影像監控系統標準公開說明會

TAICS TC5 網路與資訊安全技術委員會/資策會 資安所
高傳凱 博士

2017/12/08

大綱

- 影像監控系統資安標準現況
- 分級應用參考
- 影像監控系統資安標準-影像錄影機
  - 資安需求之強化
- 影像監控系統資安標準之測試規範-網路攝影機
  - 實體安全測試
  - 系統安全測試
  - 通訊安全測試
  - 身分鑑別與授權測試
  - 隱私保護測試
- 認證制度整體架構
- 試辦期實驗室認證流程
- 資安開發指引及自主檢測推動

影像監控系統資安標準現況

- IP CAM資安標準於 10月26日 已公告
- 正式版於11月21日發行，下載點:xxx。
- DVR/NVR 已於11月24日專家會議一致通過，於今日(12/8)正式對外公告。
- NAS因專家仍存有疑慮，尚在編修中，預期跟General Requirement同步公告。

分級應用參考

因素	None	1級	2級	3級
保護資產之價值	無價值影像(例:街景、樹木等)	無價值影像但照射在私人空間(例:寵物等)	重要影像(例:家人人像、公司新品等)	不容有失的影像(IP CAM監控對象的價值)
所處網路環境	LAN(無一對外網路接口)	LAN/Internet	Internet	Internet
實體防護	X	X	O	O
防止危害他人	X	O	O	O
具國際競爭力	X	X	X	O
檢測成本		10人天	8人天	2人天

滲透測試建議

模糊測試並行

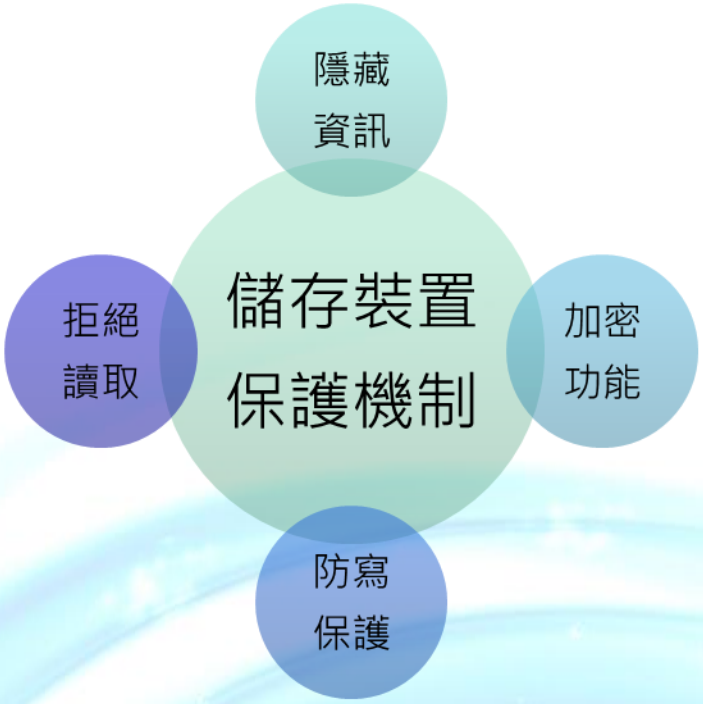
影像監控系統資安標準-影像錄影機資安需求之強化

DVR/NVR 強化之資安需求(1)

5.1.2 實體異常行為警示

2級

- 5.1.2.1(b) 產品支援儲存媒體（例如：硬碟機）保護機制，且產品之儲存媒體不應在本機以外的機器被存取。



資料來源:https://www.reneelab.net/disk-encrypt-software.html

DVR/NVR 強化之資安需求(2)

5.2.8 系統儲存安全

2級

- 5.2.8.1(c) 確保存取影像檔案具備權限控管機制，且透過通行碼鑑別機制防護。

資料來源:https://www.synology.com/zh-tw/knowledgebase/DSM/help/DSM/Tutorial/home_theater_videos

DVR/NVR 強化之資安需求(3)

5.2.9 系統備份安全

2級

- 5.2.9.2(a) 備份影像檔案須加密保護以確保機密性，且須採用FIPS 140-2 [10]所核可之加密演算法。

資料來源:https://www.reneelab.net/file-protector

DVR/NVR 強化之資安需求(4)

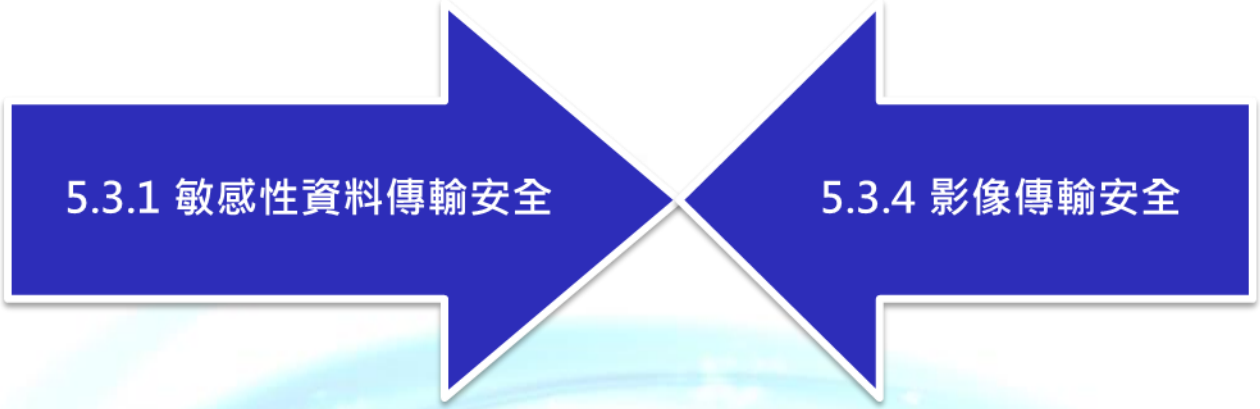
5.3.1 敏感性資料傳輸安全

1級

- 5.3.1.1(a) 敏感性資料之網路傳輸須通過安全通道，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）。

2級

- 5.3.1.2(a) 安全通道所使用之加密演算法須支援AES-256同等或以上加密強度的演算法。



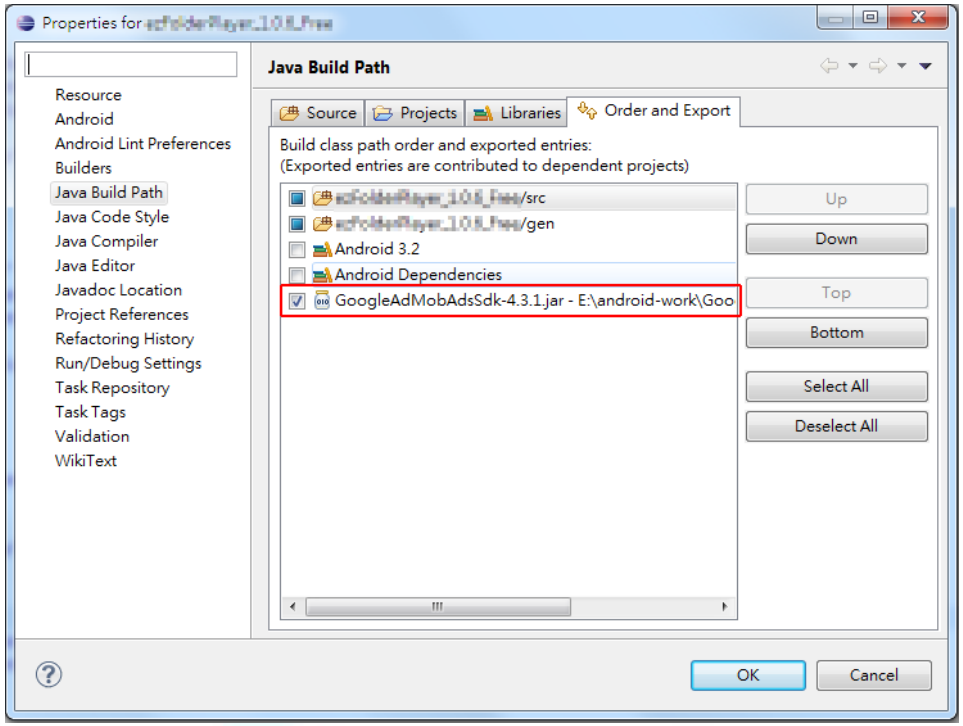
資料來源: https://play.google.com/store/apps/details?id=aes.secureencryptdecrypt

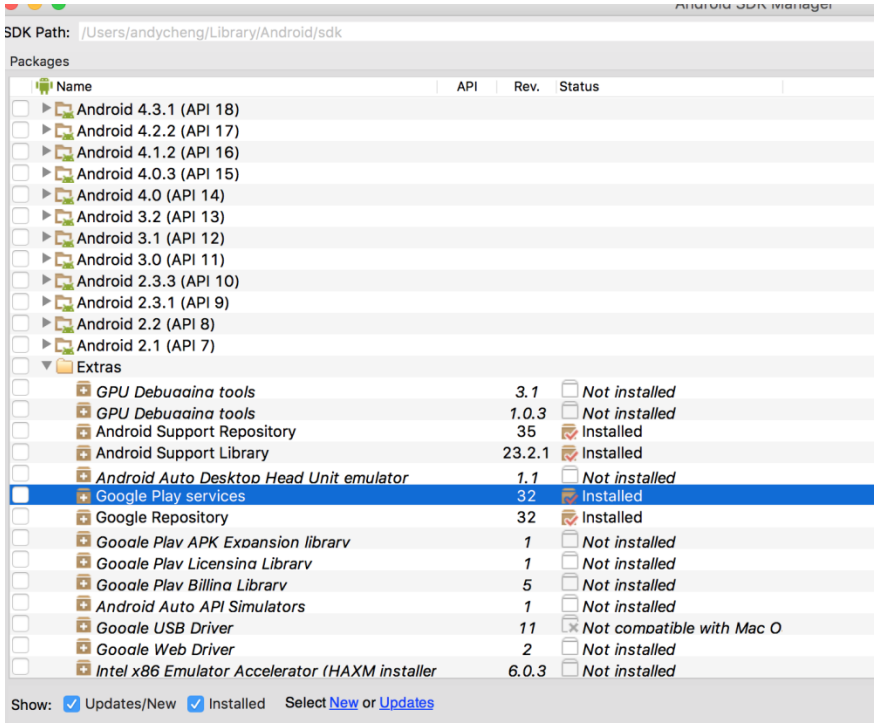
DVR/NVR 強化之資安需求(5)

5.5.1 程式信任來源

3級

5.5.1.1(a) 應用程式須於文件中標明所引用之第三方函式庫





資料來源:http://droidparadise.blogspot.tw/2012/04/adt-17noclassdeffounderror.html
資料來源:https://blog.ccjeng.com/2016/08/Firebase-Android-Library.html

影像監控系統資安標準之測試規範
-網路攝影機

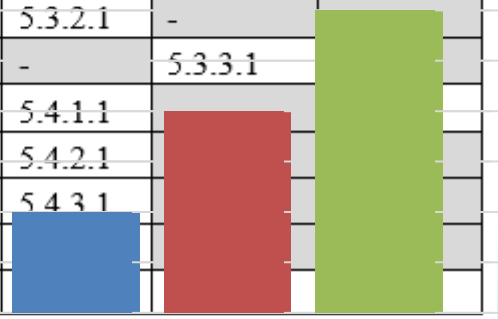
影像監控系統資安標準之網路攝影機之測試規範

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
實體安全	5.1.1. 實體埠之安全管控測試	5.1.1.1	5.1.1.2	-
	5.1.2. 實體異常行為警示測試	-	5.1.2.1	-
	5.1.3. 實體防護測試	-	5.1.3.1	5.1.3.2
	5.1.4. 安全啟動測試	-	-	5.1.4.1
系統安全	5.2.1. 作業系統與網路服務安全測試	5.2.1.1	-	5.2.1.2
	5.2.2. 網路服務連接埠管控測試	5.2.2.1	-	-
	5.2.3. 更新安全測試	5.2.3.1	5.2.3.2	-
	5.2.4. 韌體程式安全測試(選測)	5.2.4.1	-	-
	5.2.5. 敏感性資料儲存安全測試	-	5.2.5.1	5.2.5.2
	5.2.6. 網頁管理介面安全測試	5.2.6.1	-	-
	5.2.7. 操控程式之應用程式介面安全測試	5.2.7.1	-	-
	5.2.8. 系統日誌檔與警示測試	5.2.8.1	5.2.8.2	-
通訊安全	5.3.1. 敏感性資料傳輸安全測試	5.3.1.1	5.3.1.2	-
	5.3.2. 通訊介面安全設置測試	5.3.2.1	-	
	5.3.3. 通訊協定安全測試	-	5.3.3.1	
身分鑑別與授權機制安全	5.4.1. 鑑別機制安全測試	5.4.1.1		
	5.4.2. 通行碼鑑別機制安全測試	5.4.2.1		
	5.4.3. 權限管控測試	5.4.3.1		
隱私保護	5.5.1. 隱私資料的存取保護測試			
	5.5.2. 隱私資料的傳輸保護測試			

不同等級會有對應的特定安全要求

使用工具
Acunetix
Burpsuite
Binwalk
kali
Nessus
Nexpose
Nmap
PlayCap
Sslscan
Testssl.sh
Wireshark

欲符合較高等級之安全要求，必須先滿足較低安全等級要求



數字越大，安全等級越高

SECURITY TESTING
實體安全測試

- 檢測項目
  - 實體埠存取管控測試
- 測試標準
  - 使用者不應透過USB、 RJ45任一種實體埠存取作業系統之除錯模式
- 測試目的
  - 驗證產品是否提供可以直接存取除錯模式(即工程模式)的實體介面
- 備註
  - 產品須提供進入除錯模式的方法

SECURITY TESTING
實體安全測試

- 檢測項目
  - 最小實體介面測試
- 測試標準
  - 外接式儲存媒體使用的SD card插槽須移除
- 測試目的
  - 驗證是否可隨意從產品外部取得外接儲存媒體
- 備註
  - 外觀沒有，但產品的蓋子可以旋下裡面即有
  - 原規範有限制USB插槽

SECURITY TESTING
實體安全測試

- 檢測項目
  - 實體埠插拔操作記錄功能
- 測試標準
  - 產品須具有實體埠插拔操作記錄功能，包括USB埠及RJ45埠
- 測試目的
  - 驗證存取產品之實體介面是否有插拔紀錄

SECURITY TESTING
實體安全測試

- 檢測項目
  - 異常狀態警示機制
- 測試標準
  - 產品發生斷電、斷訊狀況，產品須提供警示機制
- 測試目的
  - 驗證產品遭受實體上之服務阻絕時，是否會發出警示聲
- 備註
  - 此應為安防領域關注的安全行為，修正為選測
  - 本機行為，而非遠端控制介面

SECURITY TESTING
實體安全測試

- 檢測項目
  - 實體保護測試
- 測試標準
  - 須採用一體成形或防拆螺絲等機殼防拆除保護設計
- 測試目的
  - 驗證產品是否有建立外殼拆除障礙
- 備註
  - 存在UART接腳、甚至是SD card插槽

SECURITY TESTING
實體安全測試

- 檢測項目
  - 內部實體安全測試
- 測試標準
  - 晶片與功能編號不應存在於電路板。
  - 一體成形之產品不適用此測試項目。
- 測試目的
  - 驗證產品是否在實體存取上，增加存取困難度

SECURITY TESTING
實體安全測試

- 檢測項目
  - 密碼還原機制安全設計
- 測試標準
  - 產品外觀不應有徒手即可輕易還原回預設密碼的設計
- 測試目的
  - 驗證產品的實體密碼還原設計，是否考量安全防護機制

SECURITY TESTING
系統安全測試

- 檢測項目
  - 作業系統與網路服務常見弱點與漏洞
- 測試標準
  - (初階要求)不得存在CVSS v3評分為最高風險9分以上
  - (中階要求)不得存在CVSS v3評分為最高風險7分以上
- 測試目的
  - 驗證產品是否存在已知資安漏洞而未修補
- 工具
  - Nessus

SECURITY TESTING
系統安全測試

- 檢測項目
  - 網路服務最小化測試
- 測試標準
  - 產品所開啟之網路服務連接埠(不包括UPnP所開啟之動態埠)，必須與產品自我宣告之內容相符
- 測試目的
  - 驗證產品是否潛藏未關閉之網路埠
- 工具
  - Nmap, Nessus
- 備註
  - Port 0, UDP port

SECURITY TESTING
系統安全測試

- 檢測項目
  - 韌體程式更新功能測試
- 測試標準
  - 產品應支援更新機制
- 測試目的
  - 驗證產品是否能持續更新，以填補未知漏洞的發生
- 備註
  - 僅檢查介面是否提供更新功能，不實際執行更新
  - 有更新功能卻沒有更新檔案可供下載

SECURITY TESTING
系統安全測試

- 檢測項目
  - 韌體程式更新測試 - 更新檔案的保護
- 測試標準
  - 韌體更新檔案應無法被拆解
  - 加密演算法不應使用列於「附錄A」之公認弱加密演算法機制
- 測試目的
  - 驗證產品的韌體更新檔是否有加密保護
- 工具
  - Binwalk, Hopper disassembler
- 備註
  - 是否符合附錄A由產品出示證明文件(i.e.,書審)

SECURITY TESTING
系統安全測試

- 檢測項目
  - 韌體程式更新測試 - 更新路徑的保護
- 測試標準
  - 產品支援線上更新，其更新路徑須通過安全通道，且安全通道所支援之密碼套件要求須符合「附錄B」的規定
- 測試目的
  - 驗證產品的韌體線上更新是否有傳輸加密機制
  - 產品須提供所有相連伺服器之宣告
- 工具
  - SSLScan, testssl.sh
- 備註
  - 附錄B以外的cipher suite，不允許被更新伺服器支援
  - 可能會導致產品損壞

SECURITY TESTING
系統安全測試

- 檢測項目
  - 韌體更新之完整性及可信度測試
- 測試標準
  - 經過竄改之更新檔案不應被成功更新
- 測試目的
  - 驗證產品是否會確認更新韌體的完整性及不可否認性
- 工具
  - Notepad++
  - GnuPG
- 備註
  - 可能會導致產品損壞

SECURITY TESTING
系統安全測試

- 檢測項目
  - 韌體程式碼之敏感性資料外洩(選項)
- 測試標準
  - 產品之程式碼與安裝檔內其他檔案，不應被檢出身分鑑別因子、加解密演算法之金鑰(不含非對稱加密用之公鑰)、私人資料及非預期/不合法之IP與URL
- 測試目的
  - 驗證產品之韌體檔案是否洩露敏感性資料
- 工具
  - Binwalk, Hopper disassembler
- 備註
  - 產品須提供所有相連伺服器之宣告

SECURITY TESTING
系統安全測試

- 檢測項目
  - 敏感性資料加密儲存測試
- 測試標準
  - 產品之程式碼與安裝檔內其他檔案，不應被檢出身分鑑別因子、加解密演算法之金鑰(不含非對稱加密用之公鑰)、私人資料
- 測試目的
  - 驗證產品之敏感資料於儲存狀態下是否加密保護
- 備註
  - 產品須提供所使用之加密演算法及敏感性資料儲存方式之證明文件

SECURITY TESTING
系統安全測試

- 檢測項目
  - 網頁管理介面弱點測試
- 測試標準
  - 產品之程式碼與安裝檔內其他檔案，不應被檢出身分鑑別因子、加解密演算法之金鑰(不含非對稱加密用之公鑰)、私人資料
- 測試目的
  - 驗證產品之網頁管理介面是否存在已知且尚未修補之漏洞
- 工具
  - Acunetix, Nessus, Nexpose
- 備註
  - 透過檢測工具來趨近測試標準的精神(i.e., repeatable, reproducible)

SECURITY TESTING
系統安全測試

- 檢測項目
  - 應用程式介面之認證機制
- 測試標準
  - 依5.4身分鑑別與授權機制安全測試標準
- 測試目的
  - 驗證產品之API是否具備身分鑑別與授權之功能
- 工具
  - 同5.4節
- 備註
  - 此條文不易判讀。

SECURITY TESTING
系統安全測試

- 檢測項目
  - 安全事件日誌檔測試
- 測試標準
  - 安全事件日誌的資料應包含時間、使用者身分及登入行為
  - 受測物若不具有可檢視之安全事件日誌功能，則本測試項目結果為失敗
  - 產品須對安全事件日誌檔進行權限控管，該安全事件日誌檔的身分授權須與產品自我宣告相符
  - 產品之日誌檔須具備保存期限之設計
- 測試目的
  - 驗證產品是否有安全事件紀錄供查
  - 驗證產品之安全事件紀錄是否有權限控管
- 備註
  - 供使用者檢視之介面
  - 產品須提供日誌檔保存期限之說明文件

SECURITY TESTING
系統安全測試

- 檢測項目
  - 日誌檔存取異常警示測試
- 測試標準
  - 日誌紀錄檔無法正常儲存時，須發出警示
- 測試目的
  - 驗證產品是否有確保安全事件紀錄正常執行之機制
- 備註
  - 填滿不是唯一的一條路，只要能觸發日誌檔無法儲存之事件即可
  - 日誌檔填滿是相當耗時的工作

SECURITY TESTING
通訊安全測試

- 檢測項目
  - 敏感性資料之傳輸保護初階測試
- 測試標準
  - (初階)敏感性資料之傳輸通道必須經過加密保護，且加密演算法須採用FIPS 140-2所核可之演算法
  - (中階)敏感性資料之傳輸必須採用安全通道，且安全通道所支援之密碼套件須符合附錄B的要求
- 測試目的
  - 驗證產品是否對敏感性資料有傳輸保護機制
- 工具
  - SSLScan, testssl.sh, wireshark
- 備註
  - 改成一律以安全通道為主
  - 不允許附錄B以外的cipher suite存在產品中

SECURITY TESTING
通訊安全測試

- 檢測項目
  - 通訊介面組態設置測試
- 測試標準
  - UPnP、SNMP及Bonjour服務必須提供使用者可自行開/關功能之設置
  - SNMP、Bonjour服務預設應為關閉
  - 產品具備WPS功能，則必須提供使用者WPS PIN開/關之功能，預設需為關閉
  - 無線網路預設加密模式必須使用WPA2
- 測試目的
  - 避免產品運行在具安全風險的網路設定
- 工具
  - SSLScan, testssl.sh, wireshark
- 備註
  - UPnP下一版本將會預設為關閉
  - WPS Locker安全要求移除
  - 不是WPS的功能開關，而是WPS PIN開/關

SECURITY TESTING
通訊安全測試

- 檢測項目
  - 網路介面存取設置測試
- 測試標準
  - 使用者不得透過有線或無線之網路連結方式存取作業系統之除錯模式
  - 存取作業系統之除錯模式應經過身分鑑別
- 測試目的
  - 避免產品可透過遠端連線存取作業系統之除錯模式
- 備註
  - 產品須提供進入作業系統除錯模式的方法

SECURITY TESTING
通訊安全測試

- 檢測項目
  - 通訊協定異常輸入測試
- 測試標準
  - 通訊協定必須經過異常輸入測試，產品於測試過程中不應發生程序崩潰(crash)到無法恢復運作
- 測試目的
  - 驗證產品是否存在通訊協定漏洞
- 工具
  - Doona, RTSPFuzzer, ohrwurm
  - Synopsis, Onward

SECURITY TESTING
身分鑑別與授權測試

- 檢測項目
  - 認證機制強度測試
- 測試標準
  - 身分鑑別機制具備抵抗重送攻擊的能力。
  - 從鑑別錯誤訊息無法推斷出合法使用者名稱。
- 測試目的
  - 驗證產品是否具備可靠的鑑別機制
- 工具
  - Burp Suite, Wireshark
- 備註
  - 行動裝置永遠只能自動登入，視為失敗

SECURITY TESTING
身分鑑別與授權測試

- 檢測項目
  - 裝置鑑別測試
- 測試標準
  - 產品須提供能鑑別相連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
  - 採用憑證鑑別須確保憑證有效性
- 測試目的
  - 驗證產品是否具備相連影像監控系統裝置之身分鑑別機制
- 工具
  - Burp Suite, Wireshark
- 備註
  - 檢測實驗室須考慮相連影像監控系統裝置之相容性問題

SECURITY TESTING
身分鑑別與授權測試

- 檢測項目
  - 憑證認證有效性測試
- 測試標準
  - 採用憑證鑑別須確保憑證有效性
- 測試目的
  - 驗證產品之憑證認證是否會確認憑證之發證單位、有效期限、格式錯誤及憑證簽章是否有效
- 工具
  - Burp Suite, Wireshark
- 備註
  - 須具備驗證憑證有效性的裝置，既不是手機更不是PC
  - 無法觸發

SECURITY TESTING
身分鑑別與授權測試

- 檢測項目
  - 通行碼鑑別機制測試
- 測試標準
  - 通行碼認證相關要求依GCB通行碼原則類別要求
- 測試目的
  - 強化密碼鑑別機制的強度
- 備註
  - 無防止暴力破解密碼之機制
  - 密碼強度不足
  - 首次登入未要求更改預設密碼
  - 產品不存在預設密碼者(非密碼為空)，可同時符合「相異預設密碼」及「首次登入要變更密碼」

SECURITY TESTING
身分鑑別與授權測試

- 檢測項目
  - 權限管控機制
- 測試標準
  - 透過遠端連線存取產品，必須具備權限管控機制，該使用者的身分授權須與產品自我宣告相符
  - 至少要有二個以上不同權限的角色
  - 產品之授權行為，須存在閒置時限供使用者設定，一旦遠端連線逾時、遺失或結束，須要求新的鑑別
- 測試目的
  - 確保授權機制之落實
- 備註
  - 無登出功能
  - 無授權時限，授權時限要求提供使用者設定介面

SECURITY TESTING

隱私保護測試

- 檢測項目
  - 隱私資料刪除功能
- 測試標準
  - 必須提供隱私資料的刪除功能
- 測試目的
  - 確保提供隱私資料擁有者刪除之權限
- 備註
  - 產品本身不具備影像儲存功能時，不適用

SECURITY TESTING

隱私保護測試

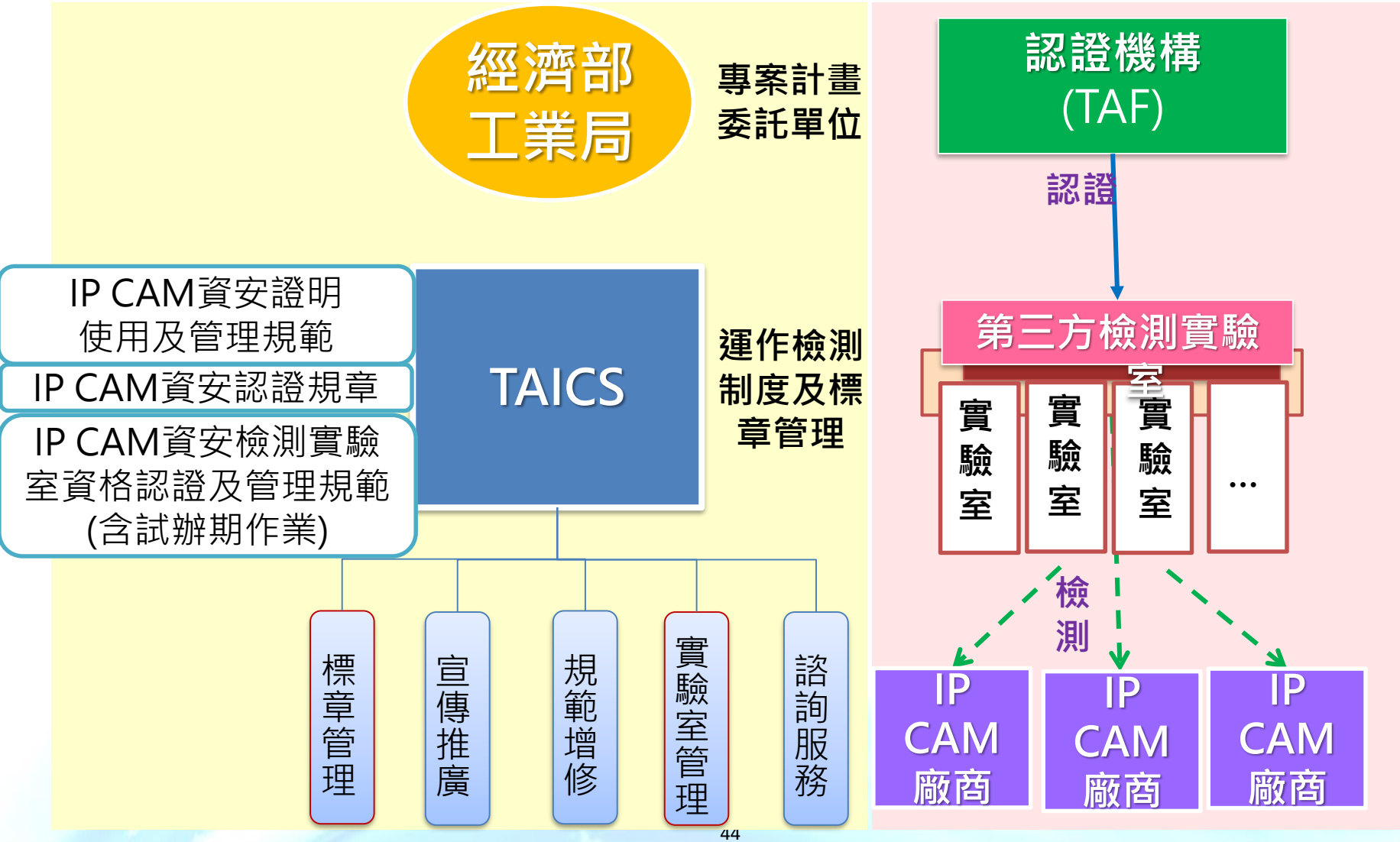
- 檢測項目
  - 登入警示功能測試
- 測試標準
  - 每次發生新的產品存取事件時，產品必須主動發出警示
  - 須於外殼設置狀態指示燈，顯示監控功能運行中
  - 以上二個測試標準擇一通過，本測試項目結果為通過
- 測試目的
  - 降低影像隱私資料外流之風險
- 備註
  - 二個測試標準擇一通過=本測項通過
  - 只要有人登入就要亮燈，不管有沒有在瀏覽監控畫面

SECURITY TESTING

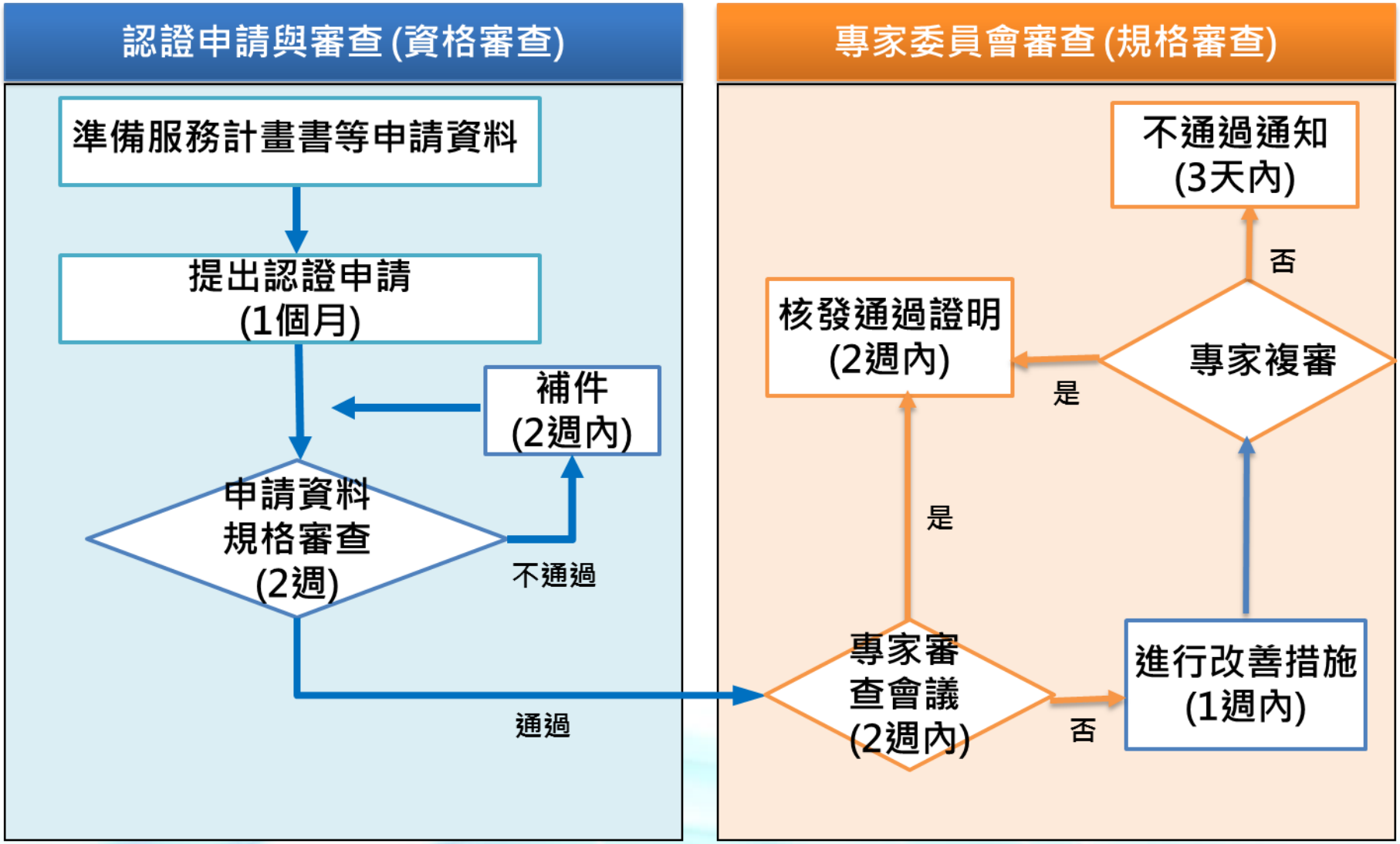
隱私保護測試

- 檢測項目
  - 隱私資料的傳輸機密性
- 測試標準
  - (1級)影像類的隱私資料不應以明文的方式傳輸，且保護資料的加密方式不應使用列於「附錄A」之公認弱加密演算法
  - (2級)影像資料與用戶資訊之傳輸必須採用安全通道，且安全通道所支援之密碼套件須符合附錄B的要求
  - (3級)確保隱私資料之網路傳輸加密演算法須支援AES-256
- 測試目的
  - 確保產品在影像隱私資料的傳輸上有加密保護
- 備註
  - 下一版，將一律要求採用安全通道
  - 下一版，在第三級將要求安全通道中與AES-256同等強度之加密演算法

認證制度整體架構


經濟部
工業局
專案計畫
委託單位
IP CAM資安證明
使用及管理規範
IP CAM資安認證規章
IP CAM資安檢測實驗
室資格認證及管理規範
(含試辦期作業)
TAICS
運作檢測
制度及標
章管理
標章管理
宣傳推廣
規範增修
實驗室管理
諮詢服務
認證機構
(TAF)
認證
第三方檢測實驗室
實驗室
實驗室
實驗室
…
檢測
IP CAM 廠商
IP CAM 廠商
IP CAM 廠商

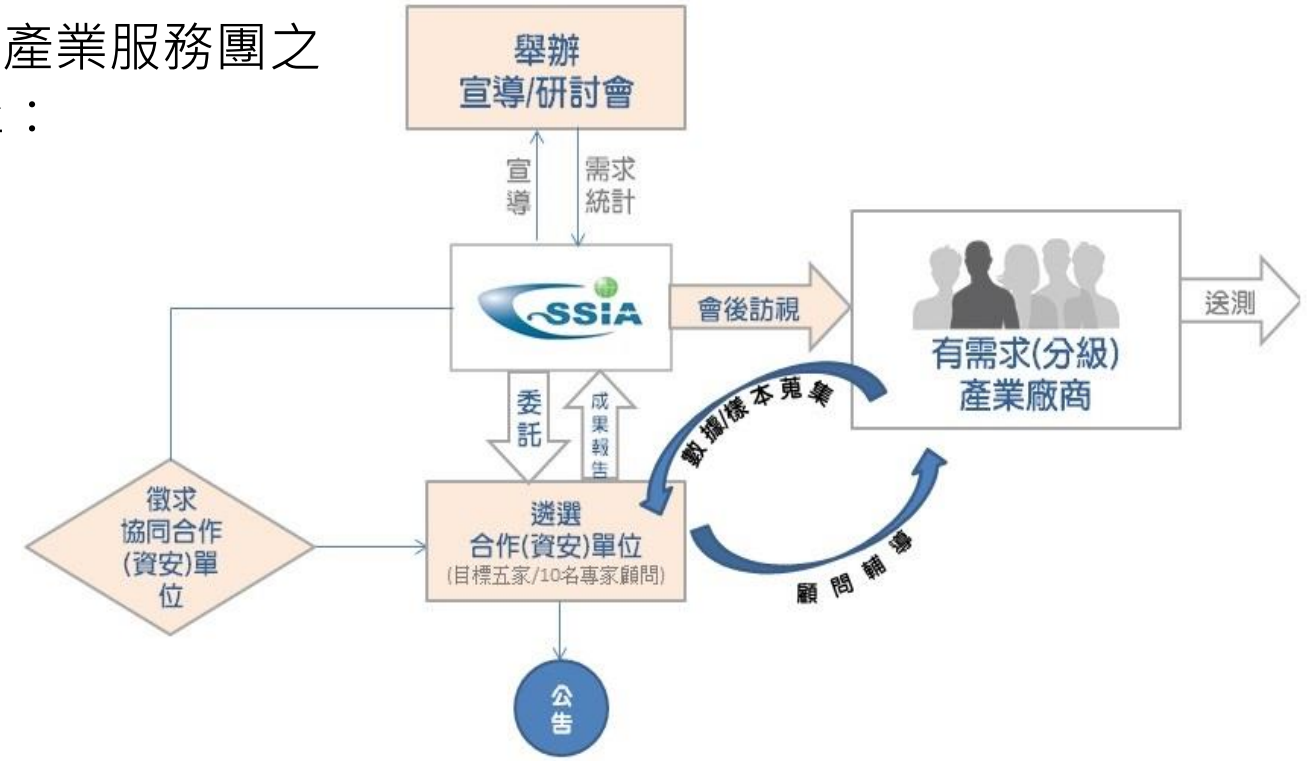
試辦期實驗室認證流程



註：實際作業將依執行狀況進行調整

資安開發指引及自主檢測推動

- TSSIA 安防協會產業服務團之工作計畫與流程：



- 資安產業標準(1.0版)推廣之廠商輔導及推廣說明會:預計於3-11月間舉辦，共計8場次
- 產業資安技術升級服務團:於上述每次宣導/研討會後，將依問卷及評量結果，產生輔導目標案；並開始請產業資安顧問進行輔導。


THANK YOU