



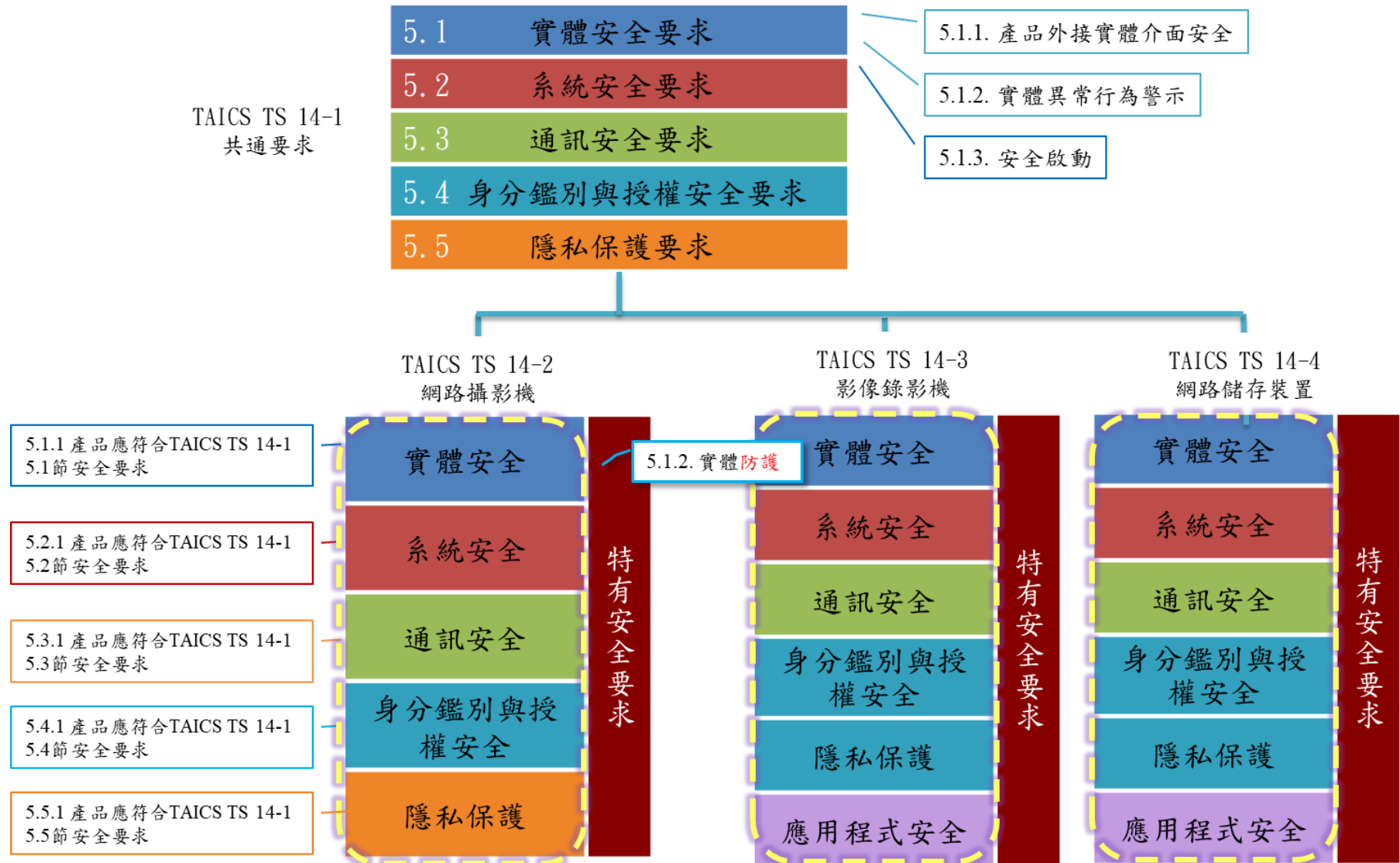
Video Surveillance System 資安產業標準精要培析

高傳凱 博士

資策會 資安所 聯網安全檢測組組長
TAICS TC Network and Security WG1 組長



影像監控系統系列資安標準框架





實體安全要求



5.1.1.1

實體介面安全管控測試 (1級)

- **測試目的：**

- ◆ 驗證是否可透過產品實體介面，存取作業系統之除錯模式。

- **測試時間：**

- ◆ 中(30分鐘內)。

- **注意：**

- ◆ 有可能燒壞待測設備或測試工具的風險。
- ◆ 實驗室應提前準備好介接工具。
- ◆ 雖然受測單位會告知Debug埠的位置，但也有可能受測單位故意隱瞞以避免被實驗室找到漏洞，實驗室則必須要有找尋電路板上Debug埠的能力。(例:三用電表)

- **正確結果：**

- ◆ 不存在debug port。
- ◆ Debug port接上去，console沒反應。
- ◆ Debug port接上去，console顯示要求認證。

- **測試複雜度：**

- ◆ 中等



5.1.2.1

實體異常行為紀錄(2級)

- **測試目的：**

- ◆ 驗證產品之實體埠是否有插拔紀錄。

- **測試時間：**

- ◆ 短(10分鐘內)。

- **注意：**

- ◆ 有些IP CAM是採用PoE供電，此時可透過PoE Adapter來介接IP CAM，避免因插拔網路線斷電而導致測項不過。
- ◆ 產品的日誌資料會記錄這類型事件。

- **正確結果：**

- ◆ 產品具備USB插槽，且對其「插」及「拔」時，日誌紀錄會顯示。
- ◆ 產品具備RJ45插槽，且對其「插」及「拔」時，日誌紀錄會顯示。
- ◆ 日誌紀錄需具備時間資訊。

- **測試複雜度：**

- ◆ 易



PoE Adapter



5.1.2.2

實體異常狀態警示機制(2級)

- 測試目的：

- ◆ 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。

- 測試時間：

- ◆ 短(10分鐘內)。

- 注意：

- ◆ 有些IP CAM是採用PoE供電，此時可透過PoE Adapter來介接IP CAM，避免因插拔網路線斷電而導致測項不過。
- ◆ 需**主動**發出警示，例如：**聲音、彈跳視窗、推播通知、警示燈**。

- 正確結果：

- ◆ 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。

- 測試複雜度：

- ◆ 易



5.1.3.1

實體防護測試(1級)

- **測試目的：**

- ◆ 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。

- **測試時間：**

- ◆ 極短(1分鐘內)。

- **注意：**

- ◆ 產品外觀上的還原預設通行碼設計，必須使用**工具**才可啟動。
- ◆ **只要不是徒手**，即使是拿迴紋針也算是使用工具。

- **正確結果：**

- ◆ 產品外觀上用以還原預設通行碼之設計，**不得**徒手即可操作。

- **測試複雜度**

- ◆ 易



5.1.4.1

安全啟動測試(3級)

- **測試目的：**

- ◆ 驗證產品於開機階段是否能確保產品之完整性及合法性。

- **測試時間：**

- ◆ 短(10分鐘內)。

- **注意：**

- ◆ 產品應該要具備安全晶片(例如:TPM、HSM)，使安全啟動功能得以確保。
- ◆ 審閱產品設計文件，該文件必須能佐證安全啟動功能。

- **正確結果：**

- ◆ 書面資料證實產品在開機過程中驗證韌體/作業系統的簽章。

- **測試複雜度：**

- ◆ 易(書審)



系統安全要求



5.2.1.1

作業系統安全與網路服務安全測試(1級~3級)

● 測試目的：

- ◆ 測試作業系統是否存在CVSS v3 評分為9.0/7.0分以上之常見資安弱點與漏洞。

● 測試時間：

- ◆ 中(30分鐘以內)。

● 注意：

- ◆ 漏洞嚴重性評比是以NVD網站為主，而不是工具。
- ◆ 3月一致性會議決議，此測項新增二級測試，要求廠商給予最高權限帳號，進行檢測。

● 正確結果：

- ◆ 1級: 未要求受測廠商所提供測試用帳號的權限，漏洞的CVSS v3為9分以下
- ◆ 2級: 要求受測廠商提供作業系統層最高權限帳號，漏洞的CVSS v3為9分以下
- ◆ 3級: 要求受測廠商提供作業系統層最高權限帳號，漏洞的CVSS v3為7分以下

新版(v2.0)將會增加的測項

● 測試複雜度：

- ◆ 易(工具掃描)



5.2.1.2

網路服務連接埠管控測試(1級)

- **測試目的：**

- ◆ 驗證產品是否存在預期以外之網路埠。

- **測試時間：**

- ◆ 冗長(超過8小時)。

- **注意：**

- ◆ 必須要驗證動態埠、TCP、UDP。
- ◆ 廠商必須自我宣告所開啟的網路埠。

- **正確結果：**

- ◆ 實驗室所檢測到開啟的網路埠**必須**與廠商宣告一致。

- **測試複雜度：**

- ◆ 易(工具掃描)



5.2.3.1 (a)

韌體檔案安全測試(1級)

- 測試目的：

- ◆ 驗證產品之韌體更新檔是否會洩露敏感性資料。

- 測試時間：

- ◆ 短(10分鐘內)。

- 注意：「以下2個情境擇1做即可」

- ◆ 「情境1」適用當韌體為**加密檔案**。=>書審
- ◆ 「情境2」適用當韌體為**未加密檔案**。=>然而實驗室用來搜尋敏感資料的關鍵字往往太缺乏。

- 正確結果：

- ◆ 「情境1」加密演算法必須採用FIPS 140-2 Annex A所認可，且不可被實際解析出檔案系統目錄
- ◆ 「情境2」韌體不能被解析出通行碼資料、金鑰、IP、URL、非公開email

- 測試複雜度：

- ◆ 中等



5.2.3.1 (b)

韌體更新路徑的保護(1級)

- **測試目的：**

- ◆ 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。

- **測試時間：**

- ◆ 中(30分鐘以內)。

- **注意：**

- ◆ 實驗室對憑證MITM的實作能力，換言之未檢查憑證有效性與合法性的產品將不會通過。
- ◆ 線上更新行為指的是從更新伺服器直接下載韌體到產品中，而不是手機App到產品中這段。
- ◆ 國內販售的IP CAM幾乎不採用此更新方式。

- **正確結果：**

- ◆ 線上更新路徑通過安全通道，且必須採用TLS 1.2以上之版本。
- ◆ 憑證公鑰或憑證資訊一旦被竄改，安全通道建立失敗。

- **測試複雜度：**

- ◆ 中等



5.2.3.2

韌體更新檔之完整性及可信度測試(1級)

- 測試目的：

- ◆ 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。

- 測試時間：

- ◆ 短(10分鐘內)。

- 注意：

- ◆ 韌體簽章方法不一，且簽章手法不一定會告知檢測實驗室，因此需要廠商配合方可測試。
- ◆ TAF核可資安測試實驗室不可執行遊測。
- ◆ 實驗室的檢測手法必須包括執行非合法簽章這段。

- 正確結果：

- ◆ 產品不得更新成功。

- 測試複雜度：

- ◆ 難



5.2.3.3

備援更新功能測試(1級)

- **測試目的：**

- ◆ 驗證當更新作業異常中斷時，產品仍可恢復正常運作狀態。

- **測試時間：**

- ◆ 短(10分鐘內)。

- **注意：**

- ◆ 產品可能會被更新，實驗室在測試前，是否有確保受測韌體版本與廠商宣告一致的程序。
- ◆ 破壞性測試，可能會導致設備無法再啟動。
- ◆ 線上更新情境下，必須是在產品更新階段，而非下載階段。

- **正確結果：**

- ◆ 更新中斷後，系統仍可回復正常運作狀態。

- **測試複雜度：**

- ◆ 易



5.2.4.1

敏感性資料權限管控測試(1~2級)

- **測試目的：**

- ◆ 產品敏感性資料的存取是否具有權限控管機制。

- **測試時間：**

- ◆ (a)書審。
- ◆ (b)中(30分鐘以內)。

- **注意：**

- ◆ 分(a)(b)二類測試，(a)類為初階測試(書審)，(b)類為中階測試(實測)
- ◆ 接受(b)類測試的受測廠商須提供一版可進入作業系統層最高權限帳號之產品。

- **正確結果：（無論書面或實測）**

- ◆ 通行碼、加解密金鑰的權限管控與產品自我宣告相符。
- ◆ 該權限管控機制至少擁有二個以上不同權限的角色。

- **測試複雜度：**

- ◆ (a)易
- ◆ (b)中等



5.2.4.2

敏感性資料加密儲存測試(1~2級)

- **測試目的：**
 - ◆ 驗證產品之敏感性資料於儲存狀態下是否加密保護。
- **測試時間：**
 - ◆ (a)書審。
 - ◆ (b)長(30分鐘以上)。
- **注意：**
 - ◆ 分(a)(b)二類測試，(a)類為初階測試(書審)，(b)類為中階測試(實測)
 - ◆ 接受(b)類測試的受測廠商須提供一版可進入作業系統層高權限帳號之產品。
- **正確結果：（無論書面或實測）**
 - ◆ 通行碼、加解密金鑰的保密機制採用FIPS 140-2 Annex A所核可之加密演算法。
- **測試複雜度：**
 - ◆ (a)易
 - ◆ (b)中等



5.2.4.3

金鑰管理程序測試(2級)

- **測試目的：**

- ◆ 確認產品的金鑰管理是否建立可靠管控程序。

- **測試時間：**

- ◆ 書審。

- **注意：**

- ◆ 受測廠商只要提供有相關內容的文件即可，文件內容的合理性及正確性，會由實驗室給予建議。

- **正確結果：**

- ◆ 文件中必須有說明對於金鑰的生成、交換、儲存、使用、銷毀及更替程序。

- **測試複雜度：**

- ◆ 易



5.2.4.4

敏感性資料隔離保護測試(3級)

- **測試目的：**

- ◆ 確認產品敏感性資料之存放與正常作業系統隔離。

- **測試時間：**

- ◆ 書審。

- **注意：**

- ◆ 產品應具備安全晶片作為安全區域使用。
- ◆ 未規定該安全晶片符合FIPS 140-2

- **正確結果：**

- ◆ 書面資料證實產品之敏感性資料存放於安全區域。

- **測試複雜度：**

- ◆ 易



5.2.5.1

網頁管理介面常見資安風險測試(1級)

- **測試目的：**

- ◆ 驗證產品之網頁管理介面是否存在已知資安漏洞。

- **測試時間：**

- ◆ 長(30分鐘以上，不同產品會有不同的反應時間)。

- **注意：**

- ◆ 絕大部份使用工具。
- ◆ **必須**是**登入**網頁管理介面的狀態下，執行測試。

- **正確結果：**

- ◆ 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。

- **測試複雜度：**

- ◆ 易



5.2.6.1(a)

ONVIF應用程式介面之鑑別機制測試(1級)

● 測試目的：

- ◆ 驗證產品的ONVIF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。

● 測試時間：

- ◆ 短(10分鐘內)。

● 注意：

- ◆ 要確認是針對ONVIF API進行測試對象。
- ◆ 大部份的測項與5.4節相同，但5.4節是針對所有管理介面作為測試對象。
- ◆ 網路環境架設是此測項是否正確執行的關鍵。

● 正確結果：

- ◆ ONVIF重送攻擊失敗。

● 測試複雜度：

- ◆ 中等



5.2.6.1(b)

ONVIF應用程式介面之身分鑑別錯誤訊息(1級)

● 測試目的：

- ◆ 驗證ONVIF應用程式介面之鑑別錯誤訊息不會造成敏感性資料的洩漏。

● 測試時間：

- ◆ 短(10分鐘內)。

● 注意：

- ◆ 首先檢查產品所提供具ONVIF通訊功能之App，若廠商不提供則建議做下一步。
- ◆ 最建議做法是檢查ONVIF封包中的錯誤訊息。
- ◆ 當認證資料輸入錯誤時，只要回覆「身分鑑別失敗」或「帳號或密碼輸入錯誤」即可。

● 正確結果：

- ◆ 身分鑑別失敗所顯示的錯誤訊息，無法推斷是帳號錯或是密碼錯

● 測試複雜度：

- ◆ 中等



5.2.6.2

ONVIF應用程式介面之通行碼鑑別強度機制測試(1級)

- **測試目的：**

- ◆ 驗證產品ONVIF應用程式介面的通行碼鑑別機制強度是否足夠。

- **測試時間：**

- ◆ 短(10分鐘內)。

- **注意：**

- ◆ 權限控管是指透過ONVIF溝通的帳號是有以下通行碼鑑別機制的要求：
 - ▶ 預設通行碼相異，或首次使用要更改通行碼
 - ▶ 密碼複雜度，8字元以上+英文大小寫+數字+特殊符號+相同字元不得連續+歷程紀錄
 - ▶ 防暴力破解，限制輸入頻率+輸入次數

- **正確結果：**

- ◆ 以上注意事項內的條件皆要達成。

- **測試複雜度：**

- ◆ 易



5.2.6.3

ONVIF應用程式介面之權限管控機制(1級)

- **測試目的：**

- ◆ 驗證產品的ONVIF應用程式介面是否存在權限控管。

- **測試時間：**

- ◆ 短(10分鐘內)。

- **注意：**

- ◆ 權限控管是指透過ONVIF溝通的帳號是有不同權限的，有些ONVIF指令是某些角色的帳號(例：系統管理者、一般使用者)所不能操作的。

- **正確結果：**

- ◆ 各角色ONVIF API的權限管控與產品自我宣告相符。
- ◆ 至少有二個以上不同權限的角色。

- **測試複雜度：**

- ◆ 易



5.2.7.1

安全事件日誌檔測試(1級)

- **測試目的：**

- ◆ 驗證產品是否有安全事件紀錄供查詢。

- **測試時間：**

- ◆ 短(10分鐘內)。

- **注意：**

- ◆ 這裡指的是「安全事件」日誌，而**不是一般的系統日誌**。
- ◆ 安全事件日誌不得因為**重新開機**而被**清除**。

- **正確結果：**

- ◆ 安全事件紀錄可供使用者檢視之介面。
- ◆ 日誌資料要有時間、使用者身分及動作。
- ◆ 重開機前之安全事件紀錄仍可查詢。

- **測試複雜度：**

- ◆ 易



5.2.7.2

安全事件日誌檔存取權限管控測試(1級)

- **測試目的：**

- ◆ 驗證產品之安全事件日誌紀錄是否具備權限控管。

- **測試時間：**

- ◆ 短(10分鐘內)。

- **注意：**

- ◆ 無。

- **正確結果：**

- ◆ 安全事件日誌的存取權限管控與產品自我宣告相符。
- ◆ 至少有二個以上不同權限的角色。

- **測試複雜度：**

- ◆ 易



5.2.7.3

安全事件日誌檔之日誌滾動功能測試(1級)

● 測試目的：

- ◆ 驗證產品是否具備處理日誌儲存空間不足之異常狀況。

● 測試時間：

- ◆ 冗長(8小時以上，視日誌存放容量)。

● 注意：

- ◆ 測試對象是安全事件日誌，**其它行為**(例:錄影)造成儲存空間不足，**不在本測項中**。
- ◆ 實驗室應該要有自動化的測試工具，以增加測試可執行之可信度。

● 正確結果：

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

● 測試複雜度：

- ◆ 易



5.2.7.4

異常警示功能測試(2級)

- **測試目的：**

- ◆ 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。

- **測試時間：**

- ◆ 冗長(8小時以上，視日誌存放容量)，可與5.2.7.3一併做。

- **注意：**

- ◆ 實驗室應先確認使用手冊，產品是否具備因儲存空間不足而發出警示的功能。

- **正確結果：**

- ◆ 產品發出安全事件日誌紀錄檔儲存空間不足之警示(例如:聲音、彈跳視窗、推播通知、警示燈)。

- **測試複雜度：**

- ◆ 易



5.3.1.1 敏感性資料之傳輸保護初階測試 (最新規定)

● 測試目的：

- ◆ 1級: 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級: 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。

● 測試時間：

- ◆ 中(30分鐘以內)。

● 注意：

- ◆ **2級**是針對受測廠商自家產品互通上(NVR<=>IP CAM)是否具備防止MITM的測試。
- ◆ 市面上尚未有安全功能之對連裝置(NVR, IP CAM)，需受測廠商提供
- ◆ **環境的搭建是本測項的門檻。**
- ◆ **一般會有ONVIF API跟廠商自家API，2種通訊方式。**

● 正確結果：

- ◆ 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。
- ◆ **(不包括ONVIF通訊)已竄改之安全通道憑證無法通過產品的身分鑑別。**

● 測試複雜度：

- ◆ 難



5.3.1.2

敏感性資料之傳輸保護中階測試(3級)

- **測試目的：**

- ◆ 驗證傳輸敏感性資料之安全通道，是否支援強加密演算法。

- **測試時間：**

- ◆ 中(30分鐘以內)，可與5.3.1.1一併做。

- **注意：**

- ◆ 無。

- **正確結果：**

- ◆ 該安全通道支援AES-256同等或以上加密強度的演算法。

- **測試複雜度：**

- ◆ 易



5.3.2.1

網路裝置資訊探詢功能測試(1級)

- **測試目的：**
 - ◆ 確認產品是否運行在具安全風險的網路設定。
- **測試時間：**
 - ◆ 中(30分鐘以內)。
- **注意：**
 - ◆ 實驗室不得只確認操作介面是否存在，**必須**實際去確認功能是否能真正關閉。
- **正確結果：**
 - ◆ 若產品支援通用隨插即用通訊協定服務，該服務提供使用者可自行開/關功能之設置。
 - ◆ 若產品支援簡單網路管理協定服務，該服務提供使用者可自行開/關功能之設置。
 - ◆ 若產品支援零配置通訊協定服務，該服務提供使用者可自行開/關功能之設置。
- **測試複雜度：**
 - ◆ 中等



5.3.2.2

網路介面存取設置測試(1級)

- **測試目的：**

- ◆ 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。

- **測試時間：**

- ◆ 中(30分鐘以內)。

- **注意：**

- ◆ 與實驗室滲透測試能力相關。
- ◆ 是不是有**可以建立遠端連線**並存取產品的**網路埠**存在。

- **正確結果：**

- ◆ **不存在**進入作業系統**除錯模式**之介面。
- ◆ 若**存在**進入作業系統除錯模式之介面，產品**要求身分鑑別**。
- ◆ 若**存在**進入作業系統除錯模式之介面，且**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

- **測試複雜度：**

- ◆ 中等



5.3.2.3

通訊協定異常輸入測試(2級)

- **測試目的：**

- ◆ 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。

- **測試時間：**

- ◆ 冗長(超過8小時)。

- **注意：**

- ◆ 檢測結果只能取決於工具優劣，檢測工具成本高昂。
- ◆ 欲通過2級廠商，須確認實驗室擁有該工具的狀態。
- ◆ 模糊測試工具是實驗室門檻，工具費用高昂，要注意受稽實驗室的license有效期限，避免在失效期間有接2級以上之檢測案，或者外包其它實驗室執行測試

- **正確結果：**

- ◆ 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)

- **測試複雜度：**

- ◆ 易



5.4.1.1

鑑別機制強度測試(1級)

- **測試目的：**

- ◆ 驗證產品是否具備可靠之身分鑑別機制。

- **測試時間：**

- ◆ 中(30分鐘以內)。

- **注意：**

- ◆ 一般會有2個操控介面，即測試電腦或行動裝置。
- ◆ 實驗室可能忽略行動裝置介面而未測，且行動裝置檢測需架設好測試環境。

- **正確結果：**

- ◆ 無論透過網頁管理介面或操控程式存取影像監控裝置時，皆經過身分鑑別程序。
- ◆ 身分鑑別機制具備抵抗重送攻擊的能力。
- ◆ 登出後確實須再次登入，方可存取產品。

- **測試複雜度：**

- ◆ 中等



5.4.1.2

身分鑑別錯誤訊息(1級)

- **測試目的：**

- ◆ 驗證鑑別錯誤訊息不會造成敏感性資料的洩漏。

- **測試時間：**

- ◆ 極短(1分鐘內)。

- **注意：**

- ◆ 當認證資料輸入錯誤時，只要回覆「身分鑑別失敗」或「帳號或密碼輸入錯誤」即可。

- **正確結果：**

- ◆ 從鑑別錯誤訊息無法推斷出合法使用者名稱。

- **測試複雜度：**

- ◆ 易



5.4.1.3

憑證上傳介面測試(2級)

- **測試目的：**

- ◆ 驗證產品是否具有提供憑證上傳的功能。

- **測試時間：**

- ◆ 中(30分鐘以內)。

- **注意：**

- ◆ 實驗室需預先準備好trusted及自簽憑證。

- **正確結果：**

- ◆ 產品所上傳之憑證可被更換為新上傳之憑證。

- **測試複雜度：**

- ◆ 中等



5.4.1.4

金鑰唯一性測試(2級)

- **測試目的：**

- ◆ 驗證產品之金鑰是否唯一。

- **測試時間：**

- ◆ 中(30分鐘以內)。

- **注意：**

- ◆ 檢查每次Reset後金鑰是否都會重新產生。

- **正確結果：**

- ◆ 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。

- **測試複雜度：**

- ◆ 易



5.4.1.5

多因子鑑別機制測試(3級)

- **測試目的：**

- ◆ 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。

- **測試時間：**

- ◆ 短(10分鐘以內)。

- **注意：**

- ◆ NIST聲明多因子認證**不可採用短訊**服務。
- ◆ **不可同時**讓二台行動裝置作為所持之物之鑑別因子。

- **正確結果：**

- ◆ 網頁管理介面或操控程式與產品之間的身分鑑別，透過多因子身分鑑別。
- ◆ 每一階段身分鑑別皆採用不同因素的鑑別因子。
- ◆ 當使用鑑別因子時，未採用短訊服務獲取通行碼。
- ◆ 當行動裝置作為所持之物之鑑別因子時，僅可在1台行動裝置上獲取鑑別因子。

- **測試複雜度：**

- ◆ 易



5.4.1.6

裝置鑑別測試(3級)

- **測試目的：**

- ◆ 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。

- **測試時間：**

- ◆ 中(30分鐘以內)。

- **注意：**

- ◆ 現況是IP CAM會要求通行碼認證。
- ◆ **NVR也必須要求連線要認證。**

- **正確結果：**

- ◆ 其它影像監控系統裝置與產品建立連線時，經過裝置身分鑑別。
- ◆ 該裝置身分鑑別機制具備抵抗重送攻擊的能力。

- **測試複雜度：**

- ◆ 難



5.4.2.1

預設通行碼安全測試(1級)

- **測試目的：**

- ◆ 驗證產品是否有相同的預設通行碼。
- ◆ 驗證產品預設通行碼是否會於首次上線後強制要求更改。

- **測試時間：**

- ◆ 極短(1分鐘內)。

- **注意：**

- ◆ 無。

- **正確結果：**

- ◆ 任2台產品的預設通行碼相異。
- ◆ 未經設定新通行碼前無法存取產品。
- ◆ 新通行碼不可與預設通行碼相同。

- **測試複雜度：**

- ◆ 易



5.4.2.2~5.4.2.4 通行碼鑑別安全測試(1級)

5.4.2.5、5.4.2.6(3級)

● 測試目的：

- ◆ 驗證產品的通行碼長度是否足夠，以確保其強度。
- ◆ 驗證產品的通行碼複雜度是否足夠，以確保其強度。
- ◆ 驗證通行碼鑑別機制是否有防止暴力破解之能力。
- ◆ 驗證產品的通行碼是否存有連續字元，以確保其強度。
- ◆ 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。

● 測試時間：

- ◆ 中等或更短。

● 注意：

- ◆ 於廠商宣告計數器重設時限內，**失敗次數未重新計算**。
- ◆ 密碼歷程紀錄**未規定要追溯的次數**。

● 正確結果：

- ◆ 無法建立或變更小於8個字元長度之通行碼。
- ◆ 無法建立或變更複雜度不足之通行碼。
- ◆ 輸入次數5次以內，會鎖定帳戶。
- ◆ 於廠商宣告之帳戶鎖定時限內，帳戶未解除鎖定。
- ◆ 無法建立或變更3個以上連續字元的通行碼。
- ◆ 無法變更曾經輸入之通行碼。

● 測試複雜度：

- ◆ 易



5.4.3 權限管控機制(1級)

- **測試目的：**

- ◆ 驗證產品資源的存取是否具有權限控管機制。
- ◆ 驗證產品是否存在有限的授權時間長度。

- **測試時間：**

- ◆ 中等或更短。

- **注意：**

- ◆ 閒置時限要提供設定UI。

- **正確結果：**

- ◆ 該權限管控機制至少擁有二個以上不同權限的角色。
- ◆ 產品之授權行為，存在閒置時限供使用者設定。
- ◆ 遠端連線閒置逾時，須經過身分鑑別方可存取產品。

- **測試複雜度：**

- ◆ 易



5.5.1.1 隱私資料的存取控制(1級)

- **測試目的：**
 - ◆ 驗證產品隱私權是否具有存取控制機制。
- **測試時間：**
 - ◆ 短(10分鐘內)。
- **注意：**
 - ◆ 僅限定對影像的存取控制。
- **正確結果：**
 - ◆ 使用者的隱私存取授權與產品自我宣告相符。
- **測試複雜度：**
 - ◆ 易



5.5.1.2 隱私資料刪除功能(1級)

- **測試目的：**
 - ◆ 驗證使用者擁有刪除自身隱私權的權限。
- **測試時間：**
 - ◆ 短(10分鐘內)。
- **注意：**
 - ◆ 無。
- **正確結果：**
 - ◆ 提供使用者刪除隱私資料的功能。
- **測試複雜度：**
 - ◆ 易



5.5.1.3 登入警示功能測試(1級)

- **測試目的：**

- ◆ 驗證產品是否具有防止隱私外洩之功能。

- **測試時間：**

- ◆ 短(10分鐘內)。

- **注意：**

- ◆ 本測項重點是在測有沒有登入警示功能。
- ◆ 實驗室應該先確認產品說明書。

- **正確結果：**

- ◆ 每次發生新的存取事件時，產品發出警示，通知已登入使用者或系統管理者。

- **測試複雜度：**

- ◆ 易



5.5.2 隱私資料的傳輸保護測試(1級~3級)

- 驗證手法同敏感性資料的傳輸。
- 但測試對象換成影像。
- 注意：
 - ◆ 實驗室常放上加密資料的擷圖佐證，但應該放上的是加密的影像資料擷圖。
 - ◆ 影像傳輸可能走RTSP、HTTP，或者廠商自家的通訊協定，可以從這幾個通訊協定確認其串流影像。
- 測試複雜度：
 - ◆ 難



DVR



5.5.1.2 影像隱私外洩防護測試(2級)

- 測試項目同網路攝影機的5.5.1.2



DVR/NVR/NAS



5.1.1.2 儲存媒體保護機制測試(2級)

- **測試目的：**

- ◆ 驗證產品之儲存媒體（例如：硬碟機），是否可在本機以外的機器被存取。

- **測試時間：**

- ◆ 中(30分鐘內)。

- **注意：**

- ◆ 無。

- **正確結果：**

- ◆ 儲存媒體內之影像資料**不可讀取**。



5.1.5.1 儲存備份機制初階安全測試(1級)

- **測試目的：**

- ◆ 確保受測產品具備有外部儲存備份之介面。

- **測試時間：**

- ◆ 極短(1分鐘內)。

- **注意：**

- ◆ 無。

- **正確結果：**

- ◆ 產品外觀具備外部儲存備份之裝置與連接介面。



5.1.5.2 儲存備份機制中階安全測試(2級)

- **測試目的：**

- ◆ 確保產品所儲存之影像，支援資料冗餘之能力，例如：RAID 1等級以上。

- **測試時間：**

- ◆ 極短(1分鐘內)。

- **注意：**

- ◆ 測試方法為於**產品啟動狀況下**，將其中一顆儲存媒體卸載。

- **正確結果：**

- ◆ 影像監控相關功能正常運行。



5.1.5.3 儲存備份機制高階安全測試(3級)

- **測試目的：**
 - ◆ 確保產品支援硬碟熱備援之功能，提升容錯能力。
- **測試時間：**
 - ◆ 極短(1分鐘內)。
- **注意：**
 - ◆ 測試方法為於**產品啟動狀況下**，將其中一顆raid硬碟卸載。
- **正確結果：**
 - ◆ 產品正常運行，且效能不變、功能依舊完整。



5.2.7.2 影像檔案寫入日誌測試(1級)

- **測試目的：**

- ◆ 驗證產品是否具有影像檔案寫入事件之紀錄供查詢。

- **測試時間：**

- ◆ 短(10分鐘內)。

- **注意：**

- ◆ 僅針對**寫入事件**。

- **正確結果：**

- ◆ 產品具有可供使用者檢視影像檔案寫入事件之安全事件日誌功能。
- ◆ 安全事件日誌的資料包含正確時間格式(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。



5.2.8.1 有效儲存空間設定機制測試(2級)

- **測試目的：**

- ◆ 確保產品儲存空間小於設定值時，提供警告機制。

- **測試時間：**

- ◆ 長(30分鐘以上)。

- **注意：**

- ◆ 無。

- **正確結果：**

- ◆ 產品發出儲存空間不足之相關警示。



5.2.8.2 儲存資料防竄改機制測試(2級)

- **測試目的：**
 - ◆ 確保產品支援影像檔案防竄改之警示機制。
- **測試時間：**
 - ◆ 中(30分鐘以內)。
- **注意：**
 - ◆ 測試時直接以其它影像檔案覆蓋。
- **正確結果：**
 - ◆ 產品發出影像檔案遭竄改之相關警示。



5.2.9.1 影像備份能力測試(1級)

- **測試目的：**
 - ◆ 確保產品支援影像檔案備份功能。
- **測試時間：**
 - ◆ 短(10分鐘以內)。
- **注意：**
 - ◆ 無。
- **正確結果：**
 - ◆ 備份功能正常運行。



5.2.9.2 影像備份保護測試(3級)

- **測試目的：**

- ◆ 確保產品之影像備份檔案之儲存機密性。

- **測試時間：**

- ◆ 短(10分鐘以內)。

- **注意：**

- ◆ 書審。

- **正確結果：**

- ◆ 備份加密採用FIPS 140-2 Annex A [2]所核可之加密演算法。



5.6.1.1 應用程式防竄改測試(2級)

- **測試目的：**

- ◆ 驗證產品預載之應用程式是否具備遭竄改之啟動防護。

- **測試時間：**

- ◆ 短(10分鐘以內)。

- **注意：**

- ◆ 無。

- **正確結果：**

- ◆ 遭替換之應用程式不可被啟動。
- ◆ 遭替換之網頁原始碼不可被啟動。



5.6.1.2 應用程式防竄改測試(3級)

- **測試目的：**

- ◆ 檢視產品所引用網路相關之第三方函式庫來源。

- **測試時間：**

- ◆ 長(30分鐘以內)。

- **注意：**

- ◆ 只檢查網路相關之第三方函式庫清單。

- **正確結果：**

- ◆ 經實測網路相關之第三方函式庫清單後，未發現CVSS v3評分為9.0分以上之資安漏洞。



網路攝影機



5.1.1.2 最小實體介面測試(2級)

● 測試目的：

- ◆ 驗證是否可輕易從產品外部取得儲存媒體。

● 測試時間：

- ◆ 短(10分鐘內)。

● 注意：

- ◆ 有2種情境，一個是產品外觀不能有SD卡/USB插槽，另一個是儲存在外接儲存媒體的影像要不可讀取。

● 正確結果：

◆ 情境1：

- ▶ 產品不存在卸除式儲存媒體使用的記憶卡插槽。
- ▶ 產品不存在卸除式儲存媒體使用的通用序列匯流排插槽。

◆ 情境2：

- ▶ 在未經授權的情況下，記憶卡內之影像資料不可被讀取。
- ▶ 在未經授權的情況下，透過通用序列匯流排接取之儲存裝置，其中之影像資料不可被讀取。



5.1.3.2 實體保護測試(2級)

- **測試目的：**
 - ◆ 驗證產品是否建立外殼拆除障礙。
- **測試時間：**
 - ◆ 極短(1分鐘內)。
- **注意：**
 - ◆ 無。
- **正確結果：**
 - ◆ 不可使用一般十字或一字螺絲。



5.3.2.2 網路裝置資訊探詢功能測試(3級)

- **測試目的：**

- ◆ 確認產品是否運行在具安全風險的網路設定。

- **測試時間：**

- ◆ 短(10分鐘內)。

- **注意：**

- ◆ 實驗室必須在預設狀態的情況下，實際去掃描是否開啟UPnP、Bonjour、SNMP等服務。

- **正確結果：**

- ◆ UPnP、Bonjour、SNMP預設皆關閉。



5.5.1.2 影像隱私外洩防護測試(2級)

- **測試目的：**

- ◆ 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。

- **測試時間：**

- ◆ 極短(1分鐘內)。

- **注意：**

- ◆ 無。

- **正確結果：**

- ◆ 隱私遮罩所圈選的圖像區塊不可視。

Thank You