物聯網資訊設備盤點集資安防護措施

重大資安事件回顧

- 物聯網設備潛在的資安危機
- 物聯網設備攻擊案例分析
- 物聯網設備的資安防護措施
- 物聯網設備盤點實務

遠端工作介面模糊化衍伸的資安問題

疫情資訊人心惶惶也成為一大誘餌，攻擊管道舉例來說，**電子郵件、假冒應用程式、惡意網域與社群等**，在企業遠距工作模式下，趨勢科技預期將有更多變臉詐騙 (Business Email Compromise, BEC) 出現，假冒供應商寄發銀行帳號或付款方式變更的郵件，企圖誘使企業員工匯款。而大眾對疫情資訊的迫切需求也將成為駭客入侵的機會點，駭客將持續利用與疫情相關的資訊散布釣魚郵件，引誘使用者點擊惡意連結或開啟惡意附件，以達到竊取個資等目的。

另外，在疫情期間不少公司**遠端辦公**，企業快速應變卻也造成資安上的漏洞，因為疫情形成混合辦公型態，使得邊界變模糊，趨勢科技認為駭客將利用家庭網路漏洞，對企業網路發動供應鏈攻擊，企圖找到 VPN 網路中具有關鍵數據或企業機密的目標，進一步攻擊以竊取企業資料。對此，零信任模式 (Zero Trust) 將在明年成為企業安全策略關鍵點之一，如何落實安全存取可視性及提升訪問資料的管理權限，將為企業防禦佈局重點。

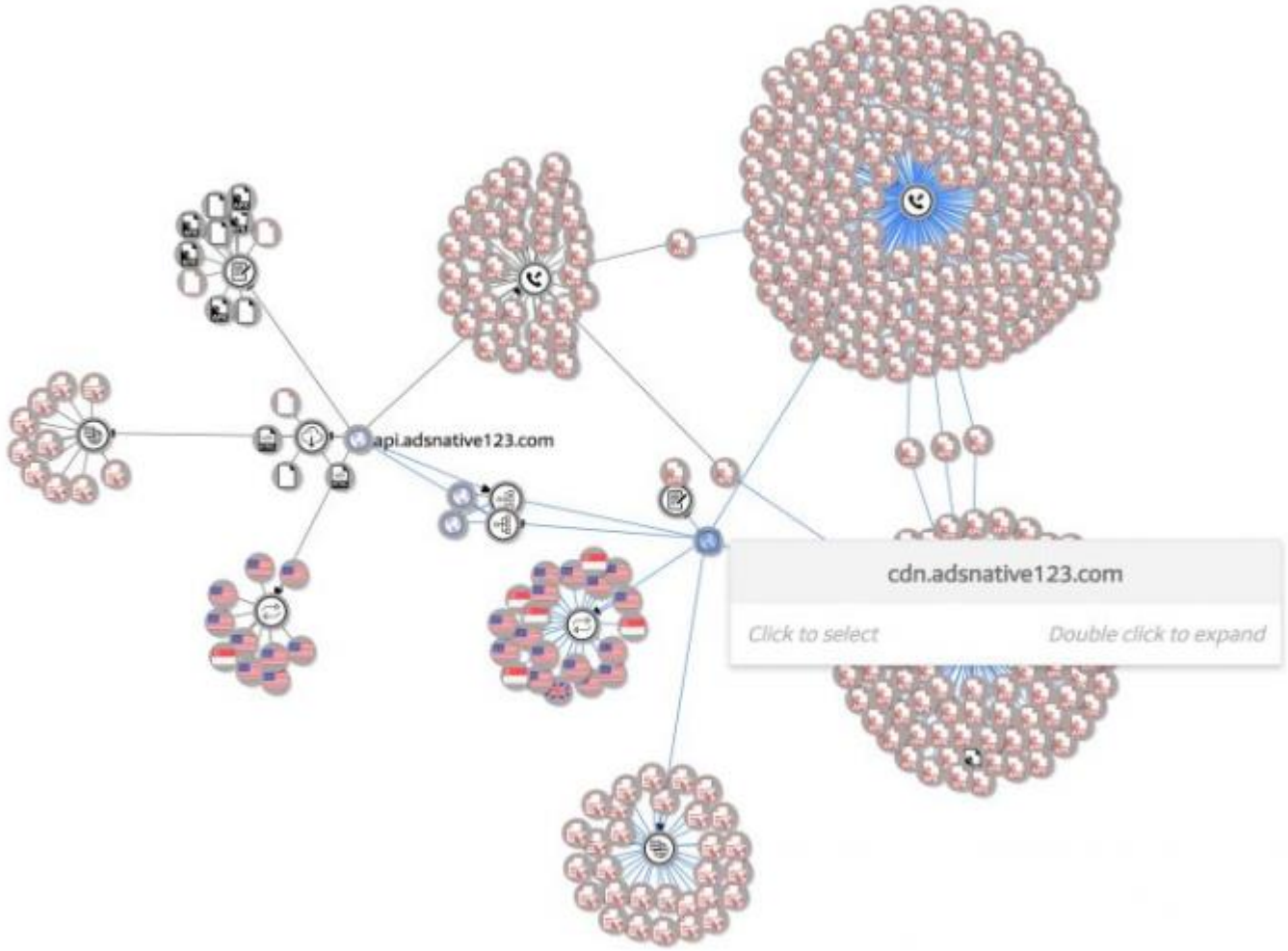
10款手機App暗藏「惡意程式」嚴重恐盜銀行帳戶

Check Point Research 發文公布了10款曾有惡意程式的手機App，分別是**Cake VPN、Pacific VPN、eVPN、BeatPlayer、QR/Barcode Scanner MAX、eVPN、Music Player、tooltipnatorlibrary、QRecorder**。

Name	Package_name
Cake VPN	com.lazycoder.cakevpns
Pacific VPN	com.protectvpn.freeapp
eVPN	com.abcd.evpnfree
BeatPlayer	com.crrl.beatplayers
QR/Barcode Scanner MAX	com.bezrukd.qrcodebarcode
eVPN	com.abcd.evpnfree
Music Player	com.revosleap.samplemusicplayers
tooltipnatorlibrary	com.mistergrizzlys.docscanpro
QRecorder	com.record.callvoicerecorder

Check Point Research公布10款App藏有惡意程式。 圖／Check Point Research

惡意廣告伺服器關聯示意圖

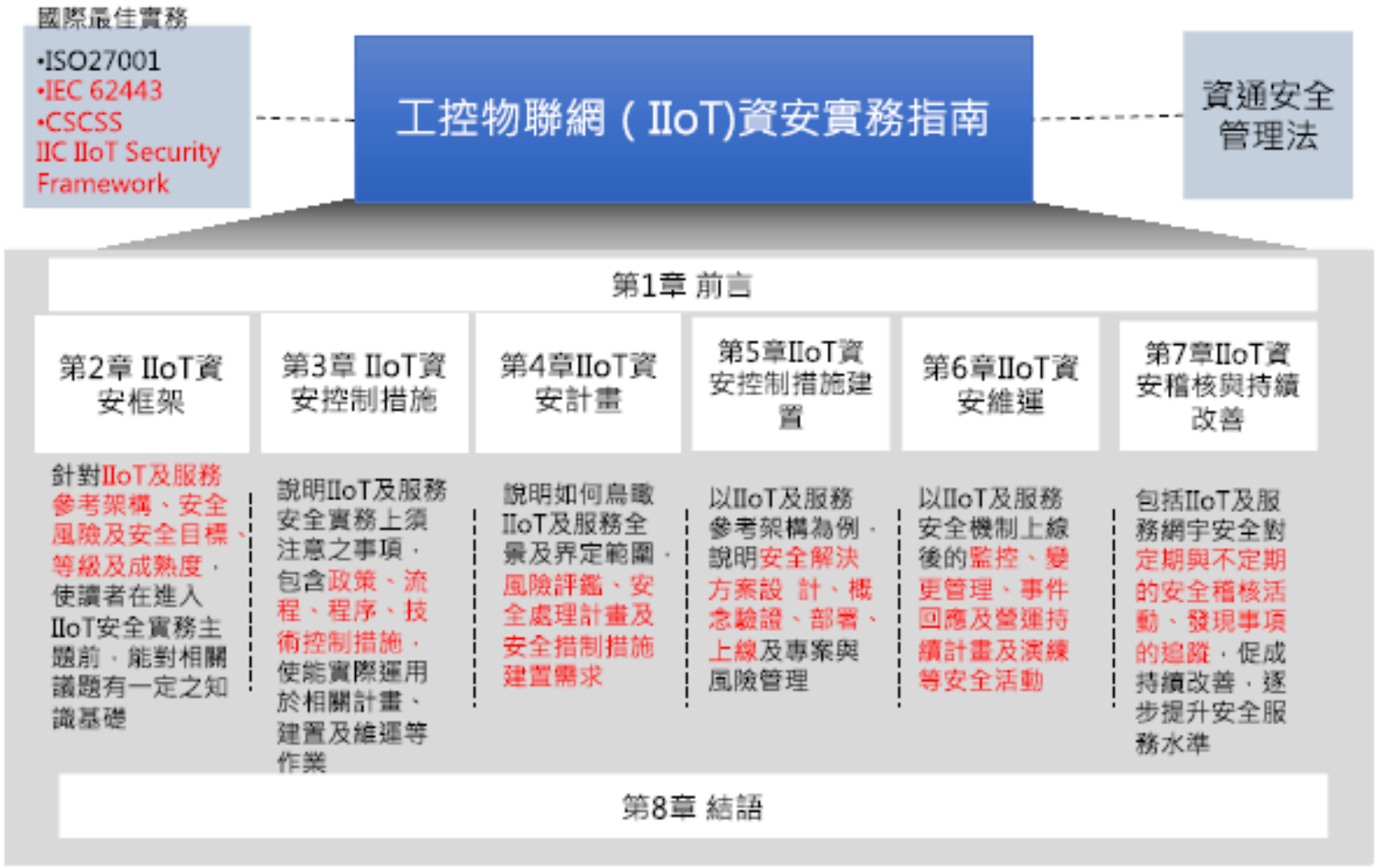


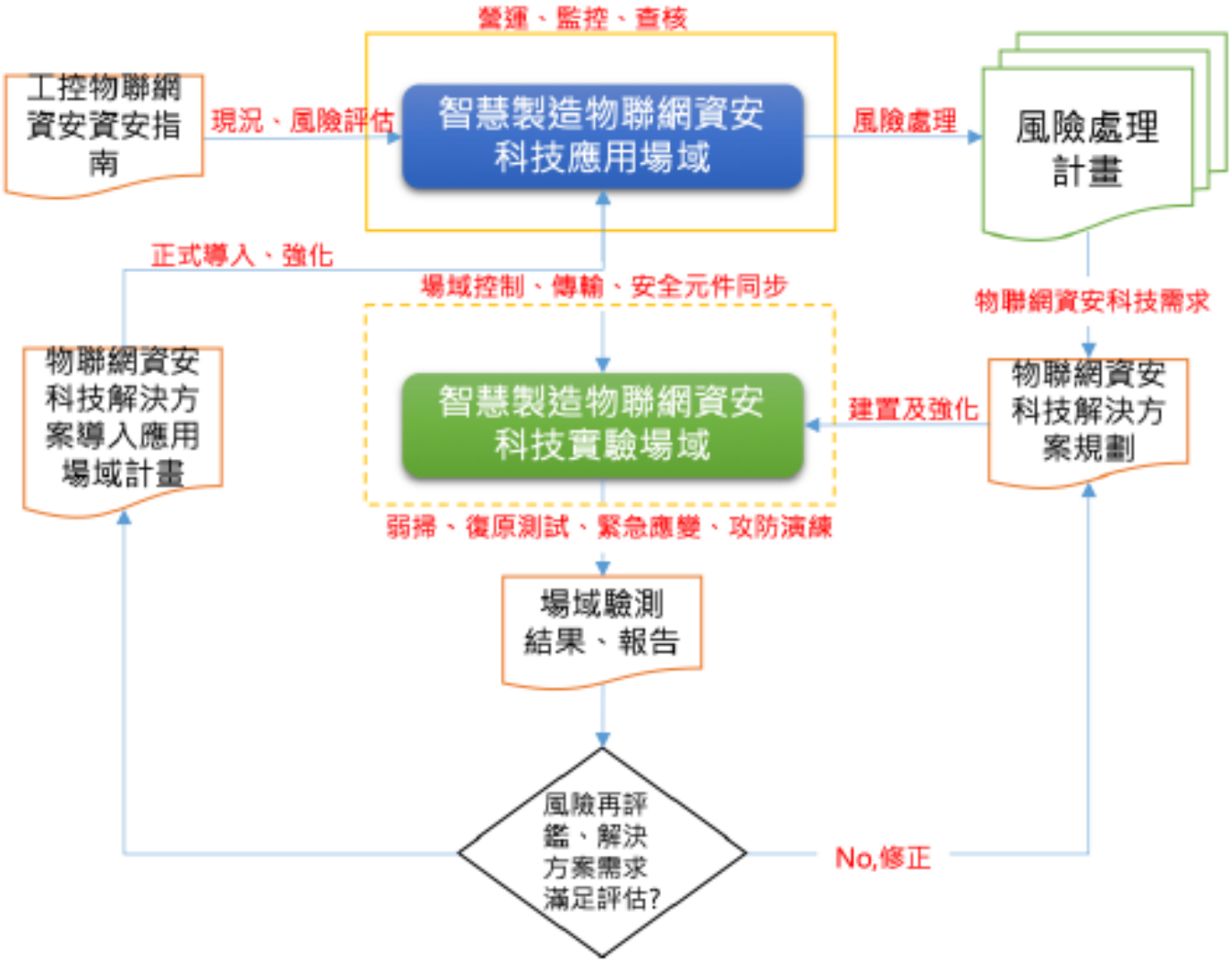
遠端工作潮 居家網路風險提升

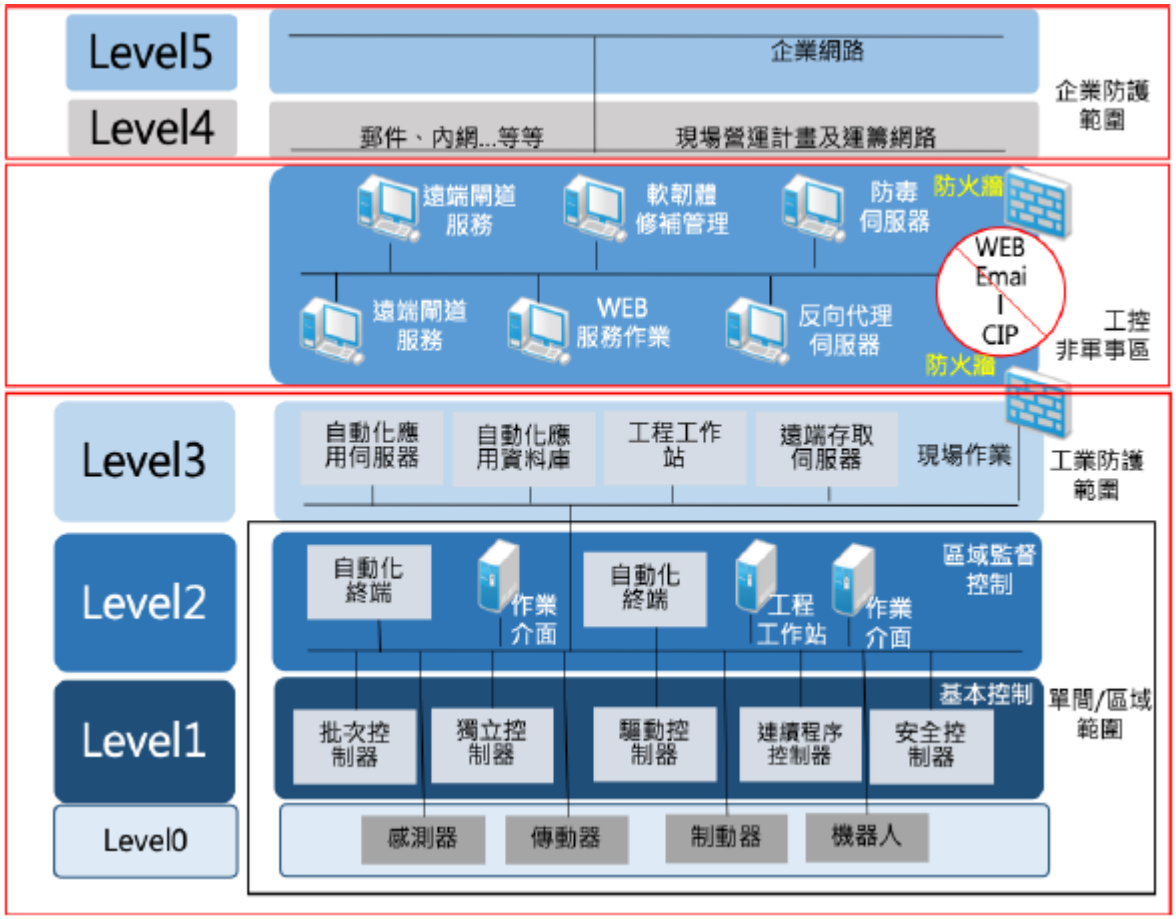
在疫情下成為辦公空間的家庭，聯網設備也越來越多，如今也可能成為駭客的攻擊對象，尤其在家庭路由器。
趨勢科技預測家用路由器將成為駭客入侵家庭網路的首要目標，同時出售路由器家庭網路訪問權限的新興商業模式也將出現，尤其是企業高層或是 IT 管理人員的網路權限更有價值，可能存在更高的風險，大家應該特別將家庭網路納入資安防護重點。

既有漏洞問題比起過去更嚴重

比起過去受到關注的零時差漏洞（0-day vulnerability），如今被稱為既有漏洞（n-dayvulnerability) 的問題更為嚴重，趨勢科技資深技術顧問簡勝財表示，這個問題其實為企業帶來的危害比新的漏洞更為嚴重，預計在未來將出現出現漏洞交易市場，不僅會交易已知漏洞，賣方還可以根據買方的攻擊需求，提供訂製漏洞的服務，然而，如果企業沒有即時修補，其實很容易成為駭客攻擊企業的破口。


國際最佳實務
•ISO27001
•IEC 62443
•CSCSS
IIC IIoT Security Framework
工控物聯網（IIoT)資安實務指南
資通安全管理法
第1章 前言
第2章 IIoT資安框架
第3章 IIoT資安控制措施
第4章IIoT資安計畫
第5章IIoT資安控制措施建置
第6章IIoT資安維運
第7章IIoT資安稽核與持續改善
針對IIoT及服務參考架構、安全風險及安全目標、等級及成熟度，使讀者在進入IIoT安全實務主題前，能對相關議題有一定之知識基礎
說明IIoT及服務安全實務上須注意之事項，包含政策、流程、程序、技術控制措施，使能實際運用於相關計畫、建置及維運等作業
說明如何鳥瞰IIoT及服務全景及界定範圍，風險評鑑、安全處理計畫及安全措制措施建置需求
以IIoT及服務參考架構為例，說明安全解決方案設 計、概念驗證、部署、上線及專案與風險管理
以IIoT及服務安全機制上線後的監控、變更管理、事件回應及營運持續計畫及演練等安全活動
包括IIoT及服務網宇安全對定期與不定期的安全稽核活動、發現事項的追蹤，促成持續改善，逐步提升安全服務水準
第8章 結語


營運、監控、查核
工控物聯網資安資安指南
現況、風險評估
智慧製造物聯網資安科技應用場域
風險處理
風險處理計畫
正式導入、強化
場域控制、傳輸、安全元件同步
物聯網資安科技需求
物聯網資安科技解決方案導入應用場域計畫
智慧製造物聯網資安科技實驗場域
建置及強化
物聯網資安科技解決方案規劃
弱掃、復原測試、緊急應變、攻防演練
場域驗測結果、報告
風險再評鑑、解決方案需求滿足評估?
No,修正



資產盤點需參考普渡企業參考架構（Purdue Enterprise Reference Architecture, PERA）模型


企業
產生標註或記錄
網際網路
可能被包含其中
地理現場
產生標註或記錄
廣域網路
可能被包含其中
本地或遠端區域
產生標註或記錄
區域或分散網路
必須被包含其中
產線、單元、單間、自動搬運車等等
產生標註或記錄
控制網路
必須被包含其中
控制設備
產生標註或記錄
控制網路
必須被包含其中
場域I/O
產生標註或記錄
I/O網路
必須被包含其中
感測或制動器

風險評估執行範例表

所在位置	系統／元件	資產名稱	資產價值	威脅列表	威脅等級	弱點列表	控制措施	控制措施安全等級（SL-C）	弱點等級	風險估值
產線區	○○產線基板組裝	生產線控制電腦	3	DDoS	2	資源不足	無	控制措施安全等級=0	3	18
產線區	○○產線基板組裝	SMT自動貼合機	3	未授權存取	2	無存取控制	本貼合機之控制面板，每個員工進行操作時需先以公司配發之帳號（每人帳號不重複）登入，具一定強度之密碼，且定期進行盤點。	控制措施安全等級=4	1	6

弱點等級：組織自身對威脅之控制能力，可由前述控制措施安全等級進行判定：

- 若控制措施安全等級為2~4，則弱點等級為1，表示此項弱點遭利用之可能性為低。
- 若控制措施安全等級為1，則弱點等級為2，表示此項弱點遭利用之可能性為中等。
- 若控制措施安全等級為0，則弱點等級為3，表示此項弱點遭利用之可能性為高。

風險估值：各重要資產之風險估值係以資產價值與威脅等級與弱點等級三者相乘而得

安全監控功能對應PERA 示意圖

檢測到的威脅範例

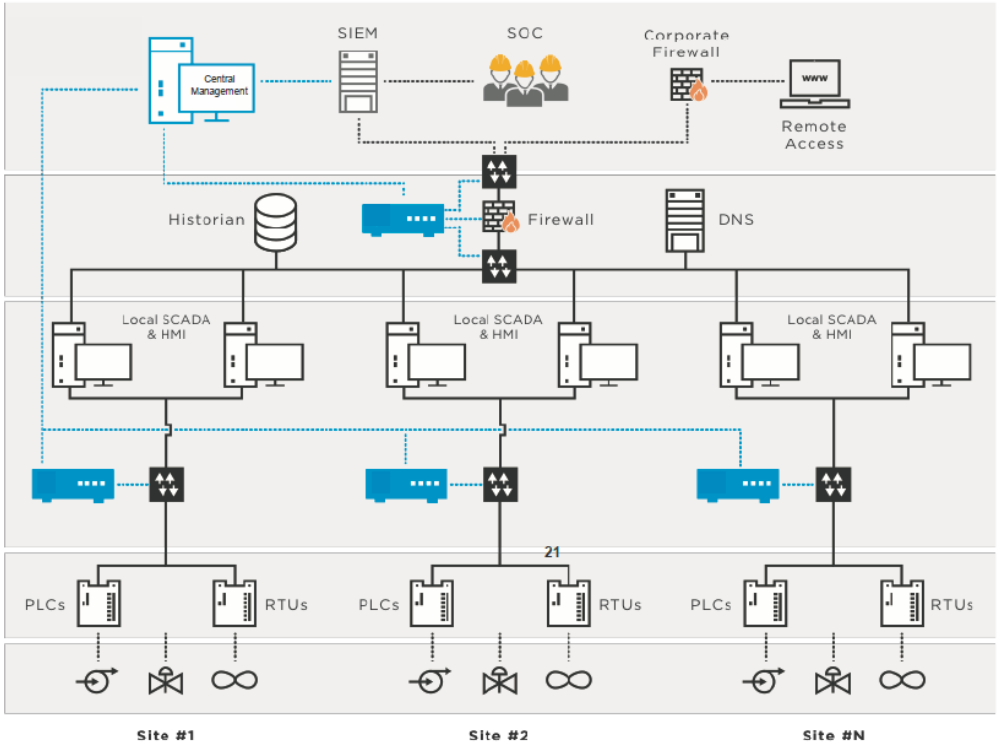
Level 4 生產調度
- 監控連接到網路的遠端存取
- 連接到Internet \企業網路DMZ
- MITM與掃描攻擊（ 連接埠、網路）
- 未經授權的跨級通信

Level 3 生產控制
- 脆弱的密碼（ FTP / TFPTP / RDP / DCERPC）
- 錯誤設定（ NTP / DNS / DHCP /等）
- 漏洞誤報
- 網路拓撲
- 使用過的端口資產
- 未加密的通信（ Telnet）
- 不安全的Internet連接

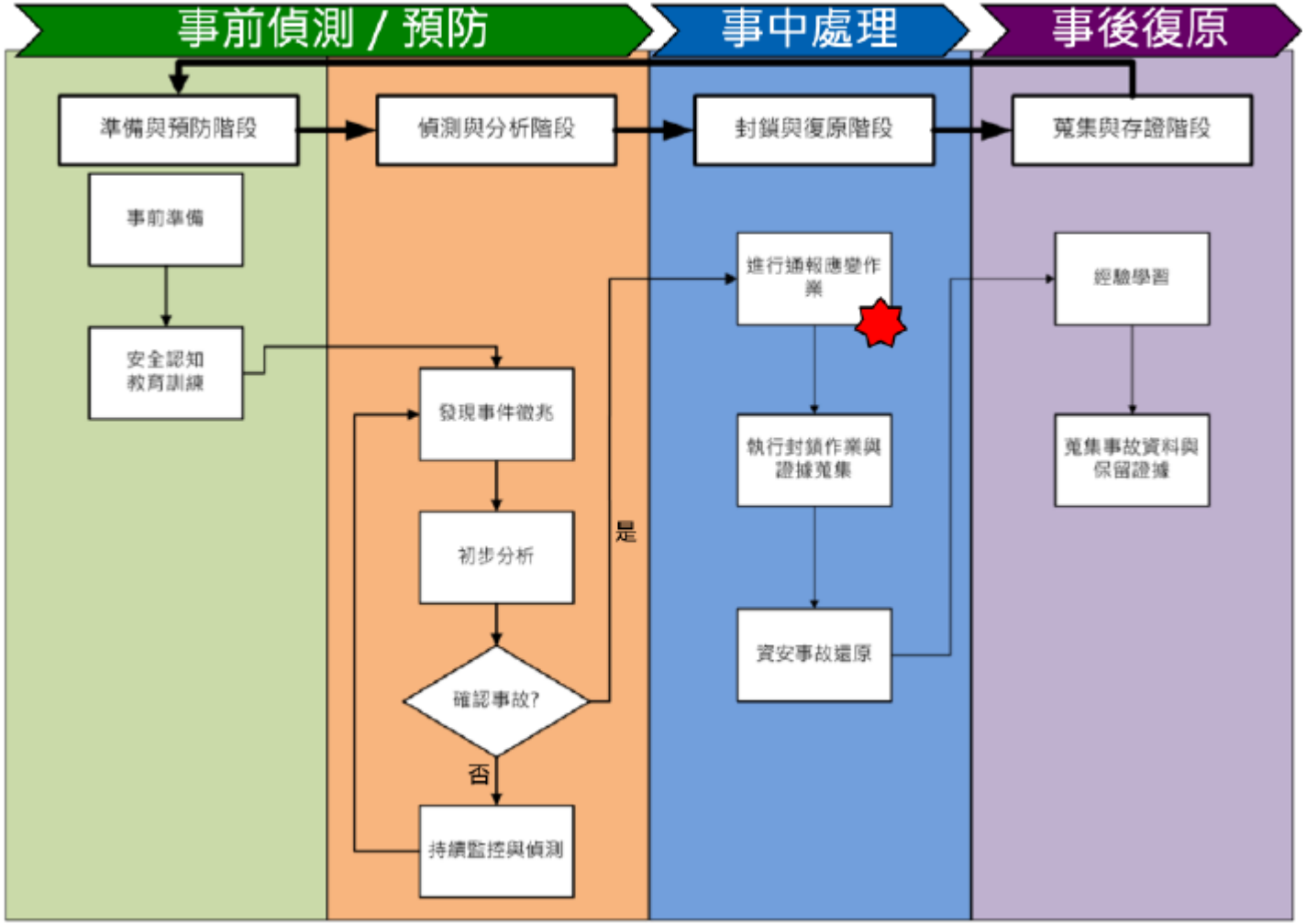
Level 2 工廠監控
- ICS DDoS攻擊
- Subnet衝突
- 異常通信協定行為
- 線上編輯PLC項目
- 改變通信
- 設定下載
- 網路中的新資產
- 無回應的資產
- 損壞的OT網路封包
- 韌體下載
- 邏輯變化

Level 1 直接控制
- 驗證到SPC/SECS/GEM
- SPC動作（ 啟動、停止、監控、執行、重啟、程式設計、測試）

Level 0 現場級別
- Fieldbus I/O監控



資訊安全事件通報流程圖



物聯網技術概念架構

全面感知

LoRa™

BT

Bluetooth® 4.0

ZigBee®

Wi Fi™

4G

RS 485

EtherNet/IP™

可靠傳遞

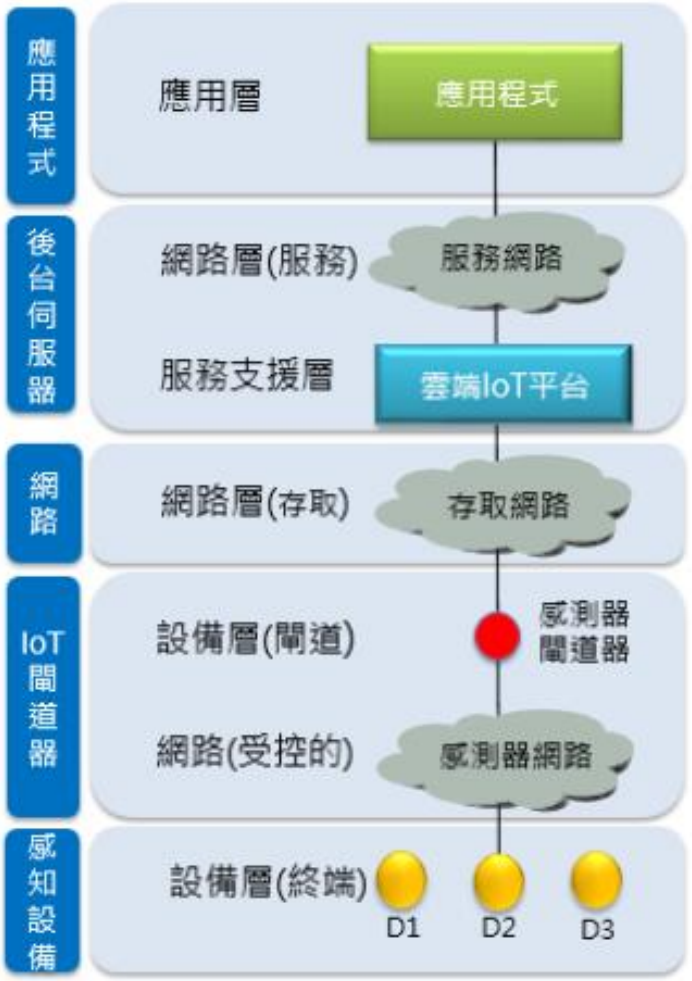
雲端
伺服器

PC/NB

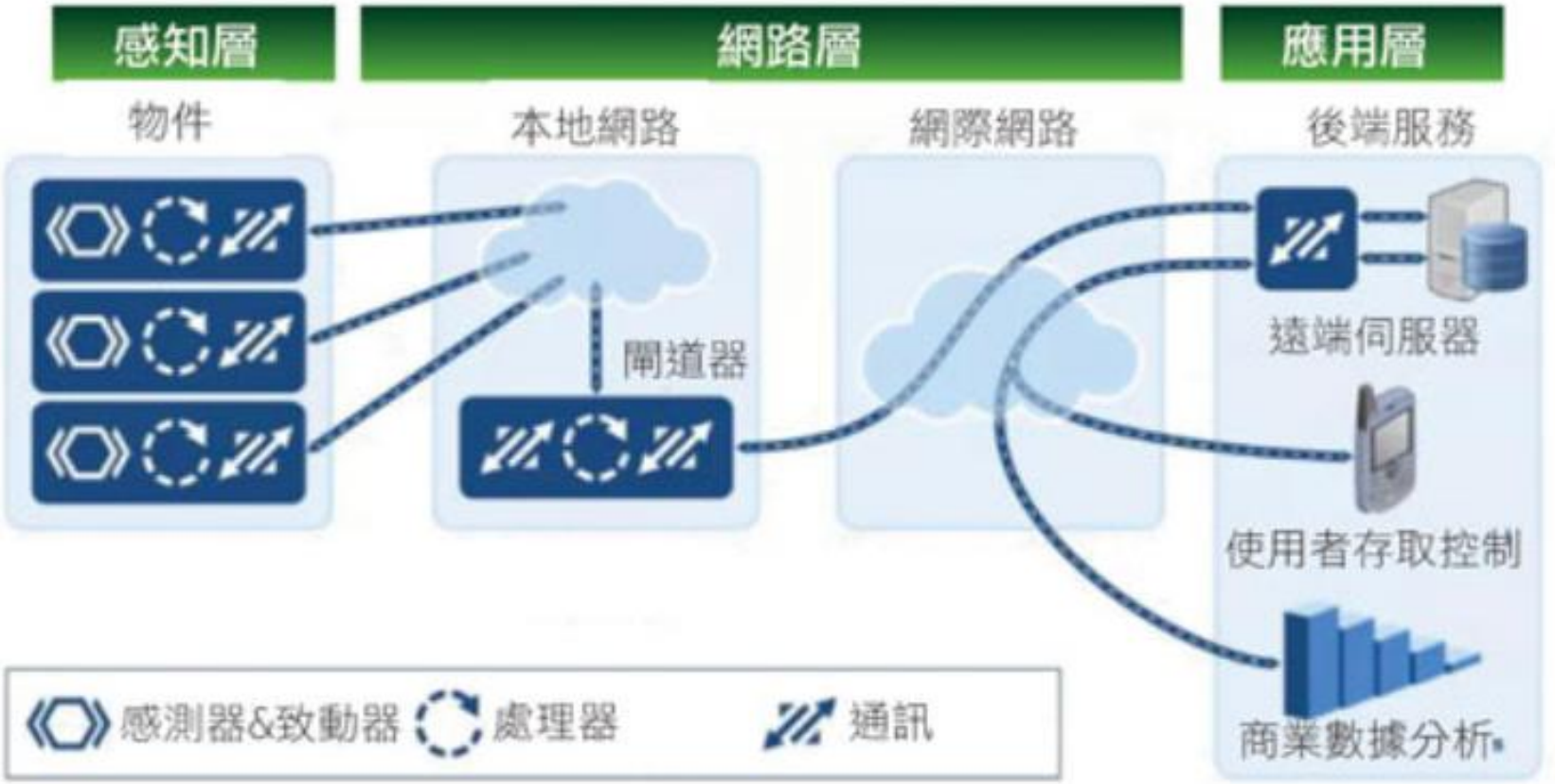
行動裝置

智慧處理

一般性的物聯網架構圖

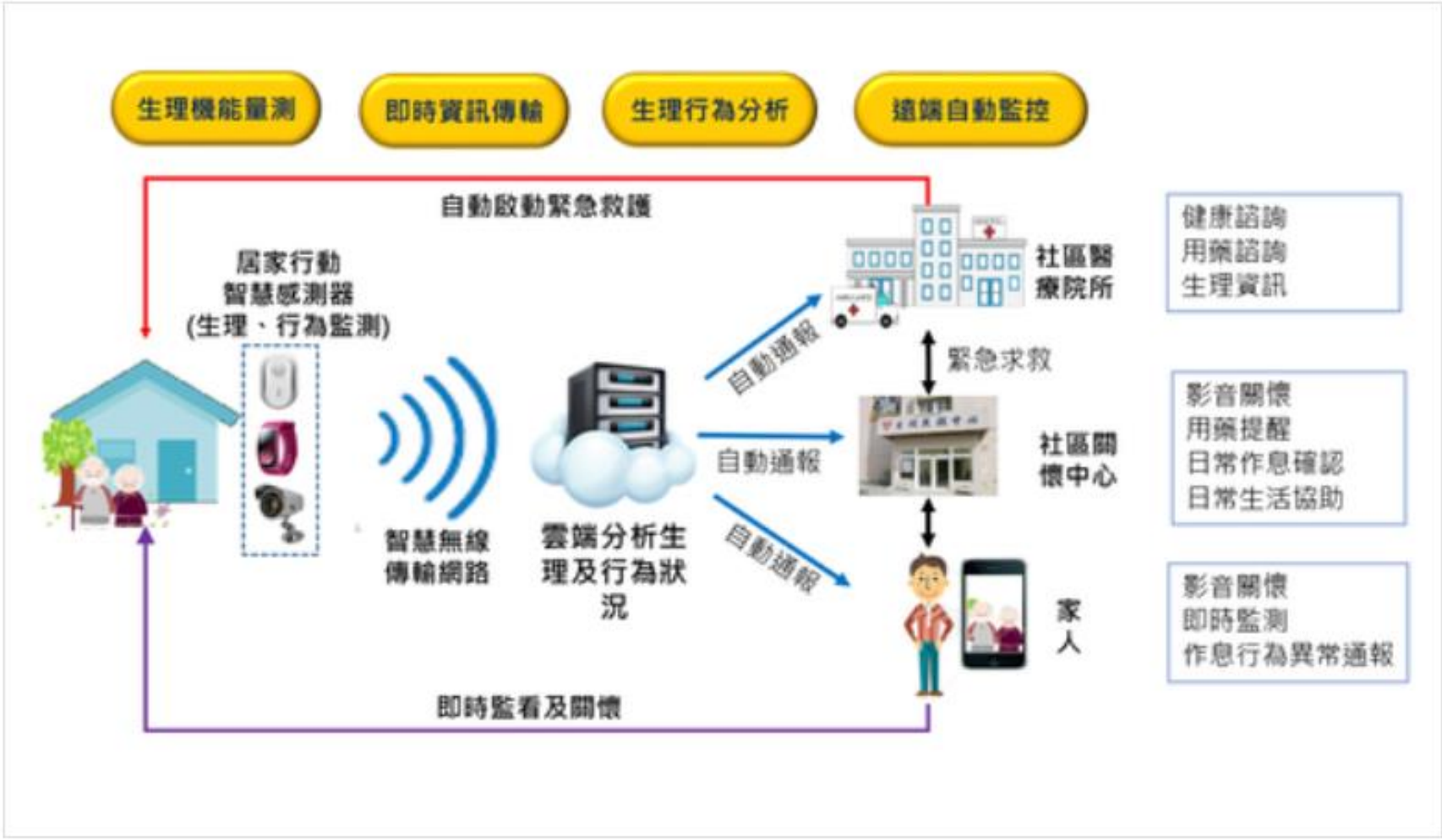

應用程式
後台伺服器
網路
IoT閘道器
感知設備
應用層
應用程式
網路層(服務)
服務網路
服務支援層
雲端IoT平台
網路層(存取)
存取網路
設備層(閘道)
感測器
閘道器
網路(受控的)
感測器網路
設備層(終端)
D1
D2
D3

物聯網技術架構



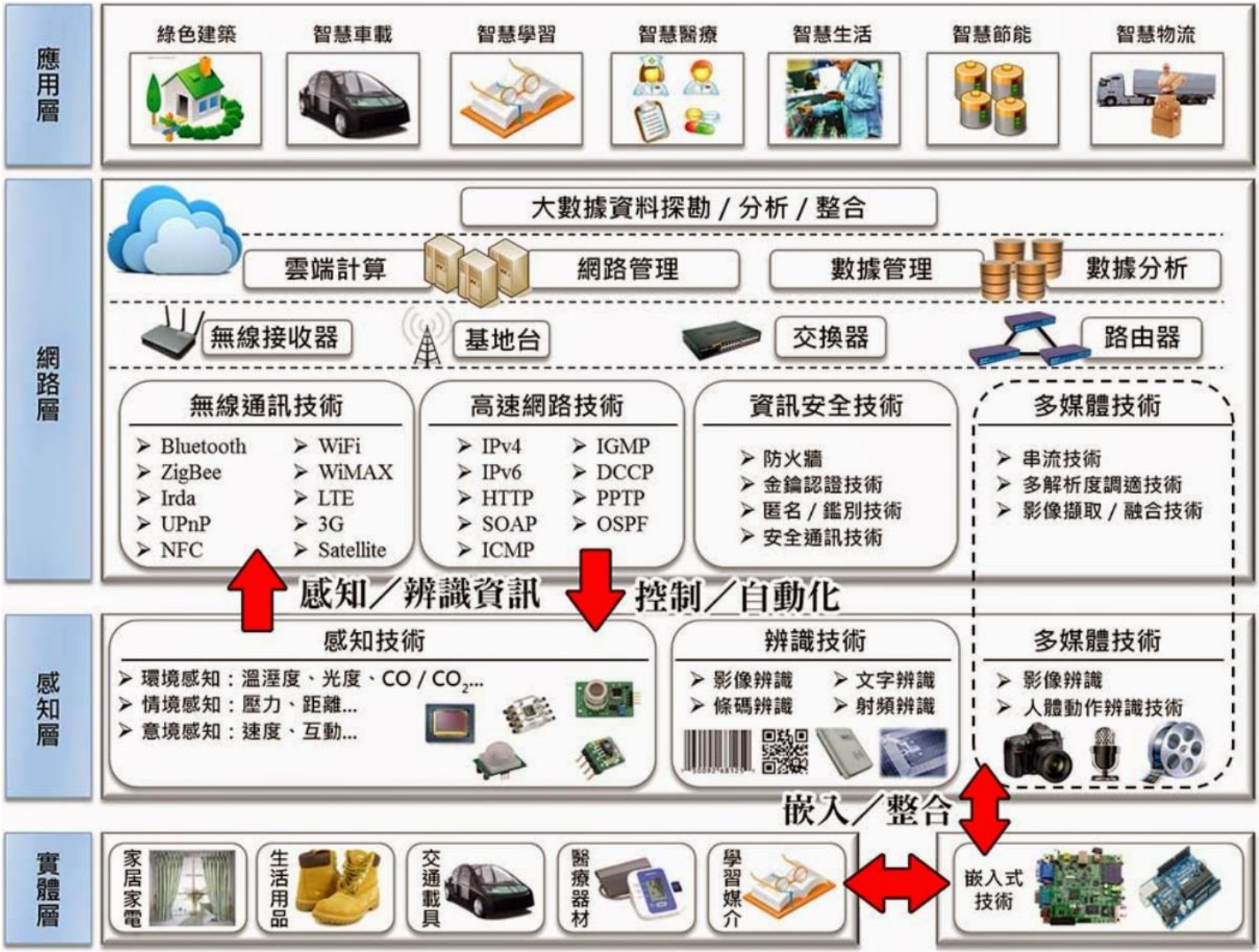
資料來源：研華、DIGITIMES整理，2017/10

蔬果花卉溫網室環境、土壤監測及遠端控制系統


生理機能量測
即時資訊傳輸
生理行為分析
遠端自動監控
自動啟動緊急救護
居家行動
智慧感測器
(生理、行為監測)
智慧無線
傳輸網路
雲端分析生
理及行為狀
況
自動通報
自動通報
自動通報
社區醫
療院所
緊急求救
社區關
懷中心
家
人
即時監看及關懷
健康諮詢
用藥諮詢
生理資訊
影音關懷
用藥提醒
日常作息確認
日常生活協助
影音關懷
即時監測
作息行為異常通報

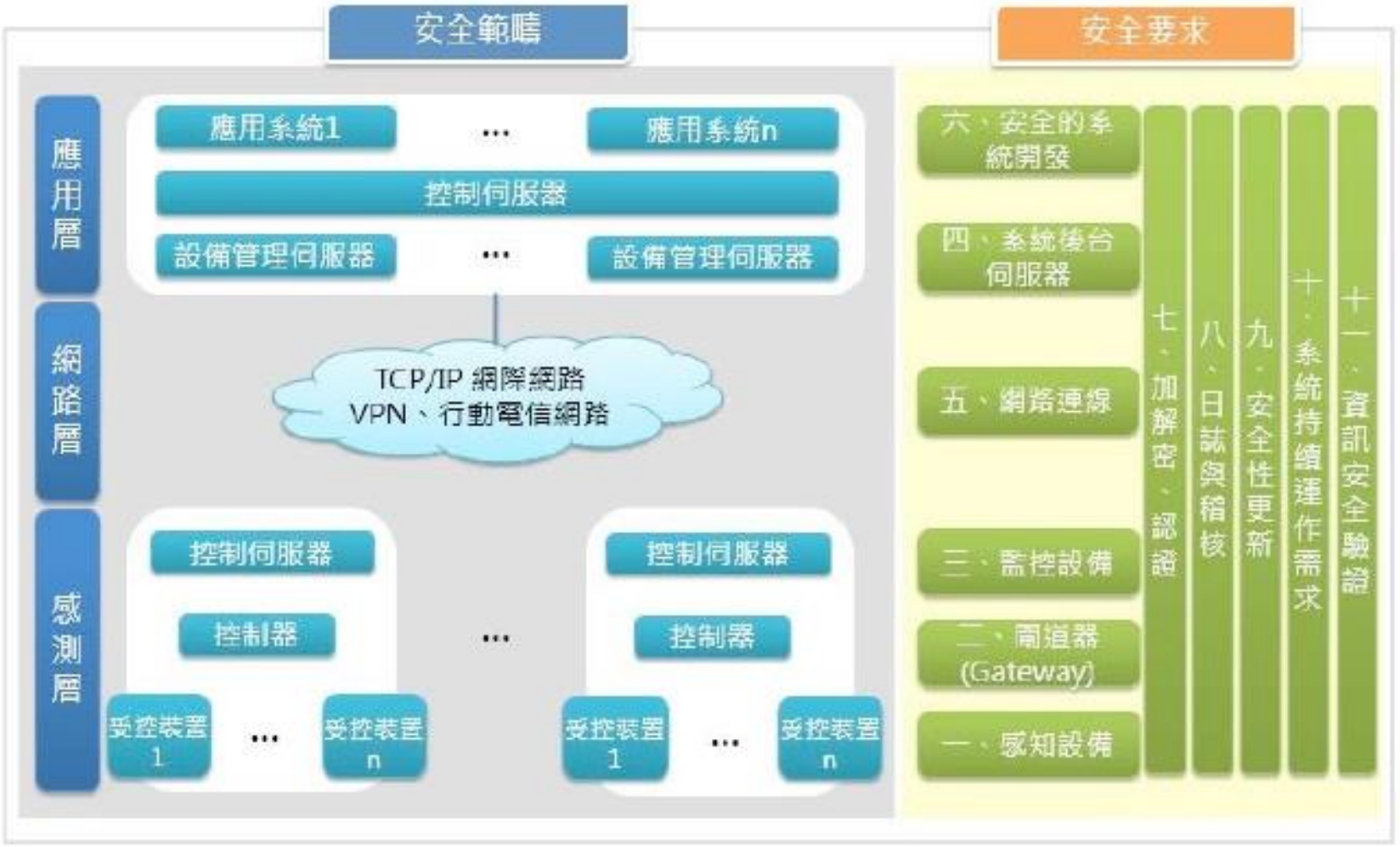
民生公共物聯網資安要求框架表

領域\原則	P1.預設就應安全	P2.資安縱深防禦	P3.可歸責性	P4.恢復能力
D1.安全功能保護	使用安全的數位簽章	使用硬體信任根	確保更新的完整性	具備援/備份能力
D2.身份辨識與認證	使用相互認證	使用多因子認證	記錄登入失敗日誌	適當的身分管理
D3.網路管理	連接最小化	使用防火牆與VPN	記錄連線授權失敗日誌	妥善的網路區隔
D4.資料安全	啟用資料加密	保護資料之傳輸，使用及儲存	記錄存取機敏資料	定期備份資料
D5.存取控制	實體存取限制	異常通報機制	異常日誌紀錄	防竄改機制
D6.加密保護	使用業界公認的加密方式	運用對稱或非對稱金鑰保護	合適的密鑰管理	使用完全前向保密(PFS)協定
D7.資安管理	強制使用強密碼	限制遠端對安全網路的存取	密鑰管理的職責分離	保持軟體/韌體更新
D8.營運持續	加密備份	自我檢測	監控及偵測容量使用情況	進行備援或備份之復原演練
D9.安全稽核	啟用日誌紀錄	加密日誌資料	限制對日誌之存取	定期備份日誌
D10.生命週期保護	採用系統強化基準	進行安全檢測	適當情資分享	設備再重新或汰除前清除資料



作者 / 張志勇（任教淡江大學資訊工程學系）、陳正昌（就讀淡江大學資訊工程學系博士班）

民生公共物聯網計畫之安全範疇與安全要求



物聯網感知設備（感測裝置）之安全要求

1.1 必要要求

1.1.1 可用性百分比，不得低於OO.OO%；不穩定性每月不得超過O次（註：1.可用性定義：服務持續不間斷的運作，服務連續中斷時間高於O 分鐘即視為不可用，以時間為計算基準；2.不穩定性定義：服務連續中斷達OO 秒以上即視為不穩定；3.前項數字由機關（構）自行訂定）。

1.1.2 感知設備對外連接端口（如USB port）需最少化並建立管理機制。

1.1.3 設備應關閉或停用不必要的通訊功能或模組，例如：行動網路或Wi-Fi 等。

1.1.4 所有管理密碼須可由管理使用者自行變更與修改。

1.1.5 權限管理，須能依不同角色，設定不同存取權限。

1.1.6 需納入異常監控機制。

1.1.7 需內建安全的軟體與韌體更新機制，以進行漏洞修補。

1.1.8 設備應提供第三方資安檢測報告。

物聯網感知設備（感測裝置）之安全要求

1.2 中階要求

1.2.1 確保感測裝置上之資料完整性，資料發送前先進行加密，收到後再解密。

1.2.2 設備應提供第三方資安檢測報告，報告中不應含有高風險（含）以上（依據CVSS 3.0）的問題。

1.3 進階要求

1.3.1 感知設備參數儲存於設備內時需加密保護。

1.3.2 資料機密性：依安全等級決定各種資料加密演算法強度及金鑰儲存方式，如使用RSA-1024、AES-128 或更高安全性的演算法。

1.3.3 需建立安全機制，確認感知設備啟動時韌體的完整性（如透過數位簽章等），設備上的軟體、韌體都經過驗證，達到系統安全啟動，並防止被植入惡意程式在設備上運作。

物聯網閘道器（Gateway）之安全要求

1.1 必要要求

2.1.1 服務可用性及穩定性：可用性百分比，不得低於99.8%；不穩定性每月不得超過1次（註：1.可用性定義：服務持續不間斷的運作，服務連續中斷時間高於5 分鐘即視為不可用，以時間為計算基準；2.不穩定性定義：服務連續中斷達30 秒以上即視為不穩定）。

2.1.2 物聯網閘道器應關閉或停用不必要的通訊功能或模組例如：行動網路或Wi-Fi 等。

2.1.3 所有管理密碼須可由管理使用者自行變更與修改。

2.1.4 權限管理，須能依不同角色，設定不同存取權限。

2.1.5 確保物聯網閘道器須具備安全性功能以達到資料完整性與不可否認性之功能。

2.1.6 資料機密性：物聯網閘道器須具備針對加密金鑰與憑證的安全保護機制或功能，以避免被竊取及複製，且金鑰保護的方式必須在建置的文件中詳細說明安全保障之做法。

2.1.7 對於重要的資料應採取較高等級或較嚴謹的保護措施，如使用RSA-2048、AES-256 同級或更佳的加密演算法進行加密保護。

2.1.8 需建立安全機制，確認閘道器上的軟體、韌體完整性，達到系統安全啟動，並防止被植入惡意程式在設備上運作。

2.1.9 應禁止非必要之網路連線。

2.1.10 場域內之物聯網閘道器正式上線前，每個閘道器必須個別發放不同憑證作為認證使用，並防止使用同一金鑰，以避免金鑰被取得或破解後，設備全面淪陷。

2.1.11 需內建安全的軟體與韌體更新機制，以進行漏洞修補。

2.1.12 設備應提供第三方資安檢測報告。

監控設備之安全管理要求

3.1 必要要求
3.1.1 傳輸資料的加密應採用安全的機制。
3.1.2 每台監控設備應使用不同的金鑰，並由後台進行監控設備的金鑰管理。
3.1.3 為防止安全監控管理設備不慎遺失，導致非法用戶對設備進行操作的安全疑慮，需建立機制可立即阻斷、防止再操作。
3.1.4 需內建安全的軟體與韌體更新機制，以進行漏洞修補。
3.1.5 設備應提供第三方資安檢測報告。
3.1.6 需權限管理與使用認證要求，避免設備遺失後及阻斷機制啟動前，遭非法用戶對設備進行操作。
3.1.7 監控範圍應涵蓋應用層、網路層及感測層；監控內容應涵蓋設備可用性及安全性等監控。
3.2 中階要求
3.2.1 設備應提供第三方資安檢測報告，報告中不應含有高風險（含）以上（依據CVSS 3.0）的問題。
3.3 進階要求
3.3.1 加密金鑰之儲存須採用硬體式安全晶片，如使用可信賴平台模組（TPM）。

系統後台伺服器之安全要求

4.1 必要要求
4.1.1 服務可用性及穩定性：可用性百分比，不得低於99.8%；不穩定性每月不得超過1 次（註：1.可用性定義：服務持續不間斷的運作，服務連續中斷時間高於5 分鐘即視為不可用，以時間為計算基準；2.不穩定性定義：服務連續中斷達30 秒以上即視為不穩定）。
4.1.2 對於重要的資料，須使用RSA-2048、AES-256 同級或更佳的加密演算法進行加密保護。
4.1.3 伺服器端必須採用 Webtrust SSL 憑證。
4.1.4 伺服器端必須受網路防火牆、網頁防火牆、入侵偵測等資安設備保護。
4.1.5 系統特權帳號管理，特權帳號僅授予執行業務及職務所必要為限。
4.1.6 系統特權帳號存取，系統均須留有完整紀錄。
4.1.7 需提供自動異常偵測機制，發送告警通知，並產出稽核報表。
4.1.8 管理密碼須定期更改。
4.1.9 伺服器應提供第三方資安檢測報告。
4.1.10 關閉非必要之服務埠。
4.2 中階要求
4.2.1 伺服器應提供第三方資安檢測報告，報告中不應含有高風險（含）以上（依據CVSS 3.0）的問題。
4.3 進階要求
4.3.1 身分認證須採用多因子驗證方式（Multi-factor authentication）。

網路連線之安全要求

5.1 必要要求
5.1.1 網路連線資料傳輸必須建立AES-128 等級同級或更佳之安全的加密通道。
5.1.2 遠端連線必須透過加密通道，登入系統必須採用安全的身分鑑別機制。
5.1.3 避免使用非公開之專屬網路協定，若有其必要且不可取代性，必須於規劃書中詳述。
5.1.4 僅開放網路連線必須使用的服務埠，其餘皆關閉。
5.2 中階要求
5.2.1 網路連線時必須檢視憑證的正確性與有效性，避免中間人攻擊。
5.3 進階要求
5.3.1 管理線路與使用者觀看線路應進行區分。

安全的系統開發

6.1 必要要求
6.1.1 物聯網的研發過程，就必須導入安全性的思維（如SSDLC 等），建立對應的安全開發流程，開發人員應受過安全開發教育訓練，以降低遭受到攻擊時的損失。
6.1.2 安全檢測：針對系統進行源碼檢測、弱點掃描及滲透測試，並於規劃書內說明風險值，且於系統上線前提供測試報告，以證明系統之安全性無慮。
6.2 中階要求
6.2.1 軟體安全開發流程應涵蓋內外部稽核等機制，以建立持續改善的循環。
6.3 進階要求
無要求。

加解密、認證之安全要求

7.1 必要要求

7.1.1 須定義與識別出服務運作時所需之應用程式、函式庫、設定檔與上述之備份檔及服務運作時所處理之機敏資料（含個人資料），上述資料於傳輸與儲存時，須採用加密演算法進行加密或簽章與驗章等方式保護資料。

7.1.2 須具備流程以定義與識別出重要之資訊系統、IoT 裝置及應用服務API，並規範對應的加密強度，如關鍵系統採用之加密技術是尚未被破解、標準化且具強固加密等級；一般系統則採用安全等級適當之標準化加密技術。

7.1.3 使用金鑰，須定義組織之信任根，並依金鑰生命週期之各階段，建立安全的金鑰管理機制，包含金鑰產生、儲存、使用、備份、銷毀、更新、復原及憑證之信任鏈建立與管理等，並確保未經身分驗證與授權之人員，不能處理或存取上述之金鑰。

7.1.4 針對安全要求較高的服務，應採用多因子認證功能，強化資安。

7.1.5 若採用對稱式金鑰，為防止金鑰被竊取，應採用非對稱金鑰加以保護。若使用密碼管理，需有如下機制：

- 須更改初始密碼，並不允許使用硬編碼之密碼或存在管理後門密碼。
- 要求密碼強度（如長度、複雜度），可參考NIST、OWASP及SANS 之密碼規範。
- 密碼失效鎖定機制（3 次密碼輸入錯誤即鎖定，至少20 分鐘後解鎖）。
- 密碼需加密保存。
- 密碼需可設定效期管控。

加解密、認證之安全要求

7.1.6 認證錯誤訊息須防止列舉攻擊。
7.1.7 進行認證時，密碼不應直接顯示於畫面中。
7.1.8 變更或重設密碼後，須要求使用者重新登入。
7.2 中階要求
7.2.1 須定義與識別出服務運作時所需之應用程式、函式庫、設定檔與上述之備份檔及服務運作時所處理之機敏資料（含個人資料），上述各項資料於傳輸與儲存時，須採用強固的加密演算法進行加密或簽章與驗章等方式保護資料，如使用RSA-2048、AES-128、ECC-256、SHA-256 同級或更佳的演算法。
7.2.2 須具備流程以定義與識別出重要之資訊系統、IoT 裝置及應用服務API，並規範對應的加密強度與施作信任錨，如關鍵系統採用之加密技術是尚未被破解、標準化且具強固加密等級，且信任錨為具防旁通道之硬體晶片；一般系統則採用安全等級適當之標準化加密技術。上述之安控措施需達成服務中的每個端點之相互認證、防護重放攻擊、完美向前加密（Perfect Forward Secrecy）及完整性需求，並可修改或撤銷遭駭之系統之身分認證與權限。
7.3 進階要求
無要求。

日誌與稽核的安全管理

8.1 必要要求
8.1.1 日誌與稽核：設定檔異動、存取均須有完整紀錄；稽核日誌之記錄內容包括使用者識別碼、登入登出之日期時間、電腦/行動裝置（Device）的識別資料或其IP、修改項目、結果等事項。
8.1.2 日誌需保留至少5 年。
8.1.3 相關設備之鐘訊，應具備標準時間源校時機制，以確保日誌時間準確性。
8.2 中階要求
無要求。
8.3 進階要求
無要求。

安全性更新

9.1 必要要求
9.1.1 不論何種感測設備、閘道器及後台伺服器，需建立安全的軟體/韌體更新、組態更新的機制，用以修補漏洞及組態異動。
9.1.2 需提供及時的弱點修補與軟體安全性更新服務。
9.1.3 需確保安全性更新資料來源之正確性。
9.2 中階要求
9.2.1 執行回復原廠設定功能，須進行通知或警示。
9.2.2 軟體/韌體更新、組態更新失敗時，須可成功回復至前一個版本。
9.2.3 設備具備更新檔通知功能，以當有更新檔可供安裝時，設備可自動通知設備管理員。
9.3 進階要求
無要求。

系統持續運作需求

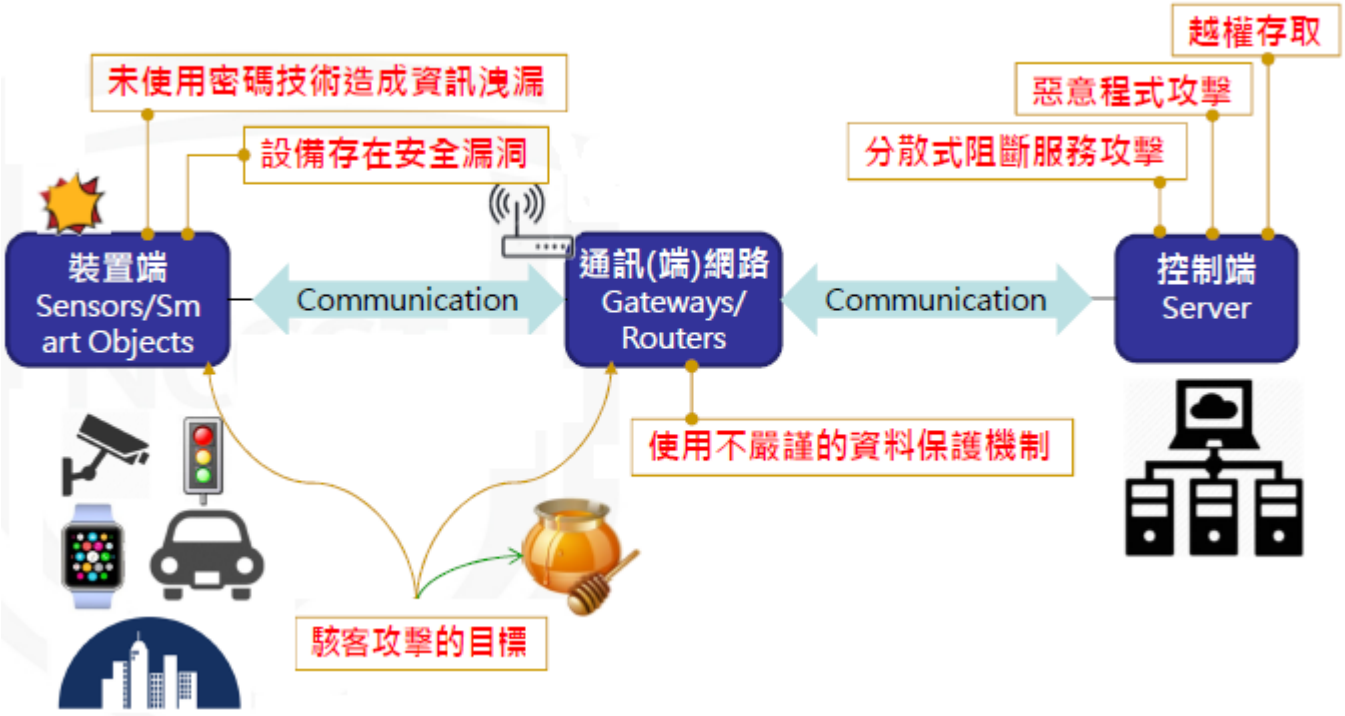
10.1 必要要求
10.1.1 需規劃資料異地備份機制與定期還原演練作業。
10.1.2 需於規劃書內提出BCP（業務持續運作計畫）及DRP（災難復原計畫）確保系統持續安全運作。
10.2 中階要求
無要求。
10.3 進階要求
無要求。

資訊安全驗證

11.1 必要要求
11.1.1 收集到的資訊如個人資料時，須遵守個資法之規定。
11.1.2 安全檢測：定期對系統進行弱點掃描及滲透測試，並於規劃書內說明風險值，以證明系統之安全性無慮。
11.1.3 物聯網為多異質網路聯接而成，難以使用單一驗證方式檢測各種不同系統，建議得標廠商可以採行ISMS（資訊安全管理制度）要求，進行第三方資訊安全稽核。
11.1.4 上述物聯網資通安全規範之各項要求，各政府機關應納入組織之資通安全政策並納入定期外部資通安全驗證範圍。
11.2 中階要求
無要求。
11.3 進階要求
無要求。

物聯網安全議題

一般物聯網架構可分為「裝置端」、「通訊(端)網路」及「控制端」，其衍伸相關安全議題



物聯網安全議題

- 控制端

–因使用的平台種類眾多，若未做好身分認證或存取控制，可能使攻擊者越權下達攻擊指令，存取機敏或他人資料–未更新伺服器之作業系統或採用存在漏洞的應用程式套件，可能讓駭客透過相關漏洞來入侵系統或植入惡意程式

物聯網安全議題

●通訊(端)網路

若傳輸未經加密或使用不安全的加密演算法，可能導致資料外洩問題

物聯網安全議題

●裝置端

–實體位置暴露於公開環境中，易遭有心人士利用–儲存空間或運算能力有限，無法執行自動安全更新，因而造成系統存在漏洞

物聯網產品漏洞案例

- 恆溫器

–資料傳輸未加密

–日誌文件洩露個人資訊

- Baby Monitors

–Web頁面更改URL的序號即可觀看他人的監視器畫面

–Web頁面更改URL上的Email位址參數，即可使用他人的管理頁面

- 智慧冰箱

–直接透過UART直接取得管理者權限


中保無限 智慧宅
9大功能
方案介紹
操作介面
申裝流程
我有興趣
AI智能安檢
dormakaba
智慧連動 | 月租只要2,000元 起
智慧電子門鎖
溫濕度顯示
家電控制
燈光控制
※本方案為預設之基本標準配備 您可依據您的實際需求額
方案介紹
我有興趣

飛利浦智能居家
2019年6月24日 ·

#飛利浦智能鎖 #教學

設定 #藍牙開鎖 及使用 #app分享權限 聽起來很困難？
沒關係，我們準備了詳細的手把手教學影片！
兩分鐘內馬上學會藍牙及app操作 😊

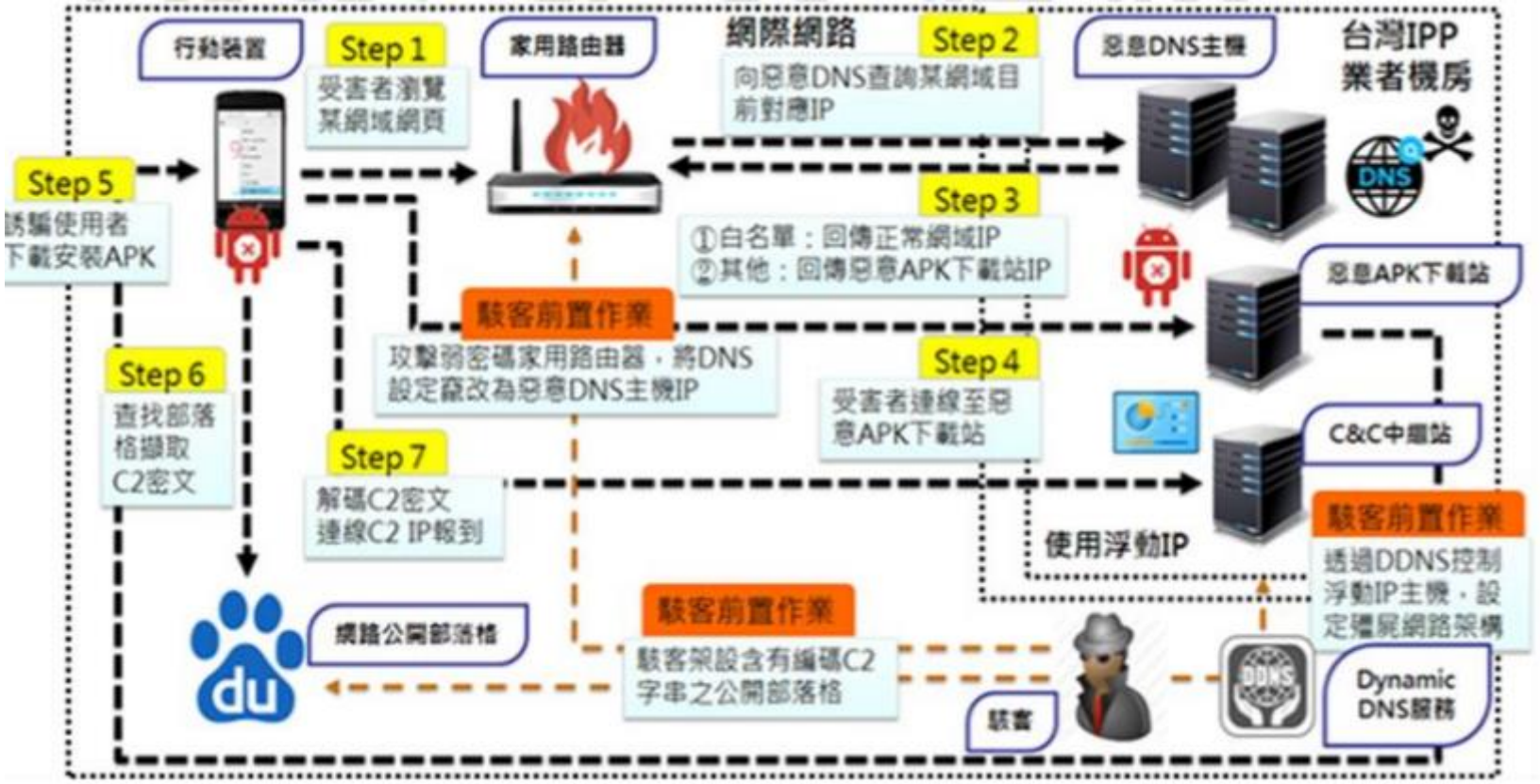
哪些型號可以使用這些便利功能呢：
👉旗艦款：9200
👉最新款：Alpha

飛利浦全自動IOT智能鎖

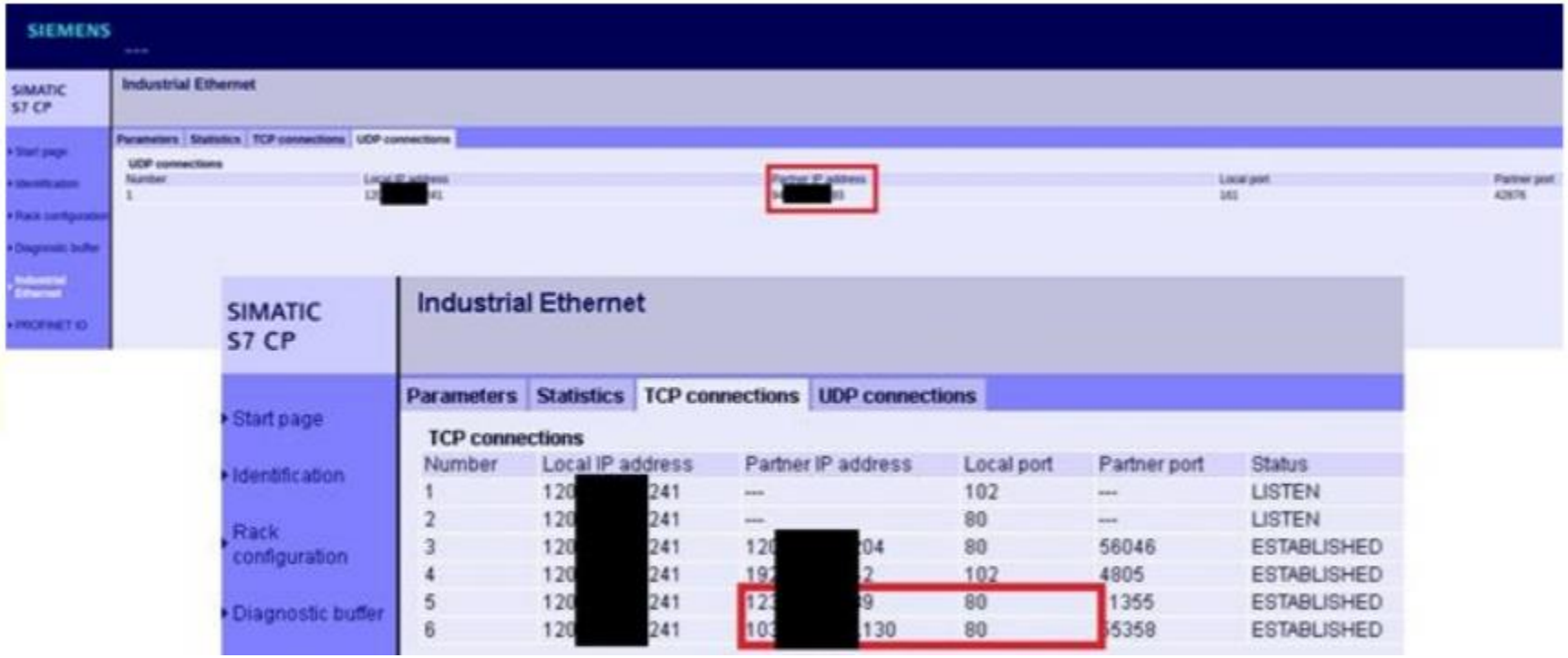
EASYKEY 9300

連接網路，管理門鎖不受限；IOT全新技術，定格全智能

了解更多

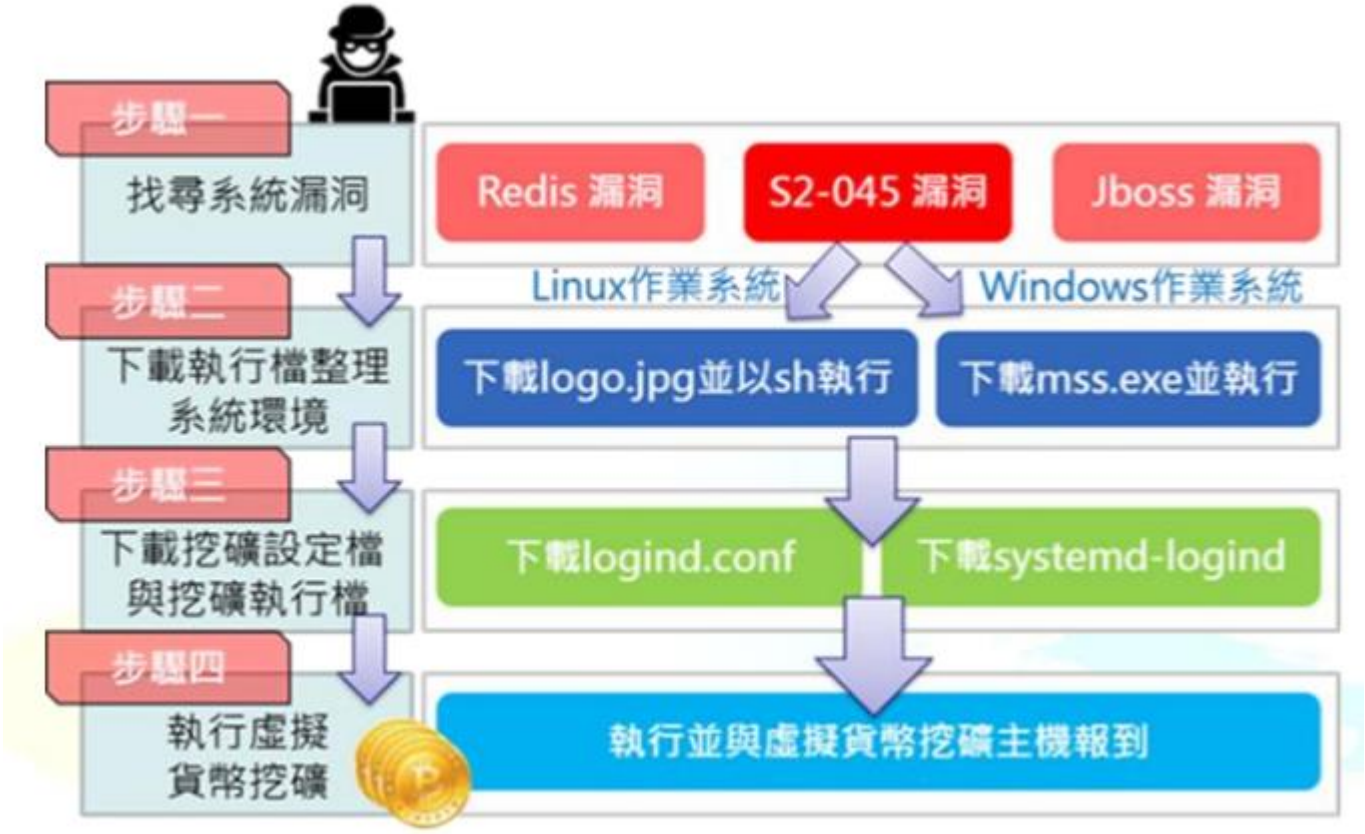

行動裝置
Step 1
受害者瀏覽某網域網頁
家用路由器
網際網路
Step 2
向惡意DNS查詢某網域目前對應IP
惡意DNS主機
台灣IPP業者機房
DNS
Step 5
誘騙使用者下載安裝APK
Step 3
①白名單：回傳正常網域IP
②其他：回傳惡意APK下載站IP
駭客前置作業
攻擊弱密碼家用路由器，將DNS設定竄改為惡意DNS主機IP
惡意APK下載站
Step 6
查找部落格擷取C2密文
Step 4
受害者連線至惡意APK下載站
C&C中繼站
Step 7
解碼C2密文
連線C2 IP報到
使用浮動IP
駭客前置作業
透過DDNS控制浮動IP主機，設定殭屍網路架構
網路公開部落格
駭客前置作業
駭客架設含有編碼C2字串之公開部落格
駭客
DDNS
Dynamic DNS服務

假冒 Facebook 更新檔中文視窗畫面



環境控制系統 IP 連線紀錄

門禁系統入侵案例


步驟一
找尋系統漏洞
Redis 漏洞
S2-045 漏洞
Jboss 漏洞
Linux作業系統
Windows作業系統
步驟二
下載執行檔整理
系統環境
下載logo.jpg並以sh執行
下載mss.exe並執行
步驟三
下載挖礦設定檔
與挖礦執行檔
下載logind.conf
下載systemd-logind
步驟四
執行虛擬
貨幣挖礦
執行並與虛擬貨幣挖礦主機報到

駭客利用 MikroTik 路由器漏洞之攻擊手法

自動導航

其實我們生活中很早就已經出現，能自主判斷，自我導航目標取代人工的全自動機器。這使得人為操控上的失誤與過勞等等人為問題消失。

打掃機器人

（圖片來源／http://www.jianshu.com/）

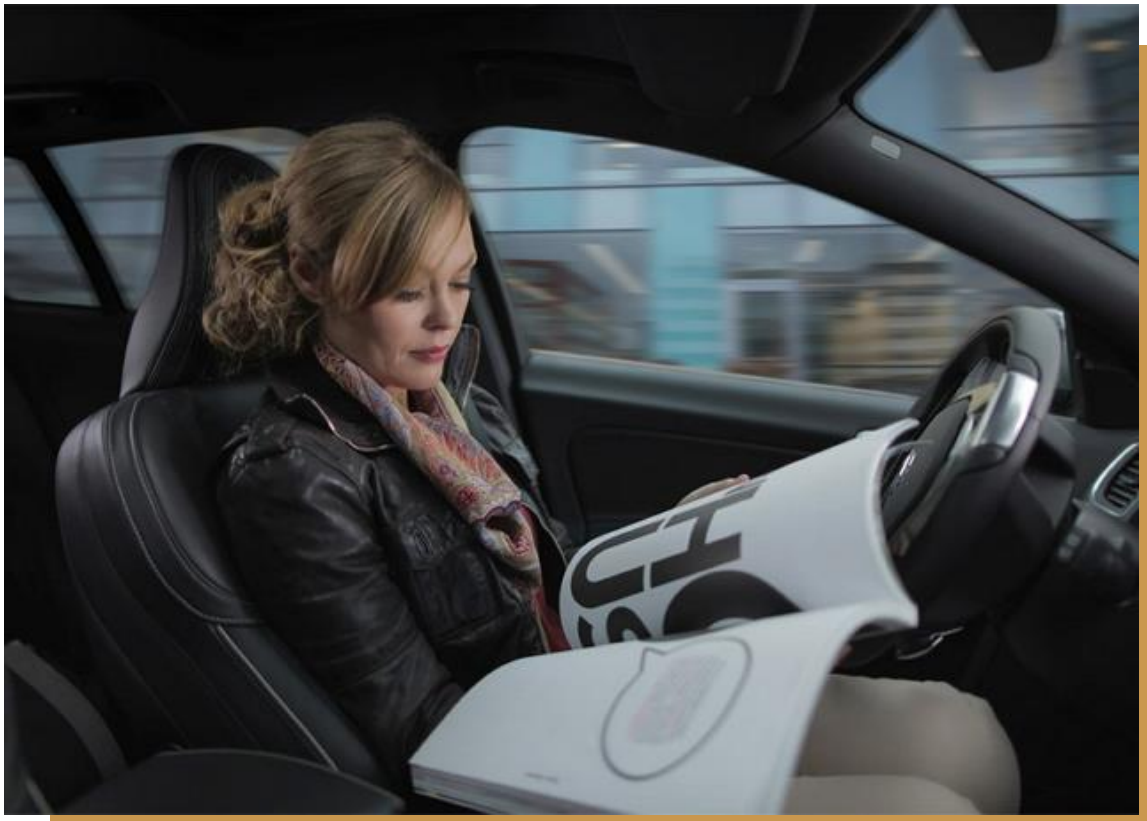
倉儲機器人

（圖片來源／fashion.keedan.com/）

自動駕駛(Self-Driving)

而在整合各項科技與技術的延伸，不久交通也漸漸開始出現一場新的革命。

人類不再需要舟車勞頓的駕駛車輛，集所有汽車工程技術於一身的自動駕駛車輛，為人類的交通帶來一個新的願景。



（圖片來源／Volvo）

自動對焦鏡頭

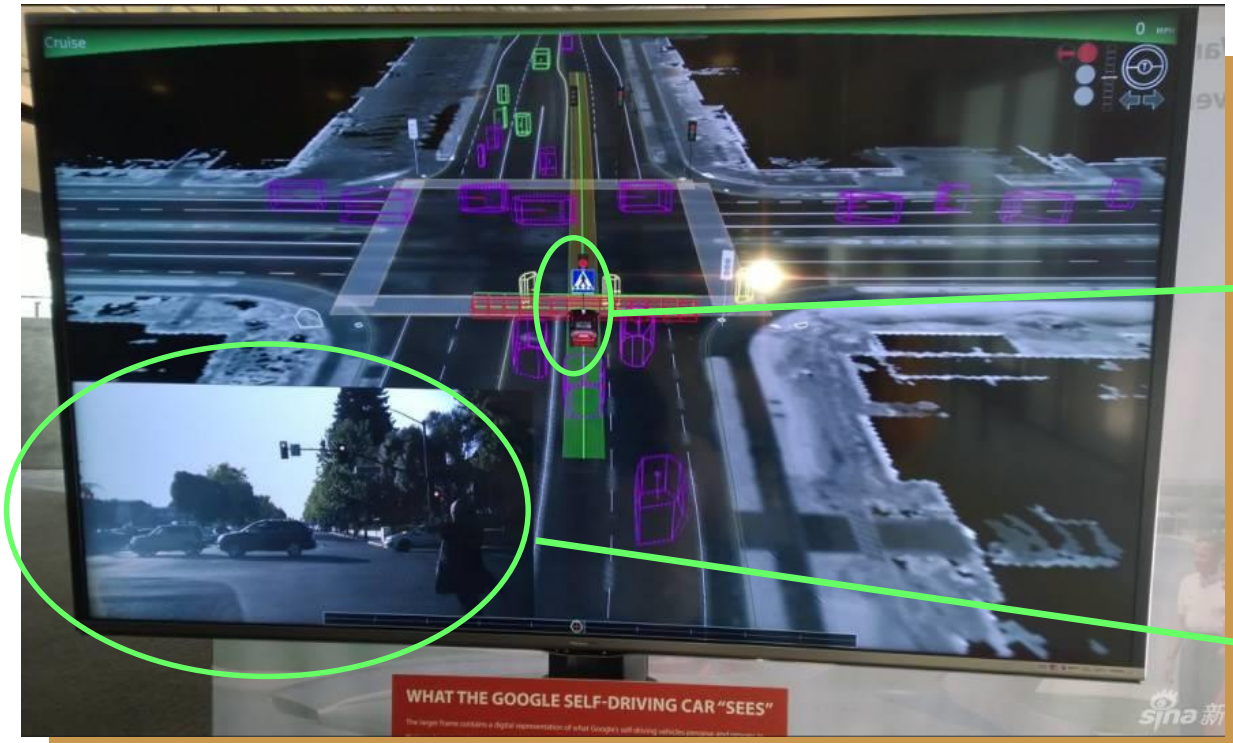
自動對焦攝影機主要用來辨識物體性質。
在車輛前後的所有東西，透過攝影機將畫面傳至電腦分析辨識物體性質，以用來協助判斷行車狀況。

後視鏡位置裝有面對前後的自動對交攝影機，用以辨識車輛前後所有物體。

（圖片來源／新浪科技）

行車電腦

綜觀雷達、攝影機、GPS、速度感知、網路資訊等等，將所有資訊匯整後，再交由電腦演算判斷。



（圖片來源／新浪科技）

由車身為中心，綜合GOOGLE MAP與雷達的三維地圖。

物體性質判斷的自動對焦攝影機畫面。

讓汽車成為充滿愛的產品

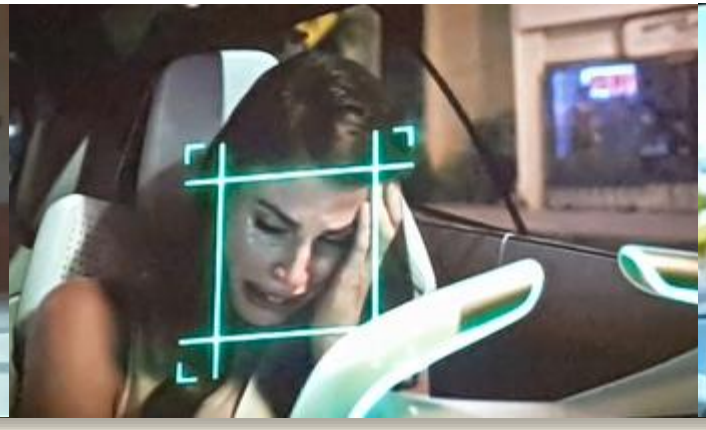
豐田概念車「Concept-愛i」發展出人與車的新關係

建議路線

駕駛支援

家人的辨識

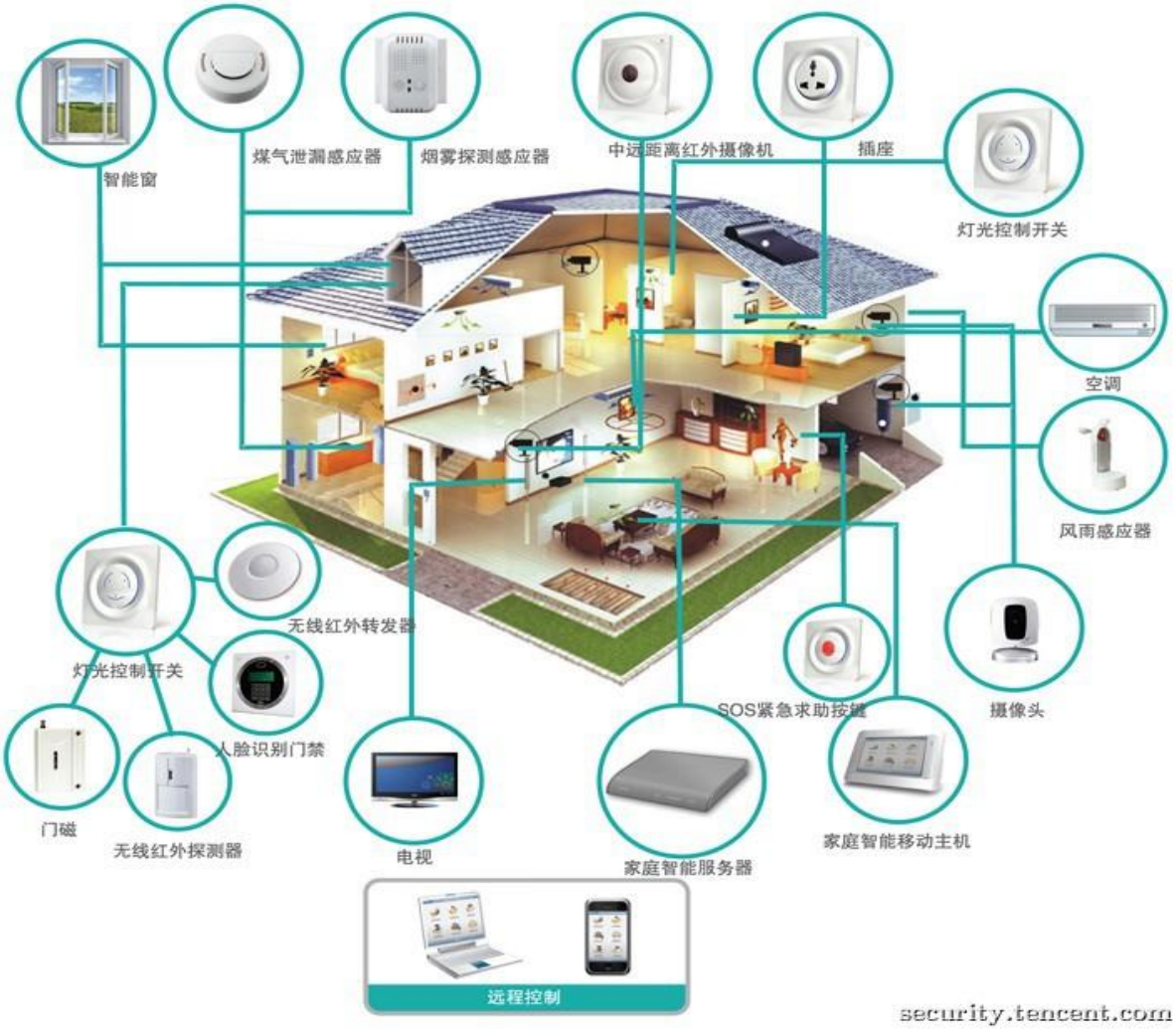
觀察人的情緒



與人對話

資料來源：豐田，DIGITIMES整理，

潛伏在身邊的危機：智慧設備安全



車聯網產品

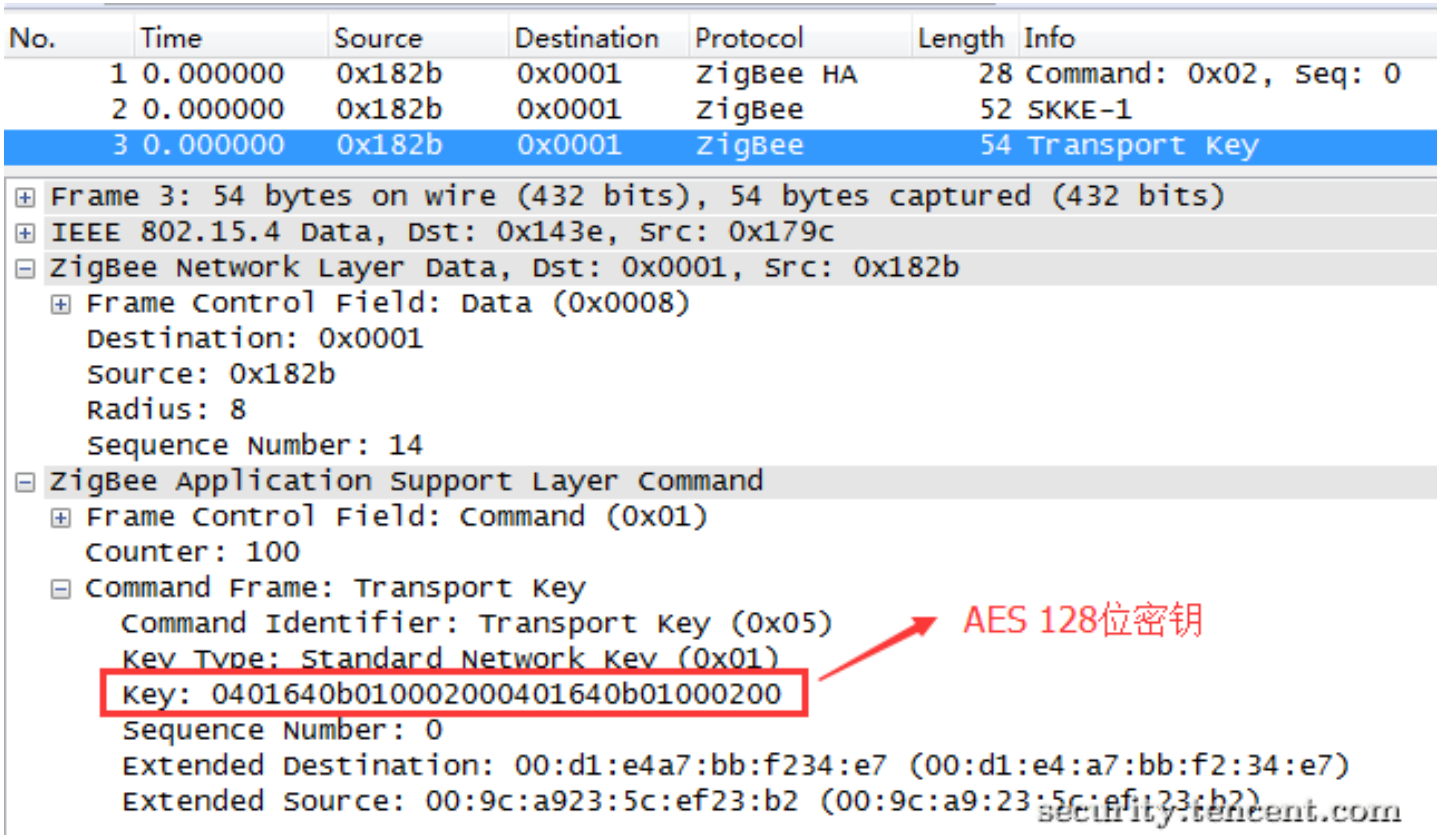

安防
娱乐
通信
Telematics Service Provider
导航&位置服务
远程救援
其它
互联网
语音
短信
车联网接入中心
内容提供商
其它
停车场
宾馆
新闻
餐厅
交通
天气
生产商
车厂
销售商
支持团队
运维
呼叫中心
互联网
车间通信网络
周边网络
互联网
其它车辆
道路基础设施
警务
消防
医务
联系
security.tencent.com

可穿戴設備


头戴显示器--Head
谷歌眼镜--Eyes
智能项链--Colpus
智能手表--Wrist
智能手环--Ring
心率带--Hand
智能内裤--Hip
智能跑鞋--Foot
PConline
太平洋电脑网
security.tencent.com

破解某智慧插座實現遠端控制

傳輸的敏感資訊被竊取


No. Time Source Destination Protocol Length Info
1 0.000000 0x182b 0x0001 ZigBee HA 28 Command: 0x02, Seq: 0
2 0.000000 0x182b 0x0001 ZigBee 52 SKKE-1
3 0.000000 0x182b 0x0001 ZigBee 54 Transport Key
Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
IEEE 802.15.4 Data, Dst: 0x143e, Src: 0x179c
ZigBee Network Layer Data, Dst: 0x0001, Src: 0x182b
Frame Control Field: Data (0x0008)
Destination: 0x0001
Source: 0x182b
Radius: 8
Sequence Number: 14
ZigBee Application Support Layer Command
Frame Control Field: Command (0x01)
Counter: 100
Command Frame: Transport Key
Command Identifier: Transport Key (0x05)
Key Type: Standard Network Key (0x01)
Key: 0401640b010002000401640b01000200
Sequence Number: 0
Extended Destination: 00:d1:e4a7:bb:f234:e7 (00:d1:e4:a7:bb:f2:34:e7)
Extended Source: 00:9c:a923:5c:ef23:b2 (00:9c:a9:23:5c:ef:23:b2)
AES 128位密钥
security.tencent.com

駭客特別愛用IOT裝置當作攻擊跳板

IoT裝置一般存在有5大安全弱點，因而容易遭駭客所利用，分別是（1）IoT裝置本身已存在潛在可利用的漏洞、（2）使用不安全的網路協定、雲端及行動App服務，或是提供不安全的軟體、韌體更新、（3）仍保留不安全的網路連接埠、（4）允許未授權的系統變更，以及（5）授權/認證強度不夠及缺乏足夠安全的加密機制。

無線網路防護措施

家用與企業無線Wi-Fi的管理方式與建議，改善無線網路安全的事項。

1.需妥善設定SSID:變更過SSID與密碼不要使用原廠預設資訊

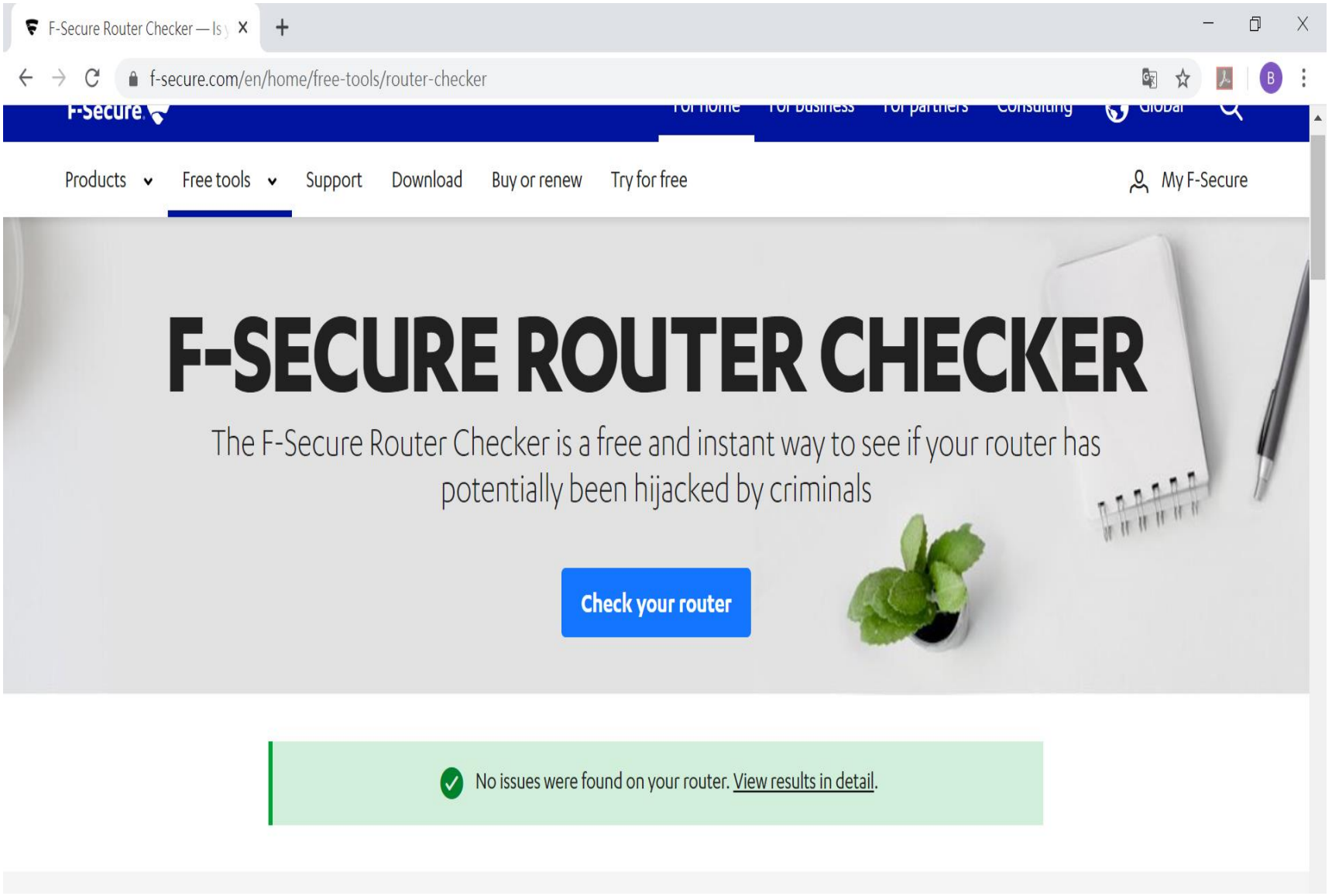
2.請將無線網路設定為WPA2加密

3.切記Wi-Fi密碼設定不可過於簡單

4.管理介面的密碼修改也很重要

5.注意韌體更新，減少設備漏洞威脅

6.藉助其他工具或服務(https://campaigns.f-secure.com/router-checker/en_global/)


F-Secure Router Checker — Is
f-secure.com/en/home/free-tools/router-checker
F-Secure
For home
For business
For partners
Consulting
Global
Products
Free tools
Support
Download
Buy or renew
Try for free
My F-Secure
F-SECURE ROUTER CHECKER
The F-Secure Router Checker is a free and instant way to see if your router has potentially been hijacked by criminals
Check your router
No issues were found on your router. View results in detail.

數位轉型下雲端風險問題

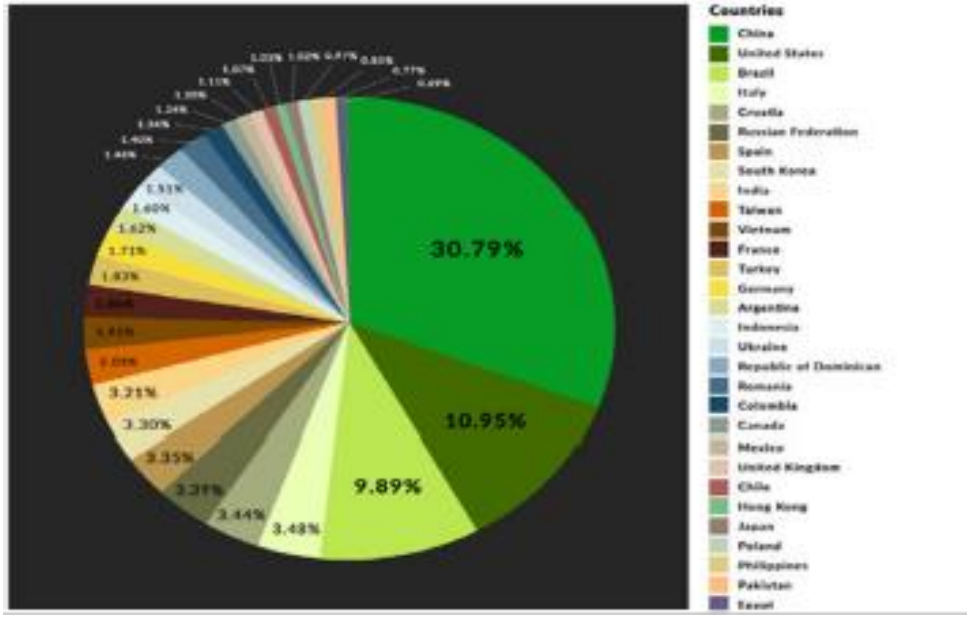
台灣在全球經貿及產業供應鏈扮演要角，疫情驅使下，企業推動數位轉型的進程將更為迅速，當今顯而易見，企業正加速將基礎架構移轉至混合雲，仰賴雲端進行資料串聯處理，趨勢科技預測企業因不適切的雲端設定所引發的資料外洩事件將會更為頻繁，雲端安全風險將來自於用戶不當操作或設定，而非雲端供應商。而被大量使用於讓外界存取內部系統的應用程式開發介面 (API)，隨著相關運用層面越來越廣，但是對安全的著墨卻仍在初始階段，意味著成為駭客入侵企業管道的機會亦將隨之擴大，在被駭客關注的同時，企業亦須注意 API 的安全風險。

物聯網設備數量攀升

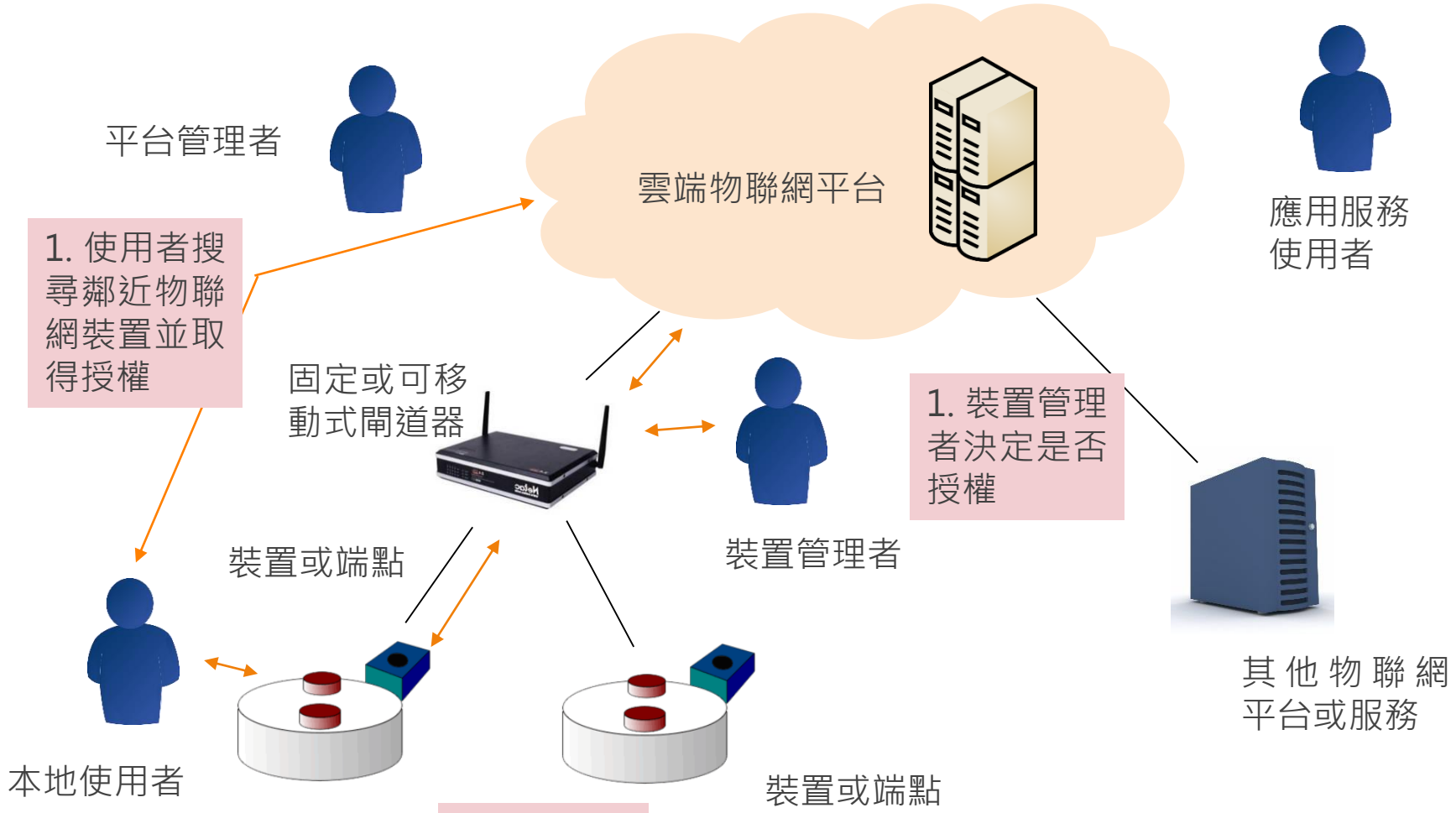
國際研究暨顧問機構Gartner預測，物聯網設備數量將快速上升，到2020年將會有204億個物聯網設備連上網路
由於物聯網裝置數量過多又缺乏安全控制措施，使得遭利用作為DDoS攻擊來源數目急遽提升
The Hacker News報告顯示，藉由遭利用的物聯網設備執行DDoS攻擊已達到Tbps的流量

物聯網惡意軟體

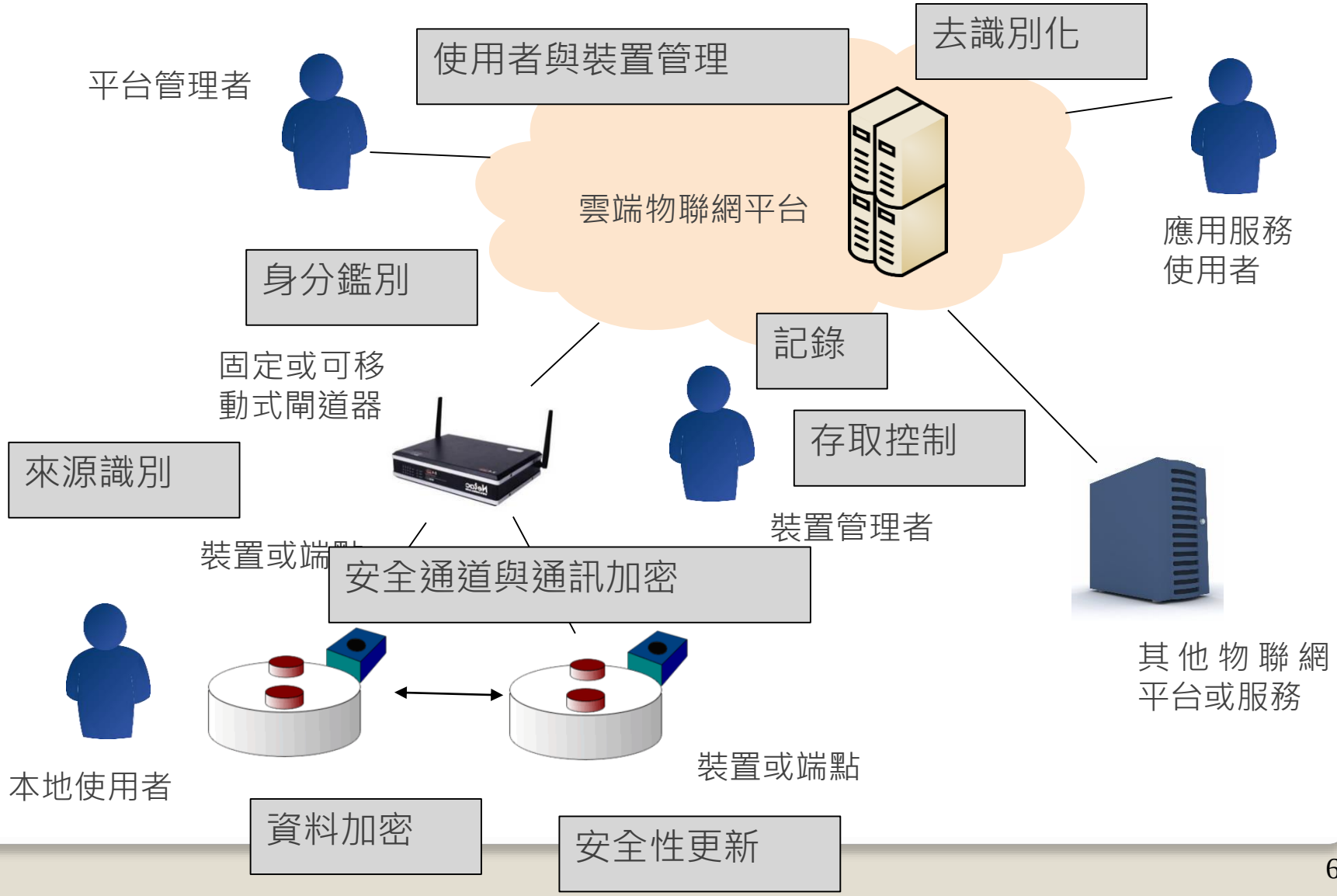
受惡意軟體所感染的物聯網裝置遍布於世界各地
–以Mirai惡意軟體為例，受Mirai惡意軟體感染的裝置，會持續在網際網路上掃描物聯網裝置的IP位址，然後辨別出容易受到攻擊的裝置，再使用預設使用者名稱與密碼登入這些裝置，以注入Mirai惡意軟體
–而受感染的裝置將會繼續正常工作，只是成為Mirai所掌握的上30萬名殭屍網路軍隊中的一員



本地使用者要求存取裝置

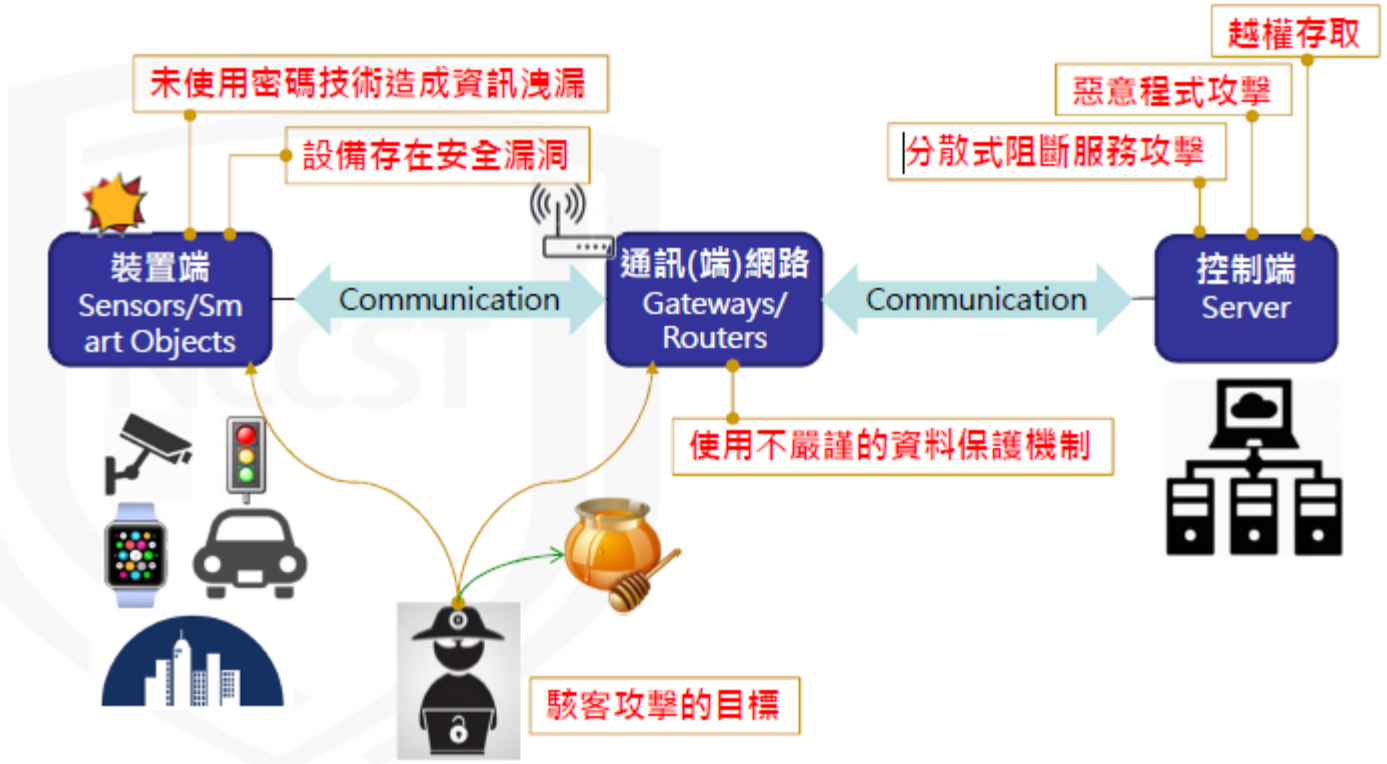


物聯網安全控制


平台管理者
使用者與裝置管理
去識別化
雲端物聯網平台
應用服務
使用者
身分鑑別
固定或可移
動式閘道器
記錄
來源識別
存取控制
裝置管理者
裝置或端點
安全通道與通訊加密
其他物聯網
平台或服務
本地使用者
裝置或端點
資料加密
安全性更新

物聯網安全議題

● 一般物聯網架構可分為「裝置端」、「通訊(端)網路」及「控制端」，其衍伸相關安全議題



物聯網安全議題

控制端

–因使用的平台種類眾多，若未做好身分認證或存取控制，可能使攻擊者越權下達攻擊指令，存取機敏或他人資料

–未更新伺服器之作業系統或採用存在漏洞的應用程式套件，可能讓駭客透過相關漏洞來入侵系統或植入惡意程式

物聯網安全議題

通訊(端)網路
–若傳輸未經加密或使用不安全的加密演算法，可能導致資料外洩問題

物聯網安全現況-Shodan

TOTAL RESULTS

45,013

TOP COUNTRIES

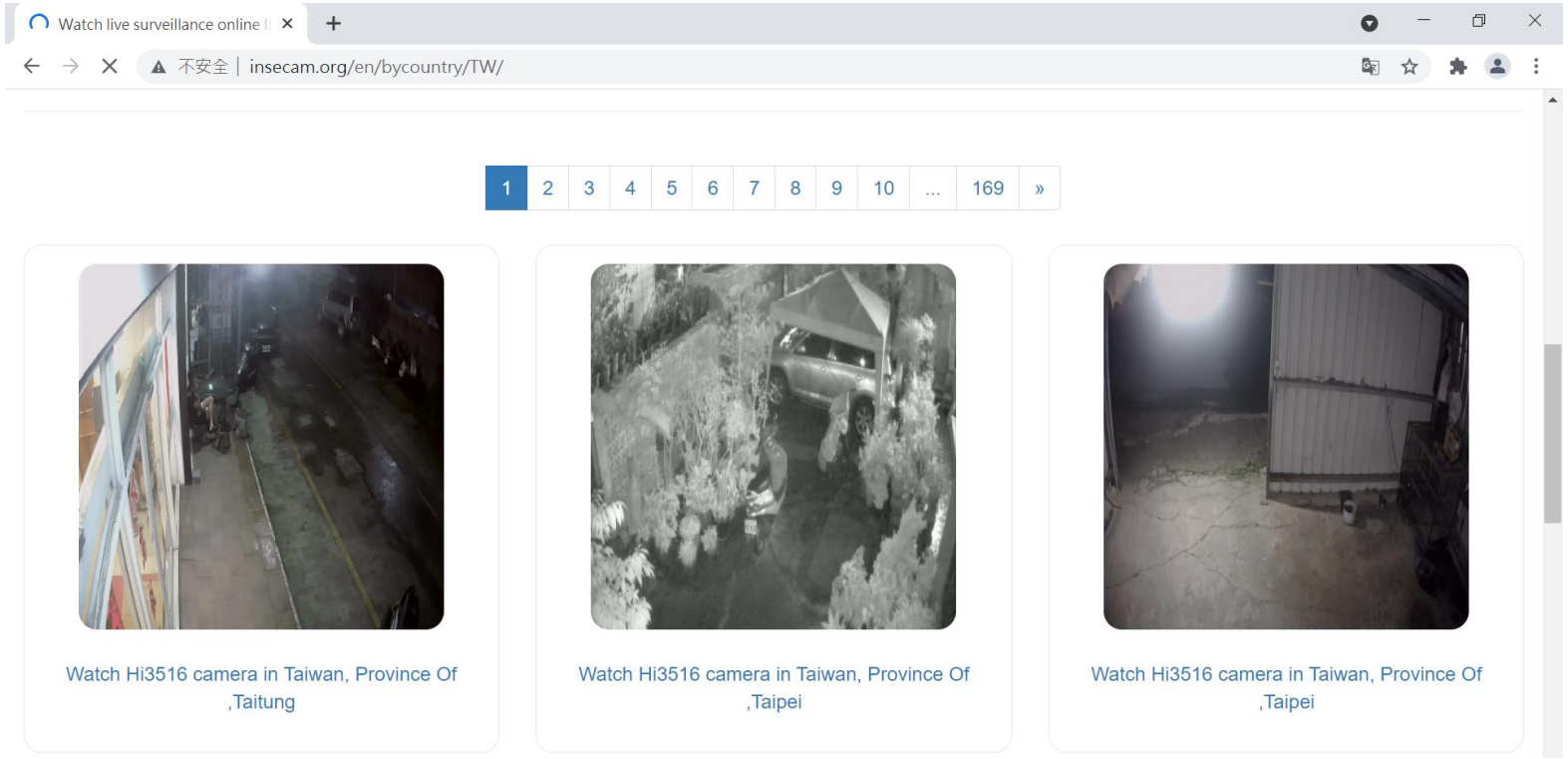
Korea, Republic of	10,841
Taiwan	10,036
China	7,554
United States	4,260
Hong Kong	2,442

TOP ORGANIZATIONS

Device Name	Model Name	Device Type	Count
Samsung Galaxy Note 3	SAMSUNG-SM-N900A	Android Smart Phone	2904
Motorola Moto X (Europe)	XT1052	Android Smart Phone	2886
Google Pixel XL	Pixel XL	Android Smart Phone	472
Google PIXEL 2 XL	PIXEL 2 XL	Android Smart Phone	454
Samsung Galaxy S5	SM-G900F	Android Smart Phone	436
OnePlus 3T	ONEPLUS A3010	Android Smart Phone	360
OnePlus 5	ONEPLUS A5000	Android Smart Phone	358
Samsung Galaxy S8 Plus	SM-G955F	Android Smart Phone	337
Samsung Galaxy S8	SM-G950F	Android Smart Phone	335
Samsung Galaxy S4	GT-I9500	Android Smart Phone	100
EVPAD PRO 電視卡盒	EVPAD-PRO-T	Android TV box	56
EVPAD PRO 電視卡盒 台灣版	EVPAD-TW-MAX	Android TV box	46
Asus ZenFone 5	ASUS T00J	Android Smart Phone	44
MXQ PRO 4K s905 p201	Android p201	Android TV box	43
EVPAD PRO 電視卡盒	EVPAD-PRO-MAX	Android TV box	33
Sunchip TV box	CX_A39	Android TV box	33
Unblock Global Edition S800	Global_Edition_S800	Android TV box	30
RockTek A2V	RT_A2V	Android TV box	24
Askey Set-top box	STI6030	Android TV box	24
JVC 65T	65T	Smart TV	21

物聯網安全現況-Insecam

- 線上監視錄影器的網站，匯流全世界網路攝影機連結，可供人看到即時直播畫面



物聯網設備預設密碼掃描檢測

```
/Users/rapid7/freetools>perl iotScanner.pl 1.23.123.431,
1.23.123.443,1.23.123.453,1.23.123.457,1.23.123.459,1.23.123.461,1.
23.123.462,1.23.123.463,1.23.123.465,1.23.123.466,1.23.123.467,1.23
.123.469,1.23.123.472,1.23.123.473,1.23.123.475,1.23.123.477,1.23.1
23.479,1.23.123.480,1.23.123.481
device 1.23.123.431 is of type Stardot still has default passwd
device 1.23.123.443 is of type Arecont has changed passwd
device 1.23.123.453 is of type American Dynamics has changed passwd
device 1.23.123.457 is of type W-Box has changed passwd
device 1.23.123.459 is of type Arecont has changed passwd
device 1.23.123.461 is of type American Dynamics has changed passwd
device 1.23.123.462 is of type W-Box has changed passwd
device 1.23.123.463 is of type Arecont has changed passwd
device 1.23.123.465 is of type American Dynamics has changed passwd
device 1.23.123.466 is of type W-Box has changed passwd
device 1.23.123.467 is of type Arecont has changed passwd
device 1.23.123.469 is of type American Dynamics has changed passwd
device 1.23.123.472 is of type W-Box has changed passwd
device 1.23.123.473 is of type W-Box has changed passwd
device 1.23.123.475 is of type W-Box has changed passwd
device 1.23.123.477 is of type W-Box still has default passwd
device 1.23.123.479 is of type Arecont has changed passwd
device 1.23.123.480 is of type American Dynamics has changed passwd
device 1.23.123.481 is of type American Dynamics has default passwd
```

適應多種類型IoT設備，和大範圍IP網路掃描

檢測設備SNMP漏洞工具

```
from snmp_set_fuzz import *
target = '192.168.81.19'
port = 80
count = 10
nic = conf.route.route(target)[0]
Target = SnmpTarget(name='test', monitor_port=port, community='tdhx',
 oid='.1.3', version=2, target=target, nic=nic, fuzz_count=count)
Target.read_test_case_from_pcap('./output/192.168.81.19_snmp_set_packet_list.pcap')
Target.fuzz()
```

SNMP操作來修改設備網卡的mac位址，但是沒有對mac位址的長度進行校驗，只要傳入過長或者過短的mac位址都會造成設備癱瘓。

弱點掃描服務使用工具

- 從系統弱點掃描網路測試(白箱測試)
  1. Nessus
  2. Microsoft Baseline Security Analyzer
  3. Shadow Security Scanner
  4. Retina Network Security Scanner
  5. SNMP Fuzzer
  6. IoT-Implant-Toolkit
  7. Attify Zigbee Framework
  8. IoTSeeker
  9. CloudMapper
  10. X-Scan
  11. 自行研發工具(新攻擊手法檢測工具)

- 黑箱測試：指在測試前，測試單位不知道測試目標資訊。以遠端的方式及以駭客的角度來檢視測試標的網路環境安全現況。

系統弱點解決方法

- 系統弱點
  - 修補弱點方法
    - 依弱點風險等級，進行修補作業
    - 比對單位資安政策，並進行調整。
- 不明程式
  - 移除
    - 已知惡意程式
    - 未知攻擊手法
    - 重新安裝作業系統

弱點掃描建議

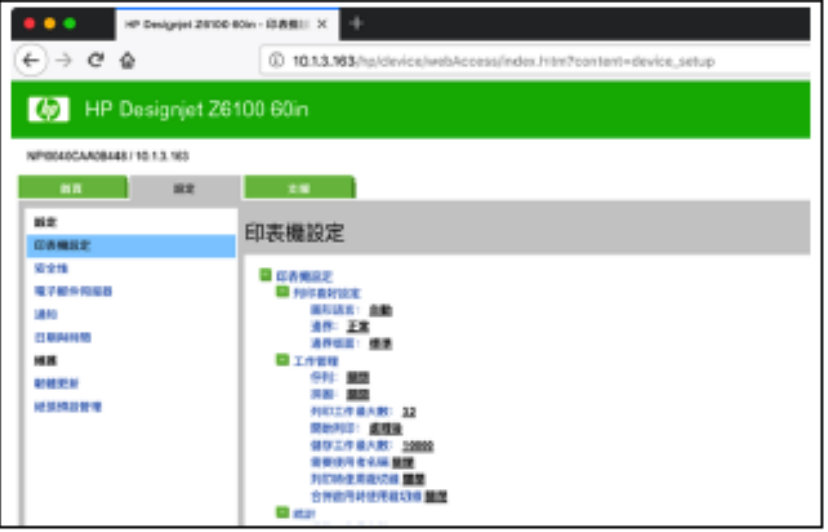
- 提升單位資安強度與調整資安政策
  - 修正檢測掃描風險的弱點
  - 修正駭客入侵系統的弱點
  - 系統層面弱點
    - 進行系統弱點修正
    - 進行應用程式修正
    - 調整單位網路架構
  - 政策層面弱點
    - 資訊安全政策調整
    - 系統使用權限控管

物聯網設備檢測結果

HP Designjet Z6100 60 in Photo

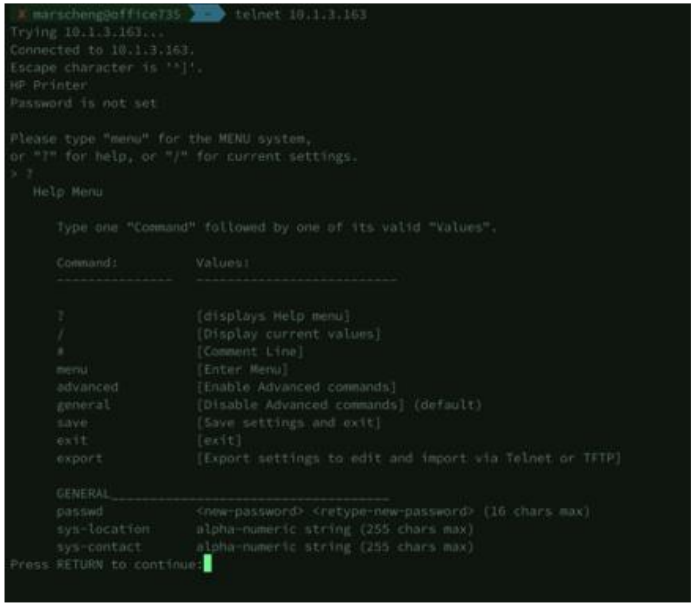
埠	服務
1/TCP	Tcpmux
21/TCP	FTP
23/TCP	Telnet
80/TCP	HTTP
280/TCP	HTTP
512/TCP	Exec
513/TCP	Login
514/TCP	Tcpwarpped
515/TCP	Line Printer Daemon protocol
2000/TCP	Tcpwarpped
5060/TCP	Tcpwarpped
8001/TCP	Vcom-tunnel
8085/TCP	Simple Object Access Protocol
8086/TCP	Simple Object Access Protocol
8090/TCP	Simple Object Access Protocol
9100/TCP	Jetdirect
9103/TCP	Jetdirect
9104/TCP	Jetdirect

物聯網設備檢測結果

弱點名稱	設備網站管理介面(服務埠 80) 未設定管理者帳號密碼	風險等級	高
CVE 編號	N/A	弱點設備	10.1.3.163
弱點分類	身分鑑別與授權不足		
弱點說明	攻擊者可在未登入的狀態下瀏覽網站管理介面，並成功關閉印表機列印服務		
修補建議	設定網站管理介面帳號密碼		
檢測說明	測試人員連線至設備網站頁面，在未登入情形下，於「網路」→「其他設置」頁面中，成功關閉「9100 打印」服務		
檢測畫面			

物聯網設備檢測結果

弱點名稱	設備 Telnet 服務未設定管理者帳號密碼	風險等級	高
CVE 編號	N/A	弱點設備	10.1.3.163
弱點分類	身分鑑別與授權不足		
弱點說明	攻擊者可在未登入的狀態下與設備 Telnet 服務連線，並成功關閉印表機列印服務		
修補建議	設定 Telnet 服務帳號密碼		
檢測說明	測試人員連線至設備 Telnet 服務，在未登入情形下，確認服務埠 9100 為「Enabled」狀態，並成功關閉服務埠 9100		



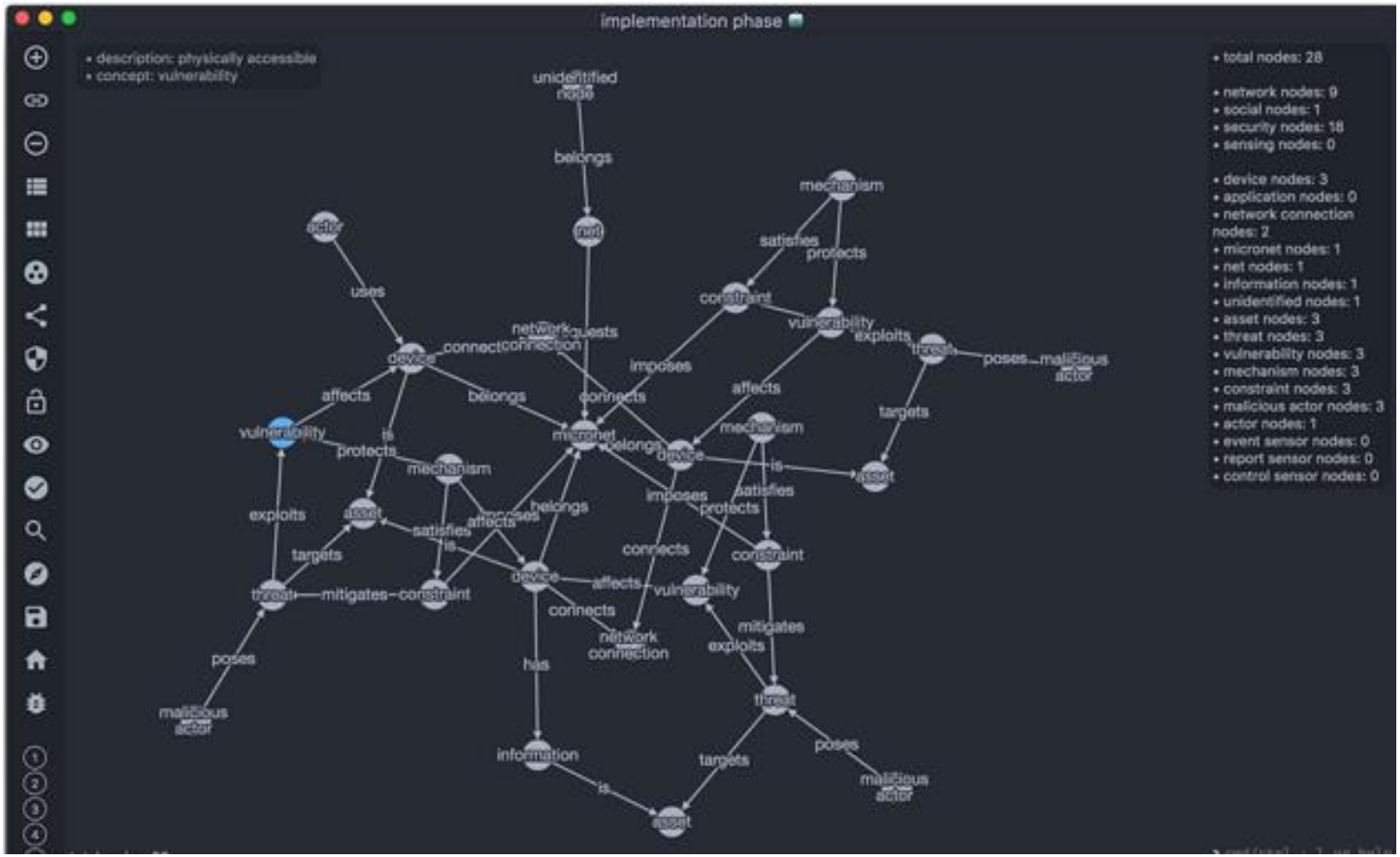
物聯網設備檢測結果

門禁設備檢測結果 **Soyal AR-829Ev5**

弱點名稱	設備存在無效的存取控管弱點	風險等級	高
CVE 編號	N/A	弱點設備	10.1.2.198
弱點分類	不安全的網頁介面		
弱點說明	攻擊者透過修改封包參數內容，修改管理者密碼，並成功取得門禁資料		
修補建議	修正程式判斷權限之邏輯，並落實權限控管		
檢測說明	測試人員瀏覽設備網站，並點選「LoginPassword」功能後，使用 Burp Sutie 工具攔截並修改封包內容，成功在未登入狀態下將管理者密碼修改為 [redacted]。接續使用修改後的帳號密碼登入，成功瀏覽設備組態設定		
檢測畫面			

IoT設備的木馬掃描檢測

物網路安全視覺分析


implementation phase
• description: physically accessible
• concept: vulnerability
• total nodes: 28
• network nodes: 9
• social nodes: 1
• security nodes: 18
• sensing nodes: 0
• device nodes: 3
• application nodes: 0
• network connection nodes: 2
• micronet nodes: 1
• net nodes: 1
• information nodes: 1
• unidentified nodes: 1
• asset nodes: 3
• threat nodes: 3
• vulnerability nodes: 3
• mechanism nodes: 3
• constraint nodes: 3
• malicious actor nodes: 3
• actor nodes: 1
• event sensor nodes: 0
• report sensor nodes: 0
• control sensor nodes: 0
unidentified node
belongs
net
actor
uses
mechanism
satisfies
protects
constraint
vulnerability
exploits
threat
poses
malicious actor
network connection
connect
connection
device
imposes
affects
belongs
connects
micronet
vulnerability
is
protects
mechanism
asset
targets
exploits
satisfies
affects
belongs
imposes
protects
connects
constraint
device
affects
vulnerability
threat
mitigates
constraint
connects
network connection
mitigates
exploits
has
poses
malicious actor
information
is
asset
targets
poses
malicious actor

弱點類型

- 參考「OWASP IoT Top 10 –2014」弱點類型
- 物聯網設備檢測中，弱點類型多為身分鑑
- 別與授權不足–其中多因使用不安全的密碼或未做好適當的權限管理

OWASP Internet of Things Top 10 –2014			
A1	不安全的網頁介面	A6	不安全的雲端介面
A2	身分鑑別與授權不足	A7	不安全的行動應用介面
A3	提供不安全的網路服務	A8	安全設定不足
A4	缺乏傳輸加密保護	A9	不安全的軟體及韌體
A5	隱私議題	A10	缺乏實體安全

OWASP IOT Top 10 2018

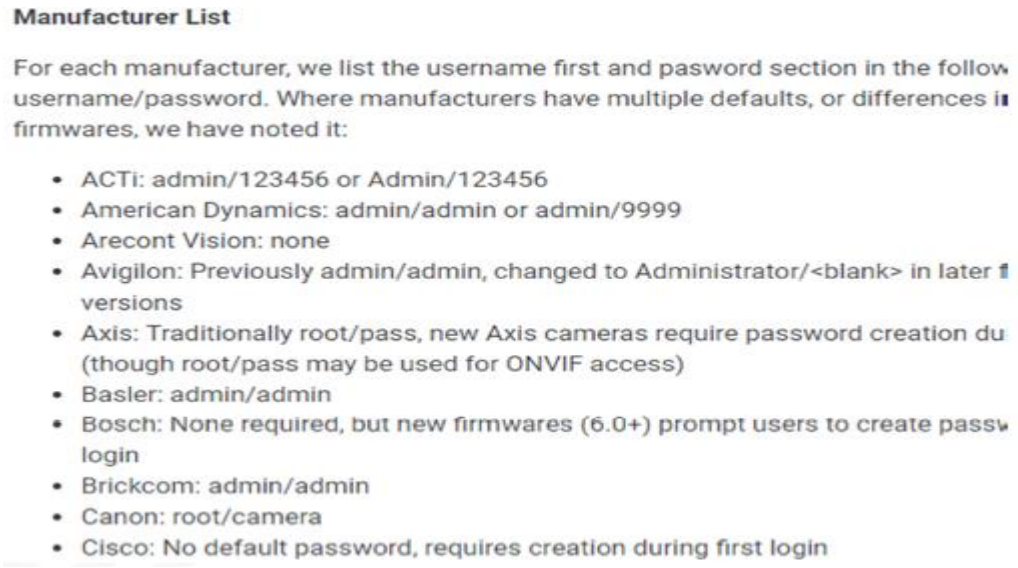
1. 弱密碼 (Weak Guessable or Hardcoded Passwords)
2. 不安全的網路服務 (Insecure Network Services)
3. 不安全的生態界面 (Insecure Ecosystem Interfaces)
4. 不安全的更新機制 (Lack of Secure Update Mechanism)
5. 使用不安全的元件 (Use of Insecure Outdated Components)
6. 隱私防護不足 (Insufficient Privacy Protection)
7. 不安全的資料轉移和儲存 (Insecure Data Transfer and Storage)
8. 缺乏裝置設定 (Lack of Device Settings)
9. 不安全的預設 (Insecure Default Settings)
10. 缺少物理加固措施 (Lack of Physical Hardening)

使用不安全的密碼

說明

– 使用者未正確的設定安全的帳號密碼，使攻擊者可透過預設的帳號密碼、密碼猜測或暴力破解等方式，取得設備管理權限

透過網路資源尋找各廠牌網路攝影機的預設帳號密碼



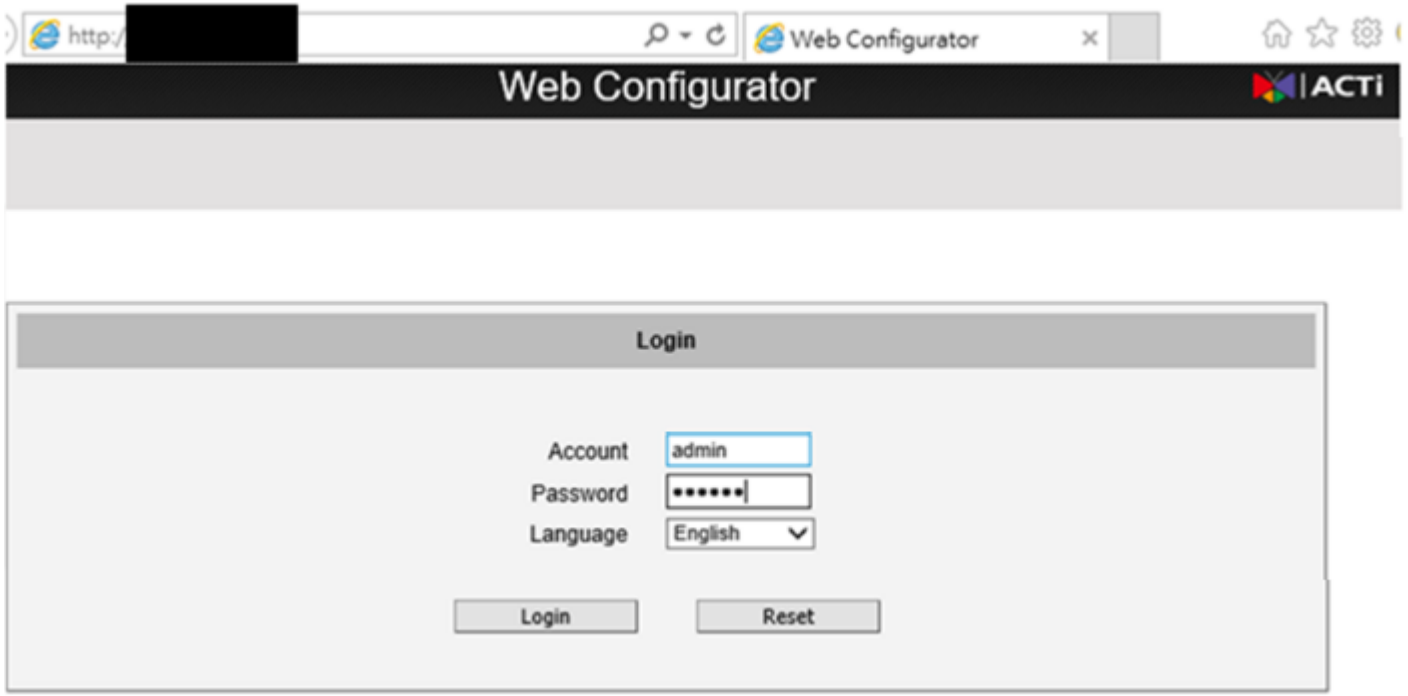
Manufacturer List

For each manufacturer, we list the username first and pasword section in the follow username/password. Where manufacturers have multiple defaults, or differences i firmwares, we have noted it:

- ACTi: admin/123456 or Admin/123456
- American Dynamics: admin/admin or admin/9999
- Arecont Vision: none
- Avigilon: Previously admin/admin, changed to Administrator/<blank> in later f versions
- Axis: Traditionally root/pass, new Axis cameras require password creation du (though root/pass may be used for ONVIF access)
- Basler: admin/admin
- Bosch: None required, but new firmwares (6.0+) prompt users to create passv login
- Brickcom: admin/admin
- Canon: root/camera
- Cisco: No default password, requires creation during first login

使用不安全的密碼

嘗試使用預設帳號密碼登入網站頁面



落實資安教育訓練，更改設備預設帳號密碼，並使用較強的密碼規則

結論

- 使用物聯網設備時，應確實檢視設備所提供的功能，並設定使用者所能存取之權限
  - 關閉設備非必要之功能
  - 透過安全性設定進行權限控管
  - 透過其他防護設備限制使用者可存取之服務
- 安全性功能之設備
  - 啟用設備上所有的安全功能
  - 關閉設備非必要的服務
  - 使用會定期更新產品韌體之廠商產品，
- 並執行安全更新可透過CVE網站注意設備版本是否存在已知漏洞


THE
END