

# 物聯網產品輔導介紹與案例 分享

財團法人台灣電子檢驗中心資通部

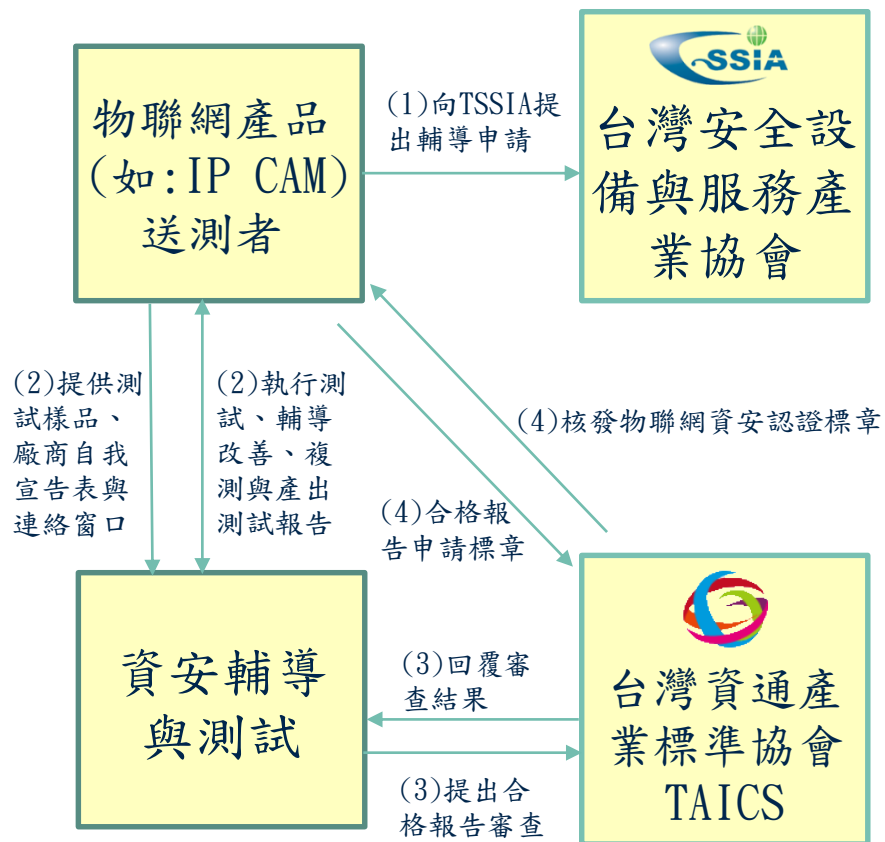
葉錫勳

2019年3月27日

# 簡 報 目 錄

- 一、 物聯網產品資安輔導、測試與驗證流程
- 二、 廠商自我宣告表填寫
- 三、 案例分享

# 一、物聯網產品資安輔導、測試與驗證流程



## (1) 向TSSIA提出測試申請

- 物聯網產品(如:IP CAM、NVR/DVR、NAS)業者向TSSIA提出受輔導標的申請。

## (2) 執行測試、輔導改善、複測與產出測試報告

- 確認所有相關文件與送測標的均取得，開始測試
- 輔導改善：提供相關改善建議予廠商
- 複測：廠商經改善後再提供新版韌體進行複測。

## (3) 向TAICS申請物聯網資安認證

- 交付相關文件：合格檢測報告。
- TAICS回覆審查結果。

## (4) 取得物聯網資安認證標章

- 當合格報告經TAICS審查通過，則實驗室寄送合格報告給廠商。
- 廠商提出相關文件(含由TAICS審查通過的合格報告)向TAICS申請物聯網資安認證標章。
- TAICS核發物聯網資安認證標章給廠商。

## 二、廠商自我宣告表填寫

填寫符合、不符合、部分符合或不支援等

針對該資安要求補充說明更詳細資訊，供實驗室判斷

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.1.1.1	產品僅提供使用者有限權限之設計，即預設不應透過實體介面存取產品作業系統之除錯模式	1級			產品須於文件中說明進入作業系統除錯模式之方法。
5.1.1.2	卸除式儲存媒體使用的插槽須移除；抑或卸除式儲存媒體支援儲存媒體保護機制，即產品之儲存媒體不應在本機以外的機器被存取。	2級(IP CAM)			

## 二、廠商自我宣告表填寫

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.1.3.2	產品須採用一體成形或防拆螺絲等機殼防拆除保護設計。	2級(IP CAM)	部分符合	有部分使用防拆螺絲,使用一般的十字或一字螺絲起子是無法拆的	
5.1.4.1	產品應支援安全啟動(Secure Boot)功能，不應以未經授權的韌體、驅動程式及作業系統執行開機，以確保系統的完整性及可信度。	3級	範例		1. 產品須提供完整韌體檔案。 2. 產品須提供韌體寫入軟體。  具備安全啟動功能證明之書面資料。 產品在開機過程中是否驗證韌體與作業系統的簽章。

## 二、廠商自我宣告表填寫

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.2.1	產品開啟之網路服務須為廠商提供必要服務之所需，防止產品因啟用網路介面而被侵入的可能性，且廠商須於產品文件中標註得啟用之網路服務，避免未宣告之網路服務被開啟。	1級	部分符合	我們會列出"預設開啟"那些網路服務於手冊，但是https的port, 我們預設不開, 所以不放在這個列出的清單. 而是在其他章節提到, 但是使用者可以透過後台打開	產品須提供所啟用之網路服務與對應埠之宣告。
5.2.3.1(a)	產品若支援離線手動更新，則更新檔案須加密保護以確保機密性，且須採用FIPS 140-2 Annex A [14] 所核可之加密演算法；抑或是產品韌體之程式碼與安裝檔內其它檔案中，不應存在明文或甚至可被解密回復之敏感性資料。	1級	不符合	範例	1. 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. 若韌體檔案經過加密處理，則廠商須提供解密工具。 3. 產品須提供所有相連伺服器之宣告。

## 二、廠商自我宣告表填寫

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.3.1(b)	產品若支援線上更新，其更新路徑須通過安全通道，且安全通道版本須符合「附錄A」的要求，同時金鑰交換協議應支援前向安全功能(Forward Secrecy)，其中於身分鑑別過程須驗證憑證合法性，以及有效性(如：發證單位、有效期限、格式錯誤及憑證簽章等)。	1級	不支援	不支援線上更新	
			範例		
5.2.3.2	產品必須具備驗證韌體之正確性及完整性的功能。	1級	不符合	請實驗室建議合適的機制	需對該韌體更新檔重新簽章，驗證完整性與可信度。

## 二、廠商自我宣告表填寫

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.3.3	產品必須具備備援更新功能，即發生更新失敗時，系統能回復正常運作。	1級	部分符合	如果firmware上傳失敗，系統無影響	
5.2.4.1	產品所儲存的敏感性資料，須被授權的個體始可存取。	1級	部分符合	目前只有admin可以看到敏感性資料	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。 (通行碼資料保存方式、加解密金鑰保存方式)
5.2.4.2	產品所儲存之身分鑑別因子、加解密用之金鑰(不含非對稱加密用之公鑰)及個人資料不應明文儲存，而保護資料的加密方式須採用FIPS 140-2 Annex A所核可之加密演算法。	1級	不符合	Android有提供disk encryption的功能，但目前尚不確定是否符合標準，需實驗室協助確認	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。

範例



## 二、廠商自我宣告表填寫

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.4.3	產品須提出金鑰管理程序，以確保金鑰管理的品質。	2級	不符合	不支援線上更新	產品須提供金鑰管理程序之說明文件。
5.2.4.4	敏感性資料須存放於產品的安全區域(Security Domain)，從正常作業環境中隔離。	3級	不符合	範例	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。
5.2.6.1	應用程式介面，須具備身分鑑別機制，且其鑑別機制安全依5.4.1.1及5.4.1.2之要求。	1級			

## 二、廠商自我宣告表填寫

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.7.1	須具備安全事件記錄與顯示功能，確實記錄使用者的存取行為，得以查核未授權或異常的登入操作。其內容須包括完整時間戳記、使用者身分及及執行結果，供後續查閱之用。	1級	部分符合	產品具有可供使用者檢視之安全事件日誌功能。(O) 安全事件日誌的資料包含正確時間(包括年、月、日、時、分、秒)、使用者身分及登入行為。(X) 重開機前之安全事件紀錄仍可查詢。(X)	產品須提供金鑰管理程序之說明文件。
5.2.7.2	產品之安全事件紀錄須具備權限控管機制，該日誌檔不應允許未經授權的存取。	1級	部分符合	產品須提供日誌檔存取權限說明。(X) 安全事件日誌檔的身分授權與產品自我宣告相符。使用Guest帳號登入時無查看相關日誌的權限。(O)	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。

範例

## 二、廠商自我宣告表填寫

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.7.3	產品之安全事件日誌檔須具備日誌滾動(log rotate)機制。	1級	符合	目前提供1G log儲存空間	
5.2.7.4	產品須提供系統警示功能以避免安全事件紀錄無法儲存之狀況發生。	2級	不支援	舊的日誌檔會被自動清除，所以無需示警	
5.3.1.1	敏感性資料之網路傳輸預設須通過安全通道，且安全通道版本須符合「附錄A」的要求，同時金鑰交換協議應支援前向安全功能(Forward Secrecy)，其中於身分鑑別過程須驗證憑證合法性，以及有效性(如：發證單位、有效期限、格式錯誤及憑證簽章等)。	1級	範例		
5.3.2.1	產品須提供使用者得自行開/關「網路裝置資訊探詢」功能，包括：通用隨插即用通訊協定(UPnP)、簡單網路管理協定(SNMP)及零配置通訊協定(Bonjour)。	1級	不支援	產品不支援upnp, snmp and Bonjour.	產品須提供所支援網路服務之說明文件。

## 二、廠商自我宣告表填寫

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.3.2.2	預設不應透過網路連線存取產品作業系統之除錯模式。	1級	不符合		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。
5.3.2.2	產品所提供之自行開/關「網路裝置資訊探詢」功能，預設須為關閉，包括：通用隨插即用通訊協定(UPnP)、簡單網路管理協定(SNMP)及零配置通訊協定(Bonjour)。	3級(IP CAM)	不支援	產品不支援upnp, snmp and Bonjour.	
			範例		
5.3.2.3	產品之關鍵通訊協定(見附錄B)，不應存在錯誤處理漏洞，包括檢視訊息長度、訊息識別碼及關鍵協定屬性欄位，導致產品因發生崩潰而服務中止的情形。	2級			
5.4.1.3	產品應具備上傳憑證之功能，以增加憑證鑑別機制之可信度。	2級			產品須提供金鑰管理程序之說明文件。

## 二、廠商自我宣告表填寫

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.4.1.4	產品每一次還原出廠設定時，憑證之金鑰(包括SSH及TLS)都須改變，確保每台產品金鑰之唯一性，及降低金鑰外洩可能引發之資安風險。	2級	範例		
5.4.2.1	廠商所生產之裝置，其預設通行碼都須相異；抑或首次成功取得產品存取之授權，須強制更改預設通行碼。	1級		會提醒使用者修改預設密碼，但無強制規定修改	
5.4.3.2	產品之授權行為，須存在閒置時限供使用者設定，假如遠端連線逾時、遺失或結束，須要求新的鑑別。	1級	部分符合	使用者可以確實登出產品。 (O) 產品之授權行為，存在閒置時限供使用者設定。(X) 遠端連線逾時、遺失或結束，要求新的身分鑑別。(O)	

## 二、廠商自我宣告表填寫

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.5.1.1	產品所儲存的隱私資料，須被授權的個體始可存取	1級	部分符合	產品須提供隱私存取權限之宣告。 產品所儲存的隱私資料，具備權限管控機制，該使用者的隱私存取授權與產品自我宣告相符。(?) 至少擁有二個以上不同權限的角色。(O)	
5.5.1.2	使用者對其儲存的隱私資料擁有刪除之權限和功能。	1級	部分符合	範例	
5.5.1.2	產品應支援隱私遮罩，避免正常作業引發之隱私外洩風險。	2級(IP CAM)	不符合		
5.5.1.3	每次發生新的存取事件時，產品必須主動發出警示。	1級	不符合	不清楚要如何主動發出警示，需要實驗室提供建議	
5.5.2.1	隱私資料傳輸機密性依「5.3.1.1敏感性資料傳輸安全」該節之要求。	1級			

## 三、 案例分享

### 範例1：5.2.3.1(a) – 情境1

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.3更新安全測試	5.2.3.1(a) 韌體檔案安全測試	1級	驗證產品之韌體更新檔是否會洩露敏感性資料。	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。

情境1：

測試方法：

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. 審閱可證明所使用加密演算法之書面資料。

預期結果：

- 韌體更新檔案無法被解析出檔案系統目錄。
- 加密演算法採用FIPS 140-2 Annex A [2]所認可。

## 三、 案例分享

### 範例1：5.2.3.1(a) – 情境2

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.3更新安全測試	5.2.3.1(a) 韌體檔案安全測試	1級	驗證產品之韌體更新檔是否會洩露敏感性資料。	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。

情境2：

測試方法：

1. 使用具韌體拆解功能之工具，對產品之韌體進行拆解。
2. 取出檔案系統之路徑目錄。
3. 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)。
4. 確認金鑰是否可被擷取。
5. 確認是否存在非公開之email 資料。
6. 確認是否存在產品所宣告之相連伺服器外之IP 或URL資料。

預期結果：

- 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。
- 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。
- 不存在非公開email 資料。
- 不存在產品所宣告相連伺服器外之IP 與URL資料。



## 三、 案例分享

### 範例2 : 5.2.6.1

安全要求分項	測試項目	安全等級	測試目的	樣品條件
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	1級	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。	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。

#### 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，開啟具ONVIF API之操控程式。
3. 透過操控程式與產品建立連線，同時側錄封包。
4. 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。
5. 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。
6. 檢視鑑別結果是否成功。

#### 預期結果：

- 存取產品經過身分鑑別。
- 重送攻擊失敗。

## 三、 案例分享

### 範例3 : 5.2.7.1

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.7系統日誌檔與警示測試	5.2.7.1安全事件日誌檔測試	1級	驗證產品是否有安全事件紀錄供查詢。	無

#### 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。

#### 預期結果：

- 產品具有可供使用者檢視之安全事件日誌功能。
- 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。
- 重開機前之安全事件紀錄仍可查詢。

## 三、 案例分享

### 範例4 : 5.3.1.1

安全要求分項	測試項目	安全等級	測試目的	樣品條件
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級	(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。	(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。

#### 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。

#### 預期結果：

- 安全通道僅支援「附錄 A」中所建議之密碼套件。
- 與測試電腦之間的帳號密碼資訊傳輸，預設採用安全通道。
- 與行動裝置之間的帳號密碼資訊傳輸，預設採用安全通道。
- 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。

## 三、 案例分享

### 範例5 : 5.3.2.3

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.3.2網路介面通訊協定的安全設置測試	5.3.2.3通訊協定異常輸入測試	2級	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。	無

#### 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。

#### 預期結果：

- 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)。

#### 註：

B1：即時傳輸協定 (Real-time Transport Protocol, RTP) & 即時傳送控制協定 (Realtime Transport Control Protocol, RTCP)

B2：即時串流協定 (Real Time Streaming Protocol, RTSP)

B3：傳輸層安全協定 (The Transport Layer Security, TLS)

## 三、 案例分享

### 範例6 : 5.4.1.4

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.4.1鑑別機制安全測試	5.4.1.4金鑰唯一性測試	2級	驗證產品之金鑰是否唯一。	產品須提供可與其相連之影像監控裝置。

#### 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。

#### 預期結果：

- 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。
- 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。
- 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。

## 三、 案例分享

### 範例7 : 5.5.2.1

安全要求分項	測試項目	安全等級	測試目的	樣品條件
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級	(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。	無

#### 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。

#### 預期結果：

- 安全通道僅支援「附錄A」中所建議之密碼套件。
- 與測試電腦之間的影像資料傳輸，預設採用安全通道。
- 與行動裝置之間的影像資料傳輸，預設採用安全通道。
- 已竄改影像傳輸用之安全通道憑證未通過產品認證。

# 簡報結束 敬請指教

資訊與通信技術服務部

葉錫勳

E-mail : [eacn@etc.org.tw](mailto:eacn@etc.org.tw)

電話：03-3280026轉621

王煜詔

E-mail : [taichi@etc.org.tw](mailto:taichi@etc.org.tw)

電話：03-3280026轉562

