財團法人電信技術中心出國報告

赴日拜訪國立研究開發法人情報通信研究機構（NICT）、電信業者 NTT DOCOMO 及第五代行動通訊推動論壇（5GMF）

單位名稱：國家通訊傳播委員會　　鄧惟中委員
財團法人電信技術中心　　吳宗成董事長
財團法人電信技術中心　　范俊逸執行長
財團法人電信技術中心　　郭作麟代理主任
財團法人電信技術中心　　林高裕代理主任
財團法人電信技術中心　　陳佳瑀副管理師

派赴國家：日本 東京

出國期間：**109** 年 **2** 月 **9** 日**-109** 年 **2** 月 **13** 日

報告日期：**109** 年 **5** 月 **5** 日

摘要

為推動 5G 建設、掌握物聯網應用及網路安全趨勢，國家通訊傳播委員會及財團法人電信技術中心以技術交流為主軸，派員赴日參訪國立研究開發法人情報通信研究機構（NICT）以了解日本最新資通訊安全防護系統；參訪電信業者 NTT DOCOMO 及其設置之 PLAY 5G，以觀摩日本 5G 應用實證場域；參訪促進 5G 創新技術研發、國際標準研析及合作等工作之第五代行動通訊推動論壇（5GMF），以參考日本推動 5G 發展之策略；同時，拜會我國台北駐日經濟文化代表處，並獲代表處提供之日本物聯網及電信產業相關資訊，以助益中心未來推展日本業務，及結交國際研究夥伴。

目次

壹、目的

2020 年全球行動通訊服務跨入 5G 時代，日本、南韓、美國及歐洲各大科技強國無不積極發展 5G 產業。值此數位科技快速演變之際，我國亦於今年 2 月完成 5G 頻譜釋照競標作業，進入 5G 商轉元年。

釋照後，國家通訊傳播委員會（以下簡稱通傳會）持續進行頻譜整備及頻段改善措施；而得標之電信業者，將挹注大筆資金布建 5G 網路基礎建設。由政府與民間企業共同合作，完善我國行動上網環境。在未來，5G 超高速、大頻寬、高密度及低延遲之特性，將提升物聯網、人工智慧及大數據分析之服務品質，影響範圍廣及娛樂、農牧、醫療、教育、零售、觀光、製造及交通各產業，引領民眾進入創新科技應用之新紀元。

為推動 5G 建設、掌握物聯網應用及網路安全趨勢，通傳會及財團法人電信技術中心（以下簡稱中心）派員參訪全球 5G 技術發展名列前茅之日本，原預定於 2020 年 7 月舉辦之日本東京奧運，更是 5G 應用之最佳展示。本次赴日參訪以技術交流為主軸，拜訪 NICT 以了解日本最新資訊及通訊安全防護系統；拜訪 5GMF 以參考日本推動 5G 發展之策略；參訪 NTT DOCOMO 及其設置之 PLAY 5G，以觀摩日本 5G 應用實證場域；同時，拜會我國台北駐日經濟文化代表處，並獲代表處提供之日本物聯網及電信產業相關資訊，助益中心未來推展日本業務，及結交國際研究夥伴。

中心以電信與通訊技術為核心開創業務版圖，主要包含：資訊安全防護與通訊設備檢測驗證服務，市場趨勢調查與法規政策研析，應用系統開發與提供平臺服務等。時逢各國政府、電信營運商、產品設備供應鏈及應用服務平臺不斷探究 5G 應用之可能性，中心亦投入人力與蓄積多年之技術研發能量，協助通傳會健全我國 5G 發展環境、活絡市場機能，讓民眾享有更好、更快、更安全之電信服務。

貳、行程

一、出國時間：109 年 2 月 9 日至 13 日

二、地點：日本東京

三、出席人員：

（一） 國家通訊傳播委員會　　鄧惟中委員
（二） 財團法人電信技術中心　　吳宗成董事長
（三） 財團法人電信技術中心　　范俊逸執行長
（四） 財團法人電信技術中心　　檢測暨網通技術組　郭作麟代理主任
（五） 財團法人電信技術中心　　資通安全組　林高裕代理主任
（六） 財團法人電信技術中心　　行政組　陳佳瑀副管理師

四、行程安排：

日期	時間	行程	行程說明
2 月 9 日（日）	09:00 12:40	前往日本 臺北松山→ 東京羽田	
	18:00 20:30	GCC Tokyo 2020	Ice Breaking Gathering
2 月 10 日（一）	09:00 12:30	GCC Tokyo 2020	Opening Session
	15:00 17:00	NICT	<u>交流分享</u> 1. 5G & IoT 技術及業務交流 2. MOU 內容討論
2 月 11 日（二）	13:00 17:00	PLAY 5G	<u>應用體驗</u> PLAY 5G 為日本重要電信營運商 NTT DOCOMO 所規劃之 5G 應用展示，體驗超高速、大容量、低延遲之 5G 應用服務。 展示項目包含： ➢ 2020 奧運應用體驗 ➢ 垂直應用體驗
2 月 12 日（三）	12:55 15:00	NTT DOCOMO	<u>應用體驗</u> ➢ Solution Room Tour（參觀 AR / VR） <u>交流分享</u> ➢ DOCOMO Activities for

日期	時間	行程	行程說明
			Connected Vehicle ➢ DOCOMO 5G Related Activities for Industry
	15:30 17:30	5GMF	<u>交流分享</u> ➢ Activity Report 2019 from 5GMF（Examination status of IoT, Connected Vehicle, and Fintech） ➢ Presentation from TTC
2 月 13 日（四）	10:00 12:00	台北駐日經濟文化代表處	<u>交流分享</u> ➢ 日本 5G、IoT 發展現況 ➢ 日本資通訊政策 ➢ 提供與日本資通訊研發及學術機構交流之建議？ ➢ 有關於日本設立辦事處，代表處提供建議及相關流程說明
	17:45 20:55	返回臺灣 東京成田→ 臺北桃園	

參、會議過程及內容

一、GCC Tokyo 2020

（一） 會議時間：

109 年 2 月 9 日 18:00 至 20:30

109 年 2 月 10 日 09:00 至 12:30

（二） 會議地點：X Wave Funabashi

（三） 會議內容：

Global Cybersecurity Camp（以下簡稱 GCC）是由臺灣 Advanced Information Security Summer School （AIS3）、日本 Security Camp Committee、南韓 KITRI BoB Programme 及新加坡 Division Zero （Div0）四個國家級資安培訓組織，以培育新一代資安人才及促進國際資安社群交流為目的，於 2018 年共同成立。每年由四國輪流主辦，以資訊安全技術為核心，制定當年度之訓練內容，參加者以資安領域內具優秀潛力之高中職與大學生為主。

本次參加日本 Security Camp Committee 主辦之 GCC Tokyo 2020，是由各國資安領域內具實務經驗之年輕學者擔任訓練員，訓練主題包含機器學習、弱點掃描及滲透測試、資安事故應變、攻擊行為分析以及社群媒體之資安防護等。參加者來自臺灣、南韓、泰國、越南、新加坡、馬來西亞及澳洲 8 國，GCC 依國籍將參加者打散分組，透過團隊合作及實戰演練進行技術交流，進一步提升其資安防禦之實務能力，同時也讓來自不同國家之參加者建立起友誼。

中心於電信技術及資安防護領域深耕多年，對技術傳承及人才培育多有想法，藉此機會觀摩國際資安社群如何培訓人力；此外，本次參加 GCC 發現資安產業人才之性別比例差距極大，在與會的 8 個國家之中，除臺灣隊有女性團員參與之外，其他僅有 1、2 位女性團員。未來，中心思考與國內大專院校產學合作，培養優秀即戰力，也將特別注重性別比例之均衡。

圖 1：GCC 交流合影並接受日本媒體訪問
（資料來源：財團法人電信技術中心）

二、NICT Cybersecurity Research Institute

（一） 會議時間：109 年 2 月 10 日 15:00 至 17:00

（二） 會議地點：NICT 會議室

（三） 會議內容：

國立研究開發法人情報通信研究機構（National Institute of Information and Communications Technology，以下簡稱 NICT）隸屬日本總務省（Ministry of Internal Affairs and Communications，MIC），為日本 ICT 領域內唯一國家級研究中心，其設立宗旨為：持續發展資通訊技術以建立人類幸福，促進 NICT 的研究與發展，以及與產業界、學界之合作與支援。

本次與 NICT 雙邊交流之主軸有二，一為針對中心及 NICT 之資安研究成果進行簡報，二為針對雙方未來合作項目進行討論，就可實質合作之內容，規劃簽署 MOU 的期程。交流開始，由中心吳宗成董事長及 NICT 的傑出研究員中尾浩二先生（Koji Nakao，Distinguished Researcher）分別開場並介紹兩邊出席人員，再由 NICT 網路安全實驗室（Cybersecurity Laboratory）室長井上大介博士（Daisuke Inoue，Director of Cybersecurity Laboratory）分享簡報。

圖 2：於 NICT 會議室進行業務交流
（資料來源：財團法人電信技術中心）

井上博士首先介紹日本政府與網路安全（Cybersecurity）相關之機關單位及受其管轄之組織（如下圖 3）；其中日本國家資訊安全中心（National Center of Incident readiness and Strategy for Cybersecurity，NISC）為其相關組織運作之總部

（Headquarter），中尾先生同時也是 NISC 的顧問，並於多個組織中兼任要職，包含 NICT 傑出研究員、ICT-ISAC 之創辦人及顧問等。NICT 為日本總務省轄下之法人機構，本次拜訪單位為 NICT 底下的網路安全研究所（Cybersecurity Research Institute）。

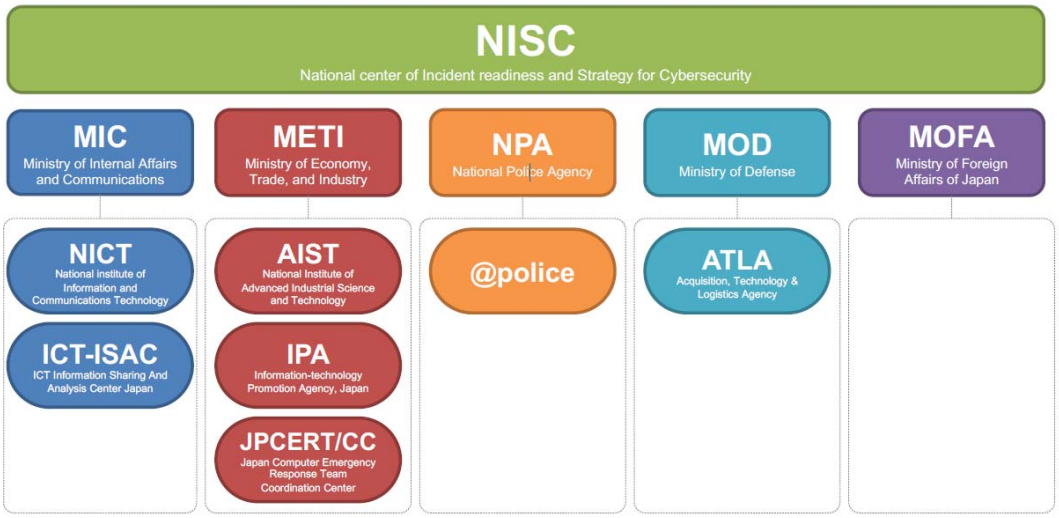

圖 3：網路安全相關之機關單位及受其管轄之組織（資料來源：NICT）

井上博士接著介紹 NICT 進行中之研究主題，分列如次：

- 日本標準時間（Japan Standard Time, JST）
- 光纖通訊（Optical Communication）
- 衛星通訊（Satellite Communication）
- 科學雲（Science Cloud）
- 遙測技術（Remote Sensing）
- 生物/奈米 ICT（Bio / Nano ICT）
- 腦部訊息接收設備/介面 ICT（Brain ICT）
- 語音多國語言翻譯器（Multi-lingual Machine Translation）
- 超現實通訊，電子化全息影像（Ultra-Realistic Communication）
- 網路安全（Cybersecurity）

在前述研究主題中，井上博士特別提及「語音多國語言翻譯器」，為一款免費、可即時翻譯 31 種語言之工具 APP，適用於 Android 及 iOS 兩種平臺；而他所帶領的實驗室主要進行「網路安全」研究，亦為今日欲分享之研究主題。

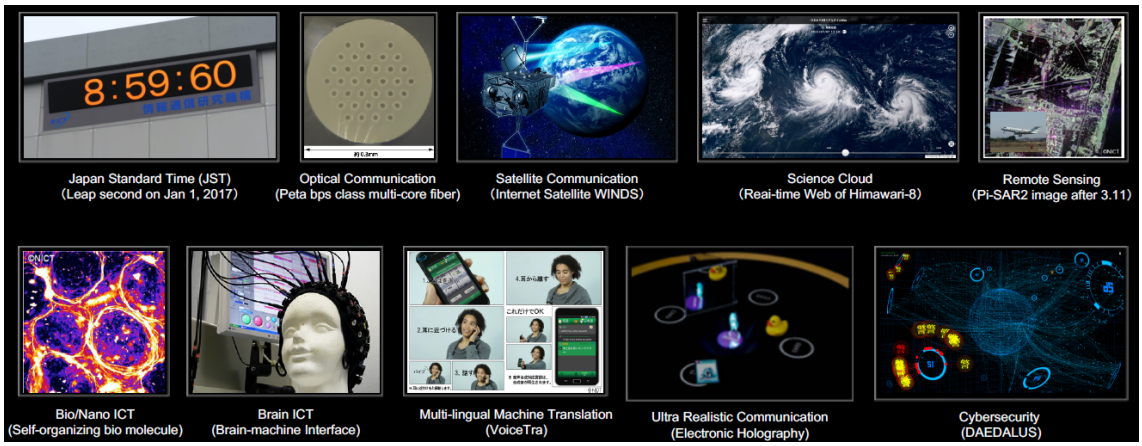

圖 4：NICT 之研究主題（資料來源：NICT）

研究並強化「網路安全」，為網路安全研究所之主要任務。其研究所設有兩個實驗室，分別為由井上博士帶領的網路安全實驗室（Cybersecurity Laboratory），以及由 Ryo Nojima 博士（Director of Security Fundamentals Laboratory ）帶領的安全基礎實驗室（Security Fundamentals Laboratory）。本次拜訪對象為網路安全實驗室，是由研究團隊（Research Team）、分析團隊（Analysis Team）、以及開發團隊（Development Team）共同組成，以發展高度應用及大數據分析相關之網路安全研究為主，利於及時掌握、密切分析並提供有效對策，以因應不斷演進之網際網路攻擊。簡要分述如下：

✓ 研究團隊（Research Team）

研究團隊具有世界級基於大數據的進階應用研究能量。

✓ 分析團隊（Analysis Team）

分析團隊主要針對大量數據且橫跨異質性資料，於蒐集數據後進行全面性精準分析，以提供內部與外部需求。

✓ 開發團隊（Development Team）

內部系統（In-house System）之開發與監控，同時發展系統視覺化呈現相關技術。

參訪過程中，井上博士特別開啟數據分析研究室的實驗場域，以展示研究人員如何進行威脅分析及其分工，例如：透過 3D 圖形化示意，系統性地呈現攻擊資訊、告警資訊……等。針對發生於日本的資安威脅活動及其應變措施，NICT 研發出被動式 NICTER 與主動式 NOTICE 兩種偵測機制（其運作架構如下圖 4），井上博士亦進一步介紹 NICTER 及 NOTICE 之應用。

圖 5：井上博士介紹數據分析研究室
（資料來源：財團法人電信技術中心）

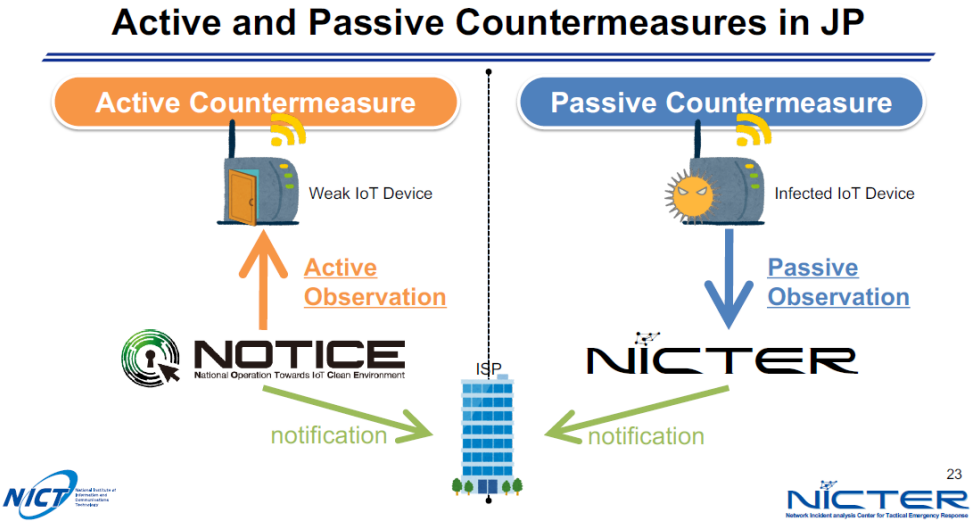

圖 6：NOTICE 及 NICTER 之運作架構（資料來源：NICT）

- NICTER：Network Incident analysis Center for Tactical Emergency Response

NICTER 使用網路安全實驗室的 Darknet 系統蒐集資料，並以 3D 展示世界地圖上來自各地對日本的攻擊。Darknet 之運作，是將系統布建在組織中未使用的網際網路 IP 上，這些 IP 理應無法與任何外部連網主機進行連線（包含連入與連出），然而實際運作時卻有極少數 IP 連線至 Darknet 系統，由 Darknet 系統接收這些封包後，再進一步分析其包含或可能衍生之惡意行為。透過 Darknet 的流量資訊，NICT 可快速掌握全球網際網路之威脅活動趨勢。

圖 7：井上博士介紹 NICTER 之運作
（資料來源：財團法人電信技術中心）

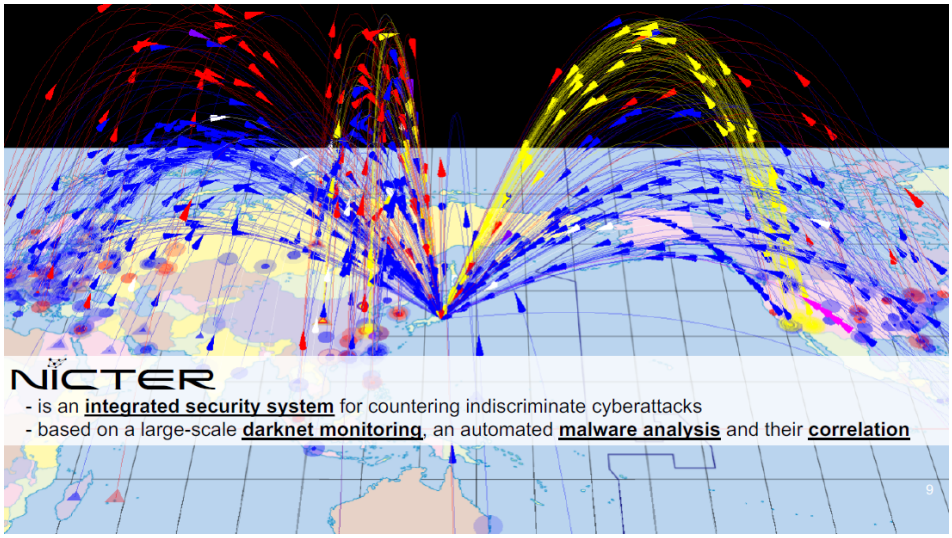

圖 8：NICTER 以 3D 影像顯示來自各地的資安攻擊（資料來源：NICT）

根據 NICT 2005 年至 2018 年統計的流量資訊顯示，自 2015 年開始 Darknet Traffic 大幅度成長且逐年上升；由 2018 年流量資訊顯示，30 萬個 Darknet IPs 蒐集到 2121 億封包數，平均每一個 Darknet IP 可蒐集到 789,876 封包數（如圖 9）。

Year	Number of packets par year	Number of IP address for darknet	Number of packets par 1 IP address per year
2005	0.31 billion	16 thousands	19,066
2006	0.81 billion	100 thousands	17,231
2007	1.99 billion	100 thousands	19,118
2008	2.29 billion	120 thousands	22,710
2009	3.57 billion	120 thousands	36,190
2010	5.65 billion	120 thousands	50,128
2011	4.54 billion	120 thousands	40,654
2012	7.79 billion	190 thousands	53,085
2013	12.9 billion	210 thousands	63,655
2014	25.7 billion	240 thousands	115,323
2015	54.5 billion	280 thousands	213,523
2016	128.1 billion	300 thousands	469,104
2017	150.4 billion	300 thousands	559,125
2018	212.1 billion	300 thousands	789,876

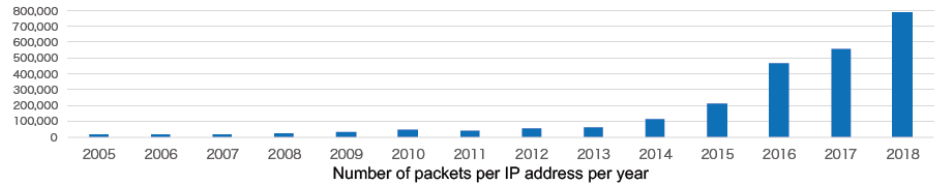

圖 9：由 Darknet 所蒐集之流量資訊（資料來源：NICT）

- NOTICE：National Operation Towards IoT Clean Environment

NICT 自 2019 年 2 月起啟動 NOTICE 計畫，其執行方式是透過 96 組 IP，主動對日本境內所有的物聯網裝置進行偵測及掃描，以分析是否存有漏洞、弱密碼以

及缺乏基本防護措施之情形。為順利執行 NOTICE 計畫，日本特別修訂了「國家資通訊技術研究所修正案（Amendment of act on the National Institute of Information and Communications Technology）」，該修正案為一特別法、凌駕於通用法「禁止未經授權的電腦存取法令（Act on Prohibition of Unauthorized Computer Access）」之上，使 NICT 具備有法源依據，可以主動偵測與掃描日本境內所有的 IoT 裝置（包含網路 IoT 設備），以偵測未經授權的 IoT 裝置。

日本橫濱大學將受影響的 IoT 裝置進行分類，包含：監控攝影機、網通裝置、電話、基礎設施、控制系統、家庭及個人、廣播類、以及其他非上述分類的裝置。而從井上博士分享的屬於 IoT 情境威脅的分析報告中可發現，透過統計 NICT 在 2018 年所偵測及蒐集到的威脅活動中，前 30 名受攻擊對象有 47.7%為與 IoT 相關的通訊埠（Ports）。

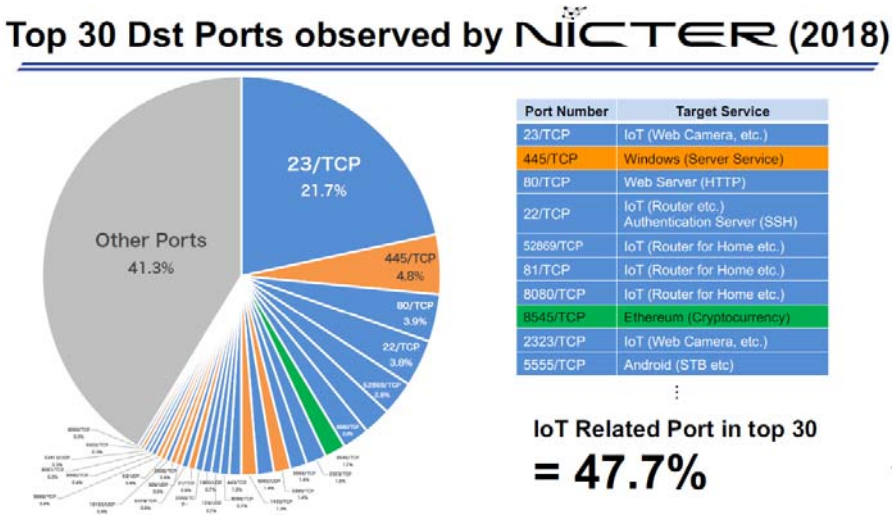

圖 10：受攻擊對象以 IoT 相關之通訊埠為主（資料來源：NICT）

NICT 藉由監控並追蹤裝置被感染的情形，於 2017 年的 6 月發現日本電信營運商 NTT DOCOMO 的 Mobile Router 的漏洞，並於同年 11 月發現 Logitec 的 Home Router 的漏洞，是第一個發現此二漏洞的研究團隊。

圖 11：日本受感染之裝置（資料來源：NICT）

此外，NICT 亦與 ICT-ISAC 及 JPCERT/CC 共同合作，將 IoT 裝置之弱點資訊有效地傳遞給設備製造商及使用者。首先由 NICT 蒐集並分析漏洞調查之結果，再將情資分享給兩個單位，接著由 JPCERT/CC 將漏洞情形通報給設備製造商，並由設備製造商提供解決方案給終端使用者；其次，透過 ICT-ISAC 分享情資給 ISP 業者，並協助 ISP 業者了解與釐清受感染裝置之情形。

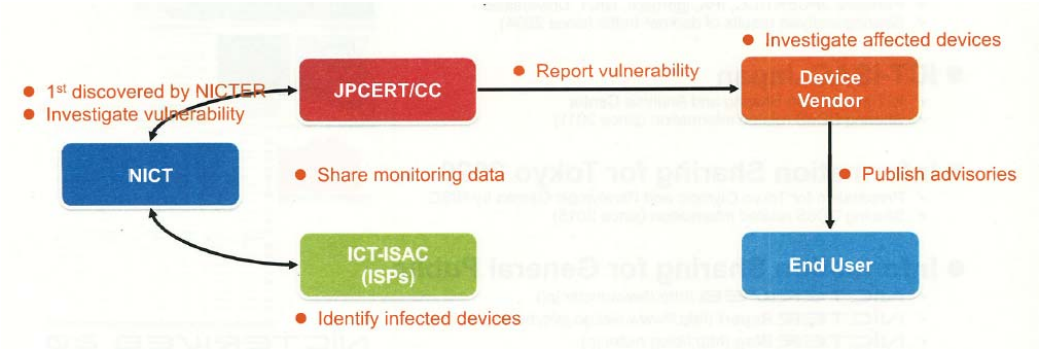

圖 12：NICT 與 ICT-ISAC、JPCERT/CC 之合作模式（資料來源：NICT）

囿於時間因素，由井上博士說明 NICT 之技術研發成果，並展示其網路攻擊監測系統後，接著就由郭作麟主任介紹中心檢測驗證實驗室的服務內容與技術能量，並進一步解說中心未來在 5G 應用方面，有關效能評估的發展方向。此外，林高裕主任亦針對中心資通安全研究的任務主軸，包含擔任政府資安智囊、資安評估與檢測實驗室、研究與發展近況等進行說明。中心亦向 NICT 提出合作邀請，

討論於臺灣網際網路環境合作建立 Darknet 系統之可行性，如未來可共享威脅情資，對提升日本與臺灣網路資安防護的能力將大有助益。范俊逸執行長亦邀請中尾先生與井上博士到臺灣參加由中心舉辦之工作坊，並將於工作坊中討論未來中心與 NICT 網路安全研究所合作之方向。

圖 12：與 NICT 交流及合影
（資料來源：財團法人電信技術中心）

圖 13：與 NICT 交流及合影
（資料來源：財團法人電信技術中心）

三、PLAY 5G Enjoy the future

（一） 參觀時間：109 年 2 月 11 日 13:00 至 17:00

（二） 參觀地點：東京晴空塔 PLAY 5G

（三） 參觀內容：

PLAY 5G 是由日本電信營運商 NTT DOCOMO 與不同產業的企業夥伴合作，結合擴增實境（Augmented Reality，AR）、虛擬實境（Virtual Reality，VR）、4K/8K 影像傳輸技術與 5G 超高速、超低延遲之通訊特性，於東京晴空塔設置的 5G 實證場域。透過 WiFi 模擬 5G 聯網環境，展出多項 5G 應用實例，包含：2020 奧運應用體驗、利用 VR 觀賞運動賽事與競賽體驗、5G 垂直應用及遠端機械工程技術等，如同其展場名稱「PLAY 5G Enjoy the future」，讓民眾體驗虛擬與真實結合的未來世界。簡述展項如次：

- Magic Leap One：

Magic Leap One（如圖 14）利用 5G 超高速、大容量、低延遲與多連接的特性，透過穿戴裝置結合現實環境與 AR，是一款沉浸式遊戲，讓參觀者體驗混合實境（Mixed Reality，MR）之應用。

圖 14：Magic Leap One（資料來源：PLAY 5G）

➢ Pocket Avatar

Pocket Avatar 利用掃描儀掃描參觀者全身後，創造出小型的 3D 人形，並以專屬 APP 為 3D 人形添加「飛」和「旋轉」等動作，製作成動態貼圖以及 AR 照片，下載後可用於 Line 或其他通訊軟體。

圖 15：Pocket Avatar（資料來源：PLAY 5G）

圖 16：體驗 Pocket Avatar 製作的 AR 照片及動態貼圖
（資料來源：財團法人電信技術中心）

➢ High Reality Remote Ensemble

利用 5G 超低延遲的特性，參觀者透過 5G 行動裝置，將彈奏樂器的視訊及音訊傳送至遠端，享受零時差的異地樂器合奏。

圖 17：體驗 High Reality Remote Ensemble
（資料來源：財團法人電信技術中心）

- Remote Control of Construction Machinery

利用 5G 低延遲的特性，參觀者透過互動式影片，體驗遠程控制高精細的大型工程機械，模擬無人駕駛的挖土機在具有潛在危險性的工地施作。

圖 18：體驗 Remote Control of Construction Machinery
（資料來源：財團法人電信技術中心）

- Cyber Wheel

利用 5G 超高速與超低延遲的特性，參觀者藉由 VR 眼鏡及 Cyber Wheel 成為輪椅賽車手，比賽路線融合淺草，澀谷，台場等著名景點，以及東京馬拉松路線的 3D 影像，在輪椅競速的同時享受觀光樂趣。

圖 19：Cyber Wheel（資料來源：PLAY 5G）

- 8K 影像通訊應用

利用 5G 超高速及大容量傳輸特性，傳送高精細、具臨場感的 8K 影像，使人如臨現場，可多方應用於運動賽事直播、遠距醫療、人臉識別等。

圖 20：日本總務省 5G 綜合實證，試驗在人口密集地達成 8K 影像平均 4-8Gbps 的超高速傳輸速度（資料來源：財團法人電信技術中心）

除前述展項之外，PLAY 5G 活用 5G 超高速、低延遲的通訊傳輸技術，讓身處不同空間的參賽者，也可於同一個 VR 空間中進行如賽馬、西洋劍等運動賽事，透過 360 度高精細的影像，在虛擬與現實的完美融合之中，體驗對戰的精彩與刺激。同時，VR 也將應用於觀賞東京奧運及其他運動賽事，通過 5G 穩定而快速地傳送大容量影像資訊，給予高臨場感的觀戰體驗。

圖 21：東京晴空塔 PLAY 5G 參觀及合影
（資料來源：財團法人電信技術中心）

四、NTT DOCOMO

（一） 會議時間：109 年 2 月 12 日 13:00 至 15:00

（二） 會議地點：NTT DOCOMO 總部

（三） 會議內容：

NTT DOCOMO 為日本規模最大、用戶數最多且歷史最為悠久之電信業者，於 2014 年開始測試 5G 關鍵基礎技術，試驗 5G 的高移動性及覆蓋率，並於 2017 年 8 月宣布其「Toward 2020 and Beyond」策略，包含在東京台場及晴空塔設置 5G 測試點、布建 5G 商業系統，並與不同產業的企業結盟、成為開放式合作夥伴，一同挑戰 5G 創新應用之可能性。今年 3 月，NTT DOCOMO 開通 5G 商用，提供高速行動寬頻，並與其企業夥伴共同為消費者帶來跨界、創新之加值服務。本次特別安排參訪 NTT DOCOMO，以了解其 5G 技術之發展情形。

抵達 NTT DOCOMO 後，由其接待人員帶領進入安全閘門並搭乘電梯至其公司大廳。不愧為日本最大之電信營運商，接待大廳的員工均穿著整齊乾淨的制服，宛如置身於大型百貨公司，專業、親切的服務態度是對其的第一個印象。另外，接待大廳有著許許多多的訪客，包含：設備供應商、服務供應商及其它配合協力廠商等……，陣容之大使人印象深刻。

隨後，我們被引領至 NTT DOCOMO 的 5G 示範場域，該場域一共建置 20 個 5G 應用示範，我們亦實際體驗了其中二個應用情境。其中之一項是「今歸仁城 VR」，是由 NTT DOCOMO 與沖繩觀光局合作開發，透過 5G 加上 VR/AR 技術，讓造訪今歸仁城的日本學生學習相關歷史。今歸仁城被列為世界遺產，是日本沖繩著名的觀光景點，沖繩過去由琉球王國統治，今歸仁城是琉球王國三山時代中北山王的領地，為一舊時城堡遺跡。該應用情境重現古城的 4K 影像，透過 VR 眼鏡，讓使用者身歷其境地體驗歷史裡的城牆與戰場上的短兵相接。此外，藉由 5G 大頻寬的無線傳輸與 AR 技術，與遠端專家共享平板電腦屏幕，學習史蹟與出土文物的相關知識，進行即時遠距離教學。

圖 22：今歸仁城 VR（資料來源：NTT DOCOMO）

另一項 5G 應用服務的體驗為「Paddle VR」，透過穿戴 First VR 裝置，藉由划槳的手臂動作以控製 360 度高清影像。現場戴上安裝有 HMD 和配備肌肉位移感應的控制器進行划槳，在 VR 空間中感受到橡皮艇在水中前進，以及划槳時水的阻力，宛如自己真的划船穿梭在紅樹林之中一樣。NTT DOCOMO 的目標是利用 5G 和 H2L 的 Body Sharing 技術提供划船感覺的回饋，以實現即時的遠程旅遊體驗。體驗時，吳宗成董事長詢問穿戴式投影頭盔對色盲、弱視者是否有同等效果？NTT DOCOMO 表示以目前技術尚無法克服，但這是一個很好的研究思路，未來考慮進行相關研發。

圖 23：Paddle VR（資料來源：NTT DOCOMO）

體驗完 5G 場域垂直應用實例後，接著來到會議室與專家們交流有關 5G 的應用與發展。首先由 5G Laboratories 主管油川雄司博士（Yuji Aburakawa）介紹日本 5G 網路布建、服務規劃以及車聯網的發展情況。如圖 24 所示，NTT DOCOMO 從 2019 年起至 2023 年，以 5 年為期投入 100 億美元進行 5G 基礎網路建設。自 2019 年開始提供 5G pre-service，並將在 2020 年的東京奧運及殘障奧運中建構高密度的 WiFi 無線網路，同時提供 5G 通訊服務。

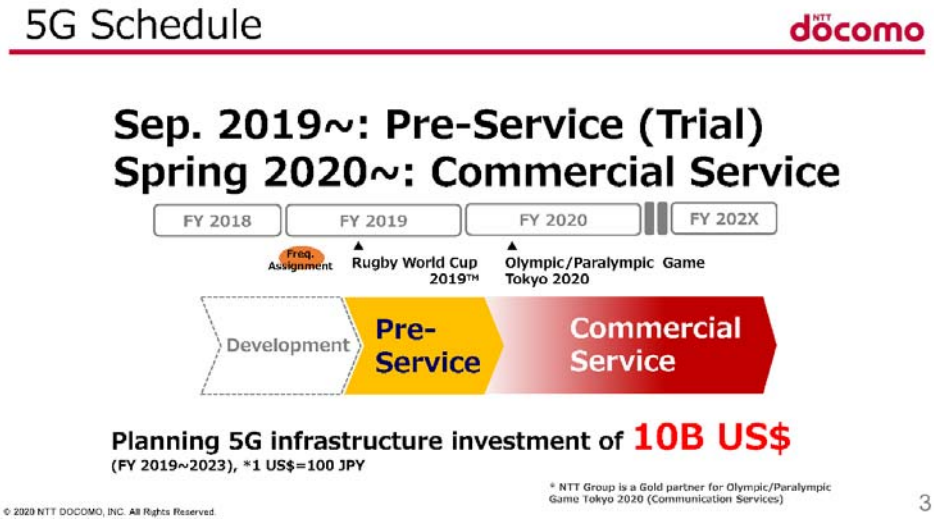

圖 24：NTT DOCOMO 之 5G 期程規劃
（資料來源：NTT DOCOMO）

藉由 2019 年 9 月 20 日世界杯英式橄欖球賽，NTT DOCOMO 針對 5G pre-service 展開一系列宣傳活動，提供 5G 解決方案及新服務體驗，並從 2020 年春季開始，全國性地從都會區到郊區，特別著重於工廠、醫院等，依頻寬及其功能性建置 5G，正式提供包含智慧交通、智慧製造、智慧城市、智慧農業及健康醫療照護等 5G 商用服務。

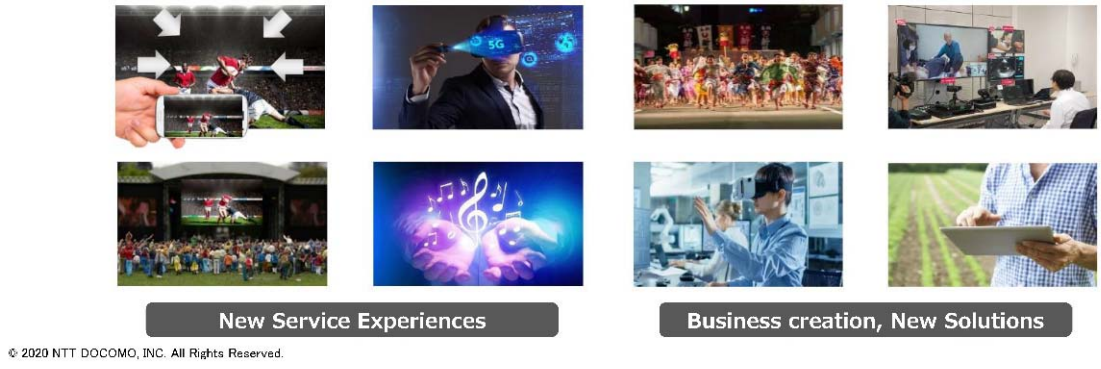

圖 25：NTT DOCOMO 將 5G pre-service 應用於英式橄欖球賽之轉播
（資料來源：NTT DOCOMO）

圖 26：NTT DOCOMO 之 5G 布建規劃（資料來源：NTT DOCOMO）

此外，NTT DOCOMO 是日本唯一以 3.7GHz、4.5 GHz 及 28 GHz 三個頻段建置 5G 電信網路之電信業者，其規劃 2020 年開始在日本 47 個專區進行 5G 網路建設，預計一年後 5G 基地臺的數量將超過 10,000 座，並在 2024 年完成 26,334 座 5G 基地臺建置作業。NTT DOCOMO 向日本總務省提出將整合全集團力量，並動用超過 10,000 名 5G 工程師，於 5 年內達成全日本 97.02%的網路覆蓋率，以滿足消費者對 5G 網路的期待。鄧惟中委員聽完後進一步詢問有關覆蓋率如何計算？油川博士解釋道，在都會區和郊區基地臺建置的密度不盡相同，因此十公里見方中有一個基地臺的話，就算有覆蓋。

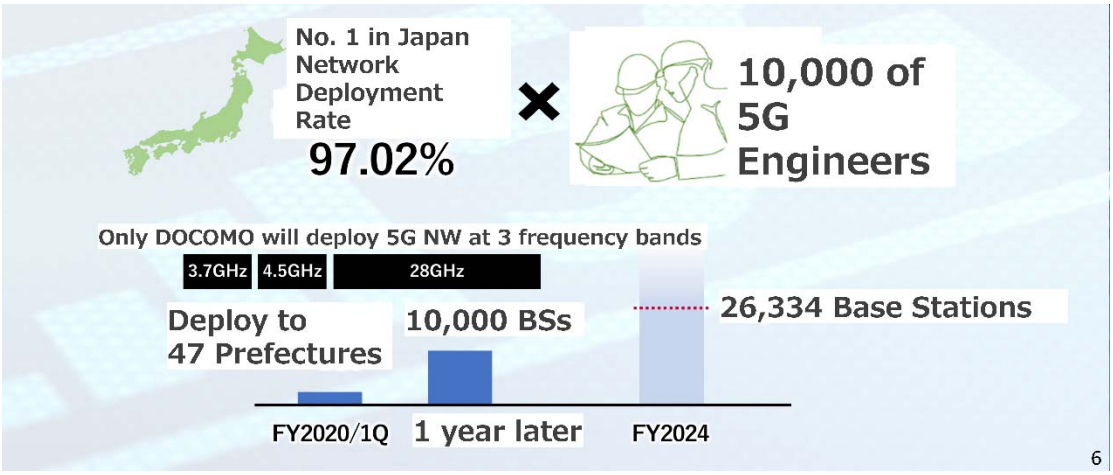

圖 27：NTT DOCOMO 之 5G 基地臺建置規劃（資料來源：NTT DOCOMO）

油川博士接著報告，NTT DOCOMO 在車聯網方面的規劃。NTT DOCOMO 與日本最大的電信協會及產業協會合作開發動態地圖，並依照不同的更新需求，將地圖區分為靜態圖層、準靜態圖層、準動態圖層及動態圖層，如交通號誌、行人及

障礙物等須在 1 秒內作即時資訊更新者，可透過車上感知器、OBU、RSU 達到即時通訊效果；其它通訊範圍較廣且對即時性要求較不高的圖資更新，則可透過 c-V2X 完成。

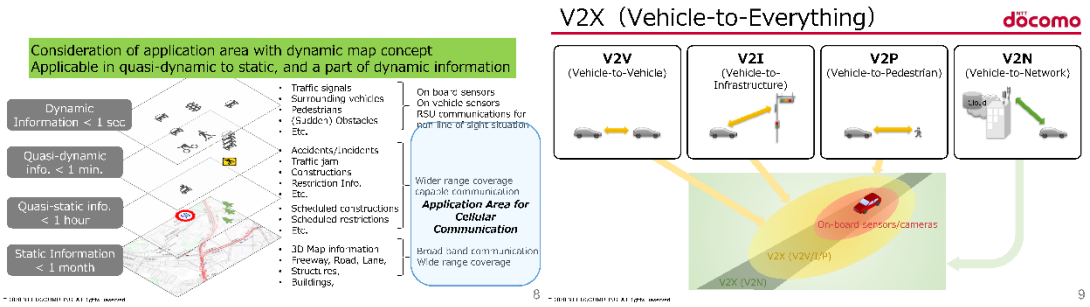

圖 28：動態地圖之圖層說明及 3GPP R14 之車聯網標準
（資料來源：NTT DOCOMO）

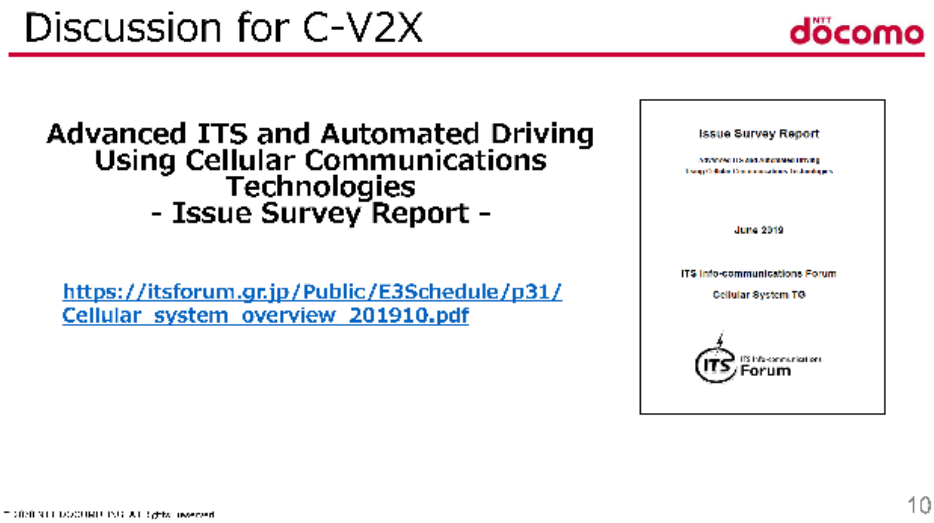

圖 29：日本於 2019 年 6 月透過 ITS Info-communications Forum 產出第一份自動駕駛 Survey Report
（資料來源：NTT DOCOMO）

另外，自 2018 年起 NTT DOCOMO 也與 Continental, Ericsson, Nissan, OKI 及 Qualcomm 等五大公司合作，建置日本第一座車聯網測試場域，其中使用了 R14 LTE 直接通訊（Direct Communication, V2V,V2I and V2P）及 DOCOMO LTE-A 網路（V2N），透過 5G 大頻寬、低延遲之特性，在東京遠端操控位於橫須賀測試場域的自駕車，以進行 Level-4 的遠端操控自駕車測試。由於自駕車上裝載之 5G 裝

置使用毫米波雷達，范俊逸執行長考量毫米波穿透力差，而車輛之包覆性強，詢問是否將影響測試結果？油川博士表示 NTT DOCOMO 與 AGC、Ericsson 合作，設計了全球第一個 5G 嵌入式天線貼片，貼於車窗上就如同一個小型移動基地臺，可強化 5G 通訊能力。

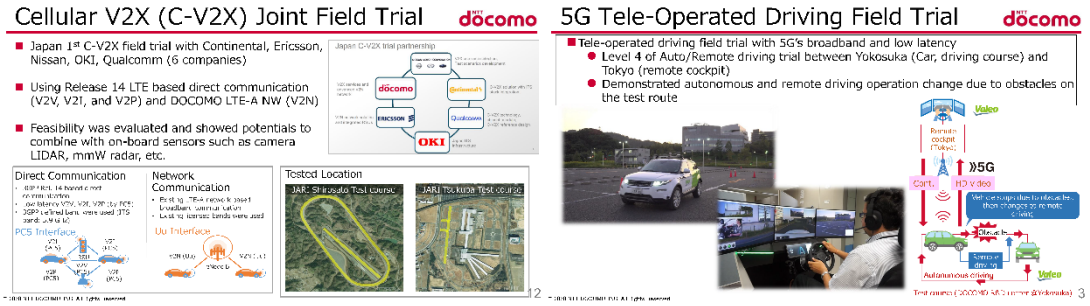

圖 30：5G 遠端操控自駕車之測試（資料來源：NTT DOCOMO）

在智慧製造產業之 5G 應用，NTT DOCOMO 也多有著墨，如圖 31 所示，與最大機器人製造商 FANUC、HITACHI、NOKIA 及 OMRON 有相關合作計畫，其戰略目標是達成無線化工廠，並可遠程操控工廠之運作。

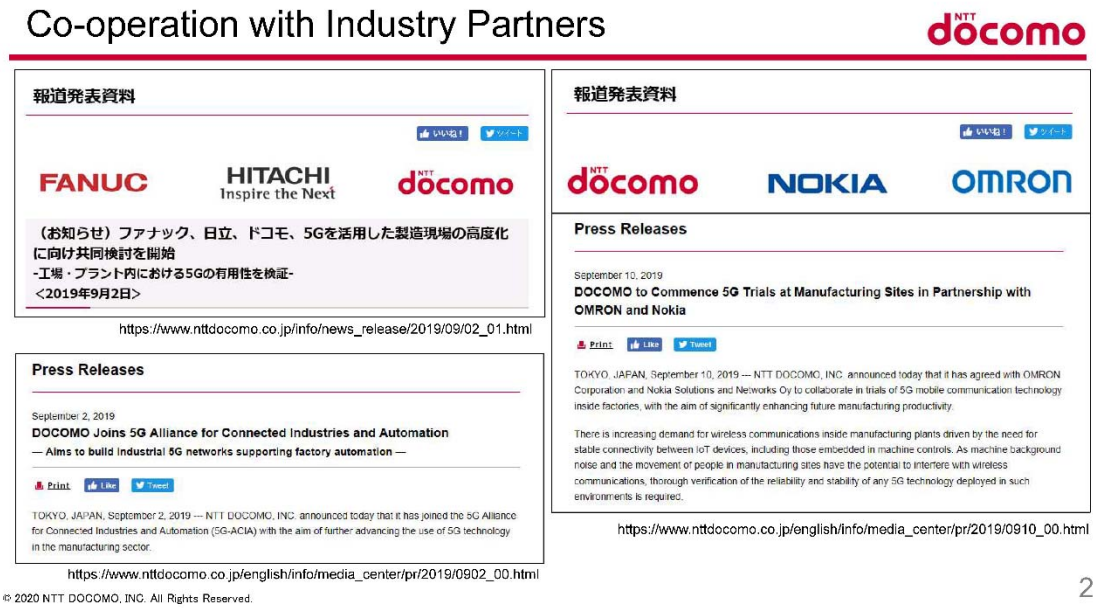

圖 31：NTT DOCOMO 智慧製造的合作夥伴（資料來源：NTT DOCOMO）

以 NTT DOCOMO 與 OMRON 合作為例，在 5G 創新服務上，進行智慧製造概念性驗證（PoC），藉由分析資深操作員動作以達成人機協作，並以自主性移動

機器人（Autonomous Mobile Robot, AMRs）串聯產線上的各個工作站，協助備料、補料及運送，大幅提升生產力，達到工廠生產線 Layout-free 的目標。

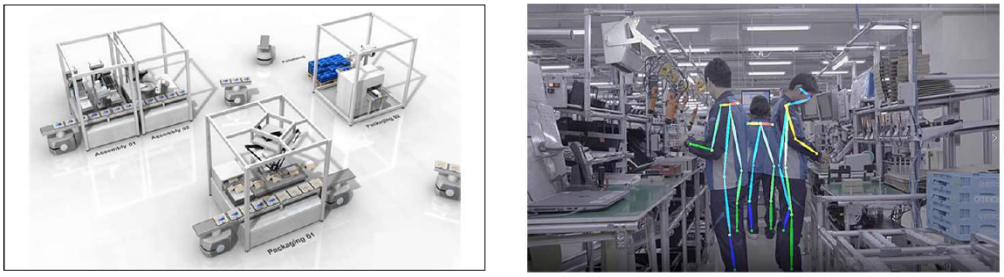

圖 33：NTT DOCOMO 與 OMRON 的概念性驗證（資料來源：NTT DOCOMO）

而 FANUC 是全世界工業機器人及 CNC 系統的最大製造商，於 2017 年發表其旗艦型 IoT 產品「FIELD System」開放平臺；HITACHI 則是日本大型跨國企業，業務包含 IT 系統、社會基礎建設、電力系統、電子系統、自動控制系統及鐵道工程等。如下圖 34 所示，NTT DOCOMO 與 FANUC、HITACHI 之合作以智慧工廠大數據分析為主，由於 FANUC 及 HITACHI 均有建置自己的平臺，可自主整合、蒐集資訊，其 5G 應用試驗聚焦於網路效能優化及機械自動化控制的正確性。

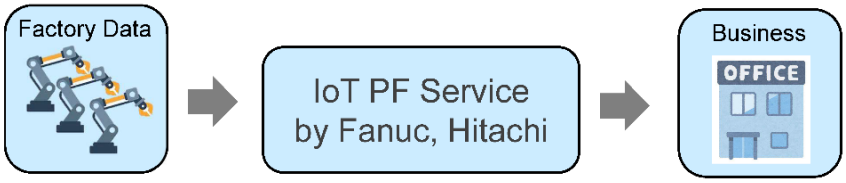

圖 34：NTT DOCOMO 與 FANUC、HITACHI 之合作（資料來源：NTT DOCOMO）

圖 35：與 NTT DOCOMO 交流及合影（資料來源：財團法人電信技術中心）

五、5GMF

（一） 會議時間：109 年 2 月 12 日 15:30 至 17:30

（二） 會議地點：ARIB 會議室

（三） 會議內容：

5G 行動通訊推論壇（The Fifth Generation Mobile Communications Promotion Forum，5GMF）成立於 2014 年 9 月，依日本政府 5G 建設之施政方針及全球 5G 發展趨勢，推動 5G 行動通訊系統相關研究。同時，5GMF 亦綜整 5G 發展動態，匯集產官學研專家學者之觀點出版白皮書，內容涵蓋 5G 應用程式、網路及無線技術革新等，並討論資通訊新興科技於各行各業中之新用途，為 5G 應用提供清晰目標，以健全電信產業環境、為人們創造豐富生活。

5GMF 首先為我們簡介其委員會運作模式、最新活動以及日本 5G 發展之總體現況。其成立之初設有戰略規劃委員會、技術委員會、服務和應用委員會、網路架構委員會等四個委員會，並於 2019 年 6 月增設資安研究委員會（Security Study Committee），及後來的區域使用促進委員會（Regional Use Promotion Committee）。本次主要拜會資安研究委員會，針對 5G 資訊安全組織之運作及物聯網相關議題交換意見。

資安研究委員會由學界、業界知名學者專家組成，目前由慶應義塾大學手塚悟教授（Prof. Satoru Tezuka）擔任委員會會長（Chairman），副會長則為日本電信公司 KDDI 代表田中俊昭博士（Dr. Toshiaki Tanaka）。資安研究委員會分設三個工作小組（Working Group，WG），小組主席皆由日本知名企業派員擔任，說明如下：

- ✓ WG1 IoT Devices：主要領域為 IoT 裝置，由日本電信公司 NTT DOCOMO 石井一彥先生（Mr. Kazuhiko Ishi）擔任主席。
- ✓ WG2 Connected Vehicle：主要領域為車聯網，由日本電信公司 KDDI 田中俊昭博士兼任主席。

- ✓ WG3 Fintech：主要領域為金融應用，由日本日立製作所川野隆（先生（Mr. Takashi Kawano）擔任主席。

根據 5GMF 發佈之時程規劃，資安研究委員會從 2019 年 8 月開始進行一般性安全議題之研究以及標準化之準備，並於 2020 年 1 月開始籌備安全性議題相關之白皮書，預計於 2020 年 4 月提出。

本次由田中博士分享 5GMF 與資訊安全相關的報告。近年有越來越多因 5G 而衍生的問題浮上檯面，包含許多過去傳統電信不會發生的安全威脅，對 5G 網路資安造成衝擊。為發揮 5G 高頻寬、低延遲、大連結之特性，技術上需更積極重視、強化的要點如下：

1. 在高頻寬及大連結的特性下，智慧手機及物聯網裝置的終端裝置，應特別注意惡意程式，以避免成為增加殭屍網路攻擊力、信令 DoS 攻擊力的元兇。
2. 在低延遲的特性下，安全及需求難以取得平衡的問題，例如：加解密的能耗、邊緣運算的安全性等。

田中博士也特別分享了幾個國際標準化組織所發佈的，有關 5G 資安的主要議題，包含有：

1. 3GPP SA3 提出：

   (1) 威脅分析、安全要求、安全架構、通訊協定規範
   (2) 17 項安全領域，例如：架構（Architecture）、身份認證（Authentication）、存取網路安全性（RAN Security）、密鑰管理（Key Management）等

2. 歐盟 ETSI ISG NFV（Network Functions Virtualization）提出：

   (1) NFV 網路功能虛擬化的安全監控及管理

(2) NFV 網路功能虛擬化平臺的安全評估

3. GSMA 提出：

(1) 5G 信任模型（5G Trust Model）、網路切片安全（Slicing Security）

(2) 網絡設備安全審核（Security Audit on Network Equipment）

4. NGMN 提出：5G 相關需求包含 DoS 防禦、網路切片（Network Slicing）、邊緣運算（MEC）
5. ITU-T SG17 提出：SDN（Soft Define Network）安全、邊緣運算安全（Edge Computing security）、網路虛擬化安全（Network Virtualization Security）等
6. 其他包含：IETF 提出 5GIP 及 NETSLICING、Open Networking Foundation 提出 SDN related security 等

另外，田中博士也總結有關 5G 資安的進程，以 Use Case 角度思考資安研究委員會的研究方向，也參考 3GPP 分兩個階段進行 5G 資安的研究。

- 第一階段：針對四大構面進行研究，有 HPLMN、VPLMN、DN、UE，其中包含了 Home Control、Primary Authentication、Key Management、Inter Operator Security、On demand security、Privacy、CU-DU separation、Secondary Authentication。第一階段已經完成了標準化文件之草案。
- 第二階段：針對有關 3GPP SA3 的工作項目進行研討，包含了 URLLC security、Vertical/LAN service security、SBA security、SCAS、V2X security、Network Slicing security。第二階段標準化文件也已接近完成（於 2020 年 2 月中拜訪時間點）。

田中博士亦特別說明 SCAS，SCAS 主要檢測 5G 網路設備商轉之互通性標準是否有資安的問題，以及 SBA（Service-based Architecture） Security 主要包含外

部開放式應用系統，例如 HTTP 等，是否衍生資安風險，其他通訊協定衍生的相關資安問題亦需列入防禦的規劃與考量。

5G 系統以開放環境及架構方式來思考，在開放的前提下，衍生的資安問題也是主要的研究面向。將優先從國際組織或標準進行研究，同時納入 Use Case 的應用情境，以進一步考量哪些資安層面特別重要。田中博士表示，由於 Use Case 的應用情境仍在研究階段，因此接下來簡單分享物聯網裝置的 5G 應用。

有關物聯網裝置資安的議題，已有許多國際組織著手進行研究，並發表出許多指導方針。其中主要仍以 GSMA 為參考及研究主軸，彙整出 Availability、ID、Privacy、Security 等四大議題進行物聯網裝置資安研究，並由此四大議題中挑選出 12 個重點議題，研究因應對策以制定白皮書草案，並依此明確對物聯網平臺運營商進行要求。12 個重點議題如下：

1. LPWA 網絡安全部署和維運
2. 運營商之間的漫遊資安議題
3. 信任轉送到終端裝置
4. 安全通信環境中輕量化終端功率限制的對策
5. 強化端點操作用戶和用戶身份認證之間的可靠度連結
6. 是否可能透過端點安全認證技術驗證終端服務
7. 提供裝置識別分析及裝置操作操作的防護措施
8. 終端的身份是否顯示給未經身份驗證的用戶
9. 是否可以將終端裝置或物聯網服務所發布的數據建立用戶屬性關聯性，例如：位置資訊
10. 是否以足夠安全的方式對於機密性/完整性建立保護措施，以確保資訊以加密方式進行應用或傳輸
11. 是否可以對數據的安全金鑰和演算法進行更新
12. 在產品和服務中即建立資安防護的最佳實踐

拜會 5GMF 過程中，與會者皆為日本 5G 產業界之專家學者，因此我方也特別請益有關日本發展 5G 專網的經驗與現況。日本 5G 專網 project 於 2020 年開始，規劃優先應用於農業、防災、教育等，希望蒐集到 10 件以上的應用服務。日本政府已於今年 1 月在網上公開募集公共意見，希望了解公眾對於建置 5G 專網的想法，同時收集 use cases。之後將於 4 月份，全國招募廠商以專案方式辦理，其廠商招募以招標評選的方式進行，預計於 2020 年 6 至 7 月份公佈評選結果，8 月份與得標業者簽訂契約，因此預計 8 至 9 月份才會知道具體由哪些廠商申請 5G 專網以及將進行哪些 5G 應用服務專案。目前開放 28 GHz 頻段預估只有 10 家會有興趣，未來若開放 4.5 GHz 頻段預計會有更多廠商參與。

然而，5GMF 認為要使 5G 專網蓬勃發展尚有許多問題待克服解決，例如：5G 專網若要開放給中小企業使用，如何降低網路布建成本將是關鍵指標因素。專網預計會使用國際大廠設備，因此也積極向海外尋求合作企業夥伴。日本於 2020 年 3 月與歐洲的協會簽署 MOU （智慧工廠），希冀讓專網的建置成本降低到符合經濟效益的程度，如此才有機會普及發展中小企業使用 5G 專網的解決方案，否則推動 5G 專網將會是很困難的一件事情。

另外，日本 5GMF 及 ARIB 與臺灣 TAICS 已簽署 MOU，並在 2016 年至 2018 年舉辦 5G workshop，目前也積極評估簽定第二期的可行性。因此，會中范俊逸執行長提問有關參與 5GMF 活動之方式，5GMF 的秘書長大村好則先生（Mr. Yoshinori Ohmura）回覆表示，如在日本有登記設立公司或法人機構就可以參加 5GMF 活動，會議將以日文進行討論。5GMF 定期出版之白皮書有英文版本，其所涵蓋之 5G 應用情境十分多元，如有試驗的 Trial Result 也會做成報告書在其網站上提供給大眾參考。

圖 36：與 5GMF 交流及合影（資料來源：財團法人電信技術中心）

六、台北駐日經濟文化代表處

（一） 會議時間：109 年 2 月 13 日 10:00 至 12:00

（二） 會議地點：台北駐日經濟文化代表處

（三） 會議內容：

此行參訪日本除與電信業者、研究機構、協會等交流專業意見，也希望深入了解日本電信與資通訊產業之發展，以及新興科技如 IoT 技術與 5G 應用之規劃，同時與研究機構及協會建立良好關係，以拓展國際科研夥伴。為達成此行目標，特別安排拜會台北駐日經濟文化代表處，諮詢有關日本 5G、IoT 發展現況及日本政府對電信及資通訊產業之施政方針；此外，中心也慎重評估於日本設立辦事處之可能性，尋求代表處之建議及相關流程說明。

感謝我駐日代表處謝長廷代表、科技組陳俊榮組長及吳悅榮秘書與全團進行意見交流。赴日其間正逢新冠肺炎於日本開始流行，謝長廷代表對我團於東京之行程也甚為關切，提醒安排參訪、交通時應以健康及安全防護為最優先考量。與代表處的交流中，感謝陳俊榮組長針對日本 IoT 及 5G 產業情況準備了豐富資料，並為我團解說。以日本現況，5G 發展如遠端智慧醫療、智慧工廠的機械手臂，以及自駕車等，日本政府給予企業極大發展空間，並鼓勵產業跨界合作，多方進行技術測試，而政府也積極完善法規政策，使產業環境利於創新技術之發展。此外，陳俊榮組長亦提供有關於日本設立辦事處之相關資訊，並舉工研院、資策會、秀傳醫院等為例，說明設立地點、設立模式及名稱等應注意事項。

圖 37：與台北駐日經濟文化代表處交流及合影
（資料來源：財團法人電信技術中心）

肆、心得及建議

本次參訪 NICT、PLAY 5G、NTT DOCOMO、5GMF 及台北駐日經濟文化代表處等單位，收獲不少獲益匪淺。以下簡述參訪心得與建議：

一、NICT

NICT 為日本國家型專業法人單位，此行主要與其網路安全研究室交流研發成果，對其主動式偵測掃描，並配合監控及誘捕系統以增加情資來源，依此提高國家資安防護能力印象深刻。同時，NICT 藉由監控大量的數據流量，以累積具代表性的數據流（Data Flow），再結合大數據技術分析以針對潛在的資安威脅來源進行剖析、溯源、阻斷，並採取必要的防護措施及應變。

因應 2020 東京奧運舉辦在即（此時武漢肺炎尚未在日本大爆發，日本仍積極推廣及行銷東京奧運），日本政府於資安領域投入龐大資源，NICT 工作規劃亦配合政府政策方向，聚焦於國家資安防護主軸：

- 主動式物聯網偵測掃描

NOTICE 計畫透過主動式掃描技術，挖掘物聯網裝置可能存在之資安威脅，並與 ICT-ISAC、JPCERT/CC、ISP 等合作，將情資傳遞至最末端之用戶端使其知悉與改善，以確保整體國家的資安意識，並透過被動式監控系統及誘捕（偵測）技術的開發（Darknet sensor、IoTPoT、AmpPOT 等），強化其資料監控與蒐集來源。

- 將大數據分析應用於資安領域

NICT 每日收到巨量的封包資訊，以年為期累積了可觀的資料儲存量，透過威脅追蹤、資料探勘、大數據分析以解析越來越龐大的網路訊息，助益於監控資安威脅，可更為自動化地掌握情資以即時分析與應變。

此行拜訪亦邀請 NICT 來臺灣進行深入的技術研討，以其與 NICT 從資安技術

面、國際資訊交換等面向，建立可長可久且持續互動互惠的交流。

二、PLAY 5G Enjoy the future

NTT DOCOMO 於東京晴空塔設置 PLAY 5G，以此讓大眾體驗 5G 虛實結合之樂趣，透過 5G 大頻寬、低延遲的特性，讓大家對未來 5G 豐富多元的應用情境有無限想像。

三、NTT DOCOMO

與 NTT DOCOMO 的交流的過程中，體驗其 5G+AR/VR+體感 Sensor 之應用，藉由前瞻技術的支持，在教學、觀光等面向提供身歷其境的應用服務。此外，AR/VR 穿戴式投影頭盔的舒適度，會影響消費者長期使用的意願，NTT DOCOMO 推薦高解析影像 ViVo 頭盔（htc 產品），並表示未來除了透過 5G 提供 AR/VR 影像解決「有線」的問題外，如可克服笨重的頭盔問題（例如：全息投影）也將是一大變革，對於日後 5G 應用將有無限延伸的效果。

此外，本次交流也感受到 NTT DOCOMO 對於投入 5G 市場及應用服務之決心。一般認知 5G 大頻寬（eMBB）、巨量聯網（mMTC）及高可靠低延遲（URLLC）之特性，將為消費者的使用習慣帶來革命性改變，創造無限想像空間的應用情境服務；但其商業模式也將從原先的 B2C 廣眾市場轉而聚焦於 B2B 企業解決方案的模式，也就是 SBA（Service Base Architecture）服務導向之網路架構。

NTT DOCOMO 明確規劃於 2024 年完成 26,334 座 5G 基地臺建置，並宣示整合集團力量動用超過 10,000 名 5G 工程師完成全日本 97.02%的網路覆蓋率，以滿足消費者對 5G 網路的期待，十足展現日本電信龍頭風範，扮演領頭羊角色。在車聯網部分， NTT DOCOMO 也坦承目前雖然有 Level 4 自駕車+5G 大頻寬低延遲技術之遠端方向盤的試驗計畫，但真正無人駕駛的自駕車要上路尚有許多問題待克服，這與我國許多自駕車試驗場域所得到之測試結果一致，自駕車目前僅適用於特殊封閉型場域使用。在智慧製造的部份，NTT DOCOMO 已與多家大型企業

合作導入具體的試驗計畫，網路優化、人機介面整合及自動控制指令的正確性、穩定性與即時性是主要的關鍵因素。

四、5GMF

5GMF 乃由民間企業、機構合作成立之研究組織，目的為與 3GPP 等 5G 國際組織對接，並積極推動日本 5G 通訊系統之發展。該組織下設有多個工作小組分別對接不同領域，並透過產學研合作，研析國際組織標準與報告，建立與國際組織交流的管道窗口，並取得最新 5G 最新資訊，建立實作準則與指引白皮書，協助日本電信業在 5G 垂直應用的發展。在這個打團體戰的世代，該組織的運作模式，值得我方借鏡與參考。為落實「資安即國安」之政策，臺灣在政府主導下建立起「資安鐵三角」；然若能針對國際標準及相關檢測規範建立單一對外窗口，將國際資訊與技術引入臺灣，接軌國際、避免混淆，著實為一個值得思考的方向。在參與國際組織的部份，5GMF 結合產學研能量，積極參與國際活動，並將國際標準及報告經討論消化後產出白皮書，協助日本國內產業發展，既可讓參與國際組織的成本效益最大化，對其國內資通訊產業的發展也將是一大助益。

五、結語

5G 時代，企業戮力跨界合作，電信與通訊傳播技術之演變持續推陳出新；當科技改變了消費型態，提供世人多元思維並為生活帶來無窮的可能性，與之相關的威脅卻也悄然滋長，使政府監理任務也越具挑戰性。2020 年，當全球電信業者積極開拓 5G 商用市場的同時，各國政府無不積極制定法規標準以防範可能之風險。我國通傳會亦透過 17 條資安防護框架，具體要求電信業者提出資安防護計畫以保障消費者權益。然而，法規及監測系統除須與時俱進，亦須與國際接軌。此行與日本電信業者、研究機構深入交流，了解其資安防護監測系統之運作模式及產業技術發展現況，建立中心與日本相關機構之聯繫管道，有助於建構未來互助合作之夥伴關係。