

# 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

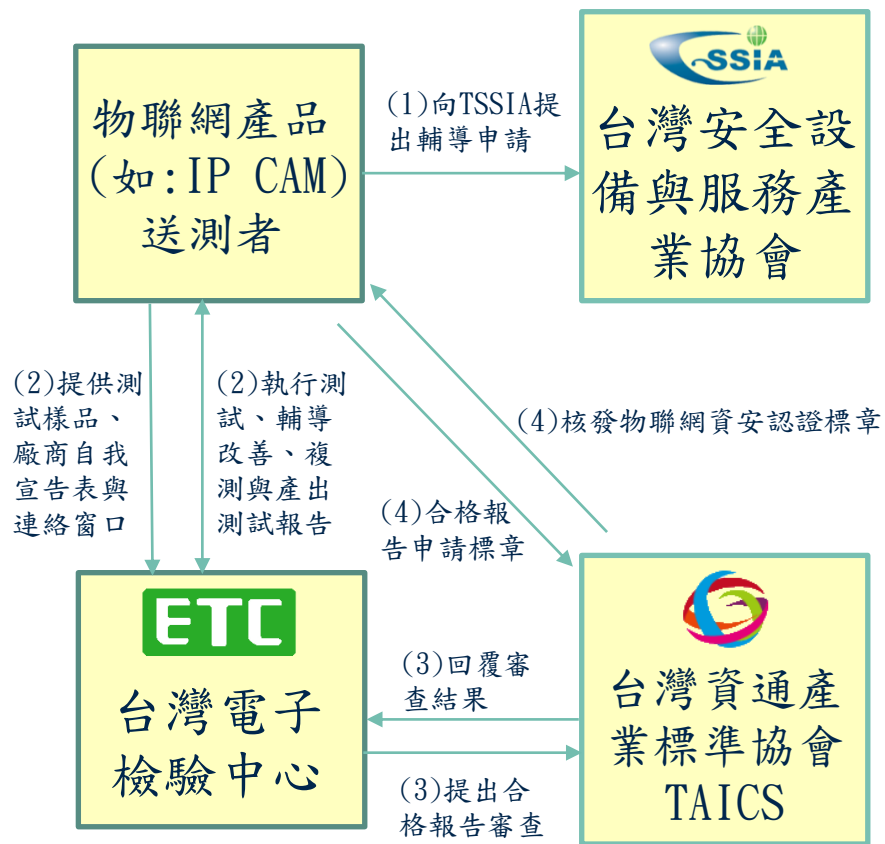
葉錫勳

2020年5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         |        |                               | 1. 產品須提供完整韌體檔案。<br>2. 產品須提供韌體寫入軟體。<br><br>具備安全啟動功能證明之書面資料。<br>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    |   | 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。<br>2.若韌體檔案經過加密處理，則廠商須提供解密工具。<br>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     |                         |
| 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。<br>(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。                       |



## 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    |         | 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。<br>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)<br>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)<br>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)<br>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。<br>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。 |

## 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   |        |                              |                    |
| 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. |                              |
| 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   |        |  |    |
| 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   | 部分符合   | 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)<br>產品之授權行為，存在閒置時限供使用者設定。(X)<br>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。<br>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。(?)<br>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   |  |    |
| 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

### 測項：5.1.1.1

| 安全要求分項          | 測試項目               | 安全等級 | 測試目的                       | 樣品條件  |
|-----------------|--------------------|------|----------------------------|---|
| 5.1.1實體埠之安全管控測試 | 5.1.1.1 實體介面安全管控測試 | 1級   | 驗證是否可透過產品實體介面，存取作業系統之除錯模式。 | (1) 產品須保持出廠預設環境狀態。<br>(2) 產品須於文件中說明進入作業系統除錯模式之方法。 |

#### 測試方法：

1. 根據文件所述進入作業系統除錯模式之方法，開啟相應之管理介面連接工具。
2. 測試電腦連接產品之 USB 埠。
3. 確認可否透過 USB 埠存取作業系統之除錯模式。
4. 若存取前須經通行碼鑑別程序，則依照 5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4 測試通
5. 測試電腦連接產品之 UART 埠。
6. 確認可否透過 UART 埠存取作業系統之除錯模式。
7. 若存取前須經通行碼鑑別程序，則依照 5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4 測試通
8. 行碼鑑別機制之安全性。

#### 預期結果：

- 透過 USB 存取作業系統之除錯模式時，產品要求身分鑑別。
- 透過 USB 存取作業系統之除錯模式時，若要求通行碼鑑別，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。
- 透過 UART 存取作業系統之除錯模式時，產品要求身分鑑別。
- 透過 UART 存取作業系統之除錯模式時，若要求通行碼鑑別，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。
- 產品若不存在進入作業系統除錯模式之介面，則此測項為「通過」。

### 三、 案例分享

#### 範例：5.1.1.1

**說明：**若存在USB、UART存取作業系統之除錯模式時，通行碼鑑別機制符合以下之測試預期結果。

5.4.2.1：是否有相同預設通行碼或首次上線後強制要求更改。

5.4.2.2：驗證通行碼長度。

5.4.2.3：驗證通行碼複雜度。

5.4.2.4：驗證通行碼的輸入頻率及次數限制。

**可行作法：**有些通過的廠商會將密碼管控機制做在web頁面。



## 三、 案例分享

### 測項：5.1.2.2

| 安全要求分項          | 測試項目              | 安全等級 | 測試目的                          | 樣品條件 |
|-----------------|-------------------|------|-------------------------------|------|
| 5.1.2實體異常行為警示測試 | 5.1.2.2實體異常狀態警示機制 | 2級   | 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。 | 無。   |

#### 測試方法：

1. 根據產品使用說明。
2. 將網路線拔除或天線遮罩，使主機因訊號中斷而無法連接上網路。
3. 檢視產品是否依照使用說明達到警示效果。

#### 預期結果：

- 發生斷訊狀況時，產品發出警示。

### 三、 案例分享

#### 範例：5.1.2.2

##### 說明：

- 需主動發出警示，例如：聲音、彈跳視窗、推播通知、警示燈。
- 以實體手法中斷網路通訊時，產品**必須**主動發出警示，讓使用者知曉。

### 三、 案例分享

#### 測項：5.2.2.1

| 安全要求分項           | 測試項目             | 安全等級 | 測試目的              | 樣品條件  |
|------------------|------------------|------|-------------------|---|
| 5.2.2網路服務連接埠管控測試 | 5.2.2.1網路服務最小化測試 | 1級   | 驗證產品是否存在預期以外之網路埠。 | (1) 產品須保持出廠預設環境狀態。<br>(2) 產品須提供所啟用之網路服務與對應埠之宣告。 |

#### 測試方法：

1. 將測試電腦連接產品。
2. 啟動具網路埠掃描功能之工具，對產品執行 TCP 與 UDP 埠 0~65535 之掃描。
3. 目視掃描結果所呈現之網路服務與對應埠。
4. 比對產品自我宣告中所聲明之網路服務與對應埠。

#### 預期結果：

- 產品所開啟之網路服務與對應埠，與產品自我宣告之內容相符。

### 三、 案例分享

#### 範例：5.2.2.1

##### 說明：

1. 自我宣告須詳細記載所開啟的網路服務與對應埠。若有特殊情形：例如有開放卻未被掃出、隨機產生埠號等，應說明其功能與原因。
2. 自行檢測指令(使用nmap為例)：  
nmap -p 0-65535 <ipcam ip>  
nmap -sU -p 0-65535 <ipcam ip>

## 三、 案例分享

### 測項：5.2.3.1

| 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。 | <p>(1) 情境 1:</p> <ul style="list-style-type: none"> <li>(i)適用韌體檔案加密保護強度測試。</li> <li>(ii)產品須支援離線更新，否則不適用此測項。</li> <li>(iii)產品須提供所使用之韌體檔案。</li> <li>(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。</li> </ul> <p>(2) 情境 2:</p> <ul style="list-style-type: none"> <li>(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。</li> <li>(ii)產品須提供所使用之韌體檔案。</li> <li>(iii)若韌體檔案經過加密處理，則廠商須提供解密工具。</li> <li>(iv)產品須提供所有相連伺服器之宣告。</li> </ul> |

#### 測試方法：

##### (1)情境 1:

- (i)使用具韌體拆解功能之工具，對產品之韌體進行拆解。
- (ii)檢視該韌體更新檔是否可被解析出檔案系統目錄。
- (iii)審閱可證明所使用加密演算法之書面資料。

#### 預期結果：

##### (1)情境 1

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

## 三、 案例分享

### 測項：5.2.3.2

| 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 | 5.2.3.2韌體更新檔之完整性及可信度測試 | 1級   | 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。 | (1) 產品須提供其數位簽章使用機制。<br>(2) 產品須提供所使用之韌體檔案。 |

#### 測試方法：

- (1) 對韌體更新檔重新簽章。
- (2) 執行產品更新，並檢視更新是否成功

#### 預期結果：

- 產品更新失敗

## 三、 案例分享

### 測項：5.2.4.1

| 安全要求分項           | 測試項目               | 安全等級 | 測試目的                  | 樣品條件                       |
|------------------|--------------------|------|-----------------------|----------------------------|
| 5.2.4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 | 1級   | 產品敏感性資料的存取是否具有權限控管機制。 | 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。 |

#### 測試方法：

(i) 審閱能證明符合此安全要求之書面資料。

#### 預期結果：

- (i) 產品通行碼資料之權限管控與產品自我宣告相符。
- (ii) 產品之加解密金鑰之權限管控與產品自我宣告相符。
- (iii) 該權限管控機制至少擁有二個以上不同權限的角色。

## 三、 案例分享

### 測項：5.2.4.2

| 安全要求分項           | 測試項目               | 安全等級 | 測試目的                    | 樣品條件  |
|------------------|--------------------|------|-------------------------|---|
| 5.2.4敏感性資料儲存安全測試 | 5.2.4.2敏感性資料加密儲存測試 | 1級   | 驗證產品之敏感性資料於儲存狀態下是否加密保護。 | (i)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。<br>(ii)產品須提供系統管理者權限供測試用。<br>(iii)產品須提供能進入作業系統層之介面。 |

#### 測試方法：

- (i)審閱能證明符合此安全要求之書面資料。
- (ii)將測試電腦連接產品。
- (iii)檢視保護通行碼資料所採用的保密機制。
- (iv)檢視保護加解密金鑰所採用的保密機制

#### 預期結果：

- (i)通行碼資料的保密機制採用 FIPS 140-2 Annex A 所核可之單向雜湊函數(one way hash)。
- (ii)加解密用金鑰的保密機制採用 FIPS 140-2 Annex A 所核可之加密演算法。



## 三、 案例分享

### 範例：5.2.4.2

#### 說明：

廠商提供韌體加解密用之金鑰保密機制

1. 保存方式：韌體加解密金鑰保存於韌體中，無法被讀取。
2. 韌體加解密用之金鑰保密機制是否符合FIPS 140-2 Annex A所核可之加密演算法？

Annex A:  
Approved Security Functions  
for FIPS PUB 140-2,  
*Security Requirements for  
Cryptographic Modules*

June 10, 2019

Draft

Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899-8930



U.S. Department of Commerce  
Penny Pritzker, Secretary

National Institute of Standards and Technology  
Willie E. May, Under Secretary for Standards and Technology and Director

## 三、 案例分享

### 測項：5.2.5.1

| 安全要求分項              | 測試項目                              | 安全等級 | 測試目的                           | 樣品條件              |
|---------------------|-----------------------------------|------|--------------------------------|-------------------|
| 5.2.5網頁管理<br>介面安全測試 | 5.2.5.1網頁管<br>理介面常見<br>資安風險測<br>試 | 1級   | 驗證產品之網頁管<br>理介面是否存在已<br>知資安漏洞。 | 產品須提供系統管理者權限供測試用。 |

#### 測試方法：

- (1) 將測試電腦連接產品。
- (2) 開啟網頁管理介面，檢視網頁是否使用超文本傳輸協定。
- (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。

#### 預期結果：

- 產品之網頁管理介面，不存在引發 OWASP web Top 10 [3]之 Injection 及 XSS 資安攻擊風險

## 三、 案例分享

### 範例：5.2.5.1

#### 常見問題與改善方式：

- 1.關於X-XSS-Protection，需要於WebServer加入Header設定  
X-XSS-Protection:1; mode=block。
- 2.關於X-Content-Type-Options，需於WebServer加入Header設定  
X-Content-Type-Options:nosniff

### 三、 案例分享

#### 測項：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：

- (i)將測試電腦或行動裝置連接產品。
- (ii)根據產品使用說明，開啟具 ONVIF API 之操控程式。
- (iii)透過操控程式與產品建立連線，同時側錄封包。
- (iv)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。
- (v)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。
- (vi)檢視鑑別結果是否成功。

#### 預期結果：

- (i)存取產品經過身分鑑別。
- (ii)重送攻擊失敗。

### 三、 案例分享

#### 測項：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：

1. 產品具有可供使用者檢視之安全事件日誌功能。
2. 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。
3. 重開機前之安全事件紀錄仍可查詢。

## 三、 案例分享

### 測項：5.2.7.3

| 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日誌檔與警示測試 | 5.2.7.3安全事件日誌檔之日誌滾動功能測試 | 1級   | 驗證產品是否具備處理日誌儲存空間不足之異常狀況。 | 產品須提供系統管理者權限供測試用。 |

#### 測試方法：

- (1) 不斷觸發安全事件日誌，以填充安全事件紀錄儲存容量，直到儲存空間不足。
- (2) 檢視產品是否無法正常記錄安全事件。

#### 預期結果：

- (1) 產品不會發生儲存空間不足的現象。
- (2) 產品仍可正常記錄安全事件

## 三、 案例分享

範例：5.2.7.3

說明：

須提供安全日誌滾動機制的設計說明。(例如：儲存容量、日誌滾動機制等)

## 三、 案例分享

### 測項：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。<br>(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。<br>(2)產品須提供可與其相連之影像監控裝置。<br>(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。

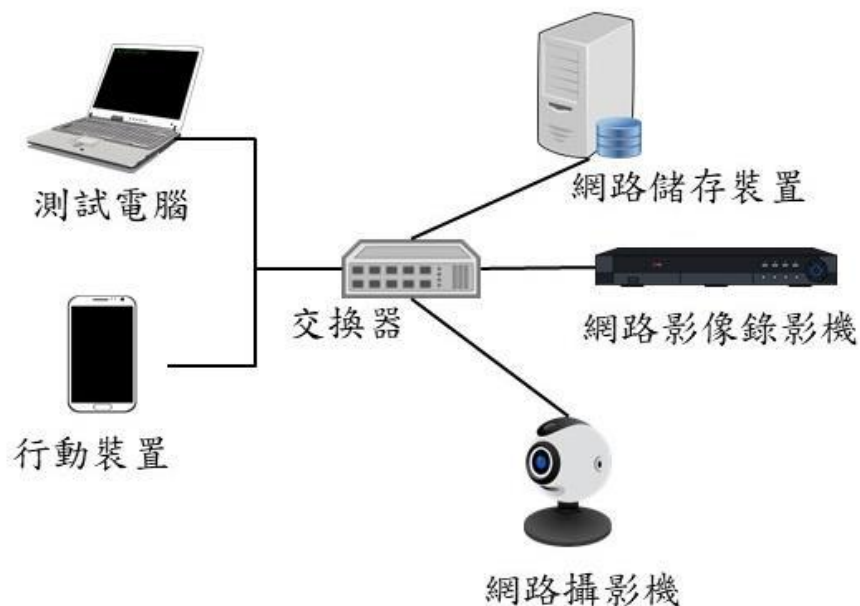
#### 預期結果：

- (1)安全通道僅支援「附錄 A」中所建議之密碼套件。
- (2)與測試電腦之間的帳號密碼資訊傳輸，預設採用安全通道。
- (3)與行動裝置之間的帳號密碼資訊傳輸，預設採用安全通道。
- (4)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。(改到2級選測)



## 三、 案例分享

### 範例：5.3.1.1



#### 成功案例分享

- (1) 待測物(網路攝影機)產生憑證
- (2) 將產生之憑證匯入其它影像監控裝置
- (3) 待測物與其它影像監控裝置進行連線動作

## 三、 案例分享

### 測項：5.4.2.4

| 安全要求分項         | 測試項目                 | 安全等級 | 測試目的                   | 樣品條件   |
|----------------|----------------------|------|------------------------|--|
| 5.4.2通行碼鑑別安全測試 | 5.4.2.4通行碼的輸入頻率及次數限制 | 1級   | 驗證通行碼鑑別機制是否有防止暴力破解之能力。 | (1) 產品須支援通行碼鑑別機制，否則此測項不適用。<br>(2) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。<br>(3) 產品須提供帳戶鎖定機制之設計說明。 |

#### 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) 不斷輸入錯誤且相異的通行碼。
- (4) 檢視產品於帳戶鎖定計數器重設為 0 前，連續登入失敗次數 5 次以內，是否會鎖定帳戶。
- (5) 帳戶鎖定後，於鎖定期間內持續輸入相異且錯誤的通行碼，比對廠商宣告帳戶鎖定時限內，檢視帳戶是否解除鎖定。
- (6) 同一帳戶任一次登入失敗後，於廠商宣告計數器重設時限內，重新輸入錯誤且相異的通行碼，檢視輸入失敗次數是否有重新計算。

#### 預期結果：

- (1) 輸入次數 5 次以內，會鎖定帳戶
- (2) 於廠商宣告之帳戶鎖定時限內，帳戶未解除鎖定。
- (3) 於廠商宣告計數器重設時限內，失敗次數未重新計算。

## 三、 案例分享

### 範例：5.4.2.4

#### 說明：

很多廠商在web介面都沒有做該機制。

此外，如有支援ONVIF或USB、UART介面登入作業系統功能，亦須符合本測項要求。

## 三、 案例分享

### 測項：5.4.3.2

| 安全要求分項      | 測試項目          | 安全等級 | 測試目的               | 樣品條件                      |
|-------------|---------------|------|--------------------|---------------------------|
| 5.4.3權限管控測試 | 5.4.3.2權限有效時間 | 1級   | 驗證產品是否存在有限的授權時間長度。 | 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。 |

#### 測試方法：

- (1) 將測試電腦或行動裝置連接產品。
- (2) 透過網頁管理介面或操控程式登入產品。
- (3) 目視產品之操控程式或網頁管理介面，閒置時限是否存在供使用者設定的操作介面。
- (4) 閒置產品直到超過閒置時限值。
- (5) 檢視是否需要重新鑑別方可存取產品。

#### 預期結果：

- (1) 產品之授權行為，存在閒置時限供使用者設定。
- (2) 遠端連線閒置逾時，須經過身分鑑別方可存取產品。

## 三、 案例分享

### 範例：5.4.3.2

#### 說明：

多數受測標的未檢出有提供閒置時限操作介面(測試規範：產品之授權行為，存在閒置時限供使用者設定。)

## 三、 案例分享

### 測項：5.5.1.1

| 安全要求分項           | 測試項目             | 安全等級 | 測試目的               | 樣品條件  |
|------------------|------------------|------|--------------------|---|
| 5.5.1隱私資料的存取保護測試 | 5.5.1.1隱私資料的存取控制 | 1級   | 驗證產品隱私權是否具有存取控制機制。 | (1) 產品須提供隱私存取權限之宣告。<br>(2) 產品必須能建立 2 個以上的帳號，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) 透過網頁管理介面或操控程式，以不同角色登入產品。
- (3) 存取影像資料，同時檢視該帳號之身分類型與其對應之隱私存取權限是否與產品自我宣告相符。
- (4) 當產品提供網頁管理介面且已經有帳號登入的情況下，檢視是否無需透過帳號切換，即可存取該帳號權限之外的隱私資料。

#### 預期結果：

- (1) 使用者的隱私存取授權與產品自我宣告相符。

## 三、 案例分享

### 範例 : 5.5.1.1

#### 說明：

範例1：由不同角色登入時，若隱私資料存於SD卡，則該角色只能存取自行錄製的隱私資料。

範例2：僅有管理者權限可存取SD卡上的隱私資料，其餘角色皆無存取權限。

## 三、 案例分享

### 測項：5.5.1.3

| 安全要求分項           | 測試項目            | 安全等級 | 測試目的               | 樣品條件 |
|------------------|-----------------|------|--------------------|------|
| 5.5.1隱私資料的存取保護測試 | 5.5.1.3登入警示功能測試 | 1級   | 驗證產品是否具有防止隱私外洩之功能。 | 無    |

#### 測試方法：

- (1) 將測試電腦或行動裝置連接產品。
- (2) 透過網頁管理介面或操控程式，以不同角色登入產品。
- (3) 根據產品使用說明，無論登入成功與否，確認是否接收到登入警。

#### 預期結果：

- (1) 每次發生新的存取事件時，產品發出警。



## 三、 案例分享

### 範例 : 5.5.1.3

#### 說明：

範例1：當發生新的產品存取事件時(登入成功或失敗)，產品發出email通知。

範例2：當發生新的產品存取事件時(登入成功或失敗)，web介面跳出視窗通知。

## 三、 案例分享

### 測項：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。<br>(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：

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

## 三、 案例分享

### 範例：5.5.2.1

說明：

安全通道須僅支援「附錄 A」中所建議之密碼套件。

#### 附錄 A

#### (規定)

#### 安全通道應使用之密碼套件

安全通道(TLS)所選用的密碼套件應遵循下述幾項要求：

- TLSv1.2
  - TLS\_ECDHE\_ECDSA\_WITH\_AES256\_GCM\_SHA384
  - TLS\_ECDHE\_RSA\_WITH\_AES256\_GCM\_SHA384
  - TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305
  - TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305
  - TLS\_ECDHE\_ECDSA\_WITH\_AES128\_GCM\_SHA256
  - TLS\_ECDHE\_RSA\_WITH\_AES128\_GCM\_SHA256
  - TLS\_ECDHE\_ECDSA\_WITH\_AES256\_SHA384
  - TLS\_ECDHE\_RSA\_WITH\_AES256\_SHA384
  - TLS\_ECDHE\_ECDSA\_WITH\_AES128\_SHA256
  - TLS\_ECDHE\_RSA\_WITH\_AES128\_SHA256
- TLSv1.3
  - TLS\_AES\_128\_GCM\_SHA256
  - TLS\_AES\_256\_GCM\_SHA384
  - TLS\_CHACHA20\_POLY1305\_SHA256
  - TLS\_AES\_128\_CCM\_SHA256
  - TLS\_AES\_128\_CCM\_8\_SHA256

# 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

