論述 》專論 · 評述

物聯網（IoT）之發展與信任挑戰

物聯網是新的網路科技潮流及趨勢，許多實體設備可無縫地整合至資訊網路，提供使用者更智慧且多元之服務，創造讓很多生活物品可藉由網路彼此相連結並整合的世界。然而，一個融入生活的物聯網服務與應用，必須提供完善的信任管理，以提供可靠且安全的服務，提高使用者接受度與使用率。本文探討物聯網之應用、挑戰及信任管理。

許建隆、林子煒（長庚大學資訊管理學系教授兼系主任、中央研究院資訊服務處資訊人員）

壹、前言

在科技及產業發展與推廣的帶動下，物聯網已成爲新的網路科技潮流及趨勢。物聯網會成爲科技熱門話題，最大的原因爲它創造了讓很多生活物品可以藉由網路彼此相連並整合的世界，這將帶給使用者更爲智慧化的服務。然而，這些新興科技所帶來的創新應用與服務，除了讓使用者體驗智慧化服務，也可能帶給使用者沒有意識到的新風險。趨勢科技資深協理張裕敏曾表示，越受歡迎、越多人愛用的各種新興科技應用，就是駭客努力鑽研的新領域；換言之，物聯網將可能暴發許多潛在的資安風險。現今的資訊社會氛圍下，一旦有了網路服務，即面臨到使用者的信任議題。網路犯罪層出不窮的現代，民眾對於個人資料隱私及資訊安全的意識逐漸提高，如何提供值得讓使用者信賴的服務是日趨重要的議題。本文將簡單介紹物聯網的起源與現況，並探討物聯網的信任管理。

貳、物聯網之發展

就像雲端運算議題發展的起源，物聯網其實不是新興的科技，而是被討論許久的技術，唯因近期科技的腳步終於發展至可以實現的階段，因此相關的討論及應用如雨後春筍般冒出。

一、物聯網之定義

物聯網的定義非常廣泛，目前並無較精確的定義。1995

年，時任微軟公司首席執行官的比爾蓋茲在他的著作《未來之路（The Road Ahead）》提及物聯網概念，但當時受限於無線網絡、硬體及感測設備的發展尚未到位，因此並未受到世人的重視；1999 年，美國麻省理工學院 AUTO-ID 中心的艾許頓（Kevin Ashton）教授研究無線射頻識別（Radio Frequency Identification, RFID） 時 提 出「Internet of Things（IoT）」，將 RFID 技術予以擴充而具有物聯網的觀念；2005 年，國際電信聯盟（International Telecommunication Union, ITU）在 2005 年世界資訊社會峰會（World Summit on the Information Society, WSIS）提出報告「The Internet of Things」，正式提出物聯網時代將要來臨。

2008 年，美國總統歐巴馬提出「物聯網振興經濟戰略」，確立物聯網的國家戰略高度，並推動感測技術與智慧型基礎設施的建置；歐盟於 2009 年推動以 RFID 技術，以及資安技術所建構的歐盟物聯網行動計畫；同年 9 月，北京舉辦的「物聯網與企業環境中歐研討會」上，歐盟委員會信息和社會媒體司 RFID 部門負責人 Lorent Ferderix 博士給了歐盟對物聯網的定義：「物聯網是動態的全球網路基礎設施，它具有基於標準和互操作通信協議的自組之能力，其中物理和虛擬的『物』具有身分標識、物理屬性、虛擬特性和智慧介面，並與訊息網絡無縫整合。」

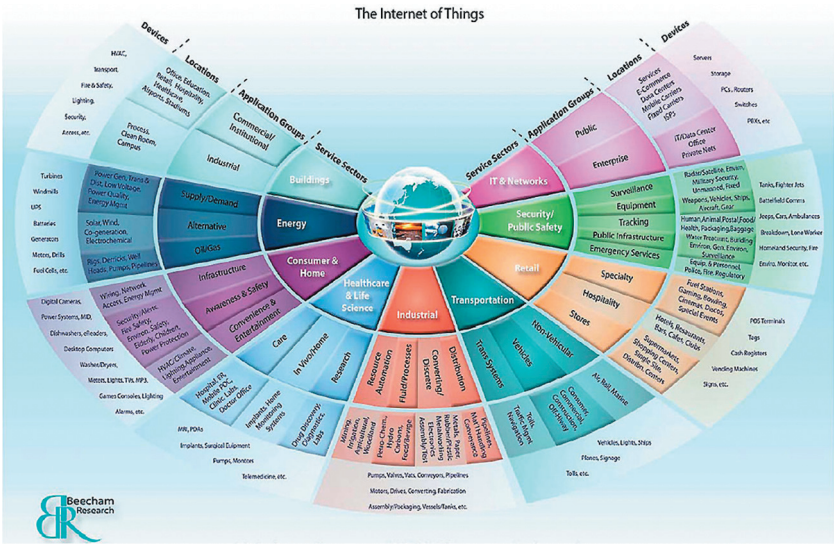
二、物聯網之應用

簡言之，物聯網就是「物物相連的網路」，在生活中的各種物體上安裝 RFID 感測器或是無線通訊晶片，讓物體透過網際網路而連結起來，回傳物體的狀態或供人類對物體進行控制。更進一步，物聯網將來會與媒體網際網路網、服務互聯網和企業互聯網構成未來互聯網。

物聯網的應用範圍相當廣泛，諸如運輸、零售、健康照護、能源管理、建築等等（圖 1）。我國電信業者已推出相關的物聯網服務，如中華電信的千里眼、iEN 智慧節能服務，或遠傳電信的科技救災、雲端血糖照護服務、雲端車隊管理服務，可窺得物聯網應用日趨成熟。

因物聯網的感測器之

圖 1　物聯網的應用範圍



資料來源：BCC Research.

論述 》專論 · 評述

體積可以非常小，因此相當適合於醫療方面的應用。瑞士 SENSIMED 公司推出名爲 Triggerfish 眼壓感測隱形眼鏡（圖 2），可以利用眼壓感測隱形眼鏡檢測青光眼患者眼睛的變化情況；以物流供應鏈應用爲例，企業利用「智慧物流」對商品從生產、包裝、運輸、倉儲管理、批發零售等供應鏈上、下游的每一個環節，進行更完善的掌控與管理（圖 3）。

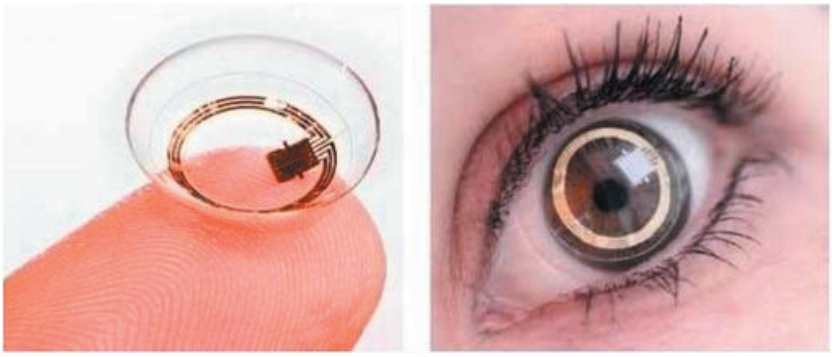
三、物聯網之安全威脅

根據研究機構 Infonetics Research 在 2014 年 1 月的報告（下頁圖 4），多數企業組織對於應用 IoT 最大的擔憂爲「安全性（Security）」。因此，資安威脅是物聯網發展的一大阻力，故如何建立值得信任（Trustworthy）的物聯網，乃一重要課題。欲了解物聯網有哪些安全性議題，需先剖析物聯網系統所涵蓋的層面，一般而言有三個（下頁圖 5）：

- 實體感知層：在物聯網內主司感測的設備，針對不同的場景進行感知與監控。使用具有感測、辨識及通訊能力的設備，例如：溫度、濕度、紅外線、光度、壓力、音量等各式感測器。
- 網路層：主司轉換並傳輸由實體感知層所送出之感知環境資料，負責將感知層收集到的資料傳輸至網際網路，作爲實體感知層與應用層間的連接通道。
- 應用層：提供即時可視之資訊。主要透過物聯網與行業間的專業進行技術融合來實現，並根據不同的需求開發出相應的應用軟體，以進行對實體應用層及網路層的管理。

若要建立值得信任的物聯網，不僅上述三層需環環相扣，彼此的訊息傳達必須暢通，各層也須發揮最佳的效能才能達

圖 2　Triggerfish 眼壓感測隱形眼鏡



資料來源：SENSIMED。

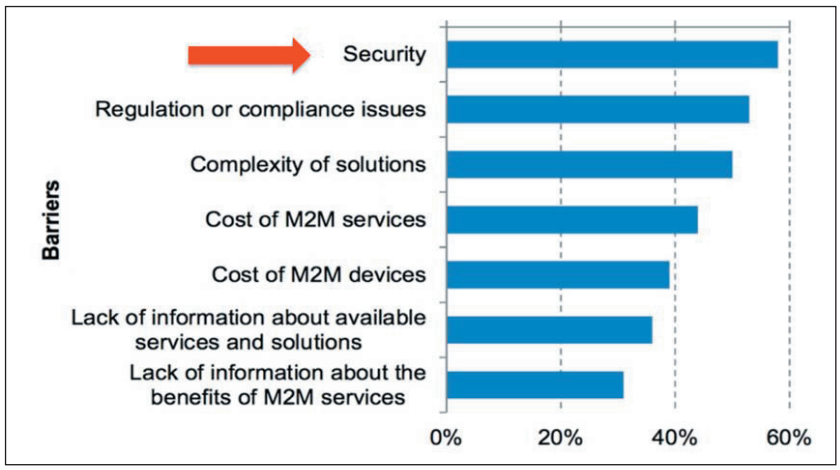
圖 3　RFID 生產履歷

資料來源：《串起智慧生活網絡－物聯網應用百花齊放》。

成。然而，各層亦有各自的挑戰需克服。首先，在進行資料收集時，若其中一個感測器被植入惡意指令可能將導致無法正常運作，服務品質將受到很大的影響；再者，若資料傳輸時無法確保資料不會外洩至外部網域，則無法滿足所需之效率、準確性、安全性、隱私保護、可靠性等。

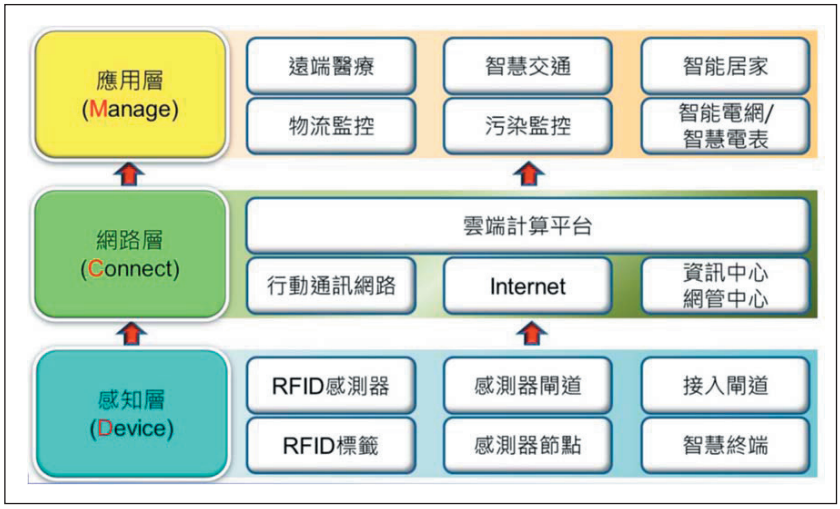
參、物聯網的信任管理

圖 4　IoT 應用於 M2M 模型之主要阻礙



資料來源：Infonetics Research.

圖 5　物聯網之三層架構



資料來源：《無線網路：通訊協定、感測網路、射頻技術與應用服務》。

物聯網的信任管理在資料流、資料探勘、服務水準，甚至使用者隱私保護及資安等方面，扮演重要的角色。物聯網系統應該建構完善的信任管理，以期達到「信任」、「安全性」及「隱私」，確保該系統與服務的使用者接受度與使用率。一個可信任的物聯網應用系統服務，必須能夠建構完善的信任管理，意即須同時考量下述十個議題（下頁圖 6）。

此十個信任議題詳述如下：

一、信任關係及決策（TRD）

信任管理提供了有效的方法供評估物聯網內元件之間的信任關係，並且協助這些元件能做出最佳化的決策。若要評估信任關係，則須考慮三層裡的所有元件。評估信任關係在建立自動化信任管理上扮演了相當基礎的角色。

二、資料感知信任（DPT）

感測器感測資料及收集資料的過程必須是可靠的。在物

論述 》專論 · 評述

聯網的範疇下，焦點會是諸如感測器的感測能力、正確性、安全性、可靠性、持久性等信任特性，以維持資料收集的效率。

三、隱私保護（PP）

任何從使用者蒐集的資料及使用者個人資料都屬於個人隱私範圍。無論於法律、政策的規定，還是對於使用者的期待，個人隱私都必須被妥善保護。我國的個資法目的即爲「爲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」；國際標準諸如 ISO27001 資訊安全管理系統認證標準、BS10012 個人資訊管理標準、支付卡產業資料安全標準 PCI DSS 等，對於個人資料保護或任何機敏資料保護皆有相關規範可依循。此項目標適用於物聯網系統中任何一個元件。

四、資料流及資料探勘信任（DFMT）

在進行大量資料處理及分析時，過程必須是可被信任的，衡量指標包括可靠性、全資料處理（Holographic Data Process）、隱私保護以及正確性。

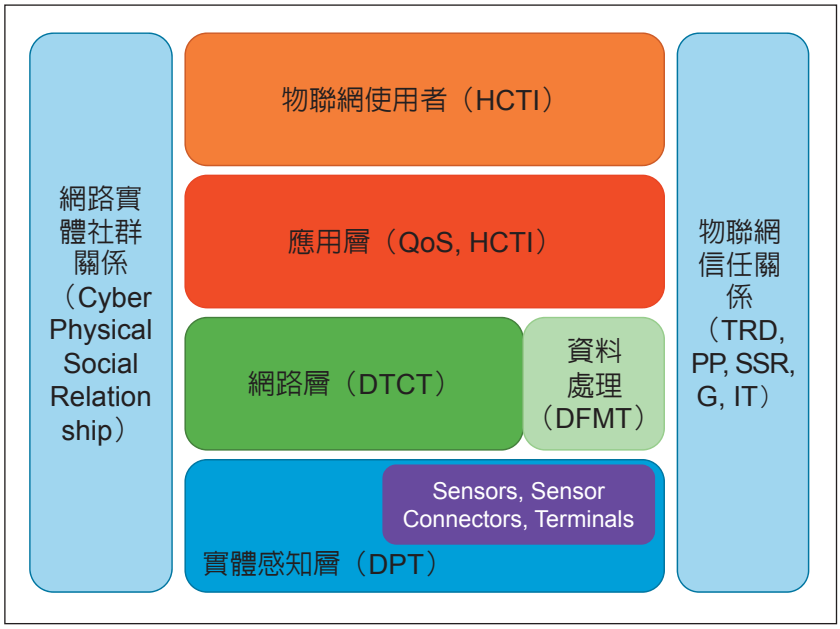
五、資料傳輸與溝通信任（DTCT）

資料在轉換及傳遞過程中必須被妥善保護，例如資料傳遞必須經過加密通道，以防竊聽、揭露、竄改等情事。另一意義爲任何未經授權的系統元件，不可在資料傳輸過程中存取任何資料。此目標與物聯網的安全性及隱私性有關，也因此更強調安全性、信任、隱私等相關解決方案的重要性。在網路層，信任的路由及金鑰管理實現上述解決方案的關鍵議題及技術。

六、物聯網服務品質（QoS）

最核心的目標是「只在此時、此刻，以及只有我」，意即物聯網的服務必須是個人化，並且在對的時間、對的地點提供給對的人。換句話說，物聯網服務必須是個人化且精確地在正確的地方提供給正確的人。主要著重在應用層的信任管理，但亦需另外兩層的支援。

圖 6　信任管理目標與物聯網系統模型的對應



資料來源：A Survey on Trust Management for Internet of Things.

七、系統安全性及穩定性（SSR）

須能有效抵抗外部攻擊，以有效地增加使用者的信任。此目標與各層皆有關聯，並把焦點放在系統的安全性與可信任性（Dependability，此特性包含了可靠性及可用性）。

八、通用性（G）

信任管理必須能適用於各種物聯網系統。

九、人對電腦的信任互動（HCTI）

信任管理提供完好的可用性，並讓人對電腦之間產生可被信任的互動，如此可較爲被使用者所接受。信任管理提供在人機互動間建立一個可信任的通道，如此便容易被使用者接受。此項要求與使用者及應用層密切相關。

十、身分信任（IT）

每個元件之使用目的都應照本身提供的服務被妥善的管理。進一步而言，需實現階層式及有效的身分管理。不但與三層皆有相關，也需要三層間相互合作。這將與所有特性（例如身分隱私）、相關主觀特性（例如使用者需求）及所有內容相關，且皆會影響相關身分管理政策或辦法。

爲順利達成上述目標，需要垂直信任管理。垂直信任指組織可控制及掌握從取得零組件到產品出售之間任一部分的運作。在物聯網中要達到垂直信任管理，需支持信任關係及決策、隱私保護、系統安全性及穩定性、通用性以及身分信任，加以融會貫通，方能實現值得信任的物聯網。信任管理需涵蓋所有面向，不僅限於安全性、隱私性及信任議題。各層、各元件需在透過信任管理科技下，彼此順暢溝通，達到可靠的合作模式。因此，唯有適用於物聯網之廣泛且整體性的信任管理，才能達成上述十項目標，缺一不可。

肆、結論

台積電董事長張忠謀先生曾在 2014 年台灣半導體協會年度會議中講演「Next Big Things」，公開表示不管是地面上、身上可戴、可測量溫度及血壓的東西，都可連結到物聯網，因此最賺錢的不是半導體公司，而是物聯網公司。在產業界的重視下，物聯網的應用將帶來不小的商機，但在發展的同時，如何提供值得讓使用者信賴的物聯網系統，是一個需要重視議題。本文以「信任」及「信任管理」作爲探討主軸，分析各層面需考量之要素，希冀可藉此提供各界先進於發展物聯網系統時之參考。

參考文獻

1. Yan, Z., Zhang, P., Vasilakos, A. V. （2014）. A Survey on Trust Management for Internet of Things. Journal of Network and Computer Applications, v 42, pp. 120-134.
2. Infonetics Research. http://www.infonetics.com/pr/2014/M2M-Provider-Survey-Highlights.asp
3. 社會計算。http://www.twwiki.com/wiki/%E7%A4%BE%E6%9C%83%E8%A8%88%E7%AE%97
4. 曾煜棋、林政寬、林致宇、潘孟鉉，《無線網路：通訊協定、感測網路、射頻技術與應用服務》，碁峰資訊股份有限公司，2011。
5. 劉家瑜，《串起智慧生活網絡－物聯網應用百花齊放》，貿易雜誌 TRADE MAGAZINE，2011，p14-20。❖