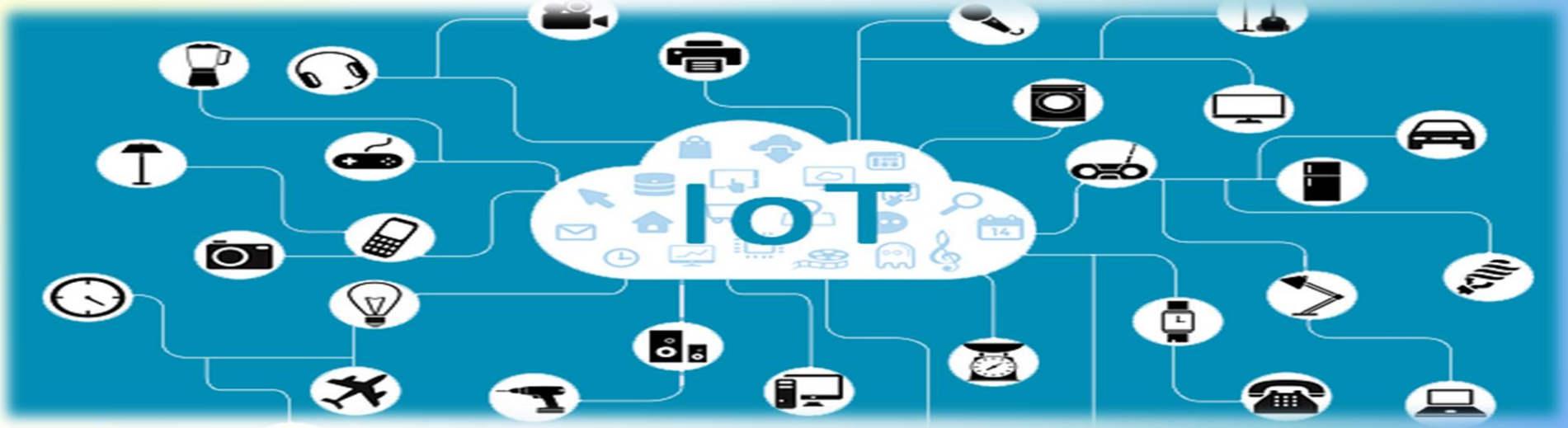


物聯網與資訊安全

BCCS 漢昕科技 資訊安全管理顧問：王信何

代理通路 顧問服務 教育訓練 資安稽核

大綱

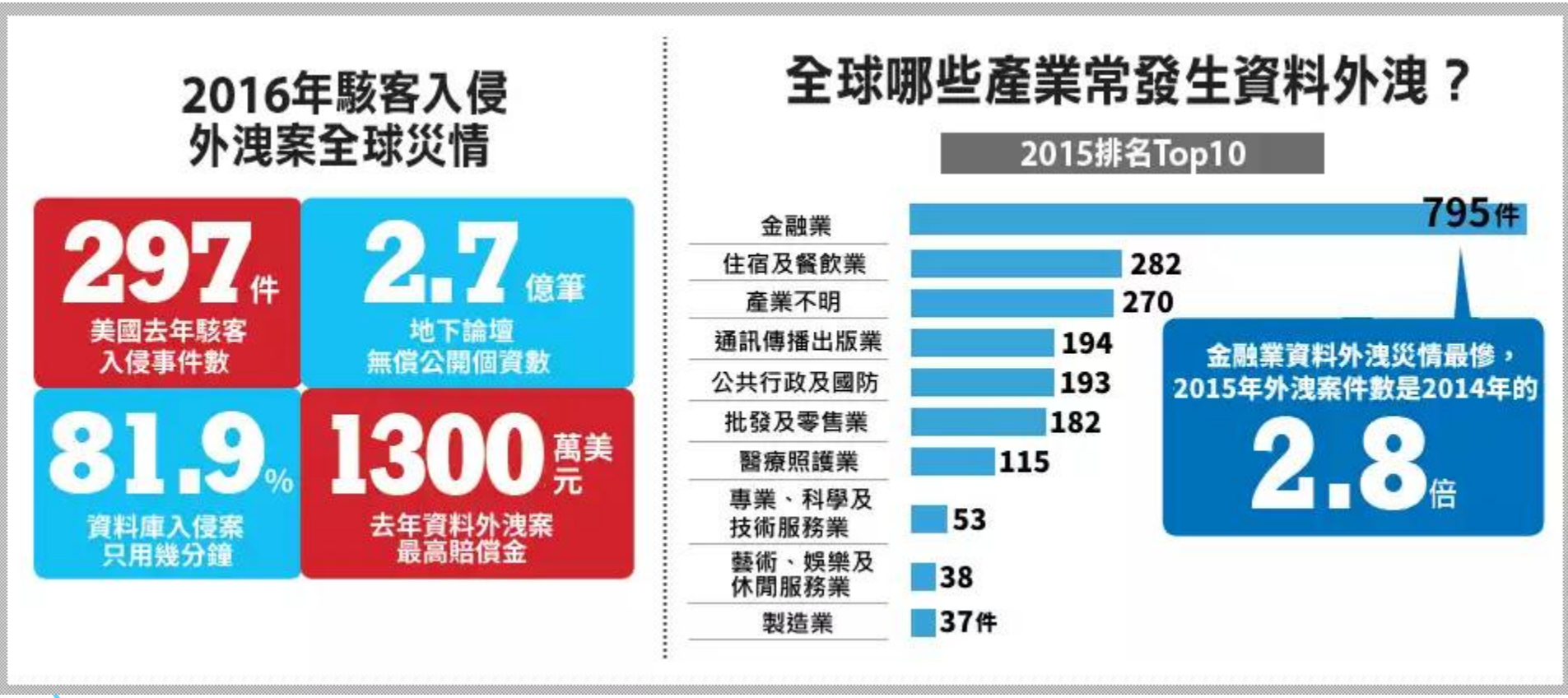
- 資安威脅
- 初探物聯網
- 物聯網之應用與發展
- 物聯網之資訊安全隱憂

前言：資安威脅


2017
CIO必看
四大資安趨勢
資安趨勢1
資料外洩
資料外洩事件翻倍暴增，金融成竊資首選
資安趨勢2
勒索軟體
勒索軟體風暴狂襲，資安跨業聯手大反制
資安趨勢3
IoT殭屍大軍
百萬IoT殭屍大軍來勢洶洶
資安趨勢4
關鍵基礎設施
連網威脅攀升，關鍵基礎設施拉警報

2017四大資安趨勢之一

- 資料外洩事件翻倍暴增，金融成竊資首選



圖片來源: 資料來源：Privacy Rights Clearinghouse、Verizon，iThome整理製圖

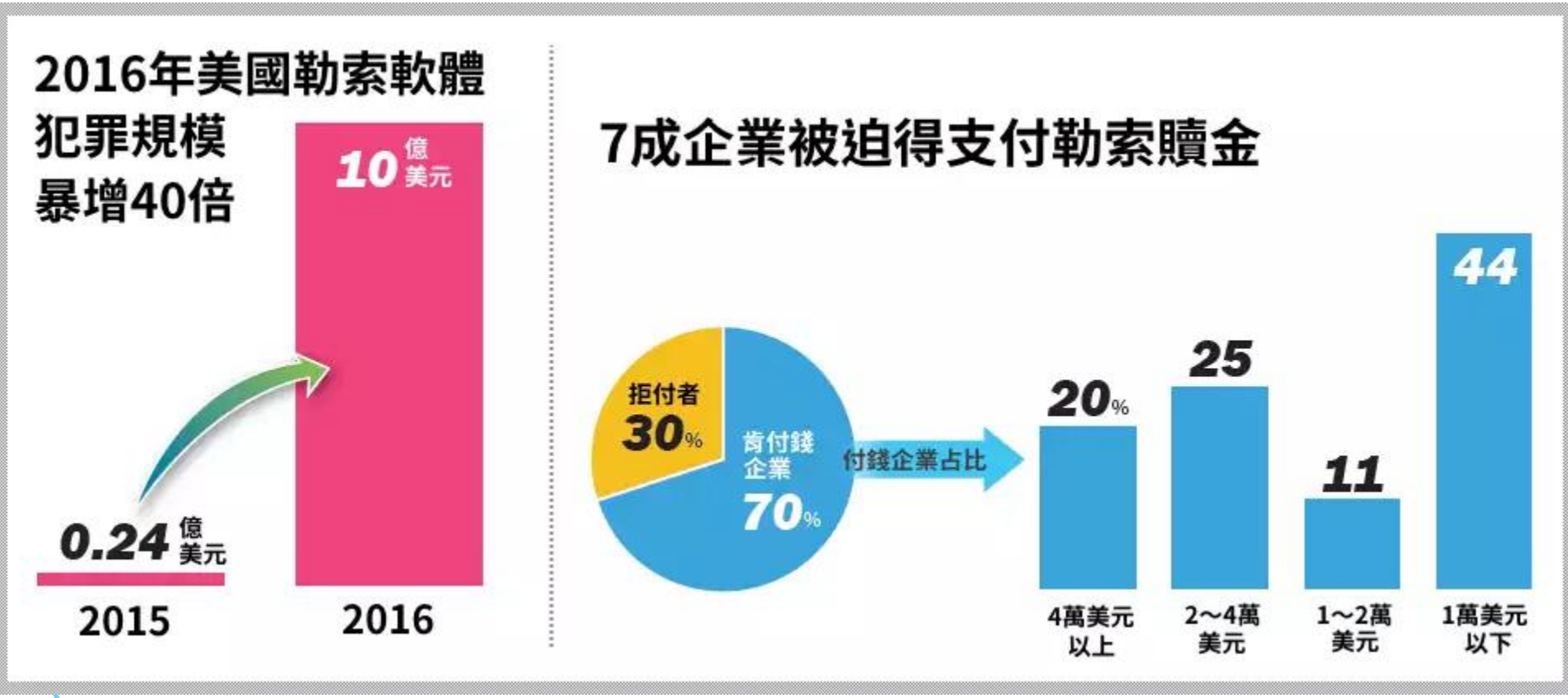
Yahoo資料外洩規模超過10億

- Yahoo在11月接獲警方通報，發現在2013年遭第三方竊取超過10億用戶資料，包含用戶姓名、電郵地址、電話號碼、生日、經雜湊處理的密碼，甚至用戶的安全問答，還有用於產生cookies的專用碼也遭到竊取

圖片來源：YAHOO

2017四大資安趨勢之二

- 勒索軟體風暴狂襲，資安跨業聯手大反制



圖片來源: 資料來源：美國FBI、IBM X-Force，iThome整理製圖

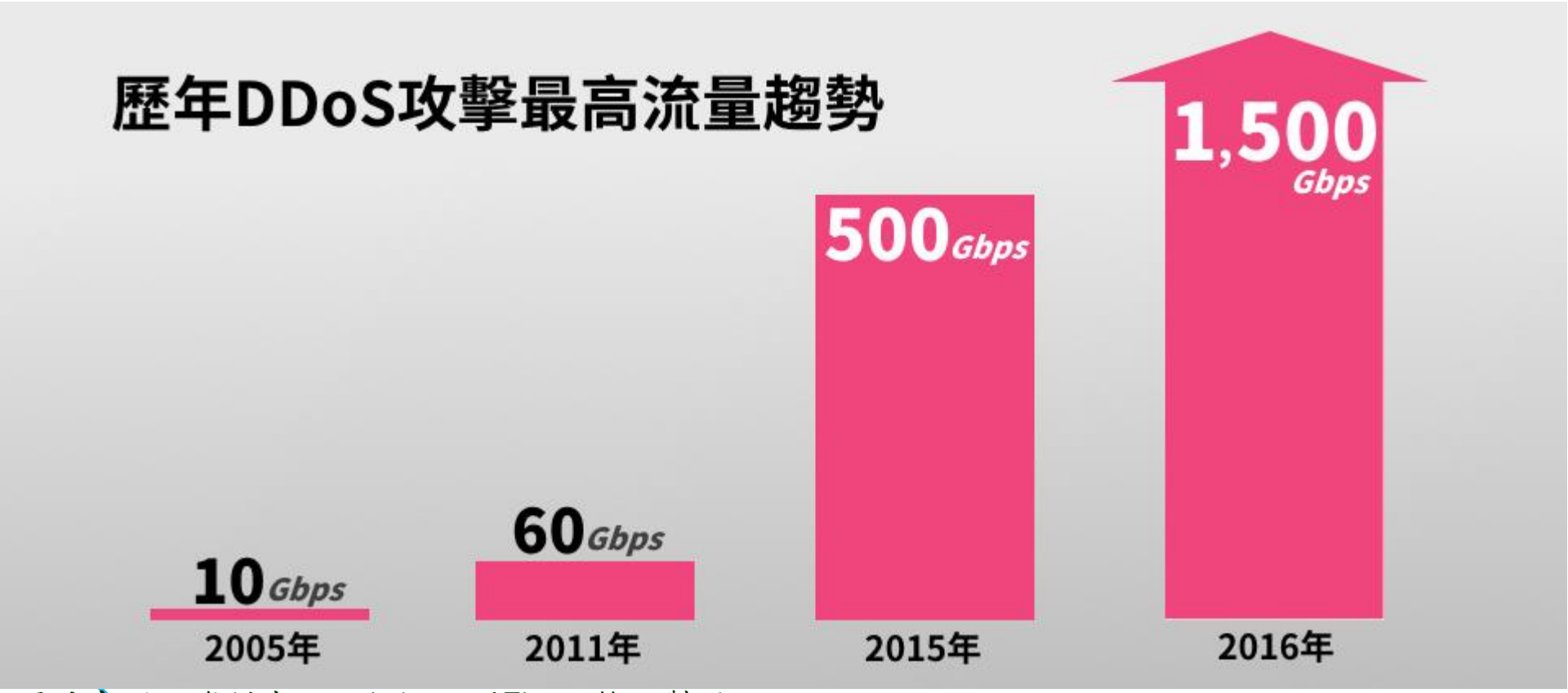
入侵醫院主機挾病歷勒索逾1億

- 美國洛杉磯好萊塢長老教會醫療中心近日對外證實，該院受到勒索軟體的危害，導到部分重要HIS系統停擺一周，被勒索9000比特幣（約1.1億元台幣）贖金。

資料來源：翻攝英國廣播公司

2017四大資安趨勢之三

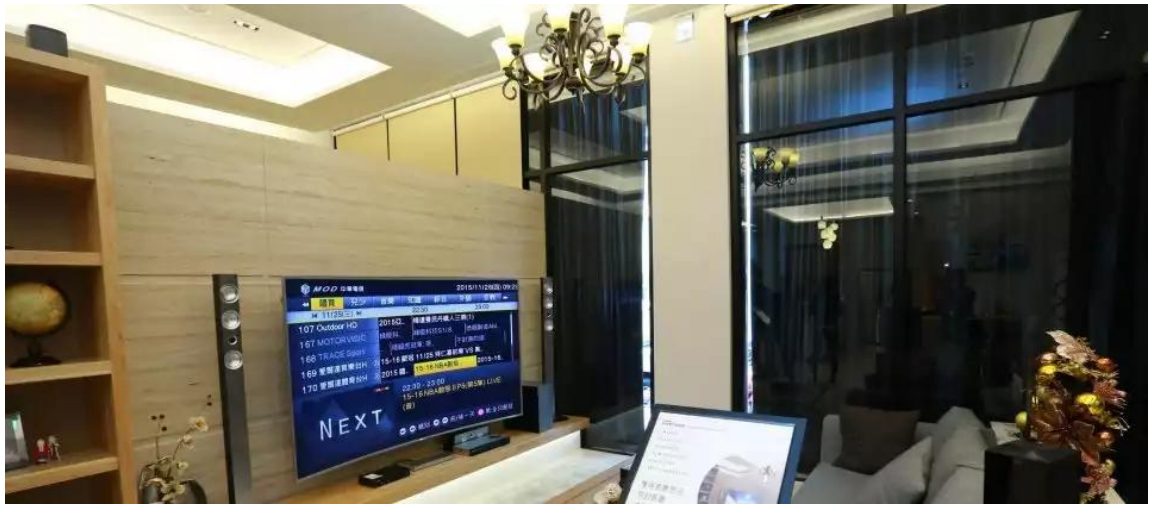
- 百萬IoT殭屍大軍來勢洶洶，Tb級DDoS攻擊越演越烈



圖片來源：資料來源：Arbor，iThome整理製圖

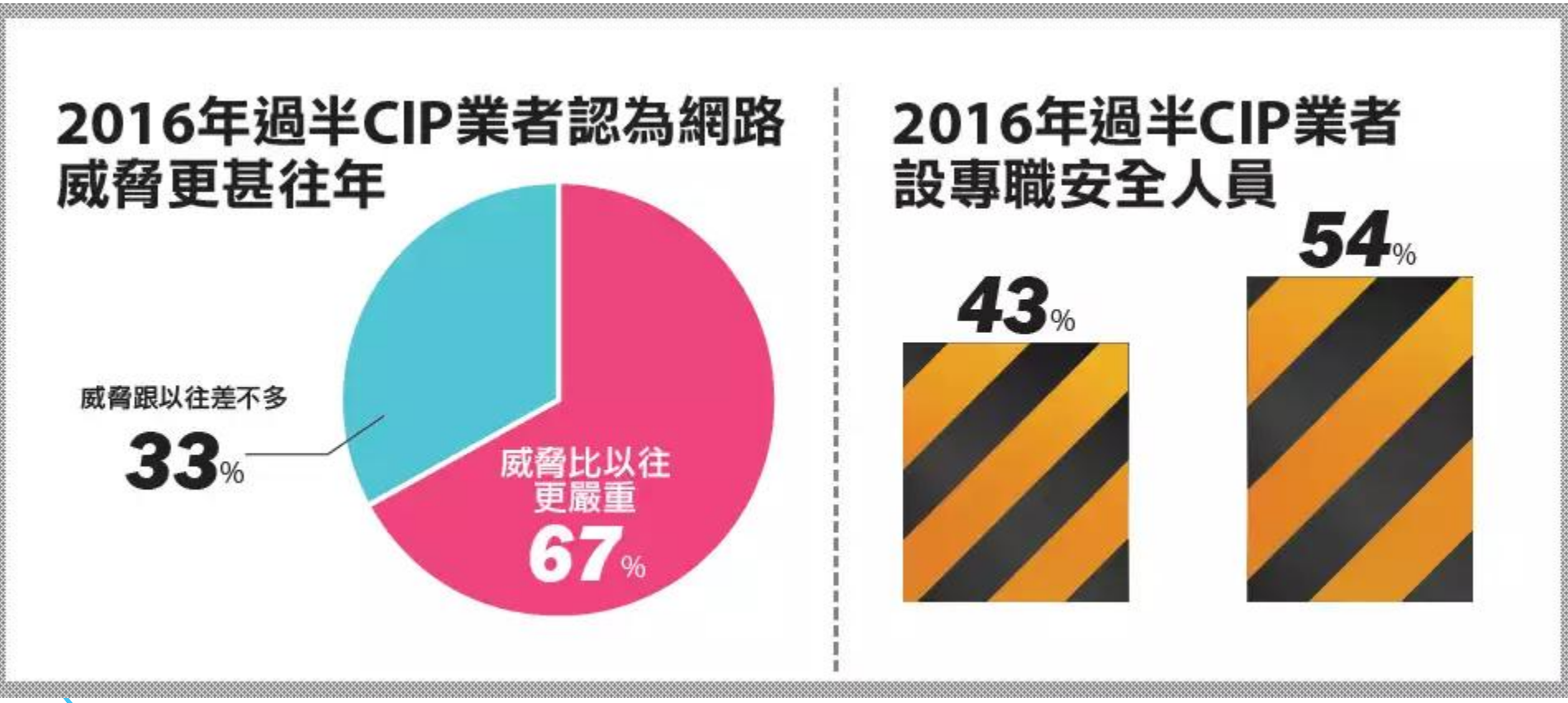
Mirai揭露後殭屍裝置數量增倍

- Level 3威脅研究中心發現在駭客公佈Mirai後，受到控制的裝置數量也從21.3萬台增加到49.3萬台，其中8成為監視器，其他為路由器、IP攝影機或Linux伺服器組成



2017四大資安趨勢之四

- **連網威脅驟升，關鍵基礎設施拉警報**



圖片來源:iThome

大停電證實是遭駭客入侵

- 世界首例，烏克蘭大停電證實遭駭客入侵
  - 2015 年 12 月 23 日，烏克蘭電力網路受到駭客攻擊，導致伊萬諾-弗蘭科夫斯克州數十萬戶大停電

初探物聯網

四分之一世紀前

25後，人類將透過全球網路，彼此交流音訊、視訊和文字，到時候，只要用一支手機，就能取得世界上所有資訊

網際網路

四分之一世紀後

從現在起，25年後物聯網革命將會把每台機械、每家企業、每個居民和每輛汽車，全都連結到一個由通訊網路、能源網路和物流網路組成的智慧網路

物聯網脈絡


比爾蓋茲在《未來之路》書中提及，成為物聯網概念的濫觴
在RFID技術上，Auto-ID公司提出了物聯網的概念
1995
1996
1999
2005
美國麻省理工學院提出物聯網
國際電信聯盟發布《ITU網際網路報告2005：物聯網》指出「物聯網」時代的來臨

IoT新興市場現況

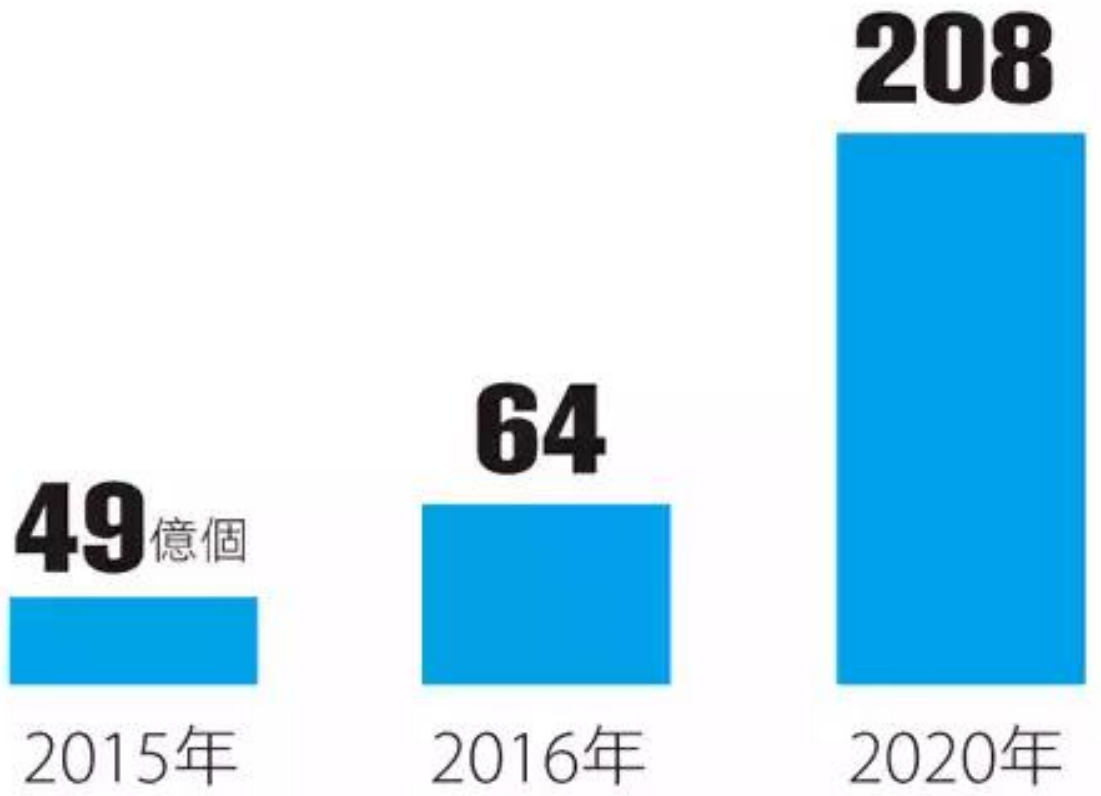
- IoT新興市場中，主要有3個IoT應用領域成長最快：
  - 消費性IoT（如頭戴式裝置、智慧家庭）
  - 工業IoT（安全監控攝影機、LED照明）
  - 醫療方面的IoT應用
- 整體來看，目前臺灣IoT市場主要仍以智慧家庭、車聯網和穿戴式裝置的市場為主。

傳輸技術大躍進，2017市場挑戰破兆

- 根據市調機構IDC預測，接下來3年，全球IoT市場將進入成長爆發期。

資料來源： iThome　(1 ZB等同於10的9次方個TB)

2020年全球IoT裝置數量將達208億

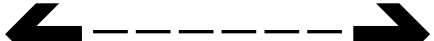


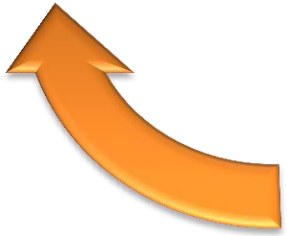
資料來源:Gartner，iThome整理，2016年6月

物聯網的未來世界

物聯網之應用與發展

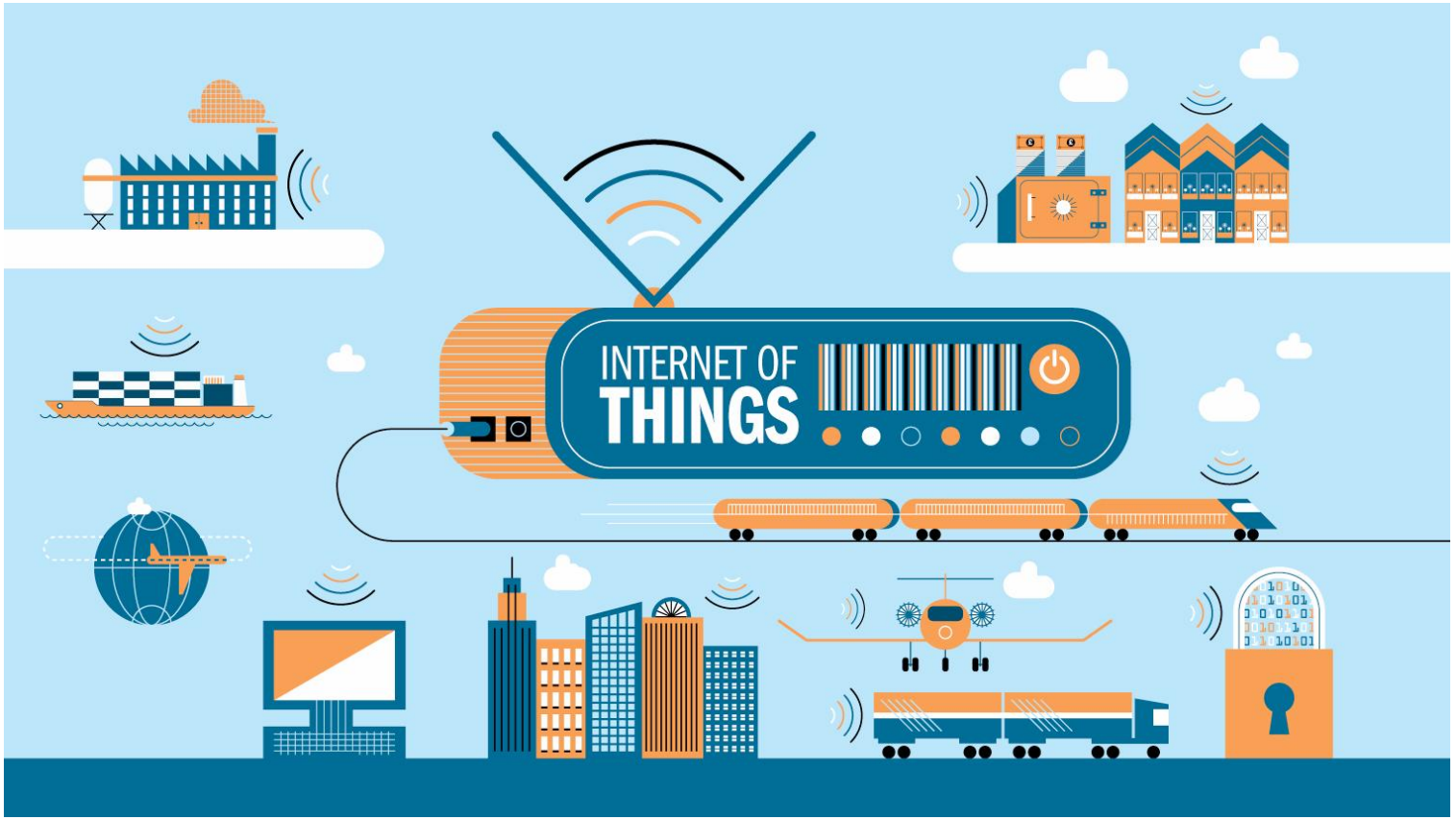
網際網路 & 物聯網

- 網際網路  人聯網



物聯網 & 網際網路

- 物聯網
  - 非建立起人與人的網路，而是物與物的網路



何物連上物聯網

- 只要「物」夠大，可裝網路傳輸器，且又有自己專用的可識別位址
  - 家用電子設備
  - 家電
  - 汽車
  - 醫療設備
  - 各種飛行器
  - 從家到國家任何可以監控的東西

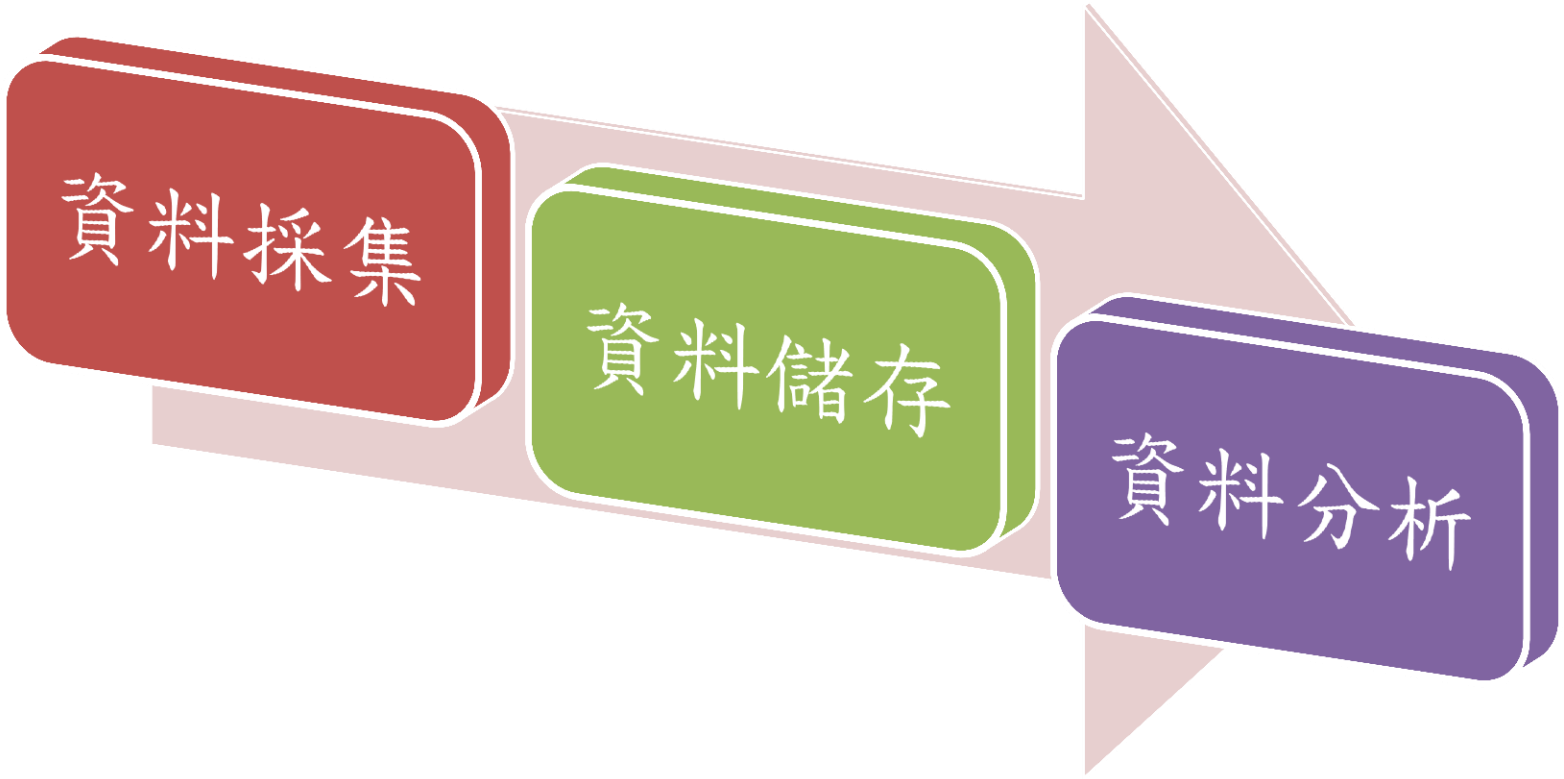
智慧化設備

- 透過連上物聯網的設備，通稱智慧化設備(如智慧電視、智慧電冰箱等)
- 其實設備本身不需要智慧化，但藉由與其他連線設備的互相合作，產生智慧化的應用。

巨量資料(Big Data)

- 籍由連線設備的零散的資料蒐整，並透過運算分析，獲得有用的結論，正是巨量資料的概念，未來這將有機會創造出更有效及更節省人力的生活方式。

巨量資料(Big Data)



物聯網發展

物聯網架構

應用層

- 個人、家庭、企業、國家及各類產業

網路層

- 2G、3G、4G無線網路、WiFi、Bluetooth、xDSL、CABLE網路等服務，各類網路平台、管理軟體、系統設備、整合系統、各式終端設備

感知層

- 各種產品感應技術(RFID、生物辨識器、條碼等)

物聯網架構


技術創新
智慧照明
智慧電網
追蹤命令與控制
智慧汽車
建築物自動化
行人導航
智慧家庭
更多其他服務
M2M
智慧農業
資產追踪
智慧停車
空氣品質控制
汽車安全
智慧標籤
智慧能源
供應鏈自動化
智慧健康
應用
微型化、flash技術革新、新一代強大且低功耗的MCU，以及雲端服務等。
軟體
技術
Sensing
Accelerometer
Magnetometer
Gyroscope
Pressure
Altimeter
Temperature etc.
Processing
MCU
MPU
Hybrid MCU/MPU
Network Processor
Connectivity
NFC
6LoPAN
Sub-Gig
ZigBee®
GPS
BT/BTLE
Wi-Fi®
RFID
Cellular

物聯網應用架構

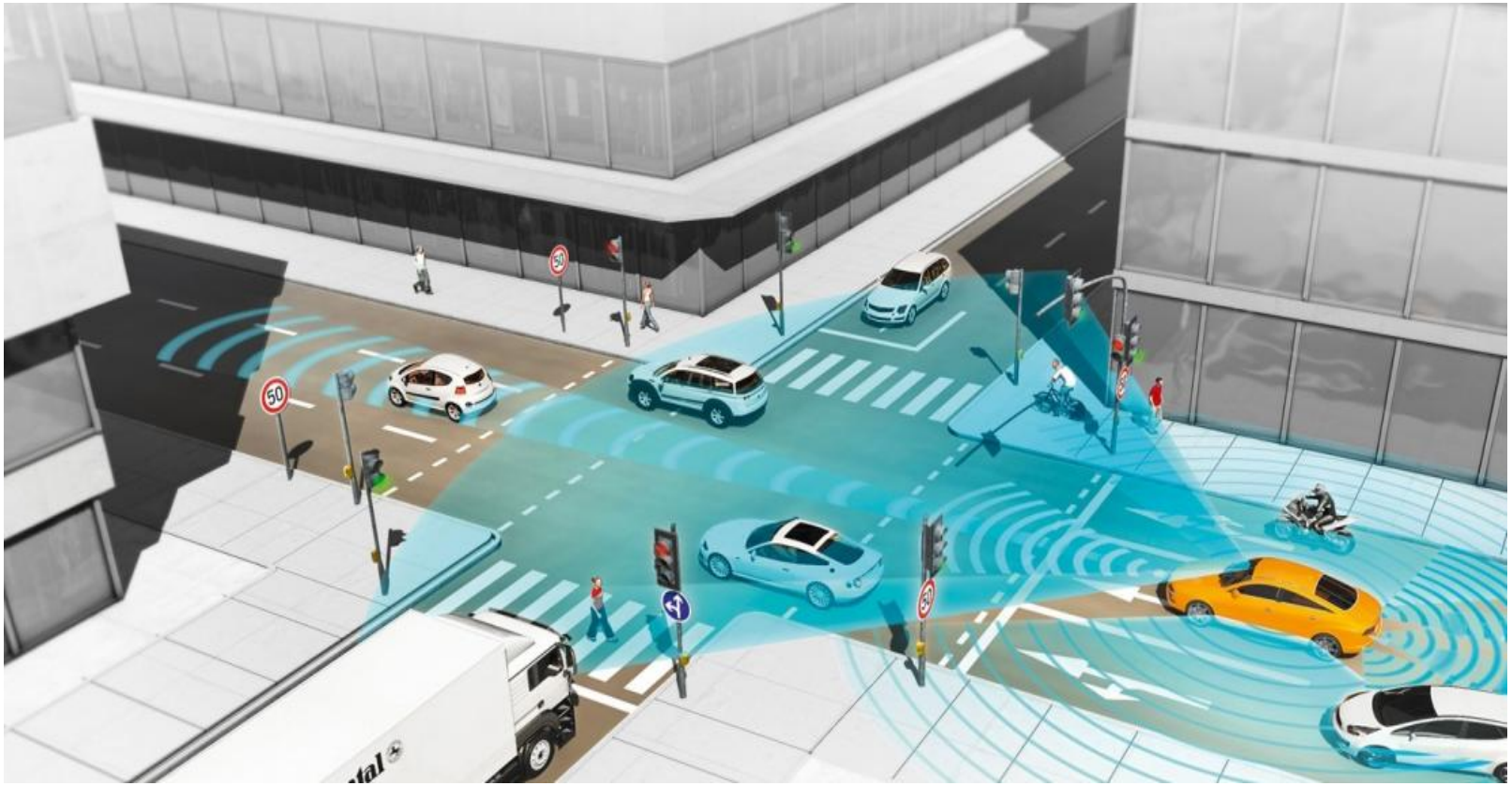
<資料來源：《數位時代》第247期>

物聯網的應用範疇

<資料來源：《數位時代》第247期>

物聯網應用

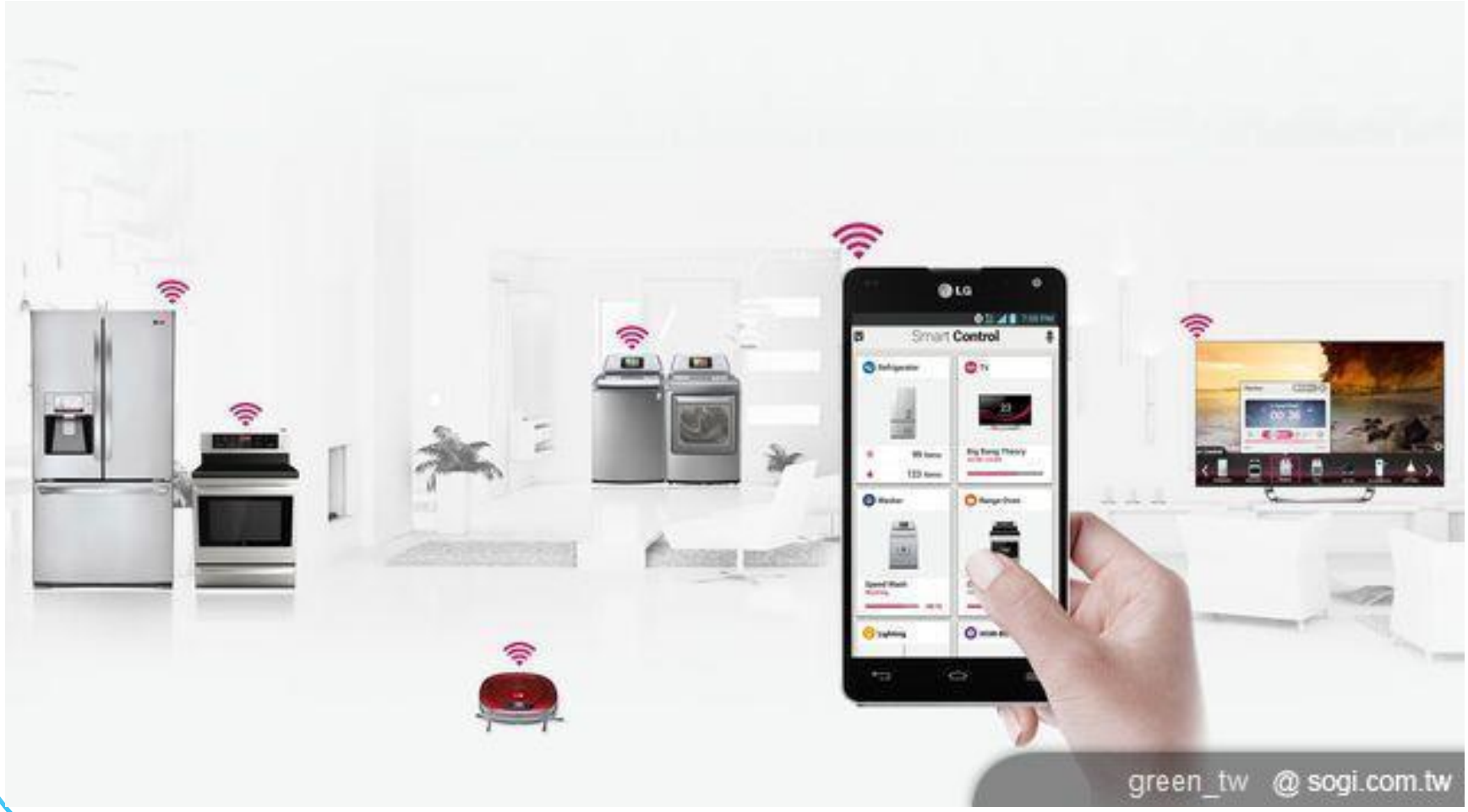
- 物聯網應用 – 汽車業、運輸業、零售業



物聯網應用

- 物聯網應用 – 銀行業、能源與公共事業、保險業

智慧家電



智慧住宅

智慧購物

創新、整合的智慧聯網商區

商業決策即時回饋（個人化服務、即時行銷方案、新商品採購決策...）

商區服務

- 智慧辨識行銷
- 自助購物商店
- ID辨識
- 消費者
- 二維條碼
- LBS服務
- NFC
- 跨店集點
- 互動購物櫥窗
- 社群行銷
- 手機付款

商區資訊蒐集

商區／商家戰情中心(Dashboarding)

商店銷售紀錄
消費行為資訊

- 通地資訊
- 交易紀錄
- 商品資料
- 顧客資料

商業分析及決策

- 消費族群分析
- 消費行為預測
- 商品銷售趨勢分析
- 商品行銷決策建議
- 最適化優惠折扣
- ……

商鏈整合

- 供銷需求預測
- 物流追蹤與控管
- 共通金流服務

感知層
網路層
應用層

商鏈資訊交換

支援服務

- 聯合行銷平台
- 小額付款金流清算
- 跨業集點平台
- 商品供應物流配銷
- ……

資料來源：經濟部商業司智慧聯網產業發展策略會議報告書

智慧購物

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研

果粉久等了，Apple Pay今早上線

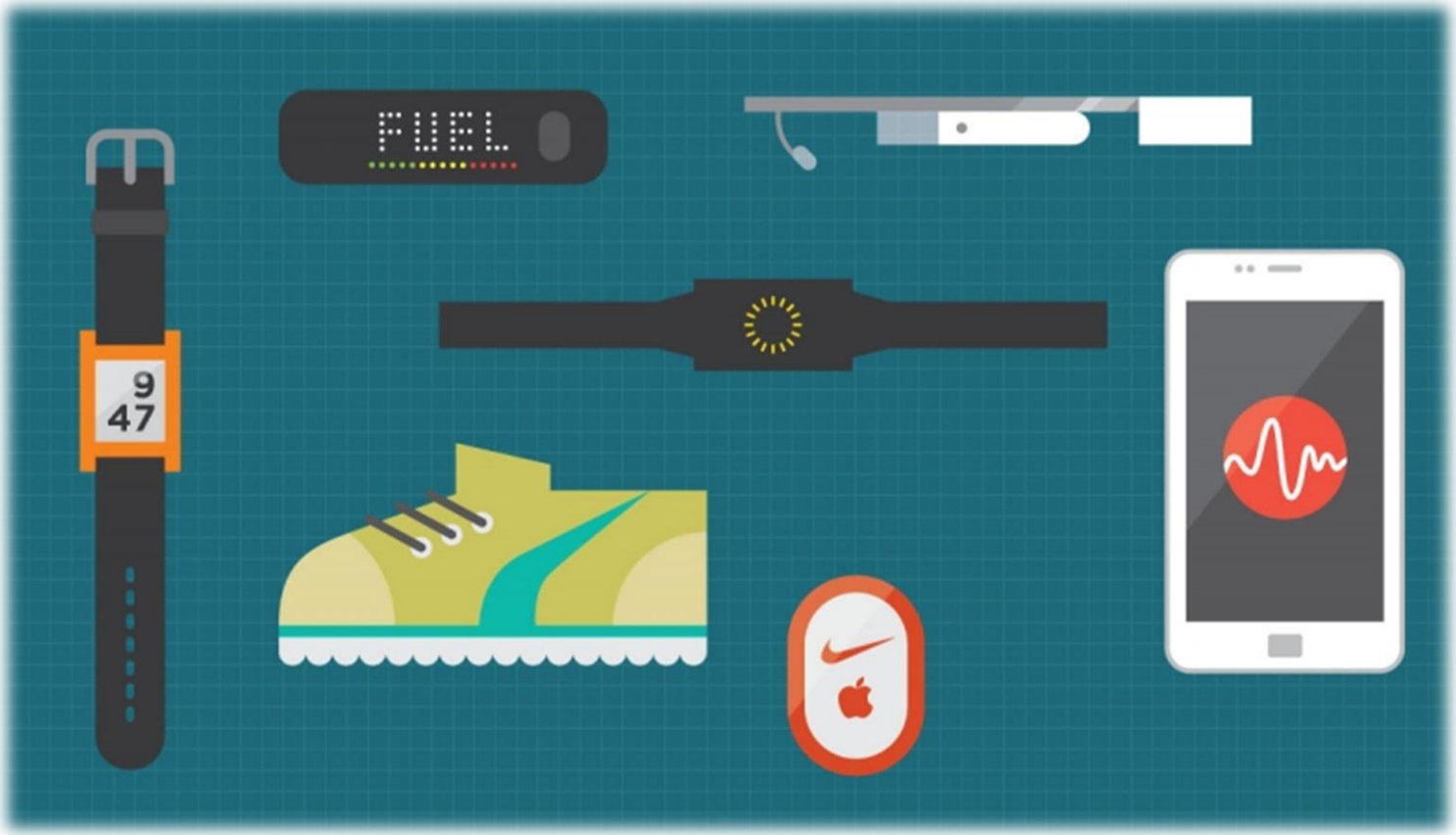
Apple Pay上線後，國內蘋果用戶可以iPhone、Apple Watch、iPad或是Mac使用Apple Pay付款，可消費的實體通路包含百貨公司、連鎖量販業者、便利商店等。

文/ 蘇文彬 | 2017-03-29 發表

讚 3.9 萬 按讚加入iThome粉絲團 讚 分享 273 G+1 1

智慧穿戴式裝置

各種穿戴式科技產品，幫助你隨時監視身體狀況



智慧汽車-連線奔馳

- IOT於汽車產業和無數駕駛帶來許多希望。現今所謂連線汽車，可以透過網際網路播放串流音樂、取得路況與天氣，甚至用全球定位系統(GPS)定位及導航。然而，要是有智慧汽車能監視路況、必要時自動導航。
- 最終極的智慧汽車，可以自動駕駛，你什麼都不用作，只要打開車門坐上去，就可以從這裡到那裡。

車聯網安全

- 駭客入侵儀表板！ 方向盤失控、煞車癱瘓

智慧城市

IOT可以串起整座城市，連線設備有助於減少道路壅塞、警告消防隊有緊急狀況，甚至告知道路需要維修，或需要加派警力巡邏

智慧醫療

IOT勢必會改變我們所認識的醫療。把現在所用(或即將採用)的各種醫療設備互相連線，醫療就立刻變得更智慧化。診斷更迅速、更準確，誤診減少，病患可以獲得更好的照顧與預防照護。這是個即將成真的醫療美夢。

物聯網醫療安全

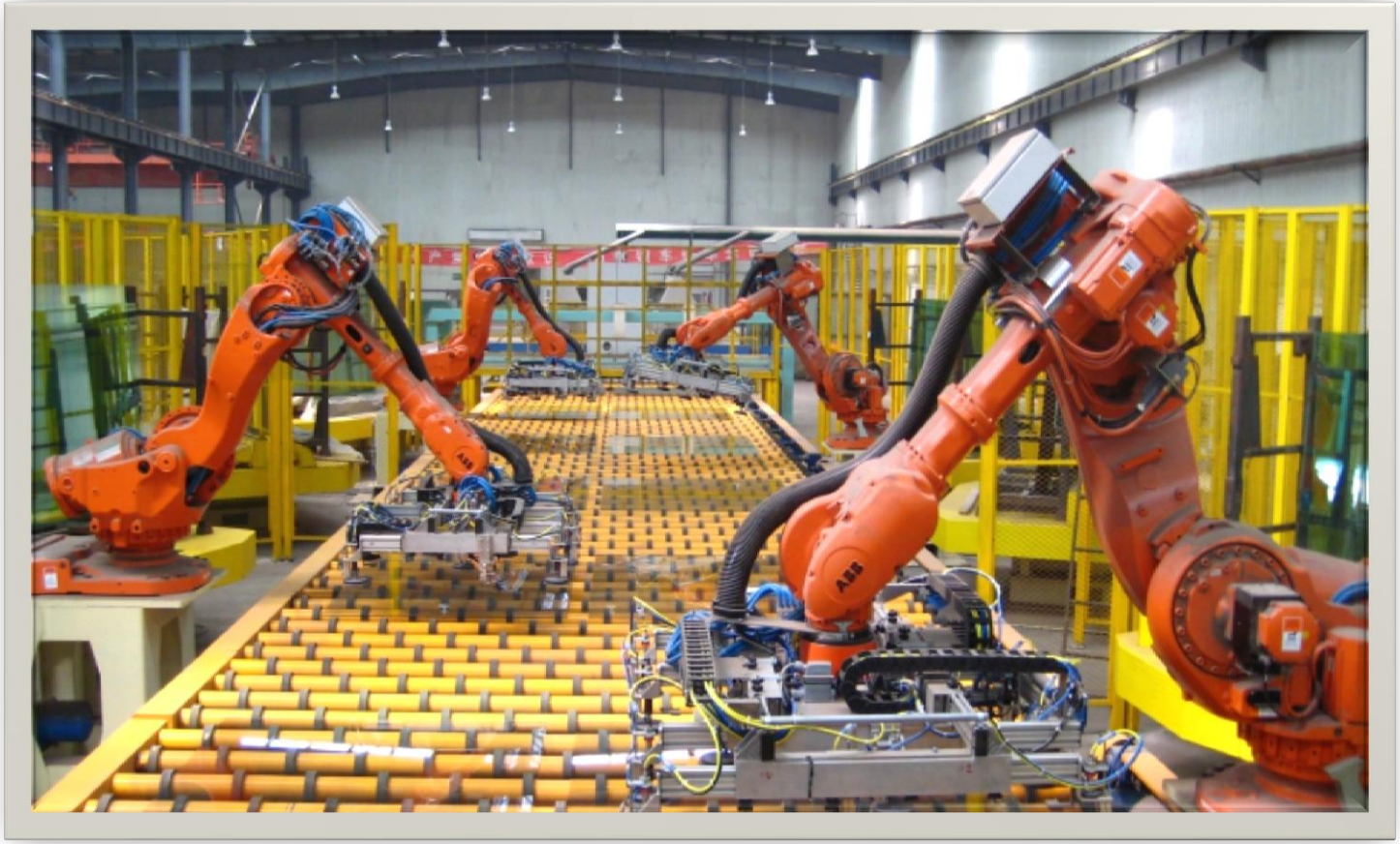
醫院聯網裝置越來越多，但資安問題未引起重視

作者 麥芯兒 | 發布日期 2017 年 03 月 07 日 7:07 | 分類 網路, 資訊安全, 醫療科技 Follow G+1 讚 分享 59

由於物聯網裝置缺乏安全措施，很容易成為駭客的攻擊目標，而聯網的醫療設備更是風險巨大。一方面，醫療設備常關係到病人的人身安全，另一方面，由於醫療設備連線到醫院網路，駭客能夠盜取私密的醫療資訊。

智慧企業

IOT可以改善辦公室、工廠與門市的效率，大幅改善企業效率，使未來需要的員工人數減少。



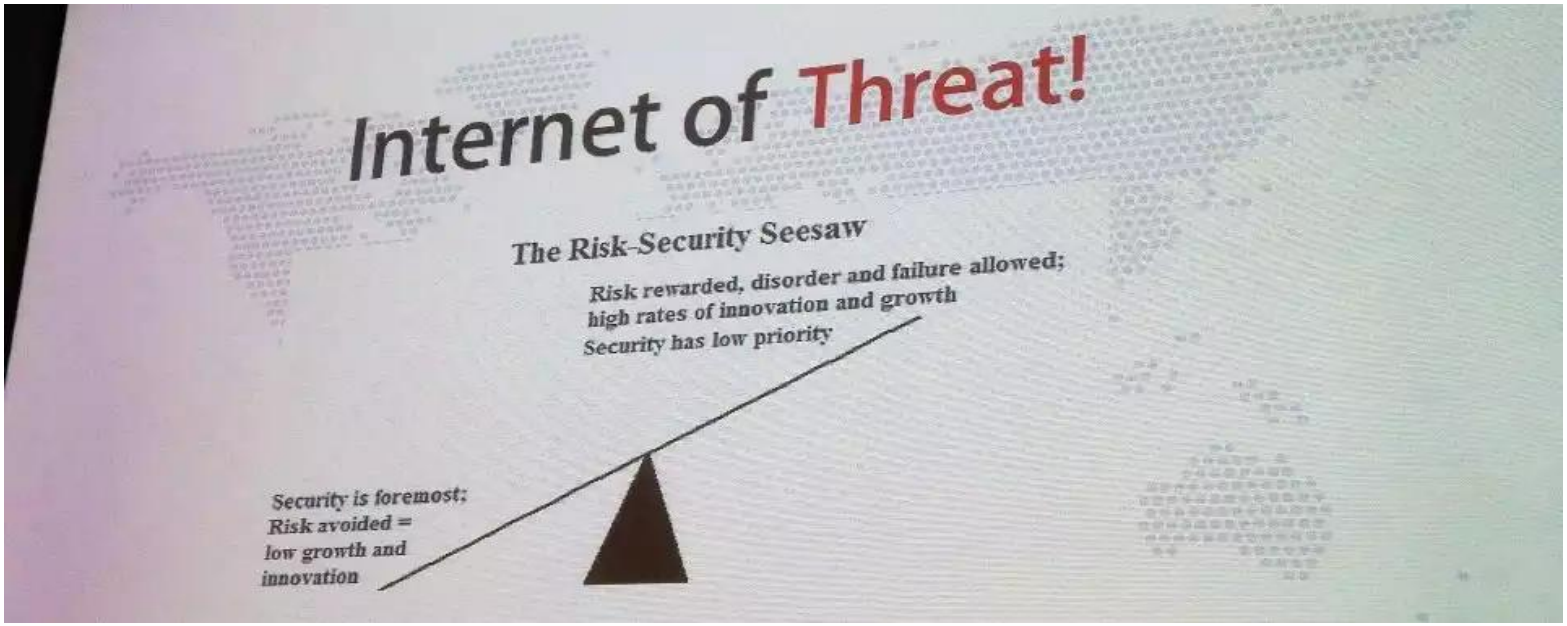
智慧世界

現今的網際網路，幾乎沒有國界，物聯網也是如此

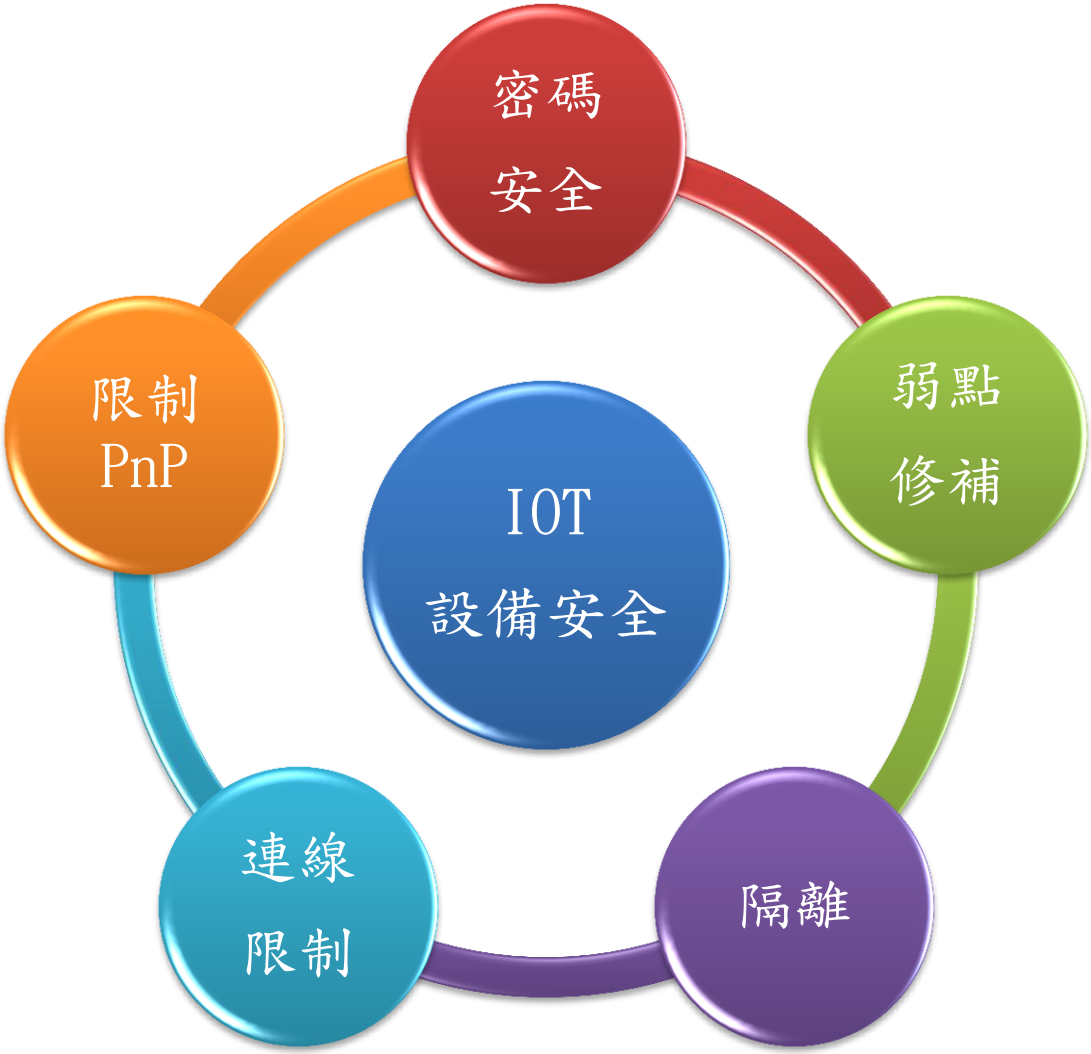
物聯網之資訊安全隱憂

無所不在的物聯網設備

- 目前物聯網裝置的應用會越來越普遍，但與其有關的資安事件頻傳，因此無論是製作的廠商，還是企業乃至於個人，都應該提高警覺，重視這些設備的安全性



物聯網設備的安全



隱私問題

- 關心你的那些事?
- 誰正在偷窺你
- 隱私與物聯網

隱私問題

- 物聯網最大的問題，可能是隱私。
- 這麼多感應器與智慧設備，會收集關於你的大量訊息。
- 大量的監視攝影機及智慧手機裡頭的全球定位系統(GPS)晶片，追蹤你的行動。

科技來好處 同時你也要付出代價

- 你希望線上零售商的網站記住你的喜好、上次買什麼，免得每次上網站都得重新輸入這些資訊;付出的代價就是網站曾在你的裝置上安裝餅乾(cookie)，追蹤你在網站上的行為，還會記錄你從哪裡上網、買東西後會去哪裡。
- 保全攝影機可以幫你避開小偷、強暴犯和恐怖份子;付出的代就是你和那些壞蛋一起被監視。

穿戴式裝置個人資料外洩

網路監視器被駭　女子入浴成實境秀

小心駭客控制你的生活用品

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群

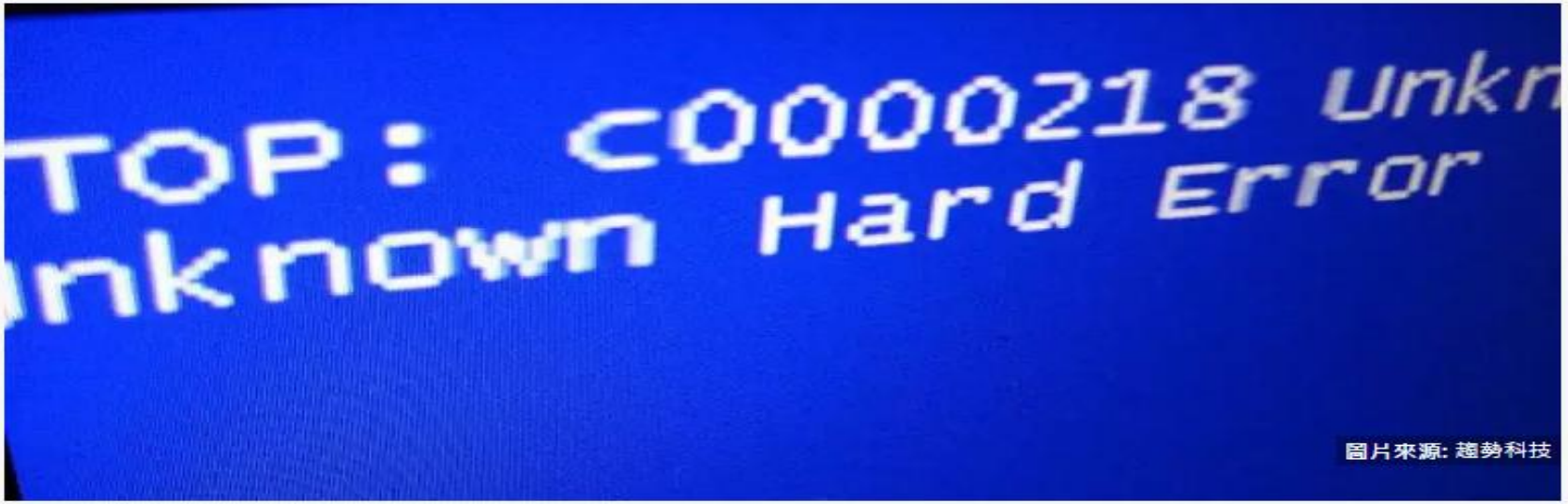
新聞

物聯網時代：小心！駭客可能悄悄控制你的情趣用品

趨勢科技在漢諾威CeBIT展示如何透過幾行程式碼，就能夠遠端啟動一隻電動按摩棒，藉此突顯出物聯網時代下，即使性玩具也可能成為駭客攻擊的目標。

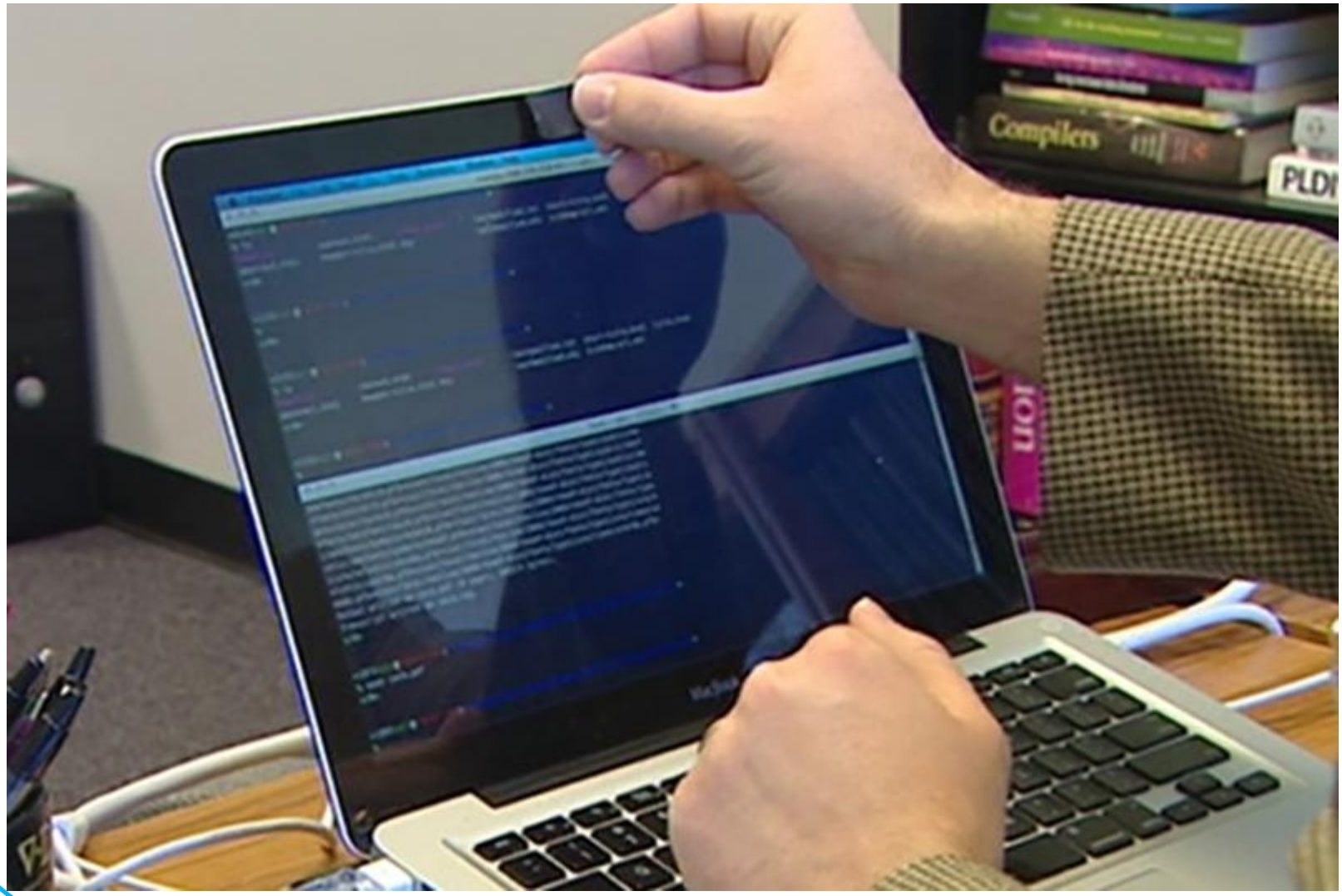
文/ 陳文義 | 2016-03-16 發表

讚 3.9萬 按讚加入iThome粉絲團 分享 41 G+1 10



資安業者早已大聲疾呼物聯網(IoT)可能擴大各種資安問題，但卻未受到重視，趨勢科技選擇直接挑戰大眾的底線：展示如何從遠端啟動情趣用品，藉此喚起外界對物聯網資安議題的重視。

想避免被駭客監視？FBI 建議!!



個人資料保護法

- 個人資料保護法(以下簡稱本法)第1條
  - 為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之**合理利用**，特制定本法。

個人資料保護法架構

第一章
總則(§ 1~14)

第二章
公務機關對個人資料之蒐集、處理、利用(§ 15~18)

第三章
非公務機關對個人資料之蒐集、處理、利用(§ 19~27)

第四章
損害賠償及團體訴訟(§ 28~40)

第五章
罰則(§ 41~50)

第六章
附則(§ 51~56)

不當蒐集處理利用個人資料

－個人資料類別

姓名
出生年月日
國民身分證
統一編號
護照號碼
特徵
指紋
婚姻
家庭
教育
職業
聯絡方式
財務情況
社會活動

病歷
醫療
基因
性生活
健康檢查
犯罪前科

得以直接或間接方式
識別該個人之資料

個資生命週期

- **蒐集**：指以任何方式取得個人資料。
- **處理**：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
- **利用**：指將蒐集之個人資料為處理以外之使用。
- **國際傳輸**：指將個人資料作跨國（境）之處理或利用。

個資新聞分享

- 郭姓會計師前年退出大型賣場特力屋會員，並要求刪除個人資料，特力屋回信允諾，但郭男後續半年內仍收到特力屋電子廣告信共五十二封，不堪其擾，怒告特力屋 違反《個人資料保護法》求償十萬元。士林地院日前判決特力屋須賠償郭男兩萬六千元。

隱私及資安問題

- 物聯網連接的設備經常監視和跟蹤消費者的行為，以此來調整和改善消費者體驗；然而用戶可能根本沒有被告知哪些數據將會被收集，又如何被使用。
- 裝置上所蒐集的資料誰可以擁有，不同組織或商業團體間互相交換這些資料是否合法等議題，目前皆未有明確法令的規範。

安全問題

- 資料在物聯網上的安全
- 物聯網本身的安全

資通安全管理法(草案)

❖ 本法以資通安全管理為核心，分為5個章節，計23條

資通安全管理法草案

第1章 總則(§1~§8)	立法目的、名詞定義、資通安全產業之推動、行政院職責、幕僚任務委任或委託、資安責任等級分級、情資分享機制、資通委外監督
第2章 公務機關資通安全管理(§9~§14)	資通安全管理與維護計畫、資通安全長之設置年度資通安全報告之提出、資通安全查核、通報應變措施、獎懲措施
第3章 非公務機關資通安全管理(§15~§18)	關鍵基礎設施提供者、資安責任等級分級納管之非公務機關資通安全維護之管理與監督、資通安全事件通報應變、行政檢查
第4章 罰則(§19~§21)	行政處分
第5章 附則(§22~§23)	施行細則授權、施行日期

資料來源：行政院資通安全處

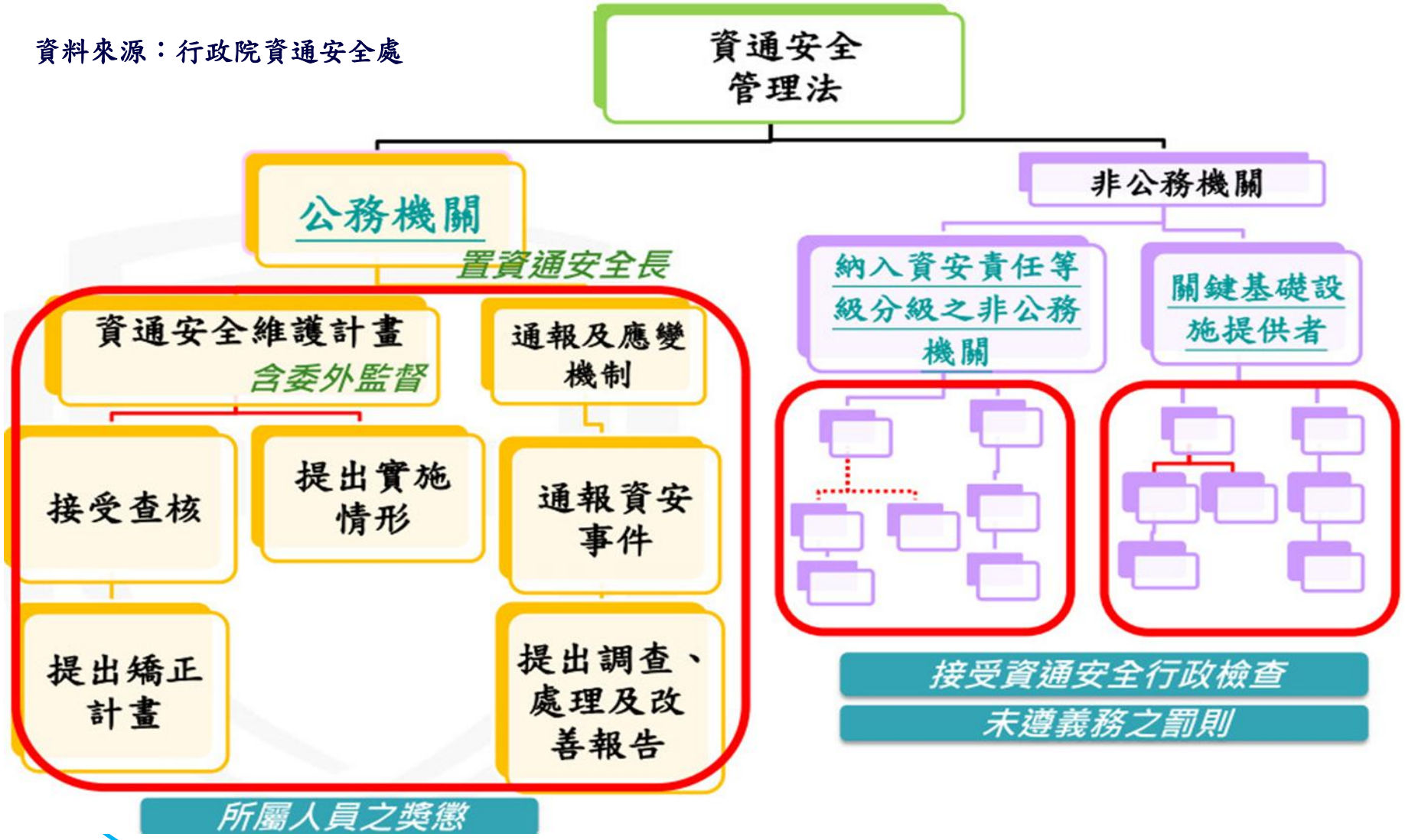
何謂關鍵基礎設施?(續)

資通安全管理法草案第十五條

- 關鍵基礎設施：指能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方機關、高科技園區等實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國民生活、經濟活動、公眾安全或國家安全有重大影響之虞。

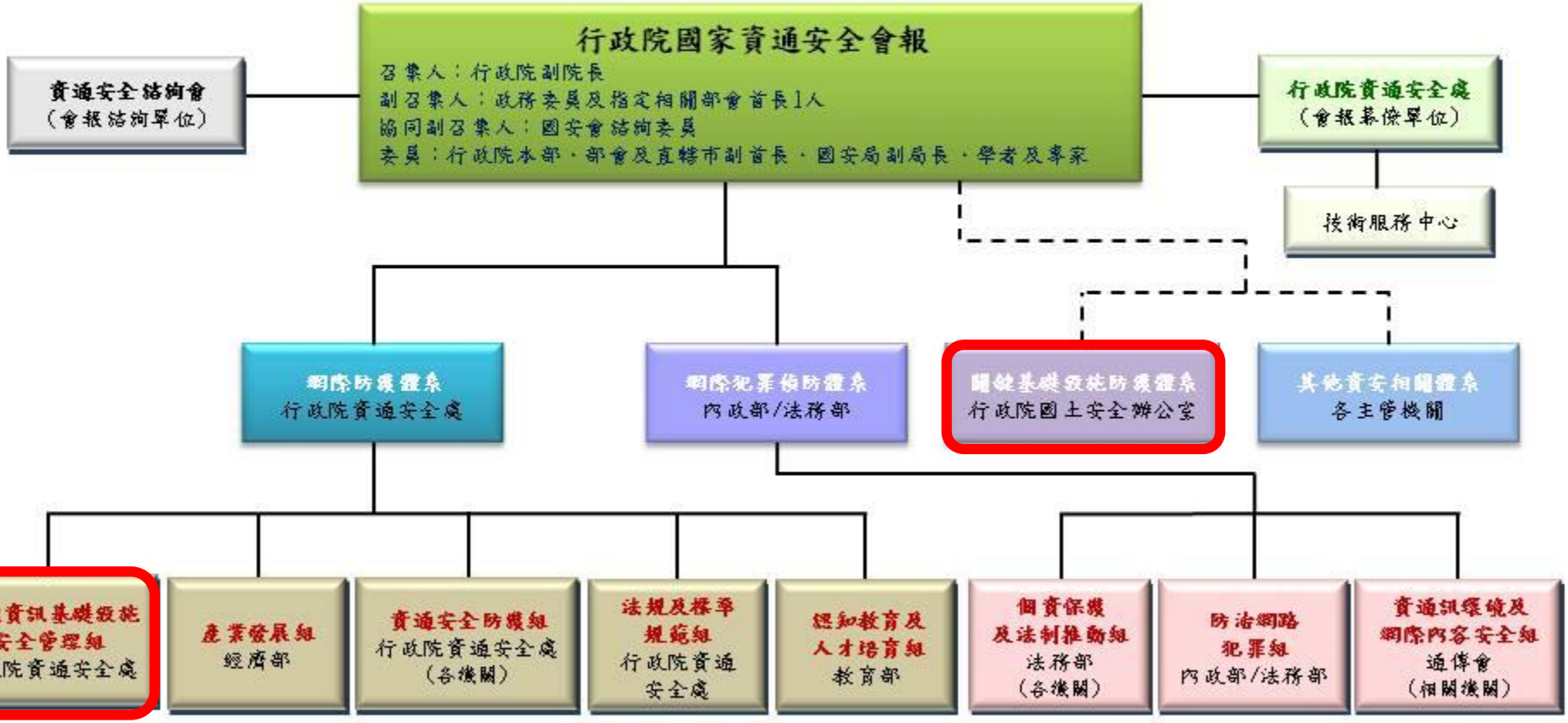
資通安全管理法(草案)

資料來源：行政院資通安全處



行政院國家資通安全會報組織架構圖

105年8月1日生效



2017年政府資安預算編列歷年最高

- 在「資安即國安」的政策方針下，透過擬定與推動8大資安旗艦計畫為國家整體資安防護奠定基礎，最重要的任務就是關鍵基礎設施的主管機關，都必須建置產業相關的ISAC（資安資訊分享與分析中心）
- 目前所有資安旗艦計畫的基本就是，與關鍵基礎設施有關的主管機關，都必須自建產業相關的ISAC（資安資訊分享與分析中心）、SOC（資安監控中心）和CERT（Computer emergency response teams，電腦緊急應變中心）等三個資安關鍵基礎平臺。

2017年政府8大資安旗艦計畫

2017年政府8大資安旗艦計畫

部會	計畫名	計畫重點
經濟部	國防資安產業推動暨關鍵設施(水資源、民營能源)資安強化旗艦計畫	1. 建立水資源、能源領域ISAC。 2. 培育、輔導國內資安產業發展與高階資安專業人才養成。
科技部	資安前瞻創新研發計畫	1. 建立科學園區領域ISAC。 2. 補助大專院校投入先進資安技術研究與專業人才培育。
衛福部	關鍵基礎設施資安資訊分享與分析中心建置計畫	建立衛生關鍵基礎設施領域ISAC。
內政部	預防暨打擊科技犯罪精進刑事科技能量計畫	針對科技犯罪提升資安鑑識能量。

2017年政府8大資安旗艦計畫

教育部	臺灣學術網路資安磐石計畫	建立臺灣學術網路資安訊息分析系統及建置防火牆聯合防禦架構系統，提升網路資訊安全。
交通部	關鍵基礎設施資安資訊分享與分析中心建置計畫	建立交通關鍵基礎設施領域ISAC。
通傳會	數位匯流/IoT資安威脅防禦機制暨資安實驗室建置與服務	國家基礎通訊網路防禦與IoT之資訊安全整體研究。
院資安處	國家資安防護前導計畫	研訂數位時代資安政策、法規及標準、發展國家資安風險評估機制、開展多層次與多邊國際合作關係、推廣資安認知方面訂定工作計畫。

資料來源：行政院資安處，2017年1月

物聯網安全威脅

連網裝置複雜管理困難

- 物聯網裝置連上網路，通訊連接設備須具互通性，導致侵入裝置或滲透網路變得越來越容易，駭客攻擊將更加頻繁

傳輸未加密

- 80%進行資料傳輸時未加密
- 60%進行軟體更新時未加密

物聯網架構安全威脅

應用層

- 連結的物品多且複雜
- 隱私機密遭竊取、惡意中斷網路連線

網路層

- 無線通訊安全
- 訊號在空氣中傳輸易遭受外部截取

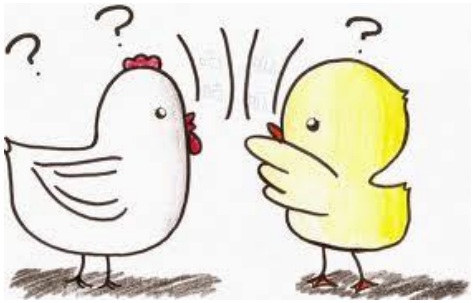
感知層

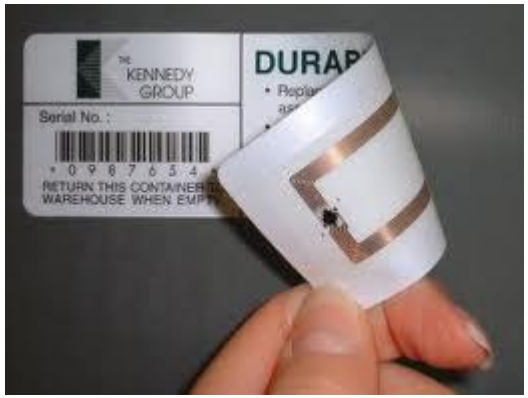
- 設備無人監控
- 機器容易被破壞盜取或冒名使用

物聯網架構安全威脅

感知層

- RFID標籤：硬體結構簡單、缺少加密性
- 容易被偽造，訊息容易被推算
- 傳輸及安全標準的不相同





物聯網安全威脅

網路層

- 存儲空間，計算能力及通信能力有限
- 資料加密、安全認證及管理，入侵檢測技術不足
- 無線傳感器網路(如IEEE 802.11、802.15等技術)，大功率無線設備可直接干擾其訊號

應用層

- 統一身份認證、統一金鑰管理及安全營運平台不足
- 整體系統和資料的故障修復

無線路由器資安問題

- IoT發展浪潮下，無線路由器安全更顯重要

物聯網安全攻擊威脅

監聽攻擊

- 竊聽任何透過網路傳送的未加密資訊

阻斷服務攻擊

- 攻擊來封鎖或阻慢對某些網路或設備的使用

金鑰淪陷攻擊與基於密碼的攻擊

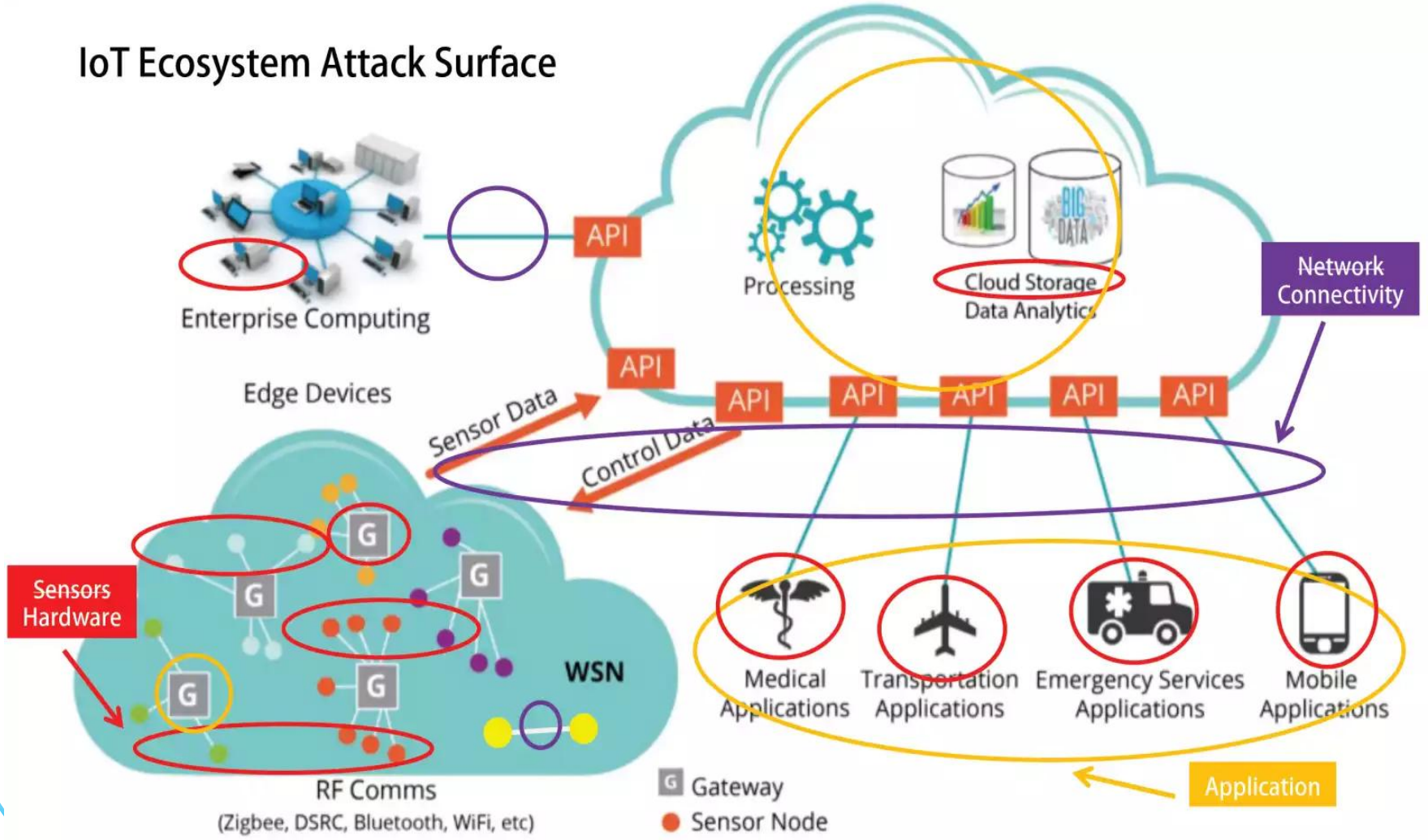
- 加密通訊的金鑰被竊或入侵網路或連到特定網路的設備

中間人攻擊

- 第三者會竊走雙方或設備間傳輸的資料

物聯網的安全隱憂

物聯網安全是一整個生態圈的事情



資料來源：iThome

物聯網安全是全民都要面對的問題

製造商

- 開始設計時，必須將資安納入考量，並且開發者需要有安全開發經驗、訓練，最好產品在上市前滲透測試

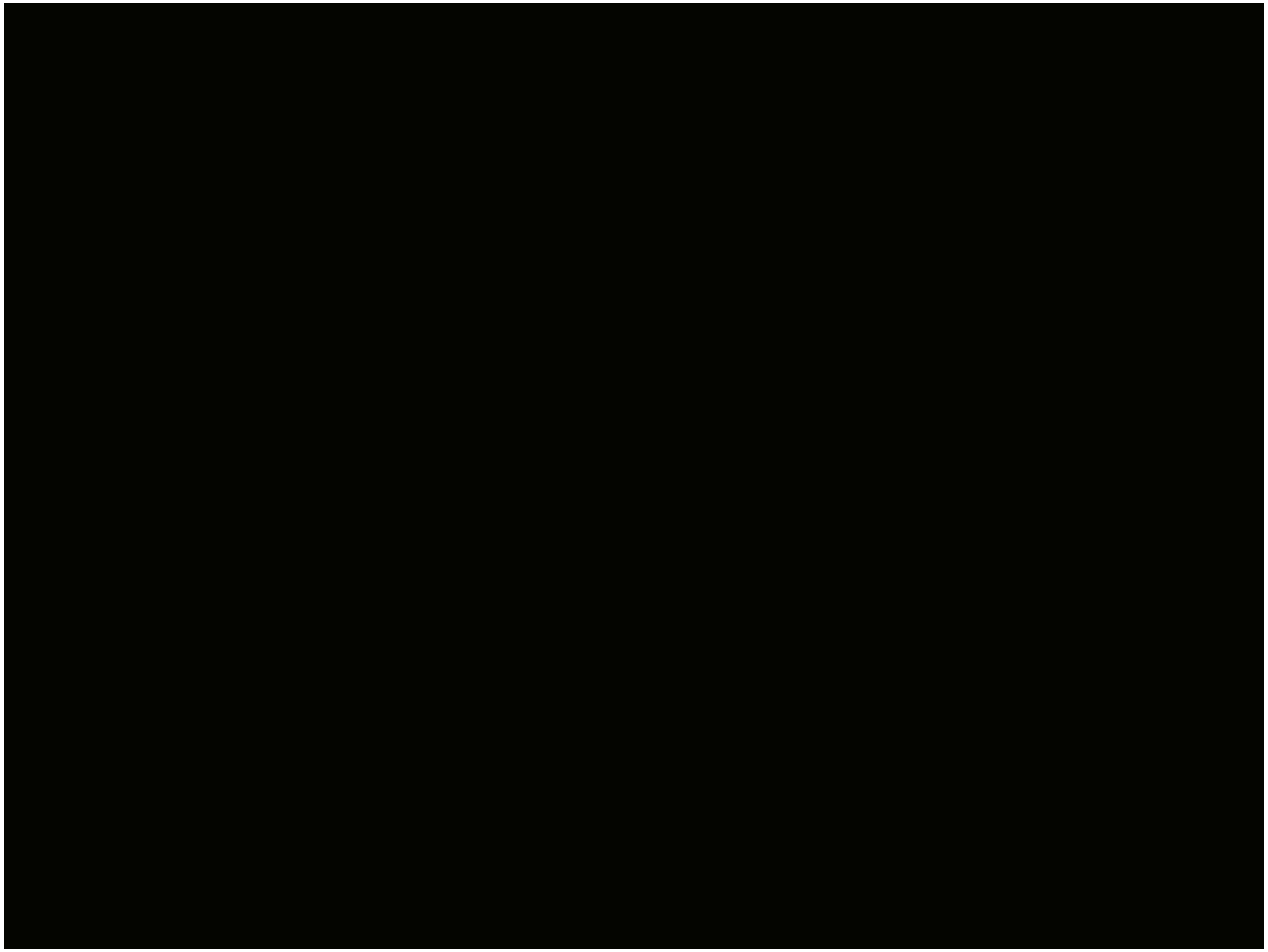
企業用戶

- 需將物聯網設備盤點並列管，若是無法修補的設備，應考慮隔絕於主要網路之外
- 防護措施需將整個網路架構納入資安考量，並在採購時，要求廠商確保設備安全性

終端使用者

- **了解使用裝置的風險，如果不確定設備的功能，最好就不要使用**
- **使用時，要將預設密碼更換成高度複雜的密碼**

蝴蝶效應



總結

- 資訊安全與個資防護應是一種習慣與文化，而不能只是一種技術與專業。

Thank You

感謝聆聽