影像監控系統資安認驗證與輔導成果

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

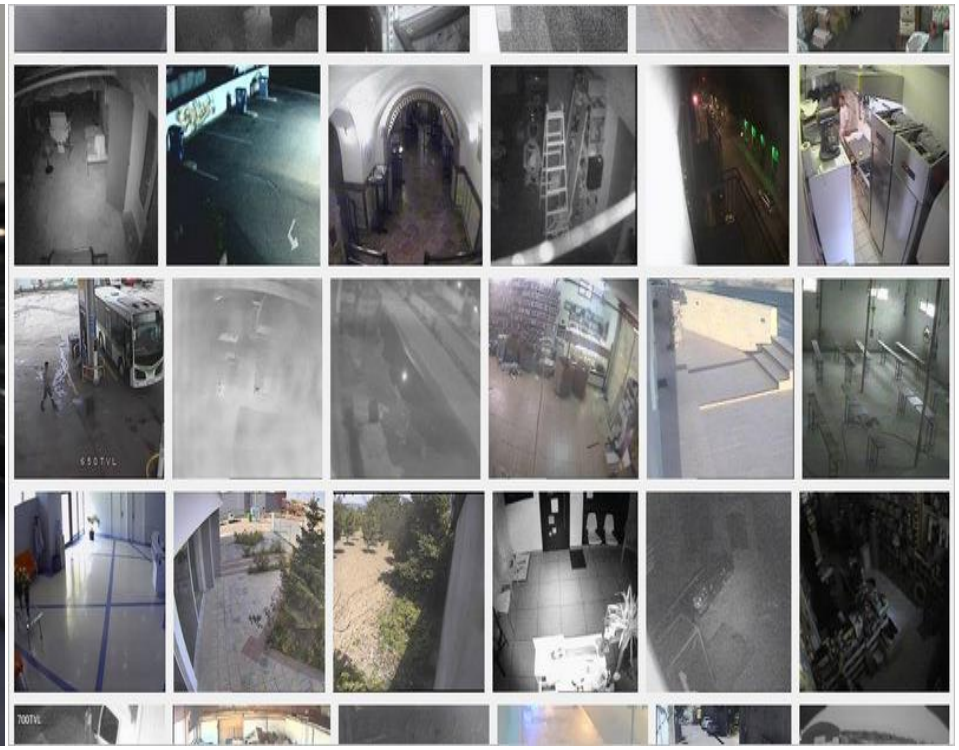
主辦單位 經濟部工業局

執行單位 財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY

台灣資通產業標準協會 Taiwan Association of Information and Communication Standards

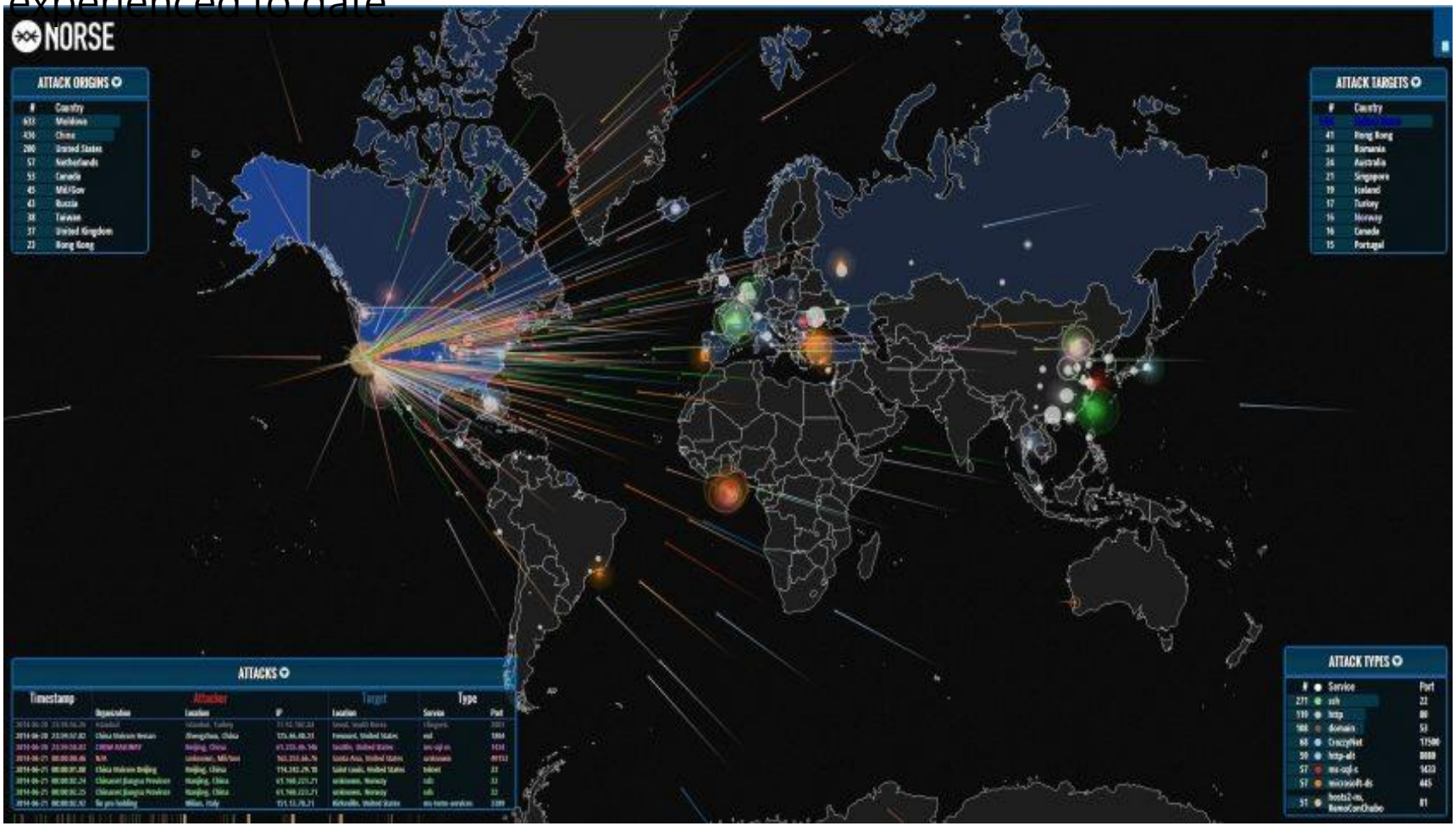
駭客入侵家用IP CAM

2015年7月，台中市一名36歲單身女子4月初在套房內裝設網路攝影機，讓她可以透過手機觀看房內2隻貓的動態，未料日前她竟意外發現，攝影機的鏡頭竟會跟著她轉動，且拍到她只穿內褲的下半身，在網路供人瀏覽，這時她才驚覺隱私已被看光光，嚇得決定搬家。



Mirai

In October 2016, 600,000 internet connected cameras, DVR’ s, routers and other IoT devices were compromised and used to for a massive Bot Net to launch what was the largest Denial Of Service (DOS) attack the internet had experienced to date.



CCTV were infected with ransomware

In the lead up to the 2017 US Presidential inauguration, 65 per cent of the recording servers for the city of Washington CCTV system were infected with ransomware. How did the attack take place? Whilst unknown, it most likely occurred by the same means as other common PC hacks such as infected USB keys, malicious web sites, or phishing attacks.

Canon相機入侵

- 2018年5月，Canon生產的網絡監控攝像頭多次遭到外部的非法訪問。千葉縣八千代市和埼玉縣上尾市設在水渠附近的水位監控攝像頭被侵佔而無法操作。迄今為止日本全國可能有 60 多台攝像頭遭到非法訪問。
- 很多事件中，畫面出現疑為黑客輸入的“I'm Hacked.bye2”字樣。雖然不清楚為何針對佳能的攝像頭，但受害的兩市等使用時均未更改初始密碼，安全弱點可能被鑽了空子。今後此類受害恐怕還會增加。

Why IP CAM

- 物聯網各領域必備的核心設備

標準制定成果 – 影像監控系統資安標準

TAICS TS0014系列標準：影像監控系統中各裝置之資安要求，包括實體安全、系統安全、身分鑑別與授權、網路安全、隱私保護。

TAICS TS0014-1：影像監控系統中各裝置之共通資安需求。

TAICS TS0014-2：網路攝影機之資安需求，特別注重在實體入侵。

TAICS TS0014-3：影像錄影機之資安需求，特別注重在影像儲存及備份。

TAICS TS0014-4：網路儲存裝置之資安需求，特別注重在影像儲存及備份。

TAICS TS0015系列標準之測試規範：提供測試目的、測試方法及預期結果等方法，以驗證受測物是否滿足TAICS TS0014系列標準中資安需求。

參與制定廠商：

中華電信、友訊科技、互聯安睿資通、安華聯網、行動檢測服務、宏達國際電子、果核數位、國立中央大學、（財）國家中山科學研究院、（財）工業技術研究院、（財）台灣電子檢驗中心、（財）資訊工業策進會、（財）電信技術中心、晶復科技、群暉科技、趨勢科技。

試行實驗室：

中華電信、安華聯網、（財）台灣電子檢驗中心、（財）資訊工業策進會

產品合規之功效

加州法規

預設密碼風險

- 產品不會使用相同預設密碼(5.4.2.1)

降低弱密碼風險

- 密碼長度、複雜度及連續字元都有要求(5.4.2.2~5.4.2.6)

防暴力破解密碼

- 禁止連續輸入錯誤且相異之密碼(5.4.2.4)

防止資料外洩

- 傳輸要走安全通道(5.3.1, 5.5.2)
- 儲存要加密，甚至存放於安全區域(5.2.4)

ONVIF API攻擊

- 防止ONVIF API偽造、重送、注入等攻擊。(5.2.6)

反韌體破解/竄改

- 韌體加密(5.2.3.1)
- 刷機防護(5.1.4)
- Hardcode禁止(5.2.3.1)

拒止中間人攻擊

- 具裝置間雙向認證(5.4.1.6)
- 憑證有效性驗證(5.4.1.4、5.4.1.6)
- 安全通道(5.3.1)

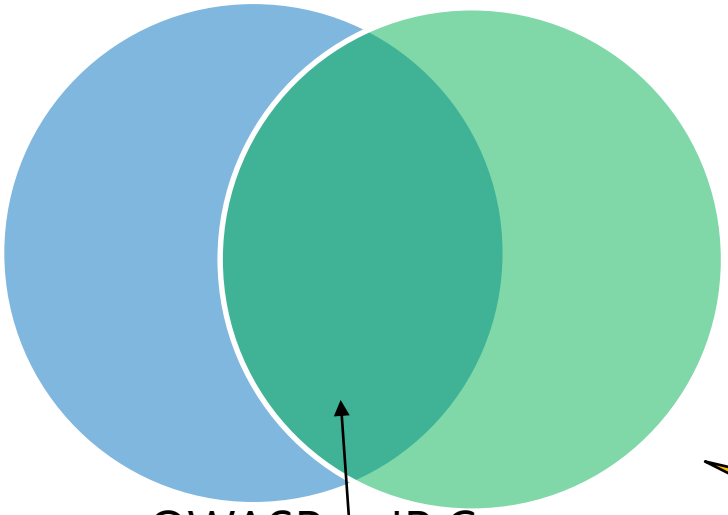
實體入侵防止

- 實體介面存取控管(5.1.1)
- SD卡存取保護(5.1.1.2)
- 外殼拆除難度(5.1.3.2)
- 安全晶片加值(5.1.4)

DDoS攻擊預防

- 強化身分鑑別機制，降低成為botnet殭屍機的機率(5.4.1.1)
- 登入警示(5.5.1.3)

OWASP IoT Top 10涵蓋率



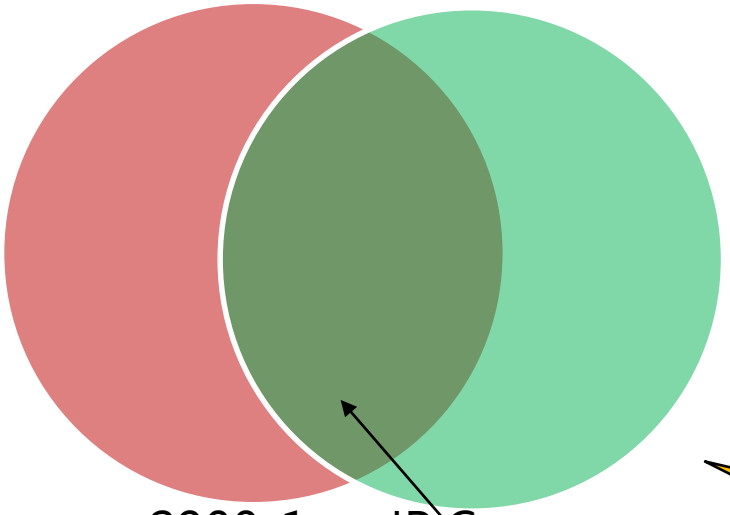
有6成的涵蓋率

For Example: (未包含的OWASP資安要求)
1. Ensuring the update server is secure.
2. the use of external ports such as USB to determine if data can be maliciously accessed on the device without disassembling the device.

8成9涵蓋率

去除掉IP CAM標準適用範圍外的要求
- I5: Privacy Concern (Privacy Notification)
- I6: Insecure Cloud Interface
- I7: Insecure Mobile Interface

ANSI/CAN/UL 2900-1 涵蓋率



For Example: (未包含的ANSI/CAN/UL 2900-1資安要求)

1. Binary code and Byte code analysis.

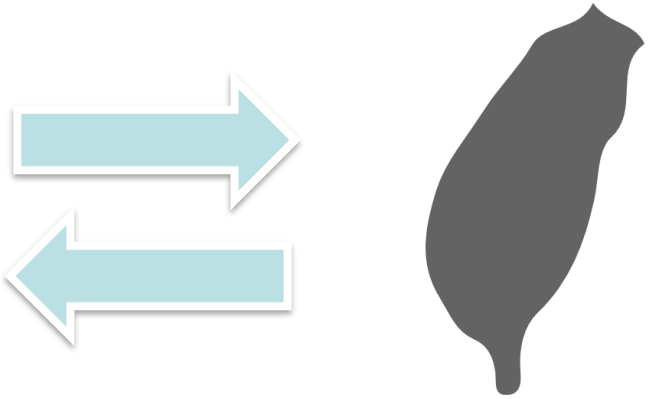
7成2涵蓋率

去除掉IP CAM標準適用範圍外的要求

- 12. Vendor Product Risk Management Process

國際推廣

與國際資安機構組織建立鏈結關係，透過相互資安標準認驗證制度交流，參與國際資安機構組織標準研訂，進而將國內完備資安標準推向國際



1. Video Surveillance Series Security Standards

廠商輔導政策

- **目的:**

  協助廠商迅速改善產品資安品質，輔導廠商產品符合標準要求。

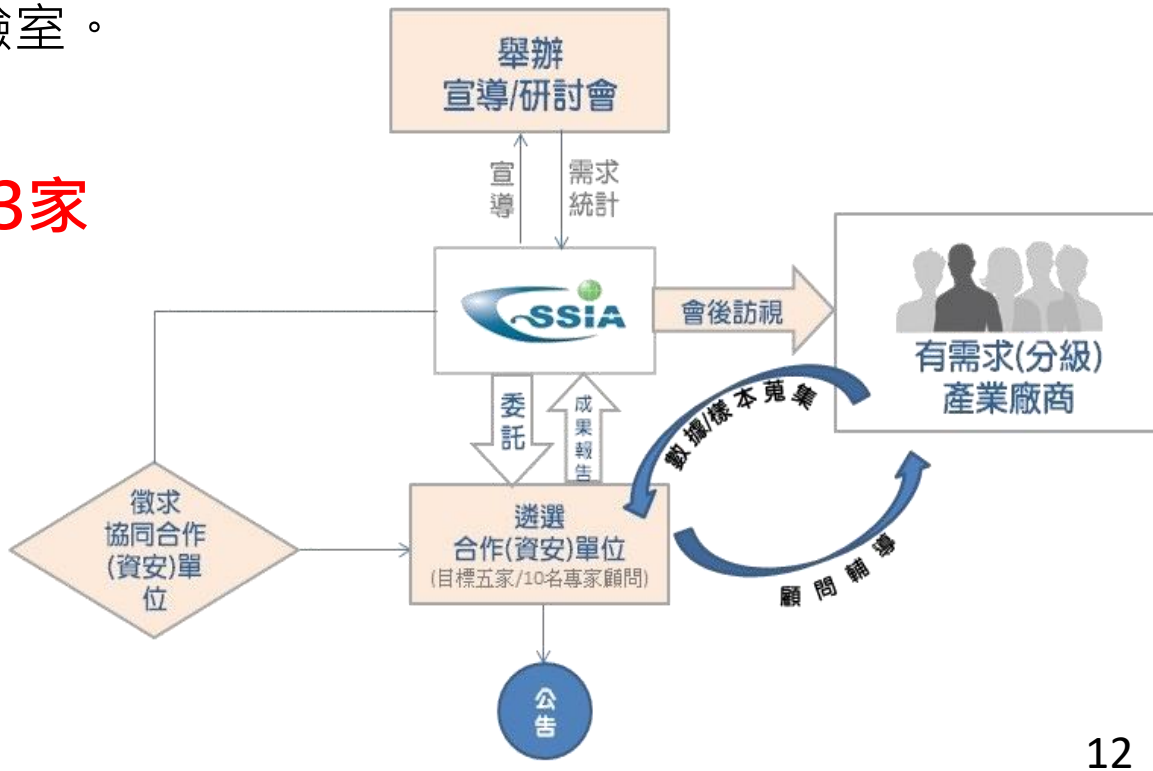
- **做法:**

  1. 開廠商輔導說明會(3場，共計16家廠商參與輔導)
  2. 資安顧問(6家資安檢測實驗室)進行輔導
  3. 媒合廠商與檢測實驗室。

- **成果:**

  通過實驗室檢測3家

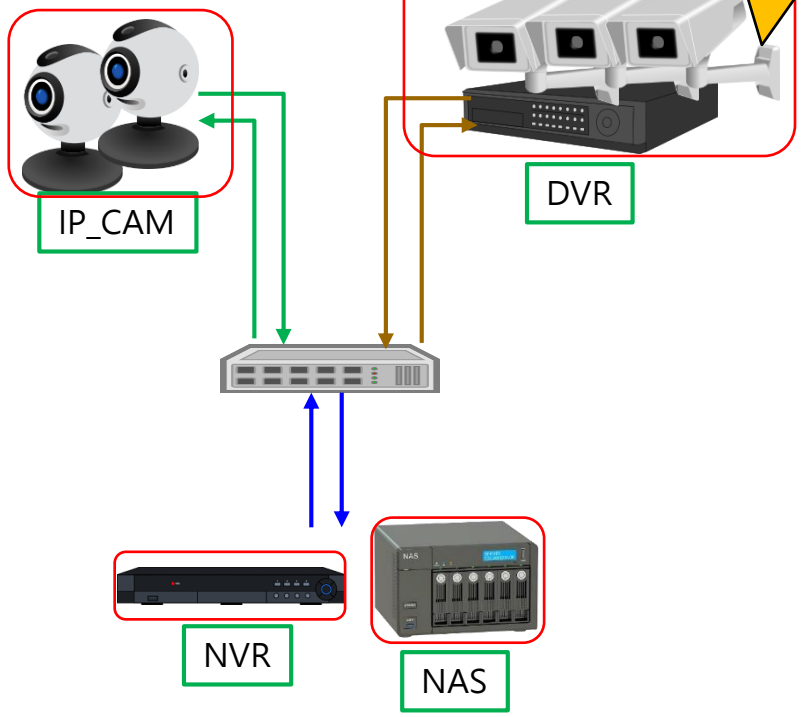
  取得證書1家

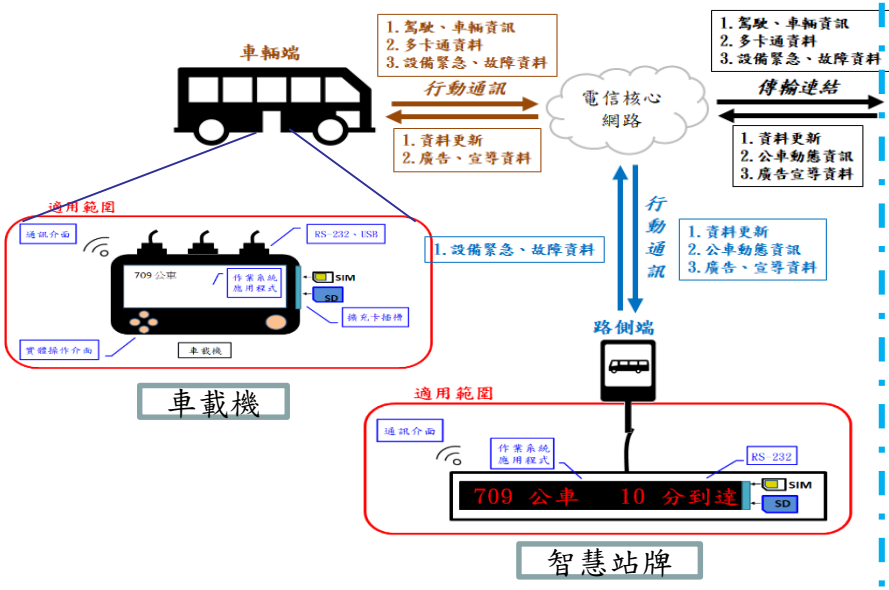


明年輔導對象

- 影像監控系列(包括: IP CAM, DVR, NVR, NAS)預計開放20個廠商輔導名額
- 智慧巴士系列(包括: 車載機、智慧站牌)預計開發5個廠商輔導名額

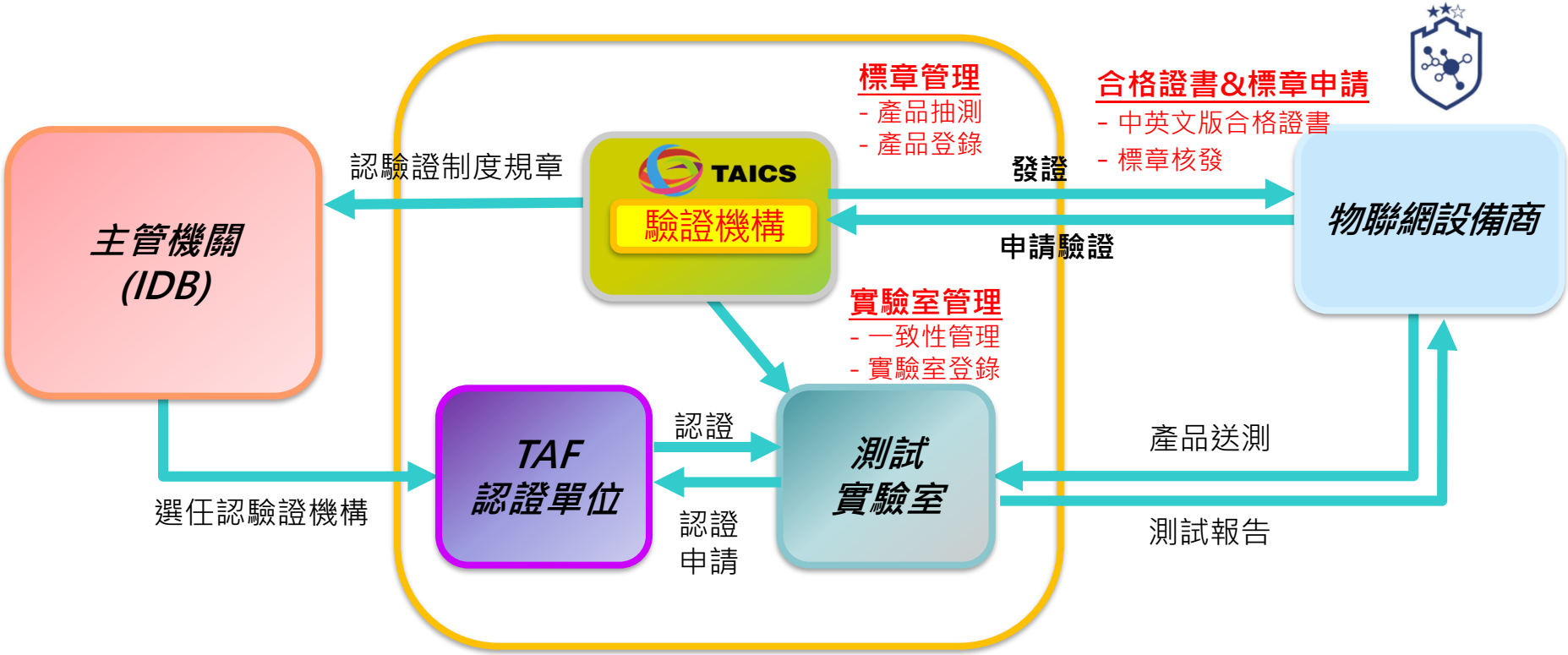
擴大輔導對象





實驗室與產品認驗證流程

制度推動暨驗證機構：由台灣資通產業標準協會(TAICS)擔任，負責實驗室管理、標章管理及產品驗證管理作業。



財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY

台灣資通產業標準協會
Taiwan Association of Information and Communication Standards

IP CAM驗證合格產品查詢

Step 1

Step 2

Step 3

序號	送檢單位名稱	設備名稱	設備型號	韌體版本	安全等級	測試機構名稱	發證日期	詳細資料
1	奇偶科技股份有限公司	兩百萬畫素網路攝影機	GV-BX2700-FD	v1.16 2018-10-15	2級	財團法人電信技術中心	2018/11/16	內容
2	奇偶科技股份有限公司	八百萬畫素半球型網路攝影機	GV-MD8710-FD	V1.00 2018-10-15	2級	財團法人電信技術中心	2018/11/16	內容

IP CAM認可實驗室查詢

Step 1

Step 2

Step 3

認證編號	機構名稱	實驗室名稱	TAF認可日期	聯絡人姓
1519	財團法人電信技術中心	資通安全檢測實驗室	2017/12/15	黃嘉章
3102	安華聯網科技股份有限公司	資安檢測實驗室	2016/01/28	劉作仁

揪團

- **推動IP CAM資安認證共同供應契約上架**
  1. 明年度制定IP CAM上架共契之制度規範。
  2. **檢測實驗室:** IP CAM資安檢測服務上架共契
  3. **IP CAM廠商:** 取得資安合格證書之IP CAM上架共契
- **推動政府相關採購補助計畫採用認證產品**

Contact:

高傳凱

資策會 資安所 聯網安全檢測組組長

TAICS TC Network and Security WG1 組長

+886-2-6607 8959

marskao@iii.org.tw