出國報告（出國類別：其它-參訪交流）

出席「MOST&JST 研究計畫成果發表會」及會後參訪活動

服務機關：科技部
姓名職稱：工程司 廖婉君 司長
科教國合司 鄭慧娟 研究員
派赴國家：日本
出國期間：106 年 4 月 16 日至 4 月 20 日
報告日期：106 年 6 月 30 日

目　次

摘要

科技部(以下簡稱本部)與日本科學技術振興機構(JST)，共同合作徵求以” Research and Development for Secure and Dependable IoT Portable Devices” 為重點領域之研究計畫。為瞭解合作計畫執行效益，邀集台日雙方計畫主持人團隊提出簡報，以檢視是否達到預期合作目標。

2017 年 4 月 16 日至 20 日，本部與日本 JST 在日本東京合辦「Taiwan-Japan Workshop on Security and Dependability Technologies for IoT Devices, 2017」和參訪活動，台日雙方分由本部工程司廖婉君司長及白木澤佳子 (Yoshiko Shirokizawa)理事率團，台日講師共 12 位發表簡報，以分享在此合作專題的研究成果，發表會另舉行學生海報展示、評選活動。

會後拜會日方相關機構，包括 KDDI、NICT 以及 AIST。藉由參訪介紹這些機構的研發環境與成果，有助於瞭解台日在相關主題合作的可能性。

壹、目的

科技部與日本科學技術振興機構(JST)每年合作徵求特定主題共同研究計畫，每兩年舉辦研究計畫成果發表會。台日國合計畫進行多年，經由此一機制，除可檢視該合作計畫的效益與成果是否符合徵案目標，亦作為日後推案的重要參考。

本次研討會「Taiwan-Japan Workshop on Security and Dependability Technologies for IoT Devices, 2017」主要參加團隊皆為台日" Research and Development for Secure and Dependable IoT Portable Devices" 共同研究計畫成員，於研討會中發表雙方合作研究成果，除可比較合作成果的差異，亦認識其他團隊成員，以拓展未來合作可能。此次會議，日方委請國立研究開發法人產業技術總合研究所(National Institute of Advanced Industrial Science and Technology，AIST)計畫主持人 Dr. Yoshio Tanaka 擔任總召集人，會中除了計畫成果報告之外，並舉行學生海報展示及評選活動，藉以鼓勵新生代研發工作。

訪日期間，由 JST 安排參訪 KDDI、NICT 以及 AIST，期透過產學研的交流互動，討論合作的可行性，厚植雙方未來進一步合作發展的基礎，對於台日科研界均有加值的效益。

貳、過程

■主要行程/

(一)舉辦「Taiwan-Japan Workshop on Security and Dependability Technologies for IoT Devices, 2017」

本次研討會在靠近東京秋葉原的 Akihabara Daibiru Bldg.舉行。首先在日方 JST 團長白木澤佳子、本部工程司廖婉君司長分別擔任主辦單位致詞下揭開序幕。接下來分由六項研究計畫團隊發表簡報：臺方報告人員包括國立臺灣科技大學鄧惟中副教授、國立臺灣大學林風教授、國家高速網路與計算中心黃維誠研究員、長庚大學資訊管理系許建隆教授，以及國立中興大學游家牧助理教授；日本報告人員包含國立東京大學中尾彰宏(Akihiro Nakao)教授、國立東北大學加藤寧(Nei Kato)教授、AIST 研究部長田中良夫(Yoshio Tanaka)博士、廣島市立大學雙紙正和(Masakazu Soshi)副教授、國立東京工業大學橫田治夫(Haruo Yokota)教授，以及明治大學菊池浩明(Hiroaki Kikuchi)教授。

有關研討會議程及會議內容紀要如下。

(1)Research on Identification of Devices and Application for Improving Security in SDN enabled IoT/Cloud System (Prof. Akihiro Nakao and Prof. Wei-Chung Teng)

中尾彰宏(Akihiro Nakao)教授為美國普林斯頓大學(Princeton University)電腦科學博士，過去曾於IBM擔任工程師及研究員，亦曾於猶他大學(The University of Utah)任教，現任職於國立東京大學，專攻電腦科學領域。鄧惟中副教授為日本東京大學(University of Tokyo)工學博士，曾任職於碩琦科技，現任職於國立臺灣科技大學，研究專長包含遠端機器人控制、虛擬實境、網路通訊協定、人機介面。該團隊的計畫目的為利用軟體定義網路(Software Defined Networks，以下簡稱為SDN)跟網路功能虛擬化(Network Function Virtualization，以下簡稱為NFV)科技的優勢確保物聯網的安全性與隱私性。該團隊試圖透過三個面向解決物聯網的安全挑戰—應用(惡意程式偵測、預防與移除)、資料(個人隱私資料)、設備(設備識別)。應用方面，為了識別與分類合法與惡意的應用程式，不僅需要Sound System Design亦需要網路深度學習；資料方面，識別個人隱私資料需要資料探勘技術；設備方面，識別上

億個感測器、設備及智慧手機需要數學化分析及針對數萬種特殊設備進行系統設計。該團隊針對上述三個面向，仔細進行團隊分工，根據三個面向分成三個團隊進行研究。

(2) Identify Management towards Internet of Things (IoT) on Machine Type Communications (MTC): Efficiency & Security (Prof. Nei Kato and Prof. Phone Lin)

加藤寧(Nei Kato)教授為國立東北大學(Tohoku University)工學研究科博士，畢業後即在該校任職至今，期間獲獎無數，研究專長為電腦網路、無線行動通訊、衛星通訊等。林風教授為國立交通大學電腦科學及資訊工程博士，曾於工研院擔任研究員、資策會及晨星半導體擔任技術顧問等，現任職於國立臺灣大學資訊工程系暨研究所，研究專長為機器與機器間的資料交換(Machine to Machine，以下簡稱為M2M)、物聯網、SDN、異質網路(Heterogeneous Network，即HetNet)、綠色通訊(Green Communications)。

物聯網是一個新興的技術領域，這個技術有希望能夠帶來連接數不勝數台機器的能力，並將這能力用於眾多令人興奮的應用。然而，在目前的網路架構下，由於物聯網要連結的設備數以千萬，因此在性能上會受到設備的效能、身份識別以及重要的信令傳遞等所影響。為解決這些問題，該團隊提出的觀點著重在物聯網中有效且具有安全性的身分管理。根據過去的研究，該團隊將問題分成下列三個全新的主題進行研究：第一、對於物聯網的觸發裝置，會針對基於身分分群概念的身分管理架構進行研究；第二、將研究使用雜湊函數以減少群組間傳遞資訊的儲存與通訊成本；第三、將開發一個密鑰暫存機制，在減少的訊息要求下保持安全性。對於該團隊所提出的所有解決方案皆進行實作和分析，提供效能評估，以助於提出全方面的模型能更凸顯這個議題。此外，改善後的的身分管理和安全架構可期望為網路營運商、服務提供商和M2M終端用戶帶來降低營運成本、提高用戶滿意度和效能以及安全通訊等優勢。

三代合作計畫(3rd Generation Partnership Project，即 3GPP)工作小組所提

出的機器類型通訊(Machine Type Communications，以下簡稱為 MTC)，是一種包含自主設備廣泛應用的技術。MTC 正在積極發展以支持物聯網，並且成為 5G 的要求之一。在物聯網環境中，大量的 MTC 設備將連接到物聯網，這可能會對網路造成極大的負擔，例如有線網路、無線網路以及設備的身份等資源。該團隊將重點放在 MTC 對物聯網的身份管理效率，作為計畫前兩年的成果。

以下介紹包含兩個主題：主題一、在 MTC 中，透過核心網域中的唯一識別碼(ID)來識別設備，其與人對人設備中識別方式相同。透過唯一的 ID，MTC 應用服務器(以下稱為 MTC AS)可以將訊息(觸發請求訊息)傳遞到 MTC 設備。因為有大量的 MTC 設備需要，因此很難使用有限數量的 ID 來支持大量的 MTC 設備。為解決這個問題，該團隊提出了一個基於「ID 共享」概念的高效身份識別管理機制，透過此機制並根據一些標準將 MTC 設備進行分組，同一組中的設備將共享相同的 ID，每一個設備可以在給定時間中連上網路，換句話說，同一組中的 MTC 設備需要依次連線到網路，等待來自 MTC AS 的觸發請求。此機制已經提交給中華民國和美國申請專利，該團隊還實作了一個平台來實現提出的機制。主題二、探討如何在同一組的 MTC 設備之間進行高效能且公平地共享網路資源，由於形成資源共享設備組為減輕瞬時訊息負擔的主要方法，該團隊提出了一種基於圖像化模型的方法，在物聯網應用程式的執行時間限制情況下最小化所需 MTC 組的數量；其中，最小化問題是裝箱問題演算法中，裝箱尺寸為動態的變化。從「群組的弱動態限制」的角度來看，可以使用有效的求解器來定義混合整數線性規劃(Mixed Integer Linear Programming，即 MILP)問題，或者唯一的動態裝箱大小可以通過專門設計的優配遞減法(Best-fit-decreasing，即 BFD)來處理，用於較低複雜度的解決方案。他們提出的機制與常用的分組標準(如設備特徵和位置)相比，可以清楚地觀察到分組數量最小化策略的優點。

(3)IoT Security Management System with Unclonable Devices (Dr. Yoshio Tanaka and Dr. Weicheng Huang)

田中良夫(Yoshio Tanaka)博士為慶應義塾大學(Keio University)數理科學研究所博士，曾先後於RWCP(Real World Computing Partnership)新資訊處理開發機構及電子技術綜合研究所(Electrotechnical Laboratory)任研究員，現任AIST研究部長，研究專長為分散式計算網路、eScience之網路架構、實體網路系統及安全。

黃維誠研究員為伊利諾大學厄巴納香檳分校(University of Illinois at Urbana-Champaign)航太工程博士，曾於中央研究院數學所及美國國家超級電腦應用中心任研究員，現任職於國家高速網路與計算中心，研究專長為分散式計算網路、網格運算、大數據。該團隊計畫目的為發展安全物聯網架構，並分成兩個子工作項目：① (WP1)物聯網安全管理；② (WP2)適用於不可複製(Unclonable)物聯網裝置之金鑰管理。物聯網裝置容易被製造與佈建，而其中一個重要議題即為物聯網安全管理，目的為識別出可信任(Trustable)之物聯網裝置。WP1已發展出基於視為根信任者(Root of Trust)的硬體安全模組(Hardware Security Module，即HSM)之軟體管理技術，使用了稱為可信任平台模組(Trusted Platform Module，以下簡稱為TPM)或可信任執行環境(Trusted Execution Environment，即TEE)之安全晶片，物聯網裝置的啟動紀錄會被儲存在TPM，而這些紀錄會被遠端認證(Remote Attestation)並被利用去偵測惡意程式注入；WP2為開發適用於物聯網裝置的金鑰管理系統。訊息序列遙測傳輸(Message Queuing Telemetry Transport，以下簡稱為MQTT)為物聯網裝置連接協定，已被資訊標準架構促進會(Organization for the Advancement of Structured Information Standards，以下簡稱為OASIS)制定成標準。OASIS標準強烈建議MQTT的安全性解決方案需利用SSL/TLS。然而，為了驗證憑證及註銷確認，此類方案需額外耗費通訊成本，為了解決此問題，WP2提出了一個適用於MQTT的簡易安全框架，簡稱為AugMQTT。此框架所利用的AugPAKE協定可在保有弱秘密(Weak Secret，例如弱密碼或PIN碼)的情形下，抵禦被動攻擊、主動攻擊及離線字典攻擊，並且比先前其他研究更有效率。況且，AugMTQQ無須進行憑證驗證及註銷確認，藉此簡化初始階段的設定及AugMTQQ整體程序。

(4)New Lightweight Cryptosystems for IoT Devices and Application to eHealth Environments in Taiwan (Prof. Masakazu Soshi and Prof. Chien-Lung Hsu)

雙紙正和(Masakazu Soshi)副教授為日本國立電氣通信大學(The University of Electro-Communications)工程博士，曾任職於日本國立電氣通信大學及AIST，現任職於廣島市立大學，研究專長為電腦安全。長庚大學許建隆教授合作計畫共同主持人宮地充子(Atsuko Miyaji)不克出席，由團隊共同主持人之一雙紙正和(Masakazu Soshi)副教授代表出席並發表成果。

物聯網已被世人討論，但其裝置之低計算資源亦困擾著系統開發者，故輕量化(Lightweight)密碼學協定為物聯網安全一個解決方案，藉此才能進一步推廣物聯網科技對健康管理的益處。因此，該計畫主要目標有二：①設計適用於物聯網物件的安全輕量化密碼模組；②開發適用於互聯網環境的人機互動式身分鑑別系統與智慧型存取控制協定。此外，計畫團隊將於長庚醫院建構一套以物聯網為基礎的電子醫療照護系統，整合開發的密碼系統，其中包含輕量化密碼模組、互動式身分鑑別與智慧型存取控制等技術。

此計畫其中一個重要議題為白箱AES(White-box AES)之應用。有鑒於物聯網環境裡的裝置易被攻擊者在未經授權的情形下進行裝置存取，進而利用手段獲得金鑰。白箱密碼協定(White-box Cryptography)為試圖不讓金鑰輕易被取得，甚至在不被信任的網路環境中也不易取得金鑰。現今大多數的白箱AES應用技術為基於學者Chow的研究，其中一項特性為建立一個查找表(Lookup-table)以觀察AES傳輸之輸入值與輸出值間的關聯性。然而，白箱AES應用已被證實為不安全。所以，計畫團隊參考由學者Luo與You提出的安全白箱AES應用，此一方法至今尚未被破解。計畫團隊將MixColumns矩陣隨機拆分成兩個子矩陣，藉此達到與原本AES相同的功能，但增強了安全性，不過安全性分析與效能分析仍須進行進一步研析。

計畫團隊於現階段已設計一套基於嚴肅遊戲及骨鬆診斷指引之智慧健康推廣系統，透過質性訪談完成接受度評估。計畫團隊亦評估系統安全性及設計安全協定；此外，亦完成物聯網傳輸架構下的透明身分鑑別機制設計與建置，利用自行設計的智慧足壓偵測器進行使用者生物資料收集，再將資料

傳送到後台伺服器進行個人生物特徵萃取，以作為身分鑑別的判定因子。於穿戴式裝置應用研究方面，計畫團隊將穿戴式裝置導入至四個不同場域(含長庚養生文化村)，並分別驗證穿戴式裝置之接受度及可用性。

(5)Reliable compromise-resilient mechanisms for managing the data integrity and privacy of heterogeneous IoT devices (Prof. Haruo Yokota and Dr. Chia-Mu Yu (co-PI))

横田治夫(Haruo Yokota)教授為國立東京工業大學(Tokyo Institute of Technology)博士，曾為日本第五代電腦計畫成員，並曾任職於富士通研究所(Fujitsu Laboratories)及 AIST，現任職於國立東京工業大學，研究專長含電腦安全、資料工程等。游家牧助理教授為國立臺灣大學電機工程博士，曾任職於中央研究院資訊所、IBM 研究院華生科學運算實驗室(IBM Thomas J. Watson Research Center)、元智大學，現任職於國立中興大學，研究專長為雲端及物聯網安全、資料隱私、密碼學。當天，該團隊先介紹了臺日合作計畫的進展情況，並提供了雙方合作的一些資料，並展示合作的研究成果及提出未來合作計畫。

計畫團隊旨在開發基礎技術，以實現可靠的保護機制，用於管理異質物聯網設備的資料完整性和隱私。在異質物聯網設備的物理限制下(例如有限的計算能力)，該團隊正在嘗試開發檢測故障或受損的物聯網設備的方法，以及使用資料的時空相關分析數據來校正來自那些設備的資料。同時，該團隊正在努力開發輕量級化的具有安全性和可靠性的保護機制，來確保物聯網系統的隱私性。日本的團隊主要著重於檢測和校正方法，而臺灣的團隊則主要著重於輕量化的具有安全性和可靠性的保護機制，兩邊團隊的相互合作，解決了雙方的研究課題。

為了讓研究計畫順利進行，各方研究人員經常訪問其他機構。從這個計畫開始，該團隊總共進行了六次面對面的會議，其中參與討論與研究的成員包含日本方的三位研究人員與臺灣方的三位研究人員。此外，該團隊在東京工業大學舉辦” The First Japan-Taiwan Workshop on Secure and Dependable IoT

Systems”研討會，這場研討會共有12位研究人員參與，分別是來自日本的6位與臺灣的6位；此外，臺灣方的一名學生已經在東京工業大學從事相關研究超過50天。作為研究計畫成果的一部分，該團隊已在國際會議上發表了兩篇論文，一篇為”Key Management in Internet of Things via Kronecker Product”，此為一適用於物聯網之新的密鑰建立方法，該方法使用克羅內克積(Kronecker Product)來實現，滿足以下條件：①減少需要存儲在IoT設備中的基本資料量；②有效地計算成對密鑰；③在計算密鑰期間不需要進行通訊。該篇論文已投稿至22nd IEEE Pacific Rim International Symposium on Dependable Computing；另一篇為”Impact Analysis for Dos and Integrity Attacks on IoT Systems”，已投稿到The 7th International Conference on Information Systems and Technologies。

(6)Secure IoT-Based Information Platform with Privacy-Preserving Data Mining on Big Data for M-Healthcare (Prof. Hiroaki Kikuchi and Prof. Chun-I Fan)

菊池浩明(Hiroaki Kikuchi)教授為明治大學(Meiji University)博士，並曾赴美國卡內基美隆大學作訪問學者；曾任職於富士通研究所及日本東海大學(Tokai University)，現任職於明治大學，研究專長為網路安全、隱私技術。范俊逸教授為國立臺灣大學電機工程博士，曾任職於中華電信，現任職於國立中山大學，研究專長為應用密碼學及資通訊安全。此次范教授因個人因素不克前往，因此委由菊池浩明教授代表報告。

當天的主題為流行病研究資料之具隱私保護的資料探勘(Privacy-preserving Data Mining，以下簡稱為PPDM)方法。在資料探勘演算法方面，該團隊把焦點放在複線性迴歸(Linear Multiple Regression)，此方法可用於在很多個變數中識別最顯著之因子，而該團隊嘗試利用此線性模型，從與病人及疾病相關之分散式資料庫(Distributed Dataset)中預估住院時間長度。該團隊已利用中風相關之醫療資料庫進行實驗，並利用含六個預測因子的複線性迴歸。該實驗研究的貢獻有：①提出了可實作之適用於複線性迴歸之具隱私保護的協定；②提出的系統利用真實醫療資料庫，且該系統具擴充性；

③不僅呈現該PPDM系統之準確率及效能，並可允許利用隨機數目的預測因子估計整體時間長度。

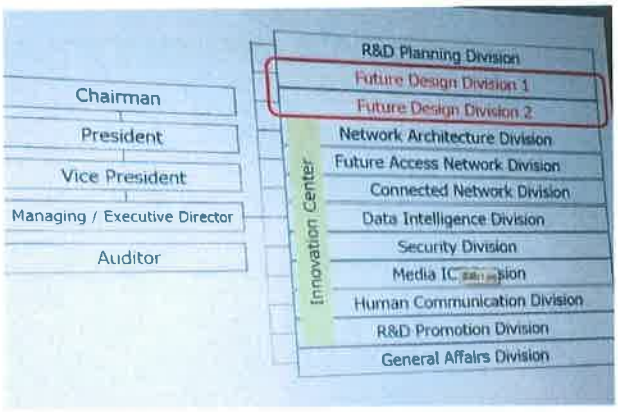
在物聯網環境中，使用者會使用許多不同的設備相互連接並分享資料，而這些設備通常不會擁有強大的計算能力及儲存空間。許多研究都把焦點放在雲端伺服器與使用者端間的輕量化認證機制，以利用雲端伺服器協助感測器或代理伺服器完成認證。然而，使用者端的設備如何在不用雲端伺服器的協助下建立團體溝通金鑰(Group Session Key)為一個重要的議題。無線身體區域網路(Wireless Body Area Network，以下簡稱為WBAN)為物聯網環境中最為知名的網路。WBAN環境中，代理伺服器通常需要控制及監控從感測器傳送來之使用者健康資料，此情況下需要團體認證方法及團體溝通金鑰。該團隊提出了一個物聯網環境中使用者端之團體認證及產生團體溝通金鑰方法，此方法為一個輕量化認證方法，並可適用於存在動態團體成員之物聯網環境。該團隊認為此方法可以滿足彈性化產生團體分享金鑰、動態參與者、主動註銷、低計算及通訊成本、無時間同步問題等特性。該方法亦可達到雙向認證、團體金鑰協議、抵禦許多已知攻擊之安全特性。

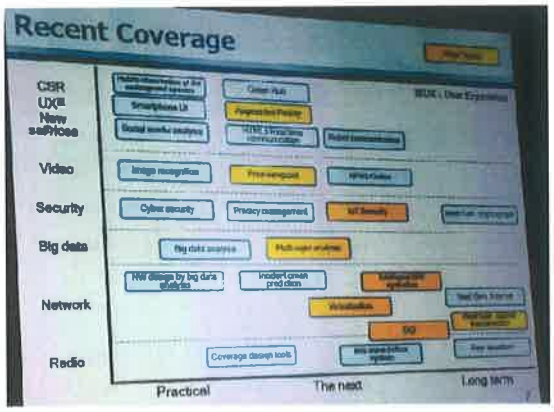
(二)參訪 KDDI Research Inc.

KDDI 集團(KDDI CORPORATION)是日本大型電信公司，主要在 au 提供手機通訊服務，也在 au one net (舊名 Dion)提供網際網路服務供應商網路服務，目前亦有網路電話與國際電話的業務項目。株式會社 KDDI 綜合研究所(即 KDDI Research, Inc.)最早於 1953 年成立，當年為「國際電信電話(KDD)株式會社」的研究部門，直至 1998 年經 KDD 公司改組，成立了株式會社 KDD 研究所。爾後經歷企業併購及組織合併改組，於 2016 年正式以「株式會社 KDDI 綜合研究所」開始營運。主要營運內容包含以資訊及通訊為中心之政策、市場、商業化等相關調查研究與顧問服務，及其相關技術、系統之研究、開發、製造及販售，另外亦提供相關教育訓練及進修機會。

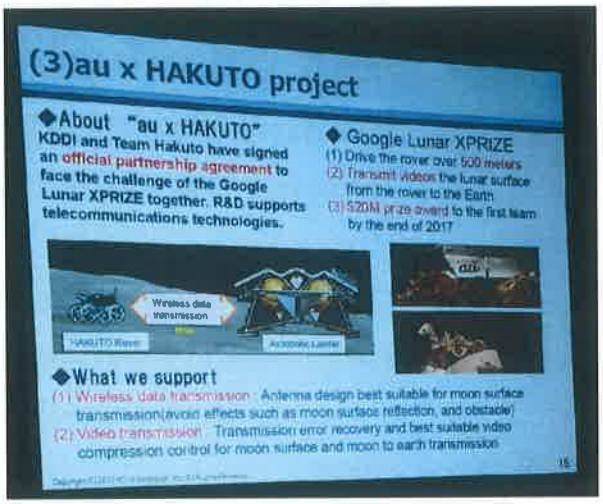
KDDI 公司接待人員，簡要地介紹了 KDDI 的組織架構，並強調較具代表性的 Future Design Division 1 & 2。其主要工作是尋找未來創新的方向與實

際可投入的領域。此一前瞻思維，不拘泥於現時短期產出，而是著眼於未來發展，與普遍瀰漫的短期投資效益的思維，大相逕庭。





此外，KDDI 更點出其現今重點研發方向包括 AR、IoT Security、Mjulti-layer Analysis、Virtualization、以及 5G 等。就計畫而言，KDDI 提供了幾個與 IoT 有關的應用，例如，" Multi-Lingual Speech Translation System" ，透過 LTE 結合雲端及音訊系統，提供國外遊客即時翻譯，並以計程車為示範場域。深度學習 Deep Learning 也被應用在捕魚方面，如透過對海水溫度及洋流水文的長期監控，結合漁民專業知識，透過深度學習，預測特定日期的漁獲量，以節省人工與油料成本。一個比較有趣的" 小" 計畫，則是與 "HAKUTO" 圖隊結合，提供無線通訊以及影片傳輸與復原機制，以在月球表面，驅動 HAKUTO 製造的月球車前行 500 公尺，並且將月表影片傳送回地球。

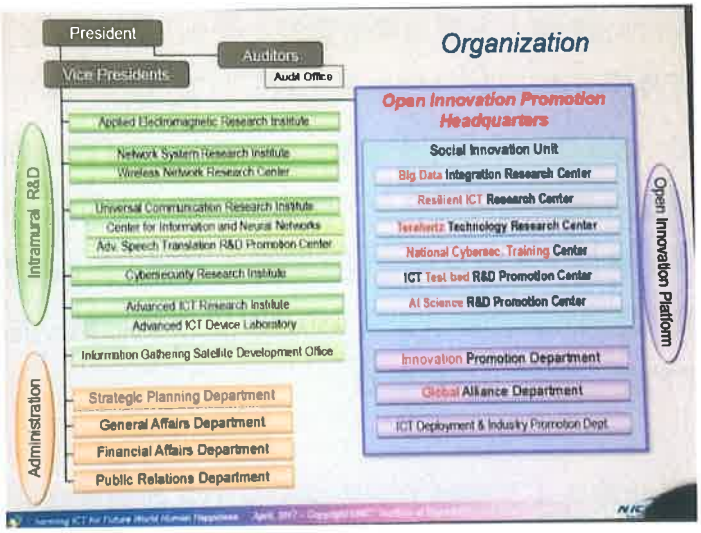


其他計畫，例如，透過手錶的震動來啟動汽車，而該手錶必須經過認證，具有無可複製的 Device ID，雖然距離實用尚遠，但其創新的想法，雖然簡單且直接，但卻是創新的嘗試。在離開 KDDI 前，於入口後方，發現 Aqua Explorer，明顯看出適用於海底探索與監測作業。其螺槳設置異於常態，頗值得注意。

(三)參訪國立通信研究所(National Institute of Information and Communications Technology, NICT)

NICT(國立研究開發法人資通訊研究機構)為日本國內資通訊領域中唯一的公家機構，最早可追溯到1896年，為了研究無線通訊而成立了通訊綜合研究所；1979年時因衛星通訊的發展，另成立了衛星廣播機構；直至2004年才將通訊綜合研究所及衛星廣播機構合併為獨立行政法人資通訊研究機構，並於2015年正式更名為國立研究開發法人資通訊研究機構。NICT的主要任務為，協助推動視為可以實現令人安心、感到安全的社會，並可以成為日本經濟成長原動力的資通訊技術(Information and Communications Technology，即ICT)之研究發展，並負責資通訊企業之振興業務。

NICT 的角色介於政府與學界及產業界之間，為政府補助單位，以其 ICT 技術協助學界以及業界研發。該單位共有 1023 位員工，其中有 524 位研究人員，其中並有 477 位擁有博士學位。到訪 NICT 時，首先參觀其過往成果展示場域。



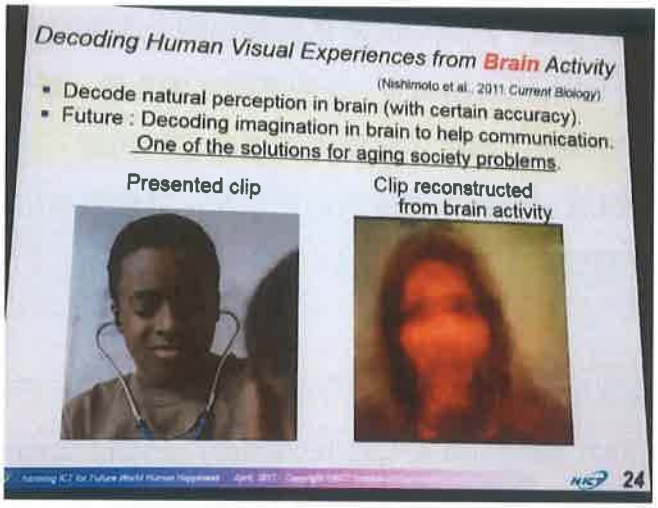
NICT 也投入語言翻譯的相關研發; Trilingual Speech-to-Speech translation system VoiceTra，可以即時對日文、中文、韓文，提供翻譯。且該計畫並提供 APP 下載至手機運用的免費服務，試圖協助降低其國內觀光產業接待外國人的語言隔閡。Multi-Sensory Interaction System，多感應器互動系統，類似 VR/AR 系統，將電子影像投注到螢幕上，讓使用者產生視覺感官的同時，藉由力回饋裝置讓使用者感受彷彿確實有物件在面前的感官刺激。其實際應用則可使用於手術模擬，以及各式需要手工介入的運用。

NICT 已經進入第四個五年計劃，這個五年計劃的重點專注在 Data Utilization and analytic platform, Integrated ICT, Cybersecurity, sensing fundamentals, 以及 Frontier researches (例如量子網路技術等)。除了上述研發成果之外，現今 NICT 較具特色的研發項目，包括結合 NICT、Toshiba 以及大阪大學的研發團隊進行的”次世代相位陣列氣象雷達(Next-Generation Phased Array Weather Radar)”，可以在極端氣候(例如暴雨、龍捲風等)發生 30 秒內，提供以 100 公尺為解析度的立體 3D 影像，對於局部地區的極端氣候預測，相較於傳統雷達需要 10 分鐘才能提供資訊的情況而言，此一雷達陣列極具有前瞻及未來性。

其他通訊科技的應用包括火山活動測報 Pi-SAR2、無線智慧網路 Wi-SUN、透過通訊衛星對海面船隻進行即時操作，一直到 photonic network、multi-core 光纖傳輸等，都極具未來性。而本次參觀 NICT 的重點是 Cybersecurity Research Institute。此次 NICT 展示了開發已久的 NICTER(Network Incident analysis Center

for Tactical Emergency Response)系統，主要目標是監控、分析、阻擋網路上的惡意程式(Malware)。其元件區分為 MacS, MicS, NemeSys 以及 HIS。除了一般的惡意程式之外，較不同一般的是會去監看所謂的 Dark IP/darknet 的活動。這些 IP 其實是已經 assign 出去，卻未被使用的 IP，而遭到惡意人士冒用。由於未被正式使用，一般也少去監控，遂成為惡意程式防禦的漏洞。此系統亦監看 IoT 網路的攻擊，在四個月期間就觀察到來自 150,000 個 IP 的攻擊，並歸納成 361 種模式，足見 IoT 的安全議題，日益嚴重。

除了資安外，NICT 也投入人工智慧方面的研究，尤其在偵測腦波訊號用來形塑出眼睛看的物體形象，投入甚多。其目前最佳案例，雖然距離真實畫面還有段差距，但以可以辨識出類似的形體！



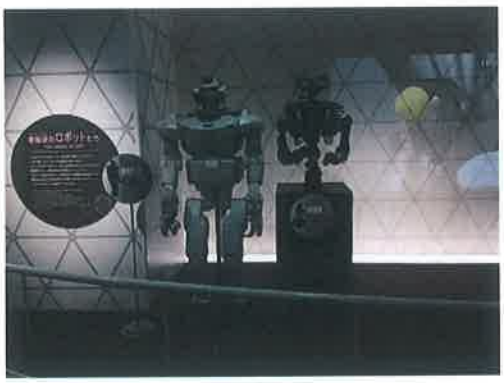
(四)參訪產業技術總合研究所(National Institute of Advanced Industrial Science and Technology, AIST)

AIST最早可追溯至1882年之農商務省地質調查所，歷經數次組織擴編及改革，於2001年4月統籌通商產業省工業技術的15個研究所及計量教習所，成為獨立行政法人產業技術總合研究所，並於2015年更名為國立研究開發法人產業技術綜合研究所。AIST是日本國內最大的公家研究機構，致力於將對於日本產業及社會有實際效用的技術加以實用，並作為創新技術商業化的橋樑。為達到此目標，AIST集合核心技術，並在體制上成立了「五大領域兩個綜合中心」以發揮綜合技術能力，於全日本有10個研究據點，共包含約兩千

名研究人員配合不斷變化的創新環境，並以國家戰略作為基礎，進行國家級創新前導研究。

AIST 的參訪，也是由該單位過往成果展示開始。以 Neuro Communicator 而言，其重點在應用腦波，協助肢體障礙者可以做到常人的活動能力。該計畫提供了 brainwave-based brain-machine interface (BMI)，作為腦波驅動機械的介面，可以提供”感覺”與聯繫照顧者及家人。另一項引起筆者興趣的是合成光線計畫，屬於綠能計畫的一部份，相較於日光，人工合成光線的重點在於尋找材料，用來產生氫，用來儲存能量，屬於綠能產業的一部份。目前已有技術上的突破，但要能變成量產，還有一段長遠的研發有待完成。

AIST 在機器人方面，也提供了幾個原型機種，供參觀。雖是原型機，尚不具實用價值，但其意圖非常明顯地朝向仿生機器人方向發展。



AIST 由 Dr. Yoshio Tanaka 介紹其在熱門科技議題方面的努力，其重點在於 Robotics, Artificial Intelligence 以及 Cyber Physical System 。同時，AIST 將在 2017 年完成 AI 基礎環境設施，提供至少 130～200PF 的運算能量，加速 AI 發展，其設計是將 Big Data 以及 HPC 結合，作為提供 AI Cloud 研發的基礎。此外，AIST 研究人員也相繼介紹的在作業系統端的研發，包括 Trusted Boot, Micro-Reset Kernel(MiRK)等，這些技術的應用都是以 IoT 裝置為目標。其中 MiRK 以實際運用於監測網路的實測中。

參、心得及建議事項

(一)成果發表會，除了再次檢討執行中的計畫進度與成效之外，也藉機讓6個計畫團隊互相觀摩，瞭解各自計畫的框架與發展進度，作為未來國際合作計畫的重要參考。在參訪方面，三個單位各有其特色與發展方向。資安和人工智慧等，都是各單位結合大資料成果的未來發展重點。這些方向與我國相同，惟在作法上仍有差異。日方於投入資源時，都是大量資源匯集，提供無後顧之憂的研發環境，其研發議題著眼於長遠發展，較少放眼於短期回收，各部門有其執掌分工，方能發揮綜效。

(二)成果發表會大致可為2大重點，「物聯網安全保護技術」及「跨國合作」。

1.物聯網安全保護技術：包含設備設計、監控技術建置、資料收集、對蒐集資料的去識別化技術，及針對已去識別化資料的分析技術，達到具資料隱私保護之資料分析與探勘。

2.跨國合作擴大國際視野：各團隊報告，對於跨國合作的過程中如何確保個資保護兼顧技術交流，同時符合相關法規，應皆是各計畫團隊在後續合作過程中要特別注意之處，例如資料蒐集會涉及到個人敏感資料，依我國個人資料保護法第21條規定，非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：①涉及國家重大利益；②國際條約或協定有特別規定；③接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞；④以迂迴方法向第三國(地區)傳輸個人資料規避本法。因此，各計畫團隊所蒐集之個人敏感資料不可跨國傳輸及分析，但可進行相關技術交流，故未來期待臺灣團隊之技術可置於日本，日本技術亦可應用於我們的場域，而各國可於自己國家領域內，應用交流的技術自行進行資料分析，俾利進行技術驗證。

(三)KDDI參訪，瞭解KDDI發展依據與背景，其中KDDI之短中長期目標可作為日後研究參考。

(1)相關技術現況：含區塊鏈、秘密分享、去識別化、物聯網應用在車載隨意行動網路(Vehicular Ad-hoc Network，以下簡稱為VANET)等技術。

(2)洽談可能的人才交流機制：KDDI提供各國學生、學者及技術人員之短期

交流與實習方案，可直接與KDDI研究單位進行3至6個月的合作，此可作為計畫團隊與之合作及交流的機會。

(四)NICT參訪，展示區展示最新技術，最驚豔的為視覺化技術應用於地理資訊系統(Geographic Information System，即GIS)、防災、地科教育課程、資安情資分析平台，是類大數據視覺化技術做得非常好，可凸顯問題及發現問題。使用物聯網技術作創新應用：例如應用在氣味模擬系統、語音翻譯平台(VoiceTra)、擴增實境應用等，另外3D建模模型未來可應用在健康照護之生理量測數據視覺化呈現技術。情資視覺化平台：NICT介紹了三個情資視覺化平台，分別為「NIRVANA改」、「DAEDALUS」及「NICTER」。「NIRVANA改」專注於從資安監控中心(Security Operation Center，即SOC)收集之Log進行視覺化分析，主要針對APT攻擊之Log資料；「DAEDALUS」主要觀測組織內部及外部惡意程式感染活動；「NICTER」收集暗網(Dark Net)資料進行物聯網連接埠(Port)的封包分析。此類研究主題，應可與國研院國家高速網路與計算中心及財團法人資訊工業策進會合作。

(五)AIST 參訪，展示區應用了許多物聯網技術，最為驚豔的為隨身導覽系統，提供適地性及情境式導覽服務。物聯網技術用於健康照護：含腦波、語意協助等。機器人發展：機器人應用於長期照護及相關自動化。技術交流：著重於物聯網於VANET之應用、安全硬體模組應用於物聯網設備之設計(HSM及TPM)、機器人AI發展趨勢，皆為務實之研究發展策略，除了相關演算法設計，都會具體實踐及應用與考量實際場域，可做為研究之借鏡。而參觀了AIST的機房，看到了機櫃防地震裝置、防水裝置、空調及消防系統等符合TIA-942、ISO27001等標準之措施，亦可為建置精密機械的參考。