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

(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 韌體更新功能測試

(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 5.2.3.1。

(b) 測試目的：

查驗產品具韌體更新功能。

(c) 前置條件：

無。

(d) 測試布局：

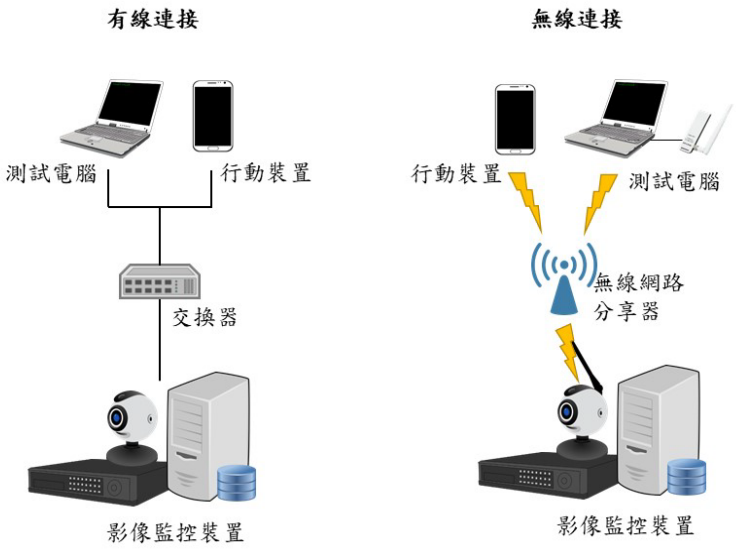

圖 6 測試示意圖

(e) 測試步驟：

(1) 將測試電腦連接產品。

(2) 根據文件所述執行韌體更新。

(f) 測試結果：

(1) 通過：產品具韌體更新功能。

(2) 不通過：產品不具備具韌體更新功能。

(3) 不適用：無。

5.2.3.2 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 5.2.3.2。

(b) 測試目的：

查驗產品之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) 使用具韌體拆解功能之工具，對產品之韌體進行拆解。

(2) 檢視該韌體更新檔是否可被解析出檔案系統目錄。

(3) 若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) 若韌體更新檔未加密，確認是否存在金鑰。

(6) 若韌體更新檔未加密，確認是否存在非公開之 email 資料。

(7) 若韌體更新檔未加密，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) 韌體具備更新功能。

(2) 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) 韌體之程式碼與安裝檔內其他檔案，無檢出通行碼資料。

(4) 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) 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) 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) 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 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 5.2.3.3。

(b) 測試目的：

查驗產品之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：

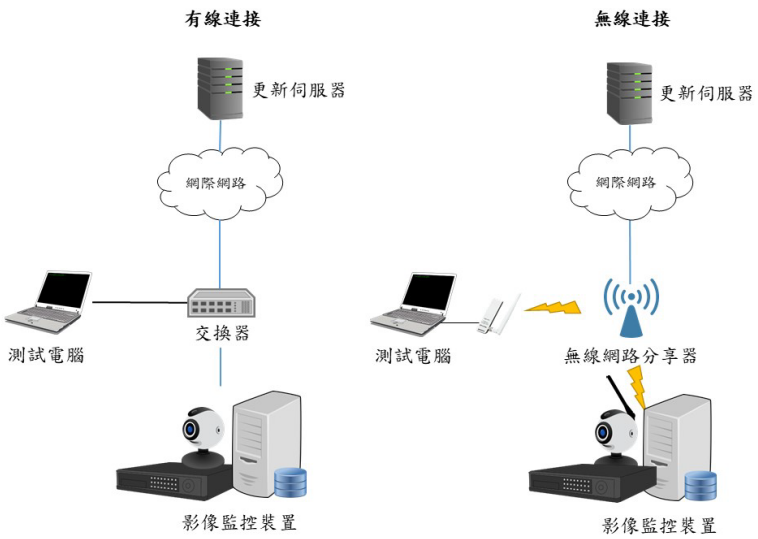

圖 7 測試示意圖

(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) 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 韌體更新檔之完整性及真確性測試

(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 5.2.3.4。

(b) 測試目的：

查驗產品具備驗證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：

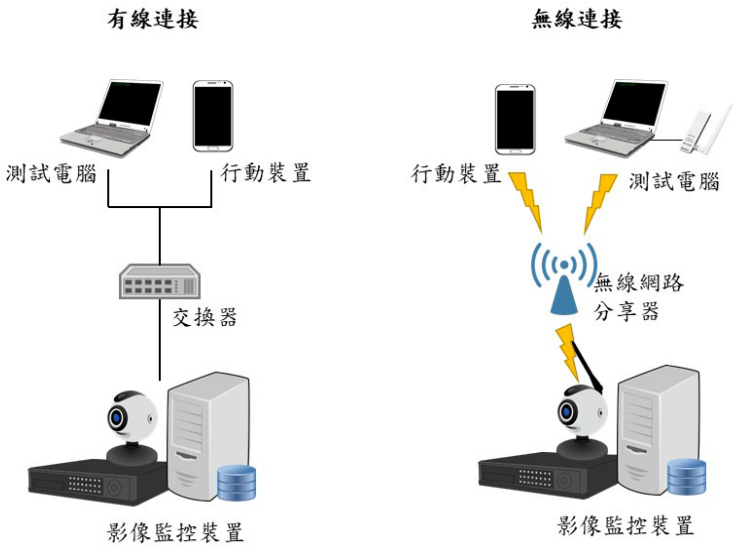

圖 8 測試示意圖

(e) 測試步驟：

方法 1 (廠商提供測試用私鑰予實驗室)：

(1) 廠商提供原始韌體並提供簽章方法，實驗室使用自簽私鑰簽署該韌體。

(2) 實驗室執行韌體更新，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韌體，並將公鑰植入於產品。

(2) 實驗室執行韌體更新，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韌體，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，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：

「TAICS TS-0014-1 影像監控系統資安標準-第一部：一般要求」之 5.2.3.5。

(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。

(d) 測試布局：

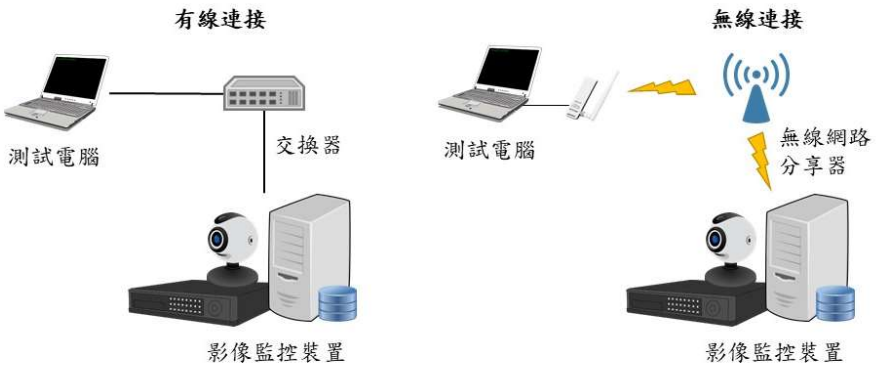

圖 12 測試示意圖

(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 應用程式介面之權限管控機制測試

(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 5.2.6.1。

(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：

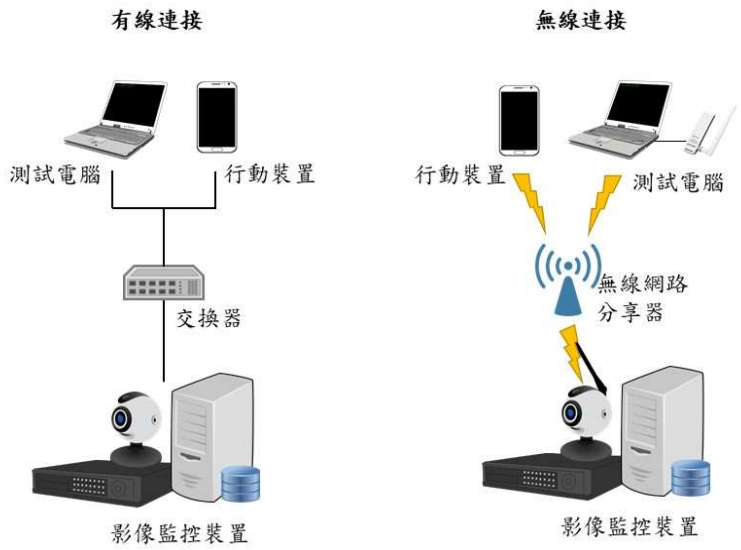

圖 13 測試示意圖

(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。

5.2.6.2 ONVIF 應用程式介面之鑑別機制測試

(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 5.2.6.2。

(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，則該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：

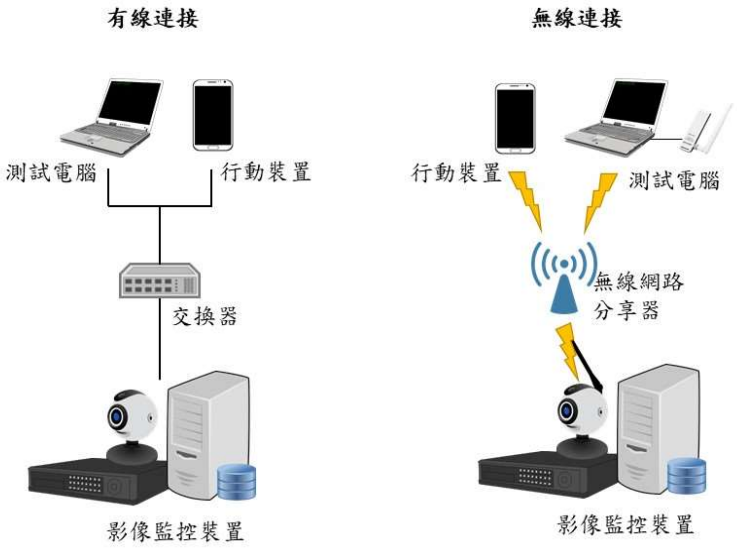

圖 14 測試示意圖

(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。

5.2.6.3 (a) ONVIF 應用程式介面之通行碼鑑別強度提示測試

(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 5.2.6.3。

(b) 測試目的：

查驗產品之 ONVIF 應用程式介面之通行碼鑑別機制強度不足時應提示。

(c) 前置條件：

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。

(d) 測試布局：

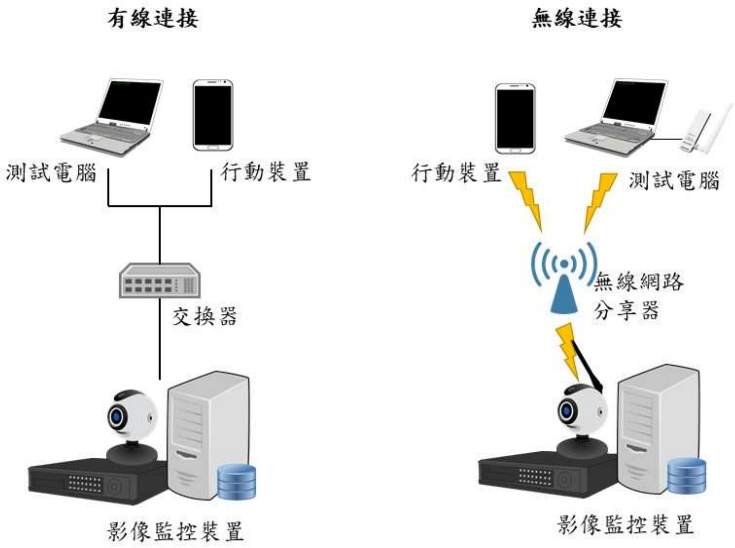

圖 15 測試示意圖

(e) 測試步驟：

(1) 將測試電腦或行動裝置連接產品。

(2) 依照 5.4.2.1 測試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 之測試結果。

5.2.6.3 (b) ONVIF 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 5.2.6.3。

(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：

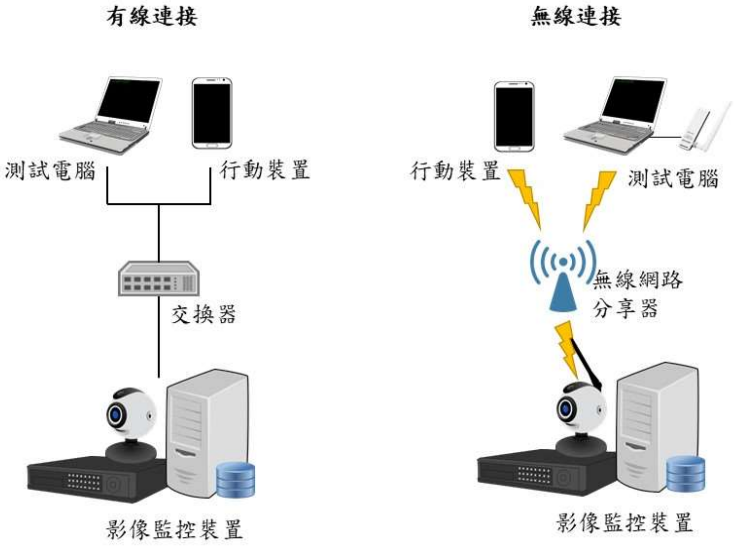

圖 16 測試示意圖

(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。

修改紀錄表

修正條文(補充文件)	現行條文(v2.0)

4. 測試項目分級

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~~(a)~~ ~~5.2.6.3(b)~~	-	-
	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	-	-

5.2.3.1 韌體更新功能測試

(f) 測試結果：↵

(1) 通過：產品具韌體更新功能。↵

~~(2) 通過：(1)或(2)項結果符合。~~↵

~~(3)~~(2) 不通過：~~(1)(2)項結果皆不符合~~產品不具韌體更新功能。

~~(4)~~(3) 不適用：無。↵

5.2.3.2 韌體檔案安全測試 (1)

(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。↵

~~(7) 產品之根金鑰(root key)不適用此測項。~~↵

5.2.3.2 韌體檔案安全測試 (2)

(f) 測試結果：↵

(1) 韌體具備更新功能。↵

(2) 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) 韌體之程式碼與安裝檔內其他檔案，無檢出通行碼資料。↵

(4) 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) 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) 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) 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~~，或產品所儲存之根金鑰~~。↵

5.2.3.4 韌體更新檔之完整性及真確性測試 (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韌體，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，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) 不適用：產品不支援線上更新。~~↵
5.2.6 ● 條文調整勘誤: – 5.2.6.1->5.2.6.3 – 5.2.6.2->5.2.6.1 – 5.2.6.3(a)刪除 – 5.2.6.3(b)->5.2.6.2 ● 5.2.6 條文搬動後及修正內容見上方頁面編號p. 38~p. 42