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 v1.0:2018)

全盲(滲透性)測試適用項目一覽表

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	驗證是否可透過產品實體介面，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	驗證產品之實體埠是否有插拔紀錄。	✓	
5.1.2.2	實體異常狀態警示機制	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。	✓	
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	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。	✓	
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	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	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。	✓	
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	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。	✓	
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	驗證產品是否存在預期以外之網路埠。	✓	
5.2.3	更新安全測試			
5.2.3.1(a)	韌體檔案安全測試	驗證產品之韌體更新檔是否會洩露敏感性資料。	✓	

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
5.2.3.1(b)	韌體更新路徑的保護	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。	✓	
5.2.3.2	韌體更新檔之完整性及可信度測試	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。	✓	
5.2.3.3	備援更新功能測試	驗證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	產品敏感性資料的存取是否具有權限控管機制。		✓
5.2.4.2	敏感性資料加密儲存測試	驗證產品之敏感性資料於儲存狀態下是否加密保護。		✓
5.2.4.3	金鑰管理程序測試	確認產品的金鑰管理是否建立可靠管控程序。	✓	
5.2.4.4	敏感性資料隔離保護測試	確認產品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	驗證產品之網頁管理介面是否存在已知資安漏洞。	✓	
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			
5.2.6.1(a)	應用程式介面之鑑別機制強度測試	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。	✓	
5.2.6.1(b)	應用程式介面之身分鑑別錯誤訊息	驗證鑑別錯誤訊息不會造成敏感性資料的洩漏。		

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	應用程式介面之通行碼鑑別強度機制測試	驗證產品應用程式介面的通行碼鑑別機制強度是否足夠。	✓	
5.2.6.3	應用程式介面之權限管控機制	驗證產品的應用程式介面是否存在權限控管。	✓	
5.2.7	日誌檔與警示測試			
5.2.7.1	安全事件日誌檔測試	驗證產品是否有安全事件紀錄供查詢。	✓	
5.2.7.2	安全事件日誌檔存取權限管控測試	驗證產品之安全事件日誌紀錄是否具備權限控管。	✓	
5.2.7.3	安全事件日誌檔之日誌滾動功能測試	驗證產品是否具備處理日誌儲存空間不足之異常狀況。	✓	
5.2.7.4	異常警示功能測試	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。	✓	
5.3	通訊安全測試			
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	(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。	✓	
5.3.1.2	敏感性資料之傳輸保護中階測試	驗證傳輸敏感性資料之安全通道，是否支援強加密演算法。	✓	
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	確認產品是否運行在具安全風險的網路設定。	✓	
5.3.2.2	網路介面存取設置測試	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。		✓
5.3.2.3	通訊協定異常輸入測試	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。	✓	
5.3.3	Wi-Fi 通訊安全測試			

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
5.3.3.1	安全的Wi-Fi 組態設置測試	驗證產品是否存在錯誤的Wi-Fi 設定。	✓	
5.3.3.2	無線網路傳輸安全機制設置測試	驗證產品是否存在不安全的Wi-Fi 通道保護設定	✓	
5.3.3.3	Wi-Fi 通訊協定異常輸入測試7	驗證產品之 Wi-Fi 通訊協定是否存在未知之資安漏洞。	✓	
5.3.3.4	Wi-Fi 認證安全機制設置測試	驗證產品是否支援 IEEE 802.1X 認證。	✓	
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	驗證產品是否具備可靠之身分鑑別機制。	✓	
5.4.1.2	身分鑑別錯誤訊息	驗證鑑別錯誤訊息不會造成敏感性資料的洩漏。	✓	
5.4.1.3	憑證上傳介面測試	驗證產品是否具有提供憑證上傳的功能。	✓	
5.4.1.4	金鑰唯一性測試	驗證產品之金鑰是否唯一。	✓	
5.4.1.5	多因子鑑別機制測試	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。	✓	
5.4.1.6	裝置鑑別測試	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。	✓	
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	(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。	✓	
5.4.2.2	通行碼長度	驗證產品的通行碼長度是否足夠，以確保其強度。	✓	
5.4.2.3	通行碼複雜度	驗證產品的通行碼複雜度是否足夠，以確保其強度。	✓	

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
5.4.2.4	通行碼的輸入頻率及次數限制	驗證通行碼鑑別機制是否有防止暴力破解之能力。	✓	
5.4.2.5	通行碼連續字元之避免	驗證產品的通行碼是否存有連續字元，以確保其強度。	✓	
5.4.2.6	通行碼歷程記錄	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。	✓	
5.4.3	權限管控測試			
5.4.3.1	權限管控機制	驗證產品資源的存取是否具有權限控管機制。	✓	
5.4.3.2	權限有效時間	驗證產品是否存在有限的授權時間長度。	✓	
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	驗證產品隱私權否具有存取控制機制。	✓	
5.5.1.2	隱私資料刪除功能	驗證使用者擁有刪除自身隱私權的權限。	✓	
5.5.1.3	登入警示功能測試	驗證產品是否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	隱私資料的傳輸機密性初階保護	(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。	✓	
5.5.2.2	隱私資料的傳輸機密性中階保護	驗證傳輸隱私資料的安全通道，是否支援強加密演算法。	✓	

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 v2.0:2018)

全盲(滲透性)測試適用項目一覽表

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			
5.1.1.2	最小實體介面測試	驗證是否可輕易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	驗證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(ONVIF API)安全測試			
5.2.6.1	應用程式介面之鑑別機制測試			
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測試			
5.3.2.2	網路裝置資訊探詢功能測試	確認產品是否運行在具安全風險的網路設定。	✓	
5.3.3	Wi-Fi 通訊安全測試			
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	通行碼鑑別安全測試			
5.4.3	權限管控測試			

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
5.5	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	驗證產品是否具備選定監控範圍內不予以顯示的影像區塊。	✓	
5.5.2	隱私資料的傳輸保護測試			