影像監控系統資安標準測試規範-第一部：一般要求(TAICS TS-0015-1 v2.0:2021)

※可依需求，部分選用測試項目

5. 資安測試規範

章節標號	章節/測試名稱	測試目的	全盲滲透測試評估結果	
			適用	不適用
5.1	實體安全測試			
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	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。	✓	
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	查驗產品之實體埠有插拔紀錄。	✓	
5.1.2.2	實體異常狀態警示機制	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。	✓	
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	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。	✓	
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	驗證產品於開機階段是否能確保產品之完整性及合法性。	✓	
5.2	系統安全測試			
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	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。	✓	
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	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。	✓	
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	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。	✔	
5.2.2	最小化網路與服務連接埠管控測試			

章節標號	章節/測試名稱	測試目的	全盲滲透測試評估結果	
			適用	不適用
5.2.2.1	網路服務最小化測試	查證產品不能存在預期以外之網路埠。	✓	
5.2.2.2	遙測資料收集測試	查驗產品不存在預期以外之遙測資料收集。	✓	
5.2.3	更新安全測試			
5.2.3.1	韌體更新功能測試	查驗產品具韌體更新功能。	✓	
5.2.3.2	韌體檔案安全測試	查驗產品之韌體有經過加密保護。	✓	
5.2.3.3	韌體更新路徑的保護	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。	✓	
5.2.3.4	韌體更新檔之完整性及真確性測試	查驗產品具備驗證韌體更新檔完整性及真確性之能力。	✓	
5.2.3.5	備援更新功能測試	查驗當更新作業異常中斷時，產品仍可恢復正常運作狀態。	✓	
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	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。	✓	
5.2.4.2	敏感性資料加密儲存測試	查驗產品之敏感性資料於儲存狀態下具有加密保護功能。	✓	
5.2.4.3	金鑰管理程序測試	查驗產品之金鑰管理具備可靠的管控程序。	✓	
5.2.4.4	敏感性資料隔離保護測試	查驗產品之敏感性資料之存放與正常作業系統隔 離。	✓	
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	查驗產品之網頁管理介面不存在Injection 及XSS 資安風險漏洞。	✓	
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	查驗產品之ONVIF 應用程式介面應存在權限管控。	✓	

章節標號	章節/測試名稱	測試目的	全盲滲透測試評估結果	
			適用	不適用
5.2.6.2	ONVIF應用程式介面之鑑別機制測試	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。	✓	
5.2.6.3(a)	ONVIF應用程式介面之通行碼鑑別強度提示測試	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。	✓	
5.2.6.3(b)	ONVIF 應用程式介面之通行碼鑑別強度機制測試	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。	✓	
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	查驗產品有安全事件日誌供查詢。	✓	
5.2.7.2	安全事件日誌檔存取權限管控測試	查驗產品之安全事件日誌具權限控管。	✓	
5.2.7.3	安全事件日誌檔之日誌滾動功能測試	查驗產品具處理日誌儲存空間不足之異常狀況的能力。	✓	
5.3	通訊安全測試			
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	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。	✓	
5.3.1.2	敏感性資料之傳輸保護中階測試	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。	✓	
5.3.1.3	敏感性資料之傳輸保護高階測試	查驗產品之敏感性資料傳輸，支援強加密演算法。	✓	
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	查驗產品未運行在具安全風險的網路探詢協定。	✓	
5.3.2.2	網路介面存取設置測試	查驗產品之遠端存取除錯模式的方法是具管控的。	✓	
5.3.2.3	通訊協定異常輸入測試	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。	✓	
5.3.3	Wi-Fi 通訊安全測試			
5.3.3.1	安全的Wi-Fi 組態設置測試	查驗產品不存在錯誤的Wi-Fi 設定。	✓	
5.3.3.2	無線網路傳輸安全機制設置測試	查驗產品具有安全的Wi-Fi通道保護設定。	✓	

章節標號	章節/測試名稱	測試目的	全盲滲透測試評估結果	
			適用	不適用
5.3.3.3	Wi-Fi 通訊協定異常輸入測試	查驗產品支援之Wi-Fi 通訊協定不存在其他資安漏洞。	✓	
5.3.3.4	Wi-Fi 認證安全機制設置測試	查驗產品支援IEEE 802.1X身分鑑別。	✓	
5.4	身分鑑別與授權機制安全測試			
5.4.1	鑑別機制安全測試			
5.4.1.1	鑑別機制強度測試	查驗產品具備安全之身分鑑別機制。	✓	
5.4.1.2	身分鑑別錯誤訊息測試	查驗產品鑑別錯誤訊息未揭露敏感性資料。	✓	
5.4.1.3	憑證更換功能測試	查驗產品具備憑證更換之功能。	✓	
5.4.1.4	金鑰唯一性測試	查驗產品之金鑰係唯一。	✓	
5.4.1.5	多因子鑑別機制測試	查驗產品之支援多因子鑑別之強身分鑑別機制。	✓	
5.4.1.6	裝置鑑別測試	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。	✓	
5.4.2	通行碼鑑別安全測試			
5.4.2.1	預設通行碼安全	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。	✓	
5.4.2.2	通行碼長度	查驗產品之最小通行碼長度是否足夠。	✓	
5.4.2.3	通行碼複雜度	查驗產品之通行碼複雜度是否足夠。	✓	
5.4.2.4	通行碼的輸入頻率及次數限制	查驗產品之通行碼鑑別機制具防止暴力破解之能力。	✓	
5.4.2.5	通行碼連續字元之避免	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。	✓	
5.4.2.6	通行碼歷程記錄	查驗產品具備通行碼歷程記錄功能，以確保其強度。	✓	
5.4.3	權限管控測試			
5.4.3.1	權限管控機制	查驗產品之資源存取具有權限管控機制。	✓	
5.4.3.2	權限有效時間	查驗產品存在有限的授權期限。	✓	

章節標號	章節/測試名稱	測試目的	全盲滲透測試評估結果	
			適用	不適用
5.5	隱私保護測試			
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	查驗產品之隱私權具有存取控制機制。	✓	
5.5.1.2	隱私外洩警示功能測試	查驗產品具有防止隱私外洩之功能。	✓	
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	查驗產品影像資料之傳輸，預設採用強度足夠之安全通道。	✓	
5.5.2.2	隱私資料之傳輸保護中階測試	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。	✓	
5.5.2.3	隱私資料之傳輸保護高階測試	查驗產品之影像資料傳輸，支援強加密演算法。	✓	

影像監控系統資安標準測試規範-第二部：網路攝影機(TAICS TS-0015-2 v3.0:2021)

5. 資安測試規範

TAICS TS-0015-2 v3.0:2021			全盲滲透測試評估結果	
章節標號	章節/測試名稱	測試目的	適用	不適用
5.1	實體安全測試			
5.1.1	實體埠之安全管控測試			
5.1.1.2	最小實體介面測試	查驗是否可徒手從產品外部取得儲存媒體。	✓	
5.1.2	實體異常行為警示測試			
5.1.3	實體防護測試			
5.1.3.2	實體保護測試	查驗產品是否建立外殼拆除障礙。	✓	
5.1.4	安全啟動測試			
5.2	系統安全測試			
5.2.1	作業系統安全與網路服務安全測試			
5.2.2	網路服務連接埠管控測試			
5.2.3	更新安全測試			
5.2.4	敏感性資料儲存安全測試			
5.2.5	網頁管理介面安全測試			
5.2.6	操控程式之應用程式介面安全測試			
5.2.6.1				

章節標號	章節/測試名稱	測試目的	全盲滲透測試評估結果	
			適用	不適用
5.2.7	日誌檔與警示測試			
5.3	通訊安全測試			
5.3.1	資料傳輸安全測試			
5.3.2	通訊協定與設置安全			
5.3.2.2	網路裝置資訊探詢功能測試	查驗產品是否運行在具安全風險的網路設定。	✓	
5.3.3	Wi-Fi 通訊安全			
5.4	身分鑑別與授權機制安全測試			
5.4.1	鑑別機制安全測試			
5.4.2	通行碼鑑別機制			
5.4.3	權限管控測試			
5.5	隱私保護測試			
5.5.1	隱私資料的存取保護測試			
5.5.1.2	影像隱私外洩防護測試	查驗產品是否具備選定監控範圍內不予以顯示的影像區塊。	✓	
5.5.2	隱私資料的傳輸保護測試			