2019 TWIGF 座談場次摘要報告

智慧物聯網（AIoT）時代的安全與隱私挑戰

特派員 許祐豪

■ 座談重點內容

- 主持人引言報告：羅金賢 / 國家通訊傳播委員會基礎設施事務處處長

  一、當人工智慧（AI）遇上物聯網（AIoT）

  二、十個易受攻擊的 AIoT 目標及網路攻擊事件

  三、AIoT 時代的安全與隱私挑戰

  四、國際 AIoT 資安防護策略

  五、我國 AIoT 資安防護策略

  六、座談會討論面向及主題

  七、與談人介紹

- 與談人：林宗男 / 國立台灣大學電機工程學系教授

  AI 是一個破壞性科技創新，需要大量資料來運作，而這些資料主要來自 IoT。舉例來說，5G最重要的應用場景是「大規模機器行通訊」（Massive Machine Type Commnications, mMTC）。

  一、消費者的資安意識

  網路攝影機遭駭客入侵事件：由於沒有改變預設密碼，造成相當嚴重的個人隱私遭侵犯。該事件反應出很多駭客不一定有很多高深的功力，只是抓住了平常大家忽略的面向。

二、廠商的資安防護

高速公路電子收費系統：由遠通電收營運的高速公路電子收費系統所收集之資料之歸屬仍值得探討。

成本及資安之權衡：廠商導入資安相關考量須提高製造成本或認證成本，且現今許多消費者是以價錢為考量來進行購買行為，使得廠商沒有動機進行資訊安全措施。在這個狀況下，政府的角色尤其重要，可以借鏡食品安全法則之應用進行規範。

- 與談人：林俊秀 / 經濟部工業局電子資訊組組長

一、消費者的資安意識

經濟部工業局陸續配合總統府及行政院資安處辦理消費者意識提升活動，也會先行模擬私人攝影機被侵入之狀況。

二、廠商資安防護

經濟部工業局業務上推廣資安產業，而近幾年隨著物聯網產業發展，政府也漸漸地針對相關廠商進行規範。

三、政府的資安策略

政府在國際輸出、向內向外之市場拓展及人才培育上都正在努力。

四、資安標章的推廣

政府部門以身作則，採購有資安標章之產品，往後也會陸陸續續與其他政府部門溝通，以擴大符合資安標準之廠商之市場。

- 與談人：張保忠 / 中華電信研究院資安所所長

一、消費者的資安意識

建議選用安全標章之產品，並且提醒消費者要有基本防護，進行換密碼之動作，也應該要定期更新設備以降低資安問題發生之可能性。

另外，如果要把裝置交給他人或丟棄，也必須清除資料或者回復原廠設定。

二、廠商資安防護

中華電信本身就是產品和服務的提供者，因此內部員工在做研發時一定會有相關防護措施，而資安應該要放在開發流程中。以中華電信研究院來說，內部已有既定開發流程及規範文件，如需求規格書等等，都已將資安列入其中。此外，中華電信也有進行第三方認證，如 ISO 27001，以了解整個研發過程中是否有遺漏之環節，從內部標準流程到外部第三方審查，落實風險管控。

- 與談人：熊全迪 / 理律法律事務所初級合夥人

主要涉及問題：

- 個資法問題：個資法是從人格權延伸出來的概念。而資安保護可能包括個人隱私，也牽涉到公司資料、商業機密、商業利益或資產安全。
- 責任問題：如果有某個人在某個環節做了某件事，因此害了其他人，所衍生之權責問題。

一、消費者的資安意識

就實務上而言，消費者應該具備下列兩項意識：

- 選擇商品：是否該向某廠商買東西？大廠是否就能提供安全商品？以第三方認證機構來判斷，相對來說比較客觀。
- 個資保護：若某商品或服務需要取得消費者資料，都會有一個很長的告知，讓消費者同意。

二、政府的資安策略

政府擔任之角色有下列兩種：

- 設備使用者（採購方）：政府能夠購買擁有資安標章之商品，成為領頭羊之角色，產生上行下效的結果。此外，政府的資安對人民來說更重要，因為國家資訊涉及國防議題，應該要以極嚴格的標準進行採購。

- 立法及執法者：金管會針對銀行委外及資料雲端化皆進行相關規範。最近政府欲修正資料雲端化、Open Data等相關事務，針對銀行交易紀錄及個資之規範也需要進行釐清。

三、資安標章的推廣

推廣相關認證，借鏡食品安全規範以保護消費者。

■ 現場交流（Q&A）

- 提問 1：在物聯網快速發展之下，出現越來越多聲浪要破壞資安，如德國刑事訴訟法及澳洲相關法規，提出廠商要給政府「留後門」，關於電腦科學和法律之間的模糊地帶，該怎麼去思考這個問題？如果是以解決恐怖主義、人口販運、刑事訴訟重罪為前提，又該如何去做權衡？

  - 答覆：羅金賢/國家通訊傳播委員會基礎設施事務處處長

  處理資安相關問題上，最難的就是用戶端。網路主要分為政府網路、學術網路及商業網路三種，而處理商業網路之難處為目前沒有法條可以規範。政府會偵測到某個用戶電腦中毒，但是通知用戶後，用戶可能無法解決或者不進行解決。目前政府是參照日本機制，以CCC（Cyber Cleaner Center）方式運作，與國內防毒業者合作，請業者通知用戶下載解毒軟體，但成功率不到 20%。往後會朝向立法邁進，讓民間及政府取得共識。

  - 答覆：張保忠 / 中華電信研究院資安所所長

以開發商來看，如果沒有法律允許的話，一定不敢做這件事情，因為企業都是依法辦事。

○ 答覆：熊全迪 / 理律法律事務所初級合夥人

如果是毫無事由地讓政府「走後門」的話，當然不允許。但要不要制定該法律，須在人民基本權及政府重大利益之間做權衡。舉例來說，恐怖主義會影響公眾利益，所以政府經過權衡之後就可以有相關權力。平常在和客戶擬合約時，在保密條款上也會有例外，如果政府在公眾利益基準上和我們要求提供相關資料的話，我們也會依法提供。

- 提問 2：目前多著墨在資料被盜用的狀況，但服務商濫用資料也是有可能。此外，駭客在做目標式攻擊的時候常常會搜尋數位足跡，如個人喜好、同事朋友等等，提高成功機率。關於數位足跡和濫用資料，想問各位有沒有什麼想法？

○ 答覆：林宗男 / 國立台灣大學電機工程學系教授

一般消費者很難去了解「所有權」的定義，最擔心的還是隱私權。我們在上網瀏覽的時候，一舉一動都被 Cookie 記錄得一清二楚。物聯網的時代，由於成本越來越低，所有足跡都可以很輕易地被追蹤，就算不是重要人物也是會被記錄。目前駭客可以分為散戶、群體或者國家級。國家級的駭客主要是分佈在中國、伊朗、以色列、美國、俄羅斯等國家。從技術觀點來看，如果設置「後門」的話，僅是增加散戶及團體駭客入侵之機會，同時也牽涉到價值權的選擇及正常程序的稽核。從隱私權的角度來看，目前沒有一個最好的解套方案。

○ 答覆：張保忠 / 中華電信研究院資安所所長

個資法已經施行好幾年，目前仍與時俱進當中，而數位足跡目前也屬於個資。針對留後門給政府是否有正當性可能與國家民族性有關，

像是日本會覺得是公益。若要落實，則需要在公益和私益之間做平衡。對個資的濫用或盜用是服務商的責任，我們都是很盡力地在保護資料。公司內部系統防禦是非常強的，從開發階段到設計階段都會將個資考慮進去。如果是駭客可能就是另外一回事，不一定防得了。以目前來說，不管是政府或者企業難免會有比較厲害的駭客，跟保險一樣不能保證絕對安全。因為沒有零風險的東西，所以消費者要有意識，也要記得更新裝置。

○ 答覆：熊全迪 / 理律法律事務所初級合夥人

只要企業沒經過同意，利用消費者個資進行行銷或其他行為，就符合濫用。資通安全管理法提及主管機關必須設定安全維護計畫，如金管會可能有指定銀行訂定安全維護計畫，但儘管有法規，風險仍不可能降為零。刑法也有制定妨害秘密罪。

■ 心得感想

身為一個數位原生代的人，過去總覺得自己可以完全操控裝置，也認為所有資料都在掌握之中，但事實並不是如此。經過今天這場座談會，接收了來自政府機關、學術界、服務提供商及法律專家的多方激盪，讓我更了解身為一個公民該怎麼去做自我保護，不僅讓我的生活更便利，也能夠享受科技帶來的改變。