財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

2018

智慧應用-物聯網系統層級資安防護

財團法人電信技術中心 林炫佑副執行長

財團法人電信技術中心-資安發展定位

- 105年8月「資安即國安策略會議」會議結論，將國家安全會議資通安全辦公室、行政院資通安全處與國家通訊傳播委員會定位為政府資安鐵三角，共同推動我國資通安全工作。TTC為為通傳會轄下之財團法人，承接政府資安技術幕僚工作。
- 為推動通訊傳播網路資通安全工作，本中心協助通傳會執行資安旗艦計畫，並與國發會「亞洲·矽谷計畫-強化物聯網資安防護」計畫互補，共同打造安全的資安環境。

國家安全會議資通安全辦公室

國安會資通安全小組的幕僚機關，主要的任務包括執行並處理資通安全小組的決議，更得要協同行政院資安處建置不同體系的資訊交換平臺（ISAC，資訊分享與分析中心），更得做到統合協調網際防禦體系、網際偵蒐體系以及外管網際防護體系的相關防護工作執行與推動等。

行政院資通安全處

統籌資安工作建立各項資安制度，例如「資通安全管理法」立法、關鍵基礎設施資安防護、資安情資分享聯防、資安人才培育及輔導資安產業展等，並完成第五期國家資通安全方案，讓國家的資通安全維護機制更趨健全和完善。

國家通訊傳播委員會

建構通訊傳播網路完善資安防禦體系。NCC自106年起已著手執行4年期之「數位匯流/IoT資安威脅防禦機制暨資安實驗室建置與服務」計畫，包括建置資通安全防護中心、資通安全分析管理平臺、資安網路實驗平臺及資安檢測實驗室等。

財團法人電信技術中心-資安技術發展

物聯網資安檢測技術

- 具備聯符合邦資訊處理標準 (Federal Information Processing Standards, FIPS)、共同準則(Common Criteria, ISO/IEC 15408)、UL2900等資通設備之安全檢測技術規範等檢測能量
- 協助物聯網系統資安稽核服務，開發APP自動檢測研發工具、研發資安分析引擎，針對惡意行為分析、資安漏洞分析進行研究

5G/IoT系統可靠度確保

- 資通訊技術之發展及量測工具研發，包含LTE, NB-IoT及5G等技術研究
- 物聯網多維度效能評測、寬頻網路效能確保平台及骨幹網路異常流量偵測
- 擁有電信等級NB-IOT等級之網路開放場域，開放給學研單位進行相關設備或解決方案進行研究及概念性驗證。

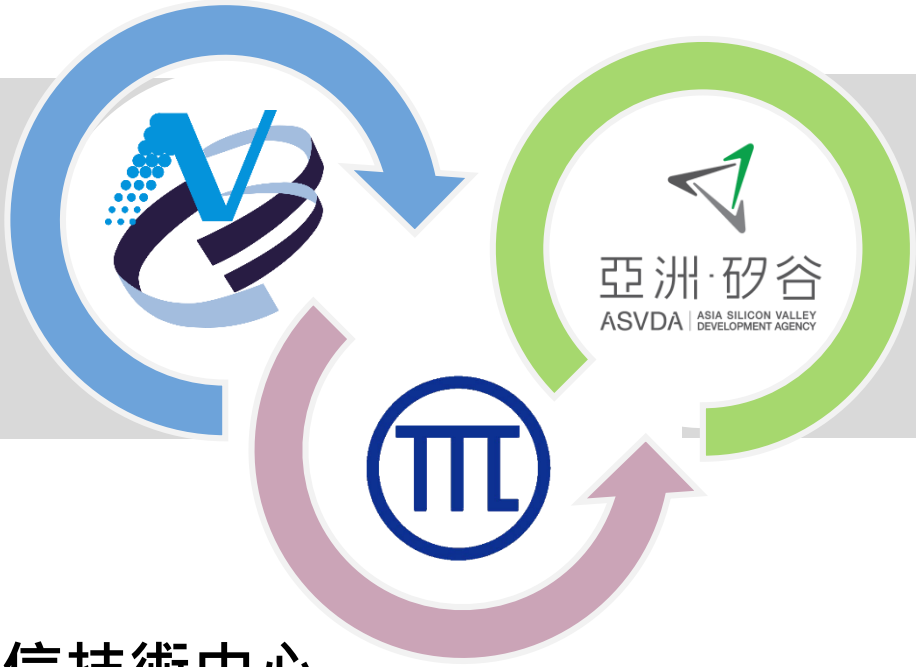
通傳網路資安防護技術

- TTC以扮演NCC技術智庫為目標，協助執行通傳網路資安聯防工作及關鍵基礎設施重大障礙管理
- 協助NCC制定資通訊產品安全技術規範及自願性認證標章推廣

計畫說明

國家發展委員會

為提升國內物聯網資通安全防護服務能量機制，協助國內企業提升其系統層級之資安防護能力，以因應物聯網新興智慧應用下所面臨的資安風險，推動本項計畫。



亞洲•矽谷計畫執行中心

亞洲•矽谷計畫執行中心將物聯網產業大聯盟區分為智慧交通、智慧家庭、智慧製造、智慧能效與環境監控、智慧商業、智慧物流、智慧農業、智慧醫療八大應用，涵蓋國際前瞻智慧城市之應用領域。

財團法人電信技術中心

執行國家發展委員會**「亞洲·矽谷—強化物聯網資安防護計畫」**，旨在建立物聯網系統層級資通防護評估與檢測機制，成立物聯網資訊分享及分析中心（IoT-ISAC），蒐集IoT相關資安事件資訊，透過分享達成資安聯防並降低IoT資安事件衝擊，協助國內企業提升資安防護能力。

物聯網資安議題

- Mirai殭屍網路，透過感染無線攝影機、路由器與監視器等非傳統運算裝置，操控包括位於**台灣在內的數十萬台IoT裝置**，用來執行分散式阻斷服務攻擊(DDoS)
- 全球透過家用網路路由器所發生的網路入侵總次數超過180萬次，其中高達八成是駭客透過遠端執行惡意程式碼入侵挾持裝置。在全球被攻擊國家次數排名中，**台灣為全球第9**。

01

複雜性與日遽增

不易確認與追蹤IoT系統新增終端設備，輕量型設備安全防護不易，異質設備統一資安等級也面臨挑戰

02

連帶效應發酵

由於物聯網終端設備數量龐大且各網互聯，即使微小的漏洞仍會造成極大的災難

03

系統更新困難

佈署在多樣化且不同網路的大量終端設備，系統更新將越來越困難

04

威脅模型難建立

物聯網新興應用造成的資安威脅模式很多可能都是沒有前例可參考，設備廠商因為缺乏資安威脅模型而無法提供好的解決方案

05

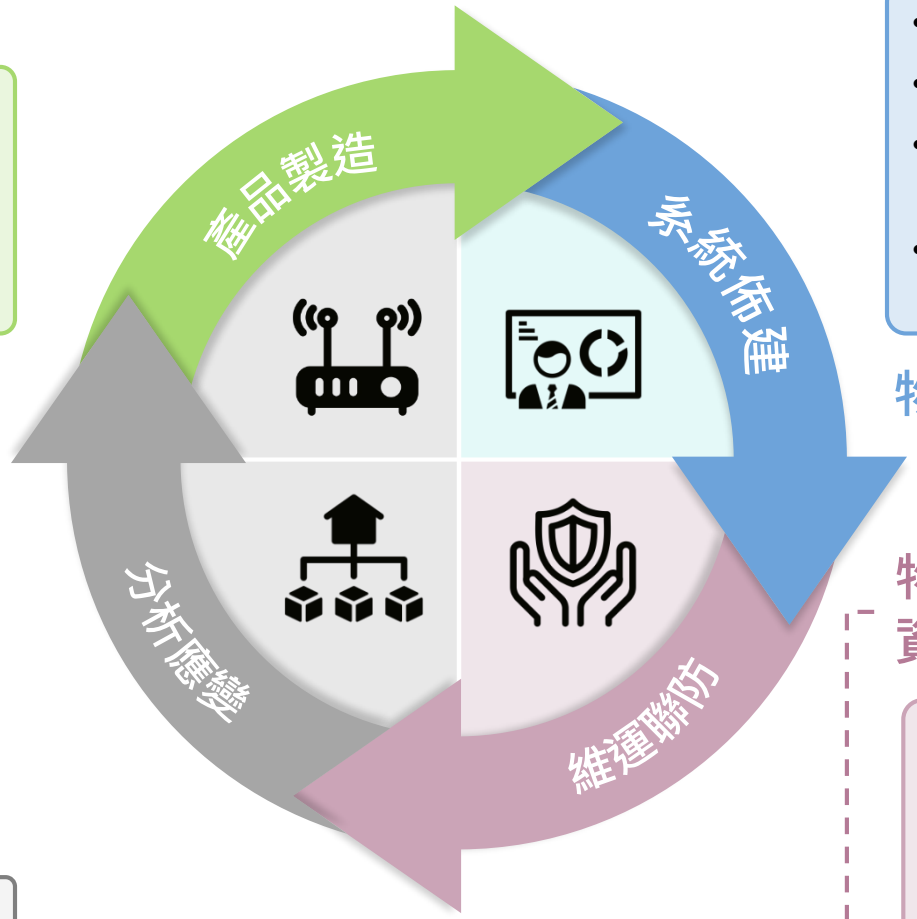
缺乏聯防機制

智慧城市推動IoT跨領域垂直應用，缺乏水平聯防以降低資安事件的衝擊

物聯網系統資安防護生命週期

- 物聯網相關電信管制射頻器材(IPCAM, WIFI AP....)檢測 (NCC)
- 手機內建APP檢測 (NCC、經濟部)
- 物聯網相關非電信管制射頻器材 (經濟部)

物聯網相關產品檢測



- 制定物聯網系統層級資安防護機制
- 整合物聯網系統層級資安試驗平台
- 與國際驗證單位合作，提供物聯網相關驗證服務
- 與工業局及NCC物聯網設備資安檢測規範互補(資安旗艦計畫)

物聯網系統層級資安防護機制

N-CERT、TW-CERT/CC

台灣電腦網路危機處理暨協調中心(中山科學研究院)結合產官學研能量，協調重大資安事件處理，提升整體資安聯防與應變能力

- 國家資安資訊分享與分析中心(N-ISAC)-行政院國家資通安全會報技術服務中心

物聯網資訊分享及分析中心

IoT-ISAC

- 針對非八大領域物聯網設備製造商、系統整合商及用戶提供ISAC服務
- 與N-ISAC及八大領域ISAC達成物聯網資安聯防目的
- 透過整合國內外情資資料庫、社群來源及檢測結果，建構IoT資安情資資料庫

亞洲·矽谷計畫-強化物聯網資安防護

建立物聯網系統層級資安防護評估機制

- 完成智慧家庭及智慧交通物聯網系統層級資安防護評估機制
- 物聯網資安試驗平臺
- 提供物聯網系統層級資安評估及檢測服務
- 與國際驗證單位合作

強化物聯網資訊分享與分析

- 規劃成立物聯網資訊分享及分析中心 (IoT-ISAC)
- 建立IoT-ISAC運作與技術服務模式

人才培育及知識擴散

- 物聯網資安防護評估機制與IoT-ISAC服務推廣
- 辦理說明會、培訓活動及成果發表會

分期推動重點

第1期
智慧家庭
智慧交通

第2期
智慧醫療
智慧製造
智慧農業

第3期
智慧能效與環境監控
智慧物流
智慧商業

建立物聯網系統層級資安防護評估機制

物聯網資安試驗平臺

智慧家庭
情境場域相關設備

智慧門鎖、門窗感應器、IP Camera、智慧門鈴、溫溼度感應器、空氣品質感測器、煙霧/可燃氣體感測器、智慧燈泡、智慧警報器、智慧掃地機器人、智慧家庭閘道器與DCU、應用及控制平臺

IoT-ISAC
WEB UI或XML

事件分析　訊息分享　事件回應

智慧交通
情境場域相關設備

感應設備閘道器、監控攝影機、WiFi AP、智慧停車應用系統、繳費設備 (Kiosk)、智慧路燈應用系統

建立物聯網系統層級資安防護評估機制

物聯網系統層級資安防評估機制

- 物聯網系統層級資安防護評估機制目的在於提供物聯網系統完整資安風險評估並確認其資安防護能力，資安風險評估事實上就是威脅確認及影響分析。
- 物聯網應用情境出發進行威脅建模Threat Modeling、漏洞檢測Vulnerability Testing、滲透測試Penetration Testing及影響分析Impact Analysis，建立最低可行安全性(Minimum Viable Security)

評估流程

威脅建模 Threat Modeling — 01

1. 確認IoT使用的軟硬體資產
2. 確認IoT系統架構及應用情境(受保護的目標)
3. 確認IoT系統資料流處理程序(Data-flow Diagram, DFD)
4. 確認並記錄威脅
5. 評估威脅(損害, 可重製性, 入侵性,是否容易被發現...)

漏洞檢測 Vulnerability Testing — 02

NIST NVD CVSS
或國內外已發佈之漏洞及風險

1. 採用Common Vulnerability Scoring System(CVSS)採用通用漏洞評分系統評估資產設備漏洞風險等級
2. 針對物聯網系統進行靜態原始碼掃描
3. 制定滲透測試項目及評估惡意程式感染風險

滲透測試 Penetration Testing — 03

1. 針對特定場域風險，執行Red Team攻防演練，以黑箱（Blackbox）測試為主以模擬外部攻擊
2. 參考OWASP IoT Top 10資安風險及已知各種場域可能的資安漏洞制定滲透測試規範
3. 根據威脅建模及漏洞檢測對應後制定滲透測試計畫

影響分析 Impact Analysis — 04

1. 依據滲透測試結果，評估IoT系統影響層面(包含技術、財務、人口、法律...)
2. 評估DREAD及OCTAVE Allegro兩種影響評估分析模型並依據不同垂直應用，選擇適當的評估方式

建立物聯網系統層級資安防護評估機制

物聯網系統層級最低可行安全評估規範(草案)

第一部通用要求

第二部為針對物聯網垂直應用制定安全防護特別要求

- 範圍 (第1章)
- 引用標準 (第2章)
- 名詞定義 (第3章)
- 最低可行安全評估 (第4章)

評估流程

威脅建模 Threat Modeling	漏洞檢測 Vulnerability Testing	滲透測試 Penetration Testing	影響分析 Impact Analysis
第 5 章	第 6 章	第 7 章	第 8 章
20 個通用威脅模型	**38** 個安全控制項目	**19** 項滲透測試情境	**2** 個衝擊分析模型
	15 項漏洞/弱點檢測	**18** 個滲透測試項目	

物聯網資安試驗平臺

物聯網系統層級資安防護評估試驗平臺

物聯網系統層級資安防護評估試驗平臺規劃必須能夠完整實現MVS評估程序，進行智慧家庭及智慧交通的最佳實務應用(Best Practice)

試驗平臺包含
1、威脅建模平臺
2、漏洞檢測平臺
3、滲透測試平臺

威脅建模平臺

第3步 根據資產表及網路與資料流架構進行資安威脅列表

第2步 解析並記錄智慧家庭或智慧交通系統架構及資料流向

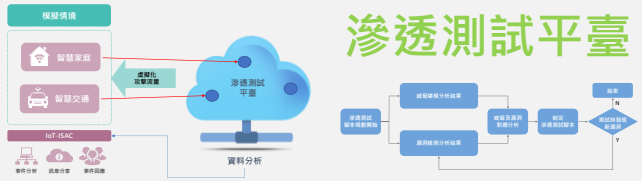
第1步 確認設備資產

- 威脅建模平臺將整合Microsoft Threat Modeling Tool(TMT)及以架構為基礎(Architecture-based)的威脅建模。
- 透過威脅建模平臺，可以得知受測智慧家庭或智慧交通系統的潛在威脅、各項設備軟硬體資訊及功能運作流程等資料

漏洞檢測平臺

- 漏洞檢測平臺對於可能產生重大資安威脅的設備及相關通訊協定進行漏洞檢測
- 以靜態源碼、韌體檔及惡意程式掃描檢測，並基於找出之CVE漏洞所對應CVSS權重值結果為主進行漏洞風險高低評估，並針對開源代碼的合規性進行檢測，確保授權(License)和智慧財產權的合法使用

滲透測試平臺



- 滲透測試主要的目的在於透過檢測手段評估威脅建模的各種威脅在各種檢出的漏洞下，確認實現該項威脅的可能性
- 滲透測試執行將參考OWASP物聯網定義的攻擊面向(Attack Surface)，針對不同攻擊面向進行評估與規劃

建立物聯網系統層級資安防護評估機制

物聯網系統層級資安防評估機制

DREAD威脅模型評估及風險值給分參考

評估風險係數的演算法模型，對這5個維度針對每個威脅進行等級評估。5個維度的平均值即為該威脅風險值，風險值越大，表示威脅風險越高

	低	中	高
給分	1	2	3

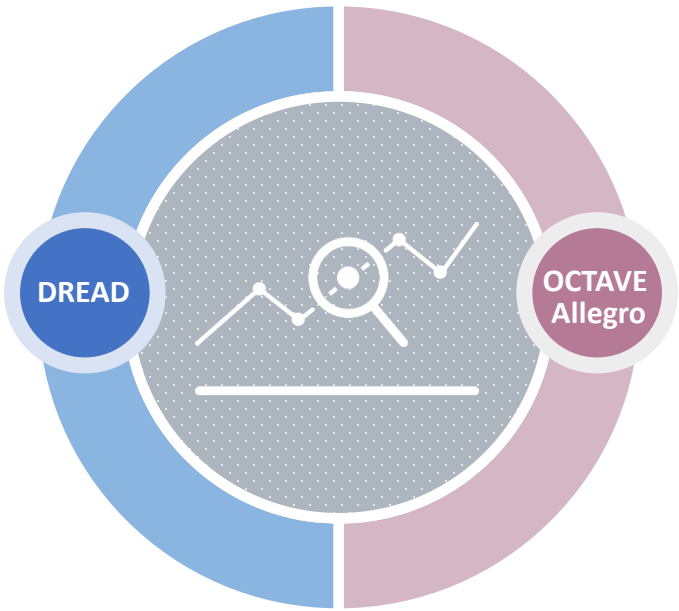
D **Damage Potential 潛在破壞性**
如果這個"漏洞風險被攻擊者利用"進行攻擊，會對企業和組織造成多少破壞

R **Reproducibility 重現難度**
要重現這個漏洞攻擊的難度有多大

E **Exploitability 可利用性**
要發動這個攻擊需要哪些條件

A **Affected Users 受影響用戶**
有多少用戶會遭受到這個風險漏洞的影響

D **Discoverability 發現難度**
對於攻擊者來說，要發現這個漏洞的難度有多大



OCTAVE Allegro影響程度評估準則

偏重於威脅發生造成使用者各種層面的影響評估。各維度的影響程度區分低(Low)、中(Moderate)、高(High)三級。

Reputation and Customer Confidence 聲譽及客戶信心
非商業用戶商譽受影響，商譽回復費用為0或低於或高於1萬美金；商業用戶回復費用為0或低於或高於10萬美金，且流失率低於 5 %或5-10%或10%上者

Financial Loss 財物損失
非商業用戶增加的年維運費用及一次性財務損失；商業用戶的年營收損失

Productivity 生產力
商業用戶增加人力成本低於5萬美金、介於5~10萬美金或高於10萬美金

Life Safety and Health 生命安全與健康
對於使用者生命、健康及安全性等影響程度

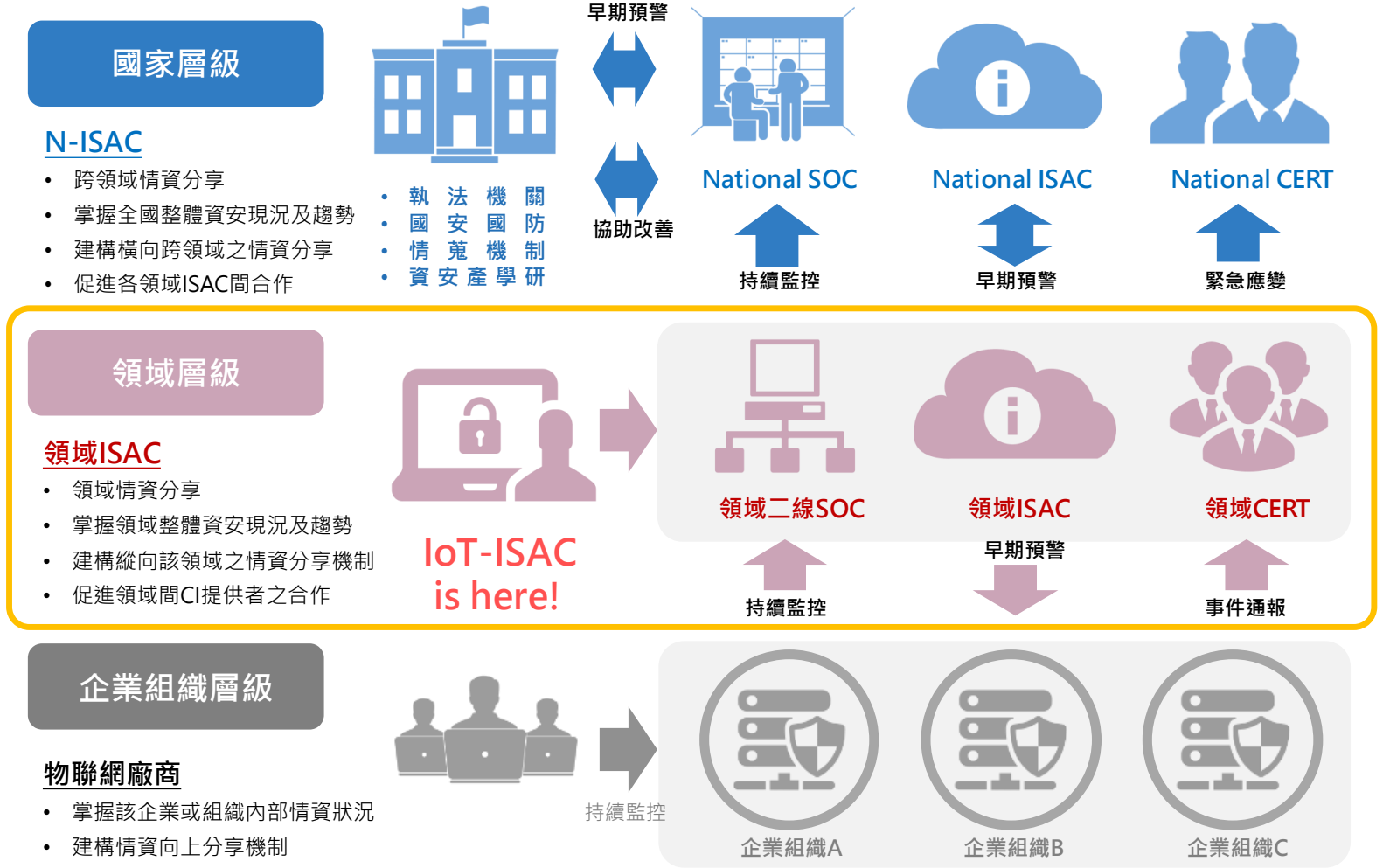
Fine and Legal Penalty 罰金與法律懲罰
罰金、無法律訴訟或訴訟損失及是否須接受政府部分或其他調查單位查詢等影響


IoT-ISAC

物聯網資訊分享及分析中心 (IoT-ISAC)

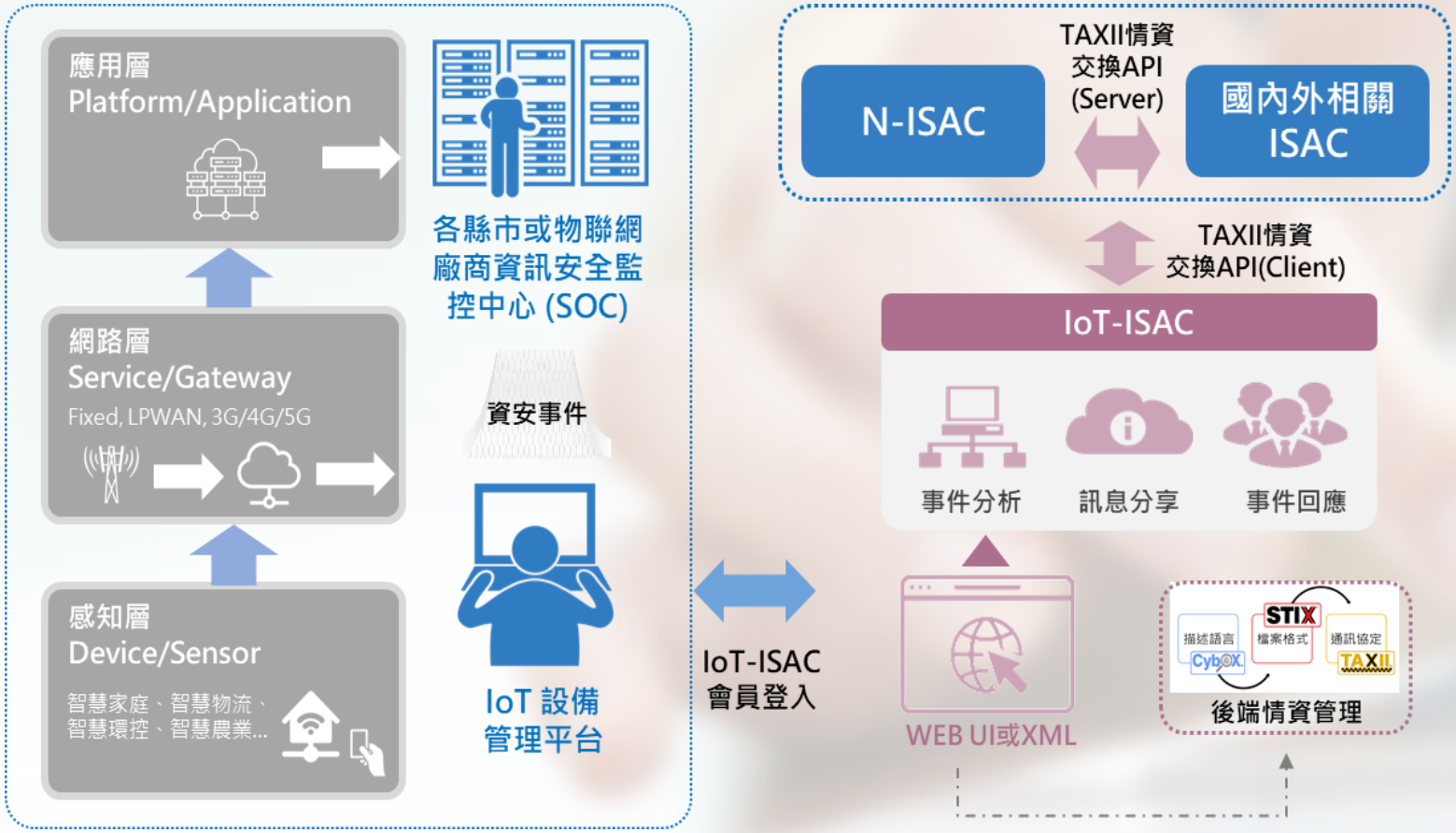
物聯網資訊分享及分析中心(IoT-ISAC)定位

- 規劃成立亞洲矽谷物聯網九大SIG新興應用領域的物聯網資訊分享及分析中心(IoT-ISAC)，以因應物聯網新興智慧應用下所面臨的資安風險。
- IoT-ISAC建置步驟依據「106年國家資通安全防護整合服務計畫-領域ISAC實務建置指引」進行規劃，採用STIX與TAXII，保留未來介接之彈性，完備領域 CERT、SOC及 ISAC間的協同合作。
- IoT-ISAC體系中第二層為各CI領域層級，角色為各CI領域主管機關所維運之領域ISAC。其主責為CI領域內之情資分享，以掌握轄管領域內資安防護現況與趨勢，透過建構縱向之情資分享機制，促進該領域內相關成員之合作。



物聯網資訊分享及分析中心 (IoT-ISAC)

IoT-ISAC服務對象及平臺架構



- IoT-ISAC平臺主要服務對象為新興應用領域特有設備器材、資訊系統、相關應用服務、物聯網系統及各縣市或物聯網廠商資訊安全監控中心(SOC)，其資安威脅、弱點及已知事件等情資需求，皆屬IoT-ISAC平臺情資分享範圍。
- 為使IoT產業組織及相關使用單位(如各縣市政府、亞矽辦公室等)等服務對象能有效接收與利用情資，將依據服務項目內容，規劃與分配相關資源。

物聯網資訊分享及分析中心 (IoT-ISAC)

IoT-ISAC會員服務項目

資安事件通報

即時對資安事件進行蒐集及分析，並可分享至其他領域ISAC，以達成政府與民間資安聯防效益。

資安情資分享

針對IoT-ISAC服務對象之資安風險進行情資蒐集、交換以及分析，與IoT-ISAC會員分享，以利管理與資安人員及早因應，考量資安訊息龐大且雜，未來針對付費會員可進行客製化服務。

資安監控與偵測

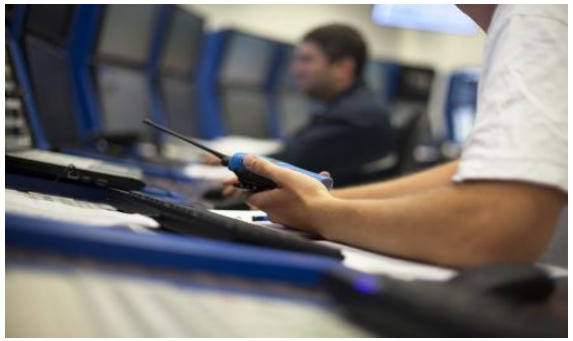
針對IoT-ISAC進行監控，透過網頁查詢事件分類、事件通報、事件處理、事件管理、知識庫、日誌紀錄（包括事件日誌與監控設備維運日誌）及相關資安統計圖表

緊急情況合作

研判與通知緊急資安事件，協助掌握整體資安現況及趨勢

威脅與弱點分析

結合本計畫物聯網資安試驗平臺及IoT-ISAC蒐集的資安威脅情資進行分析，並將分析結果納入資安通報系統，以防範未發生的資安威脅



國際交流

IoT-ISAC初期將提供國外情資分享與交流，並與國際驗證單位合作追蹤全球網路事件，加強跨國事件應變能力。

資安教育訓練

提供資安教育訓練，定期針對資安相關人員進行初階及中高階之培訓，同時結合其他領域ISAC共同舉辦資安人才培育活動。

資安事件協助處理

協助IoT-ISAC會員進行資安控管、漏洞評估及系統層級資安評估服務以及資安事件提供緊急應變的處理方式

說明會、教育訓練及相關培訓活動

免費參加培訓、推廣等各項資安相關活動

推廣說明會

資安防護評估與檢測機制及IoT-ISAC推廣說明會，分別於北、中、南辦理，分享國內外最新資安技術及產業趨勢議題，與產、官、學、研代表共同交流，現場提供物聯網資安防護評估機制與IoT-ISAC說明，及加入會員與相關Q&A服務。

資安研討與人才培訓

辦理資安技術研討交流，建立人員培訓機制，針對一般人員、資訊人員及主管等不同對象，規劃資安認知、作業實施、專業技術或管理課程，以提升人員的資訊安全意識，落實資安通報流程、事件處理等作業流程，並強化資安人員技術的研發創新能力，培育物聯網資安關鍵人才能量。

防禦測試與攻防演練

- 協助物聯網廠商及縣市政府等相關人員瞭解IoT-ISAC運作模式，共同參與系統層級資安防護審核平台測試。
- 舉辦實際攻防演練並展示資安防禦測試平臺，同步與產業串連，將整體資安分享及防禦機制能移轉給產業。

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

2018

亞洲·矽谷計畫-強化物聯網資安防護(第1期)

謝謝聆聽，敬請指教