TAICS

TAICS TS-0015-1 v1.0:2018

影像監控系統資安標準測試規範
－第一部：一般要求

Video Surveillance System Security Test Specification
- Part 1: General Requirement

2018/06/08

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

影像監控系統資安標準測試規範

-第一部：一般要求

Video Surveillance System Security Test Specification - Part 1: General Requirements

出版日期: 2018/06/08
終審日期: 2018/05/30

誌謝

本規範由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC 主席：安華聯網科技股份有限公司 洪光鈞 總經理

TC 副主席：資訊工業策進會 蔡正煜 組長

TC 物聯網資安工作組組長：資訊工業策進會 高傳凱 博士

此規範制定之協會會員參與名單為(以中文名稱順序排列)：

行政法人國家中山科學研究院、財團法人工業技術研究院、財團法人台灣電子檢驗中心、財團法人資訊工業策進會、財團法人電信技術中心、中華電信股份有限公司、友訊科技股份有限公司、安華聯網科技股份有限公司、宏達國際電子股份有限公司、果核數位股份有限公司、國立中央大學、晶復科技股份有限公司、群暉科技股份有限公司、趨勢科技股份有限公司、行動檢測服務股份有限公司、互聯安睿資通股份有限公司。

本規範由國家通訊傳播委員會及經濟部工業局支持研究制定。

目錄

前言

本規範係依台灣資通產業標準協會(TAICS)之規定，經技術管理委員會審定，由協會公布之產業標準。

本規範並未建議所有安全事項，使用本規範前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本規範之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

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。

「TAICS TS0015-1 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)，依據台灣資通產業標準協會所制定之「TAICS TS-0014-1 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**

3. 用語及定義

「TAICS TS-0014-1 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「TAICS TS-0014-1 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	5.1.1.1	-	-
	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	-	5.2.1.2
	5.2.2. 網路服務連接埠管控測試	5.2.2.1	-	-
	5.2.3. 更新安全測試	5.2.3.1 5.2.3.2 5.2.3.3	-	-
	5.2.4. 敏感性資料儲存安全測試	5.2.4.1(a) 5.2.4.2(a)	5.2.4.1(b) 5.2.4.2(b) 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. 日誌檔與警示測試	5.2.7.1 5.2.7.2 5.2.7.3	5.2.7.4	-
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
	5.3.2. 通訊協定與設置安全	5.3.2.1 5.3.2.2	5.3.2.3	-
	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
	5.4.1. 鑑別機制安全測試	5.4.1.1	5.4.1.3	5.4.1.5

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
身分鑑別與授權機制安全		5.4.1.2	5.4.1.4	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 5.5.1.3	-	-
	5.5.2. 隱私資料的傳輸保護測試	5.5.2.1	-	5.5.2.2

5. 資安測試規範

5.1 實體安全測試

檢視影像監控裝置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 實體介面安全管控測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證是否可透過產品實體介面，存取作業系統之除錯模式。

(c) 樣品條件：

(1) 產品須保持出廠預設環境狀態。

(2) 產品須於文件中說明進入作業系統除錯模式之方法。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 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。

(2) 測試電腦連接產品之 USB 埠。

(3) 確認可否透過 USB 埠存取作業系統之除錯模式。

(4) 若存取前須經通行碼鑑別程序，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。

(5) 測試電腦連接產品之 UART 埠。

(6) 確認可否透過 UART 埠存取作業系統之除錯模式。

(7) 若存取前須經通行碼鑑別程序，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) 預期結果：

(1) 透過 USB 存取作業系統之除錯模式時，產品要求身分鑑別。

(2) 透過 USB 存取作業系統之除錯模式時，若要求通行碼鑑別，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。

(3) 透過 UART 存取作業系統之除錯模式時，產品要求身分鑑別。

(4) 透過 UART 存取作業系統之除錯模式時，若要求通行碼鑑別，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。

(5) 產品若不存在進入作業系統除錯模式之介面，則此測項為「通過」。

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：

「TAICS TS-0014-1 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：

驗證產品之實體埠是否有插拔紀錄。

(c) 樣品條件：

無。

(d) 測試佈局：

無。

(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) 插拔 USB 埠，檢視插拔紀錄。

(4) 插拔 RJ45 埠，檢視插拔紀錄。

(f) 預期結果：

(1) 產品具有 USB 埠插拔記錄。

(2) 產品具有 RJ45 埠插拔記錄功能。

(3) 該實體埠插拔記錄之時間正確。

5.1.2.2 實體異常狀態警示機制

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品之網路服務遭受實體層阻絕時，是否有相應之警示機制。

(c) 樣品條件：

無。

(d) 測試佈局：

見圖 2。

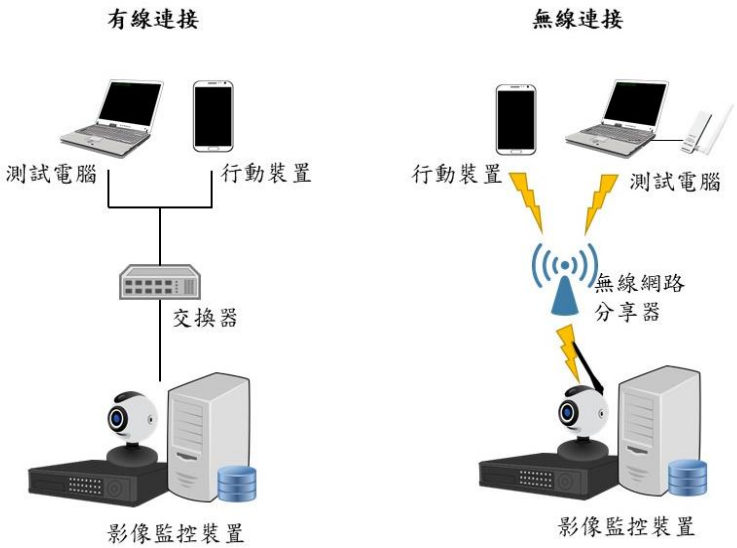

圖 2 測試示意圖

(e) 測試方法：

(1) 根據產品使用說明。

(2) 將網路線拔除或天線遮罩，使主機因訊號中斷而無法連接上網路。

(3) 檢視產品是否依照使用說明達到警示效果。

(f) 預期結果：

(1) 發生斷訊狀況時，產品發出警示。

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：

「TAICS TS-0014-1 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：

驗證產品實體層的預設通行碼還原設計，是否考量安全防護機制。

(c) 樣品條件：

無。

(d) 測試佈局：

無。

(e) 測試方法：

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

(f) 預期結果：

(1) 產品外觀不存在徒手即可輕易還原回預設通行碼的設計。

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：

「TAICS TS-0014-1 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) 樣品條件：

產品須提供安全啟動功能之設計文件。

(d) 測試佈局：

無。

(e) 測試方法：

(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) 預期結果：

(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。

5.2 系統安全測試

檢視影像監控裝置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 測試作業系統是否存在 CVSS v3 評分為 9.0 分以上之常見資安弱點與漏洞

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品之作業系統與網路服務是否存在已知 CVSS v3 重大資安風險之漏洞。

(c) 樣品條件：

產品須保持出廠預設環境狀態。

(d) 測試佈局：

系統安全測試架構，如圖 3 所示，可採用有線或無線連線方式與產品建立鏈結，包括測試電腦(供測試人員連線至影像監控裝置之終端設備)、有線連線(乙太網路線或光纖纜線)、無線連線與受測之影像監控裝置，用以測試受測裝置是否符合測試規範。

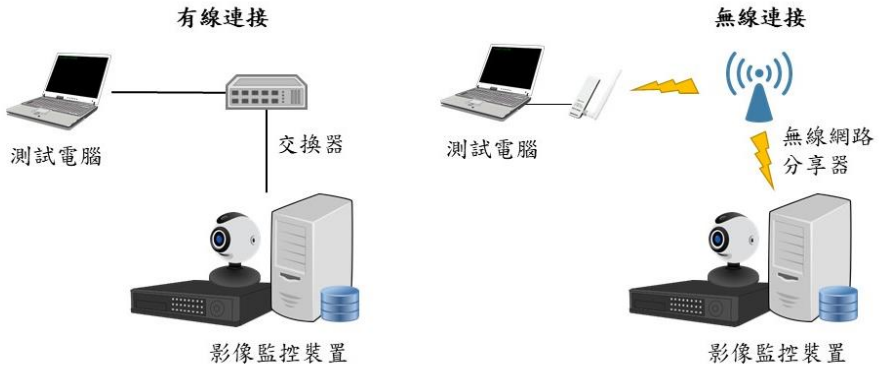

圖 3 測試示意圖

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 啟動具作業系統及網路服務弱點掃描功能之工具，對產品執行弱點掃描。

(3) 目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 評分為 9.0 分以上之資安漏洞。

(f) 預期結果：

(1) 作業系統與網路服務不存在國家弱點資料庫評分 CVSS v3 為 9.0 分以上之資安漏洞。

(2) 當檢測出之資安漏洞不具有 CVSS v3 評分時，以 CVSS v2 評分為依據。

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

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品之作業系統與網路服務是否存在已知 CVSS v3 高資安風險之漏洞。

(c) 樣品條件：

產品須保持出廠預設環境狀態。

(d) 測試佈局：

見圖 4。

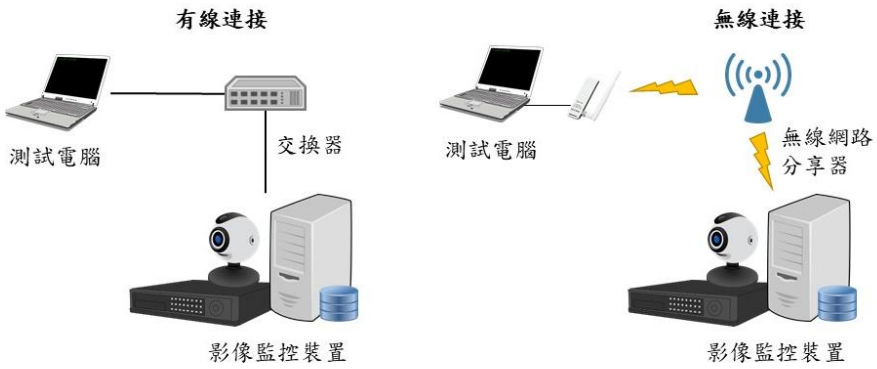

圖 4 測試示意圖

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 啟動具作業系統及網路服務弱點掃描功能之工具，對產品執行弱點掃描。

(3) 目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 評分為 7.0 分以上之資安漏洞。

(f) 預期結果：

(1) 作業系統與網路服務不存在國家弱點資料庫評分 CVSS v3 為 7.0 分以上之資安漏洞。

(2) 當檢測出之資安漏洞不具有 CVSS v3 評分時，以 CVSS v2 評分為依據。

5.2.2 網路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：

「TAICS TS-0014-1 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：

驗證產品是否存在預期以外之網路埠。

(c) 樣品條件：

(1) 產品須保持出廠預設環境狀態。

(2) 產品須提供所啟用之網路服務與對應埠之宣告。

(d) 測試佈局：

參照圖 5。

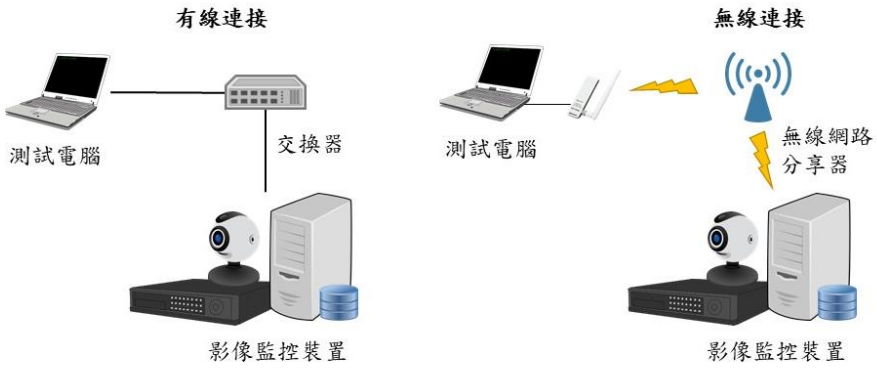

圖 5 測試示意圖

(e) 測試方法：

(1) 將測試電腦連接產品。

(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) 目視掃描結果所呈現之網路服務與對應埠。

(4) 比對產品自我宣告中所聲明之網路服務與對應埠。

(f) 預期結果：

(1) 產品所開啟之網路服務與對應埠，與產品自我宣告之內容相符。

5.2.3 更新安全測試

5.2.3.1 (a)韌體檔案安全測試

(a) 測試依據：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.2.3.1(a)。

(b) 測試目的：

驗證產品之韌體更新檔是否會洩露敏感性資料。

(c) 樣品條件：

(1) 情境 1:

(i)適用韌體檔案加密保護強度測試。

(ii)產品須支援離線更新，否則不適用此測項。

(iii)產品須提供所使用之韌體檔案。

(iv)產品須提供所使用之加密演算法書面資料作為審查依據。

(2) 情境 2:

(i)適用韌體檔案是否存在明文或可解密回復明文之敏感性資料測試。

(ii)產品須提供所使用之韌體檔案。

(iii)若韌體檔案經過加密處理，則廠商須提供解密工具。

(iv)產品須提供所有相連伺服器之宣告。

(d) 測試佈局：

見圖 6。

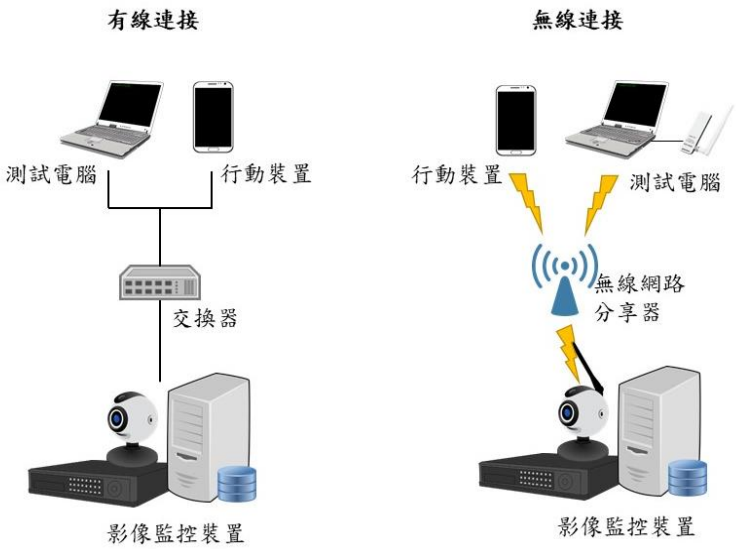

圖 6 測試示意圖

(e) 測試方法：

(1) 情境 1:

(i)使用具韌體拆解功能之工具，對產品之韌體進行拆解。

(ii)檢視該韌體更新檔是否可被解析出檔案系統目錄。

(iii)審閱可證明所使用加密演算法之書面資料。

(2) 情境 2:

(i)使用具韌體拆解功能之工具，對產品之韌體進行拆解。

(ii)取出檔案系統之路徑目錄。

(iii)確認系統通行碼資料的保密機制是否採用 FIPS 140-2 Annex A 所核可之單向雜湊函數(one-way hash)。

(iv)確認金鑰是否可被擷取。

(v)確認是否存在非公開之 email 資料。

(vi)確認是否存在產品所宣告之相連伺服器外之 IP 資料。

(vii)確認是否存在產品所宣告之相連伺服器外之 URL 資料。

(f) 預期結果：

(1) 情境 1

(i)韌體更新檔案無法被解析出檔案系統目錄。

(ii)加密演算法採用 FIPS 140-2 Annex A [2]所認可。

(2) 情境 2

(i)產品之程式碼與安裝檔內其他檔案，無檢出通行碼資料、抑或通行碼鑑別機制符合 5.4.2 節之測試預期結果。

(ii)產品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，抑或加解密金鑰不能被解密回復。

(iii)不存在非公開 email 資料。

(iv)不存在產品所宣告相連伺服器外之 IP 資料。

(v)不存在產品所宣告相連伺服器外之 URL 資料。

上述 2 情境之預期結果，符合其中之一則本測試結果為通過。

5.2.3.1 (b)韌體更新路徑的保護

(a) 測試依據：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.2.3.1(b)。

(b) 測試目的：

驗證產品的韌體線上更新是否採用安全通道，同時是否具有鑑別安全通道所使用憑證之合法性及有效性。

(c) 樣品條件：

(1) 產品須支援線上更新，否則不適用此測項。

(2) 產品須提供所有相連伺服器之宣告。

(3) 受測廠商須協助觸發產品之線上更新。

(4) 產品須保持出廠預設環境狀態。

(d) 測試佈局：

韌體線上更新之測試架構如圖 7，測試對象同時針對產品及更新伺服器。

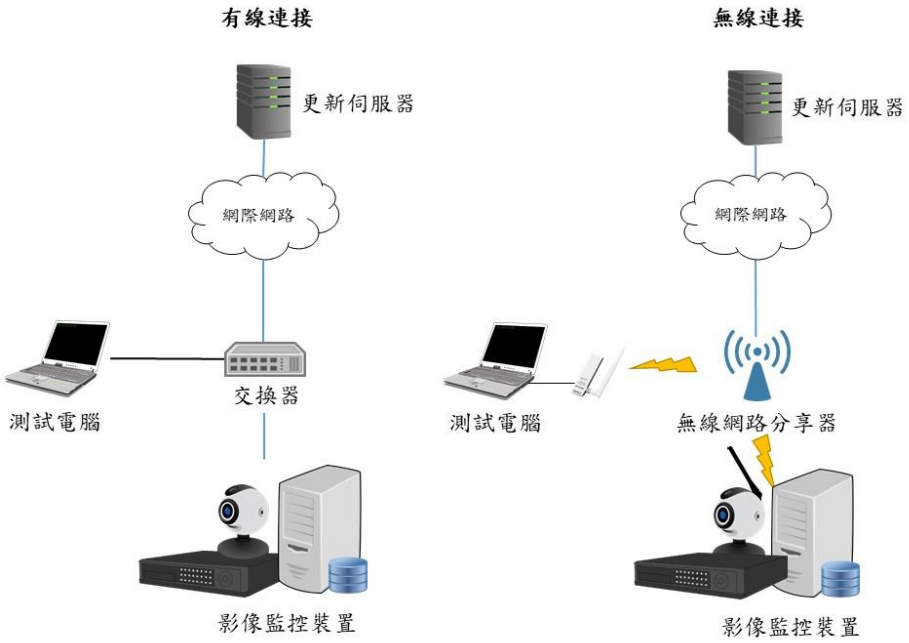

圖 7 測試示意圖

(e) 測試方法：

(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影像監控裝置，並啟動更新。

(4) 側錄更新伺服器與產品之間的封包，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之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、格式錯誤及憑證簽章。

(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監聽封包，檢視產品是否接受此憑證。

(f) 預期結果：

(1) 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。

(2) 更新伺服器之憑證公鑰或憑證資訊其一被竄改，安全通道建立失敗。

5.2.3.2 韌體更新檔之完整性及可信度測試

(a) 測試依據：

「TAICS TS-0014-1 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：

確認產品是否具備驗證韌體更新檔案完整性與不可否認性之能力。

(c) 樣品條件：

(1) 產品須提供其數位簽章使用機制。

(2) 產品須提供所使用之韌體檔案。

(d) 測試佈局：

見圖 8。

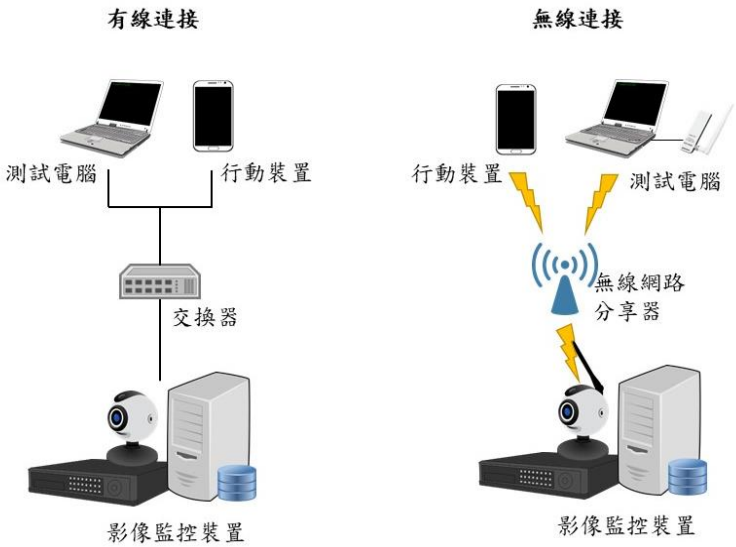

圖 8 測試示意圖

(e) 測試方法：

(1) 對韌體更新檔重新簽章。

(2) 執行產品更新，並檢視更新是否成功。

(f) 預期結果：

(1) 產品更新失敗。

5.2.3.3 備援更新功能測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證當更新作業異常中斷時，產品仍可恢復正常運作狀態。

(c) 樣品條件：

(1) 情境 1

產品須支援離線手動更新。

(2) 情境 2

產品須支援線上更新。

(d) 測試佈局：

(1) 情境 1

見圖 9。

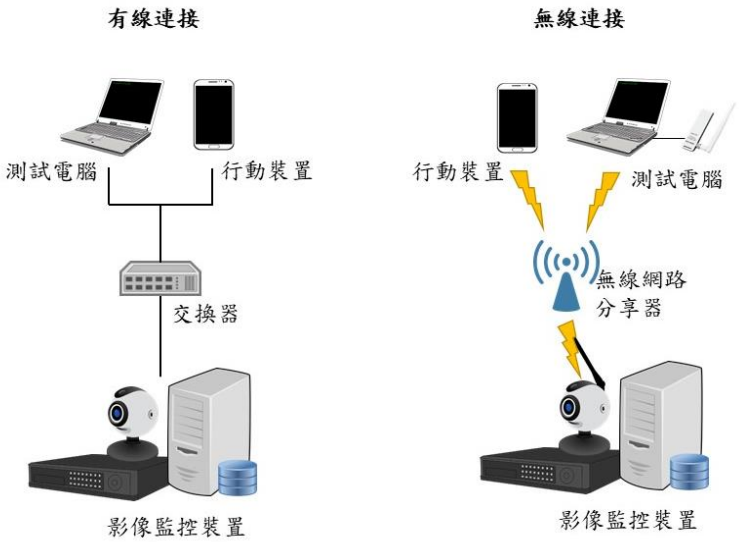

圖 9 測試示意圖

(2) 情境 2

見圖 10。

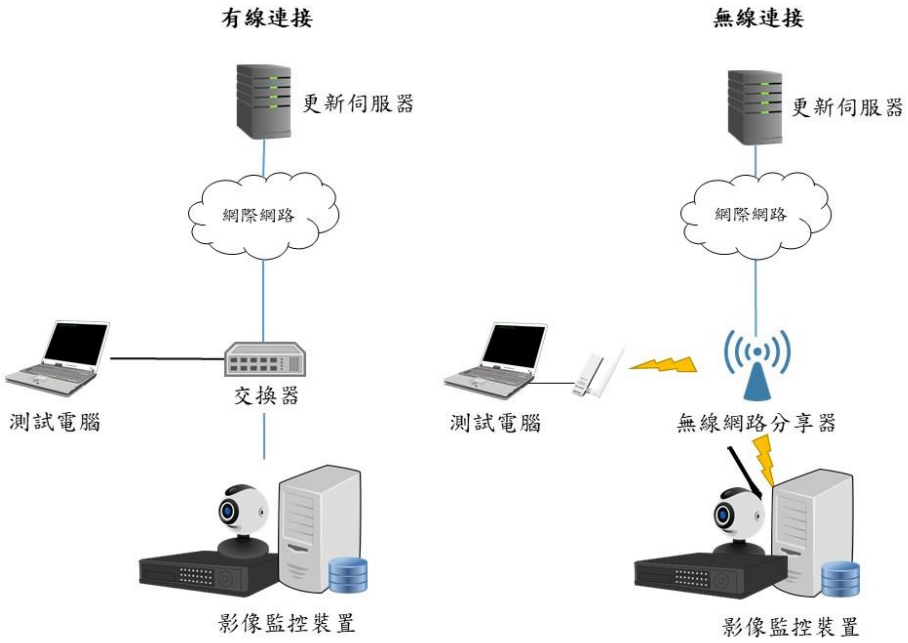

圖 10 測試示意圖

(e) 測試方法：

(1) 情境 1

(i)將測試電腦連接產品。

(ii)啟動離線手動更新。

(iii)於更新過程中，觸發更新中斷。

(2) 情境 2

(i)將測試電腦連接產品。

(ii)啟動線上更新。

(iii)於更新過程中，觸發更新中斷。

(f) 預期結果：

(1) 更新中斷後，系統仍可回復正常運作狀態。

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) 初階測試：

(1) 測試依據：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.2.4.1。

(2) 測試目的：

產品敏感性資料的存取是否具有權限控管機制。

(3) 樣品條件：

產品須提供敏感性資料保存方式之書面資料作為審查依據。

(4) 測試佈局：

無。

(5) 測試方法：

(i)審閱能證明符合此安全要求之書面資料。

(6) 預期結果：

(i)產品通行碼資料之權限管控與產品自我宣告相符。

(ii)產品之加解密金鑰之權限管控與產品自我宣告相符。

(iii)該權限管控機制至少擁有二個以上不同權限的角色。

(b) 中階測試：

(1) 測試依據：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.2.4.1。

(2) 測試目的：

驗證產品敏感性資料的存取是否具有權限控管機制。

(3) 樣品條件：

(i)產品須提供敏感性資料保存方式之書面資料作為審查依據。

(ii)產品須提供系統管理者權限供測試用。

(iii)產品須提供能進入作業系統層之介面。

(4) 測試佈局：

見圖 11。

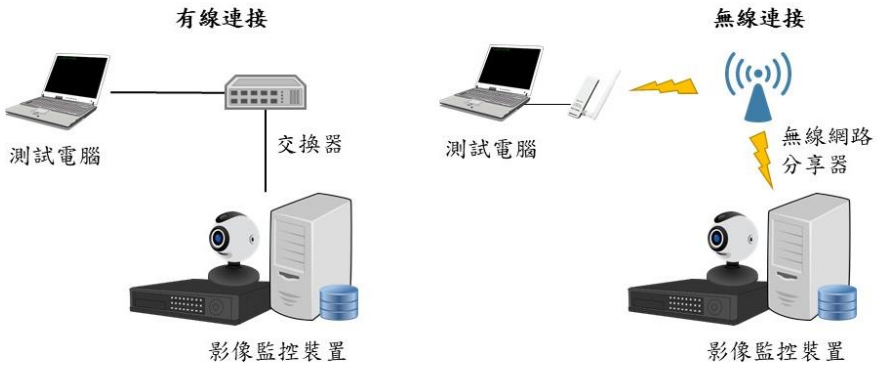

圖 11 測試示意圖

(5) 測試方法：

(i)將測試電腦連接產品。

(ii)依據廠商所提供之通行碼資料保存方式，檢視其存取權限。

(iii)依據廠商所提供之加解密金鑰保存方式，檢視其存取權限。

(6) 預期結果：

(i)產品通行碼資料之權限管控與產品自我宣告相符。

(ii)產品之加解密金鑰之權限管控與產品自我宣告相符。

(iii)該權限管控機制至少擁有二個以上不同權限的角色。

5.2.4.2 敏感性資料加密儲存測試

(a) 初階測試：

(1) 測試依據：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.2.4.2。

(2) 測試目的：

驗證產品之敏感性資料於儲存狀態下是否加密保護。

(3) 樣品條件：

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。

(4) 測試佈局：

無。

(5) 測試方法：

(i)審閱能證明符合此安全要求之書面資料。

(6) 預期結果：

(i)通行碼資料的保密機制採用 FIPS 140-2 Annex A 所核可之單向雜湊函數(one way hash)。

(ii)加解密用金鑰的保密機制採用 FIPS 140-2 Annex A 所核可之加密演算法。

(b) 中階測試：

(1) 測試依據：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.2.4.2

(2) 測試目的：

驗證產品之敏感性資料於儲存狀態下是否加密保護。

(3) 樣品條件：

(i)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。

(ii)產品須提供系統管理者權限供測試用。

(iii)產品須提供能進入作業系統層之介面。

(4) 測試佈局：

見圖 12。

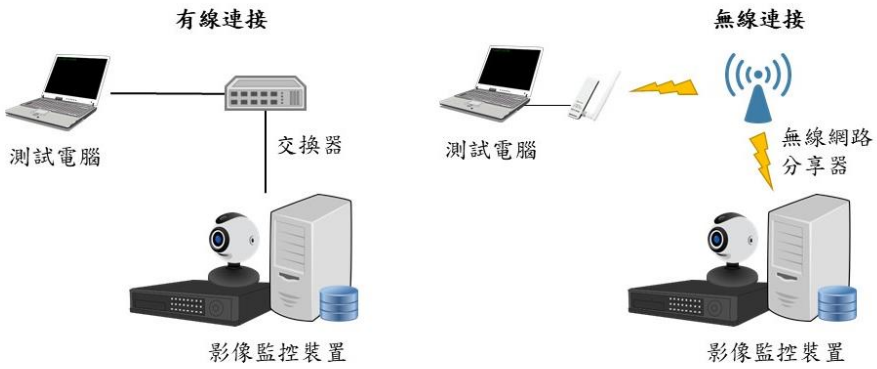

圖 12 測試示意圖

(5) 測試方法：

(i)審閱能證明符合此安全要求之書面資料。

(ii)將測試電腦連接產品。

(iii)檢視保護通行碼資料所採用的保密機制。

(iv)檢視保護加解密金鑰所採用的保密機制。

(6) 預期結果：

(i)通行碼資料的保密機制採用 FIPS 140-2 Annex A 所核可之單向雜湊函數(one-way hash)。

(ii)加解密用金鑰的保密機制採用 FIPS 140-2 Annex A 所核可之加密演算法。

5.2.4.3 金鑰管理程序測試

(a) 測試依據：

「TAICS TS-0014-1 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：

確認產品的金鑰管理是否建立可靠管控程序。

(c) 樣品條件：

產品須提供金鑰管理程序之說明文件。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 審閱具備此程序說明之書面資料。

(f) 預期結果：

(1) 產品有制定金鑰生成、交換、儲存、使用、銷毀及更替之程序，且該程序須以達到監督、保證和證明金鑰得到妥善管理為目標。

5.2.4.4 敏感性資料隔離保護測試

(a) 測試依據：

「TAICS TS-0014-1 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：

確認產品敏感性資料之存放與正常作業系統隔離。

(c) 樣品條件：

(1) 產品須提供敏感性資料保存方式之書面資料作為審查依據。

(2) 產品須聲明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) 測試佈局：

無。

(e) 測試方法：

(1) 審閱具備此功能證明之書面資料。

(f) 預期結果：

(1) 書面資料證實產品之敏感性資料存放於安全區域。

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：

「TAICS TS-0014-1 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：

驗證產品之網頁管理介面是否存在已知資安漏洞。

(c) 樣品條件：

產品須提供系統管理者權限供測試用。

(d) 測試佈局：

見圖 13。

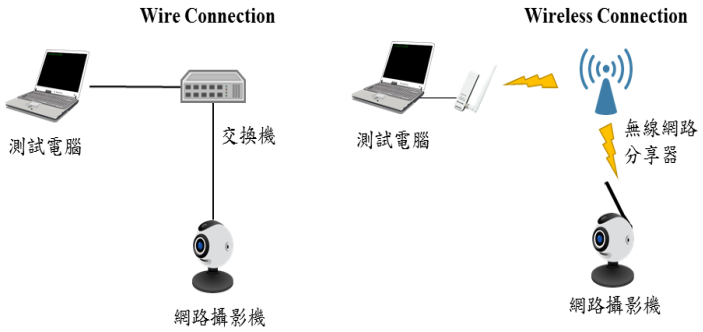

圖 13 測試示意圖

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 開啟網頁管理介面，檢視網頁是否使用超文本傳輸協定。

(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) 預期結果：

(1) 產品之網頁管理介面，不存在引發 OWASP web Top 10 [3]之 Injection 及 XSS 資安攻擊風險。

5.2.6 操控程式之應用程式介面(ONVIF API)安全測試

5.2.6.1 應用程式介面之鑑別機制測試

(a) 應用程式介面之鑑別機制強度測試

(1) 測試依據：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.2.6.1。

(2) 測試目的：

驗證產品的應用程式介面呼叫是否經過身分鑑別程序，且該身分鑑別程序具備重送攻擊抵抗能力。

(3) 樣品條件：

產品須具備電腦或行動裝置之操控程式介面(即 ONVIF API)，否則此測項不適用。

(4) 測試佈局：

見圖 14。

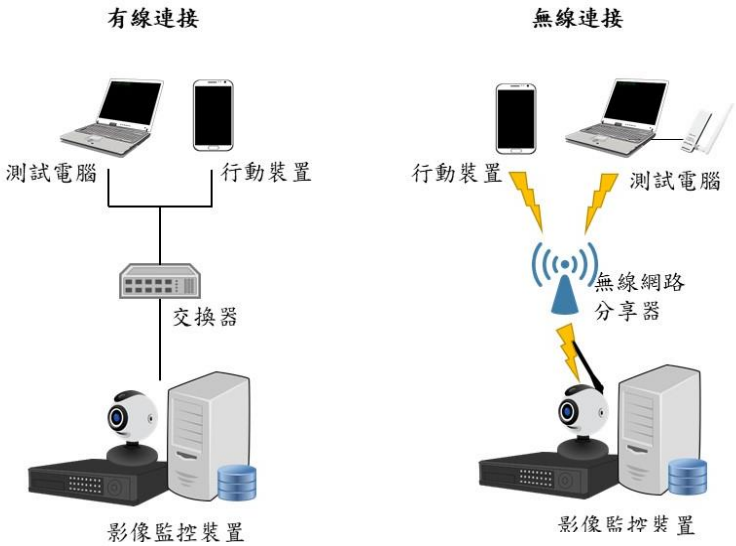

圖 14 測試示意圖

(5) 測試方法：

(i)將測試電腦或行動裝置連接產品。

(ii)根據產品使用說明，開啟具 ONVIF API 之操控程式。

(iii)透過操控程式與產品建立連線，同時側錄封包。

(iv)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。

(v)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。

(vi)檢視鑑別結果是否成功。

(6) 預期結果：

(i)存取產品經過身分鑑別。

(ii)重送攻擊失敗。

(b) 應用程式介面之身分鑑別錯誤訊息

(1) 測試依據：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.2.6.1。

(2) 測試目的：

驗證鑑別錯誤訊息不會造成敏感性資料的洩漏。

(3) 樣品條件：

產品之用戶帳號已經建立。

(4) 測試佈局：

見圖 15。

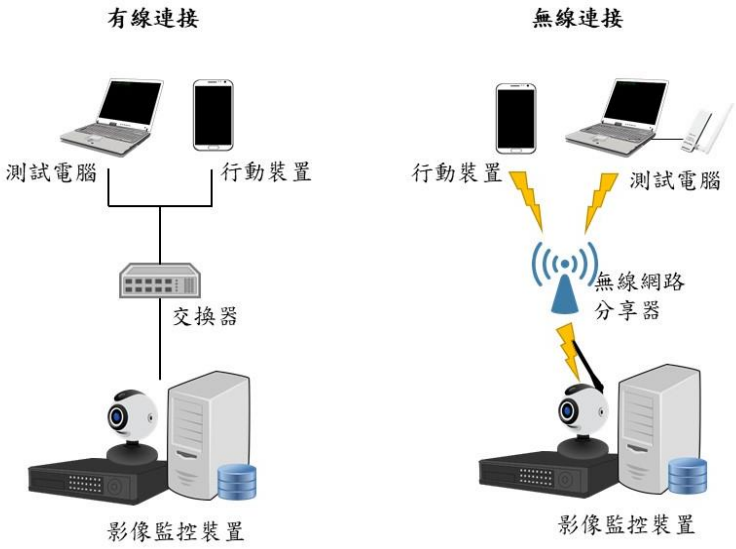

圖 15 測試示意圖

(5) 測試方法：

(i)將測試電腦連接產品。

(ii)根據產品使用說明，開啟具 ONVIF API 之操控程式。

(iii)透過操控程式與產品建立連線。

(iv)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。

(v)輸入已存在之用戶帳號搭配錯誤的通行碼，檢視鑑別錯誤訊息。

(vi)輸入不存在之用戶帳號，檢視鑑別錯誤訊息。

(6) 預期結果：

(i)從鑑別錯誤訊息無法推斷出合法使用者名稱。

5.2.6.2 應用程式介面之通行碼鑑別強度機制測試

(a) 測試依據：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.2.6.2。

(a) 測試目的：

驗證產品應用程式介面的通行碼鑑別機制強度是否足夠。

(b) 樣品條件：

(1) 產品之應用程式介面須支援通行碼鑑別機制，否則此測項不適用。

(2) 產品須提供帳戶鎖定機制之設計說明。

(c) 測試佈局：

見圖 16。

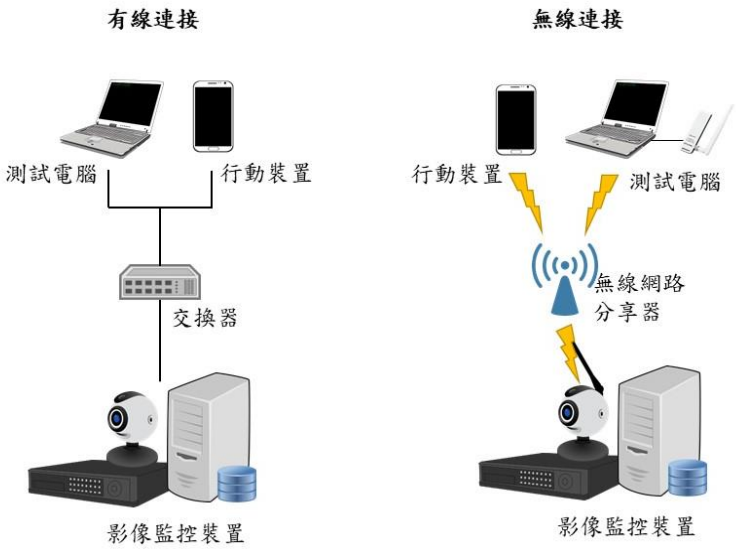

圖 16 測試示意圖

(d) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 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。

(e) 預期結果：

(1) 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 應用程式介面之權限管控機制

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品的應用程式介面是否存在權限控管。

(c) 樣品條件：

(1) 產品須提供角色之應用程式介面存取權限之宣告。

(2) 產品須具備電腦或行動裝置之操控程式介面，否則此測項不適用。

(3) 產品之用戶帳號及通行碼已經建立，並且存在系統管理者及一般使用者二類帳號。

(d) 測試佈局：

見圖 17。

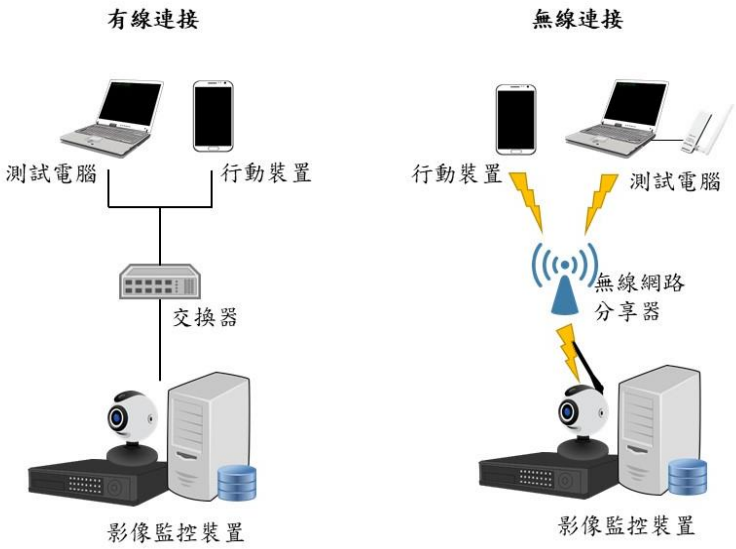

圖 17 測試示意圖

(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，開啟電腦或行動裝置之操控程式。

(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) 同時檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(f) 預期結果：

(1) 各角色 ONVIF API 的權限管控與產品自我宣告相符。

(2) 至少有二個以上不同權限的角色。

5.2.7 日誌檔與警示測試

5.2.7.1 安全事件日誌檔測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品是否有安全事件紀錄供查詢。

(c) 樣品條件：

無。

(d) 測試佈局：

見圖 18。

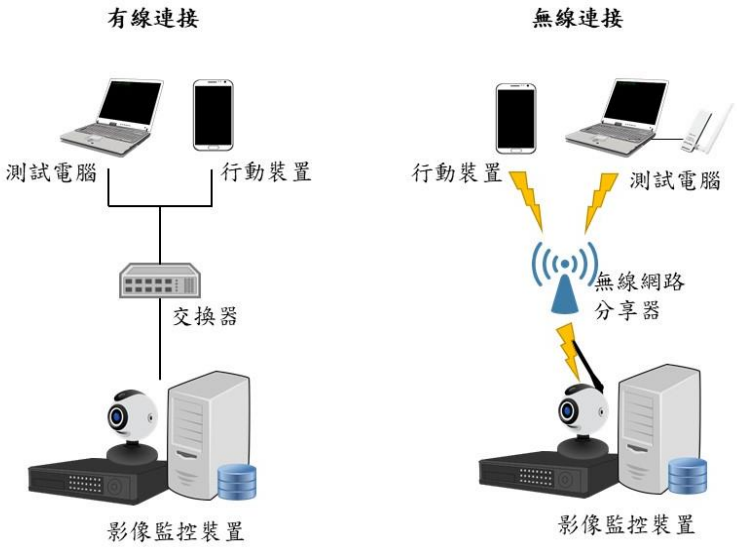

圖 18 測試示意圖

(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) 檢視日誌內容是否記載使用者的登入紀錄。

(4) 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。

(5) 將產品重新開機。

(6) 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。

5.2.7.2 安全事件日誌檔存取權限管控測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品之安全事件日誌紀錄是否具備權限控管。

(c) 樣品條件：

(1) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，並且存在系統管理者及一般使用者二類帳號。

(2) 產品須提供安全事件日誌檔存取權限說明。

(d) 測試佈局：

見圖 19。

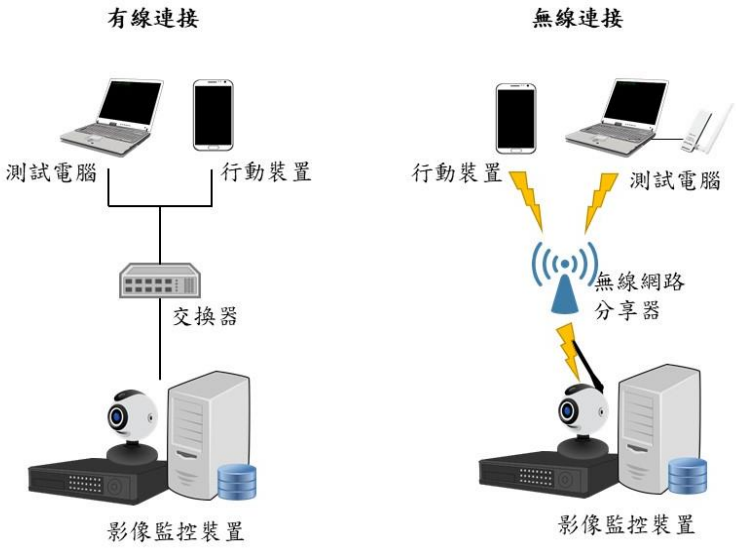

圖 19 測試示意圖

(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) 檢視帳號之身分類型對安全事件日誌檔的存取權限是否與產品自我宣告相符。

(f) 預期結果：

(1) 安全事件日誌檔的身分授權與產品自我宣告相符。

(2) 至少有二個以上不同權限的角色。

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：

「TAICS TS-0014-1 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：

驗證產品是否具備處理日誌儲存空間不足之異常狀況。

(c) 樣品條件：

產品須提供系統管理者權限供測試用。

(d) 測試佈局：

見圖 20。

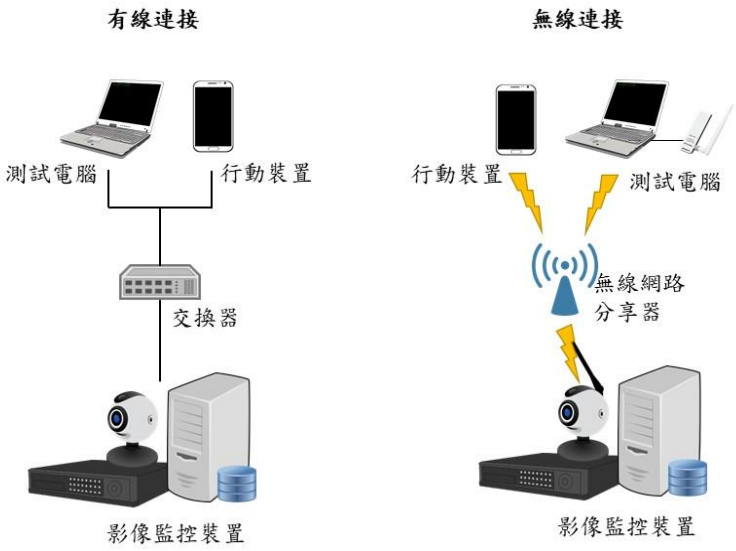

圖 20 測試示意圖

(e) 測試方法：

(1) 不斷觸發安全事件日誌，以填充安全事件紀錄儲存容量，直到儲存空間不足。

(2) 檢視產品是否無法正常記錄安全事件。

(f) 預期結果：

(1) 產品不會發生儲存空間不足的現象。

(2) 產品仍可正常記錄安全事件。

5.2.7.4 異常警示功能測試

(a) 測試依據：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.2.7.4。

(b) 測試目的：

驗證產品是否具有確保安全事件日誌紀錄檔可用性之功能。

(c) 樣品條件：

(1) 產品須提供系統管理者權限供測試用。

(2) 產品須提供當安全事件日誌檔儲存空間不足時，異常警示之運作說明。

(d) 測試佈局：

見圖 21。

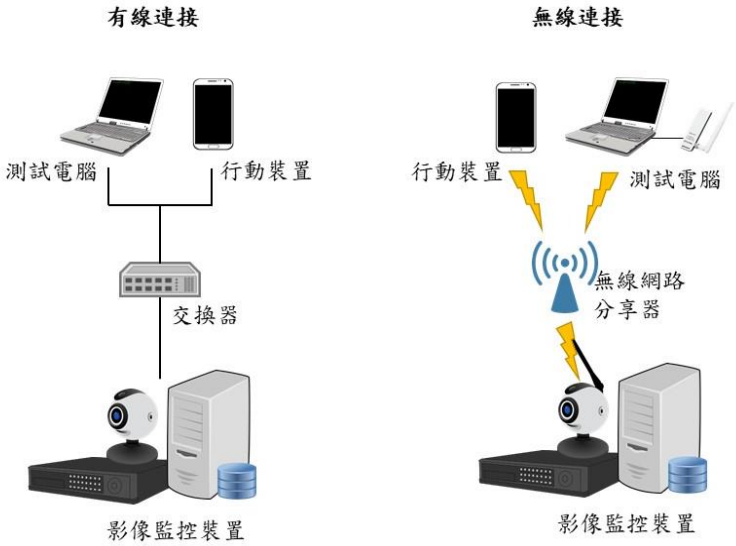

圖 21 測試示意圖

(e) 測試方法：

(1) 不斷觸發安全事件日誌，以填充安全事件紀錄儲存容量，直到儲存空間不足。

(2) 檢視產品是否發出警示。

(f) 預期結果：

(1) 產品發出安全事件日誌紀錄檔儲存空間不足之警示。

5.3 通訊安全測試

檢視影像監控裝置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 敏感性資料之傳輸保護初階測試

(a) 測試依據：

「TAICS TS-0014-1 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：

(1) 驗證產品敏感性資料之傳輸，預設是否採用強度足夠之安全通道。

(2) 確認產品是否具備驗證此安全通道憑證有效性及合法性之能力。

(c) 樣品條件：

(1) 產品須保持出廠預設環境狀態。

(2) 產品須提供可與其相連之影像監控裝置。

(3) 若與產品對連之影像監控裝置採用自簽發憑證，則產品須提供可編輯中繼憑證之介面。

(d) 測試佈局：

見圖 22。

圖 22 測試示意圖

(e) 測試方法：

(1) 對產品使用安全通道掃描工具。

(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) 於相應之管理介面輸入帳號密碼，同時側錄封包。

(5) 檢視所側錄之封包是否採用安全通道。

(6) 將產品與其它影像監控裝置連接，並啟動安全通道之建立程序。

(7) 當其它影像監控裝置發送憑證予產品之間時攔截其憑證，並置換憑證公鑰或憑證資訊，包括發證單位、有效期限、格式錯誤及憑證簽章。

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

(f) 預期結果：

(1) 安全通道僅支援「附錄 A」中所建議之密碼套件。

(2) 與測試電腦之間的帳號密碼資訊傳輸，預設採用安全通道。

(3) 與行動裝置之間的帳號密碼資訊傳輸，預設採用安全通道。

(4) 已竄改敏感性資料傳輸用之安全通道憑證未通過產品認證

5.3.1.2 敏感性資料之傳輸保護中階測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證傳輸敏感性資料之安全通道，是否支援強加密演算法。

(c) 樣品條件：

無。

(d) 測試佈局：

見圖 23。

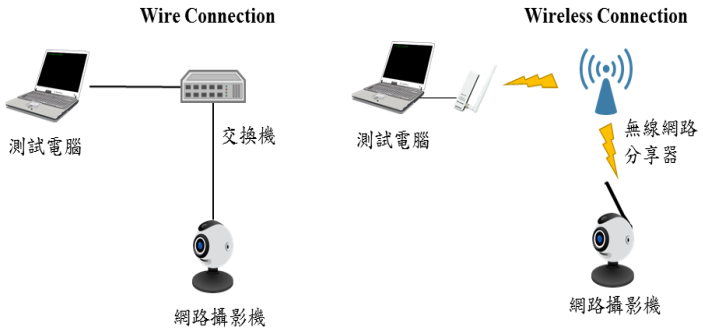

圖 23 測試示意圖

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 使用安全通道掃描工具。

(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) 預期結果：

(1) 該安全通道支援 AES-256 同等或以上加密強度的演算法。

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：

「TAICS TS-0014-1 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：

確認產品是否運行在具安全風險的網路設定。

(c) 樣品條件：

(1) 產品須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) 產品須保持出廠預設環境狀態。

(3) 產品須提供所支援網路服務之說明文件。

(d) 測試佈局：

見圖 24。

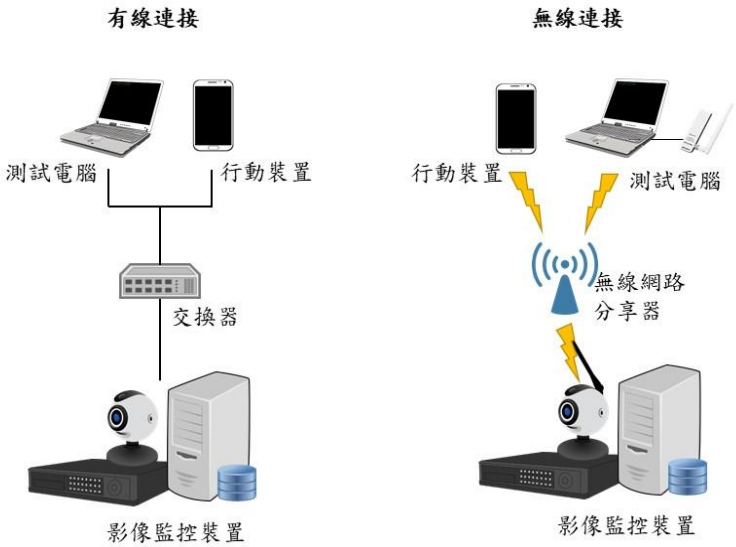

圖 24 測試示意圖

(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) 若產品支援通用隨插即用通訊協定，目視產品之操控程式或網頁管理介面，通用隨插即用通訊協定是否存在供使用者操作的開/關介面。

(4) 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，同時確認使用者是否可自行開/關通用隨插即用通訊協定服務。

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

(6) 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，同時確認使用者是否可自行開/關簡單網路管理協定服務。

(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確認產品是否支援零配置通訊協定服務，同時確認使用者是否可自行開/關零配置通訊協定服務。

(f) 預期結果：

(1) 若產品支援通用隨插即用通訊協定服務，該服務提供使用者可自行開/關功能之設置。

(2) 若產品支援簡單網路管理協定服務， 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。

5.3.2.2 網路介面存取設置測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品是否可安全的透過遠端方式存取作業系統除錯模式之設計。

(c) 樣品條件：

(1) 產品須保持出廠預設環境狀態。

(2) 產品若存在進入作業系統除錯模式之介面，須提供進入之方法。

(d) 測試佈局：

見圖 25。

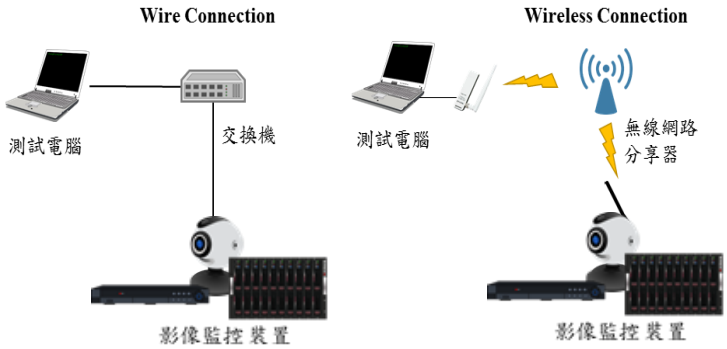

圖 25 測試示意圖

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 根據產品使用說明，開啟相應之管理介面連接工具。

(3) 確認可否透過網路連線存取作業系統之除錯模式。

(4) 測試電腦連接產品之 USB 埠。

(5) 確認可否透過 USB 埠存取作業系統之除錯模式。

(6) 若存取前須經通行碼鑑別程序，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) 預期結果：

(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，產品要求身分鑑別。

(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。

5.3.2.3 通訊協定異常輸入測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品影像傳輸相關之通訊協定是否存在未知之資安漏洞。

(c) 樣品條件：

無。

(d) 測試佈局：

見圖 26。

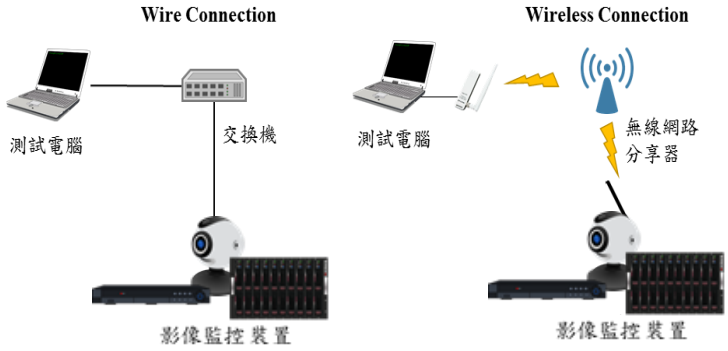

圖 26 測試示意圖

(e) 測試方法：

(1) 將測試電腦連接產品。

(2) 啟動具模糊測試功能之工具。

(3) 執行對「附錄 B」中各種類(例如：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一個測試案例。

(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) 預期結果：

(1) 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)。

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：

「TAICS TS-0014-1 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：

驗證產品是否存在錯誤的 Wi-Fi 設定。

(c) 樣品條件：

(1) 產品須支援 Wi-Fi 保護設置功能，否則此測項不適用。

(2) 產品須保持出廠預設環境狀態。

(d) 測試佈局：

見圖 27。

圖 27 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，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) 預期結果：

(1) 有提供使用者 WPS PIN 開/關之功能。

(2) WPS PIN 功能預設為關閉。

5.3.3.2 無線網路傳輸安全機制設置測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品是否存在不安全的 Wi-Fi 通道保護設定

(c) 樣品條件：

(1) 產品需支援 Wi-Fi 功能，否則此測項不適用。

(2) 產品須保持出廠預設環境狀態。

(d) 測試佈局：

見圖 28。

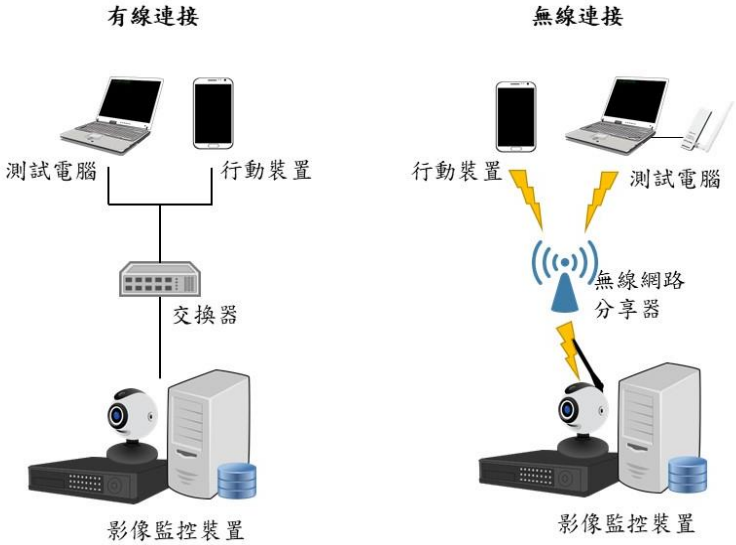

圖 28 測試示意圖

(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) 與產品建立連線，同時側錄 Wi-Fi 封包。

(4) 根據側錄結果確認傳輸是否採用「Wi-Fi 保護存取 2」加密方式。

(f) 預期結果：

(1) Wi-Fi 預設加密模式為「Wi-Fi 保護存取 2」。

5.3.3.3 Wi-Fi 通訊協定異常輸入測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品之 Wi-Fi 通訊協定是否存在未知之資安漏洞。

(c) 樣品條件：

無。

(d) 測試佈局：

見圖 29。

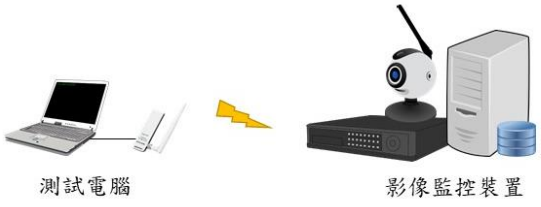

圖 29 測試示意圖

(e) 測試方法：

(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，或者最少 8 小時的異常輸入測試。

(4) 確保同時間只能進行一個測試案例。

(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) 預期結果：

(1) 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)。

5.3.3.4 Wi-Fi 認證安全機制設置測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品是否支援 IEEE 802.1X 認證。

(c) 樣品條件：

無。

(d) 測試佈局：

見圖 30。

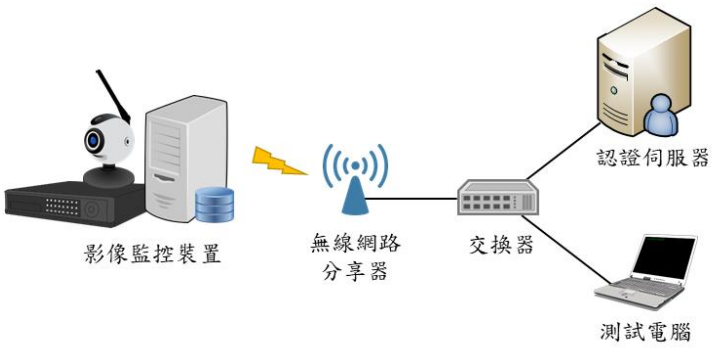

圖 30 測試示意圖

(e) 測試方法：

(1) 將產品之 802.1X 功能開啟。

(2) 連接已啟用 802.1X 功能之 Wi-Fi AP。

(f) 預期結果：

(1) 產品可透過 IEEE 802.1X 建立 Wi-Fi 連線。

5.4 身分鑑別與授權機制安全測試

檢視影像監控裝置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 鑑別機制強度測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品是否具備可靠之身分鑑別機制。

(c) 樣品條件：

無。

(d) 測試佈局：

見圖 31。

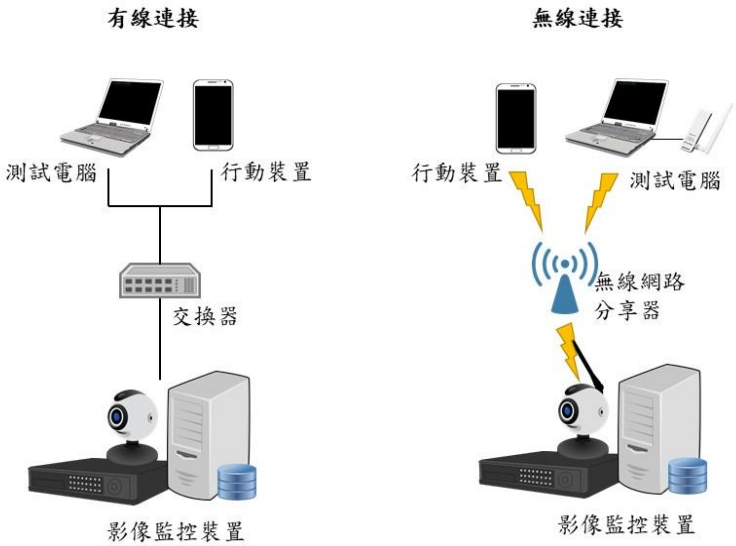

圖 31 測試示意圖

(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) 執行身分鑑別操作，同時側錄封包，並檢視是否確實執行身分鑑別。

(4) 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。

(5) 檢視鑑別結果是否成功。

(6) 執行產品登出並再次登入，檢視身分鑑別功能是否正常執行。

(f) 預期結果：

(1) 無論透過網頁管理介面或操控程式存取影像監控裝置時，皆經過身分鑑別程序。

(2) 身分鑑別機制具備抵抗重送攻擊的能力。

(3) 登出後確實須再次登入，方可存取產品。

5.4.1.2 身分鑑別錯誤訊息

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證鑑別錯誤訊息不會造成敏感性資料的洩漏。

(c) 樣品條件：

無。

(d) 測試佈局：

見圖 32。

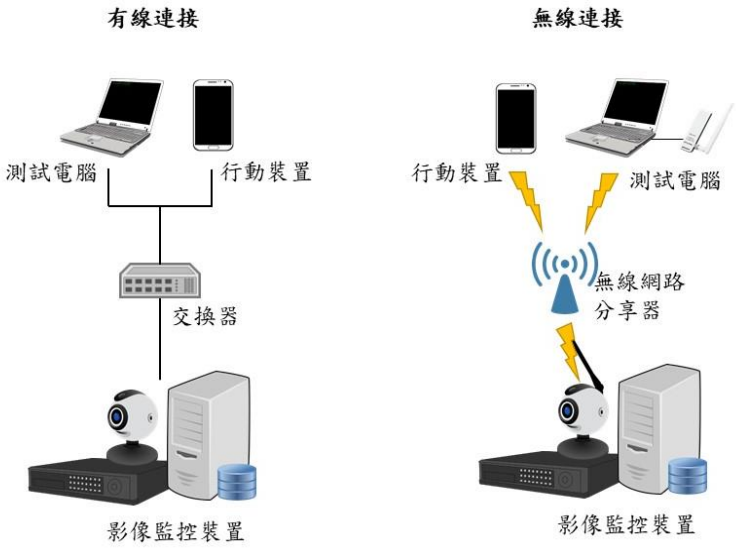

圖 32 測試示意圖

(e) 測試方法：

(1) 分別將測試電腦及行動裝置連接產品。

(2) 根據產品使用說明，開啟相應之管理介面連接工具以執行身分鑑別。

(3) 輸入已存在之使用者搭配錯誤的通行碼，檢視鑑別錯誤訊息。

(4) 輸入不存在之使用者，檢視鑑別錯誤訊息。

(f) 預期結果：

(1) 從鑑別錯誤訊息無法推斷出合法使用者名稱。

5.4.1.3 憑證上傳介面測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品是否具有提供憑證上傳的功能。

(c) 樣品條件：

(1) 產品須提供憑證上傳的操作說明。

(2) 產品須提供可與其相連之影像監控裝置。

(d) 測試佈局：

見圖 33。

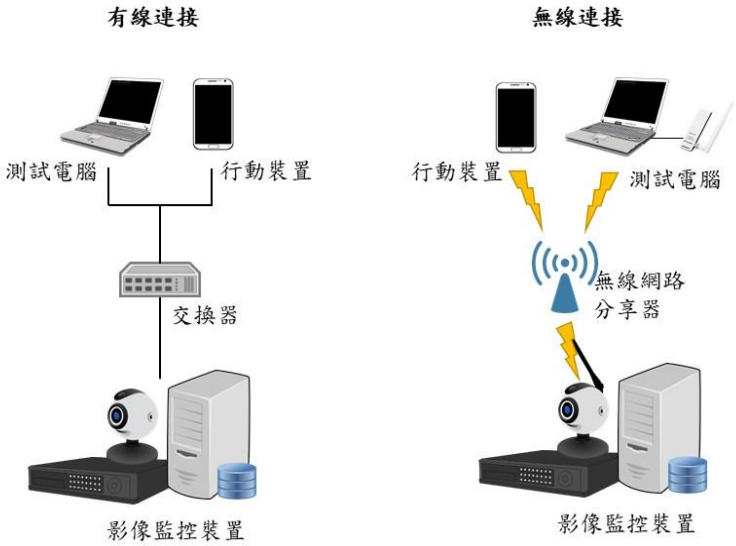

圖 33 測試示意圖

(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以執行憑證上傳。

(3) 連接其它可驗證此上傳憑證之影像監控裝置，確認憑證是否可被鑑別接受。

(f) 預期結果：

(1) 產品所上傳之憑證可被相連之影像監控裝置鑑別接受。

5.4.1.4 金鑰唯一性測試

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品之金鑰是否唯一。

(c) 樣品條件：

產品須提供可與其相連之影像監控裝置。

(d) 測試佈局：

參照圖 34。

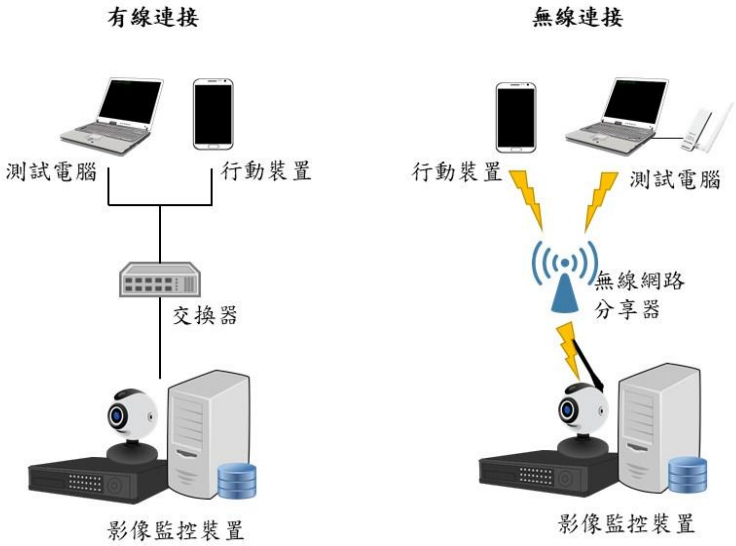

圖 34 測試示意圖

(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以執行身分鑑別。

(3) 側錄封包並擷取產品之憑證，檢視其指紋碼(fingerprint)。

(4) 重置產品至出廠預設狀態。

(5) 重覆步驟 2~3。

(6) 與其它影像監控裝置建立連線，並執行身分鑑別。

(7) 側錄封包並擷取產品之憑證，檢視其指紋碼(fingerprint)。

(8) 重置產品至出廠預設狀態。

(9) 重覆步驟 6~8。

(f) 預期結果：

(1) 若測試設備透過圖形化管理介面連接產品，重置出廠預設狀態前後，憑證之指紋碼是相異的。

(2) 若測試設備透過安全外殼協定(SSH)連接產品，重置出廠預設狀態前後，憑證之指紋碼是相異的。

(3) 若測試是產品與其它影像監控裝置互連，重置出廠預設狀態前後，憑證之指紋碼是相異的。

5.4.1.5 多因子鑑別機制測試

(a) 測試依據：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.4.1.5。

(b) 測試目標：

驗證裝置之身分鑑別機制是否支援多因子認證之強認證機制。

(c) 樣品條件：

(1) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，且多因子鑑別功能已經啟用。

(2) 須提供具多因子鑑別操作之產品說明文件。

(d) 測試佈局：

見圖 35。

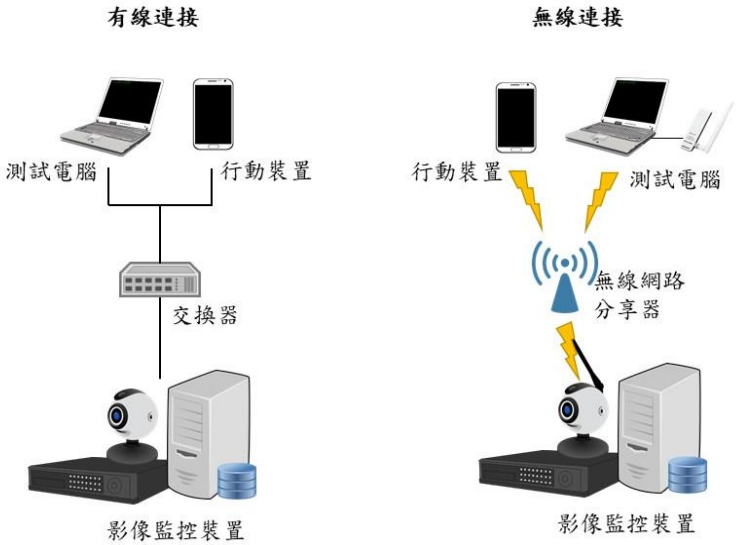

圖 35 測試示意圖

(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以執行身分鑑別。

(3) 執行多因子身分鑑別操作，檢查是否每次的身分鑑別都採用不同種類之鑑別因子。

(4) 檢查鑑別過程中是否採用短訊服務(Short Message Service, SMS)獲取通行碼。

(5) 檢查鑑別過程中，使用行動裝置作為所持之物(something you have)之鑑別因子時，檢視是否僅可在 1 台行動裝置上獲取鑑別因子。

(f) 預期結果：

(1) 網頁管理介面或操控程式與產品之間的身分鑑別，透過多因子身分鑑別。

(2) 每一階段身分鑑別皆採用不同因素的鑑別因子。

(3) 當使用鑑別因子時，未採用短訊服務獲取通行碼。

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

5.4.1.6 裝置鑑別測試

(a) 測試依據：

「TAICS TS-0014-1 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：

產品須提供能鑑別相連之影像監控系統裝置身分的功能，且其裝置鑑別機制具備抵抗重送攻擊的能力。

(c) 樣品條件：

產品須提供與其相連之影像監控裝置。

(d) 測試佈局：

參照圖 36。

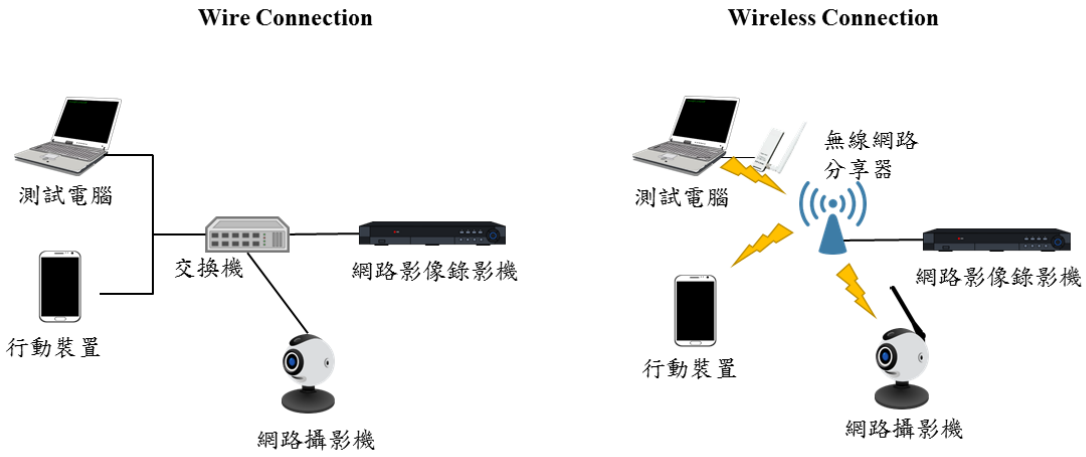

圖 36 測試示意圖

(e) 測試方法：

(1) 將產品與其它影像監控系統裝置建立連線。

(2) 將測試電腦或行動裝置連接其它影像監控系統裝置。

(3) 檢查是否要求對連裝置之身分鑑別。

(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，再另一次身分鑑別操作時，重新發送至產品。

(6) 檢視鑑別結果是否成功。

(f) 預期結果：

(1) 其它影像監控系統裝置與產品建立連線時，經過裝置身分鑑別。

(2) 該裝置身分鑑別機制具備抵抗重送攻擊的能力。

5.4.2 通行碼鑑別安全測試

5.4.2.1 應用程式介面之預設通行碼安全

(a) 測試依據：

「TAICS TS-0014-1 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：

(1) 情境 1：

驗證產品是否有相同的預設通行碼。

(2) 情境 2：

驗證產品預設通行碼是否會於首次上線後強制要求更改。

(c) 樣品條件：

(1) 產品須支援通行碼鑑別機制，否則此測項不適用。

(2) 產品須保持出廠預設環境狀態。

(d) 測試佈局：

見圖 37。

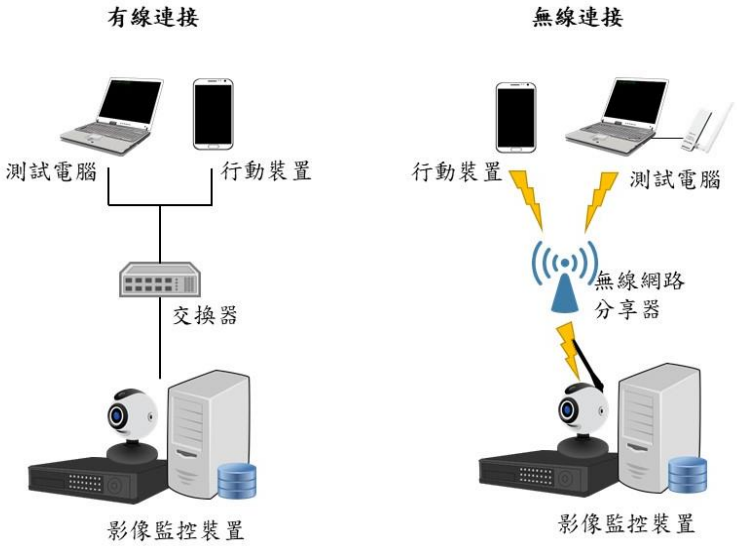

圖 37 測試示意圖

(e) 測試方法：

(1) 情境 1：

(i)準備 2 台以上產品。

(ii)將測試電腦或行動裝置連接產品。

(iii)透過網頁管理介面或操控程式，根據產品使用說明輸入預設通行碼。

(iv)比對 2 台影像監控裝置的預設通行碼是否相異。

(2) 情境 2：

(i)將測試電腦或行動裝置連接產品。

(ii)從網頁管理介面或操控程式輸入通行碼。

(iii)確認在未設定新通行碼的情況下，是否可存取產品。

(f) 預期結果：

(1) 情境 1：

任 2 台產品的預設通行碼相異。

(2) 情境 2：

未經設定新通行碼前無法存取產品。

上述 2 情境之預期結果，符合其中之一則本測試結果為通過。

5.4.2.2 通行碼長度

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品的通行碼長度是否足夠，以確保其強度。

(c) 樣品條件：

產品須支援通行碼鑑別機制，否則此測項不適用。

(d) 測試佈局：

見圖 38。

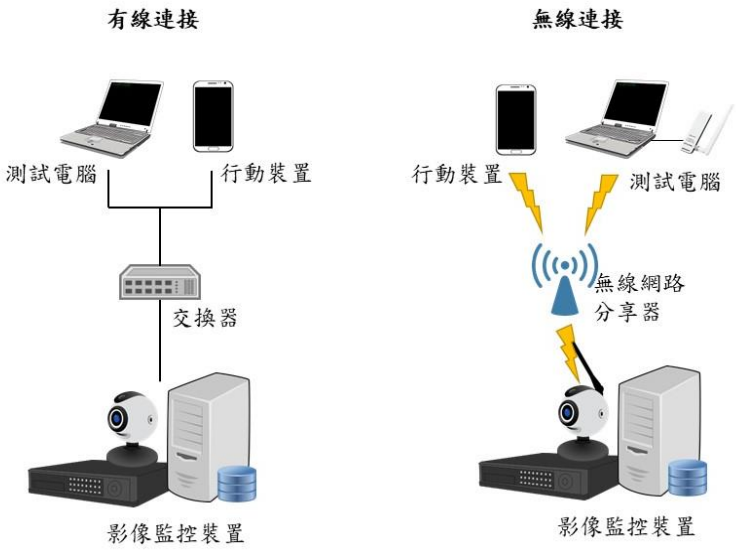

圖 38 測試示意圖

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 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，檢查通行碼是否能成功建立或變更。

(f) 預期結果：

(1) 無法建立或變更小於 8 個字元長度之通行碼。

5.4.2.3 通行碼複雜度

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品的通行碼複雜度是否足夠，以確保其強度。

(c) 樣品條件：

產品須支援通行碼鑑別機制，否則此測項不適用。

(d) 測試佈局：

見圖 39。

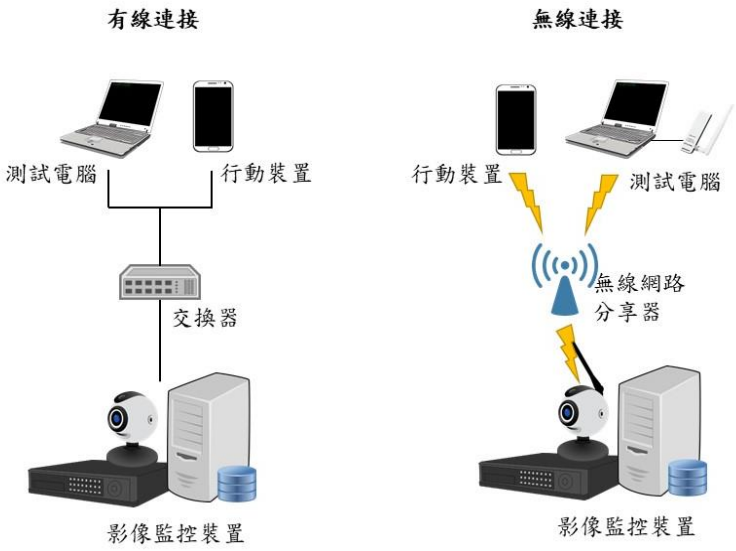

圖 39 測試示意圖

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 從網頁管理介面或操控程式，建立或變更通行碼。

(3) 輸入僅同時含下述四者字元中的一種及二種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.10 進位數字 (0 到 9)；4.非英文字母字元 (例如：！、$、#、%)，檢查通行碼是否能成功建立或變更。

(f) 預期結果：

(1) 無法建立或變更通行碼。

5.4.2.4 通行碼的輸入頻率及次數限制

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證通行碼鑑別機制是否有防止暴力破解之能力。

(c) 樣品條件：

(1) 產品須支援通行碼鑑別機制，否則此測項不適用。

(2) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。

(3) 產品須提供帳戶鎖定機制之設計說明。

(d) 測試佈局：

見圖 40。

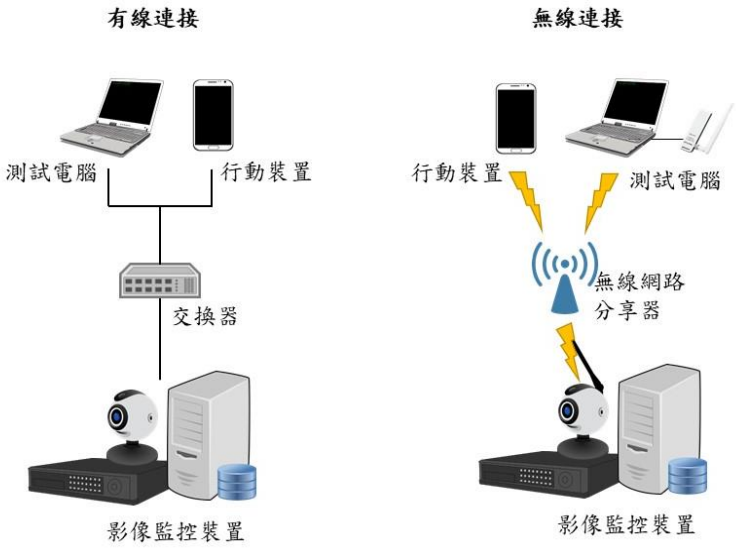

圖 40 測試示意圖

(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以執行身分鑑別。

(3) 不斷輸入錯誤且相異的通行碼。

(4) 檢視產品於帳戶鎖定計數器重設為 0 前，連續登入失敗次數 5 次以內，是否會鎖定帳戶。

(5) 帳戶鎖定後，於鎖定期間內持續輸入相異且錯誤的通行碼，比對廠商宣告帳戶鎖定時限內，檢視帳戶是否解除鎖定。

(6) 同一帳戶任一次登入失敗後，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，檢視輸入失敗次數是否有重新計算。

(f) 預期結果：

(1) 輸入次數 5 次以內，會鎖定帳戶。

(2) 於廠商宣告之帳戶鎖定時限內，帳戶未解除鎖定。

(3) 於廠商宣告計數器重設時限內，失敗次數未重新計算。

5.4.2.5 通行碼連續字元之避免

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品的通行碼是否存有連續字元，以確保其強度。

(c) 樣品條件：

產品須支援通行碼鑑別機制，否則此測項不適用。

(d) 測試佈局：

見圖 41。

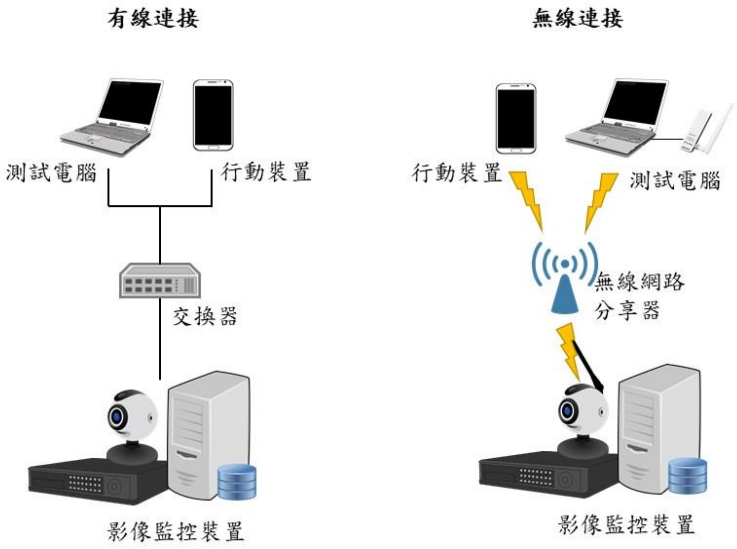

圖 41 測試示意圖

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 從網頁管理介面或操控程式，建立或變更通行碼。

(3) 輸入含使用者的帳戶名稱全名中，3 個以上的連續字元，檢查通行碼是否能成功建立或變更。

(f) 預期結果：

(1) 無法建立或變更通行碼。

5.4.2.6 通行碼歷程記錄

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品的通行碼是否執行通行碼歷程記錄功能，以確保其強度。

(c) 樣品條件：

產品須支援通行碼鑑別機制，否則此測項不適用。

(d) 測試佈局：

見圖 42。

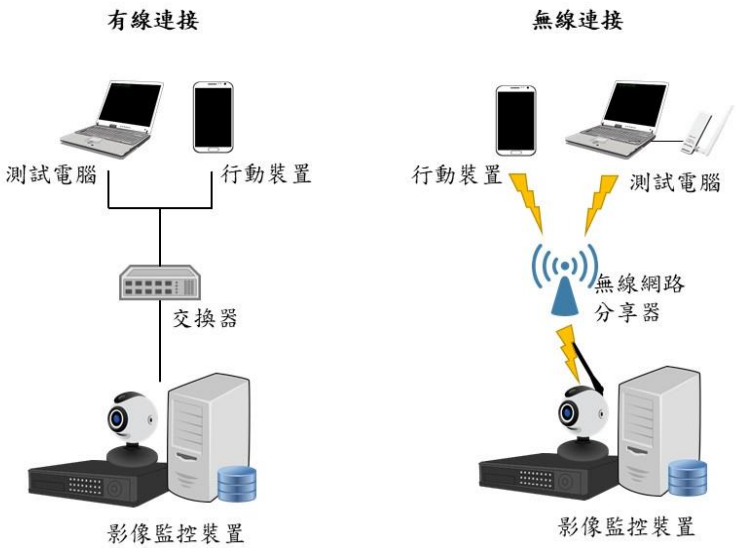

圖 42 測試示意圖

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 從網頁管理介面或操控程式，建立或變更通行碼。

(3) 從網頁管理介面或操控程式變更通行碼，輸入產品曾經使用過之通行碼，檢查通行碼是否能成功變更。

(f) 預期結果：

(1) 無法變更通行碼。

5.4.3 權限管控測試

5.4.3.1 權限管控機制

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品資源的存取是否具有權限控管機制。

(c) 樣品條件：

(1) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，並且存在系統管理者及一般使用者二類帳號。

(2) 產品須提供角色存取權限之宣告。

(d) 測試佈局：

見圖 43。

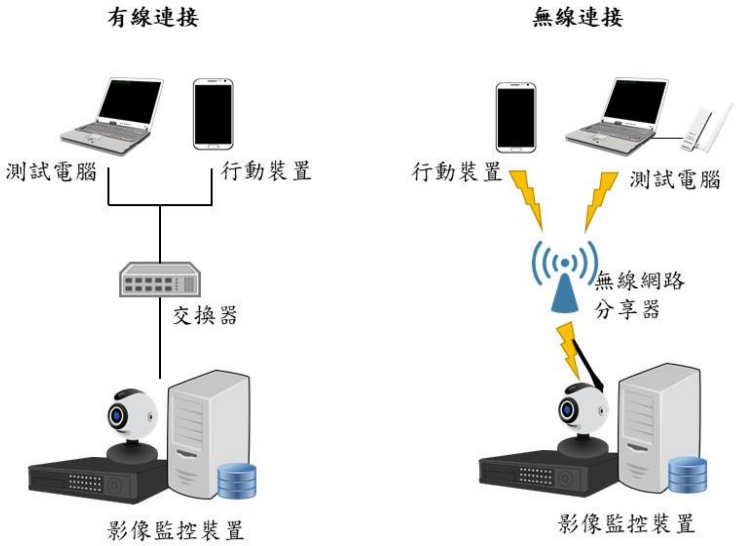

圖 43 測試示意圖

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 透過網頁管理介面或操控程式，分別以不同角色登入產品。

(3) 存取產品資源，同時檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(4) 若為網頁管理介面，嘗試以同一頁面讓不同權限的角色存取。

(f) 預期結果：

(1) 使用者的身分授權與產品自我宣告相符。

(2) 至少擁有二個以上不同權限的角色。

5.4.3.2 權限有效時間

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品是否存在有限的授權時間長度。

(c) 樣品條件：

產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。

(d) 測試佈局：

見圖 44。

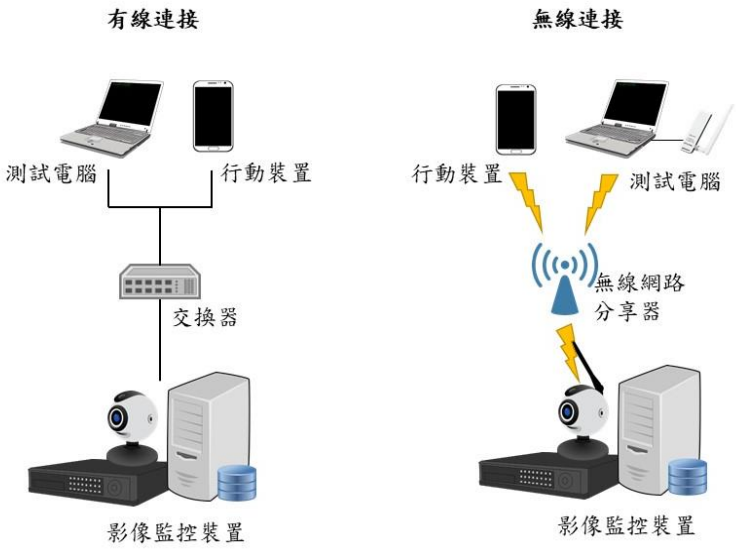

圖 44 測試示意圖

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 透過網頁管理介面或操控程式登入產品。

(3) 目視產品之操控程式或網頁管理介面，閒置時限是否存在供使用者設定的操作介面。

(4) 閒置產品直到超過閒置時限值。

(5) 檢視是否需要重新鑑別方可存取產品。

(f) 預期結果：

(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，須經過身分鑑別方可存取產品。

5.5 隱私保護測試

檢視影像監控裝置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

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證產品隱私權否具有存取控制機制。

(c) 樣品條件：

(1) 產品須提供隱私存取權限之宣告。

(2) 產品必須能建立 2 個以上的帳號，否則此測項不適用。

(d) 測試佈局：

見圖 45。

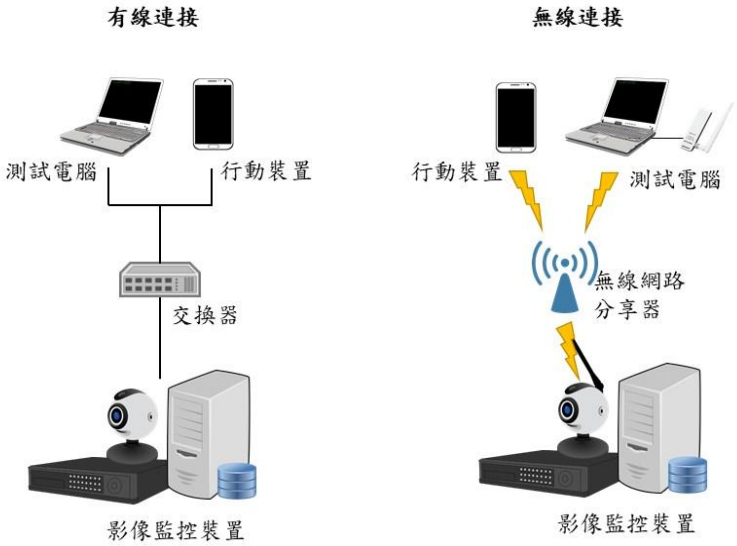

圖 45 測試示意圖

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 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，同時檢視該帳號之身分類型與其對應之隱私存取權限是否與產品自我宣告相符。

(4) 當產品提供網頁管理介面且已經有帳號登入的情況下，檢視是否無需透過帳號切換，即可存取該帳號權限之外的隱私資料。

(f) 預期結果：

(1) 使用者的隱私存取授權與產品自我宣告相符。

5.5.1.2 隱私資料刪除功能

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證使用者擁有刪除自身隱私權的權限。

(c) 樣品條件：

(1) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，並且存在系統管理者及一般使用者二類帳號。

(2) 每一角色已建立所屬之影像及用戶資訊。

(d) 測試佈局：

見圖 46。

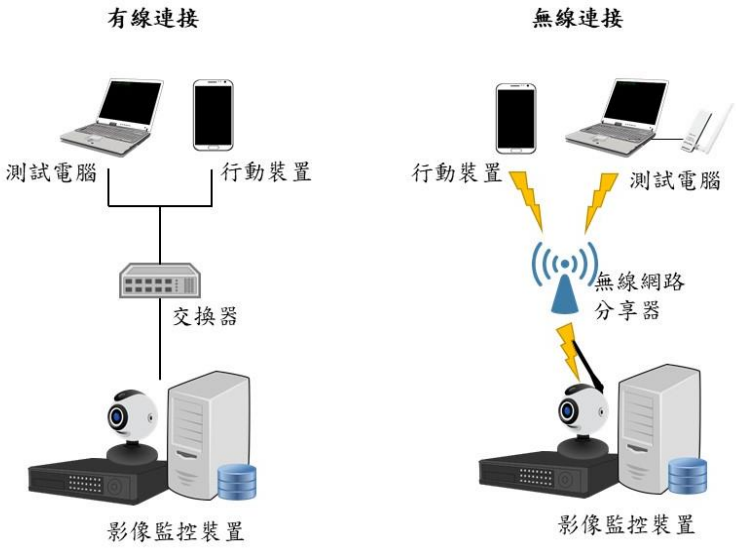

圖 46 測試示意圖

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 透過網頁管理介面或操控程式，以不同角色登入產品。

(3) 目視產品之操控程式或網頁管理介面，影像資料是否存在供使用者刪除的操作介面。

(4) 執行刪除功能後，確認產品之隱私資料是否已被移除。

(f) 預期結果：

(1) 提供使用者刪除隱私資料的功能。

(2) 隱私資料確實刪除。

5.5.1.3 登入警示功能測試

(a) 測試依據：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.5.1.3。

(b) 測試目的：

驗證產品是否具有防止隱私外洩之功能。

(c) 樣品條件：

無。

(d) 測試佈局：

見圖 47。

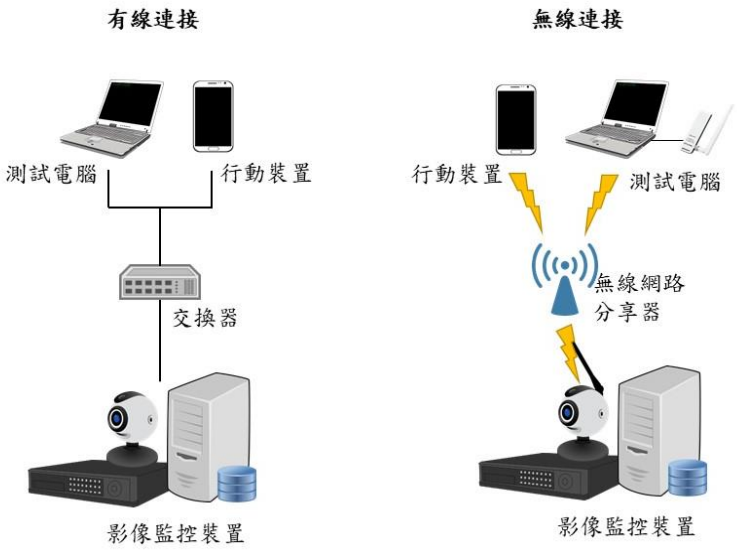

圖 47 測試示意圖

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 透過網頁管理介面或操控程式，以不同角色登入產品。

(3) 根據產品使用說明，無論登入成功與否，確認是否接收到登入警示。

(f) 預期結果：

(1) 每次發生新的存取事件時，產品發出警示。

5.5.2 隱私資料的傳輸保護測試

5.5.2.1 隱私資料的傳輸機密性初階保護

(a) 測試依據：

「TAICS TS-0014-1 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：

(1) 驗證產品隱私資料的傳輸，是否採用強度足夠之安全通道。

(2) 確認產品是否具備驗證此安全通道憑證有效性及合法性之能力。

(c) 樣品條件：

無。

(d) 測試佈局：

見圖 48。

圖 48 測試示意圖

(e) 測試方法：

(1) 對產品使用安全通道掃描工具。

(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。

(6) 將產品與其它影像監控裝置連接，並啟動影像傳輸之安全通道建立。

(7) 當其它影像監控裝置發送憑證予產品之間攔截其憑證，並置換憑證公鑰或憑證資訊，包括發證單位、有效期限、格式錯誤及憑證簽章。

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

(f) 預期結果：

(1) 安全通道僅支援「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) 與行動裝置之間的影像資料傳輸，預設採用安全通道。

(4) 已竄改影像傳輸用之安全通道憑證未通過產品認證。

5.5.2.2 隱私資料的傳輸機密性中階保護

(a) 測試依據：

「TAICS TS-0014-1 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：

驗證傳輸隱私資料的安全通道，是否支援強加密演算法。

(c) 樣品條件：

無。

(d) 測試佈局：

見圖 49。

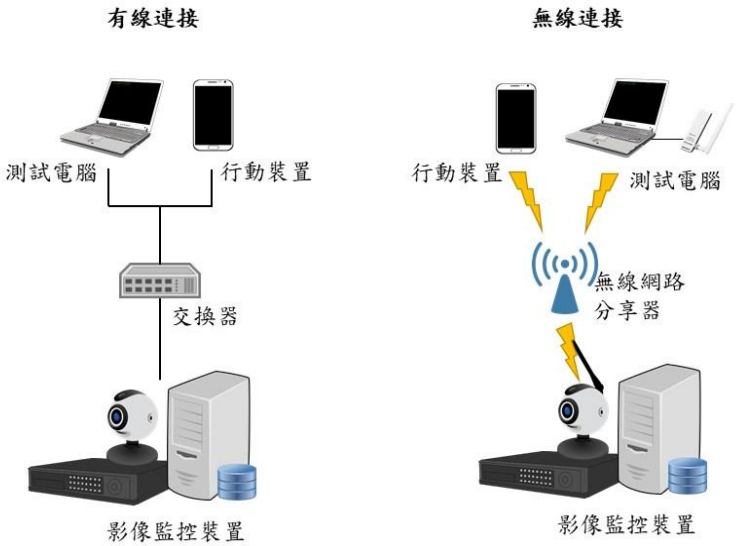

圖 49 測試示意圖

(e) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 使用安全通道掃描工具，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) 預期結果：

(1) 該安全通道支援 AES-256 同等或以上加密強度的演算法。

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

B.1 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.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。

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：

表一、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, RJ-45
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：

表二、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. **日誌功能可用性警示**	描述當日誌檔空間不足時，日誌檔的處理機制及警示方法，或提供佐證文件。	

機制	*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，必須提供。 *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，必須提供。 *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，必須提供。 *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，必須提供。 *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] TAICS TS-0014-1 v1.0:2018 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., 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.

版本修改紀錄

版本	時間	摘要
v1.0	2018/06/08	v1.0 出版
-	-	-
-	-	-
-	-	-
-	-	-
-	-	-
-	-	-

台灣資通產業標準協會

Taiwan Association of Information and Communication Standards

地　址・台北市中正區重慶南路二段51號8樓之一
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw