無線網路攝影機

資通安全檢測技術指引

中華民國 107 年 8 月 29 日

目　次

1. 前言 1

2. 適用範圍 1

3. 引用標準 1

4. 用語釋義 2

5. 檢測方式及安全等級 3

6. 書面審查合格標準 4

7. 實機測試合格標準 6

表　次

表一、書面審查之檢測項目及對應安全等級 3
表二、實機測試之檢測項目及對應安全等級 3
表三、設備概述說明 8
表四、安全架構描述表 9
表五、安全功能介面表 11
表六、子系統描述與分類表 12

圖　次

圖一、模糊測試環境示意圖 6
圖二、使用者識別及鑑別功能測試環境示意圖 7

無線網路攝影機資通安全檢測技術指引

1. 前言

為確保具 Wi-Fi 連網功能之嵌入式網路攝影機（以下簡稱 IP CAM）之連網資安品質，爰訂定本指引。

2. 適用範圍

本指引適用於影像監控系統中具 Wi-Fi 連網功能之 IP CAM，亦適用同時具備有線及 Wi-Fi 連網功能之 IP CAM。

3. 引用標準

本指引參考標準如下，測試項目與相關國際標準對照詳附錄一。

3.1. ISO/IEC 15408（Common Criteria for Information Technology Security Evaluation， CC），Version 3.1. Revision 5，2017/04，CCRA。

3.2. Collaborative Protection Profile for Network Devices，Version 2.0，2017/05，NIAP。

3.3. Network Device Collaborative Protection Profile（NDcPP）Extended Package-Wireless Local Area Network（WLAN）Access Systems， Version 1.0，2015/05，NIAP。

3.4. Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations，Revision 4，2013/04，NIST。

3.5. Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements，Version 1.0，2017/07，UL 2900-1。

3.6. 影像監控系統資安標準—網路攝影機（TAICS TS-0014-2 最新版，以下簡稱 TS-0014-2），台灣資通產業標準協會。

4. 用語釋義

4.1. IEEE 802.1x

指在資料連結層上，鑑別使用者身分之網路安全標準。

4.2. 共同準則（Common Criteria，CC）

指國際資通安全產品評估及驗證之標準（ISO/IEC 15408），用以評估及驗證資通安全產品之安全等級與功能性，其評估保證等級（Evaluation Assurance Level，下稱 EAL）分為 7 個等級，最低等級為 EAL 1，最高等級為 EAL 7。

4.3. 評估標的（Target of Evaluation，TOE）

指待測物。

4.4. 保護剖繪（Protection Profile，PP）

指評估標的之安全基本需求文件。

4.5. 安全標的（Security Target，ST）

指評估標的符合保護剖繪或特定安全需求之規格文件。

4.6. 安全功能（TOE Security Functions，TSF）

指評估標的實現安全標的所列安全規格之功能。

4.7. 安全功能需求（Security Functional Requirement，SFR）

指依共同準則第二部份之安全需求規定描述安全功能，據以陳述評估標的具備之安全功能。

4.8. 安全功能介面（TOE Security Functions Interface，TSFI）

指評估標的用於實現安全功能需求所需對外溝通之介面。

4.9. 安全領域（Security Domain）

指評估標的實現安全功能需求時依不同權限所配分之資源。

4.10. 自我保護（Self-Protection）

指防護安全功能不被無關之程式碼或外力破壞之機制。

5. 檢測方式及安全等級

5.1. 檢測方式分為書面審查及實機測試。

5.1.1 書面審查之檢測項目包括設備概述、安全架構、安全功能規格、設計安全性。

5.1.2 實機測試之檢測項目包括基本要求、模糊測試、使用者識別及鑑別功能。

5.2. 安全等級依書面審查及實機測試之檢測項目之差異，分為初階、中階與高階三級。

5.3. 檢測項目及對應之安全等級如表一及表二，申請者應依待測物申請之安全等級檢附表一所列文件。

表一、書面審查之檢測項目及對應安全等級

檢測項目	應檢附文件	安全等級		
		初 階	中 階	高 階
設備概述	設備概述說明（表三）	6.1	6.1	6.1
安全架構	安全架構描述表（表四）	--	--	6.2
安全功能規格	安全功能介面表（表五）	--	--	6.3
設計安全性	子系統描述與分類表（表六）	--	--	6.4

表二、實機測試之檢測項目及對應安全等級

檢測項目	安全等級		
	初 階	中 階	高 階
基本要求	7.1.1 （TS-0014-2 安全等級 1 級）	7.1.2 （TS-0014-2 安全等級 1 級與 2 級）	7.1.3 （TS-0014-2 安全等級 1 級、2 級與 3 級）
模糊測試	7.2.1	7.2.2	7.2.3
使用者識別及鑑別功能	--	--	7.3.1

6. 書面審查合格標準

6.1 設備概述

設備概述說明（如表三）應載明下列事項：

（1）設備名稱、廠牌、型號。

（2）申請者名稱（製造商、進口商、經銷商）。

（3）製造商名稱。

（4）軟體、韌體版本。

（5）通訊介面。

（6）安全功能，申請高階安全等級之代測物應符合 TS-0014-2 安全啟動之要求。

（7）外觀：檢附待測物 4x6 吋以上之彩色照片或圖片彩色照片，其廠牌及型號須清晰可辨讀，並包含樣品之頂視圖、底視圖、左視圖、右視圖、正視圖及背視圖。

6.2 安全架構

安全架構描述表（如表四）應載明下列事項：

（1）因執行安全功能所區隔之安全領域。

（2）安全功能之安全初始程序。

（3）安全功能之自我保護機制。

（4）安全功能執行如何避免被繞道。

6.3 安全功能規格

安全功能介面表（如表五）應載明下列事項：

（1）安全功能介面名稱。

（2）目的。

（3）可實現的安全功能需求。

（4）操作方式。

（5）參數。

（6）執行動作。

（7）錯誤訊息。

6.4 設計安全性

子系統描述與分類表（如表六）應載明下列內容：

（1）子系統名稱。

（2）目的。

（3）子系統隸屬之安全功能介面。

（4）子系統行為說明。

7. 實機測試合格標準

7.1. 基本要求

7.1.1. 初階基本要求：應符合 TS-0014-2 安全等級 1 級之規定。

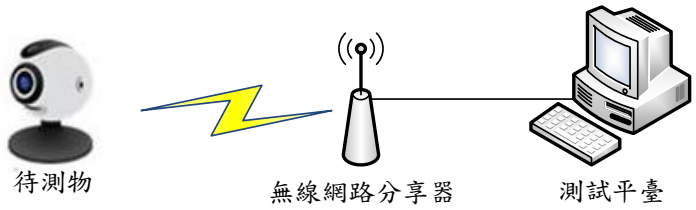
7.1.2 中階基本要求：應符合 TS-0014-2 安全等級 1 級與 2 級之規定。

7.1.3 高階基本要求：應符合 TS-0014-2 安全等級 1 級、2 級與 3 級之規定。

7.2. 模糊測試

7.2.1 初階模糊測試

（1）測試環境：使用 Wi-Fi 方式連接測試平臺與待測物，提供測試人員直接透過測試平臺進行模糊測試。（示意圖如圖一）



圖一、模糊測試環境示意圖

（2）測試方法：在測試平臺使用模糊測試工具（參考附錄二），對待測物進行 5,000 筆隨機樣本之測試，並將結果儲存在測試平臺。前述隨機樣本至少應包含 IEEE 802.11i 標準下產生變異樣本。

（3）判定標準：測試過程中待測物應正常運作，且不得重新開機。

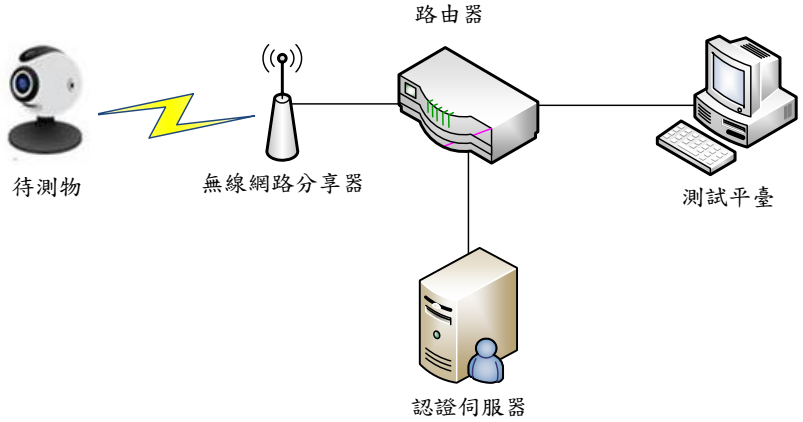
7.2.2 中階模糊測試：測試環境、測試方法及判定標準依 7.2.1 之規定，但模糊測試之隨機樣本增加至 7,000 筆。

7.2.3 高階模糊測試：測試環境、測試方法及判定標準依 7.2.1 之規定，但模糊測試之隨機樣本增加至 10,000 筆。

7.3. 使用者識別及鑑別功能測試

7.3.1 高階 802.1x 使用者識別及鑑別功能測試

（1）測試環境：使用有線網路線將路由器與測試平臺、認證伺服器及 Wi-Fi AP 連接，供測試人員於測試平臺觀察待測物是否與認證伺服器成功連線。（示意圖如圖二）



圖二、使用者識別及鑑別功能測試環境示意圖

（2）測試方法：

A.開啟待測物之 802.1x 存取鑑別功能。

B.透過測試平臺觀察是否可瀏覽待測物所攝影之視訊或捕捉之靜態圖像。（測試工具之名稱及應具備功能，可參考附錄二測試工具應備功能及要求說明表）

（3）判定標準：通過認證伺服器鑑別後，測試平臺可瀏覽待測物在測試期間所攝影之視訊或捕捉之靜態圖像。

表三、設備概述說明

設備名稱		
廠牌		
型號		
申請者 （公司、商號名稱）	□製造商 □進口商 □經銷商	
製造商		
軟體、韌體版本		
通訊介面		
安全功能		
外觀		

表四、安全架構描述表

項目	說明	申請者填寫內容
1.安全領域	列出各安全功能介面對應之安全領域名稱，並在安全功能操作環境及內部執行限制下，如何區隔所需保護的資料。 *範例：TSFI_GUI:* *Domain_SecureLogAudit* *Domain_SecureConnection* *透過 TSFI_GUI 來執行管理功能時，該 TSFI 同一時間只能有單一遠端連線，並只能執行單一稽核資料處理請求。*	
2.初始程序	操作待測物的相關元件/環境 *範例：待測物網路連接程序* 提供安全啟動待測物之相關元件起始步驟及安裝程序。 *範例：* *1. 從端口標記為 0/0（ethernet0/0 接口）連接一個 RJ-45 電纜到交換機或路由器 Trust 安全區。* *2. 從端口標記為 0/1（ethernet0/1 接口）連接一個 RJ-45 電纜到交換機或路由器中的 DMZ 安全區。*	
3.自我保護機制	1. 自我保護功能 列出各安全功能介面對應之自我保護機制 *範例：TSFI_WEB* *自我保護 1:身分驗證* *自我保護 2:遠端連線加密* 2. 與外部設備之關係 說明安全功能及其介面與外部設備之資料交換動作 *範例：遠端以瀏覽器連線待測物進行管理功能時，以 TSFI_WEB GUI 介面進行身分認驗證*	

	3. 自我保護機制說明 安全功能介面提供實體上或邏輯上的自我保護機制 *範例：* *（1）應輸入通行碼才能進入介面。* *（2）資料傳輸機制：TLS/SSL。* *（3）特殊執行方式：指紋辨識。* *（4）特殊設備需求：指紋辨識器。*	
4.防止繞道	1. 列出各安全功能對應之防止繞道機制 *範例：TSF_Authentication 身分驗證功能* 2. 列舉可能繞道之手法 *範例：可能直接以維護介面不經身分鑑別操控待測物。* 3. 說明防範作法，包含進入安全功能的介面如何被保護、執行階段的資料處理如何保護、是否存有其他對外通道及相關防範非法進入之機制等。 *範例：防範作法為以實體封鎖方式，防止利用維護介面繞道身分鑑別程序。*	

表五、安全功能介面表

項目	項目說明	申請者填寫內容
1.安全功能介面名稱	列出所有安全功能介面。 *範例：TSFI_CLI*	
2.目的	說明各安全功能介面之安全功能目的。 *範例：提供命令列模式操作介面*	
3.可實現的安全功能需求	說明各安全功能介面如何實現表二所列之實機測試檢測項目。 *範例：SFR_安全管理：提供安全管理功能*	
4.操作方式	說明如何使用各安全功能介面。 *範例：以 ssh 連接待測物，即提供命令列模式操作介面*	
5.參數	說明各安全功能介面所有參數及其意義。 *範例：ID & password*	
6.執行動作	說明各安全功能介面如何運作及其執行細節。 *範例：可下達管理命令操作待測物*	
7.錯誤訊息	說明執行各安全功能介面產生之錯誤訊息，包含其意義及產生條件。 *範例：連接失敗、鑑別失敗*	

表六、子系統描述與分類表

項目	項目說明	申請者填寫內容
1.子系統名稱	列出各安全功能介面之子系統。 *範例：Subsystem_ssh*	
2.目的	說明各子系統之安全功能目的。 *範例：提供 ssh 服務*	
3.子系統隸屬之安全功能介面	說明各子系統隸屬於表五所列之安全功能介面。 *範例：TSFI_CLI*	
4.子系統行為說明	說明各子系統行為如下： 1. 如何實現安全功能介面的功能。 *範例:提供 TSFI_CLI 命令列模式操作介面* 2. 與其他子系統間互動之資訊，包含不同子系統間的溝通以及傳遞資料的特性。 *範例：與其他子系統之互動：* *（1）Subsystem_auth: 傳遞鑑別資訊給 Subsystem_auth，並由回覆訊息確認鑑別是否成功* *（2）Subsystem_terminal: ...*	

附錄一、實機測試項目與國際標準對照表

檢測項目	審查標準	參考來源	參考內容
基本要求	本指引 7.1.1、7.1.2、7.1.3	TAICS TS-0014-2	
模糊測試	本指引 7.2.1、7.2.2、7.2.3	NIST Special Publication 800-53Security and Privacy Controls for Federal Information Systems and Organizations	SA-11 DEVELOPER SECURITY TESTING AND EVALUATION (8) DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS
		UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	15 Malformed Input Testing
使用者識別及鑑別功能	本指引 7.3.1	NIAP Network Device Collaborative Protection Profile（NDcPP）Extended Package-Wireless Local Area Network（WLAN）Access Systems	FTP_ITC.1 Inter-TSF Trusted Channel

附錄二、測試工具應備功能及要求說明表

檢測項目	測試工具	
	工具名稱	具備功能
模糊測試	模糊測試工具	（1）可隨機產生不同測試案例。 （2）可針對 IEEE 802.11i 協定產生模糊測試案例。
使用者識別及鑑別功能	不適用。	須架設認證伺服器