

(4) 發送已竄改之憑證予產品，於安全通道建立的交握過程中側錄封包，檢視產品是否接受此憑證。

(f) 測試結果：

(1) 通過：已竄改影像資料傳輸用之安全通道憑證未通過產品鑑別。

(2) 不通過：已竄改影像資料傳輸用之安全通道憑證通過產品鑑別。

(3) 不適用：無。

5.5.2.3 隱私資料之傳輸保護高階測試

(a) 測試依據：

「IoT-1001-1 影像監控系統資安標準-第一部：一般要求」之 5.5.2.3。

(b) 測試目的：

查驗產品之影像資料傳輸，支援強加密演算法。

(c) 前置條件：

產品應具備安全通道功能。

(d) 測試布局：

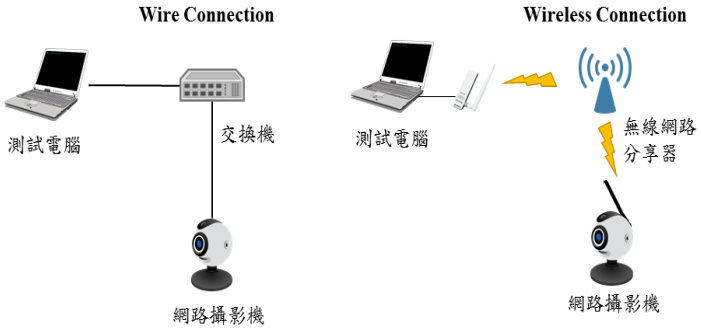

圖 48 測試示意圖

(e) 測試步驟：

(1) 將測試電腦及行動裝置連接產品。

(2) 掃描產品使用之安全通道。

(3) 比對掃描結果是否為附錄 A 中所包含之密碼套件，且支援 AES-256 同等或以上加密強度的演算法。

(f) 測試結果：

(1) 通過：該安全通道支援 AES-256 同等或以上加密強度的演算法。

(2) 不通過：該安全通道不支援 AES-256 同等或以上加密強度的演算法。

(3) 不適用：產品不具備安全通道功能。

附錄 A
(規定)
安全通道應使用之密碼套件

安全通道(TLS)所選用的密碼套件應遵循下述幾項要求：

- TLSv1.2
  - TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
  - TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES256_SHA384
  - TLS_ECDHE_RSA_WITH_AES256_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES128_SHA256
  - TLS_ECDHE_RSA_WITH_AES128_SHA256
- TLSv1.3
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_SHA256
  - TLS_AES_128_CCM_8_SHA256

附錄 B
(規定)
影像監控裝置所使用之通訊協定

(a) 即時傳輸協定 (Real-time Transport Protocol, RTP) & 即時傳送控制協定 (Real-time Transport Control Protocol, RTCP)：

定義在 RFC 3550 規範中(5)，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，而 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)。

(b) B.2 即時串流協定 (Real Time Streaming Protocol, RTSP)：

定義在 RFC 2326 規範中(6)，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) B.3 傳輸層安全協定 (The Transport Layer Security, TLS)：

定義在 RFC 5246 規範中(7)，在兩個應用程式之間透過網路建立起安全通道，於交換資料時可防止遭受到竊聽及篡改。

附錄 C
(規定)
產品概述說明(範例)

送測之產品應提供下表供測試實驗室參閱：

表 C.1 設備概述表

製造商	xxx
設備名稱	xxx
廠牌	xxx
型號	xxx
軟、韌體版本	xxx
通訊介面	Wi-Fi,
網路服務(埠號)	https (443)
相連伺服器(IP)	SAMBA (8.8.8.x)
ONVIF API 權限	RemoveIPAddressFilter: Administrator
日誌存取權限	USER A: 唯讀
日誌檔保存期限	90 天
角色存取權限	Administrator: 可執行網頁管理介面任何服務

隱私權存取權限	Administrator: 所有使用者影像
外觀	<picture>

附錄 D
(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 D.1 安全功能規格表

項目	說明	申請者填寫內容
1. **除錯模式**	一步步描述進入作業系統除錯模式的方法，或提供佐證文件。 *範例：* *1. 登入管理介面。* *2. 點選「設定」。* *3. 點選「SSH」。* *4. ...。*	
2. 加密演算法	列出產品所提供之加密演算法及其應用。 *範例：* *遠端加密連線： RSA-2048* *加密儲存 https 金鑰： AES-128*	
3. 數位簽章演算法	列出產品所使用之數位簽章演算法。 *範例：* *安全啟動：RSA* *韌體簽章：DSS*	
4. **日誌功能可用**	描述當日誌檔空間不足時，日誌檔的處理機制及警示方法，或提	

性警示機制	供佐證文件。 *範例：* *當日誌檔空間不足時...。*	
5. **金鑰管理程序**	列出各金鑰管理階段所應執行的程序，或提供佐證文件。 備註： 產品要驗 2 級安全時，應提供。 *範例：* *1. 生成： ...。* *2. 交換： ...。* *3. 儲存： ...。* *4. 使用： ...。* *5. 銷毀： ...。* *6. 更替： ...。*	
6. 憑證上傳	一步步說明要如何自行增加產品之安全通道憑證，或提供佐證文件。 備註： 產品要驗 2 級安全時，應提供。 *範例：* *1. 登入管理介面。* *2. 點選「設定」。* *3. ...。*	
7. 多因子鑑別機制	一步步說明要如何執行多因子鑑別機制，或提供佐證文件。 備註： 產品要驗 3 級安全時，應提供。 *範例：*	

	1. 登入管理介面。 *2. 點選「設定」。* *3. …。*	
8. 安全區域	說明產品使用的安全區域種類、廠牌、型號、使用方式及其保護之資料，並提供佐證文件。 備註： 產品要驗 3 級安全時，應提供。 *範例：* *種類： HSM* *廠牌： xxx* *型號： xxx* *使用方式： 當要建立安全通道時，傳送請求封包至 HSM…。* *資安功能： 登入通行碼、https 金鑰、安全啟動金鑰。*	
9. 帳戶鎖定機制	說明產品在通行碼輸入錯誤時，相關之帳戶鎖定機制。 *範例：* *失敗達 5 次，鎖定帳戶。* *鎖定 1 分鐘後，方解除鎖定。* *遭鎖定後 2 分鐘，重設鎖定計數器。*	

參考資料

(1) IoT-1001-1 v2.0: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 SP 800-140C, CMVP Approved Security Functions, March 2020.

(3) Open Web Application Security Project (OWASP) org., OWASP Top 10 – 2017 [viewed 2018-05-16]. Available at https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

(4) 國家通訊傳播委員會, 無線網路攝影機資通安全檢測技術指引, 2018.

(5) RFC 3550, RTP: A Transport Protocol for Real-Time Applications.

(6) RFC 2326, Real Time Streaming Protocol (RTSP).

(7) RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2.