1100218coco

110 年度「下世代電信網路號碼技術研析及管理」委託研究報告



執行單位：財團法人電信技術中心

委託機關：交　通　部

中華民國 110 年 12 月

本報告為研究案並不代表交通部意見

1100218coco

110 年度「下世代電信網路號碼技術研析及管理」委託研究報告

著者：林永勝、卜慶玲、卓卿敏、陳志宇、
王彥中、簡嘉儀、夏慧馨

執行單位：財團法人電信技術中心

委託機關：交　通　部

中華民國 110 年 12 月

國家圖書館出版品預行編目資料

110 年度「下世代電信網路號碼技術研析及管理」委託研究報告 / 林永勝, 卜慶玲, 卓卿敏, 陳志宇, 王彥中, 簡嘉儀, 夏慧馨著. -- 初版. -- 臺北市 : 交通部, 民 110.12
冊 ; 公分
ISBN 978-986-531-354-8(全套 : 平裝)

1.通訊工程 2.技術發展

448.73 110020588

著　　者：林永勝、卜慶玲、卓卿敏、陳志宇、王彥中、簡嘉儀、夏慧馨
出版機關：交通部
地　　址：10052 臺北市仁愛路一段 50 號
網　　址：http://www.motc.gov.tw
電　　話：(02)2349-2900
出版年月：中華民國 110 年 12 月
印 刷 者：大手印企業有限公司
版(刷)次冊數：初版一刷 30 冊
定　價：1200 元
本書同時登載於交通部網站
展售處：五南文化廣場 40042 臺中市中區中山路 6 號
電話: (04) 2226-0330 轉 10 或 28
http://www.wuan.com.tw
國家書店松江門市 10485 臺北市松江路 209 號 1 樓
電話: (02) 2518-0807
國家網路書店: http://www.govbooks.com.tw
GPN：1011002098
ISBN：978-986-531-354-8
著作財產權人：交通部
本著作保留所有權利，欲利用本著作全部或部分內容者，須徵求著作財產權人書面同意或授權。

交通部郵電司委託研究計畫出版品摘要表

<table>
<tr><td colspan="3">出版品名稱：110 年度「下世代電信網路號碼技術研析及管理」委託研究報告</td></tr>
<tr><td>國際標準書號(或叢刊書)</td><td>政府出版品統一編號</td><td>計畫編號</td></tr>
<tr><td>978-986-531-354-8</td><td>1011002098</td><td>1100218coco</td></tr>
<tr><td rowspan="2">主管：王廷俊
聯絡電話：02-23492200
傳真號碼：02-23813928
e-mail：
tc_wang@motc.gov.tw
承辦人：林姝宜
聯絡電話：02-23492181
傳真號碼：02-23813928
e-mail：sy_lin@motc.gov.tw</td><td rowspan="2">研究單位：財團法人電信技術中心
計畫主持人：林永勝
聯絡電話：02-8953-5971
傳真號碼：02-8953-5655
e-mail：BillLin@ttc.org.tw
研究人員：林永勝、卜慶玲、卓卿敏、陳志宇、王彥中、簡嘉儀、夏慧馨
通信地址：新北市板橋區遠東路 1 號 3 樓 B 室
聯絡電話：02-8953-5600</td><td>其他參與合作之研究團隊
無
研究期間
自 110.03
至 110.12
研究經費
壹仟參佰柒拾伍萬陸仟壹佰零貳元整</td></tr>
<tr><td colspan="3">關鍵詞：電信網路號碼、編碼技術、編碼標準、5G 物聯網、DNS 編碼</td></tr>
<tr><td colspan="3">摘要：
隨著 5G 時代來臨，物聯網、網路切片等新興應用服務快速發展，惟目前電信產業採用之 E.164、E.212 等電信編碼原則沿用已久，對應下世代嶄新的電信環境，在技術及管理上應有全面檢視之必要。本計畫核心架構係以國際 5G 前瞻技術趨勢及資通訊安全之政策走向，致力於 5G 網路切片技術之專網編碼系統與場域平臺之開發、建置與維運之整合性服務，並開發網域名稱系統(Domain Name System, DNS)與 5G 網路切片技術融合、跨場域編碼互通相關研究彙整成最終成果。本計畫研究報告書以四個分項架構進行撰寫。
分項一「下世代電信網路號碼技術及政策」部分，為超前部署下世代電信編碼技術與標準，報告盤點電信網路號碼資源 E.164、E.212、IPv6 及新創技術區段路由（Segment Routing IPv6, SRv6）之發展，與其他國家之號碼管理或應用情形，並研析物聯網編碼及新型態網路編碼的演進情形，以觀測下世代電信網路號碼技術及電信號碼未來之發展趨勢。
分項二「下世代電信網路號碼資安稽核」部分，透過研析歐盟網路與資訊安全指令、新加坡網路安全策略、美國網路安全框架等網路安全政策與法規，爬梳國際指標性國家在國家網路安全總體政策脈絡與資安體制之發展，以及未來網路的資安防護措施，並產出號碼管理資安稽核框架。
分項三「下世代電信網路號碼驗證機制」部分，以驗證 5G 專網環境，開發</td></tr>
</table>

DNS 編碼系統。物聯網設備可透過 5G 核心網路進行認證，同時配發 IPv4 及 IPv6，並完成在同域或跨域之不同基站間移動測試，以利使用管理平臺儲存、管理及提供查詢相關 DNS 自動編碼的歷史軌跡資料。

分項四「下世代電信網路號碼人才培育」之目標為培養參與相關國際標準制訂工作及可擔任該等組織重要幹部之專業人才，以確保我國在資通訊領域的國際空間及影響力。

透過上述本計畫研究結論，綜整出以下政策建議。首先在下世代電信網路號碼技術及政策部分，建議號碼政策應以技術中立原則，依服務需求進行號碼之分配管理。而在下世代電信網路資安稽核部分，建議宜在我國資通安全管理法及其子法之法制體系下，建立利害關係人之風險溝通框架，以落實資安及國安之願景目標。另外不同於傳統公眾電信網路通用之 E.164 及 E.212 編碼，主要應用於人與人之通訊與識別，在下世代電信網路環境將會有人與物或物與物之通訊與識別情境，因此本計畫提出下世代電信網路號碼驗證機制，目的為提供使用者對物聯網裝置易於直覺式辨識及管理之編碼解決方案，以因應 5G 時代更加多元的 IoT 應用場景，並增加更多對移動性 IoT 設備之需求。本研究下世代電信網路號碼技術在國際實屬前瞻技術議題，為使我國掌握全球最新技術發展趨勢及確保在資通訊領域的國際空間，本計畫提出以四年為基準之人才培育短、中、長期參與策略與效益，透過參與國際相關組織會議，及強化與國際該等社群互動交流等策略，並加強所需之政策專業知能，以累積國際影響力及爭取擔任國際組織之幹部。

出版日期	頁數	定價	本出版品取得方式
110 年 12 月	1030	1200	凡屬機密性出版品均不對外公開，普通性出版品；公營、公益機關團體及學校，由本部依業務性質函送參考，其他需要者可函洽本部免費贈閱，或逕進入 www.motc.gov.tw 之出版品項下下載。

機密等級：

☐限閱☐密☐機密☐極機密☐絕對機密

(解密【限】條件：☐ 年 月 日解密，☐公布後解密，☐附件抽存後解密，
☐工作完成或會議終了時解密，☐另行檢討後辦理解密)

☑普通

備註：本研究之結論與建議不代表交通部之意見

全文摘要

隨著 5G 時代來臨，物聯網、網路切片等新興應用服務快速發展，惟目前電信產業採用之 E.164、E.212 等電信編碼原則沿用已久，對應下世代嶄新的電信環境，在技術及管理上應有全面檢視之必要。本計畫核心架構係以國際5G前瞻技術趨勢及資通訊安全之政策走向，致力於5G網路切片技術之專網編碼系統與場域平臺之開發、建置與維運之整合性服務，並開發網域名稱系統(Domain Name System, DNS)與5G網路切片技術融合、跨場域編碼互通相關研究彙整成最終成果。本計畫研究報告書以四個分項架構進行撰寫。

分項一「下世代電信網路號碼技術及政策」部分，為超前部署下世代電信編碼技術與標準，報告盤點電信網路號碼資源 E.164、E.212、IPv6 及新創技術區段路由（Segment Routing IPv6, SRv6）之發展，與其他國家之號碼管理或應用情形，並研析物聯網編碼及新型態網路編碼的演進情形，以觀測下世代電信網路號碼技術及電信號碼未來之發展趨勢。

分項二「下世代電信網路號碼資安稽核」部分，透過研析歐盟網路與資訊安全指令、新加坡網路安全策略、美國網路安全框架等網路安全政策與法規，爬梳國際指標性國家在國家網路安全總體政策脈絡與資安體制之發展，以及未來網路的資安防護措施，並產出號碼管理資安稽核框架。

分項三「下世代電信網路號碼驗證機制」部分，以驗證 5G 專網環境，開發 DNS 編碼系統。物聯網設備可透過 5G 核心網路進行認證，同時配發 IPv4 及 IPv6，並完成在同域或跨域之不同基站間移動測試，以利使用管理平臺儲存、管理及提供查詢相關 DNS 自動編碼的歷史軌跡資料。

分項四「下世代電信網路號碼人才培育」之目標為培養參與相關國際標準制訂工作及可擔任該等組織重要幹部之專業人才，以確保我國在資通訊領域的國際空間及影響力。

透過上述本計畫研究結論，綜整出以下政策建議。首先在下世代電信網路號碼技術及政策部分，建議號碼政策應以技術中立原則，依服務需求進行號碼之分配管理。而在下世代電信網路資安稽核部分，建議宜在我國資通安全管理法及其子法之法制體系下，建立利害關係人之風險溝通框架，以落實資安及國安之願景目標。另外不同於傳統公眾電信網路通用之 E.164 及 E.212 編碼，主要應用於人與人之通訊與識別，在下世代電信網路環境將會有人與物或物與物之通訊與識別情境，因此本計畫提出下世代電信網路號碼驗證機制，目的為提供使用者對物聯網裝置易於直覺式辨識及管理之編碼解決方案，以因應 5G 時代更加多元的 IoT 應用場景，並增加更多對移動性 IoT 設備之需求。本研究下世代電信網路號碼技術在國際實屬前瞻技術議題，為使我國掌握全球最新技術發展趨勢及確保在資通訊領域的國際空間，本計畫提出以四年為基準之人才培育短、中、長期參與策略與效益，透過參與國際相關組織會議，及強化與國際該等社群互動交流等策略，並加強所需之政策專業知能，以累積國際影響力及爭取擔任國際組織之幹部。

關鍵詞：電信網路號碼、編碼技術、編碼標準、5G 物聯網、DNS

目次

第一章　緒論.....1
第一節　研究背景.....1
第二節　研究範圍與目標.....3
第三節　研究流程與方法.....4
第四節　預期成果與效益.....6
第二章　下世代電信網路號碼技術及政策.....9
第一節　下世代電信網路願景及標準發展.....9
第二節　IPv6 技術標準之發展.....19
第三節　主要國家或地區推動 IPv6 發展政策.....24
第四節　新興網路技術與通訊協定發展.....35
第五節　國際電信號碼標準與管理發展.....45
第六節　主要國家或地區電信號碼管理政策與物聯網編碼之調和.54
第七節　網際網路標識及通訊協定.....70
第八節　小結.....75
第三章　下世代電信網路號碼資安稽核.....84
第一節　下世代網路資通安全研析.....84
第二節　國際網路安全政策與法規研析.....125
第三節　下世代電信號碼管理系統安全及跨網互通安全策略.....176
第四節　小結.....239
第四章　下世代電信網路號碼驗證機制.....244
第一節　下世代電信網路號碼系統評估.....244
第二節　實測驗證平臺之規劃.....265
第三節　電信號碼分配與設備對應之測試項目及測試結果.....292
第四節　小結.....341
第五章　下世代電信網路號碼人才培育.....351
第一節　計畫背景及目標.....351
第二節　計畫架構及研究流程.....352
第三節　執行內容與成果.....355

第四節　小結 410
第六章　研究結論與政策建議 421
第一節　研究結論 421
第二節　政策建議 429
第三節　下世代電信網路號碼與數位經濟發展政策 437
附錄一、參考文獻 440
附錄二、中英文名詞對照 457

表目次

表 2- 1、近期 IETF IPv6 相關 RFC 提案 21
表 2- 2、電信層及應用層優缺點 82
表 3- 1、Network 2030 網路架構原則 85
表 3- 2、系統資安威脅及改善技術 100
表 3- 3、NIST 網路安全框架框架實施層級 128
表 3- 4、5G 網路系統範圍對照說明 180
表 3- 5、物聯網生態圈各節點資安風險 190
表 3- 6、IEC/ISO27001: 2013 章節架構 197
表 3- 7、IEC/ISO27001: 2013 條文項目原則之摘要 200
表 3- 8、IEC62443-1-1 基本功能需求分類 209
表 3- 9、IEC 62443-2-4 安全計畫（SP）要求 211
表 3- 10、DNS 網路安全框架核心檢核項目 217
表 3- 11、下世代電信網路號碼資安評估指引框架章節安排 232
表 4- 1、5G 核心網路元件功能 250
表 4- 2、ETSI MEC 技術標準 257
表 4- 3、當 UE 註冊時 Gn DNS 解析 APN 或 DNN 之註冊流程 259
表 4- 4、當 UE 移動中 Gn DNS 解析行動網路網元之流程 260
表 4- 5、GSMA IR.67 指引行動網域裡子網域（sub-domain）定義 ... 263
表 4- 6、行動網路 Gn DNS 的 FQDN 解析運用 264
表 4- 7、PoC 實測驗證場域採用 5G 模擬器功能說明 268
表 4- 8、網路切片 SST 參數設定 270
表 4- 9、行動網路傳輸延遲比較 273
表 4- 10、PoC 實測驗證場域之 DNS 編碼組成欄位 275
表 4- 11、PoC 實測驗證場域之硬體設備列表 281
表 4- 12、PoC 場域軟體列表 292
表 4- 13、基本驗證項目彙整表 293
表 4- 14、IoT 設備初始參數 294
表 4- 15、同域測試 295

表 4- 16、同域移動之 IP 註冊與 DNS 動態管理流程 297
表 4- 17、同域移動測試結果 299
表 4- 18、IoT 設備註冊後之 Dashboard System Log 302
表 4- 19、跨域測試 303
表 4- 20、跨域移動之 IP 註冊與 DNS 動態管理流程 304
表 4- 21、跨域移動測試結果 306
表 4- 22、IoT 設備跨域移動測試後之 Dashboard System Log 309
表 4- 23、大量 IoT 終端設備測試項目一 310
表 4- 24、大量物聯網裝置測試項目一之 IP 註冊與 DNS 動態管理 311
表 4- 25、IoT 終端設備參數 312
表 4- 26、100 臺 IoT 終端設備註冊測試結果 313
表 4- 27、100 臺 IoT 終端設備註冊後之 Dashboard System Log 316
表 4- 28、大量 IoT 終端設備測試項目二 319
表 4- 29、大量 IoT 終端設備測試項目二之 IP 註冊與 DNS 動態管理 320
表 4- 30、IoT 終端設備持續移動之測試結果 320
表 4- 31、IoT 終端設備持續移動之 Dashboard System Log 322
表 4- 32、同域測試 326
表 4- 33、同域移動之 IP 註冊與 DNS 動態管理流程 328
表 4- 34、同域移動測試結果 331
表 4- 35、IoT 終端設備註冊後之 Dashboard System Log 334
表 4- 36、跨域測試 335
表 4- 37、跨域移動之 IP 註冊與 DNS 動態管理流程 336
表 4- 38、跨域移動測試結果 338
表 4- 39、IoT 終端設備跨域移動測試後之 Dashboard System Log 341
表 4- 40、PoC 實測驗證成果彙整表 343
表 5- 1、IETF 工作領域表 358
表 5- 2、ICANN 71 會議參與及效益表 364
表 5- 3、ICANN 72 會議參與及效益表 366
表 5- 4、ICANN 會議報告與本計畫關係說明表 368

表 5- 5、網域名稱註冊資料與 NIS2 指令草案規管範圍表..... 370
表 5- 6、零接觸通用 IoT 裝置識別安全性策略說明表 372
表 5- 7、零接觸通用 IoT 裝置識別互通性安全性策略說明表 372
表 5- 8、IETF 111 會議參與及效益表..... 377
表 5- 9、IETF 112 會議參與及效益表..... 379
表 5- 10、 座談會議題及結論綜整表 389
表 5- 11、經驗分享會主題場次表 398
表 5- 12、經驗分享會內容綜整表 399
表 5- 13、人才培育成果質化與量化綜整表 414
表 5- 14、短、中、長期人才培育策略規劃表 419
表 6- 1、以 DNS 為 IoT 設備命名之國際文獻..... 427

圖目次

圖 1-1、網路切片概念圖 4
圖 1-2 、預期成果及產出 7
圖 2-1、ITU-T 組織架構 12
圖 2-2、Internet 與 NDN 的沙漏結構對照 37
圖 2-3、NDN 結構中的封包格式 38
圖 2-4、NDN 轉發工程模型 39
圖 2-5 、歐盟 ECC 建議的 E.164 號碼指配管理模式 47
圖 2-6 、使用於美國 CBRS 頻段專網之 IMSI 號碼格式 49
圖 2-7、Internet 標準的維護組織 71
圖 2-8、基於實用性的 RFC 文件分類 71
圖 2-9、DNS 運作流程示意 74
圖 3-1、使用者服務與前端 88
圖 3-2、前端、中繼、回程網路 89
圖 3-3、V6OPS 工作小組目審核之草稿文件 98
圖 3-4、整體安全架構圖 180
圖 3-5、美國、德國、日本製造業面臨的 IT、OT 資安挑戰 192
圖 3-6、ISO27001 與 PDCA 循環 199
圖 3-7、ISA/IEC 62443 架構圖與進度 206
圖 3-8、NIST SP 800-207 零信任架構與核心元件關聯圖 230
圖 3-9、下世代電信網路號碼資安評估指引整體架構 232
圖 3-10、下世代電信號碼管理政策關聯議題 236
圖 3-11、關注方對應 DNS 號碼管理議題之要求 238
圖 3-12、下世代電信號碼安全管理議題背景分析 242
圖 4-1、 ITU 的 5G 三大應用場景 248
圖 4-2、服務系統架構圖 249
圖 4-3、參考點系統架構圖 249
圖 4-4、5G 網路切片架構示意 253
圖 4-5、MEC 實體部署的範例 255

圖 4- 6、行動網路 DNS 之部署與角色 258
圖 4- 7、Gn DNS 解析行動網路網元之流程圖 261
圖 4- 8、5G 模擬器所包含之網路功能元件 266
圖 4- 9、RADIUS accounting update 267
圖 4- 10、3GPP TS 23.501 所定義之 SST 參數規格 270
圖 4- 11、MEC 架構 272
圖 4- 12、IoT 設備建立連線時之 FQDN 資訊來源 278
圖 4- 13、功能邏輯架構圖 280
圖 4- 14、硬體設備架構圖（以 5G Gateway 連線） 282
圖 4- 15、硬體設備架構圖（以 5G Dongle 連線） 283
圖 4- 16、 PoC 實測驗證場域的 UE 註冊流程圖(以 5G Gateway 連線) 284
圖 4- 17、 PoC 實測驗證場域的 UE 註冊流程圖（以 5G Dongle 連線） 285
圖 4- 18、伺服器系統軟體架構圖 285
圖 4- 19、PoC 場域 Dashboard 首頁示意圖 289
圖 4- 20、PoC 場域 Dashboard 歷史資料示意圖 289
圖 4- 21、PoC 場域 Dashboard System Log 示意圖 290
圖 4- 22、5G 模擬器對 RADIUS 傳送運作流程圖 291
圖 4- 23、同域移動之 IP 註冊與 DNS 動態管理流程 296
圖 4- 24、IoT 設備註冊 IP 以及自動註冊 DN 後之參數 298
圖 4- 25、IoT 設備在同域的不同 Cell 移動後之參數 298
圖 4- 26、IoT 設備註冊後之 Dashboard 畫面 300
圖 4- 27、IoT 設備同域移動後之 Dashboard 畫面 301
圖 4- 28、跨域移動之 IP 註冊與 DNS 動態管理流程 303
圖 4- 29、IoT 設備跨域移動後之參數 305
圖 4- 30、IoT 設備跨域移動測試前之 Dashboard 畫面 307
圖 4- 31、IoT 設備跨域移動測試後之 Dashboard 畫面 308
圖 4- 32、大量 IoT 終端設備註冊並產生 RADIUS 資料流程 310

圖 4- 33、100 個 IoT 終端設備自動註冊展示畫面..... 314
圖 4- 34、100 臺 IoT 自動註冊 System Log 315
圖 4- 35、大量 IoT 終端設備跨域移動之 IP 註冊與 DNS 動態管理流程 319
圖 4- 36、IoT 終端設備持續移動 Dashboard System Log..... 321
圖 4- 37、同域移動之 IP 註冊與 DNS 動態管理流程..... 327
圖 4- 38、IoT 終端設備註冊 IP 以及自動註冊 DN 後之參數 329
圖 4- 39、IoT 終端設備在同域的不同 Cell 移動後之參數..... 330
圖 4- 40、IoT 終端設備同域移動之 Dashboard 畫面 332
圖 4- 41、IoT 終端設備同域移動之 Dashboard 畫面 333
圖 4- 42、跨域移動之 IP 註冊與 DNS 動態管理流程..... 335
圖 4- 43、IoT 終端設備跨域移動後之參數 337
圖 4- 44、IoT 終端設備跨域移動測試前之 Dashboard 畫面 339
圖 4- 45、IoT 終端設備跨域移動測試後之 Dashboard 畫面 340
圖 4- 46、PoS 情境規劃..... 350
圖 5- 1、計畫架構圖 353
圖 5- 2、IETF 標準制定流程..... 359
圖 5- 3、ICANN 多方利益共同體組成圖 361
圖 5- 4、ICANN 組織圖..... 362
圖 5- 5、零接觸通用 IoT 裝置識別之識別發行流程圖 374
圖 5- 6、零接觸通用 IoT 裝置識別之信任認證圖 374
圖 5- 7、零接觸通用 IoT 裝置識別之驗證及授權圖 375
圖 5- 8、計畫參與分配架構..... 387
圖 5- 9、組建專業團隊架構圖 403
圖 5- 10、SSAC 委員申請流程 407
圖 5- 11、國際會議參與回饋流程圖 412
圖 5- 12、ICANN 72 會議成果發表..... 413

第一章　緒論

第一節　研究背景

目前國際上，電信設備相互聯繫主要依據 ITU E.164 國際編碼方式，「國碼」+「區碼」+「電話號碼」格式即可互通互連。

隨著 5G 時代來臨，物聯網(Internet of Things, IoT)、網路切片及專網等服務成為快速發展下的新興應用，目前電信產業採用之 E.164、E.212 等電信編碼原則在下世代嶄新的電信環境下應有全面檢視之必要。

網際網路網域名稱及位址指配機構（Internet Corporation for Assigned Names and Numbers, ICANN）考量即時通訊軟體(Instant Messaging, IM)的興起及普及，技術上這些即時通訊軟體(如 Line、Telegram、Facetime、Messenger)已不使用 E.164 號碼做為用戶識別，以及 5G IoT 設備使用電信號碼的特性有別於傳統，針對此議題，近年相關組織已召開一系列會議研討相關技術及管理議題。

ICANN 於 2017 年 11 月在阿布達比舉辦的國際研討會上，展示使用網域名稱系統（Domain Name System, DNS）作為取代 E.164 編碼方式的可能性。其中針對 IoT 設備的編碼方式，該機構亦於 2020 年 1 月 23 日發表其對「5G Technology」[1]及 ITU「Network 2030」[2]之看法。

有鑑於資通訊技術及服務應用日新月異，相關國際組織(如 ITU、3GPP、GSMA、ICANN)針對網路切片(Network Slicing)、電信號碼管理(Telephone Numbering Plan)及 DNS 管理應用等不斷提出新的技術方案。

本計畫為 110 年度交通部「5G/B5G 電信資源整備及通訊網路發展研究計畫」之子計畫之一，旨在研究下世代 5G /B5G 電信編碼標準及加強與國內單位及國際合作。本計畫「下世代電信網路號碼技術研析及管理」委託研究計畫，從研析「國際下世代電信號碼機制及各國政策發

[1] ICANN Office of the Chief Technology Officer ,"5G Technology", Alain Durand,OCTO-004(2020) < https://www.icann.org/en/system/files/files/octo-004-23jan20-en.pdf>.（最後瀏覽日：2021/6/12）

[2] ICANN Office of the Chief Technology Officer," New IP", Alain Durand,OCTO-017 (2020) < https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf>.（最後瀏覽日：2021/6/12）

展」、「Network 2030 與非 IP 網路之電信號碼策略」與「網路切片之電信號碼方向」，了解國際電信網路編碼議題及相關技術，並對國內相關領域產學研專家進行深度訪談後，綜整提出政策發展方向建議。

此外，進行基於 DNS 之 5G IoT 電信編碼實測驗證，建立我國下世代電信網路號碼驗證機制，並研析下世代電信號碼資安稽核，及研提下世代電信號碼管理系統安全及跨網互通安全策略；另外，為維護及確保我國科技發展與國際並駕齊驅，透過參與國際組織之電信號碼相關會議及活動，如網際網路工程任務組（Internet Engineering Task Force, IETF）及 ICANN 首席技術官辦公室（Office of the Chief Technology Officer）等組織之連結及合作，培養參與相關國際標準制定工作及可擔任該等組織重要幹部之專業人才，以掌握國際下世代電信網路號碼技術發展。

第二節　研究範圍與目標

隨著 5G 技術的優勢使物聯網應用快速的成長，依據國際數據資訊（International Data Corporation, IDC）的 2019-2023 趨勢預測報告（Worldwide Internet of Things Forecast, 2019-2023），物聯網整體市場投資由 2019 年的 7,265 億美元將成長至 2023 年的 1.12 兆美元，年複合成長率將達 12.6%[3]。至此，預期在 5G 與物聯網的創新應用服務逐漸成熟後，企業採用專網的意願也會逐年攀高，成為推動產業轉型與奠基數位經濟之利器。

伴隨著創新應用服務的發展，在既有 E.164 號碼資源有限及物聯網之新辨識及管理需求下，及早掌握下世代新型態的編碼機制，有助於國家後續資通訊政策擬定、技術應用與產業發展。

除了號碼的管理外，如何能讓 5G 專網中的網路達成互連與持續通訊，將會是 5G 專網的關鍵。由於，企業專網在不連接公眾網路，以及得自行決定使用者範疇之情況下，更具備網路、或資料的控制權，增加資訊安全的保障，使我國的部分業者表達欲申請企業專網之意願，促使產業進行轉型。惟我國若讓企業申請專用頻譜，並自行建置網路，相較於直接連接電信業者之公眾網路、或是介接電信業者之頻譜以建置專用網路，勢必有多項議題需要留意。首先，伴隨著企業自建網路的蓬勃發展，預期智慧工廠、車聯網等創新應用服務將會如雨後春筍般的盛行，惟企業自行申請專用頻譜並自建網路設備，仍需考慮資安之防禦。最後，企業專網的蓬勃發展亦有可能造成頻率干擾的問題，降低頻譜使用效率。

本計畫核心架構係以國際 5G 前瞻技術趨勢及資通訊安全之政策走向，致力於 5G 網路切片技術之專網編碼系統探討與實證，其 5G 網路切片概念如圖 1-1，透過利用不同服務將 5G 核心網切割不同功能網路，將 DNS 系統與 5G 網路切片技術融合、跨場域編碼互通相關研究彙整成最終成果。

[3] IDC Worldwide Global DataSphere IoT Device and Data Forecast, 2019–2023), IDC, .May, 2019 .

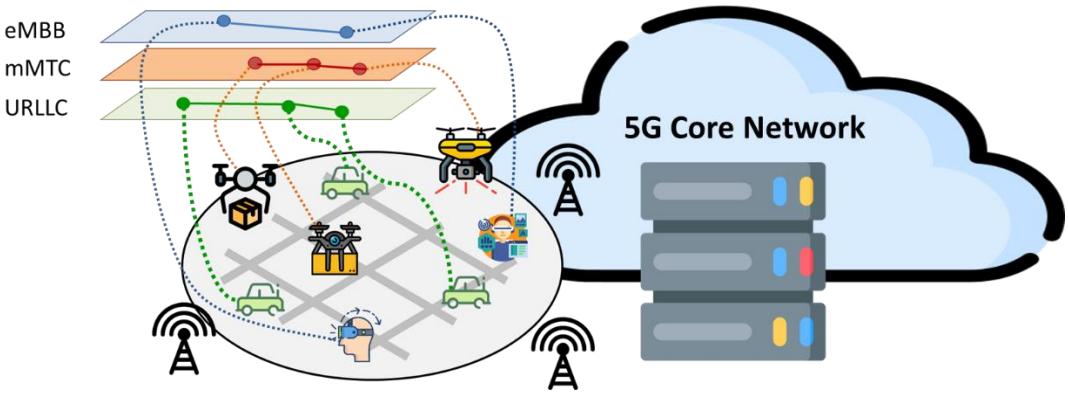


圖 1- 1、網路切片概念圖

資料來源：本計畫製作

為能完善我國 5G 網路切片機制，奠基臺灣創新經濟環境，促使在 2024 年建立一個 5G 專網服務架構，本計畫規劃第一年藉由完成 5G 專網編碼服務之概念驗證（Proof of Concept, PoC）、第二至三年服務驗證（Proof of Service, PoS）以及未來商用驗證（Proof of Business, PoB）三階段計畫目標，研析國家以 5G 網路切片專網可能面臨的問題及應對策略。

為了邁入商用驗證，本計畫於今(2021)年完成概念驗證（PoC）服務，未來可持續執行 PoS 及 PoB 後，提出符合我國發展 5G 專網之路徑，奠基我國數位經濟環境，以促進我國 5G IoT 與網路切片相關產業技術與國際接軌，協助國內產業及早因應及進行市場布局，進而提升我國相關產業自主研發能力。

第三節　研究流程與方法

由於本案涉及層面甚廣，計畫分成四個分項：

分項一「下世代電信網路號碼技術及政策」部分，著重在 5G IoT 號碼機制議題，理解現今 IPv6、E.164 電信編碼機制，說明國際組織在下世代電信網路願景及標準發展，並說明主要國家或地區推動 IPv6 發展政策與新興網路技術發展等。另外，說明國際電信號碼標準與管理發展，並針對主要國家或地區電信號碼管理政策與物聯網編碼，並綜整出

政策發展方向建議。

分項二「下世代電信網路號碼資安稽核」進一步點出 DNS 在網路切片間之管理層面，以及 5G 專用網路與公眾網路介接之通訊機制層面所涉及的資訊安全需求，並研析 IoT 網路環境下可能產生的資安缺口，提出相對應的指標或防禦機制，以建立資安稽核策略。

分項三「下世代電信網路號碼驗證機制」則奠基在分項一之研究基礎，以網路切片技術建置一個以 DNS 為基礎的 5G 專用網路，實際模擬 IoT 裝置運行之通訊機制，進行同域及跨域的概念性驗證。

分項四「下世代電信網路號碼人才培育」，藉由參加國際相關組織會議，以及鏈結國內專業人才進行相關訓練，以確保研究進程符合發展趨勢，同時精進研究團隊人員專業與經驗，培育我國下世代網路號碼人才。

期末研究報告書以六大章節進行撰寫，章節內容涵蓋委辦機關要求，說明如下：

第一章緒論說明「下世代電信網路號碼技術研析及管理」計畫之研究背景、研究範圍與目標、研究流程與方法及預期成果效益。

第二章「下世代電信網路號碼技術及政策」為根據本計畫之背景及目標，深入研析下世代電信網路號碼技術發展，瞭解現行 ITU-T、IETF 對下世代電信網路願景及標準發展，並研析 IPv6 技術標準及各國推動 IPv6 發展政策；另外，研析下世代電信網路號碼政策，透過研析國際主要國家之電信號碼管理政策及物聯網編碼發展，及研析網際網路標示及通訊協定，並綜整提出政策發展方向建議。

第三章「下世代電信網路號碼資安稽核」研析 5G 電信編碼系統與裝置設備的稽核、驗證與管理層面之研究，評估 5G 專用網路場域潛在的資安風險，並綜整提出資安稽核策略。

奠基於第二至三章之研究結果，第四章「下世代電信網路號碼驗證機制」為評估 5G 號碼系統，擬定 PoC 平臺系統，建立下世代電信號碼驗證機制，並驗證下世代電信號碼分配與設備對應。第五章「下世代電

信網路號碼人才培育」即呈現研究團隊參與 ICANN 等國際標準組織會議成果，使 5G 網路切片技術與電信編碼服務研究能發揮最大效益。最後，綜合前述章節之研究內容，提出第六章「研究結論與政策建議」。

第四節　預期成果與效益

本計畫預期產出之研究成果與效益說明如下。

一、 預期成果

電信編碼機制及網路切片是 5G/B5G 電信網路之關鍵技術，網路切片技術是依據電信服務需求，將網路從核心網或接入網運用虛擬化技術切割成多個虛擬的端對端網路，以達到資源調整及靈活使用。目前國際 5G 處於商轉，整體基礎建設及產業價值鏈仍在發展，如何使我國產業得在安心、安全的環境善用 5G 網路切片及自建 5G 專網，需解決 5G 網路切片及專網之編碼技術、資安及新興技術等議題。

本計畫為超前部署 5G 網路切片及專網之電信技術，進而促進我國 5G IoT 與網路切片相關產業技術與國際接軌，協助國內產業及早因應及進行市場布局，提升我國相關產業自主研發能力。透過「下世代電信網路號碼技術及政策」、「下世代電信網路號碼資安稽核」、「下世代電信網路號碼驗證機制」及「下世代電信號碼人才培育」等研究產出，並分別綜整出「政策發展方向建議」、「資安稽核策略」、「電信號碼管理機制驗證」及「人才培育成果報告及人才培育短、中、長期參與策略與效益」。



圖 1- 2 、預期成果及產出

資料來源：本計畫製作

二、 預期效益

本計畫目標為觀察國際下世代電信網路號碼機制及各國政策發展、建立 5G 網路切片之通訊機制層面所涉及的資安稽核策略、建立以 DNS 為基礎之 5G IoT 電信號碼管理驗證機制、提出人才培育成果及人才培育短、中、長期參與策略與效益，以促進我國下世代 5G IoT 與網路切片產業發展及我國產業具備自主開發 5G 電信編碼轉譯技術，本計畫成果所預期效益為「使我國掌握全球最新下世代電信網路號碼發展」、「協助國內產業及早因應及進行市場布局」及「確保我國在資通訊領域的國際空間及影響力」，其效益說明如下。

(一) 掌握全球最新下世代電信網路號碼發展

本計畫蒐集國際下世代電信網路號碼機制及各國政策發展，針

對 ITU「Network 2030」、非 IP 網路文獻及 ICANN「5G Technology」等國際組織所發布之電信編碼文獻進行研析，並研析中國、日本及歐盟等國家之物聯網號碼政策，以提出下世代電信網路號碼政策方向，並透過平臺系統建置、測試電信號碼分配與設備對應。此外，透過辦理座談會將蒐集之國際趨勢及實測驗證成果等相關資訊予國內各產業(電信業者、物聯網業者、製造商等)交流及分享，以作為未來創新服務推動之參考。

(二) 協助國內產業及早因應及進行市場布局

藉由本計畫研究下世代電信 5G/B5G 電信編碼標準及實際參與相關國際組織，故本計畫辦理座談會及成果發表會，邀請政府機關相關單位、電信業者及設備商等相關利害關係人，藉由本計畫之座談會進行跨界之交流與意見蒐集，以促進我國下世代 5G IoT 與網路切片相關產業技術與國際接軌，並提升我國相關產業自主研發能力。

(三) 確保我國在資通訊領域的國際空間及影響力

透過觀測國際下世代電信號碼發展及國內投入國內研究經費，並積極參與 5G/B5G 新興通訊技術之國際標準組織會議，強化與網際網路工程任務組(IETF)及 ICANN 首席技術長辦公室等組織鏈結，培養參與相關國際標準制訂工作及可擔任該等組織重要幹部之專業人才，以確保我國科技發展與國際並駕齊驅。

第二章　下世代電信網路號碼技術及政策

第一節　下世代電信網路願景及標準發展

一、下世代電信網路之概念與定義

鑒於通訊技術發展日新月異，當使用者想要連上網際網路，無論是藉由行動寬頻或固網寬頻，支援上網服務的主要網路架構均已從傳統電路交換（circuit switch）演進為封包交換（packet switch），並對下世代網路（Next Generation Network, NGN）的建設與發展起了重要的推動作用。

依據 ITU-T「NGN 概述」文件的宏觀定義，NGN 是一種以封包為基礎的網路，能夠向用戶提供電信服務，並利用多種寬頻接取、支持服務品質（Quality of Service, QoS）的傳輸技術。由於服務功能獨立於底層傳輸技術，用戶能夠不受限制地接取網路，並且得以選擇競爭服務業者所提供之服務。NGN 支持通用移動性，允許向用戶提供一致和無處不在的服務[4]。為能更好地描述 NGN 管理需求和功能體系結構，文件列舉出 NGN 應具備的基本特性，包括：

- 以封包為基礎的傳送；
- 控制功能和承載能力、呼叫/會話以及應用/業務相分離；
- 業務提供與傳輸無關，提供開放的接口；
- 提供廣泛的業務、應用和基於業務構建模塊（包括即時/串流/非即時和多媒體業務）的機制；
- 具備端到端 QoS 的寬頻能力；
- 通過開放介面與傳統網路互通；
- 通用移動性；
- 用戶不受限地接取多個服務提供業者；
- 多樣的認證方案；

[4] ITU-T, Recommendation Y.2001 (12/04) - General overview of NGN, available at https://www.itu.int/rec/T-REC-Y.2001-200412-I/en (Last visited:Dec. 5, 2021)

- 對同一業務用戶感受到統一的業務特徵；
- 固網與行動網路之間的業務融合；
- 與業務相關的功能獨立於底層傳輸技術；
- 支持多種最後一哩技術；
- 滿足所有的管制方面的要求，例如關於應急通訊、安全、個人隱私、合法偵聽等方面。

諸如會話、媒體、資源、業務傳遞、安全等 NGN 功能實體（functional entities），在部署時可採分散式架構，功能實體之間通過開放介面通訊。參考點的標識（the identification of reference points）是 NGN 中非常重要的一環。通訊功能實體之間要順利進行通訊，協定就必須標準化。

NGN 由相互連接的異質網路組成，採用各不相同的接取方式與用戶設備。由於 NGN 應提供與接取方式及網路無關的無縫通訊能力，故在設計上應考量到編號、命名及定址（Numbering, naming and addressing）的問題。用戶終端可由名字或號碼來辨識，通過名字與號碼的解析系統，將一個給定的名字或號碼翻譯成有效的可路由位址，例如，網際網路通訊協定（Internet Protocol, IP）位址。編號、命名方案的範例如下：

- E.164 編號方案（numbering scheme）；
- 全球資源定址器（Universal Resource Locator, URL）；
- 任何具唯一性的名稱系統，如：1800Airways；
- 其他的命名方式（naming conventions），如 H.323、會話發起協定（Session Initiation Protocol, SIP）、帶有電話及電子郵件之 URL 等。

當兩個用戶需要彼此聯繫時，可以直接輸入以上所提到的標識（identifiers），用戶終端根據其內部或外部的資料庫，例如，通過 DNS 域名系統，將所輸入的標識翻譯成 IP 位址，以用於建立傳送連接。

在公眾網路上，NGN 必須滿足對名稱解析的要求，如下所列：

- 可靠性（Reliability）：由於名稱與號碼解析系統（name/number resolution system）與 NGN 的運行直接相關，因此必須具備電信服務級別的可靠性。在架構上，不應存在單點故障（single point of failure），且應有優秀的負載平衡機制（load balancing mechanisms）。
- 完整性（Integrity）：由於名稱與號碼解析系統與公用網的運行直接相關，所以必須確保名字/號碼解析系統間互不矛盾，名字/號碼翻譯系統數據庫只能有可靠的有效的條目，用以確保整個系統的完整性不受影響，尤其是在採用分佈式系統時。
- 安全性（Security）：名稱與號碼解析資料是非常重要的網路資料，可能直接影響到網路的運行，他們同時也是反映網路運行的結構及政策的敏感的商業資料。基此，名稱與號碼解析系統應該是只能由本系統所能使用的特殊系統，必須採取一定的安全措施。安全性主要是通過對用戶接取認證、資料安全性、資料秘密性、網路資料同步及故障恢復這些方式來保證。
- 主權（Sovereignty）：雖然網路及名稱與號碼解析系統旨在提供國內及全球服務，但需要確保受影響國家的治理主權不受質疑。

二、電信網路號碼標準

電信號碼做為全球電信用戶通訊溝通之用，其編碼規則須經協調，並設定電信技術標準加以規範使用。國際電信聯合會（International Telecommunication Union, ITU）是從事電信領域之國際交流與合作的聯合國專門機構，轄下之電信標準化部門（ITU-Telecommunication Sector, ITU-T）負責研究技術及其他問題，並發布相關技術標準[5]，在全球範

[5]在 ITU 慣稱為建議書（Recommendations）。

圍內促進並實現電信標準化。

ITU-T 的標準化工作主要在各電信領域研究組（Study Group, SG）進行[6]。ITU-T 的組織架構如圖 2-1 所示。

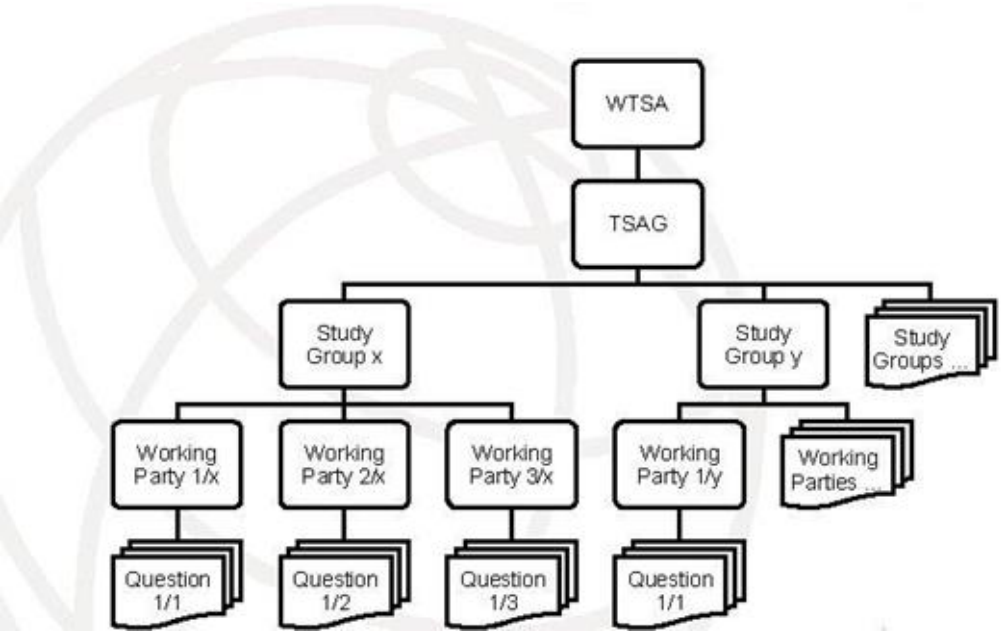


圖 2- 1、ITU-T 組織架構

資料來源：ITU

ITU-T 成員可指派代表參加 SG 的研究工作。原則上，每個 SG 負責一個特定資通訊領域的研究，若領域較大，可再分成數個工作組（Working Party, WP），以聚焦於特定專業領域或技術（或業務）項目的標準制定。

世界電信標準化全會（World Telecommunication Standardization Assembly, WTSA）每四年召開一次大會。其主要任務為確定 ITU-T 的總體政策、修訂或發布新的決議（Resolution）、建立 SG、批准包含未來四年期間研究課題（Question）的工作計畫，以及任命各 SG 經選舉產生的主席、副主席。原定 2020 年 11 月舉行的下期 WTSA 大會受

[6] ITU-T, Standards Development, available at https://www.itu.int/en/ITU-T/about/Pages/development.aspx (Last visited:Jul. 15, 2021)

Covid-19 影響已二度推遲，改至 2022 年 3 月[7]。

在 2016 年 10 月 25 日至 11 月 3 日舉行的 WTSA-16 大會，除決定保持 ITU-T 現有 11 個 SG，亦發布共 60 件決議（含修訂 47 件）及 1 份意見書[8]，其中與「編號、命名、定址和識別」（numbering, naming, addressing, and identification, NNAI）等電信網路號碼資源相關的文件包括：

- 第 20 號決議－《國際電信號碼、命名、定址和識別資源的分配與管理程序》；
- 第 47 號決議－《國家（或地區）的頂級網域》；
- 第 48 號決議－《國際化（多語言）域名》；
- 第 49 號決議－《ENUM》；
- 第 60 號決議－《應對識別/號碼系統的演進及其與 IP 系統/網路匯流所帶來的挑戰》；
- 第 61 號決議－《對國際電信號碼資源挪用及濫用行為的抵制和打擊》；
- 第 64 號決議－《IP 位址分配以及推進向 IPv6 的過渡》；
- 第 65 號決議－《發話對象號碼傳送、主叫用戶識別和始發地識別資訊》；以及
- 第 91 號決議－《加強對 ITU-T 編碼計畫資訊所設電子資料庫的訪問》。

《WTSA 行動計畫》，由電信標準化顧問組（Telecommunication Standardization Advisory Group, TSAG）提供，作為監督和促進 WTSA 成果落實的工具[9]。

[7] ITUT-T, WTSA-20, available at https://www.itu.int/en/ITU-T/wtsa20/Pages/default.aspx (Last visited:Jul. 15, 2021)
[8] ITU-T, Resolutions and Opinions 2016 editions, available at https://www.itu.int/pub/T-RES (Last visited:Jul. 15, 2021)
[9] ITU-T, ITU-T TSAG (Study Period 2017) Temporary Document 789: Action plan related to the Resolutions and Opinion of WTSA-16, available at https://www.itu.int/md/T17-TSAG-200921-TD-GEN-0789 (Last visited:Jul. 15, 2021)

三、ITU-T 未來網路及行動網路之發展

ITU-T 第 13 研究組（SG13）除了領導開展 ITU 有關 NGN 的標準制定工作外，亦持續致力於研究未來網路（Future Network, FN）相關議題及行動通訊網路之架構設計。

從廣義的角度來說，NGN 係指全球電信網路由傳統電路交換向封包交換的過渡，其主要目的為降低服務提供者的資本支出（Capital Expenditure, CAPEX）和運營支出（Operating Expense, OPEX），並能協助其提供加豐富多樣的業務，例如 IPTV 網路電視。NGN 不但已經實際應用於固定與行動匯流（Fixed Mobile Convergence, FMC）、電信與廣播匯流，亦通過智慧交通系統（Intelligent Transportation System, ITS）來支援資通訊科技（Information and Communication Technology, ICT）產業與汽車製造業等跨行業、跨領域之匯流。

SG13 所制定之標準主要為 ITU-T 建議書的 Q 系列《交換及信令》和 Y 系列《全球資訊基礎建設、網際網路協定、下世代網路、物聯網及智慧城市》。SG13 並將研究重點放在雲端運算（cloud computing）、泛在網路（ubiquitous networking）、分散式服務聯網（distributed service networking）、隨意（ad-hoc networks）網路、軟體定義網路（Software-Defined Networking, SDN）、網路虛擬化（Network Virtualization）、物聯網（Internet of things, IoT）、節能（energy saving）網路等。

2018 年 7 月，SG13 會議通過成立 FG-NET-2030 焦點小組（Focus Group on Technology foe Network 2030），並設定目標為：

- 檢討並盤點現今的技術、平臺和標準，確認其與未來網路之間的落差與挑戰；
- 提出未來網路之願景、需求、架構、使用情境、評估方法等；
- 為標準化路徑提供指引；以及
- 與其他標準制定組織建立聯繫。

在為期兩年的研究後，FG NET-2030 共召開了 6 次研討會，最後在

2020 年 6 月提出白皮書等相關文件報告，並於同年 7 月結束其工作。

在前述相關文件報告中，提出了一些對於 2030 未來網路使用案例與情境以及其規格需求，包括：

- 全息式通訊（Holographic Type Communications, HTC）
- 觸覺網際網路（Tactile Internet for Remote Operations, TIRO）
- 智慧營運網路（Intelligent Operation Network, ION）
- 網路和運算匯流（Network and Computing Convergence, NCC）
- 數位分身（Digital Twin, DT）
- 太空地面整合網路（Space Terrestrial Integrated Network, STIN）
- 結合雲端運算的工業物聯網（Industrial Internet of Things, IIOT）

以上需求可再歸納為提供精確時間控制的確定性時間延遲服務、多種媒體和資料串流傳送的異質網路互通和超大頻寬流量的服務等。當多種應用共存時，也可以分為多個適當損失級別的網路容錯需求。針對 2030 年以後的通訊技術要滿足上述需求，就需要發展出確定性時間延遲網路能力、多協定異質網路互通能力，以及靈活智慧的通訊策略制定和控制能力。

四、IETF 下世代網路技術標準之發展

眾所周知，網際網路工程任務組（Internet Engineering Task Force, IETF）不但是致力於 Internet 標準研究的民間標準制定組織，亦是網路技術領域諸多重要標準的發源地，故在全球業界擁有廣泛的影響力。自成立 30 多年來，IETF 已制定逾 9 千份徵求意見稿（Request for Commends, RFC）形式的文件，這些成果支撐起了整個 Internet 的標準體系和運行。

為了應對各種業務的新需求，網路技術領域的研究人員一直在致力於對網際網路通訊協定（Internet Protocol, IP）的改善。面對 IP 網路「盡力而為」設計初衷所強調的基本特性，業界存在著保守派和改良派兩種技術演進路線。以 IETF 社群為首的保守派推崇繼續以修補方式（patch）解決 TCP/IP 協定堆疊的不足。改良派則傾向於進一步完善 IP

網路頂層設計，並認為修補作法無法從根本上解決 IP 網路長期以來所積累的諸多問題，包括：

- IPv6 延伸標頭所產生的問題：延伸標頭（Extension Header, EH）是 IPv6 與 IPv4 之間的重要區別。IPv6 改採固定長度並簡化基本標頭的設計，雖讓封包轉送效能提高，但也由於將 hop-by-hop 選項移至 EH，不但容易導致傳輸頻寬的浪費（overhead），亦不利於發展對合理功耗益加重視的下世代通訊技術與協定。
- IPv6 需有固定的位址長度：IETF IPv6 低功率無線個人區域網路（IPv6 over Low-Power Wireless Personal Area Network, 6LoWPAN）工作小組規定的標頭壓縮技術，目前由電池供電的物聯網設備，過於佔用 CPU 資源。
- IPv6 不提供高品質的服務：某些應用程式需要規範嚴謹的端到端（E2E）延遲需求，需無重傳封包與無數據封包丟失的服務傳輸。在一些特定的需求下，是需要確定 E2E 吞吐量和延遲。因此，當前的 TCP/IP 不適合，重要的可靠度傳輸與即時 E2E 應用程式。
- 在自適應視頻串流中，缺乏標準化的解決方案：像 RFC 2205 資源預留協定(Resource Reservation Protocol, RSVP)這樣的解決方案，是借於路由器的發布，並不能擴展。路由器發布是 IPv6 數據封包中的特殊選項，用於向路由器發出信號以執行特定處理。當資料封包過於擁塞時的管理，還有改進空間，例如讓路由器知道這些應用程式，所擁有最小可接受頻寬限制，並可能做出更好的決定方向，來丟棄數據封包數據，例如將數據品質需求降級到可接受的級別。
- IETF DetNet 工作組僅規範最大延遲，而不是界定延遲範圍：DetNet 也尚未確定所規劃引入的服務，是否能在網路上成功運行；而目前主要關注的短期目標，是使它們能夠在有限制

的網域內網路中使用。

- 路由控制平面協定仍有改善空間：在高階路由器中，常見控制平面與轉發平面分離設計，並個別配置獨立的處理器。然而，目前多數廠商僅針對轉發平面發展到可用非常快的硬體加速性能（network functions virtualization infrastructure forwarding plane, NFVI FP），相對地對於控制平面則無類似之設計，以更能滿足未來新興應用情境下對通訊技術之要求。
- 用戶到網路端的應用程式介面(Application Programming Interface, API)是必要的需求：一些網路佈建模型需要來自用戶與應用程式的特定訊號機制，這是 E2E 服務所需要的，以儘可能提供品質或高精度網路。

為應對前述 IP 網路長期以來積累的諸多問題，在 ITU-T FG NET-2030 所提出的「未來垂直通訊網路和協定（Future Vertical Communication Networks & Protocols, FVCNP）」概念中，總結出未來網路將支援多項特點，其包括：

- 位址定義
- 可變長度位址
- 異構網路
- 服務確定性
- 內容安全與隱私
- 高吞吐量
- 定義端點轉發操作

五、太空地面整合網路之定址問題

相比地面行動通訊網路，利用運行在太空的高、中、低地球軌道（Low Earth Orbit, LEO）衛星可實現廣域甚至全球的訊號涵蓋，為更多用戶提供無差別的通訊服務。

3GPP TR38.811、TR22.822 等文件中，討論了衛星通訊相關議題，

包括非地面網路（Non-terrestrial Network, NTN）的技術特性、優勢及垂直應用等。5G 地面通訊 LEO 衛星通訊的整合，目前已知將衍生相關問題，包括：

- LEO 衛星覆蓋範圍隨時間與區域變化
- 傳播延遲
- 都卜勒效應

網際網路號碼分配局(Internet Assigned Numbers Authority, IANA)甫於 2021 年 10 月 25 日發布一篇名為〈太空地面整合網路中的定址問題與需求（Problems and Requirements of Addressing in Integrated Space-Terrestrial Network）〉的資訊文件，除介紹低軌衛星星座、地面終端/地面站及其互連網路的基礎知識，並明確地分析了低軌衛星相對於地面的移動性，以及在網路拓撲、定址和路由的影響與挑戰；該文件並詳細討論了太空地面整合網路對定址的要求，包括唯一性、穩定性、局部性、可擴展性、效率以及與地面網際網路的向後兼容性。最後概述了在該類網路中定址的問題和要求。

六、衛星寬頻上網服務之規範原則

近年間，包含 Starlink、OneWeb、Project Kuiper 等數家外國企業積極建構低軌衛星星座，其主要目的是在全球覆蓋範圍內（包含我國）提供高速寬頻衛星上網服務，經初步研判，除非 Starlink 等公司未來將增加全球語音通話服務，否則應無向我國申請 E.164、E.212 等號碼資源之必要。

在我國法規及行政體制下，以衛星通訊方式提供高速寬頻上網服務，至少涉及電信事業使用頻率及配合通訊監察等監管義務，由電信管理法及相關子法規管之。經參考過去允許國際衛星電話服務在國內提供服務之規管經驗，本計畫綜整提供應加注意之政策原則如下：

- 使用本地 IP
- 合作形態核備
- 合作需經主管機關許可

- 通訊監察
- 資料在地化
- 使用者實名制，包括外國人攜帶自有設備之入境申報與短暫使用規定等。

第二節　IPv6 技術標準之發展

一、IETF 主導 IPv6 技術標準發展

自 1994 年起，IETF 組織全球 Internet 工程師和專家積極參與 IPv6 技術標準、過渡、營運等各方面標準的制定工作，最終形成了 IPv6 的系列標準。在 2016 年年底，隸屬於網際網路協會（Internet Society, ISOC）的網際網路架構委員會（Internet Architecture Board, IAB）發布關於 IPv6 的一項重大聲明，即停止要求在新的或者擴展協定繼續相容於 IPv4，將來的協定制定和優化工作都應該基於 IPv6 來進行。

2017 年，IETF 對 RFC 2640 進行更新，發布新版 IPv6 技術規範—RFC 8200，IPv6 由此從「標準草案（Draft Standard）」成為「正式標準（Standard Track）」，足以證明 IPv6 基本技術已經成熟，具備高度的可用性。

作為 Internet 的新一版網路層協定，IPv6 協定具有通用性，與資訊網路系統中的終端、管理、雲端、應用等各個環節均密切相關。IPv6 協定設計工作在 IETF 是由多個工作組（Working Group, WG）共同推動，並以網路領域（Internet Area, INT）的 WGs 最具代表性，包括：6lo（IPv6 over Networks of Resource-constrained Nodes）、6man（IPv6 Maintenance）、6tisch（IPv6 over the TSCH mode of IEEE 802.15.4e）和 lpwan（IPv6 over Low Power Wide-Area Networks）等，每個 WG 都有其任務定位和目標[10]。

此外，儘管有些 WG 不是專門負責制定 IPv6 標準，但其工作和

[10] TWNIC (2021), IETF 網路領域中負責 IPv6 相關工作組簡介, available at https://blog.twnic.tw/2021/05/27/18758/ (Last visited:Dec. 5, 2021)

IPv6 具有密切的關係，例如在維運與管理領域（Operations and Management Area, OPS）下設的 v6ops（IPv6 Operations）和 mboned（MBONE Deployment）[11]，以及在路由領域（Routing Area, RTG）下設的 Babel（Babel routing protocol）、idr（Inter-Domain Routing）、lsr（Link State Routing）、lsvr（Link State Vector Routing）、mpls（Multiprotocol Label Switching）、rift（Routing In Fat Trees）、roll（Routing Over Low power and Lossy networks）和 spring（Source Packet Routing in Networking）[12]等。

其中，6man WG 負責維護 IPv6 基礎標準，也是討論 IPv6 相關問題的主要場所。IPv6 網路維運的研究工作主要在 v6ops WG 開展，重點討論現有或者新建網路中如何部署和維運 IPv6，並為 IPv6 的運行提供指南。在 IPv6 與物聯網匯流方面的工作主要分佈在 6lo、6tisch 等 WGs。6lo 主要是研究將 IPv6 適配在多種類型的 6loWPAN 通訊技術上並制定相關標準。6tisch 負責制定運行在 IEEE 802.15.4 時隙調頻（Time Slotted Channel Hopping, TSCH）模式上的 IPv6 的架構和技術標準。

二、IPv6 最新技術標準

IPv6 基礎標準主要為定義 IPv6 的基本標頭、延伸標頭、分段、上層處理等方面的技術。以 RFC 8200 為代表的系列 RFC 標準，在 IPv6 技術體系中具有根本性的地位。其他 IPv6 相關技術（如基於 IPv6 的原始路由 SRv6）都構建在 IPv6 基礎標準之上，因此 IPv6 基礎標準也就是核心標準。其他新的協定標準制定時必須參考 RFC 8200，並遵循其中的規定才能最終有效。

自 2020 年 4 月以來，IETF 陸續發布多項與 IPv6 相關之 RFC 提案，如表 2- 1 所示。

[11] TWNIC (2021), IETF 維運與管理領域中負責 IPv6 相關工作組簡介, available at https://blog.twnic.tw/2021/08/31/19855/ (Last visited:Dec. 5, 2021)
[12] TWNIC (2021), IETF 路由領域中負責 IPv6 相關工作組簡介, available at https://blog.twnic.tw/2021/10/29/20706/ (Last visited:Dec. 5, 2021)

表 2- 1、近期 IETF IPv6 相關 RFC 提案

編號	標題	發布日期	文件狀態
RFC 9099	Operational Security Considerations for IPv6 Networks	2021/8/13	Informational
RFC 9098	Operational Implications of IPv6 Packets with Extension Headers	2021/9/20	Informational
RFC 9085	Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing	2021/8/1	Proposed Standard
RFC 9034	Packet Delivery Deadline Time in the Routing Header for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	2021/6/1	Proposed Standard
RFC 9030	An Architecture for IPv6 over the Time-Slotted Channel Hopping Mode of IEEE 802.15.4 (6TiSCH)	2021/5/29	Informational
RFC 9011	Static Context Header Compression and Fragmentation (SCHC) over LoRaWAN	2021/4/1	Proposed Standard
RFC 9010	Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves	2021/4/1	Proposed Standard
RFC 9008	Using RPI Option Type, Routing Header for Source Routes, and IPv6-in-IPv6 Encapsulation in the RPL Data Plane	2021/4/1	Proposed Standard
RFC 8994	An Autonomic Control Plane (ACP)	2021/5/1	Proposed Standard
RFC 8992	Autonomic IPv6 Edge Prefix Management in Large-Scale Networks	2021/6/9	Informational
RFC 8986	Segment Routing over IPv6 (SRv6) Network Programming	2021/2/1	Proposed Standard
RFC 8983	Internet Key Exchange Protocol Version 2 (IKEv2) Notification Status Types for IPv4/IPv6 Coexistence	2021/2/1	Proposed Standard

編號	標題	發布日期	文件狀態
RFC 8981	Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6	2021/2/1	Proposed Standard
RFC 8956	Dissemination of Flow Specification Rules for IPv6	2020/12/1	Proposed Standard
RFC 8950	Advertising IPv4 Network Layer Reachability Information (NLRI) with an IPv6 Next Hop	2020/11/1	Proposed Standard
RFC 8931	IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Selective Fragment Recovery	2020/11/1	Proposed Standard
RFC 8930	On Forwarding 6LoWPAN Fragments over a Multi Hop IPv6 Network	2020/11/1	Proposed Standard
RFC 8929	IPv6 Backbone Router	2020/11/1	Proposed Standard
RFC 8925	IPv6-Only Preferred Option for DHCPv4	2020/10/1	Proposed Standard
RFC 8885	Proxy Mobile IPv6 Extensions for Distributed Mobility Management	2020/10/1	Experimental
RFC 8880	Special Use Domain Name 'ipv4only.arpa'	2020/8/1	Proposed Standard
RFC 8801	Discovering Provisioning Domain Names and Data	2020/7/1	Proposed Standard
RFC 8754	IPv6 Segment Routing Header (SRH)	2020/3/1	Proposed Standard
RFC 8724	SCHC: Generic Framework for Static Context Header Compression and Fragmentation	2020/4/1	Proposed Standard

資料來源：本計畫整理

上面的表格中可以看出，提案主要集中在三個領域，一是應用在物聯網之低功耗廣域網路，以“RFC 9034 Packet Delivery Deadline Time in the Routing Header for IPv6 over Low-Power Wireless Personal Area

Networks (6LoWPANs)”為代表；二是持續完善 IPv6 過渡標準，以“RFC8950 Advertising IPv4 Network Layer Reachability Information (NLRI) with an IPv6 Next Hop”為代表；三是 IPv6 網路創新，以“RFC 8754 IPv6 Segment Routing Header (SRH)”為代表。IPv6 標準制定與 IPv6 發展部署息息相關，在加快 IPv6 過渡的同時，一方面保持持續創新，提升 IPv6 網路價值，另一方面積極在萬物互聯的場景下不斷拓展 IPv6 應用，為 IPv6 可持續發展建設完善的生態鏈[13]。

三、IPv6 技術趨勢分析

透過 IETF 主導 IPv6 發展脈絡及最新標準提案之文獻探討，可歸納出 IPv6 技術趨勢如下[14]：

- 遵循 Internet 開放式架構並促進開放化發展：IETF 是將 IPv6 作為未來 Internet 演進的根本性技術，目前沒有能與 IPv6 並駕齊驅的其他候選技術，而且其他所有的網路層技術更新和創新都是在 IPv6 的基礎上進行。而且，基於 IPv6 的 Internet 總體上還是延續了 IPv4 時代 Internet 的開放式端到端（End-to-End）架構，即「網路是一個服務於各種業務的通用系統，和應用層相關的功能不要放置在網路的核心」。可以預見，未來隨著 IPv6 的進一步引入，網路的開放式架構將持續發揮作用。
- IPv6-Only 將使得網路回歸簡潔：IPv6-Only 以 IPv6 協定作為網路的基礎通訊協定，提倡更多的 Internet 服務提供商用業務向 IPv6 遷移。IPv6-Only 在近期內也不是完全杜絕 IPv4，而是將 IPv4 作為 IPv6 基礎網路的業務，即 IPv4 即服務(IPv4 as a Service)。由於網路只需維護 IPv6 協定堆疊，因此 IPv6 單棧網路比雙棧網路更加簡潔，網路的管理維護負擔顯著減小。引入 IPv6-Only 的好處是利用 IPv6 大量位址滿足了終端的編址需

[13] GITC, 2021 全球 IPv6 支持度白皮書, available at https://www.ipv6ready.org.cn/public/download/ipv62.pdf (Last visited:Dec. 5, 2021)
[14] 解衝鋒，「從 IETF 動態看 IPv6 的發展趨勢」，信息通信技術與政策，2020，46(8): 12-17.

求，解決了位址不足的問題。新的業務場景，如工業 Internet、物聯網、車路協同等，沒有 IPv4 的歷史包袱，更應該在新的起點上採用 IPv6-Only 技術來發展，而不是沿用老的 IPv4 協定。不可否認的是，在當前 IPv4 業務流量仍處於主流的情況下，世界各國的商用網路仍處於引入 IPv6 的過渡階段，在網路從雙棧向 IPv6-Only 演進的過程中，網路層演進會相對較快一些，而業務完全遷移到 IPv6-Only 將會需要較長時間。

- SRv6 促進網路的智慧化：從技術角度看，SRv6 可以簡化網路的狀態和協定，適應雲端網路匯流和 5G 發展的趨勢，同時也提供了更好的網路可編程能力，在跨域方面也比基於多協定標籤交換的轉發平面路由(Segment Routing MPLS, SR-MPLS)更易部署，因此將成為 IP 網路未來發展的方向。結合目前 SRv6 標準成熟度，目前世界範圍已經有超過十多家的商業部署案例。
- IPv6 物聯網促進網路的普及化：隨著物聯網上 IPv6 相關技術逐漸成熟，Internet 從面向人的通訊逐漸延伸到人對物通訊、物對物通訊，終端的數量將從幾十億級向百億級甚至千億級發展，支撐這麼龐大的網路，也只有 IPv6 技術才能做到。另外，IPv6 的特點將滿足物聯網特有的一些需求，如基於 IP 位址的反向控制，這在 IPv4 網路中是難以做到的。從可行性來說，隨著物聯網晶片性能的提升，物聯網終端內的資源已經可運行完整的 IPv6 協定堆疊，並具備商用化的能力。IPv6 在物聯網的廣泛應用也將反過來推動 IPv6 技術本身的升級完善，如在路由、安全及可管理性等方面提出新的需求。

第三節　主要國家或地區推動 IPv6 發展政策

一、歐盟 IPv6 政策

在國際 IPv6 發展初期，主要以歐洲地區發展最為迅速、亞太地區

次之，而北美地區則因為起初掌握了大量的 IPv4 位址，當時短期內尚無 IPv4 位址枯竭之疑慮[15]。近年來隨著 IPv6 的未來發展與需求日趨顯著，世界各國亦正研擬各項 IPv6 的推動政策，以因應 IPv6 的使用需求以及未來網際網路發展趨勢。現今為網際網路快速發展的時代，網際網路服務與應用在 5G 行動通訊的蓬勃發展趨勢下，5G「超高速、低延遲、大連接」特性，帶動物聯網的大規模部署與需求，未來將進入萬物連網的時代，對於 IP 位址的需求也將明顯上升。

歐盟在 5G 發展的時代背景下，由歐洲電信標準協會（European Telecommunications Standards Institute, ETSI）產業規範小組（IPv6 Industry Specification Group, ISG IPv6）於 2020 年 8 月發布《IPv6 最佳實踐、優勢、過渡挑戰及未來展望》第 35 號白皮書，探討 IPv6 最佳實踐、使用範例、優勢和部署策略以及經驗等，並說明 IPv6 部署的案例經驗以及在 5G、物聯網和物聯網雲端運算（IoT Cloud Computing）下對於網路產生的新需求等[16]。該白皮書討論到以下幾點問題：

- IPv6 如何成為 5G、物聯網或雲端運算等技術優先發展的方向?
- IPv6 如何在各項指標，例如用戶數量、內容百分比和流量等，成長幅度皆較 IPv4 迅速?
- 在 IPv6 的部署上，雲服務提供商和營運商是如何成功部署，而其經驗為何?
- 在 5G 時代發展下，自駕車、智慧電網與工廠自動化等應用，如何藉由使用 IPv6 於 M2M 通訊上受益?
- IPv6 的應用如何為 5G、低功耗無線電、SDN、網路功能虛擬（Network Functions Virtualization, NFV）、雲端運算提供益處?

本計畫針對 ETSI 提出之 IPv6 白皮書，分別從 IPv6 的優點、IPv6

[15]〈先進國家業 IPV4/IPV6 位址經驗分析報告〉，《九十八年度新一際網路協定互通認證計畫期末研究報告附件》，法規政策分類，2009，
<http://www.ipv6.org.tw/docu/elearning8_2009/1009804292b-08.pdf> p.165

[16] ETSI, IPv6 White Paper outlines best practices, challenges, benefits and the way forward, available at https://www.etsi.org/newsroom/news/1814-2020-08-etsi-ipv6-white-paper-outlines-best-practices-challenges-benefits-and-the-way-forward (Last visited:Dec. 5, 2021)

轉換的解決方案、IPv6 部署策略以及 ETSI 對於歐盟 IPv6 發展之建議說明之。

1. IPv6 的優點

雖然作為網際網路的新一代網路協定 IPv6 已存在 25 年，但隨著 5G、物聯網、雲端服務等新興技術的問世，更多新興應用服務孕育而生，並對 IPv6 的部署亦產生更多新的需求以及要求。而 IPv6 提供的特質正好為以下幾種新的網際網路要求以及需求帶來好處，包括:

- 有利於網際網路編程（Network Programming）：由於營運商必須快速提供服務，並提供客製化服務來滿足客戶的要求，因此於此方面，IPv6 與做為基於 IPv6 數據層（IPv6 data plane）的 SRv6 網路編程概念具有關連性。
- 符合低延遲需求（Low Latency）: 由於網際網路應用對於低延遲的需求與日俱增，有低延遲需求之數據應沿著沒有過載的路徑傳送，或者需要新的佇列技術（queue technique）優化延遲，因此 IPv6 易於與低延遲技術整合。
- 能配合網路切片的需求（Nework Slicing）:有鑑於現今或未來某些網路服務需要專用的網路與其他網路服務區隔，而這類型網路服務之數量可大於具有 QoS 之流量等級的數量，產生於公共基礎設施上創建多種獨特類型和虛擬化網路的要求，即網路切片。而 SRv6 和 IPv6 的端到端模式能配合網路切片的需求運作。
- 滿足物聯網與日遽增的需求（IoT）:IPv6 在位址的運用上用更加靈活，且可在不使用網路位址轉換（Network Address Translation, NAT）的情況下進行分配。另外，有些物聯網應用甚至為 IPv6 能夠在設備的生命週期內維持位址不變，因此藉由 IPv6 可更加容易接取和控制設備位址。

2. 過渡到 IPv6 的解決方案

ETSI 將 IPv4 過渡到 IPv6 的建議作法分為兩類，包括從 IPv4 過渡到 IPv6 技術的 IPv6 連接，以及 IPv4 過渡到 IPv6 技術的 IPv4 連接[17]。

除了上述解決方案外，白皮書亦提出兩個 IPv6 的轉換過程，包括導入 IPv6（IPv6 introduction）以及 IPv6-only。IPv6 導入為於既有的 IPv4 網路中部署 IPv6 服務。而 IPv6 服務為在 IPv4 服務之上或從旁提供，並採用 IPv4/IPv6 雙軌模式（IPv4/IPv6 dual-stack pattern），並於此階段獲得 IPv6 的使用經驗。

當 IPv6 流量增加至某種程度限制時，即可轉移至 IPv6-only 階段。而在該階段為訂戶提供的服務僅於 IPv6 上提供，即用戶終端設備（Customer Premise Equipment, CPE）在 WAN 側（WAN side）只有一個 IPv6 位址，並使用 IPv6 連接到網路服務業者的閘道器（gateway），例如寬頻網路閘道器（Broadband Network Gateway，BNG）或封包閘道器（Packet Gateway, PGW）以及用戶平面管理功能（User Plane Function, UPF）。但是主機（the host）和內容服務器（content server）仍可為 IPv4 和/或 IPv6。例如，NAT64 可以使 IPv6 主機訪問 IPv4 伺服器，且骨幹網路（backbone network）底層亦可為 IPv4 或 IPv6。另外服務傳遞架構（The service delivery architecture）純粹為 IPv6，唯在接入（access）面，IPv4 服務是透過 IPv6 提供。

3. IPv6 部署策略

在 IPv6 的部署策略上，ETSI 認為除了須明確區分前述所提 IPv6 的兩個轉換階段，即 IPv6 導入以及最終的 IPv6-only 外，亦須注意調整人和組織對於 IPv6 的認識、審視基礎設施之 IPv6 能力、導入 IPv6 以及升級其他類型網路以降低成本。

4. ETSI 對於歐盟 IPv6 發展之建議

[17] ETSI, GR IP6 006 V1.1.1 (2017-11) - Generic migration steps from IPv4 to IPv6, available at https://www.etsi.org/deliver/etsi_gr/IP6/001_099/006/01.01.01_60/gr_IP6006v010101p.pdf (Last visited:Dec. 5, 2021)

ETSI 認為歐盟應負起責任力促各成員國部署 IPv6，再者，ETSI 亦認為可借鏡一些國際上政策作為鼓勵改用 IPv6 或加強 IPv4 的安全性。例如美國於 2020 年 3 月所發布的 IPv6 備忘錄。該備忘錄更新美國聯邦政府對於 IPv6 的營運部署和使用的指引，並強烈建議應在規定期限前完成 IPv6 的轉換。

即使在沒有提供各界轉換 IPv6 資金的支持下，ETSI 建議亦可強制公部門增加與 IPv6 的相容性，藉此提高 ISP 業者發展 IPv6 的意願與動力等，強化基礎設施支援 IPv6；政府應在 IPv6 的政策推動上扮演重要的推手，帶領國家進行轉型；在 ITU 的支持下，鼓勵 RIR 和其他區域組織在政府、行業和學術界的參與下共同協調研究、傳播和培訓行動，以促進 IPv6 在歐盟各國的部署和使用；在歐盟境內，協調區域之間的舉措，以促進其在國際的部署。

另外，ETSI 亦建議應鼓勵製造商在除了向市場供應 IPv4 外，亦支持 IPv6 的全功能客戶端設備；提高資訊服務提供商（Information Service Provider, ISP）對透過 IPv6 提供服務重要性的認知等。

二、美國 IPv6 政策

從 2005 年開始，聯邦政府的 IPv6 起到催化作用，促進了 IPv6 技術的商業開發和採用。IPv6 在產業中的發展趨勢顯著增強，許多大型網路營運商、軟體供應商、服務供應商、企業、州政府和外國政府已經部署 IPv6 關鍵基礎建設。鑒於在 IPv4/IPv6 雙協定運作下，帶來相當程度的複雜性、營運成本和風險威脅，美國開始積極轉向 IPv6-only 網路環境之部署。

2020 年 11 月 19 日，美國總統行政辦公室（Executive Office of the President, EOP）行政管理和預算局（Office of Management and Budget, OMB）向行政部門和機構負責人發布 M-21-07《完成向 IPv6 過渡》備

忘錄，提出各機構為完成向 IPv6 過渡可採取的具體步驟[18]，備忘錄指示：

- 在此備忘錄發布後 45 天內，成立包括採購、政策和技術成員的完整團隊，以有效治理和執行 IPv6 工作。
- 在此備忘錄發布後 180 天內，在機構公開網站上發布 IPv6 政策，要求至 2023 財政年度末，所有新的聯邦網路資訊系統都支援 IPv6，並逐步停用 IPv4。
- 在 2021 財政年度末前，完成至少一個 IPv6-only 作業系統之試點，並向 OMB 報告試點結果。
- 在 2021 財政年度末前，制定 IPv6 實施計畫，並包括下列階段目標：
  a. 2023 財政年度末，至少 20%的聯邦網路資產只支援 IPv6；
  b. 2024 財政年度末，至少 50%的聯邦網路資產只支援 IPv6；
  c. 2025 財政年度末，至少 80%的聯邦網路資產只支援 IPv6；
  d. 確定和證明無法轉換至 IPv6 的聯邦資訊系統，並擬定更換或停用這些系統的時間表。
- 與外部合作夥伴合作，確定與聯邦網路連結的系統，並制定計畫將其轉換至 IPv6。

備忘錄中提及「向 IPv6 全面過渡」是確保未來網路技術和服務能增長和創新的唯一可行選擇，美國聯邦政府必須擴大和增強其向 IPv6 過渡的戰略承諾。同時，該備忘錄也要求行政部門和機構的外部合作夥伴與聯邦網路系統介接連結，須制定計畫將所有網路介接移轉支援 IPv6。諸如 Web、電子郵件，DNS 和 ISP 服務等公用／外部服務和內部用戶端應用服務，均在升級支援 IPv6-only 的範圍。

由於 IPv6 推動較難具備外顯的商業利益，多由政府或學術機構擔任領頭羊角色。美國聯邦政府採取政府示範帶動企業跟進的策略，透過行政命令，訂定機構內網路基礎至服務的全面性改造，以此帶動設

[18] US EOP, Completing the Transition to Internet Protocol Version 6, available at https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf (Last visited:Dec. 5, 2021)

備及服務業者支援，並藉此達到技術成熟，更有利推動一般企業進而採用，加速網路向 IPv6-only 發展。

此外，美國聯邦政府採購之 IPv6 資通設備，必須通過國家標準暨技術研究院（National Institute of Standards and Technology, NIST）之 USGv6 測試計畫[19]，為了回應 OMB 發布之 M-21-07 備忘錄，NIST 亦再發布特別出版物 SP500-267，對 USGv6 規範和測試計畫進行重大修正，以更新其技術規範[20]。根據備忘錄要求，機關（構）在購買網路資訊技術和服務時，應繼續使用 USGv6 規範與測試計畫。

1. 聯邦能源管理委員會 IPv6 政策

按照 OMB 備忘錄 M-21-07 之規定，聯邦能源監管委員會（Federal Energy Regulatory Commission, FERC）於 2021 年 5 月 18 日發布《聯邦能源管理委員會 IPv6 政策》[21]，該政策旨在確保和執行過渡到 IPv6 過程，達成聯邦政府的推進計畫。此政策適用於所有 FERC 資訊系統，包括由承包商和其他機構正在開發、使用、管理或營運的資訊系統。

具體來說，包含落實 IPv6 部署，於 2023 年全面啟用 IPv6，並逐步淘汰所有使用 IPv4 之機構系統；在 2021 年底前完成至少一個 IPv6-only 營運系統之試點，並向 OMB 報告試點結果；制定 IPv6 實施計畫，設立 2023 年 20%、2024 年 50%、2025 年末 80%過渡至 IPv6-only 之里程碑。確保網路資訊技術採購符合《聯邦採購條例》規定的 IPv6 要求，包括參考 NIST SP500-267 以及 USGv6 規範文件和測試計畫。所有 FERC 資訊系統也需符合全面支持 IPv6 服務的規劃；驗證所有支持網路營運或企業安全服務的系統（例如，身份識別和存取管理系統、防火牆和入侵檢測／保護系統、

[19] NIST, Updates USGv6 Program in Support of New Federal IPv6 Initiatives, available at https://www.nist.gov/news-events/news/2020/12/nist-updates-usgv6-program-support-new-federal-ipv6-initiatives (Last visited:Dec. 5, 2021)
[20] NIST, IPv6 Profile, available at https://www.nist.gov/publications/nist-ipv6-profile (Last visited:Dec. 5, 2021)
[21] US FERC, Internet Protocol Version 6 (IPv6) Policy, available at https://www.ferc.gov/media/ferc-internet-protocol-version-6-ipv6-policy (Last visited:Dec. 5, 2021)

存取控制和政策執行系統等）可以在 IPv6-only 的環境中運作；確保所有安全和隱私政策評估、授權和監控程序可完全處理聯邦資訊系統中 IPv6 的生產使用。

2. 國防部之 IPv6 實施

為遵循 OMB 要求所有部門和機構從 2023 年開始到 2025 年轉向 IPv6 only 環境，2021 年國防部發布 DoD 備忘錄 DTM 21-004《國防部之 IPv6 實施》[22]，於 6 月 29 日生效，並在國防部於網站上發布之日起 12 個月內到期。

根據聯邦要求，國防部將成立執行委員會，管理和執行 IPv6 過渡工作，並確定需要解決的挑戰，以確保持續取得進展。並根據 OMB 備忘錄 M-21-07 中的國防部和聯邦 IPv6 要求，所有政府資訊系統將發展到完全支持 IPv6 操作，並逐步停止使用 IPv4。遵守 NIST USGv6 規範，並且在可能的情況下，利用 NIST USGv6 測試計畫對商業產品進行基本的一致性和互操作性測試。完成至 2025 年末，國防部至少 80%的網路資訊系統支援 IPv6-only 環境的總目標。

三、中國大陸 IPv6 政策

中國大陸於 2017 年根據《國民經濟和社會發展第十三個五年規劃綱要》、《國家信息化發展戰略綱要》、《十三五國家信息化規劃》，制定《推進互聯網協議第六版（IPv6）規模部署行動計畫》[23]（以下簡稱 IPv6 規模部署計畫），促進網路升級與創新發展。IPv6 規模部署計畫主要目標為用 5 至 10 年時間，形成下一代網路自主體系和產業生態，建成全球最大規模的 IPv6 商業應用網路，實踐下一代網路在經濟社會各領域深度融合應用。並透過「加快網路應用服務升級，不斷豐富網路

[22] US DoD, Implementation of Internet Protocol Version 6, available at https://media.defense.gov/2021/Jul/13/2002761414/-1/-1/0/DOD-MEMORANDUM-DEPARTMENT-OF-DEFENSE-IMPLEMENTATION-OF-INTERNET-PROTOCOL-VERSION-6.PDF (Last visited:Dec. 5, 2021)

[23] 中國大陸，印發《推進互聯網協議第六版（IPv6）規模部署行動計劃》，2017 年 11 月 26 日，http://www.gov.cn/zhengce/2017-11/26/content_5242389.htm

信源」、「開展網路基礎設施改造，提升網路服務水平」、「加快應用基礎設施改造，優化流量調度能力」、「強化網路安全保障，維護國家網路安全」以及「突破關鍵前沿技術，構建自主技術產業生態」等重點任務，全面完成向下一代網路前進升級。

透過推動 IPv6 規模部署計畫，中國大陸 IPv6 規模部署顯著進步，2021 年 7 月，依據《國民經濟和社會發展第十四個五年規劃和 2035 年遠景目標綱要」對於提升 IPv6 基礎建設要求，中國大陸發布《關於加快推進互聯網協議第六版（IPv6）規模部署和應用工作的通知》[24]（下稱：「IPv6 規模部署計畫通知」），敦促各級政府機關加速推動網路升級。

IPv6 規模部署計畫通知主要以全面推進 IPv6 技術創新與融合應用為主軸，並以提升應用廣度與深度為計畫推進方向，聚焦建構開放創新的技術體系、效能先進的設施體系、全面覆蓋的應用體系、生態良好的產業體系、系統完備的標準體系、自主可控的安全體系，實現 IPv6 規模部署和應用，打造創新發展優勢，為中國大陸的網路應用提供堅實的基礎。此外，透過「政府引導、市場驅動」、「創新賦能、應用落地」、「問題導向、分類施策」、「系統推進、保障安全」等基本原則，推動促進 IPv6 各項工作項目 。

在實施重點上，以「強化網路承載能力」、「優化應用服務性能」、「提升終端支持能力」、「拓展行業融合應用」、「加快政務應用改造」、「深化商業應用部署」、「培育創新產業生態」、「加強關鍵技術研發」、「推動標準規範制定」、「強化安全保障能力」等十大關鍵項目，簡述如下。

- 強化網路承載能力：包括提升 IPv6 網路性能和服務水平，確保 IPv6 網路關鍵性能指標和服務指標與網路協議第四版（IPv4）網路相同。並且為行動物聯網終端分配固定 IPv6 位址。增強 IPv6 網路互聯互通能力，物聯網交換中心與節點全

[24]中國大陸，關於加快推進互聯網協議第六版（IPv6）規模部署和應用工作的通知，2021 年 7 月 12 日，http://www.gov.cn/zhengce/zhengceku/2021-07/23/content_5626963.htm

面支援 IPv6。積極推進 IPv6 單軌網路部署，推進 5G 獨立組網（SA）、物聯網等網路部署 IPv6 單軌網路。加快廣電網路 IPv6 改造，全面推進廣播電視傳輸網路及寬頻數據網路 IPv6 改造，提高寬頻接入網路 IPv6 服務能力。

- 優化應用服務性能：強化應用基礎設施業務承載能力，推動新上線雲產品和新建節點全面支援 IPv6。推動 IPv6 與資訊基礎設施匯流發展。推動人工智慧、雲計算、區塊鏈、國家超級計算中心、智慧計算中心等資訊基礎設施全面支援 IPv6。
- 提升終端支持能力：補齊家庭網路終端 IPv6 接入的缺點，透過政策指導、標準引領、終端產品啟用 IPv6 功能以及家庭閘道器評測與升級等，完善家庭網路終端 IPv6 接取。完善智慧家庭 IPv6 產業生態：建構智慧家庭標準化體系，明確 IPv6 支援要求。同時，推動國內主要企業的智慧家居系統平台、設備產品、應用等對 IPv6 支援能力，並開展智慧家庭場景 IPv6 試點示範。

強化物聯網終端 IPv6 部署應用：明確 IPv6 網路接入要求，完善物聯網終端入網檢測標準規範；加強技術研發，提升物聯網終端 IPv6 網路連接能力。此外，推動消費物聯網終端、生產物聯網終端，以及公共物聯網終端同步支援 IPv6。同時，加快企業物聯網應用平台 IPv6 調整和舊有物聯網終端升級替換。

1. 拓展行業融合應用、深化商業應用部署、培育創新產業生態：中央企業、金融業、工業物聯網、數位鄉村建設、智慧醫療、媒體業等各行各業全面推動網路系統支援 IPv6，打造 IPv6 產業應用生態圈。推動商業平台進行 IPv6 網路應用全面升級，並強化商業應用 IPv6 入口管理，使全新網站與應用全面支援 IPv6，引領網站與應用朝向 IPv6 過渡。推動 IPv6 產業鏈共同創新，以及 IPv6 應用創新，建構 IPv6 創新產業生態系。
2. 加快政務應用改造、強化安全保障能力：推動電子政務公共平

台與政府網站 IPv6 升級，確保全面支援 IPv6 應用。建構 IPv6 網路安全防護體系，同時，提升 IPv6 環境下新興領域安全保障能力。

3. 加強關鍵技術研發、推動標準規範制定：研發 IPv6 關鍵核心技術，以及推動 IPv6 技術匯流創新。建構 IPv6 標準體系，並積極參與國際標準制定。

同時，中國大陸預計再五年後，將完成向 IPv6 單軌的過渡，IPv6 與各行業及各部門全面深度融合應用，成為全球網路技術創新、產業發展、基礎建設、應用服務、安全保障、網路治理等領域的重要力量。

目前中國大陸 IPv6 推動成果，主要為：

- 網路基礎設施全面支援 IPv6，全面完成 LTE 網路與固網 IPv6 升級改造，中國大陸三大營運商完成 30 個省的 LTE 網路、城域網網路 IPv6 改造，骨幹直聯點實現 IPv6 互聯互通，中國大陸的北京、上海、廣州、鄭州以及成都等 13 個骨幹直聯點全部完成 IPv6 改造，使 IPv6 網路質量與 IPv4 相同。
- 雲端平台的 IPv6 改造處於推進初期階段，阿里雲、天翼雲、騰訊雲以及華為雲等雲端平台已完成 IPv6 雲端主機、域名解析、雲端數據庫、應用程序接口（API）閘道器、Web 應用防火牆、分散式阻斷服務（DDoS）攻擊等公有雲產品的 IPv6/IPv4 雙軌化改造，公有雲產品平均改造率超過 70%，但支援 IPv6 之雲產品可用域的數量仍偏低。
- 部分物聯網終端支援 IPv6，家庭閘道器與路由器方面，90% 設備可支援 IPv6，但 IPv6 管理功能仍較弱，均不支援查看用戶信息，未來占比最大的產業物聯網終端目前基本不支援 IPv6[25]。

[25] 中國信息通信研究院，物聯網白皮書（2020 年），第 19-20 頁，2020 年 12 月，http://www.caict.ac.cn/kxyj/qwfb/bps/202012/P020201215379753410419.pdf

中國大陸期望透過各項加快推動 IPv6 規模部署工作項目，分別於 2030 年末以及 2025 年末達到以下目標：

- 2023 年末，IPv6 活躍用戶數達到 7 億；物聯網 IPv6 連結數達到 2 億；行動網路 IPv6 流量佔比達到 50%；城域網 IPv6 流量占比達到 15%；家庭無線路由器 IPv6 使用率達 30%。政府網站 IPv6 支援率達 80%；主要商業網站與行動網路應用 IPv6 支援率達 80%；IPv6+創新應用項目數量 100 個 。
- 至 2025 年末，IPv6 活躍用戶數達到 8 億；物聯網 IPv6 連結數達到 4 億；行動網路 IPv6 流量佔比達到 70%；城域網 IPv6 流量占比達到 20%；家庭無線路由器 IPv6 使用率達 50%。政府網站 IPv6 支援率達 95%；主要商業網站與行動網路應用 IPv6 支援率達 95%；IPv6+創新應用項目數量 500 個 。

第四節　新興網路技術與通訊協定發展

一、命名資料網路

雖然目前已有相對成熟的網路技術與通訊協定，使網際網路能夠滿足使用者的多數需求，但仍有組織提出預測，未來的網路流量成長速度遠高於網路建設速度，而當這樣的技術不斷地演進，網際網路本身的問題層出不窮，如使用者在查詢或分享資料時，習慣以查詢的資料名稱做為描述資料的資料（Metadata），而不是一連串沒有意義的數字，例如 IPv4 或 IPv6 位址。

為解決上述問題，網域名稱系統（Domain Name System, DNS）服務應運而生，但傳統集中式架構易造成單點錯誤與系統過載問題，因此，當熱門資訊需要重覆且快速地傳遞給每位使用者時，資訊核心網路（Information-Centric Network, ICN）的概念及相關技術因應而生，其目標是將目前以主機為基礎（Host-based）的網路轉換成以資訊為基礎（Information-based）的網路；另外，在網路結點安排可以暫時儲存資料的緩衝記憶體（Buffer），再加上良好的替換演算法，就可以節省

並降低網路頻寬的使用。此外，為了確保資料內容的安全性與可信度，也加入密碼學中的數位簽章及加密機制等。

綜合上述幾點特性，包括定址方式、路由機制、安全模型等，並搭配快取功能的概念，產生了新的網路架構，即為命名資料網路（Named Data Networking，NDN）[26]。

(一) NDN 基礎概念

當前，網際網路的沙漏體系結構係以通用的 IP 協定為中心，在網路層實現了全球互聯的最小必需功能。通過細腰結構上層（應用層）和下層（接取層）技術的獨立革新，使得網際網路普及率能夠迅速增長。

然而，IP 被設計來創建一個通訊網路，封包只在通訊端節點被命名。在電子商務、數位媒體、社交網路、智慧手機應用程式方面的持續增長導致了對於分散式網路的使用佔據統治地位。分散式網路比通訊網路更加普遍，通過點對點通訊協定解決分散式問題是複雜和易出錯的。

相較於 IP 協定封包係以主機是否到達、路由是否可用等網路訊息為主體，NDN 改以資料為中心重新思考，另闢途徑尋找一個新的網路架構設計，以解決目前傳統網路所遇到的問題及困境，因此被視為新一代網際網路候選方案。此一觀點上的改變，移除了傳統網路只能對終端命名的限制，讓使用者或網上服務不再專注於需要到何處獲取資料，取而代之的是著重於所需資料本身的形容。

NDN 提出了一個 IP 體系結構的革新，保留了沙漏結構中的細腰角色，以便封包可以命名物件而不被限制於通訊端節點。如圖 2-2 所示。

[26] Lixia Zhang et al., Named Data Networking, ACM SIGCOMM Computer Communication Review, Volume 44, Number 3, July 2014.

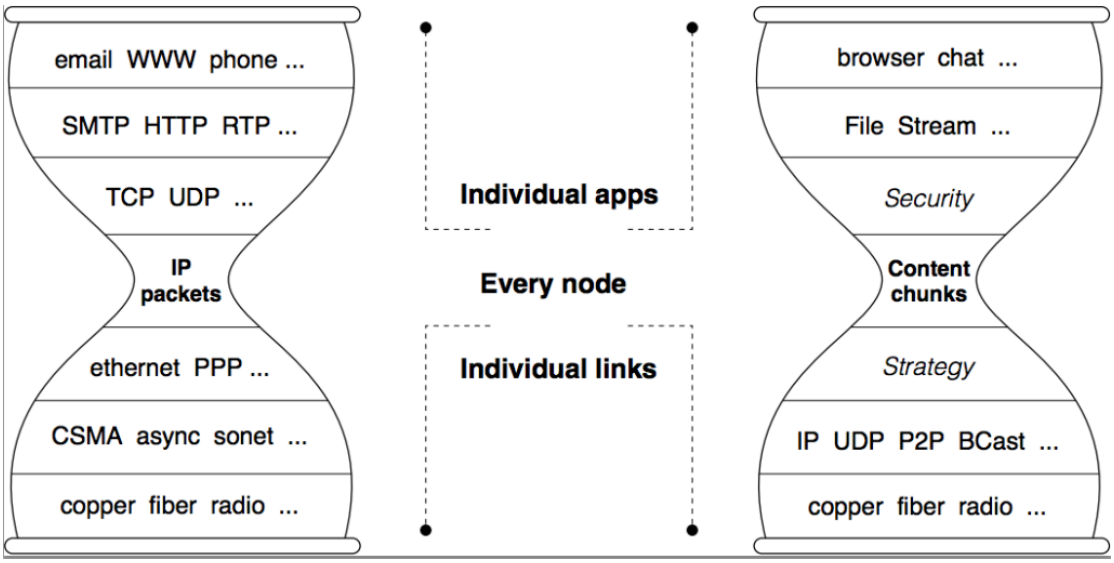


圖 2- 2、Internet 與 NDN 的沙漏結構對照

資料來源：named-data.net

NDN 中的通訊由接收者（例如資料消費者）通過交換兩種類型的封包驅動，興趣封包（Interest Packet）和資料封包（Data Packet），其各自的封包欄位與組成，如圖 2- 3 所示。當使用者想搜尋某資料時，只需要送出該資料名稱的興趣封包，路由器將會進行興趣封包的轉發，任何符合該名稱且擁有該標識資料的路由器，皆可以回傳相應之資料封包。

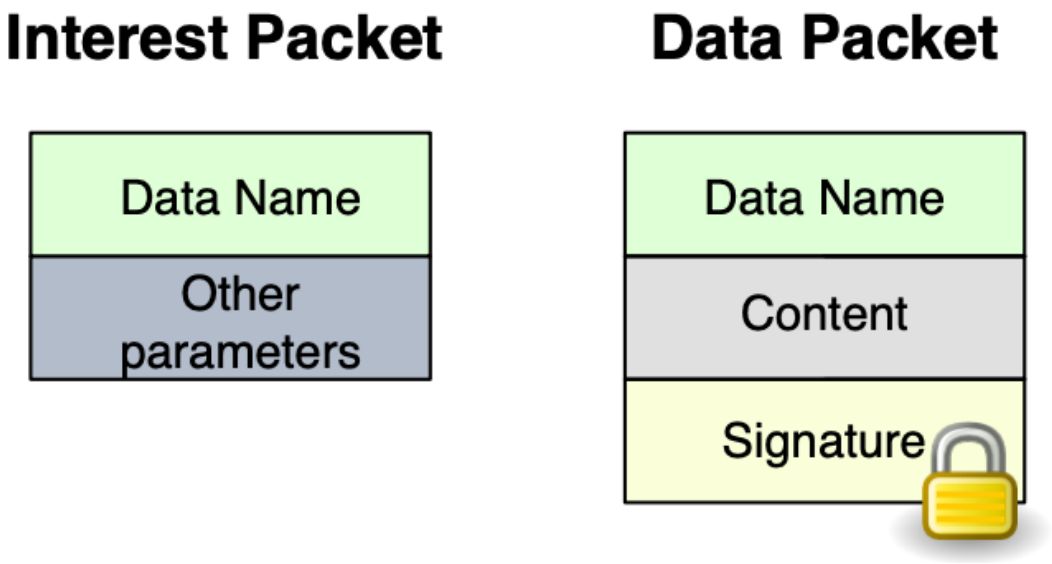


圖 2- 3、NDN 結構中的封包格式

資料來源：named-data.net

為了實現興趣封包和資料封包轉發功能，每個 NDN 路由器維護三個資料結構：待定興趣表（Pending Interest Table, PIT），轉發資訊表（Forwarding Information Base, FIB）和內容緩存（Content Store, CS），如圖 2- 4 所示。

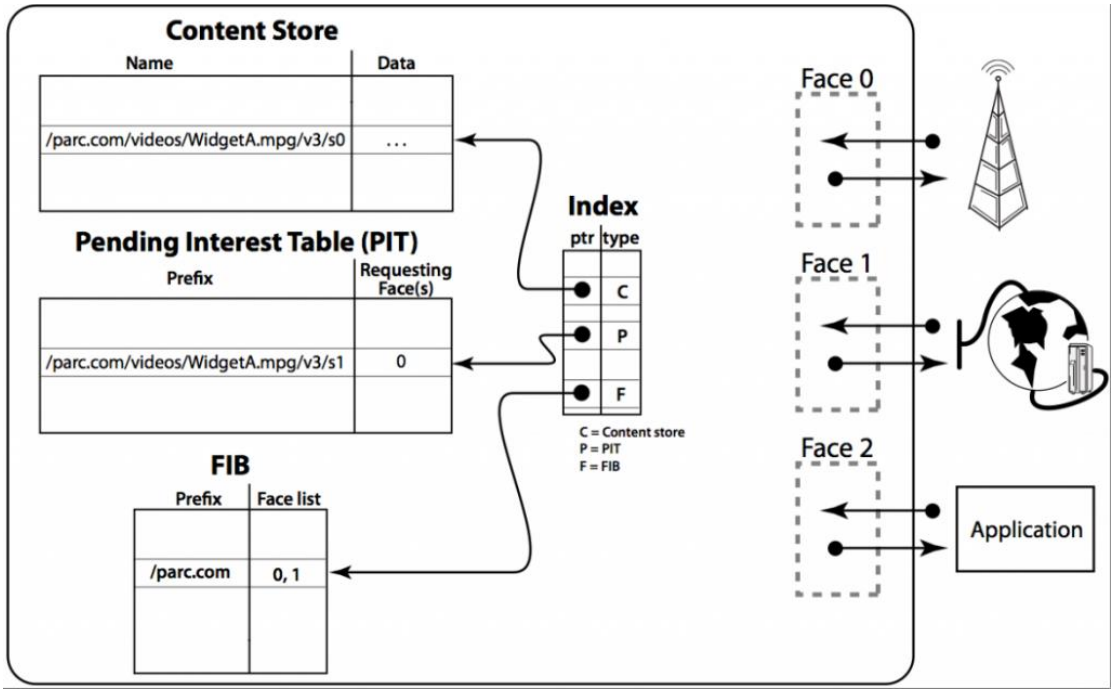


圖 2- 4、NDN 轉發工程模型

資料來源：named-data.net

PIT 主要用途為記錄且追蹤尚未被滿足的興趣封包及其來源。當興趣封包轉發時，會在 PIT 留下紀錄，而當資料封包回傳時，將會依據 PIT 的紀錄內容，將資料封包回傳至興趣封包的來源，同時將 PIT 中相對應的資料刪除。

FIB 提供查詢且轉發封包至潛在資料來源位置的功能。與現今網路 IP 路由器的 FIB 相同，用於查詢潛在的資料來源，但因 NDN 本身架構可以避免迴圈問題，所以允許同時發送多個請求。

CS 用於暫時存放資料，方便其他使用者可以就近地獲取資料。暫時存放曾經轉送過的資料封包，根據路由器中本身的機制來決定資料是否丟棄或保留，盡可能留下重覆可使用的資料，當不同的使用者需要相同的資料時，即可增加資料的可獲性，而不必再到終端拿取資料，使用者同時可以透過簽署資訊或是特徵來確保資料正確性。

(二) NDN 最新進展

除了前述 NDN 基本協定規範外，構建一個可操作的 NDN 網路尚需要額外的軟體架構來支援命名、高性能轉發和路由、轉發策略和信任管理。由參與 NDN 專案的諸多學術組織所設計和開發的 NDN 平台、模擬工具、軟體模組、應用架構，亦極大地便利了此領域的研究者，同時加快了技術發展的步伐。

- NDN Testbed：隨著 NDN 專案誕生的跨國性測試平台，其包含了來自多個國家參與機構的軟體路由器、應用程式主機節點和相關設備的共享資源[27]。另亦提供可運行在開放網路實驗室（Open Network Laboratory, ONL）的模擬版本，可用於快速測試、調適及評估應用程序，而沒有任何干擾 NDN Testbed 的風險。
- ndnSIM：最早版本完成於 2012 年 6 月，目前版本已更新至 2.0，是以 NS-3 為基底且最被廣泛使用中的 NDN 模擬器[28]。其主要為 NDN 模型的網路層協定實作，可以運行在任何的連接層、網路層或傳輸層協定之上。
- NDN Forwarding Daemon (NFD)：NFD 是一個實現 NDN 轉發機制及其功能的軟體模組。在最初版本編寫完成後，NFD 與 NDN 協定一起成為 NDN 平台的核心元件，並且遵循著相同的更新發布週期[29]。NFD 在設計上強調模組化和可擴展性，以支持新協定功能、演算法和應用程序等 NDN 技術進行試驗。NFD 專案團隊還編寫了一份開發人員指南，詳細介紹了當前實作及提供擴展 NFD 各個方面的技巧[30]。

---

[27] NDN Project, NDN Testbed, available at https://named-data.net/ndn-testbed/ (Last visited:Dec. 5, 2021)
[2828] ndnSIM Documentation, Introduction, available at https://ndnsim.net/current/intro.html (Last visited:Dec. 5, 2021)
[29] NDN Project, NFD Overview, available at https://named-data.net/doc/NFD/0.7.0/overview.html (Last visited:Dec. 5, 2021)
[30] NDN Project, NFD Developer's Guide (Latest Revision 11), available at https://named-data.net/publications/techreports/ndn-0021-11-nfd-guide/ (Last visited:Dec. 5, 2021)

- NDNoT：該專案旨在利用 NDN 命名規範（naming conventions），提供相關元件及整體架構，為物聯網應用程序開發人員的自動配置、服務發現、以資料為中心的安全、內容交付和其他需求提供解決方案。與現有基於 IP 的其他物聯網架構最大的區別，NDNoT 去除了各種可讀名稱標識（例如，URI、服務名稱）和網路標識（例如 IPv6 地址）之間映射機制（例如，DNS、multicast DNS）[31]。在專為資源受限物聯網設備所開發的 RIOT-OS 中，亦已有 NDN 協定堆疊、封包轉發邏輯及具資料安全性的高級應用程式介面的設計與實作。研究結果證明了 NDN 協定在僅有 10KB RAM 和 Flash 的受限設備上運行應用程序的可行性[32]。
- VANET via NDN (V-NDN)：該計畫旨在解決車載隨意網路（Vehicular ad-hoc network, VANET）對於移動性的要求，研究者利用了 NDN 模型，將資料命名與主機地址分離。因此，只要存在任何形式的網路接取，汽車就可以利用任何可用的介面從任何其他節點獲取資料。該項研究已在加州大學洛杉磯分校車輛測試平台上實施並測試了具有約 10 輛汽車的 V-NDN 原型，除了初步效能評估，也界定出相關之研究挑戰[33]。

(三) NDN 技術趨勢分析

ICN 架構發展主要目標是因應 Internet 上進行內容分發的高效性和可擴展性的需求。該架構基於對於資料物件（data object）的命名表示。許多研究工作紛紛表明，新一代 Internet 需要擺脫當前

[31] Zhiyi Zhang et al.,. NDNoT: A Framework for Named Data Network of Things, ACM Information Centric Networking Conference 2018, available at https://conferences.sigcomm.org/acm-icn/2018/proceedings/icn18posterdemo-final22.pdf (Last visited:Dec. 5, 2021)
[32] NDN Project, NDN Technical Report NDN-0043: The Design and Implementation of the NDN Protocol Stack for RIOT-OS, available at https://named-data.net/publications/techreports/ndn-0043-2-ndn-riot/ (Last visited:Dec. 5, 2021)
[33] Giulio Grassi et al., VANET via Named Data Networking, available at https://named-data.net/publications/vanet_via_ndn_infocom_nom/ (Last visited:Dec. 5, 2021)

以主機為中心的連接模式，改採不同的方法和架構設計，例如以資訊（或內容）為中心的新模式。尚處於研究階段的 NDN，在轉發策略、轉發引擎、路由協定的設計方面仍有諸多挑戰。隨著物聯網的發展，許多應用 NDN 解決現實世界問題的努力已經展開。如同 IP 問世的過程，通過大規模使用確定並解決重要問題，學界與業界愈發期望 NDN 架構能通過新應用程序和部署工作中學到的經驗逐漸成熟。

NDN 可以運行在任何可以轉發資料封包（乙太網、WiFi、藍牙、蜂窩網路、IP、TCP 等）的協定之上，任何協定也可以運行在 NDN 上，包括 IP。不需試圖替換或者改變已經部署的 IP 基礎設施，NDN 可以簡單地運行在 IP 基礎設施之上。因此，NDN 在內容分發上的優勢、應用程式友好的通訊和命名、具強健性（robustness）的安全設計、移動性的支持和廣播都可望實現。

二、DOA 及 X.1255

ITU-T SG2 主要負責號碼標準的制定。ITU-T SG17 負責網路安全架構、數位身份安全管理、物聯網應用等安全標準制定，旨在提高網路安全性。ITU-T SG20 負責物聯網和智慧城市標準制定，包括架構、安全、互通性等，旨在提高城市智慧化水準。

2013 年 9 月，ITU 發布 ITU-T X.1255 建議書：發現身份管理的資訊框架。該建議書支援提供開放架構框架，包括數位實體模型、資料介面協定、標識註冊和解析系統以及中繼資料註冊表等。

2017 年 9 月，ITU 發布 ITU-T Y.4805：智慧城市應用中互通性對標識服務的需求。該標準規定了智慧城市應用中標識服務的系列需求，以確保應用是可交互操作和安全的。標準中的需求也可以作為智慧城市領域開發新標識服務的指導原則，包括服務完整性、資料保密性等特徵。

2020 年 1 月，ITU 發布 ITU-T X.4459 建議書：物聯網交互操作的數位實體架構。該建議書規定了面向資訊的服務體系框架，包括數位

物件標識註冊、發現、解析和傳播機制，旨在促進跨域資料的共用。

三、Non-IP

2020 年 4 月，歐盟 ETSI 成立一個新的產業規範小組 “Non-IP Networking”（ISG NIN），取代 2015 年成立之 “Next Generation Protocol”（ISG NGP），並延續為行動網路研究開發新的通訊協定之目標[34]。

2021 年 4 月，ISG NIN 發布了第一批研究報告，其內容分別為：

- GR NIN 001《在 2020 年代使用 TCP/IP 組網的問題》；主要在陳述 TCP/IP 協定對當今行動網路的限制，以及替代方案應如何克服這些缺點。涵蓋主題包括無線電頻譜的有效使用、命名和尋址（包括尋址生命週期）、QoS 與時間敏感流量（time-sensitive traffic）、安全性、網路管理、高效轉發和遷移。
- GR NIN 002《利用 3GPP 行動網路之無線電接取實作 Non-IP 及測試方法》；說明在 3GPP PHY 層直接啟用 Non-IP 協定堆疊的細節。該報告還建議了適用於低功耗物聯網設備、視頻與音頻服務，以及遠程手術中的觸覺反饋等可以進行概念驗證測試的應用場景。

GR NIN 003《Flexilink 網路模型》；詳述將 ETSI GS NGP 013 所提 Flexilink 技術構成之網路模型作為基礎，可廣泛支持新的和現有的協定，並以使用於遞迴網路架構（Recursive InterNetwork Architecture, RINA）、TCP/IP 和數位音訊、視頻等作為釋例，進一步解釋資料封包格式和控制平面協定的要求。

ICANN 特別針對 NIN 提出了一份技術分析文件[35]，當中述及，ISG NIN 認為 TCP/IP 並不適用於 5G 所承諾的新形態應用，如觸覺應用與工業用機器人。NIN 沒有拓展 IP 標頭（IP header）以包含更多的資訊，如被路由器與交換機所執行的 QoS 合約，而是提出一種虛擬電路的方法，

[34] ETSI, ETSI launches new group on Non-IP Networking addressing 5G new services, available at https://www.etsi.org/newsroom/press-releases/1749-2020-04 (Last visited:Dec. 5, 2021)
[35] ICANN OCTO, Non-IP Networking (NIN), available at https://www.icann.org/en/system/files/files/octo-026-12jul21-en.pdf (Last visited:Dec. 5, 2021)

其中數據封包在 SDN 模型中被分類為流向，是被交換機轉發根據與流向相關聯的虛擬電路標幟符。NIN 所推廣的技術被稱為 Flexlink 且在先前的 ISG NGP 所記錄。Flexilink 讓人想起非同步傳輸模式（Asynchronous Transfer Mode, ATM），這是一種在 1990 年代短暫流行的網路傳輸技術，但在 2005 年後即被多協定標籤交換（Multiprotocol Label Switching，MPLS）所取代而在電信網路中逐漸消失。

目前尚不知 NIN 是否可以完全取代 IP 或者僅用於特定本地應用的東西，例如：網際網路範圍之外的家庭網路或者工業網路。在此階段，NIN很大程度上仍然是一項研究活動而非工程活動。目前有些實驗性程式碼可能存在，但ISG尚未提出完整且可互相操作的提案。特別是NIN模型嚴重依賴於目前尚未定義的外部協定來發出創建、修改或者刪除的虛擬電路信號。任何 NIN 可帶來的簡化與用於虛擬電路創建、修改或刪除的未指定信令協定可能增加額外的複雜性與花費相平衡是毫無價值的。

隨著前述三份報告發布，ISG NIN 的工作仍然在進行中。儘管如此，還是可以看到 NIN 的總體方向：它提議回歸虛擬電路，將鏈路容量劃分為時隙並以一次傳送 64 個字元。

然而，Flexilink 只定義了資料平面。如果不查看未指定的控制平面，或者如果要使用多個控制平面，就無法理解該提案的全部影響。根據流量的性質，一方面在於效率、安全性、彈性等方面的益處很容易被另一方面的損失抵銷。此外，網路的彈性仍是一個尚未解決的問題。由於尚未指定控制平面，因此無法得知中間節點在發生故障時後發生什麼事。同樣不清楚的是控制平面對於網路操作的複雜性的影響。NIN 的主要驅動因素之一看起來是集中 Robust Header Compression（ROHC）功能的成本上，該功能可以將 IP 標頭的荷載減少到幾乎為零。為了解決這個明顯的業務問題，NIN提議對整個網際網路架構進行改革。然而NIN並沒有提供對於提議替代解決方案的佈署總成本的全面分析，這些費用不僅網路服務業者承擔，還必須由大量的網際網路生態系統的第

三方承擔。

ISG NIN 的目標是 RAN 中的 Flexilink。將 RAN 視為不支持 TCP/IP 的特殊網路並不是什麼新鮮事。NTT DOCOMO i-mode 與 WAP 在早期曾經試過。然而手機容量(智慧型手機)的增加與無線頻寬的增加使得 TCP/IP 成為這些無線設備的規範。目前尚不清楚 TCP/IP 對於即將到來的無線應用任何感知限制是否需要對網路架構進行重大改革，或僅只是等待下一代手機就足夠。話說如此，由於 Flexilink 可以被視為像 MPLS 或網路服務業者的乙太網路一樣的第 2.5 層協定，如果佈署模型僅限於 RAN，對全球網際網路架構可能是最小的。

與 New IP 類似，NIN 正在重新檢視一些基本的網路原則。這毫無疑問的是一個健康的活動。然而，在此兩種情況下，所提出的解決方案都圍繞著過去架構的回歸，這似乎是上世紀資料封包與虛擬電路爭辯的重新訴訟。

ICANN 對 NIN 技術分析文件最後總結，確保任何新提議的網路模型的架構與網際網路架構兼容是端點到端點連接和保持一個世界、一個網際網路的願景的關鍵因素。

第五節　國際電信號碼標準與管理發展

公眾交換電話網路（Public Switched Telephone Network, PSTN）的發展時間較網際網路早，在整體網路設計及布建上，主要使用 E.164 電話號碼來識別呼叫的目的地，並在兩個固定點之間通過網路路由呼叫。隨著行動網路的不斷發展，為了更確保用戶終端設備（手機）安全性，基於 E.212 標準的國際行動用戶識別碼（International Mobile Subscriber Identity, IMSI）被用來確定手機與基站間可以建立連接，並提供用戶全球性的唯一識別碼。

為使各種電信網路得以在網網互連之下，使用相同的電信編碼規則，TSB 根據 ITU 所制訂之 E.164、E.212 等電信號碼技術標準，將國碼（Country Code, CC）、行動國碼（Mobile Country Code, MCC）指配

給國家或地區；另也有指配給特定組織或系統的情形，例如在 E.164 CC 部分：

- 指配 888 給聯合國人道事務協調辦公室[36]，以便為搜索救援工作所使用的終端裝置提供國際命名和定址系統；
- 指配 870 給國際海事衛星組織[37]，提供全球性的海事、航空及陸地衛星行動通訊服務。

一、新型態的 E.164 號碼指配管理方式

在歐洲 ECC 的 311 號報告《次級指配與號碼託管：E.164 號碼在電子通訊供應鏈中的實施模式、使用權及義務》[38]中，提出 5 種號碼管理模型，如圖 2-5 示意。

該模型有別於 E.164 號碼指派等電子通訊供應鏈的基本模型，而是聚焦在使用次級指配與號碼託管的新型態模型進行規劃，因應未來法規監理可能會涉及的透明度（transparency）議題，並提供增加透明度之方法與建議，讓號碼計畫管理者（Numbering Plan Administrator, NPA）瞭解各事業體於電子通訊供應鏈中之權利及義務，以利國家進行有效率之號碼管理，如降低市場進入門檻、增加市場競爭。

[36] UN Office for the Coordination of Humanitarian Affairs (OCHA)，設有國際搜索救援諮詢組織 (International Search and Rescue Advisory Group, INSARAG)、聯合國災難評估協調隊 (United Nations Disaster Assessment and Coordination team, UNDAC) 兩大協調部門。

[37] International Maritime Satellite Organization plc (Inmarsat)，現已改制為總部設置於英國倫敦的衛星通信公司。

[38] CEPT Electronic Communication Committee, 2020. ECC Report 311 - Sub-assignment and number hosting - Implementation models, rights of use and obligations for E.164 numbers across the electronic communications supply chain, available at https://docdb.cept.org/document/14735 (Last visited:Jul. 15, 2021)

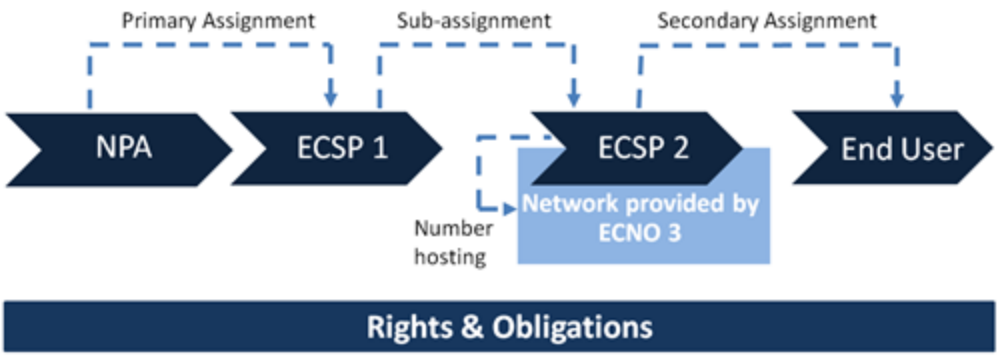


圖 2- 5 、歐盟 ECC 建議的 E.164 號碼指配管理模式
資料來源：CEPT ECC

二、物聯網發展對 E.164、E.212 電信號碼之影響

近年由於物聯網、衛星通訊等跨國性電信服務的興盛，ITU-T 亦規範了特定字首的 CC、MCC 作為共享用途，直接由 TSB 負責管理核配，包括按照 E.164.1 建議書在 881、882 和 883 等 CC 代碼分配的全球業務和網路代碼列表 ，或是預留或已分配的 ITU-T E.212 共用 MCC 和相關 MNC 等。

2020 年 6 月，ITU-T 根據 E.164.1 與 E.212 Annex A 兩份編碼規則建議，增訂關於 M2M/IoT 之補充準則（Supplement 11），並視需求開放物聯裝置使用 E.118 之 IIN 號碼指配。該準則列舉在特定情況下之特定裝置能同時提供 IoT 與語音服務、且在變更 M2M/IoT 裝置時亦採取較寬鬆的證明機制。

歐洲電子通訊委員會（Electronic Communications Committee, ECC）在 2010 年第 153 號報告－《使用於機器間通訊的號碼與定址》[39]及 2011 年第 3 號建議書中[40]，提出 4 種 E.164 號碼資源運用於物聯網服務之基本選項，該選項係根據行動設施與底層網路做為區分方式，做為業者

[39] CEPT Electronic Communication Committee, 2010. ECC Report 153 - Numbering and Addressing in Machine-to-Machine (M2M) Communications, available at https://docdb.cept.org/document/261 (Last visited:Jul. 15, 2021)
[40] CEPT Electronic Communication Committee, 2011. ECC Recommendation (11)03 - Numbering and Addressing for Machine To Machine (M2M) Communications, available at https://docdb.cept.org/document/499 (Last visited:Jul. 15, 2021)

依不同服務類型之 M2M 號碼選擇依據。

另在 E.212 號碼編配供物聯網或行動專網之使用方面，考量到 MNC 業者編碼多為 2 至 3 位數，為避免因 MNC 數量不足造成之問題，在監理上可採取限於內部使用、申請國際代碼，或類似於美國、德國之細分化作法，簡列如下：

- 僅限專網內部使用: MCC=999（無須通報 ITU-T)[41]；
- 國際共用:MCC=90x（直接向 ITU-T 申請核發)[42]；
- 實例：MulteFire Alliance: 902(MCC)01(MNC)[43]
- 美國 CBRS 頻段專網: Shared 315(MCC)010(MNC) + 4 位數(IBN) + 5 位數(UIN)[44]；如圖 2- 6 所示。
- 德國行動專網: Shared 262(MCC)98(MNC) + 4 至 6 位數 block ID + 剩餘位數[45]

[41] ITU-T, Recommendation E.212 (2016) Amendment 1 (07/18), available at https://www.itu.int/rec/T-REC-E.212-201807-I!Amd1/en (Last visited:Dec. 5, 2021)
[42] ITU-T, Recommendation E.212 (2016) Amendment 3 (12/20), available at https://www.itu.int/rec/T-REC-E.212-202012-I!Amd3/en (Last visited:Dec. 5, 2021)
[43] MFA, MulteFire Alliance (MFA) simplifies path to 5G private network deployment for Enterprise, available at https://www.mfa-tech.org/2021/06/22/mfa-simplifies-path-to-5g-private-network-deployment-for-enterprise/ (Last visited:Dec. 5, 2021)
[44] ATIS, IMSI Assignment and Management Guidelines for Shared HNI for CBRS Range, available at https://www.atis.org/wp-content/uploads/2020/10/IMSI-CBRS-Guidelines_v2.pdf (Last visited:Dec. 5, 2021)
[45] BNetzA, Mitteilung Nr. 101/2020, available at https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/TechnischeNummern/IMSI/Mitteilung101.pdf (Last visited:Dec. 5, 2021)

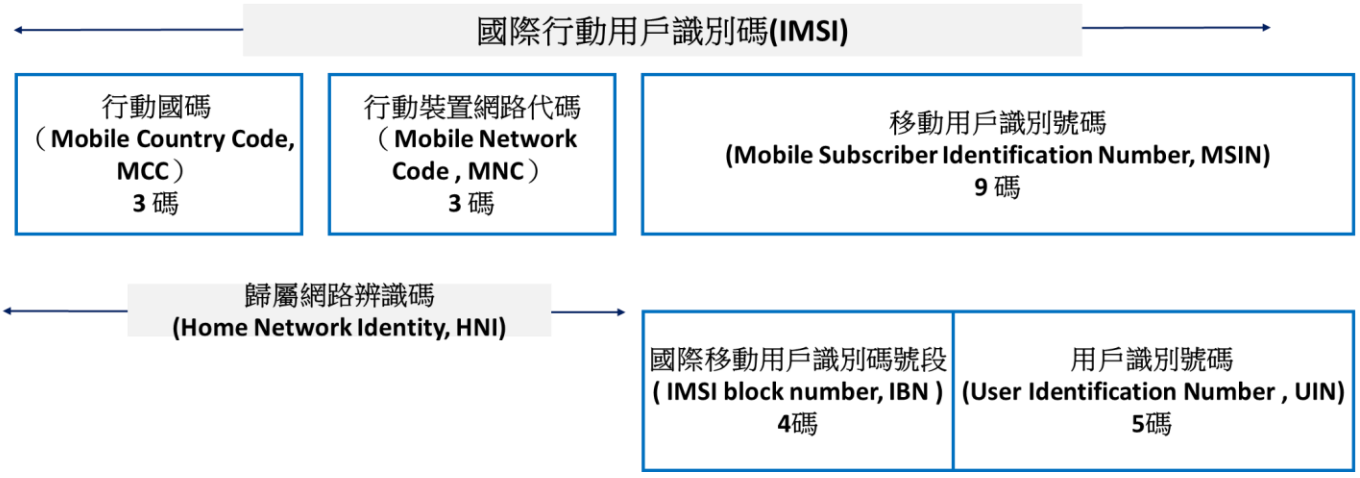


圖 2- 6 、使用於美國 CBRS 頻段專網之 IMSI 號碼格式

資料來源：FCC

三、物聯網之號碼分配管理

(一) 物聯網編碼需求

為了實現人與人、人與物、物與物的通訊以及各類應用互連互通，產業各界已發展出多種識別碼來對人和物等物理實體、網路和設備等通訊實體以及各類業務和服務等應用實體進行標識，並通過識別碼解析與定址系統進行翻譯、映射與轉換，以獲取相應的位址或關聯資訊。該等系統通常包括命名（Naming）和定址（Addressing）兩部分。通過不同名稱間的轉換，可提供更直接或更豐富的名稱映射關係及其附加屬性資訊。

(二) 物聯網命名機制

物聯網是對現有網路的拓展和延伸，從而將實體物件連接入網路中，再通過網路獲取資訊和管理資源。物聯網資源是指任何可以被定址或者引用的物聯網主體物件，而名稱就是用來唯一辨識資源的抽象識別字。命名機制所要研究的則是如何設計合理的編碼規則來辨識資源。由於物聯網設備種類繁多、數量龐大易造成管理不易，故在考量不同系統間獲取及傳遞多元資料的溝通成本上，將產生為眾多實體物件的命名架構及其可辨識性建立規則之需求。

物聯網體系架構通常分為感知層、網路層、應用層等三個層次，此處以相應的識別目標和應用場景將名稱劃分為三類：物件識別碼用於識別各種實體資源，通訊識別碼用於識別具備通訊能力的網路節點，應用識別碼則是用於識別物聯網各項應用服務組成元素[46]。

1. 物件識別碼

物件識別碼用於識別物聯網中被感知的物理、邏輯或資訊物件，例如茶杯、動物、人、設備產品、文章、溫度等。物件識別碼的應用場景通常為基於其進行相關物件資訊的檢索與獲取，或者是對識別碼物件進行相關控制與管理，而不用於網路通訊或定址。賦予性識別碼是指為了識別方便而人為分配的識別碼，通常由一系列數位、字元、符號或任何其他形式的資料按照一定編碼規則組成，是物聯網中的主要識別碼形式。網路可通過多種方式獲取賦予性識別碼，包括：

- 被動式：通過標籤閱讀器讀取存放於標籤中的物體識別碼，例如條碼相關識別碼（如 EAN 碼、UPC 碼、128 碼）、RFID 相關識別碼（如 EPC 碼、ucode 碼等）；
- 通過人機介面從物聯網終端獲取：物件識別碼（OID）、統一資源名稱（URN）、Handle 等。

2. 通訊識別碼

通訊識別碼用於識別物聯網路中具備通訊能力的網路節點，例如使用者手機、RFID 讀寫器、感測器節點、網路設備等。這類識別碼的形式可以為 E.164 號碼、IP 位址等。通訊識別碼在用於識別物件的同時，還可明確物件的通訊屬性，可作為相對或絕對位址用於通訊或定址，以建立到識別碼物件的通訊連接。

3. 應用識別碼

應用識別碼用於對物聯網應用層中的業務或應用服務進行識別，

[46] 劉陽等人，《物聯網名字服務關鍵技術研究》，2014 年 10 月，http://idconsensus.cn/u/cms/www/202001/16093226cjt9.pdf

例如業務接入號碼、資訊服務接入功能變數名稱或位址等，在識別碼形式上可以為功能變數名稱、URL 等。

工業物聯網在通訊識別碼方面的需求與傳統網路的差異有二：一是通訊終端設備的大規模增加以及生產資源的數據連網，帶來對 IP 位址等號碼資源的壓力，IPv6 位址在解決工業網路定址需求上，不但為網內各設備提供全球唯一位址，為更好地進行數據交換和資訊整合提供了條件；二是以無線感測器網路為代表的智慧物件組成的近距離無線通訊網路，對通訊識別碼提出了降低電力、頻寬、處理能力消耗的新要求，為此，部分網路廠商成立了 IP for Smart Objects（IPSO)，IETF 也分別提出 6LowPAN、ROLL RPL、CoAP 等與 IPv6 相關通訊協定的標準化研究。

(三) 物聯網標識解析機制

所謂的標識解析機制，是一種在不同名稱間進行映射資訊轉換的查詢過程。該機制可以分為集中式和分散式兩類。前者將所有資源紀錄存放在唯一的名稱伺服器上，而無需考慮多個名稱伺服器之間的資料同步問題，網路結構簡單，但是不適應物聯網作為大規模分散式網路的性能和安全需求；後者則將資源紀錄分散存放在多個名稱伺服器上，它們之間可能是主從關係，也可能是對等關係。

對於分散式定址網路，根據索引分佈方式的不同，又存在層次式和扁平式兩類設計風格。層次式主要基於分級的樹狀形式組織名稱伺服器的體系架構，以 DNS 最為突出；扁平式主要基於對等的環狀結構組織名稱伺服器的體系架構，以分散式散列表（Dis-tributed Hash Table, DHT）的形式最為常見。除此之外，近年來也有許多研究者提出兼有層次式和扁平式兩種設計思想的混合式服務。

(四) 物聯網時代的挑戰與展望

從 Internet 拓展和延伸出來的物聯網，由於把巨量的物理實體接入網路，所以不僅攜帶了原來 Internet 所存在的一些缺陷，還面

臨諸多新的問題，並對名稱系統帶來了新的挑戰。

1. 異質相容

物聯網的終極目標是實現各種資源統一定址和互連互通，不會被侷限於為某一種應用只在一定的國家或者組織內部使用單一的組網技術、命名手段和解析服務來構建封閉式環境。因此，異質多編碼的相容性解析成為物聯網名稱系統的重要研究方向。

長遠來看，什麼樣的標準識別碼能夠為各國家、各標準組織所接受，由誰來負責維護此類識別碼的分配和管理，都值得進一步商榷。現有的各種命名機制中並沒有預先分配標準識別碼，即使未來的技術能夠全面支持這些改進，如何相容現有編碼方案會非常困難。

2. 對等解析

出於主權安全以及商業競爭的目的，世界各國、各組織都希望能夠管控與其所擁有物聯網資源相關的名稱系統。集中式控制體系勢必造成根節點單極化的問題，影響名稱系統作為一個公共服務的可用性和可靠性。對等解析就是試圖在根層級上，將單根伺服器分解為多個對等的伺服器，保證每一個對等根的權級相同。從而實現不同名稱系統系統間的互連互通，從根本上保障安全性。

公平、對等的解析環境對自治性很強的物聯網而言至關重要，在保證名稱系統可以處理跨越多個自治子網的資源定位和資訊檢索並助力於物聯網實現真正互連互通的同時，又能保證資源擁有者對資源的自主控制權，自行維護和管理本地的名稱系統設施。雖然已有部分提出的方案可以解決此一問題，但仍然需要進一步考慮採取何種措施來保證根節點映射表內資訊的真實性和可靠性。

3. 隱私保護

以 Internet 為依託的物聯網，不可避免的也會遇到 Internet 中原有的各種安全隱患，最突出的就是隱私保護問題。一方面是名稱資源紀錄發布者的權益，另一方面則是名稱資源紀錄查詢請求者

的權益。

名稱系統作為一種向整個物聯網開放的公共協力廠商查詢服務，在提供資訊共用的同時，個人隱私的保護也是一個巨大的挑戰。任何單一角色都無法完全解決這一問題，需要名稱系統架構中的名稱伺服器、資訊伺服器、解析器、註冊器等各種組成元素都參與進來，才能構建一個完整的安全體系，充分保障使用者在資訊發布、資訊查詢等各個環節的隱私安全。同時，各種隱私保護機制還需要與服務品質、資訊損失、查詢多樣性和執行時間進行權衡。因此，如何定義可動態靈活變化的安全性原則，以及研究時間複雜度更低的隱私保護演算法等都具有重要意義。

1983 年發明 DNS 經過將近四十年的發展，至今仍是 Internet 中最為核心的名稱系統。但 DNS 並不是一種放諸四海皆準的通用解決方案，特別是在物聯網中，從性能角度看，要求名稱系統在資料量大、查詢量大的情況下仍需保持較快的回應速度；從功能角度看，產生了相容異質識別碼、公平對等解析、安全需求增強等新的挑戰。

在未來，物聯網名稱系統的發展方向可能是：首先，混合式名稱系統架構的探索。鑒於 DNS 的層次式設計和基於 DHT 的扁平式設計各有優缺點，都無法滿足物聯網對名稱系統的需求。綜合使用這兩種技術的混合式解決方案值得進一步探索，並可通過真實環境的實際部署探索其有效性。其次，固定名稱系統向靈活搜索服務的演變。傳統名稱系統（如 DNS）都是採用固定的訊息格式和單一的名稱資源紀錄，無法滿足物聯網在靈活性方面的需求。其對應之基於時間屬性或空間屬性等間接識別碼、支援區間識別碼的查詢、多關鍵字查詢、部分關鍵字查詢等其它形式的名稱系統等問題，在物聯網環境下都值得進一步研究和探索。

第六節　主要國家或地區電信號碼管理政策與物聯網編碼之調和

一、歐盟電信網路號碼政策

(一)　號碼資源分配指南草案

在 2019 年 6 月 12 日至 6 月 14 日的第 39 次會議上，歐盟監管委員會（the Board of Regulators）批准了歐盟電子通傳監管機構（The Body of European Regulators for Electronic Communications, BEREC）關於評估電子通訊網路（electronic communications network, ECN）或電子通訊服務提供商（electronic communications service, ECS）以外的企業管理號碼資源能力的通用標準之指南草案。該指南草案旨在評估電子通訊網路或服務提供商以外的企業，管理號碼資源的能力的通用標準，以及探討如果將號碼分配給此類企業，則可能會耗盡號碼資源。

因此，上述的指南草案的目的旨在討論是否允許將號碼分配給除電子通訊網路或服務提供商之外的企業，以促進歐盟市場監管的清晰化以及達成歐盟監管的一致性。

有鑑於此，該指南草案認為歐盟號碼資源的分配應考慮涵蓋所有類型的服務和號碼，包括機器對機器（Machine to machine, M2M）通訊，並且為此類型服務提供特殊的號碼資源；應考慮若將號碼資源分配給具有域外使用權（extra-territorial use rights）的 ECN/ECS 提供商以外的企業時可能產生的影響。

BEREC 為了評估該指南草案的適當性以及尋求業界對於該指南草案之意見與建議，於 2019 年 6 月 14 日至 8 月 28 日進行了公眾諮詢，邀請了一共 9 個歐洲國家相關利害關係人參與公眾諮詢，並於 2020 年 3 月 6 日發布了有關評估電子通訊網路或服務提供商以外的企業管理號碼資源能力的通用標準之指南草案的公眾諮詢結果報告。本計畫將就此公眾諮詢報告討論的內容說明之。

在此份公眾諮詢報告中，提供諮詢意見與建議的一共 9 個歐洲

國家相關利害關係人，包括歐洲競爭性電信協會（European Competitive Telecommunications Association, ECTA）、歐洲電信網路營運商協會（European Telecommunications Network Operators, ETNO）、GSM （Groupe Spéciale Mobile） Association （GSMA）、與德國電氣與電子工業協會（Zentralverband Elektrotechnik- und Elektronikindustrie, ZVEI），及奧地利（A1 Telekom Austria）、波蘭（Krajowa Izba Komunikacji Ethernetowej, KIKE）、義大利（FastWeb）、西班牙（Asociación de Empresas Operadoras y de Servicios de Telecomunicaciones, ASTEL）電信業者或英屬電信集團（COLT）。

在這份公眾諮詢報告中，整體而言上述的利害關係人反對將公共號碼資源分配給非 ECN 和 ECS 提供商，而反對的原因主要為有些利害關係人認為此分配並無產生好處或是基於客觀上的需求，因為非 ECN/ECS 者必須仰賴 ECN 或 ECS 提供商的基礎設施，並且號碼資源的使用必須屬於網路和/或服務的提供業者。再者，亦認為將號碼分配給非 ECN/ECS 提供商，則 ECN/ECS 提供商將產生需要事先評估的額外費用等。

針對上述有關相關利害關係人對公眾諮詢提出之論點以及 BEREC 對其做出的回應，以下將由本計畫就不同面向說明之。相關利害關係人之論點，主要可分：

1. 號碼資源的分配
    - 將號碼資源分配給非 ECN/ECS 提供商具有歧視性，恐有不公平之嫌疑，因為非 ECN/ECS 提供商不必遵守任何公共監管之義務，例如法律攔截（legal intercept）、緊急服務（emergency services）與攜碼（number portability）等。然而 ECN/ECS 提供商必須遵守任何公共監管之義務，以確保其遵守在法律框架中規定的所有公共監管義務及其相對應需支付的費用。

- 若是歐盟會員國決定於該國法律中增加將公共號碼資源分配給非 ECN/ECS 提供商，則呼籲應對 ECN/ECS 提供商以及非 ECN/ECS 提供商之間在號碼資源的使用上，建立公平的競爭環境，並對跨境服務的發展採取一致的做法。
- 將公共號碼資源分配給非 ECN/ECS 提供商應該只考慮提供非 ECN/ECS 提供商提供的服務，並提到國家監管機構 National Regulatory, NRA）或其他主管當局（Competent Authorities, CA） 亦應事先確認哪些服務可能需要這些公共號碼資源。
- 強烈建議不要將 MNC 分配給非 ECN/ECS 提供商，因為存在稀缺風險，並表示在遠程提供嵌入式 SIM 卡（the remote provisioning of eSIMs）會更有效，並且可能成本更低。
- 認為 既然空中下載技術（over the air, OTA）解決方案很容易獲得，因此應該使用這些解決方案，而非將 E.212 資源分配給非 ECN/ECS 提供商。
- 強調不應將號碼資源分配給非 ECN/ECS 提供商，因為 E.212 號碼資源用盡的風險較高，並且此類分配亦將導致號碼資源的低效使用。

2. 號碼資源的發展
   - 呼籲 BEREC 要求防止 ECN/ECS 提供商與非 ECN/ECS 提供商之間可能出現的任何競爭扭曲現象，以及影響 OTA 和 eSIM 發展，並為 ECN/ECS 提供商給予保留和開發的機會，因為塑造基於號碼的解決方案的未來供應亦相當重要。
   - 呼籲 BEREC 定義一種機制，以避免號碼資源耗盡的風險。

- 敦促 BEREC 向 NRA/CA 提供指示，以便為 eSIM 重新配置 OTA 解決方案的特權，避免其他耗盡 MNC 的解決方案，因為它們是稀缺資源，應予以保留。

3. 指南草案的號碼範圍
   - 某些利害關係人認為並無發布非 ECN/ECS 提供商使用公眾號碼資源指南的必要性。在 BEREC 指南的範圍上，應僅側重於如何將號碼資源分配給非 ECN/ECS 提供商的標準訂定和評估可能用盡號碼資源風險的標準，不應涉及建議可能分配給非 ECN/ECS 提供商的號碼範圍。
   - 關於非 ECN/ECS 提供商可能使用的號碼範圍，認為對於提供 M2M/IoT 服務，E.164 號碼之攜碼的理由尚需釐清，並建議 M2M/IoT 用戶只需在任何網路業者轉換後的服務啟用階段時配置新的 E.164 號碼，以減輕負擔，並藉此延長國家 E.164 號碼提供上述服務。
   - 並非所有利害關係人皆屬於當前 BEREC 指南的範圍，因此要求 BEREC 提供關於號碼資源一般使用的指南，以確保整個歐盟於在滿足 ECN/ECS 提供商的條件方面有一個真正的公平競爭環境。
   - 部分利害關係人認為指南不應該說明應將哪些號碼範圍分配給非 ECN/ECS 提供商，因為這應取決於每個會員國的決定。

BEREC 之回應如下：

1. 號碼資源的分配：鑑於號碼資源與各種 M2M/IoT 服務的相關性日益增加，BEREC 明確提出了歐盟會員國向非 ECN/ECS 提供商授予號碼資源使用權的可能性。因此，若有足夠的號碼資源來滿足當前和未來可預見的需求，此種分配的可能性也將可支持基於號碼資源服務發展，而這些資源在非人際通訊服務的情況下具有域外使用權。另外，

由於 EECC 的第 246 條和第 93（4） 條顯示過去的監管框架並未明確禁止或允許將號碼資源可分配給非 ECN/ECS 提供商。因此在此方面，一些歐盟會員國認為可將號碼資源分配給此類提供商以提供特定服務。

NRA/CA 可以根據 EECC 第 93（2）條，在非歧視的基礎上授予國家號碼計畫中號碼資源的使用權，以便向非 ECN/ECS 提供商提供特定服務。但在這方面，一個強制性的先決條件是非 ECN/ECS 提供商應證明對此類號碼資源的需求以及他們管理號碼資源的能力；這些供應商必須遵守 NRA/CA 制定的任何相關要求。

如果歐盟會員國決定將號碼資源分配給非 ECN/ECS 提供商，則將會有兩個主要選擇：

- 將 E.164 號碼資源分配給非 ECN/ECS 提供商，並推廣和使用 OTA。
- 將所需的號碼資源分配給非 ECN/ECS 供應商，無需指定類型並逐步根據該類型分析其需要分配的資源。

應由每個會員國選擇應將何種類型的號碼資源分配給非 ECN/ECS 提供商（該問題被認為超出了指南的範圍）。M2M 服務可分配給非 ECN/ECS 供應商，並可用於國內或域外使用，以確保支持 EECC 第 3 條第 2 款規定，以促進內部市場發展的總體目標。

BEREC 認為會員國或 NRA/CA 應根據需求，決定應將哪種類型的號碼資源分配給非 ECN/ECS 提供商，因此建議將某些特定類型的號碼資源列入指南，以限制某些特定類型號碼資源的分配。但 NRA/CA 仍然可以自由決定將指配限制為僅 ECN/ECS 提供商，或決定將非 ECN/ECS 提供商的分配限制為特定類型的號碼資源。

2. 號碼資源的發展：BEREC 認為確保 ECN/ECS 提供商和非

ECN/ECS 提供商之間擁有公平競爭的環境至關重要，以防止市場內的競爭扭曲現象發生。考量每個會員國可以決定將哪些號碼資源分配給非 ECN/ECS 提供商（如果有），BEREC 認為每個會員國有責任確保不會因 OTA 和 eSIM 造成號碼資源市場競爭扭曲之事態發展。

在出現耗盡風險的情況下，NRA/CA 應立即啟動流程以識別新資源，同時向 ITU-T 請求新的號碼資源或修改分配規則，同時限制客觀上沒有必要的分配。在號碼資源耗盡風險增加的情況下，NRA/CA 將採取的行動取決於每個會員國而定，且同意應始終遵循有效和高效利用號碼資源的原則，但同時分配則交由會員國決定。

3. 指南草案的號碼範圍：BEREC 考慮了區分一般標準和特定號碼標準的建議，並且所諮詢的指南草案中規定的標準應提出可適用的最低要求，無論各自的號碼範圍如何，必須使指南可於所有會員國中實施。但是，這並不排除會員國根據各國立法決定將號碼資源分配給非 ECN/ECS 提供商，並同時考慮到號碼內在要求。
4. 其他：如果 ECN/ECS 提供商提供託管非 ECN/ECS 供應商的號碼資源，他們提供的服務需要付費。

(二) 歐盟物聯網號碼分配

歐盟成員國主管機關多在 2011 至 2017 年間陸續進行物聯網編碼與既有國家電信編碼計畫的調和研究與政策實施，說明如下：[47]

- 比利時郵政與電信機構(BIPT)理事會早於 2011 年即確立將 077 字首號碼作為 M2M 服務使用，總碼長 14 碼（含冠碼 0），該決議通過後，自 2011 年 10 月 1 日起可以提供物聯網號碼申請核配；自 2012 年 10 月 1 日起可向用戶提出物

[47] 陳思豪等人，5G 異質網路下號碼監理政策及規範之研究，2019 年 12 月。

聯網服務；若原於 2012 年 10 月 1 日前於該號碼區塊核配之電信號碼，則須至遲在 2022 年 10 月 1 日前逐步收回，以轉作為物聯網號碼使用。

- 法國主管機關電子通訊與郵政管理局(ARCEP)在 2012 年經公眾諮詢程序，決議修正電信號碼管理規範，建立 0700 字頭號碼供 M2M 使用，總碼長 14 碼。

雖然部分國家考量到物聯網數量龐大對號碼形成之壓力，故選擇以專屬號碼範圍（特定碼頭）及碼長最大化作為因應，但亦有未提供專屬編碼的國家，例如：

- 德國主管機關聯邦網路管理局（BNetzA）前經 2011 公開諮詢，於 2013 年決議以行動號碼資源做物聯網服務使用其包括 15 至 17 開頭之 11 碼（冠碼 0 不計）行動電信號碼。
- 英國在 2014、2015 年經兩次公眾意見諮詢，決定維持以行動電話號碼資源作為物聯網服務使用，其包括 071 至 075、 077 至 079 開頭之 10 碼行動電信號碼。主管機關 Ofcom 認為有許多可以作為身份辨識的替代資源，例如內部路由號碼（Internal Routing Codes）、E.212 號碼、設備識別（Equipment Identifiers）及 IP 位址等。整體而言，短期、中期的使用上，可以利用 IPv4 進行物聯網連結的相關作業。長期來說，Ofcom 認為隨著物聯網對 IP 位址的需求增加，以及網路業者技術設備的提升，未來 IPv6 將會出現在許多物聯網服務的應用。

二、美國電信網路號碼政策

(一) 北美地區電信號碼計畫

《北美地區電信號碼計畫》（North American Numbering Plan, NANP）早於 1947 年制定，1951 年實施，涵蓋範圍包括美國、加

拿大等二十多個北美國家和地區。NANP 之格式表示為 NXX-NXX-XXXX，其中 N 為 2-9、X 為 0-9 之任一數字，是由 3 位區域碼（Numbering Plan Area, NPA；或稱 area code）以及 7 位本地號碼（local number）組成，號碼長度共 10 碼。

NANP 編碼資源之管理，是由北美地區電信號碼計畫管理者（North American Numbering Plan Administrator, NANPA）全面負責，並由美國 FCC 透過競標程序選擇擔任 NANPA 的公司，以公正且妥善地管理有限資源。NANP 編碼資源的規劃、管理、分配和使用，主要依循產業編號委員會（Industry Numbering Committee, INC）制定之指南，各類號碼皆有獨立的規範指南，由電信產業解決方案聯盟（Alliance for Telecommunications Industry Solutions, ATIS）代表發行。參加 NANP 之各個國家的監管機構皆各自任命國家管理者來監督 NANP 編碼資源在國內的分配。

(二) 物聯網號碼分配

美國目前的電信號碼編碼計畫並未設立物聯網專用號碼，但在現行之 NANP 計畫中，5XX-NXX 號碼已針對機器對機器／物聯網（M2M/IoT）制定相關規定。根據 ATIS 在 2020 年發布的《5XX-NXX 非地理型號碼核配指南》（5XX-NXX Code Assignment Guidelines）[48]，5XX-NXX 號碼長度為 10 碼，格式表示為 5XX-NXX-XXXX，主要用於固定和行動設備之通訊，該資源亦可用於機器與操作後台及資料庫分享資訊，包括但並不限於無線設備，包含 M2M 之應用 。5XX-NXX 號碼屬於非地理性應用，並未分配給費率中心（Rate Centers），應用上不一定會透過 PSTN，不過仍然符合 E.164 格式。此號碼目前雖不具號碼可攜，不排除未來會開放號碼可攜服務 。

[48] ATIS, ATIS-0300052(2020-03), Non-Geographic 5XX-NXX Code Assignment Guidelines, available at https://access.atis.org/apps/group_public/document.php?document_id=51937 (Last visited:Dec. 5, 2021)

根據 2020 年 NANPA 年度報告（NANPA 2020 Annual Report），2020 年 NANPA 共核配了 1186 組新 5XX-NXX 號碼；相比之下，其 2019 年核配了 994 組，2018 年核配了 940 組。至 2020 年底，共核配了 8705 組 5XX-NXX 號碼，並回收 68 組，仍有 73 組可用於核配；使用中的 5XX NPA 共有 11 組，包括 NPA 500、521、533、544、566、577、588、522、523、524 和 525 。

依據 NANPA 於 2020 年 4 月發布之《5XX-NPA 匱乏分析》（April 2021 5XX NPA Exhaust Analysis），截至 2020 年 4 月使用中的 5XX NPA 有 500、533、544、566、577、588、522、521、523、524、525 和 526 。NANPA 使用 NRUF 之資料，預測 2021 年至 2025 年對 5XX-NXX 的總體預測需求範圍為每年 1600 到 2100 組 NXXs，年均需求為 1900 組 NXXs。假設當已分配和不可分配的 NXX 號碼數達到 800 組時，即需要一組新的 5XX NPA，預估未來五年將需要 12 組新的 5XX NPA。預留未來擴展的 5XX NPAs 包括 526、527、528、529、532、538、542、543、545、547、549、552、553、554、556、569、578、589、550、535、546 和 558。

(三) IMSI 核配情形與匱乏分析

根據 ITU-T E.212 建議書，MCC 格式為 NXX，其中 N 等於 2-9，X 等於 0-9 中的任意一數，MCC 由 ITU-T 配予成員國家，目前分配給美國的 MCC 為 310 到 316；每組 MCC 可提供 1,000 組 MNC（000-999），因此分配給美國的 7 組 MCC 可提供 7,000 組 MNC。在美國，MSIN 的長度為 9 位，格式為 XXXXXXXXX，其中 X 為 0-9 之間的任何數字，此格式為每個 MNC 提供 10 億個 MSIN。

ATIS 於 2020 年更新了第十六版國際行動用戶識別碼指南（IMSI Guidelines v16）[49]，此指南交由 IMSI 管理者（The IMSI

[49] ATIS, International Mobile Subscriber Identity (IMSI) Assignment and Management Guidelines and Procedures, available at https://www.atis.org/wp-content/uploads/2020/10/IMSI-Guidelines-v16.pdf (Last visited:Dec. 5, 2021)

Administrator, IMSI-A）負責管理，並由 ATIS 之 IMSI 監督委員會（IMSI Oversight Council , IOC）監督，以確保資源的適當使用。

當分配給美國的其中任何兩組 MCC 中的所有歸屬網路識別碼（Home Network Identity，HNI）[50]都已分配，或每季分配超過資源的 10%時，IMSI-A 將通知 IOC。當 IMSI-A 通知 IOC 分配給美國的 MCC 即將耗盡時，IOC 將對當前的 IMSI 分配進行審計，以確保有效的 IMSI 使用，如果沒有，建議啟動額外程序以實現更有效的 IMSI 使用，或者如果有效使用。

IOC 須向美國國務院提供必要的數據，並在需要時要求其從 ITU-T 獲得額外的 MCC 資源。憑藉 IOC 提供的數據，美國國務院將向 ITU-T 請求提供額外的 MCC 資源，並將結果通知 IOC。目前未分配之 MCC 尚有 317-329。如果美國需要額外的 MCC，則可以請求此段未分配列表中的 MCC，以便繼續進行分配。

三、中國大陸電信網路號碼政策

(一) 電信編碼管理法制

隨著新興技術發展日新月異，電信產業與創新應用服務對於電信號碼資源的需求產生極大變化，為了提供電信產業更好的基礎支援，中國大陸工業和信息化部（以下簡稱工信部）針對 2010 年版《電信網編號計畫》中 E.164 號碼與 E.212 號碼的相關規劃內容進行更新與修正，於 2017 年 4 月發布 2017 年版《電信網編號計畫》，同時廢止 2010 年版之電信網編號計畫，且為因應發展與管理需要，工信部將在必要時針對編號計畫進行調整。

(二) 電信號碼計畫

依據 2017 年版《電信網編號計畫》，電信號碼可分類為「ITU-T 的 E.164 號碼首位為 0-9 的全部號碼」;「固網與行網中的*/#號碼」;

[50]即 MCC+MNC。

「七號信令點編碼」;「分組數據網的編號」;「ITU-T E.212 國際行動用戶識別碼（International Mobile Subscriber Identity, IMSI）」等。以下針對 E.164 及 E.212 電信號碼進行簡述。

1. E.164 電信號碼編碼

中國大陸 E.164 電信號碼編碼結構大致可分為：

- 固定網電話號碼：採用「長途區號」的結構，即：國家碼（86）＋長途區號＋本地用戶號碼。市內電話國內有效號碼長為 11 碼。
- 行動網電話號碼：採用「網號」的結構，即：國家碼（86）＋網號＋HLR 識別號（H0H1H2H3）＋用戶號碼（ABCD）。其中包含公眾行動網電話號碼，碼長為 3 位，採用等位編號，有效號碼長為 11 碼。物聯網網號則為 5 位，亦採用等位編號，有效號碼長為 13 位。

E.164 電信號碼規劃：可分為首碼為 0、首碼為 1、首碼為 2 至 8，以及首碼為 9 等 4 類。

- 首碼為 0：首碼為 0 之電信號碼服務包含國內長途電話服務的起始號碼，以及國際長途電話業務的起始號碼。
- 首碼為 1：首碼為 1 的電信號碼為全中國大陸統一使用的號碼，該號碼按照用途可分為，業務號碼以及用戶號碼。業務號碼包含：緊急業務號碼（3 碼）、短碼（5 碼）、短消息類服務接入代碼、營運商業務代碼、路由碼以及其他電信業務接入號碼等。用戶號碼部分則包含號碼等長 11 碼的公眾行動網電話號碼，以及號碼等長 13 碼的物聯網號碼。其中，106 號段規劃用於短消息類服務，採用不等位長編碼，不同用途的短消息類服務接入代碼管理碼長不同，管理位長 5 位，使用位長等長 13 位。
- 首碼為 2 至 8：首碼為 2 至 8 的號碼，是在中國大陸本地範圍內使用的號碼，主要作為本地市內電話的用戶號碼，

同時也做為全國與省內的智慧業務的接入碼 。

- 首碼為 9：首碼為 9 之電話號碼服務包含 92 與 98 之「公眾行動電信號碼」、號碼 95 之「跨省/全國範圍內統一使用的客戶服務短號碼、電信業務接入號碼等」、以及號碼為 96 之「省（自治區、直轄市）區域內統一使用的客戶服務短號碼、電信業務接入號碼等」。除此之外，99 號段已啟用 999（僅限北京地區）與 9977（僅限部分本地網的應急通訊專用號段），其餘首碼為 9 之號碼為備用。

2. E.212 編號計畫

IMSI 用於區分蜂巢式網路中不同使用者的，同時該識別碼在所有蜂巢式網路中不重複。碼長最常 15 位。目前中國大陸 IMSI 的碼長位數即為 15 位數字的號碼。IMSI 主要由三部分組成：

- 行動國家號碼（MCC），由 3 個數字組成，用於識別行動用戶所屬的國家，中國大陸之 MCC 為 460。
- 行動網路識別碼（MNC），用於識別行動用戶所屬之行動網，中國大陸之 MNC 採取 2 位數。
- 行動用戶識別碼（MSIN），用於識別行動通訊網中的行動用戶，中國大陸之 MSIN 採 10 位數。

(三) 電信號碼核配與收回規定

中國大陸電信號碼核配之法源依據為《電信網碼號資源管理辦法》第二條，在中國大陸境內管理與使用電信網路號碼資源，應遵守該辦法。同時，依據該辦法第三條規定，號碼資源屬於國家所有。

依據該辦法，申請跨省、自治區、直轄市行政區域範圍使用的號碼，應向工信部提出申請；申請在省、自治區、直轄市行政區域範圍內使用的號碼，應向當地省、自治區、直轄市通訊管理局提供申請。電信主管部門可以委託號碼資源諮詢受理機構承擔號碼資源申請的受理工作 。

該辦法亦規定，電信主管部門應該根據號碼資源規劃、申請號碼的用途與申請人的預期服務能力審批號碼。因此，在號碼申請流程上，可分為工信部核配之各類電信號碼申請，與省、自治區、直轄市通訊管理局核配之各類電信號碼申請進行規範。

工信部收到電信號碼申請後，應當自收到申請人的申請材料之日起 10 個工作日內，發出是否受理的通知。自發出受理通知之日起 50 個工作日內，完成對申請材料的審查，作出批准或不予批准的決定。予以批准的，發給申請人正式批准文件，並抄送相關省、自治區、直轄市通訊管理局和相關基礎電信業務經營者；不予批准的，書面通知申請人並說明理由 。

省、自治區、直轄市通訊管理局應當自收到申請人的申請材料之日起 10 個工作日內，發出是否受理通知。自發出受理通知之日起 30 個工作日內，完成對申請材料的審查，作出批准或不予批准的決定。予以批准的，發給申請人正式批准文件，並報工信部備案；不予批准的，書面通知申請人並說明理由 。號碼申請人獲准使用號碼資源後，電信主管部門可以採用指配、隨機選擇和拍賣等方式分配號碼 。

至於電信號碼收回機制，依據該辦法第 38 條規定，工信部或省、自治區、直轄市通訊管理局在號碼資源管理中，發現有下列情形之一，可以收回已分配的號碼資源：

- 已終止占用號碼資源的業務；
- 在規定時間內未啟用號碼資源；
- 以欺詐手段獲得號碼資源；
- 超過規定期限使用號碼資源；
- 改變電信主管部門規定的號碼結構、位長、撥號方式和使用範圍使用號碼資源；
- 擅自啟用、擴大範圍、改變用途、改變長途編號區或跨本地網使用用戶號碼資源；

- 轉讓、出租號碼資源或將號碼作為商標進行註冊；
- 拒不按照規定繳納號碼資源使用費；
- 拒不執行電信主管部門的號碼調整要求。

(四) 物聯網專用號碼區塊之規劃

在 2017 年版電信網編號計畫中，工信部新增物聯網號段 ，首碼為 1 之號碼作為物聯網號碼開頭。目前物聯網號碼可分為三個號碼區塊，分別為 140xx-144xx 的物聯網號碼區塊、145xx-149xx 的公眾行動通訊號碼專用於物聯網業務，以及用於機器通訊號碼，僅限用於非語音業務的 1064x 號段。

140xx-144xx 號碼區塊為物聯網服務專用，有效號碼長 13 碼（若含國碼則為 15 碼長）。目前，140xx 分配給予中國聯合網路通訊集團股份有限公司（以下簡稱中國聯通）、141xx 分配給予中國電信集團有限公司（以下簡稱中國電信）、142xx-143xx 尚未分配、144xx 則分配給予中國移動通訊集團公司（以下簡稱中國移動）使用。前述物聯網號碼將依據各電信營運商的需求核配啟用。

1. 公眾行動通訊號碼物聯網專用號段

中國大陸在物聯網號碼資源使用上，亦包含公眾行動通訊號碼 145xx-149xx 之號碼區塊，有效號碼長 11 碼，其中 146xx、148xx、149xx 之公眾行動通訊號碼亦規劃作為物聯網業務專用號碼，目前 145xx-149xx 物聯網號號碼資源規劃情形為（截至 2018 年 10 月 31 日）：中國移動獲得分配 148（0-9）號段（物聯網業務專用號段）、中國聯通則獲得分配 146（0-9）號段（物聯網業務專用號段），以及中國電信獲得分配 149（0-9）號段 。

2. 物聯網專用號碼資源（機器通訊號碼，僅限用於非語音業務）

電信號碼首位為 1 號碼的號碼規劃中，106 號段規劃用於短消息類服務。其中，1064 號段用於機器通訊業務（僅限用於非語音業務），管理位長 5 位，使用位長等長 13 位（若含國碼則為

15 碼長），該號碼由工信部負責分配與管理 。至於，1064x 號段物聯網專用號碼資源（機器通訊號碼，僅限用於非語音業務）規劃情形，依據 2020 年 5 月 21 日公布之電信網號碼資源使用審批結果（短消息服務接入代碼），截至 2017 年 5 月 31 日，10646 號段獲得分配予中國聯通；10647 號段獲得分配予中國移動；10648 號段獲得分配予中國移動；10649 則核配給予中國電信 。

(五) 物聯網號碼資源核配與使用情形

工信部於 2017 年首次核配物聯網號碼給予三大營運商：中國移動、中國電信以及中國聯通，三大電信營運商均獲得物聯網號碼資源，其中，公眾行動通訊號碼物聯網業務專用號段核配情形：中國移動獲得 148（0-9）號段（物聯網業務專用號段）、中國聯通則取得 146（0-9）號段（物聯網業務專用號段）。

物聯網專用號碼區塊核配情形：中國移動取得 1440（0-9）號段（物聯網網號）。中國電信則取得 1410（0-9）號段（物聯網網號） 。後於 2020 年 4 月，工信部發布 2020 年第 5 批「電信網碼號資源使用證書」，中國移動再次獲得核配 1441（0-9）號段（物聯網網號）。

此外，2020 年 3 月，工信部發布《支持和規範移動通訊轉售企業開展移動物聯網業務轉售試點辦法》，要求於 2020 年 5 月 1 日起開展行動物聯網業務轉售試點，並將物聯網轉售納入 2020 年工信部的重點工作。接者 2020 年 4 月，工信部發布《關於深入推進移動物聯網全面發展的通知》中，再度重申支持行動通訊轉售企業開展物聯網業務，充分發揮行動通訊轉售企業快速、靈活的響應機制與跨行業優勢資源能力，在工業網路、車聯網等垂直行業應用領域開展行動物聯網業務創新，促進與實體經濟融合發展 。基此，中國聯通於 2021 年 1 月率先啟動物聯網轉售試點，首批物聯網轉售企業共有七家企業，以推進行動轉售業務發展 ，中國聯通也因透過行動通訊業務轉售，獲得工信部核配 10641 物聯網轉售專用號段，

目前中國電信、中國移動並未獲發物聯網轉售專用號碼資源。

四、日本電信網路號碼政策

根據 IEEE 的「M2M 和 IoT 裝置號碼計畫」（Numbering Plan for M2M and IoT Services）[51]研究指出，日本總務省（Mnistry of Internal Affairs and Communications, MIC）於 2011 年即已針對 M2M 編碼進行諮詢。M2M 通訊可用於災難預警、環境預警、農業創新等應用，原使用隸屬行動電信號碼的 070/080/090 號碼，以及不包含語音通話的行動數據通訊（mobile data communication）。

隨著物聯網應用快速成長，總務省於 2017 年公布「M2M 等專用號碼創建」（M2M 等専用番号の創設）[52]，並修訂電信號碼規則（電気通信番号規則）及相關規範，將 020 號段（除 020-4 外）指定為 M2M 服務的專用號碼，明定 M2M 服務範圍、號碼核配標準及使用規則。020 號碼長度為 11 碼，原是提供 BB.Call 使用，由於其使用量迅速減少，在 2017 年後改為限用以 020-4 開頭之號碼，其他 020 號碼則規劃為 M2M 專用。在使用上，020 號段作為 M2M 專用號碼，僅提供有限的語音通話，設計為受話方（M2M 服務使用者）無需識別號碼，且僅與特定人員（例如呼叫中心操作員）可進行語音通話。此前使用 070/080/090 之 M2M 服務，在設置 M2M 專用號碼後仍可持續使用原號碼，不過將對此額外進行收費。

2017 年設置之 M2M 專用號碼 020 號碼，號碼容量為 8,000 萬門，為避免號碼資源枯竭，總務省除了設置 M2M 專用號碼 020 號碼外，後續也於 2019 年公告「IoT 時代電信號碼相關研究會報告書」（IoT 時代の電気通信番号に関する研究会 報告書）[53]，檢討 020 號碼容量，並探

[51] 總務省，〈M2M 等専用番号の創設〉，1/4/2017，<https://www.soumu.go.jp/menu_news/s-news/01kiban06_02000056.html>。

[52] Hu, Chih-Nan, Shih-Hsiung Lee, Chu-Sing Yang, "Numbering plan for M2M and IoT services- A study of United States, Japan, China and Taiwan," 2017 International Conference on Information Society (i-Society), 2017, pp. 40-43.

[53] 總務省，〈IoT 時代の電気通信番号に関する研究会 報告書〉，7/3，2019，

討由 11 碼增碼至 14 碼等相應對策。由於無論是增碼至 12 碼、13 碼或是 14 碼，對於使用者以及系統修改成本的影響差異並不大；然而若採取階段性增碼將增加系統修改的對應期間與成本，且對於使用者影響較大。020-0 為尚未核配之號碼，因此總務省擬定未來規劃將 020-0 增碼至 14 碼，以因應迅速成長的物聯網號碼需求。

第七節　網際網路標識及通訊協定

一、發展沿革

上個世紀 60、70 年代由美國部署的高等研究計畫署網路(Advanced Research Projects Agency Network, ARPANET）是網際網路（Internet）的雛形。後來，各種各樣的電腦網路在規模和數量上的提升，促成了不同網路之間的互連需求，最終導致了 TCP/IP 協定及 Internet 的誕生。初期的 Internet 主要基礎是 WWW/HTTP，TCP/IP，分組傳輸，Ethernet 等，完成的業務也比較簡單，大部分是實現基礎的資料互聯，設計理念是簡單、開放和低成本。

經過幾十年的發展，隨著業務類型、用戶數量、終端類型的不斷演進，Internet 自身也變得越來越複雜。Internet 相關創新技術也是層出不窮，例如內容傳遞網路（Content Delivery Network, CDN）、SDN/NFV、雲端運算、邊緣運算等等。可以預見的，隨著更多的業務場景、接取方式的出現，尤其是 6G 網路的各種探索和需求驅動，未來的 Internet 或者未來的 IP 網路也需要更多的創新技術來支撐。

二、網際網路的標準化工作

網際網路架構委員會（Internet Activities Board, IAB）是一個技術監督和協調的機構，並負責定義整個 Internet 架構和長期發展規劃。IAB 其下有兩個重要單位：網際網路工程工作組（IETF）和網際網路研究工作組（Internet Research Task Force, IRTF）。IETF 主要負責

<https://www.soumu.go.jp/main_content/000631590.pdf>。

Internet 技術標準之制定，IRTF 則努力 Internet 的未來方向之研究，如圖 2-7 所示。

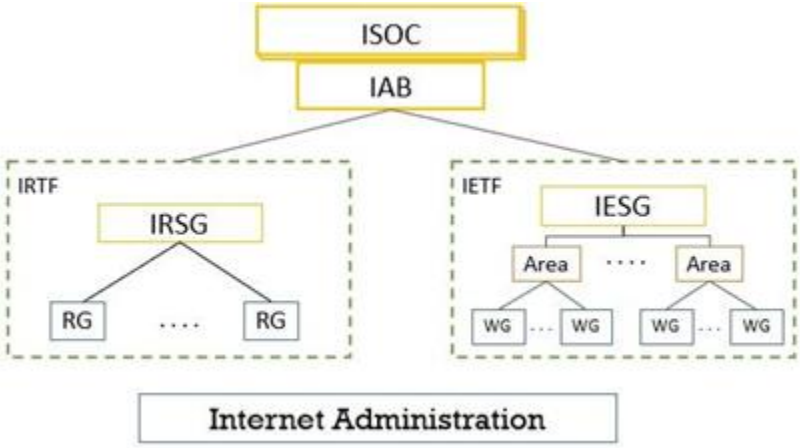


圖 2- 7、Internet 標準的維護組織

資料來源：ISOC

網際網路技術標準可以是單一或一組特殊的意見徵求稿（Request For Comments, RFC）。一個 RFC 文件在成為正式的技術標準前一般至少要經歷三個階段：建議標準（Proposed Standard）、草案標準（Draft Standard）以及網際網路標準（Internet Standard），如圖 2-8 示意。

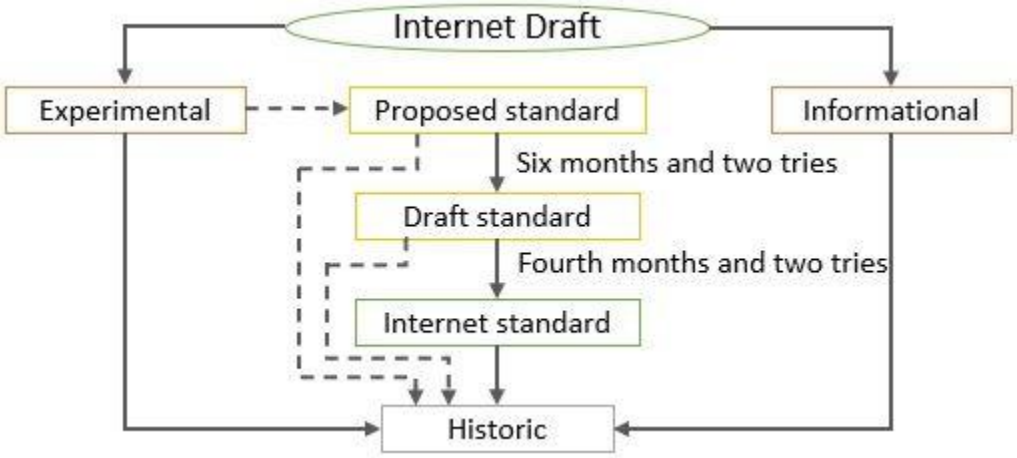


圖 2- 8、基於實用性的 RFC 文件分類

資料來源：IETF

RFC 文件除了部分成為網際網路標準，另有 Experimental 及 Informational 等型態。Experimental 為提出實驗性質為主的方案，在驗

證後可能成為建議標準或草案標準；Informational 則是具資訊性質的文件，或用於廣泛性的描述問題點。RFC 文件的詳細制定程序及文檔撰寫指引可參見：

- RFC 2026 - The Internet Standards Process -- Revision 3
- RFC 6410 - Reducing the Standards Track to Two Maturity Levels
- RFC 2223 - Instructions to RFC Authors

現今，絕大部分網路技術標準的制定都是以 RFC 形式開始，經過大量的論證和修改過程，最後獲得主要的標準發展組織（standards development organization, SDO）所採用。

三、IP 位址及網域名稱技術標準

Internet 萌芽之初，為使電腦網路得以相互溝通及傳輸訊息，分別制定傳輸控制協定（Transmission Control Protocol, TCP）及網際網路通訊協定（Internet Protocol，下稱 IP 通訊協定），並以此定義電腦網路的「資訊傳輸方式」及「電腦的位置」。其中，IP 通訊協定主要定義網路上連線裝置的位置，而每一台網際網路連線的裝置均需透過 IP 通訊協定配置一組 IP 位址，如同電信號碼與位址，使電腦或連線裝置得以將資料傳輸至正確目的地。

IP 位址為有限資源，必須透過全球統一協調、分配以及管理。第一個被廣泛使用的通訊協定版本為 IPv4（Internet Protocol version 4），由網際網路號碼分配機構（Internet Assigned Numbers Authority, IANA）依據全球階層架構及分配政策配發。隨著新型態通訊技術對於 IP 位址需求大增，IETF 自 1990 年開始著手檢視 IPv4 位址短缺問題，其後於 1995 年提出下一路通訊協定 IPv6（Internet Protocol version 6），最終在 1998 年 12 月正式發布於 RFC 2460 文件。

IPv6 不僅比 IPv4 具備更多連網與擴充功能，同時也納入許多早期 TCP/IP 通訊協定不具備的優勢特色，大幅提升網際網路傳輸的效能 ：

- IPv6 具有 128 位元長度的位址空間，足以提供電腦、手機、汽

車等多種網路終端應用裝置之 IP 位址；

- IPv6 通訊協定支援自動組態（Auto-Configuration），因此電腦主機接上 IPv6 網路後即可自動取得 IPv6 網路位址資訊；
- IPv6 通訊協定內建個人電腦身分認證加密功能（Internet Protocol Security, IPSec）大幅提升網路安全性；
- 支援 Mobile IP 機制，Mobile IPv6 可提供較 Mobile IPv4 更強大的移動性，解決以往跨網段漫遊所發生的連線障礙；
- 強化服務品質保證（Quality of Service, QoS）機制。

對於網際網路及其他基於 IP 的分封交換網路，遵循 IETF RFC 1035 文件所定義的網域名稱（Domain Name, DN）形式早就為大家所熟知並使用。基於 DN 的統一資源識別碼（Uniform Resource Identifier, URI）可用於識別用戶／主機（例如 user@domain.com），IP 位址則用於路由到主機連接的接口。參與通訊的主機可在網域名稱系統（Domain Name System, DNS）的協助下，將 DN 解析為 IP 位址。

IETF 針對 DNS 最初公布的標準為 RFC 882 與 RFC 883，之後更新為 RFC 1033、RFC 1034 以及 RFC 1035。DNS 為分層式架構，由上至下分別根網域（Root domain）、頂層網域（Top Level domain）、第二層網域（Second Level domain）以及主機網域（Host domain）。由於 DNS 為分層式架構，其名稱空間亦為分層，因此 DNS 的各分層級別僅須於名稱的「樹系」（Tree）中提供並維護有關下一級別的訊息。

以 DNS 運作機制而言，當行為人使用瀏覽器訪問網站，瀏覽器首先會要求本地操作系統查詢該網站名稱，因此本地操作系統會向配置的 DNS 解析伺服器之一發送查詢的請求，並且等候回應瀏覽器所需的 IP 位址。當解析伺服器接收到查詢的請求後，會立刻對其快取進行檢查，以便查找有用的回應。若無法找到所需的訊息，解析伺服器會與相應的 DNS 權威伺服器對話，以獲取所需的資訊。在 DNS 的分層式架構下，從最上層的「根伺服器」（Root Server）開始，根伺服器會告訴本地系統在哪裡可以找到頂層網域伺服器（例如.org）；並且向.org 伺服

器詢問（例如 wikipedia.org），最後向（wikipedia.org）伺服器詢問（例如 www.wikipedia.org），其運作流程如圖 2- 9、DNS 運作流程示意所示。

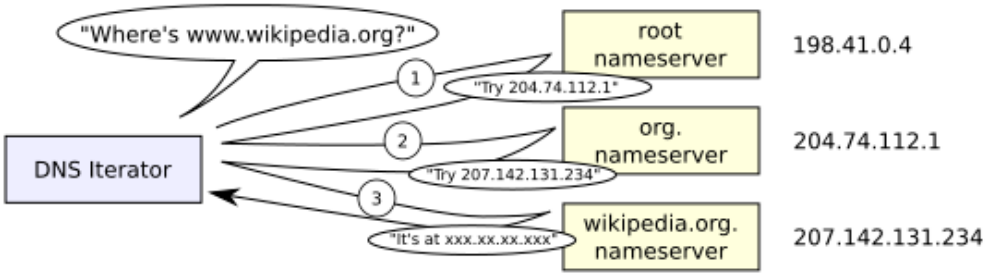


圖 2- 9、DNS 運作流程示意

資料來源：維基百科

時至今日，全世界共有 1,000 餘種不同種類的頂級網域（Top-Level Domain, TLD），主要類型包含通用頂級網域名稱（Genetic Top Level Domain, gTLD）及國家（或地區）的頂級網域（Country Code Level Domain, ccTLD），均由 ICANN 負責管理。

ICANN 於 2012 年 1 月啟動「New gTLD 計畫」，接受公眾依各自需求，依《新頂級網域申請人指南》(Applicant Guidebook, AGB)中所規範的程序，向 ICANN 提出申請。此為 ICANN 首次對公眾開放頂級網域的申請，共有超過 1900 件的申請案提出申請，在臺灣也有「.TAIPEI」、「.HTC」與「.ACER」提出申請，隨著頂級網域的普及化讓多元化的網路世界變得更為多彩多姿。

自 2012 年開放公眾申請 New gTLD 登記以來，ICANN 也持續準備為下一輪的開放作業，終於在經過多年的準備與討論後，相關項目草案在 2020 年結束前完成，並經 Generic Names Supporting Organization（GNSO) 理事會於 2021 年 2 月採納相關建議並隨後向 ICANN 董事會

提交終版報告[54]，目前尚待 ICANN 董事會表決通過，其後預期將在 2022 年啟動新一輪的新 gTLD 申請。

第八節　小結

經廣泛分析電信、網際網路號碼標識之國際標準及主要國家推動 IPv6 之政策的成果發現，下世代網路朝向全面採用網際網路通訊協定(All-IP)、接取端異質網路技術融合匯流發展的基本趨勢仍未改變。從各國對物聯網編配 E.164 號碼政策經驗的比較與對照，亦可確認依據 ITU-T E.164 規約編定的公眾電信網路號碼計畫，在維持全球電信網路互通性原則不變之下，目前尚無有力的論點或證據支持其已不再能滿足下世代電信網路對於號碼、命名、定址和識別資源（NNAI）相關需求。

作為下一代 Internet 的核心和基礎性的技術，IPv6 正在成為未來網路空間競爭和話語權的重要指標，IPv6 影響著各國在未來全球 ICT 競爭中的地位和作為全球下一代 Internet 網路和資源中心的佈局。IETF 是制定以 IPv6 為代表的 Internet 技術標準的主要組織，其新近的動向反映了 Internet 網路技術的發展趨勢，因此觀察 IETF 的技術動態對於準確把握網路技術發展及趨勢，並支撐我國的資訊網路建設具有重要作用。

從 IETF 內與 IPv6 技術比較密切的幾個 WGs 研究重點來看，大致可綜合出 IPv6 的技術趨勢，即未來向開放化、IPv6-Only 化、智慧化及普適性方向發展。我國產業界應該順應趨勢，一方面積極參與國際的 Internet 技術創新，參與 Internet 規則的制定，為國際 Internet 的發展作貢獻；另一方面，推進 IPv6 技術的產業化應用，特別是發揮 IPv6 的技術優勢，將 IPv6 和雲端網路匯流、工業 Internet、智慧城市等新興場景結合，促進 IPv6 與經濟社會各領域的深度匯流應用，也促進我國資訊基礎設施的升級換代。

---

[54] ICANN GNSO - Final Report on the new gTLD Subsequent Procedures Policy Development Process, available at https://gnso.icann.org/sites/default/files/file/field-file-attach/final-report-newgtld-subsequent-procedures-pdp-20jan21-en.pdf (Last visited:Jul. 15, 2021)

此外，由 IPv6 構建出新的網路空間平臺與垂直應用，將會產生更多的技術創新機會；值在大力推動 5+2 產業創新政策與數位國家之際，如何有效地引導產業及學研界，協同建構並深化 IPv6 規模部署、產業發展和應用創新，應屬現階段較為迫切也是政府應予重視的任務，其理由如下：

1. IPv6 有助於數位轉型推動

在我國政府及各行業推動數位轉型的過程中，物聯網是重要的一個環節，物聯網節點負責數據的採集、處理和控制，物聯網傳感器的爆炸式增長使數字孿生成為可能。與採用 IPv4 或者其他私有協定相比，採用 IPv6 協定將使得網路架構更加靈活，數據採集的覆蓋範圍進一步擴大，相應地也帶來物聯網設備成本的降低。另外，IPv6 的特點將滿足物聯網特有的一些需求，如基於 IP 位址的反向控制，這在 IPv4 網路中是難以做到的。從可行性來說，隨著物聯網晶片性能的提升，物聯網終端內的資源已經可運行完整的 IPv6 協定堆疊，並具備商用化的能力。IPv6 在物聯網的廣泛應用也將反過來推動 IPv6 技術本身的升級完善，如在路由、安全及可管理性等方面提出新的需求。

網路的開放式架構把應用層的創新開放給了用戶，才使得網際網路的業務空前繁榮，也促使網際網路特別是行動網路的成功，因此說開放性是網路成功的精髓也毫不為過。在網際網路的發展過程中，隨著網路從學術網路向商業化網路的轉變，各方從自己的利益出發希望調整甚至改變網際網路的架構，如嘗試將網路做成封閉式，但最終都以失敗而告終。作為下一代網路的核心和基礎性的技術，IPv6 正在成為未來網路空間競爭和話語權的重要指標，IPv6 影響著各國在未來全球 ICT 競爭中的地位和作為全球下一代網路和資源中心的佈局。

2. 持續關注 IETF 網路技術標準發展

IETF 是制定以 IPv6 為代表的 Internet 技術標準的主要組織，其

新近的動向反映了網際網路技術的發展趨勢，因此觀察 IETF 的技術動態對於準確把握網路技術發展及趨勢，並支撐我國的資訊網路建設具有重要作用。

從 IETF 內與 IPv6 技術比較密切的幾個工作組工作，大致可綜合出 IPv6 的技術趨勢，即未來向開放化、IPv6-Only 化、智慧化及普適性方向發展。我國產業界應該順應趨勢，一方面積極參與國際的網際網路技術創新，參與網際網路規則的制定，為國際網際網路的發展作貢獻；另一方面，推進 IPv6 技術的產業化應用，特別是發揮 IPv6 的技術優勢，將 IPv6 和雲端網路匯流、工業網路、智慧城市等新興場景結合，促進 IPv6 與經濟社會各領域的深度匯流應用，也促進我國資訊基礎設施的升級換代。

於此同時，IETF 工作小組仍持續針對 IPv6 進行優化，已於上述。而 3GPP 亦正在考慮將 5G SA（Standalone）全面採用 IPv6，因為在科技與網際網路發達的當代，設備、網路、內容所構成的通訊鏈（device – network – content communication chain）已做好採用 IPv6 的準備，當電信營運商讓更多使用者採用 IPv6 時，即可受益於 IPv6 所帶來的各項優勢。例如，藉由消除網路位址轉換成電信級（Network Address Translation, NAT）或營運商級（NAT／ Carrier Grade NAT, CGNAT）網路時，在技術上帶來的複雜性，並能減少資本支出（Capital Expenses, CAPEX）和營運支出（Operational Expenses, OPEX）

在電信網路（電信層）及網際網路（應用層）不同網路層級下，「號碼」均賦予設備唯一的識別性，並使網路中的其他設備可以透過定址機制，與該設備互連通訊。

電信網路所使用之 E.164、E.212 號碼，係仰賴冠碼及首字碼達成國家、地區、服務性質的辨識。在網際網路上，IP 位址的辨識性雖然非常低，但透過 DN 命名及 IP 轉換解析機制（即 DNS 系統），則不但強化了辨識性，同時得力於網路應用層的開放性，可進一步擴增號碼

之功能，因應物聯網大量裝置的需求，可使用自動命名及管理系統，強化管理需求以及安全性。

一、下世代電信網路號碼技術與物聯網發展對電信號碼之需求

E.164 電信號碼用於基礎電信語音服務，可說是電信網路互連通訊的最基礎號碼，我國的《公眾電信網路號碼計畫》即為我國 E.164 號碼之分配管理計畫。依據《電信號碼核配及管理辦法》第 3 條，我國的電信號碼之編定主要用以辨識國家、地理區域、電信網路以及服務類型；而在服務面向，則包含市話、行動、衛星、網路電話、智慧虛擬碼以及物聯網號碼。因此，觀察 E.164 號碼的使用變化，係隨電信技術及網路技術演進而修訂，但歸根究底，新型態電信服務是否被納入國家的號碼計畫，與該服務是否需與既有電信網路互連互通有極大關連。

在下世代電信網路號碼技術發展上，則可先行觀察 5G/B5G 電信網路技術發展，在 5G 技術標準逐漸完成下，預估 M2M 及物聯網 IoT 等移動設備將蓬勃發展，而妥善的號碼計畫則是促進企業和應用服務發展的基本要件。

物聯網發展對於國家電信號碼計畫會產生何種影響？對此，在〈機器間通訊和物聯網服務之編碼計畫－對美國、日本、中國大陸和臺灣之研究〉[55]當中，可知 M2M 和物聯網通訊領域迅速發展的同時，將對國家電信號碼計畫產生影響，而 M2M 等設備須有唯一識別性和定址才能與其通訊，而本文分析至少在中短期內，M2M 裝置使用 E.164 號碼資源是可行解決方案。

GSMA 在 2018 年發布的〈E.164 regulatory exceptions for IoT connected services〉立場文件中，對於物聯網連結服務使用 E.164 電信編碼之探討，提出不同觀點[56]。首先，該組織認為物聯網連結服務可部

[55] CN Hu, Numbering plan for M2M and IoT services - A study of United States, Japan, China and Taiwan, available at https://ieeexplore.ieee.org/document/8354667 (Late visited, May, 26,2021)
[56] GSMA, E.164 - regulatory exceptions for IoT connected services, available at https://www.gsma.com/iot/iot-knowledgebase/e-164-regulatory-exceptions-iot-connected-services-gsma/ (Last visited:Dec. 5, 2021)

署及使用 E.164 號碼，在現有的電信網路架構中，以提供相對簡單的功能，例如計費及支持營運系統，避免建立不同編碼方案帶來的複雜性及提升成本，故使用 E.164 作為物聯網號碼有其意義。

該組織另提出兩個爭議點，第一，是否所有的物聯網設備都需要使用 E.164 號碼資源才能運作？第二，物聯網設備是否適用傳統行動網路的相同編碼方式？

GSMA 並認為，就產業的立場來看，廣泛被接受使用 E.164 編碼方式，與物聯網設備之性質並無非常強烈的關聯性，而管理機關應考量需求與服務性質，而不單考量號碼編碼方式。在探討物聯網連結服務使用 E.164 的需求方面，如智慧電表、資產追蹤工具，可由以下需求項目進行評估：

- 設備間的互通需求
- 整合至定價透明規則及納入國家電信號碼計畫
- 號碼可攜服務（Number portability）
- 緊急電話服務
- 主叫用戶識別（Calling Line Identification, CLI）規則

其實，不僅是物聯網號碼，若我們將當前的號碼計畫重新以上述原則評估，亦可初步推論，衛星通訊、網路電話及物聯網號碼，其實可能無須刻意給予獨立的號碼區塊，或者無須給予號碼區塊。從另一方來說，E.164 號碼在辨識性上的強化，其解決方案仍來自於應用層，例如業者開發 whoscall 網路 APP 以阻擋惡意來電等。

二、下世代電信網路與物聯網發展的號碼分配管理議題

承上述，物聯網是否使用 E.164 號碼資源或是採行新的編碼方式，仍是目前國際上探討的議題，並沒有統一及具體的共識。然而，從國際文獻當中也觀察到，由於物聯網設備種類繁多、數量龐大易造成管理不易，故在考量不同系統間獲取及傳遞多元資料的溝通成本上，將產生為眾多實體物件的命名架構及其可辨識性建立規則之需求。如同

前述GSMA報告提到，使用E.164號碼和與物聯網連接設備需求無關，而物聯網唯一識別及定址的重要性，並沒有在E.164號碼中呈現。

在E.164之外，國際陸續有針對物聯網編碼的研究陸續展開，例如韓國學者 J. Jeong 在 IETF 工作小組提出將存在於車聯網中的物聯網設備使用 DNS 命名解決方案[57]，該文章提到物聯網設備可以在有線和無線網路環境，透過 DNS 自動配置，可管理物聯網設備型號、並進行遠端控制管理。DN機制之運作介於電信層與應用層之間，其定址為IP位址，因此實際的分配管理為IP位址的分配。IP位址分為IPv4與IPv6，若為IPv6則可進一步強化唯一識別性，DN由於命名機制極為彈性，故DN/IP機制用於物聯網號碼，可兼具定址、辨識性以及唯一識別性。

今（2021）年召開的 ICANN 72 會議，由 CIRA 提出"Zero-Touch Universal IoT Device Identity"報告，該報告提出利用現有的公共金鑰基礎設施(Public key Infrastructure,PKI)(IETF DANE 架構)進行物聯網設備識別之解決方案。而本計畫也於分項三進行物聯網編碼 PoC 驗證，依據 ICANN 所建議的 DNS 技術及 ETSI 發布的 MEC 邊緣運算架構。本實驗的目的為解決E.164號碼資源有限性、掌握及分配物聯網設備識別性並進行管理。

DNS 機制出現在號碼分配管理的議題中，除了電信網路上的號碼功能在辨識性、識別性均相當有限外，其互通性的需求也低與 TCP/IP 所形成的網際網路。下世代電信網路號碼技術可能包含更多的異質網路整合需求，由5G核心網路IP化的發展可以推論，異質網路的互通性可能於IP層加以解決，對於電信號碼的需求逐漸下降；而IP與DNS的運作已相當普及而成熟，已可說是成為新型態的數位基礎設施。

三、技術演進趨勢與號碼需求

在既有E.164號碼的基礎下，從基礎服務、識別、辨識、定址、互

[57] J. Jeong, DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks, available at https://www.ietf.org/id/draft-jeong-ipwave-iot-dns-autoconf-11.html (Last visited:Dec. 5, 2021)

通等條件，觀察下世代電信網路號碼技術的發展，在接取網路上，新技術（如衛星）首要提供寬頻接取而不提供語音接取，對於納入 E.164 的需求亦不顯著。

本計畫評估，未來無論是新電信技術或是物聯網，是否需編定特別的號碼區塊，應由具體的服務需求而定。例如車聯網服務，編定首碼識別其為車輛；或因人工智慧之發展，未來需辨識非人類對象等，針對特定物聯網類型的需求，考量公共性、而非技術性，以編定號碼區塊。現行的編碼計畫，070 網路電話以及 040 物聯網則可配合前項建議進行回收重整，未來則建議以技術中立之概念進行評估、分配管理。

另一方面，觀察下世代電信網路架構下，不論行動通訊或是物聯網通訊仍使用 E.164 編碼規則，在電信層並未出現新的取而代之編碼標準。本計畫所觀測之新編碼機制均建立於應用層、IP 網路基礎上，並能辨識或定址更多類型的資訊、物件等。

國際文獻探討中雖並未排除 E.164 用於物聯網編碼，然而在網路切片、軟體定義網路及網路虛擬化等下世代電信網路號碼技術中，物聯網編碼仍多於應用層討論其可行的編碼方式。提供域名和 IP 位址相互轉換的 DNS 不但是網路世界中最為普遍使用的標識解析（Identifier Resolution）服務，未來亦能在建構工業物聯網的關鍵基礎中作為核心要素。

新型態編碼多出現於應用層，且於分配、管理、應用上均能開發出更多的創新服務；然而，電信網路編碼仍有其穩定可靠、且基礎電信服務為最基本、也具全球互通性的既有需求與優勢存在。本計畫在此分析電信層及應用層編碼的優缺點分析（詳如表 2-2）。

蒐集目前國際文獻，綜整設計及規劃在網路切片環境下進行物聯網的編碼機制。在網際網路上面可以衍生出更多面向的應用，並提升網路應用效能。例如物聯網裝置管理及資源管理面向。

表 2-2、電信層及應用層優缺點

	優點	缺點
電信層 (E.164)	・高度穩定性與可靠性 ・可全球互通	・變更或擴充時的行政成本高昂 ・屬國家資源、監管力道較高
應用層 (DNS)	・高使用彈性及可擴充性 ・相對較低的監管程度	・需要 DNS 標識解析服務 ・易受資安攻擊、較高的資安風險

資料來源：本計畫整理

四、其他議題建議

本章首先呈現國際電信網路號碼機制以及網際網路主要標識與通訊協定之發展分析，特別著重於所涉相關國際標準形成機制的介紹，針對「超前部署下世代電信編碼技術與標準」之目的，並可藉此作為將來在基礎科研與人才培育執行上的依據，以充分達到參與標準發展、洞悉國際標準發展趨勢、發揮我國資通訊技術研發實力之目的與效益。

在 5G 和雲端時代，IPv6 從根本上解決了 IP 位址不足的問題。此外，未來應用如自動駕駛、工業自動化、VR（Virtual Reality）、智慧醫療和物聯網等，需要具有突破性的〝IPv6+〞網路技術，如 SRv6、BIER6 等新協定為代表，並結合機器學習(Machine Learning,ML)與人工智慧(AI)技術進行網路分析，智慧調整等，而 IETF 也針對未來技術需求持續進行相關標準制定。持續關注 IPv6 網路產業技術標準，才能讓國內網路環境與時俱進，符合未來應用發展需求。

此外易衍生有關資料在地化及跨境傳輸等個資及數據保護相關議題，在國際實務上，可概分為：全面禁止跨境自由流通、於特定範圍內禁止或有條件允許跨境自由流通，以及未禁止跨境資料自由流通等三類。我國對於資料跨境傳輸之相關規範可參照《個人資料保護法》第 21 條規定，乃採「原則允許，例外限制」之規範模式。

國發會自 108 年元月起接替法務部成為個資法的法規解釋機關，並於本（110）年召開跨部會個資保護會議，要求各部會須修正各自的

《個資安全維護辦法》，對於使用資料者的身分確認及保護機制、個人資料顯示之隱碼機制、網際網路傳輸之安全加密機制等訂定資安標準規範，並依據不同業別、不同規模的企業採分級管理。由於尚待各部會完成法規修訂，建議列為下年度議題續作研究。

最後，為更具體規劃電信編碼政策發展方面及其可操作的策略方法，本計畫謹先就將來成立專案小組編撰政策藍皮書之架構主軸，試擬如列：

- 我國電信號碼機制現況分析、當前挑戰與因應，以及未來願景之探究。
- 公眾電信網路號碼計畫整備，包括：檢討現行各類智慧虛擬碼之存廢或整併，040 及 070 字頭號碼於物聯網使用之區別，對自動語音呼叫(Robocall)使用地理性號碼（市話號碼）、手機號碼或智慧虛擬碼之限制或規定等。
- 資料在地化及跨境傳輸議題之探討
- 自廣泛的文獻探討及專家意見收攏聚焦出技術演進、標準制定及電信網路號碼資源編配管理相關組織之參與策略及其重要性。
- 透過盤點技術缺口、科研投入、人才培育等系列舉措之規劃與執行，重點強化與 ICANN、IETF 等全球網際網路組織之連結，緊密跟隨國際 IPv6+技術發展趨勢，俾為我國在電信網路領域積極布局、爭取更多的國際空間。

第三章　下世代電信網路號碼資安稽核

第一節　下世代網路資通安全研析

一、下世代網路資通安全

在 2019 年 5 月，國際電信聯合會電信技術標準部門（ITU Telecommunication Standardization Sector, ITU-T）下之 2030 網路技術焦點組 （Focus Group Technologies for Network 2030, FG-Net-2030）發表「科技、應用及 2030 市場驅力藍圖」（Network 2030 : A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond）」，進一步揭櫫未來 2030 年新興科技應用趨勢、願景、重點發展領域以及對既有網路的影響。

在 Network 2030 的願景下，屆時全球的網路技術發展將超越當前的想像，發展出跨世代的通訊科技整合應用型態，諸如全息投影通訊（Holographic Type Communication）、急難災防情境下可快速整合及反應的新資通訊技術、多重感知網路（Multi-sense Network），以及能支援高時間精準、智慧化、自動化服務系統運作的「時間工程應用」（Time Engineered Application）等前瞻性通訊服務需求。

FG-Net-2030 預測，現今網路技術研發途徑將不再只專注在水平網路層級的技術優化，重點是以創新網路技術滿足民眾在人際溝通的互動需求，特別是新的媒介工具（New Media），例如全息影像溝通方式（Holographic Approaches）使民眾即使處於遠距溝通情境，也如同親身見面，而此類的技術需要更大容量和更高傳輸能力的網路。此外，隨著固網與無線電接取網路技術（Accessed Technologies）的演進，網路技術能量將會滲透至各個垂直層，使網路技術由垂直層級（Networked Verticals）進行更緊密的整合。

為達到 Network 2030 的下世代網路願景，網路建構的原則必須要符合上述之新型態通訊服務特性（詳參表 3-1），簡言之，未來網路將是一個點對點整合型態（end-to-end integrated）的動態結構。未來網路

的核心建立在使用網路切片的環境基礎下，每個切片中支援各種功能與非功能性的需求（Functional/Non-functional Requirements）。Network 2030 在行動通訊上，除了加強 4G LTE 盡力而為（Best effort）的網路技術特性之外，更在 5G/B6G 技術逐漸成熟的同時，鼓勵原生網路功能技術持續演進，亦即，發展跨介面之通訊協定與機制，並於內部網路層中設定相對應的傳輸保證 KPI、QoS，建構一個異質網路基礎設施共存、符合數據傳輸即時性（timeliness of data delivery）的未來網路環境。

表 3- 1、Network 2030 網路架構原則

原則		未來型態
1	簡單明瞭(Simpliicty)	簡化服務傳輸路徑中的元件數量
2.1	具原始編程能力 (Native Programmability)	在標準化程式介面下，增加網路設備的動態編程能力以達到服務客製化
2.2	向下相容性 (Backward Compatibility)	有能力支援、整合新/舊 IoT 裝置的網路通訊協定
3	異質性(Hetreogeneity)	擁有整合多個異質網路通訊、運算、存取的能力
4	原生切片(Native Slicing)	在單一基礎設施中可輕易且有效執行各種網路服務
5	明確的網路與服務命名機制 (Unambiguious naming)	使用者直接連結至內容/服務/功能型主機
6	內部匿名與安全性 (Intrinsic Anonymity Security)	採取終端匿名機制，並加強身分認證，打造值得信賴的網路
7	韌性(Resiliance)	透過控制系統強化基礎設施，用來抵禦天災或駭客攻擊
8	網路確定性 (Network Determinism)	精準地提供符合該網路需求之功能與維運設備

資料來源: 本計畫製作

然而當網路結構改變、效能與規模擴大提升的同時，仍需保持各類型的應用服務層保持資訊安全的敏感度。原因在於，未來技術缺陷或網路攻擊所導致資訊安全風險與經濟損失，因網路效能或規模的擴張，將會導致較以往更為嚴重、涉及層面更為廣泛的影響；新型態應用服務使得資訊攻擊的本質已經超越對既有網際網路進行弱點掃描等脆弱性（Vulnerabilities）檢視的層次。尤其在新網路架構下，「關鍵基礎設施」的定義也將隨之改變，不再僅指特定的產業領域或設施，而是隨著資通訊服務的重要性而呈現動態性，故而其資訊安全的防護較以往顯得更為至關重要。

故 FG-Net-2030 在建立異質網路通訊架構、擴大網路服務型態的同時，也提高在既有內部匿名與安全性（Intrinsic Anonymity Security）、韌性（Resilience）的資訊安全需求（如表 3-1）。詳述如下：

1. 匿名安全性：未來網路打造的終端可具有不被其他通訊端所識別的特性。網路的營運與數據及服務傳遞密不可分，在網路營運上，必須考量網路服務的匿名性，以及對基礎設施提高保護層級，以確保網路中各種數據傳遞的安全性。在眾多網路接取介面暴露於公眾網路的情況下，需根本性建構安全的網路架構，才能解決既有如惡意攻擊、機敏資料於傳輸中繼（intermediaries）被攔截的資訊安全問題，對於終端裝置的身分識別、網路安全、網路平臺安全、資料保護、和商業安全保證作一系統性的信任保證。
2. 韌性：強化網路拓樸（Topology）及網路佈局的架構，以全面性的強化網路韌性。各類型用來監控、自動化的關鍵基礎設施，例如監控與數據採集系統（Supervisory Control and Data Acquisition, SCDA）、工業控制系統（Industrial Control Systems, ICS），因其被利用於核能、水利、油管等關鍵能源網路，除需抵抗天災導致的電力短缺、系統負載與人為疏失之外，還需額外加強網路控制層與管理層的韌性，以防範更趨多樣化的網

路攻擊。

循此脈絡，本計畫將下世代網路的資安需求概分為二。

首先是多接取邊緣運算（Multi-access Edge Computing, MEC）的形成。隨著B5G/6G行動通訊技術與固網的介接技術更加成熟，AR/VR通訊、超清（Ultra HD）內容傳輸需求大量產生，網路邊緣（Edge）的資料處理需求大增，將使 MEC 此種具智慧性、能協同作業與共享的基礎設施應用情境漸趨普及；然而，網路邊緣的安全設計畢竟不如網路核心（Core）完整。

另一方面，則是網路的「路由與定址」更加的複雜化。未來智慧化的邊緣網路，將會面臨不同網路層的通訊協定整合，此時將會更依賴於完善的路由與定址設計，以使不同層級網路能快速進行資料交換與傳輸，網路整合也因此更加的異質化。當網路切片技術已能切分出非公眾網路（Non-public Networks）與公眾網路，同質網路的單一切片、同質網路的切片與切片之間、異質網路的切片與切片之間，就存在關於「網路對接與網路互連」、「IoT 設備號碼識別」與「通訊模組重新設計」等潛在的資安議題。

基此，本計畫由多接取邊緣網路（MEC），以及複雜化的路由與定址兩方面，分別深入說明。

(一) 多接取邊緣網路的資安需求

現今接取與邊緣網路運作已有能力支援區域資料分流（Traffic Steering）等區域網路導流（Local Internet Breakout）與區域性娛樂內容的流量分流。由於使用者在關鍵服務上仍需仰賴電信服務，以及訂閱多重的接取科技服務，未來的邊緣網路將支應以服務與使用者資訊（User Profile）導向的優化接取技術。

為創造高度獨立性的邊緣網路，安全性與低延遲、時脈抖動（Jitter）[58]等網路品質指標考量同等重要。從通訊傳輸架構觀之，

[58] 時脈抖動根據 ITU 定義為「信號在轉態時，相對其理想位置的偏移量」。抖動問題通常自內部產生或外部傳入之雜訊。抖動可分為週期性(period jitter)、週期對週期(cycle to cycle jitter)、長期性

在前端（Fronthaul）會由分布單元（Distributed Unit, DU）或任何相似的元件進行資料處理，加強型的邊緣運算可能安置於此處的通訊節點，建置組合非常仰賴運作情境與網路設備；舉例而言，現今使用者可以選擇使用固網或行動通訊，邊緣運算可能直接作用在無線通訊的終端裝置（參考圖 3-1）。而回程網路（Backhaul）資料中心與中央單元（Centralized Unit, CU）的中繼（Midhual）也會成為網路功能與運算性能強化之處（參考圖 3- 2）。

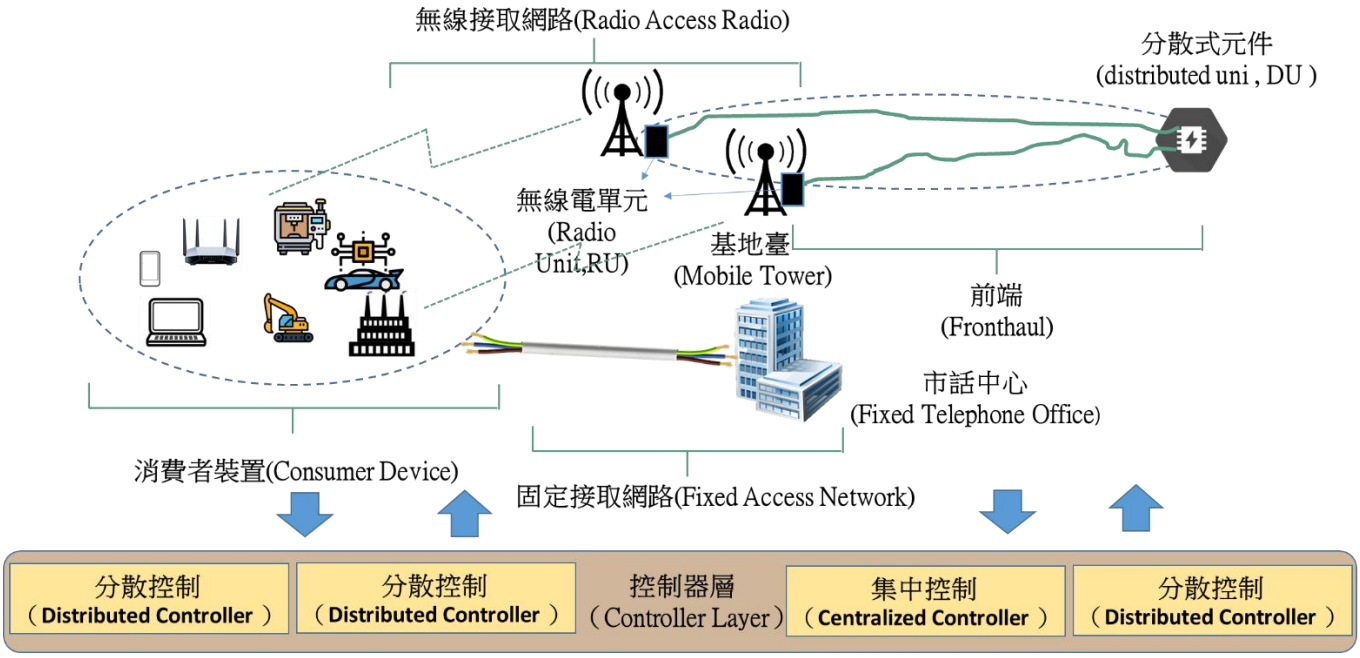


圖 3- 1、使用者服務與前端

資料來源：ITU

(long –term jitter)時脈，不同的應用重視的抖動類型不同。簡言之，IP 網路中若封包大達目的地時間不一，就會產生時脈抖動，對時脈抖動的敏感度會影響即時性訊務品質。

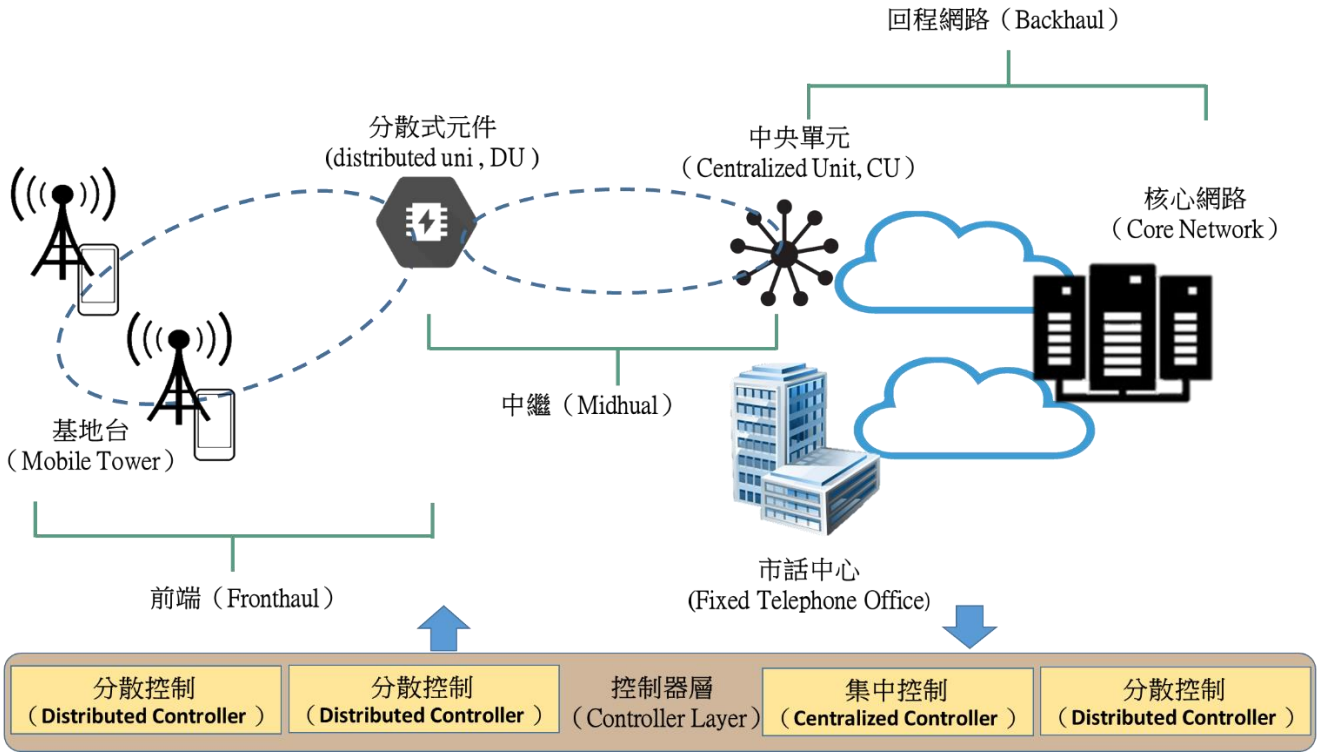


圖 3- 2、前端、中繼、回程網路

資料來源：ITU

在介接邊緣接取網路層中的控制器層（Controller Layer）也扮演主機（Host）的角色，需提供一致的控制器性能支應基礎網路。屆時，邊緣交互工作（Edge inter-working）可能是作為邊緣運算節點或企業網路垂直整合的解決方案，如何成功傳輸客製化的資通訊服務將為首要任務。當來自固網與行網的邊緣網路，是與不同利害關係人進行邊緣交互工作時，資安需求就必須從資料面、整合面，管理面作通盤考量。

另一方面，當切片技術可以將邊緣網路切分成各種應用情境，形成內網邊緣運算子集（Edge Clusters），裝置本身可以短暫提供分層的特定服務，進而產生多重接取、多重技術應用（Multi-Technology）、多重所有權的情況。當邊緣節點以及基礎設施由私人網路擁有者所提供，產生諸如企業用、娛樂用網路設備、日常使用的家用連網設備、加上公共網路等 ManyNets 彼此連網的情境。

在此情境架構下，支援資訊安全等級較高的複合服務（Contextual Service）的邊緣接取基站（或為硬體、或為虛擬化），更需具有提供隨需服務（on-Demand）的網路性能。

從通訊協定與介面角度觀之，強化接取網路運算意味著各層服務的通訊識別需仰賴一命名基礎層（Name-based Layer），賦予命名基礎層為已命名之服務交換（Named-service Transaction, NST）任務，用以識別各個服務層，其中服務主機（Service Hosts）用來識別該服務切片（Service Instances）；硬體設備/服務則需透過代理裝置（Proxy Devices）整合，而命名基礎層在傳輸層（Transport Substrate）上運作，傳輸層執行封包的前向路徑通訊協定（Path-based Forwarding Protocol），該路徑資訊被儲存於快取，且需持續維持/更新路徑，以具備韌性，並能夠適應服務層指令改變的彈性。

在訊息服務（Messaging Services）、資料流設定（Flow Setup）上，新型態的多播（Multicast Messaging）、群播（Group Messaging），需有預防偽造、假訊息機制，並預防伺服器遭受資安威脅，例如避免被駭客獲取（Compromise）具識別功能的伺服器，使其加入不受歡迎的接收帳號；抑或是在應用層（Application layer）強化應用程式介面（Application Programming Interface, API）[59]的安全性，確保服務的呼叫是來自已認證之使用者。或於傳輸需高度資安層防護的資料時，在網路流量入口（Ingress Point）作切分，以便兼顧高流量、低延遲及安全的網路性能。

基此，接取與邊緣網路有許多容易產生資安疑慮與洩漏隱私的環節，在未來網路拓樸與機敏資料傳輸上需具特定資安防護措施，並且將新形態使用情境納入考量。然而，各個國家均具有不同的資安與隱私架構、且MEC服務供應商所能提供的服務類型均

[59] API為系統、跨系統間溝通的介面，該介面可以呼叫或請求應用程式執行指令。

有差異，同樣的挑戰也落在國際電信業者身上，經營跨域網路的國際電信業者也必須了解區域性的網路規範來彌補其不足。

(二) 路由與定址（Routing and addressing）的複雜化

路由通訊協定是網路提供更好的服務的基礎。未來網路在跨網域（Domain）的需求須達到降低營運成本/改善管理環境、提高安全性的同時，增加規模與穩定性、以及更快速的匯流（Convergence）、並具備應用知覺（Application Aware Routing），來辨認來自不同應用軟體的資料流。路由應用知覺（Application-aware Routing）是用來監控各網路層隧道與邊緣路由器來蒐集資訊，並運算出最佳封包傳輸路徑。以往流量判斷、路徑選擇兩個功能分別由路由通訊協定、以及路由協定的演算法（Routing Protocols Algorithm）中與所含的目標位址資訊的位元組決定（Accommodation）。路由應用知覺藉由分析傳輸時的封包遺失、延遲率與時脈抖動，與深度封包偵查引擎（Deep Packet Inspection Engine）偕同運作，達到特定應用網路的需求[60]。

未來網路將面臨路徑與拓樸政策（Path and Topology Policies）指標、可預測的路徑選擇（Predictive Routing）、專門處理域名的路由通訊協定與演算法（Domain-Specific Routing Protocols and Algorithms）、工業網路與物聯網（Industrial Internet and Internet of Things）、多網路由與太空路由（Manynets and Routing in Space）等多元的網路路由效能目標。然而，為達到不同的效能需求，要架構一個既符合最佳路徑選擇、又具備安全性的網路拓樸著實充滿挑戰，例如遭受路由劫持（Route-hijacking）、拒絕服務（Denial-of-service）等攻擊，不同網路型態設定與路由安全性是眾多學者討論的議題。Hollick（2015）等學者更將確保通訊協定的安全性視為「路由安全」的內涵。

[60] Cisco SD-WAN and Cloud Networking, “Cisco SD-WAN: Application Aware Routing”, available at https://www.youtube.com/watch?v=KR4jqWmcRTk.

路由安全具體落實於資訊部門對身分識別、網路路徑選擇、網路拓樸、資訊傳輸等一般性服務，涉及到不同類型之資訊資源、性能的安全保護。

相較於跨網域路徑選擇的安全設定（inter-domain Routing），內部網路路由通訊協定（Intra-domain Routing Protocol）是被大量忽略的一環，原因在於內部網路被視為一單一控制且具良好控制的環境。現有的內部網路路由通訊協定下其實容易招致可用性（Availability）、拒絕服務（Denial-of-service）、流量誤導（Traffic Redirection）等攻擊。解決途徑為在鏈結狀態（Link-state）加上加密簽證（Cryptographic Signature），加密方式與在開放式最短路徑優先（Open Shortest Path First, OSPF）相同。這是在單一網域的環境下的解決途徑，由網路管理員（Administer） 建立加密金鑰認證，分配給裝置與系統的問題相對能夠簡化作業。不過，考量到越來越多 host 主機/物聯裝置存於未來網路，路由協定中的內部閘道協定（Interior Gateway Protocols, IGPs）在未來是提供不中斷服務（non-disrupted service）的關鍵通訊協定。

不過既有的跨網域路由（Inter-Domain Routing）依然面臨資安挑戰。舉例而言，已發展超過20年的邊界閘道器通訊協定（Border Gateway Protocol, BGP），經歷過安全邊界閘道器通訊協定（Secure Border Gateway Protocol, S-BGP）、邊界閘道器協定安全擴充（Border Gateway Protocol Security, BGPSEC）等 4 個版本已存在既有的運作限制，包括規模化能力相較 BGP 來得低、持續更新認證與路由軟硬體更新導致維運不易、受到如 AS 路徑選擇（AS path alternation）等網管政策的中斷，或無法因應新形態的網路攻擊。目前在 S-BGP 協定下將網管工具在資源公開金鑰基礎設施（Resource Public Key Infrastructure, R-PKI）上，提供前置字串（Prefix）和 AS 認證機制；然而在 R-PKI 本身的認證機制仍介接（Fetch）一個 R-PKI 資料庫伺服器，與此同時，R-PKI 本身亦存在

因惡意攻擊導致錯誤授權，無法正確傳遞位址等資安弱點。

於網路安全管理（Security Management）層面，管理範圍應同時涵蓋網路與應用服務、服務相關資料流流入/途經維運者的接取點控制（Access Control），管理層面應具備使用者/服務認證、支援授權使用者進行多種類型的 API 存取控制。管理工具應包括加密技術與金鑰管理、預防未經授權之使用者進行數據竄改或刪除。資訊安全管理須包含相應之策略，例如：濾除（Filtering）特定資料流以降低資安威脅與攻擊之可能風險。

綜上所述，在檢視網路拓樸、多邊緣接取網路中的重要節點、資料傳輸與通訊協定層的問題，歸納新型態網路待解決的資安議題在於，該如何建立異質網路的信任關係。網路科技的歧異性創造出 ManyNets、多重接取串連的網路環境，分散式阻斷攻擊（Distributed Denial of Service, DDoS）將來自基礎網路層、應用層。如何透過正規認證機制，還能兼顧低延遲保證與資訊安全防護需求，將增加通訊協定的複雜性；在物聯裝置充斥、多種裝置接取的環境下，若缺乏規模化的密碼認證機制，也隱藏著潛在的資安風險。

Network 2030 為網路安全、隱私與信任設定目標，並列舉出相應的資訊安全需求，以及達成安全與信任的可能途徑。其所設定的資訊安全目標包括：

- 加強信任模型（Improved trust model）
- 符合經濟與規模化之自主系統與 Host 主機層級資訊認證機制（Autonomous systems and host-level information）
- 針對隱私與資料可信度（Source accountability）的權衡
- 網路前饋路徑（Forwarding paths）的透明度與控制
- 提升密碼演算敏捷度（Algorithm agility）
- 不同應用與資料傳輸面臨的資訊安全等級差異
- 終端通訊機密性
- 不信任的網路節點識別訊息來源的問題等

然而，我們由 2019 年新冠疫情爆發起之影響可觀察到，整體社會的實體活動降低，線上經濟活動持續活躍至今，流量穩定的網路與穩定的連線品質、速度已初步面臨考驗。由於網路流量大增，意味著數據傳輸量也大幅成長，在維持網路性能的同時，仍須兼顧網路與資訊安全，保護網路安全與資訊安全，只靠一兩項技術並不夠，須整合多種手段，諸如認證體系、加密體系、密鑰分發體系等方可竟全功。

2030 年的網路情境尚未到來，然而我們已經可想像到，未來有增無減的通訊終端以及物聯網的發展，必然使大量的 IP 位址與 DNS 應用於網路中。因此，各種異質網路架構逐步成熟、網速更快、延遲率低、資料流龐大的傳輸狀態，各網路節點該如何呼應此種資安需求？在當前的網路技術中，我們推估，IPv6 位址以及 DNS 的發展將仍持續在未來網路發展中扮演重要角色。

基於上述推論，研究團隊下以 IPv6、DNS 的資訊安全需求進一步探討未來網路情境的資安需求。

二、IPv6 資訊安全需求

Google[61]與 APNIC[62]截至 2021 年 5 月之統計數據顯示，臺灣 IPv6 使用率達 45%以上，目前處在一 IPv4 與 IPv6 網路環境共存之環境。隨著 5G 通訊與物聯網應用發展，物聯網裝置之各種感測器，若要達到 M2M 傳輸能力，則需大量不受數量與連結限制的 IP 位址，基此，在 IPv4 枯竭後，政府、終端使用者、企業及網際網路服務提供者以及營運商積極向 IPv6 過渡與部署，既有 IPv4 之資安風險部分隨之轉移至 IPv6。

與 IPv4 相比，IPv6 在網路保密性、完整性做了改善，且能阻擋針對 IPv4 的資安攻擊。過去 TCP 或 IP 網路存在之基本安全威脅，包括遭

[61] Google IPv6 Statistics, available at https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption (last visited, 2021/5/25).
[62] TWNIC, Taiwan IPv6 Global Ranking: 6, available at https://ipv6now.twnic.tw/ipv6/index.html (last visited, 2021/5/25).

受阻斷攻擊（Denial of Service, DoS）或 DDoS 攻擊、竊聽（eavesdropping）、修改（modification）以及偽造（fabrication）等攻擊，使得政府、企業以及網路服務提供者面臨許多的資安問題。在新一代 IPv6 協定上，IPv6 之最大傳輸單位（Maximum Transmission Unit, MTU）最小值為 1280 個位元組，已經初步降低駭客掃瞄通訊埠（port）偵察漏洞的機率，電腦病毒與蠕蟲（worm）也不易傳播。再者，由於 IPv6 本身位址空間巨大，封包小於 1280 個位元組時將會被丟棄（除非為最後一個封包），將有助於防止封包切割（Fragment）等攻擊。

IPv6 利用 IPSec 提供端對端的安全保證，針對網路安全進行更多強化。 IPSec 是在 IP 表頭後方加上資料封裝加密表頭（Encapsulating Security Payload Header, ESP）與認證表頭（Authentication Header, AH），將接在後方之資料進行加密使之不易破解；封裝完成可對通訊端的驗證與資料加密保護，使通訊兩端得安全的傳遞資訊，若加上與 IPSec 協定中的建立網際網路金鑰交換（Internet Key Exchange, IKE）建構安全環境，降低中間人攻擊（Man-in-the-middle attack, MITM）[63]之風險，避免表頭被中途竄改、或利用封包分片等攻擊行為。

此外，IPv6 位址可聚集（aggregate-able）且具層次化的位址特性，使路由器接入 IPv6 時，得對用戶進行來源位址檢查，使入侵防禦系統（IPS）得以實現入口過濾（ingress filtering）的功能，驗證客戶位址的合法性，使得欲透過欺騙（Spoofing）的攻擊停留於用戶端，而不會持續擴散至主機。

至於主機本身可能遭受的路由攻擊，也會造成被害主機無法正常將封包傳送到目的地，或導致傳送至錯誤的目的地。IPv6 亦可啟動存取控制清單（Access Control List, ACL）、防火牆防護，進一步以 IPsec 預防路由攻擊，或透過資源公開金鑰基礎設施（R-PKI）做為系統基礎，有助於抵禦網路上的身分偽裝與位址欺騙。若進一步採用 DNS 安全擴

[63] 為一種駭客從中接收兩端通訊內容，亦能從中插入自己資料的攻擊手法，透過使用 IPSec 可降低被攻擊的機會。

展（DNS Security Extensions, DNSSEC）協定，則可防禦新的 DNS 攻擊。

據臺灣網路資訊中心報告[64]指出，使用 IPv6 在資安方面仍有需要強化的之處。一是 IPv6 雖然已能抵禦 IPv4 攻擊，然而 IPv4 網路與 IPv6 網路介接的方式與類型，也可能會成為資安的弱點，像是 IPv6 可接取同時具備兩種協定的區域網路，將擴大非法接取之範圍，或透過 IPv4 與 IPv6 建構的隧道（tunnel）針對 IPv4 相關網路設備展開惡意攻擊。

其次是 IPv6 網管設備與網管軟體、資安產品成熟度。目前需針對 IPv4 的網管設備與軟體再作安全性升級，IPv6 的網管設備與軟體對 IPv6 的支援性亦需提高，以提高網路監測管理、大範圍定位網路故障、網路性能監控的有效機制，資安產品方面，IPv6 於虛擬私人網路（Virtual Personal Network, VPN）、入侵檢測系統（Intrusion-detection system, IDS）、漏洞掃描、防病毒閘道器、防火牆等既有的產品，須考量到 IPv6 的特性，例如防火牆進行封包過濾時，須辨識與處理移動性（mobility）、封包分割之訊息來源[65]等可能會有資安漏洞之處。

此外，IPv6 可能面臨不同層級資源同時消耗等資訊安全挑戰。隨著 IPv6 協定提升不少安全性，但常見之病毒、蠕蟲等網路攻擊皆存於應用層，而非 IP 層。換言之，若網路攻擊和威脅大都來自應用層，IP 協定位於網路層，IPv6 並無法直接消除應用層的攻擊行為，僅可能因為 IPv6 具備較高之安全性，而減緩攻擊擴散之速度與擴散範圍，若遇到量能強大的泛洪攻擊（flooding）或放大攻擊（amplification），將必須強化主機（Host）與網路設備之安全檢查與防護，以避面伺服器耗盡所有資源導致癱瘓、駭客趁機非法接取，或導致網路壅塞，使目標伺服器無法提供服務。

誠如上述之 IPv4、IPv6 網路環境說明，並不能如以往單就 TCP/IP 網路層角度觀之，亦須考慮來自應用層，諸多新興資通訊科技應用於

[64] 財團法人臺灣網路資訊中心，〈Native IPv6 連網環境建置及 IPv6 用戶安全防護研析〉，2020。
[65] 為降低路由器負擔，IPv6 封包分割的工作只在起來源主機執行，如果電腦傳送超過最大傳輸單位大小的封包，路由器會將收到的封包丟棄，回傳 ICMPv6 回應封包，並透過這個封包告知該來源主機。

商業、社群領域衍生出的資安疑慮。舉例而言，線上會議軟體 Zoom、語音社群軟體 Clubhouse 的竄起，曾引發用戶個人資料使用授權不完善、封包攔截分析流量、竊取帳號或進階持續性威脅（Advanced Persistent Threat, APT）資料等疑慮；此外未來企業內網、私人網路逐漸興盛當下，內部網路的拓樸與資安亦須與連外網路架構同步檢視 IPv4 與 IPv6 轉換（transition）至純 IPv6 環境時應用場景的資安需求。

(一) IPv6 轉換的資安需求與應用場景

IETF 於 2020 年發布 RFC-7381 文件[66]，以 IPv6 觀點出發，提供 IPv6 轉換（transition）的階段性途徑（Phased Approach），從系統、資安政策、資產的準備評估、到外部階段、內部階段需重視的資安環節，並針對特殊企業，如內容傳遞網路（Content Delivery Networks, CDN）、虛擬資料中心（Data Center Virtualization）、校園網路（University Campus Network）等特殊網路的資安需求。

ETSI 也於 2020 年度發布白皮書「IPv6 最佳實務、優勢與未來轉換挑戰（IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward）[67]。開宗明義即說明優先採用 IPv6 的重要性。目前 IPv6 轉換的解決方案包括行動寬頻（Mobile BroadBand, MBB）、固網寬頻（Fixed BroadBand, FBB）以及企業服務均蓄勢待發；已有 464XLAT[68]與 Dual stack Lite (DS-Lite)提供給純 IPv6（IPv6-only）服務環境。而在車聯網、智慧電網（smart grid）、

[66] IETF, Enterprise IPv6 Deployment Guidelines, available at https://tools.ietf.org/html/rfc7381（Late visited: May,26,2021）

[67] ETSI, IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward , available at https://www.etsi.org/images/files/ETSIWhitePapers/etsi_WP35_IPv6_Best_Practices_Benefits_Transition_Challenges_and_the_Way_Forward.pdf (Late visited, May, 26,2021)

[68] 464XLAT 為解決 IPv4 與 IPv6 不相容網路之間互通性問題的關鍵技術之一，一般在客戶端轉換器(customer-side translator, CLAT)和伺服器端轉換器(provider-side translator, ,PLAT)上執行。464XLAT 提供 IPv4-CLAT-IPv6-PLAT-IPv4 的應用情境，可使裝置及應用程式的運作維持透通性，用於 IPv4 與 IPv6 通訊轉換。詳見〈TWNIC IPv6 之 NAT64 464XLAT 技術介紹〉，12/29，2020，＜https://blog.twnic.tw/2020/12/29/16531/＞。

乃至工業聯網的垂直應用、以及雲端運算等需要規模化（in scale）的服務採用上，能讓 ISP、網路營運商、供應鏈利害關係人均受惠於純 IPv6 的網路環境。

(二) 2021 年 IPv6 的資安議題

IETF 亦持續針對 IPv6 駭客（IPv6-Hackers）、IPv6 營運（IPv6-OPS）的資安議題論壇與工作小組，透過意見投稿與詢問的詢問清單（Mailing List）與討論清單（Discussion List），積極發展 IPv6 網路安全的依循指導原則。IPv6-OPS 於 2021 年已收到針對用戶 IPv6 重新編號（Renumbering）對邊緣伺服器（Edge Routers）的重新強化、IPv6 部署狀態、IPv6 封包延展表頭（Extension Headers）、IPv6 對 IPv4aaS（IPv4 as a Service）的轉換技術等的意見待審核，如圖 3-3，可略窺未來 IPv6 之資安議題走向。

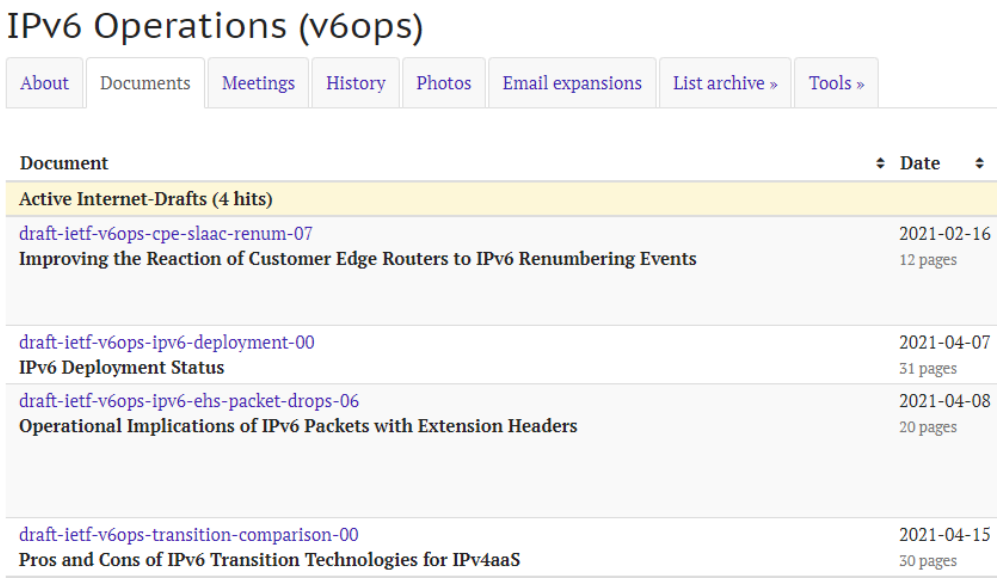


圖 3- 3、V6OPS 工作小組目審核之草稿文件

資料來源：V6OPS

三、DNS 資訊安全需求

電信號碼、IP 位址以及網域名稱等機制的主要功能，係在電信網路或是網際網路中識別、定位通訊對象，並與之建立連線。尤其在 5G

的發展中，物聯網（IoT）技術崛起，大幅擴展網路連接設備的數量，包含感測器等不具運算能力的資通訊設備連結至網路，大量增加的物聯網裝置對網路安全造成沈重的壓力。為了強化下世代電信網路之資安管理，網路編碼機制在物聯網技術發展下，既扮演建立網路連線的角色，也同時需肩負裝置認證與管理的任務。因此，電信號碼機制的安全性，與物聯網安全息息相關。目前各種下世代電信網路號碼機制的討論中，係以網域名稱服務（DNS）為主要。

DNS 為網域名稱系統（Domain Name System, DNS），透過將網路位址（IP）轉換為網域名稱（DN），可謂網際網路世界重要的一項基礎建設與第一道關卡，由於 DNS 原本承擔的任務相當簡單，故其原始的通訊安全性較低。在網路規模擴大、各項網路服務越加多元性後，DNS 也面臨許多的安全威脅。

首先，DNS 通訊協定的原始設計重視效率，因此在 DNS 查詢時近端的伺服器會將 DNS 查詢結果暫存於快取（cache）中，以利使用者再次查詢時可快速回應；然而，快取機制可能受到偽造的資料改寫，此時在技術上便以 DNS 安全擴展（DNSSEC）加以因應，透過數位簽章的機制驗證 DNS 來源的合法性。

另外則是 DNS 查詢時，係將網域名稱傳送至 DNS 伺服器，但在傳送過程中資訊可能遭到攔截而洩漏，此時則利用加密機制保護資料。

另一方面，由於 DNS 服務掌握了資通訊設備連網的關卡，因此若 DNS 服務系統被入侵，或是 DNS 服務遭到 DDoS 攻擊，就會影響到資通訊設備連網的能力，進而造成網路功能的癱瘓；此時則透過 DNSSEC 加強 DNS 通訊的安全性，或是利用 DDoS 的減緩服務，阻擋 DDoS 癱瘓網路。上述 DNS 資安威脅及改善技術初步整理如表 3-2：

表 3- 2、系統資安威脅及改善技術

攻擊來源	攻擊類型	威脅減輕
DNS 協定（Protocol）	DNS 快取（cache）中毒（poisoning）	DNS 安全擴展（DNSSEC）
	隱私保障不足	DNS-over-HTTPS（DoH）和 DNS-over-TLS（DoT）等數位認證（digital certificates）機制
DNS 服務	DNS 劫持（hijacking）	DNS 安全擴展（DNSSEC）
	分散式阻斷服務（DDoS）	DDoS 減緩（mitigation）服務

資料來源：CircleID

進一步言之，當 DNS 加上安全防護後，如同手機的來電過濾功能，一旦透過資料比對以及安全認證等防護關卡，即可於第一時間保護使用者與詐騙網站連結，並藉由過濾惡意連結，確保重要資訊安全無虞[69]。

DNS 技術一開始出於資訊安全問題不顯著的年代，然而隨著網際網路技術的蓬勃發展與日新月異，DNS 遭遇的資安議題便漸漸浮上檯面。例如，由於 DNS 的查詢與回應並未經加密，若經駭客從中假造 DNS 封包，將使用者與要連結的網址相連，將致使錯誤回應之 IP 被導向駭客端，進而讓使用者的帳號密碼被駭客竊取[70]。

透過 DNSSEC 的防護，可減少資安漏洞的產生。DNSSEC 可以針對 DNS 主機之間的資料傳遞，加以驗證來源與資訊內容的可信度，防

[69]科技新報，〈網路安全的第一道防線，就從 DNS 防護做起〉，8/06，2020，<https://technews.tw/2020/08/06/infoblox-dns-security/>

[70]國立臺灣大學計算機及資訊網路中心電子報，〈DNSSC 安全計設簡介〉，9/20，2012，<https://www.cc.ntu.edu.tw/chinese/epaper/0022/20120920_2206.html >

止例如 DNS 快取中毒（DNS Cache Poisoning ）、中間人攻擊（MITM）、DNS 綁架（DNS Hijacking）、DNS 嫁接/釣魚假冒（DNS Pharming）等[71]。

DNSSEC 優點在於可完全兼容於現行 DNS，並提供另外三項資訊安全，包括資料完整性（data integrity）、來源可驗證性（origin authentication of DNS data）、可驗證之不存在性（authenticated denial of existence）[72]。

上述三項功能主要採用雜湊函式（Hash Function）與公開金鑰加密（Public-key cryptography） 之技術。雜湊函式為將資料壓縮成一組驗證值（Hash Value），使資料量變小且固定。雜湊函式是多對一的（失真的）映射，故無法由其輸出值計算出原本的輸入訊息。意即，由於是多對一的方式，故存在許多訊息其映射值為相同[73]上述三項功能主要採用雜湊函式（Hash Function）與公開金鑰加密（Public-key cryptography） 之技術。雜湊函式為將資料壓縮成一組驗證值（Hash Value），使資料量變小且固定。雜湊函式是多對一的（失真的）映射，故無法由其輸出值計算出原本的輸入訊息。意即，由於是多對一的方式，故存在許多訊息其映射值為相同[74]。

公開金鑰加密（下稱公鑰加密）又稱為非對稱式（asymmetric）加密，其特點為將加密及解密時須使用兩組成對的鍵值（鑰匙），將其中的一組鍵值稱為私有鑰匙（Private Key），由個人妥善保管。而另一組則稱為公眾鑰匙（Public Key），公佈大眾提供下載。意即，當大眾中某人 A 欲傳送資料給某人 B 時，A 可先將資料以 B 的公眾鑰匙加密之後再傳給 B，B 收到後再以其私有鑰匙解密，因為 B 的公眾鑰匙眾所皆知，因此眾人皆可以它加密後傳送給 B，而僅 B 持有私有鑰匙，因此任

[71] 資安人，〈DNS 安全防護傘-DNSSEC〉，9/06，2010，<https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=5886>

[72] 國立臺灣大學計算機及資訊網路中心電子報，〈DNSSC 安全計設簡介〉，9/20，2012，<https://www.cc.ntu.edu.tw/chinese/epaper/0022/20120920_2206.html >

[73] 同前註。

[74] 同前註。

何第三方皆無法讀取 B 的資料[75]。

常見的公鑰加密的應用是數位簽章，例如對於資料完整性，DNSSEC 可運用數位簽章技術，將每筆資源紀錄（Resource Record, RR）做簽章產生資源紀錄簽章（Resource Record Signature, RRSIG），而收到資料可透過「Public Key + RRSIG」驗證是否為原本詢問 RR 紀錄，以此驗證是否中間有被竄改。這把 Public Key 在 DNSSEC 中又稱為 DNSKEY；對於來源可驗證性，當資料完整性被驗證後，已可確認資料未被竄改，且由負責該域之 DNS 伺服器提供，但透過何種方式驗證該域（domain）之 DNS 伺服器確實是非駭客自行架設的 DNS 伺服器？因此，在個人數位簽章中，通常需將個人 Public Key 交由公正第三方驗證，驗證 Public Key 確實代表該個人。而從 DNSSEC 而論，公正第三方即上層 DNS 域名伺服器（Domain DNS Server），意即 DNS 伺服器必須將自己的 DNSKEY ，做一次數位簽章後放入母域伺服器（Parent Zone Server）；這種新的 RR 類型稱為 DS（Delegation Signer），藉由母域中的 DS 紀錄，可驗證子域（Child Zone）中的 DNSKEY 確實正確且未經竄改；對於可驗證之不存在性，DNSSEC 將所有 DNS 紀錄依照字母排序，並在每個網址間加上一筆安全紀錄稱作 Next Secure（NSEC）並做為電子簽章。換句話說，當查詢到不存在網址時，DNSSEC 會回應 NSEC 紀錄，而查詢者可比對 NSEC 紀錄中前後對應的字母，以確認是否真的不存在[76]。

簡言之，DNSSEC 的運作是利用數位簽章達成驗證的目的，並同時輔以公鑰密碼學的機制，對於互相溝通的不同 DNS 主機間，以單向雜湊函數來檢視訊息內容，並生成一組雜湊值。管理者再透過私鑰將驗證訊息與雜湊值加密，製作成數位簽章。而當 DNS 接收端接收到訊息時，需先將數位簽章進行解密，然後再藉由雜湊值確認訊息內容是否未受竄改。因此，DNSSEC 可藉數位簽章的簽署與驗證過程，強化

[75] 同前註。
[76] 同前註。

DNS 不被假冒的可能性。

雖然 DNSSEC 的建立可降低資安漏洞產生的風險，但卻仍有 2 個主要限制，包括隱密性（Confidentiality）以及服務可用性（Availability）。例如隱密性，DNSSEC 傳遞的 RR 及 RRSIG 傳輸過程皆未經加密，因此中間將可能被封包偵測（sniffer）之設備或程式讀取。但被讀取不代表能假造，因為駭客並無 DNS 伺服器 之 Private Key，因此無法假造出 RRSIG 的資料而不被發覺；在服務可用性上，DNSSEC 僅為一項服務，若有駭客發動 DDoS 攻擊，不斷的詢問成千上萬個網址，則 DNS Server 可能因負荷過重而無法正常運作。但這項弱點應是所有網路服務皆共有的現象，而不僅只是 DNSSEC 的弱點[77]。

另外，由於 DNS 的設計始中存在「最後一哩」的問題，即 DNS 的客戶端與本地端 DNS 伺服器間之通訊長久以來透過明碼（即未加密）傳輸方式，因此容易遭受假冒攻擊（spoofing）、攔截或是其他干擾。有鑑於此，網際網路工程任務組（IETF）提出了二種機制解決 DNS 最後一哩路之問題，包括 DNS over TLS（DOT）與 DNS over HTTPS（DOH）。進一步言之，當 DNSSEC 對 DNS 加入身份驗證與數據完整性的檢查機制時，一般而言 DNS 客戶端的安全性會被忽略，因此本地端的 DNS 伺服器會執行 DNSSEC 的驗證，並建立其數據資料的真實性與完整性，最後將結果傳送給 DNS 客戶端，但卻將可能遭受到假冒的攻擊[78]。

因此，上述兩種機制可對於 DNS 客戶端與本地端 DNS 伺服器間加密，以及對數據的機密性以及完整性進行加密，使 DNS 客戶端可選擇使用任一協議對 DNS 伺服器進行驗證[79]。

DOT 為透過傳輸層安全協議（Transport Layer Security, TLS）對 DNS 進行加密。此協議主要目地為防止中間人對於 DNS 數據進行攻擊

[77] 同前註。
[78] 創泓科技，〈DNS 資訊安全防護的最後一哩路〉，
<https://www.uniforce.com.tw/edcontent_d.php?lang=tw&tb=1&id=217>
[79] 同前註。

與控制，以保護數據與隱私，使 DOT 可作為防範駭客透過中間人攻擊，對 DNS 數據進行監聽或操控的防範模式。DOH 為一個對 DNS 解析進行安全化功能的方式，主要目的為以加密的 HTTPS 協定進行 DNS 解析請求，以避免原始 DNS 協定之用戶的 DNS 解析請求遭竊聽或是修改（例如中間人攻擊），以保護用戶隱私[80]。

然而，即使技術上開發出各種安全增強的方案，但由於 DNS 機制是各種裝置連網的基礎，為了降低網路延遲，讓使用者能快速連上網路，DNS 運作原則上重視效率；若在 DNS 通訊協定上附加安全性要求，雖可增進 DNS 機制安全，但卻可能大幅度降低 DNS 運作的效率。網際網路上本已存在各式各樣的資安威脅，在下世代電信網路的各種新興應用下，由於連網裝置的數量大增，網路資安威脅只會更加嚴重，加諸物聯網本身的資安需求，DNS 機制已經面臨必須大幅強化其資安防護能力的狀況。

(一) 5G 發展下 DNS 的資訊安全需求

在上述 DNS 機制的資安威脅下，下世代電信網路的應用受其影響，各網路層級也面臨不同型態的資安威脅，分別為：

1. 裝置安全影響

在下世代電信網路新興應用場景中，物聯網應用的裝置系統結構相對於其他類型的資通訊設備而言較為單純，同時，物聯網裝置的預設運作期間相當長，可能達 5～10 年以上，因此裝置本身在漏洞的修補與系統升級上，均受到相當大的限制。而物聯網裝置目前亦仰賴 DNS 機制連上網路，若裝置內的 DNS 參數被改寫，或是 DNS 暫存（cache）機制受到入侵，則當裝置對外連線時，便可能因連線錯誤而將資訊傳送至錯誤的目的地，或是裝置流量被導引至不正當的用途，如 DDoS 攻擊。

2. 通訊安全影響

[80] Semisphere，〈[資安] DNS over HTTPS(DoH)與 DNS over TLS(DoT) 〉，6/29，2019，<https://firsemisphere.blogspot.com/2019/06/dns-over-httpsdohdns-over-tlsdot.html>

如前所述，由於初始的 DNS 通訊協定重視效率，因此相較於其他網路層級的通訊協定，欠缺安全性的設計，在裝置進行 DNS 查詢時，便可能洩漏裝置相關的資訊，影響網路通訊的安全。在 DNS 的架構上，越是低層級的查詢，傳送出去的資訊越多，若 DNS 連線並未附加安全機制，或加密，則資訊洩漏的風險也提高。因此，DNS 通訊協定本身的安全性也需要予以加強。

3. 網路安全影響

在下世代電信網路的編碼機制中，除了讓各種網路裝置查詢連線對象的所在位址，編碼系統本身還可以成為網路裝置的識別管理機制。由於各種網路裝置帶有名稱，同時亦為外界連線的對象，編碼管理機制此時則可對內管理裝置，避免未經認證、不帶有識別名稱（ID）的裝置在網路內運作，或是透過 DNS 機制對外連線，從而維護新興電信網路的安全性，避免偽造的、未經許可的裝置在網路中活動，提高網路的安全性。

而另一方面，當內部資通訊設備向外部連線時，也須向號碼管理機制查詢連線對象的網路位址，此時便可透過號碼管理機制加以限制，當資通訊設備查詢不合法的名稱時，除可限制設備連線，亦可由管理機制中發現可能潛在的網路安全問題。

4. 隱私保護

在新興網路應用的場景中，其連線裝置可能帶有個人的隱私資訊，例如智慧家庭的裝置、車聯網的車輛裝置等，這些裝置本身與使用者的關係相當密切，與使用者生活高度結合，故帶有使用者隱私資訊。因此，尤其在使用者由外向內進行連線時，如何認證使用者的身份，並確保使用者可合法的與裝置通訊，同樣是電信網路編碼系統可加以管理的範疇。

故整體而言，下世代電信網路編碼機制及其管理系統，除承擔網路上的裝置對外連線安全，也需管理由外部向內部連線的需求，並管理網路裝置的識別（ID）、名稱（DN）、位址（IP）與擁

有者（Owner）等資訊之間的相互對應，以確保網路運作的安全性。

由上述的介紹可知，電信號碼機制在新世代網路應用服務的需求下，已不僅扮演協助網路設備連網的角色，更可擔任網路安全的關卡；然而，為了使編碼機制能夠完善的扮演安全關卡，下世代電信號碼機制如 DNS 機制，需從管理面及技術面加以改良，強化其安全性與可靠性，方能發揮保障對內及對外的網路通訊安全。

趨勢科技總經理洪偉淦認為，5G 時代的來臨將明顯改變現有資安防護機制，使防禦方式須轉為更加彈性，並且也面臨更多不同挑戰。5G 架構為軟體定義網路（Software Define Network, SDN），不同於過去以後端設備架構的 4G 網路架構。軟體定義網路無網路實體邊界，因此 5G 世代的網路資安防禦亦須由軟體定義之，即網路功能虛擬化（Network Functions Virtualization, NFV）。過去面對資安威脅，企業會以內網作為公網與內網的隔絕方式。然而，5G 世代開始，網路暴露於公開的無線網路中，因此企業須透過虛擬化方式切出一環境，作為阻隔。

基此，企業採用的防禦技術亦須虛擬化，以軟體定義之方式使網路流量經過虛擬化的入侵防禦系統以及防火牆，5G 於資安所面臨的挑戰包含：建立新的虛擬化技術以及資安防禦加裝後，不可對於 5G「超高速、低延遲、大連接」之網路品質造成影響[81]。

隨著 5G 網路技術的發展，目前亦有許多技術正在推動 HTTP 以及 DNS 的發展，並帶動網際網路架構朝著虛擬化技術快速演進。亦即，NFV 與 MEC 正帶動 5G 網路為 HTTP 以及 DNS 發展創造出新的要求，例如 HTTP 與 DNS 協議的變革。舉例而言，HTTP 需要變得更加精簡和輕量級，以滿足 5G 的高傳輸量（throughput）

[81] 數位時代，〈5G、純網銀上路，資安風險更棘手？4 大資安趨勢老闆需注意〉，12/13，2019，<https://www.bnext.com.tw/article/55909/trendmicro-estimation2020-cybersecurity>

和低延遲要求；對於 DNS，由於未來預計將推出十億個 5G 物聯網設備，因此 DNS 亦將為這些物聯網設備創造關於發現（discovery）以及位址（addressing）之全新的要求，例如 DNS 服務探索（DNS Service Discovery, DNS-SD）的發展，是在裝置彼此群播（multicast）連結情形下，快速發現區域裝置與服務，並適度允許無須人力介入的輕微錯誤校正。[82]

根據全球知名德國科隆 OX 軟體股份有限公司（OX Software GmbH）發行之白皮書「DNS 於 5G 網路新需求」（DNS in a 5G Network New Requirements and Demands）預測，未來 IoT 設備將在 5G 快速發展下爆炸性成長，而自動駕駛汽車、醫療保健以及工業設施等垂直應用市場尤為重要，而 mMTC 和 URLLC 將會持續帶動成長。據預估，2025 年將會有 50 億個物聯網裝置[83]。

由此可推斷下一波的連網設備將不再侷限於電腦與智慧型手機，未來物聯網設備之機器與機器之間的通訊將為常態。5G 網路特性應用於垂直市場，也引起國際對於 DNS 於 5G 網路切片以及物聯網發展的關注。

進一步言之，現今物聯網設備製造商通常使用各自的特有系統對設備進行識別與存取，且該物聯網設備製造商可以選擇採用不同類型的方式作為識別，例如設備的序列號（the serial number of the device）、國際行動裝置辨識碼(International Mobile Equipment Identity，簡稱 IMEI)、MAC 位址（Media Access Control Address）、數據來源認證（data origin authentication）以及其他類型識別碼等。上述方式多做為硬體的識別，且通常可以長期使用。倘若將上述識別碼與設備的擁有者與使用者屬於映對（mapping）關係，長期使用將衍生隱私的問題。

[82] COMPUTERWORLD, "5G AND FUTURE MOBILE" (2017), <https://www.computerworld.com/article/3204594/http-and-dns-in-a-5g-world.html>
[83] Ox software GmbH, " OX Whitepaper DNS in a 5G Network New Requirements and Demands" ,*WHITEPAPER VERSION 1.0*,p.5

為了解決物聯網設備的隱私問題，以 DNS 為基礎的編碼機制與管理為未來較合適的解決方案，並能夠確保不同網路切片與場域的互通。透過 DNS 的編碼機制與管理，將有助於管理物聯網設備，減少既有物聯網設備的資安問題[84]。

關於 DNS 編碼於物聯網的發展趨勢，ICANN 轄下的網路安全及穩定諮詢委員會（Security and Stability Advisory Committee，簡稱 SSAC）於 2019 年 5 月提出的「關於 DNS 以及物聯網的機會、風險與挑戰」（SAC 105 The DNS and the Internet of Things: Opportunities, Risks and Challenges），以及國際電機電子工程師學會（Institute of Electrical and Electronics Engineers，簡稱 IEEE）於 2020 年發布的「DNS 在物聯網的機會、風險與挑戰」（The DNS and IoT: Opportunities, Risks and Challenges），均說明未來 IoT 與 DNS 的關係以及其交互作用，亦凸顯未來國際物聯網設備朝向 DNS 編碼機制為基礎的資安發展趨勢。

關於國際上對於 IoT 與 DNS 的關係與發展之看法，認為物聯網的部署與實體環境間的感應作用，其實並無涵蓋人類的參與以及人類意識，因此將產生對於新的安全、穩定以及透明度的需求，而在此同時長期以來一直為全球通用的網路架構模式下，DNS 可用來實現下世代安全、穩定與透明之網路資安需求要件。例如，在未來智慧家庭的運用中，DNS 編碼的機制可使智慧門鎖僅與特定物聯網設備通訊，而不會隨意接受來路不明的惡意訪問。[85]

進一步言之，如 SAC 105 報告所推測與強調，未來大量物聯網的設備將可能啟用 IP，並將使用 DNS 來定位其執行功能所需的遠端服務。因此，DNS 未來在物聯網將持續扮演重要角色與發揮關鍵作用。而從安全性以及穩定性的角度而論，更凸顯 DNS 角色

[84] *Id*.p.8-9
[85] ICANN Security and Stability Advisory Committee（SSAC）,"The DNS and the Internet of Things: Opportunities, Risks, and Challenges " ,*SAC 105*(2019)p.11

與功能的重要性。[86]

(二) ICANN 對於 DNS 的網路安全評估

現今國際對於 DNS 於 5G 網路切片以及物聯網發展應用之研究，主要以國際組織 ICANN 推動較為積極。針對 DNS 在 5G 網路切片以及物聯網的應用，ICANN 於 2017 年有 DNS 得以作為物聯網編碼的可行性之說明[87]。隨著 5G 網路切片與物聯網的蓬勃發展與應用，5G 網路切片與物聯網的 DNS 編碼，為未來物聯網世界中機器與機器間通訊可能的運作與管理機制。

在 5G 技術與物聯網的快速發展模式下，ICANN 於去（2020）年開始重新審視現有的網路模式，例如網際網路協議（TCP/IP protocol suite）是否仍適用於 5G。因此，ICANN 針對上述的議題提出幾個對於 DNS 的觀點，例如：[88]

- 針對 5G 超高速、低延遲的應用場景，既有的 DNS 是否仍適用於 5G ？
- ICANN 維護的全球網路唯一識別碼系統（unique identifier system）是否仍適用於 5G，抑或是 5G 的問世是否帶來了其他關於識別碼系統的需求？
- 5G 的發展是否仍須使用電話號碼？

另一方面，近年來物聯網牽涉的資安問題層出不窮。若結合 DNS 與電信編碼機制作為物聯裝置之編碼機制，將為 DNS 帶來發展的新機會，同時也對 DNS 既有運作機制帶來風險。於機會部分，DNS 提供之功能與數據有助於讓 IoT 更加安全、穩定和透明，此外 DNS 可以有利於 IoT 設備：[89]

- 對解析器（resolver）進行身分驗證並加密 DNS 流量；

---

[86] *Id*. p.24
[87] 根據 ICANN 首席技術辦公室 （ICANN Office Of the Chief Technology Officer, OCTO，為識別碼研究、運作及安全部門 （Identifier Research, Operations and Security, IROS） 前身）於 2020 年 1 月發佈的「5G Technology 」報告，即有提及。
[88] Alain Durand, "5G Technology",*ICANN Office of the Chief Technology Officer*(2020)p.1-13
[89] *Id*. p.10-13

- 透過 DNSSEC 保護 IoT 設備不受惡意攻擊或威脅
- DNS 協定（DNS protocol）可有助於再次確認（double check）IoT 設備的真實性；
- DNS 可為 IoT 設備提供檢查其連接的服務是否有效的方法，並對註冊服務商提供用於 IoT 部署之其他安全服務的機會；
- 保護 IoT 設備免於域名註冊劫持；
- DNS 查詢機制為終端使用者提供了更佳透明的 IoT 環境；
- 考慮到 IoT 所帶來的安全問題，開發 DNS 安全防護機制與系統，可確保未來 DNS 與物聯網的運作安全。

至於 DNS 的風險，SAC 報告提到物聯網設備可能會對於 DNS 造成三種壓力，進而造成資安風險，包括:[90]

- IoT 級別對於 DNS 不利之 IoT 編程（Programing）：過多的 DNS 查詢，會造成營運商 DNS 解析器緩存增加，大量消耗內存，產生對解析器的 DDoS 攻擊，使營運商無法阻擋流量，同時設備亦正在進行正常查詢，必須等到新版本發布後始得處理。
- IoT 殭屍網路產生 DDoS 的大規模攻擊與增加複雜性：由一組被惡意破壞的物聯網設備組成的 IoT 殭屍網路所產生 DDoS 的大規模攻擊 DNS（以及其他類型的網路基礎結構）、增加其複雜性。
- 公開伺服器的增加：在公開的伺服器大規模增加的情況下，DDoS 可放大公開解析器被錯誤配置接受網路上任何客戶端的 DNS 查詢規模，而非對於其欲服務之客戶端訪問網路。意即，攻擊者可以藉由向打開的解析器發送許多 DNS 請求，並將查詢的源 IP 地址設置為欺騙受害者的 IP 地址，並利用這種錯誤配置。 因此，解析程序會將任何回應發送給受害者而不

[90] *Id*. p.14-17

是攻擊者，從而增加了放大倍數，因為 DNS 回應通常大於 DNS 請求。[91]

此外，為有效推廣 DNS 安全機制應用，ICANN 於 2019 年發布之「ICANN 財務年度 2021-2025 戰略計畫」（ICANN Strategic Plan for Fiscal Years 2021-2025）建議，ICANN 應與社群合作，針對 DNS 的安全及穩定議題，建立一個有效協作的機制。基此，ICANN 於 2020 年 5 月成立 DNS 安全協調技術研究小組（Domain Name System Security Facilitation Initiative Technical Study Group, DSFI-TSG），以探討並促進 ICANN 在「強化 DNS 生態系統中多方利害關係人協作互動、進而加強 DNS 安全」的能力與義務。此小組召集人為 ICANN 安全與穩定諮詢委員會（Security & Stability Advisory Committee, SSAC）駐董事會聯絡人，組內成員背景各異，匯集了 DNS 標準和營運方面的專家，以及具有處理網路犯罪和安全事件、註冊管理機構和受理註冊機構運作以及關鍵基礎設施營運經驗的專家[92]。該小組每雙週召開會議，並定期將討論成果放在 ICANN blog 與小組的網頁（dashboard）上，其討論議題包括事件回報、技術標準、ICANN 政策及既有程序、執行現況，亦確保持有多元觀點。

DSFI-TSG 小組經過一年運作後，於 2021 年 10 月發布了「DNS 安全協調技術研究小組期末報告」（DNS Security Facilitation Initiative Technical Study Group - Final Report）[93]，報告中分別針對憑證洩露（Credential Compromise）、存取控制（Access Controls）、資源假冒攻擊（Resource Impersonation Attacks）、號碼和協定漏洞（Code and Protocol Vulnerabilities）、基

[91] ICANN Security and Stability Advisory Committee（SSAC）,"The DNS and the Internet of Things: Opportunities, Risks, and Challenges " ,*SAC 105*(2019)p.14-17

[92] ICANN, Domain Name System Security Facilitation Initiative Technical Study Group Begins Its Work, July 1, 2020, available at https://www.icann.org/en/blogs/details/domain-name-system-security-facilitation-initiative-technical-study-group-begins-its-work-1-7-2020-en

[93] DSFI-TSG, DNS Security Facilitation Initiative Technical Study Group - Final Report, Oct. 15, 2021, available at https://community.icann.org/display/DSFI/DSFI+TSG+Final+Report

礎設施選擇（Infrastructure Choices）、DNS 作為攻擊向量（DNS as the Attack Vector）以及阻斷攻擊（Denial of Service）等問題，列出各種惡意攻擊事件使用的攻擊向量（attack vector），且確立對應的緩解措施。

在每個類別中，DSFI-TSG 小組側重於 DNS 實際面臨的已知威脅，透過檢視多起 DNS 攻擊事件中常見的攻擊模式，並討論可以防止或減輕這些事件嚴重性的現有緩解措施，報告提供了 12 項建議 ICANN 可以採取的行動，以提高 DNS 的安全性。報告亦指出，雖然 這些建議是針對 ICANN 所提出，但它們需要經由更廣泛的利益相關者共同努力才能實現。此外，小組主要觀察攻擊的機制，而非事件之內容，並且係以變更政策作為建議方向，而不傾向制定新政策。

針對每個攻擊向量，DSFI-TSG 小組透過以下問題進行分析：

- 有哪些既有、可用於促進 DNS 安全的機制或功能？
- 目前 DNS 安全整體狀況中，最重要的落差在哪裡？彌補這些差距需要哪些技術要求？需要發展、調整、推廣或實施哪些可運作的最佳實務（best practices）來彌補差距？部署最佳實務和其他技術措施的障礙是什麼？
- 與這些落差衍生的風險為何？需要注意哪些外部性？
- 是否有某些特徵，導致 DNS 比起其他網際網路服務更容易引發安全問題？可以從面臨類似問題的其他產業（例如關鍵基礎設施產業）借鑒什麼？如何改進現有做法？

基於上述考量，DSFI-TSG 小組於期末報告中，就下列攻擊向量研析相關案例及已知的緩解技術，藉以確立具體的緩解措施，並指出緩解措施的運作落差與緩解限制。

1. 身份識別與存取管理（Identity and Access Management）

在域名系統中，幾乎每個地方都需要使用憑證，對於憑證系統的攻擊可能導致諸如註冊資料遭到修改、網域劫持（domain

hijacking）、流量攔截（traffic interception）、社交工程攻擊（social engineering attacks）等問題。以下分別敘述憑證洩露對註冊人、註冊管理機構、受理註冊機構和經銷商的影響，以及針對這些攻擊類型的具體緩解措施。

(1) 註冊人憑證洩露（Registrant Credential Compromise）

註冊人是註冊域名的個人或實體。註冊域名後，註冊人即與受理註冊機構或註冊管理機構簽訂合約，內容包含同意註冊和維護請求域名的條款和條件。在大多數情況下，註冊人可以使用用戶名／電子郵件地址和密碼進行身份驗證，以續訂和修改其域名。如果註冊人的憑證被盜用，攻擊者將能夠冒充註冊人，將域名轉移到註冊人的控制之外、將終端使用者重新導向到惡意端點或服務、刪除或註銷域名，或刪除 DS 記錄來修改 DNSSEC 相關資料，從而取消 DNSSEC 提供的保護。

下列攻擊容易使註冊人發生憑證洩露，包括：

- 憑證填充（credential stuffing）和密碼噴灑（password spraying）攻擊
- 釣魚（phishing）（包括 SMS 和語音釣魚）
- 社交工程（social engineering）
- 電子郵件帳戶的入侵（讓攻擊者進行密碼重置）
- 透過惡意軟體、間諜軟體和中間機器攻擊（machine-in-the-middle attacks）來破解密碼
- 密碼管理不善（如密碼重複使用、可猜密碼、短密碼等）
- 內部憑證盜用和濫用

(2) 註冊管理機構、受理註冊機構與經銷商憑證洩露（Registry, Registrar, and Reseller Credential Compromise）

由於註冊管理機構負責頂級域名（Top-Level Domains, TLDs）和附屬網域（affiliated zone）申請，因此成為許多惡意行為者具吸引力的目標。註冊管理機構也受到憑證洩露影響，

它們在 DNS 系統中的位置可能會使憑證洩漏的結果產生更深遠的影響，例如影響其之下的所有受理註冊機構、經銷商和註冊人。且註冊管理機構通常提供廣泛的網路服務，因此任何線上業務的標準設備，例如郵件、DNS 和 Web 服務，也都面臨風險。如果沒有適當的安全控制，一旦對於任何一項服務的攻擊成功都可能為攻擊者創造其他攻擊機會。

基於 DNS 產業的慣例，註冊管理機構通常透過受理註冊機構向註冊人出售域名，故註冊管理機構可能與特定網域的註冊人沒有直接關係，而是經由受理註冊機構對更改請求進行身份驗證。同時，受理註冊機構則藉由各種憑證來提供註冊人的查詢、購買、更新或刪除域名等資訊給註冊管理機構，假如這些憑證遭到入侵，可能會導致受理註冊機構或經銷商喪失對其註冊對象部分或全部的控制權。

(3) 憑證洩露的緩解措施

憑證管理的最佳實務包括（但不限於）使用複雜密碼、一次性使用憑證、多重要素驗證（multi-factor authentication）以及密碼管理器。此外，其他已知的緩解措施包括：

- 使用如「Have I Been Pwned」[94]等服務來限制已洩露的密碼被重複使用，防止密碼噴灑或填充攻擊。
- 持續對擁有憑證的所有實體進行風險意識、常見攻擊（例如網路釣魚）和緩解技術的教育。
- 部署檢測憑證洩露的機制和實務，例如檢測密碼（scanning password dumps）或監控使用者行為異常。
- 主動監控文件夾的 WHOIS 記錄，以快速檢測未經授權的更改。
- 定期編寫、審查和測試憑證洩露回應的程序。

[94] 此網站收錄歷年被駭客竊取、公佈在網路上的名單資料，使用方式為輸入個人 E-mail 或電話號碼，即可透過其資料庫比對查詢者的個人資料有無洩漏。

- 針對高價域名提供域名安全鎖（Registry Lock）。
- 透過要求其他程序或人來確認身份驗證請求，進行頻外驗證（out-of-band verification）。

在實際運作上，註冊管理機構可能會受到資源限制，沒有可用的資源來部署安全策略，而且由於經銷商在確保客戶帳戶安全方面不受任何合約義務的約束，若註冊管理機構未支持使用強身份驗證，多重要素驗證等較為複雜的驗證程序將很難啟用。此外，出於對潛在後果、責任問題等考量，以及報告違規行為的法律義務不一致，受害組織通常對於入侵事件保持隱密態度，如果對這些類型的攻擊沒有共同理解，則難以評估問題的廣度並集中資源來共同解決這些問題。

2. 存取控制與授權（Access Control and Authorization）

存取控制問題是指經過身份驗證以存取特定服務或資料之實體，可能無意中存取未經授權的服務或資料的情況；或者在缺乏對某些操作執行驗證的情況下，允許更改的請求。例如未授權的子域名接管（Unauthorized Subdomain Takeover），子域名接管指非授權使用者獲得存取權限以在他們無權控制的 DNS 標籤下發佈內容的行為，可能會影響實際所有者的可信度。存取控制問題會導致與權限相關的漏洞，然而此類漏洞相關的入侵事件很少公開。

正確管理帳號及其權限是大多數組織面臨的持續挑戰，一般組織可以採取兩個具體步驟來緩解存取控制方面的問題，即域名驗證（domain verification）和操作驗證（operational validation）。服務提供商可以使用域名驗證技術（例如 ID 驗證）來驗證域名／資產之所有權／控制權。然而，實施適當的存取控制機制在運作方面存在重大挑戰，由於目前沒有明確定義的方法可用以驗證資產的所有權或表示實體之間的控制授權，也沒有通用的方法可測試特定操作是否得到充分驗證，在某些情況下，組織可能因為難

以教育客戶如何使用這些控制以及管理員工以執行這些控制，而選擇不實施強存取控制機制。

3. 資源假冒（Resource Impersonation）

有多種方法可以將 DNS 查詢重新導向到第三方，這種重新導向有幾個潛在的影響，包括導向到惡意目標，或用於收集終端使用者的資料，例如 DNS 劫持（DNS hijacking）。

(1) 假冒遞迴解析器（Impersonating a recursive resolver）

遞迴解析器是網路使用者和權威 DNS 伺服器之間的中介，處理來自終端使用者設備的 DNS 查詢，查詢根、頂級和低級別的權威伺服器，並將回應儲存在快取中，以便更快地回應未來的查詢。

犯罪者可能會在使用者的電腦上安裝惡意軟體或接管路由器等路徑網路設備，執行 DNS 劫持（DNS hijacking）等攻擊，透過虛假的 DNS 資訊將使用者重新導向到惡意站點，這些類型的攻擊案例包括 DNSChanger 惡意程式以及 GhostDNS 殭屍網路攻擊。

(2) 冒充權威域名伺服器（Impersonation of Authoritative Server）

域名伺服器的冒充也可以讓攻擊者能夠接收（並可能回應）發往權威域名伺服器的 DNS 查詢，透過這種方式，攻擊者能夠觀察 DNS 查詢訊息並回應錯誤的資料。另一方面，冒充者亦可能會做出正確的回應（例如透過代理、轉發或中繼對真實伺服器的查詢和回應），這會使冒充活動特別難以檢測。

(3) 資源假冒攻擊的緩解措施

在許多資源冒充的攻擊中，常見的已知緩解技術如下：

- 使用 VPN 等穿隧傳輸（Tunneling）技術，確保包括 DNS 在內的所有訊務都透過加密通道傳輸；不過此方式在大型組織中難以擴展，且 VPN 必須進行相互驗證。

- 情況允許下，限制僅限於已知資源可存取 DNS 連接埠。
- 監控網路上使用的解析器和伺服器是否有任何非預期的偏差。

作為具體緩解措施，DSFI-TSG 小組建議，終端使用者應安裝並經常更新保護軟體，而且若有必要，組織應將之列入 IT 管理政策之一部分。此外亦可以使用動態主機設定協定（Dynamic Host Configuration Protocol, DHCP），藉由其附加的記錄監控功能，可以查看是否有人試圖覆蓋配置。

4. 號碼和協定漏洞（Code and Protocol Vulnerabilities）

此種攻擊涉及用於運行 DNS 服務的軟體或定義 DNS 的協定中的漏洞，部分漏洞是由於開發人員對於協定規範的理解相異或不完整，或是因規範不夠明確而產生的。這些漏洞可能允許攻擊者存取不應存取的資訊或系統，覆蓋快取或檔案系統中的資訊，或以其他方式對系統產生負面影響。一般而言，協定漏洞通常更難以緩解，由於協定的任何修改都可能導致操作性問題，需要大量實施者和營運商進行協調。

(1) DNS 快取毒害攻擊（DNS Cache Poisoning）

DNS 快取中毒指將錯誤資料插入遞迴域名伺服器快取，使該伺服器的終端使用者接收並使用錯誤資料的情形。當惡意伺服器在回應中包含錯誤資料，或是當路徑上的攻擊者攔截查詢並生成自己的回應，或者當偏離路徑的攻擊者成功欺騙終端使用者，皆可能導致 DNS 快取中毒。

(2) 號碼和協定漏洞的緩解措施

DSFI-TSG 小組指出，DNSSEC 數位簽章及區域驗證是消除快取中毒攻擊的唯一方法，其他緩解措施只能作為臨時解決方案，增加執行攻擊所需的工作量，例如在解析器和授權伺服器之間使用加密的 DNS 傳輸協定（DoT、DoQ）可以減輕許多路徑攻擊（on-path attacks），但新的攻擊仍會出現並繞過措施

（例如 SAD DNS），因此部署 DNSSEC 簽章和驗證是防止快取中毒的最佳技術。

不過，儘管 DNSSEC 已推出十多年，但在許多註冊管理機構中，域名註冊人（即二級域）的採用率依然很低。DNSSEC 驗證之部署主要歸功於大型第三方遞迴服務（如 Google、Cloudflare、Quad9），在這樣的狀況下，終端使用者只有在他們存取的域名經簽署以及解析器經過驗證時才會受到保護。

5. 基礎設施選擇（Infrastructure Choices）

在某些情況下，由於管理員對於 DNS 服務的配置考量，例如 DNS 記錄的存留時間（Time To Live, TTL）、使用軟體的選擇（例如較舊的、無補丁的軟體版本），如果著眼於降低成本，可能較容易引入漏洞。因此，基礎設施的選擇需要經過深思熟慮的風險評估，必須考慮其運行的環境，包括信任關係和配置，且應定期重複審查，因為雖然基礎設施本身可能不會改變，但其使用情況和周圍環境可能會發生變化，這些變化都會對基礎設施的使用和安全性產生重大影響。

在 DNS TTL 選擇方面，一般而言，TTL 的選擇涉及彈性（resilience）、敏捷性（agility）、性能（performance）以及伺服器負載（server load）之間的權衡，較長的 TTL 有利於彈性和性能，而較短的 TTL 有利於敏捷；短 TTL 通常為數分鐘或數秒，而長 TTL 則可存留數小時甚至數天。對於大多數組織而言，下列兩種時間的 TTL 最為重要，即更新記錄時，或是面臨針對權威域名伺服器的攻擊時。雖然域名營運商可以修改 TTL，但多數情況下皆依賴於固定的 TTL。

當遭受攻擊時，在選擇較長的 DNS 記錄 TTL 的情況下，服務需要較長時間才能恢復；但若是 DNS 供應商受到攻擊（例如 DDoS 攻擊）時，則使用長 TTL 為佳。如果是能夠更改 DNS 授權（DNS delegations）或區域資料（zone data）的攻擊者，則可能會

透過長 TTL 來獲得優勢；且劫持的影響會保留在 DNS 快取中，直到 TTL 到期，可能是在劫持被檢測到並更正的數天之後。另一方面，短 TTL 常使用於需要靈活性的服務，如果 DNS 供應商的客戶使用短 TTL，則可能會較突然地感受到針對供應商的攻擊。此外，由於快取的短暫性，以及普遍缺乏記錄，短 TTL 可能會覆蓋掉攻擊者的蹤跡，而使取證變得更加複雜。

6. 阻斷攻擊（Denial of Service）

阻斷攻擊（DoS）攻擊是一種網路攻擊，係指攻擊者試圖透過暫時或無限期中斷目標的服務和／或連接來使其目標使用者無法使用機器或網路資源。DoS 攻擊的變體為分散式阻斷攻擊（DDoS）攻擊，發生於多個系統對目標進行同步 DoS 攻擊時，通常攻擊者使用可公開存取的開放遞迴解析器或殭屍網路，使 DNS 回應訊務淹沒目標系統，這些類型的攻擊通常會選擇導致大量回應的查詢來最大化放大係數。

針對 DoS 攻擊，已知的緩解措施包括：

- 訊務檢測、深度檢測等防火牆優化。
- 使用 DNS Cookie。
- 在專用伺服器上運行遞迴伺服器。
- 使用存取控制機制來限制第三方對解析器的使用。
- 配置遞迴伺服器以使用 DNSSEC 驗證。
- 監控並定期檢查記錄。
- 定期更新軟體。

然而這些措施通常只能解決攻擊的結果，而非原因。此外，由於風險政策不同等原因，以上措施通常只能由基礎設施的所有者各自實施，因此組織必須定期和快速更新產品供應商提供的軟體，確保提供 DNS 服務的系統保持在最新的狀態；若是無法使系統保持在最新狀態的組織，則應盡可能考慮外包 DNS 服務。

7. DNS 作為攻擊向量（DNS as the Attack Vector）

DNS 除了可能被當作攻擊的直接目標，也可能被用作攻擊的通道，使其他攻擊能夠滲透到系統或網路並從該系統或網路中提取資料。

(1) 使用 DNS 作為隱蔽通道（Use of DNS as a Covert Channel）

將 DNS 作為隱蔽通道使用，也稱為「DNS 通道穿越」（DNS Tunneling），是藉由 DNS 查詢和回應通道來實現設備之間的秘密通訊，同時讓 DNS 訊務看起來是良性的。其通常使用偽裝成 DNS 查詢和回應的加密資料，而不是 DNS 原本作為資源查找協定的用途。

由於 DNS 訊務通常可以在很大程度上不受阻礙和不受監控地穿越網路邊界，因此可用作受防火牆保護資源與具有惡意意圖的外部第三方之間的通訊通道，同時也為不法份子提供機會，以在受保護或隔離的受感染設備與外部資料收集點之間建立隱蔽的資訊傳遞通道，進而秘密地從受保護的網路或資產中竊取資料。

(2) DNS 作為攻擊向量的緩解措施

目前緩解做法是透過 DNS 解析器的重新導向（也稱為 DNS 防火牆），向查詢設備提供已知的惡意域名，不過若要使當前 DNS 隱蔽通道域名的準確情報保持最新，便需要花費大量精力來更新這些域名列表。此外，許多開放的公共解析器都有「DNS 中立」（DNS neutral）的政策，其可能使客戶端容易受到透過 DNS 的攻擊。

綜上所述，DSFI-TSG 小組提出各個攻擊向量的緩解措施，其緩解限制經常涉及整體系統環境實務的運作，包括在組織內部政策上，缺乏可用資源部署安全策略，而在外部 DNS 與基礎維運溝通上，無明確契約規範 DNS 域名註冊管理相關機構或經銷商、設備商在資訊安全上的責任義務，此亦延伸涉及憑證取得、DNS 系

統更新等資安技術的採用與持續優化。ICANN 站在數據資源的立場來看，亦在推廣將 DNS 納入組織 IT 政策的可能性。

(三) 企業對於 DNS 的資訊安全需求

由上述可知 DNS 與 5G、IoT 發展之關聯性，DNS 作為網路重要的運作機制，卻也因此容易成為攻擊的弱點。當未來是雲端網路時代為主流，人類的生活的樣貌將會陸續逐漸朝向雲端網路時代蓬勃發展；未來可能對於實體資安系統的投資需求將有可能逐步下降，使 DNS 對於資訊安全的重要性更為顯著[95]。資安廠商與網通業者為此提出強化 DNS 防護的技術解決方案。

Infoblox[96]亞太區技術長（CTO of APJ） Yong Kwang Kek（下簡稱 Kek）指出，與其他網路系統相較，DNS 擁有「更簡單」、「更彈性」與「更安全」三大特性。「更簡單」: 對於企業而言，僅需調整 DNS 的設定，就可以從基礎上獲得安全防護，而若透過高安全性的 DNS 協定將可有效阻斷大部分藉由 DNS 產生的網路危害；「更彈性」: 不論是企業規模的大小或是其他因素等，亦不論是否有 VPN 等外部連線等需求，DNS 如同地基般，可於其之上設置各式裝置。再者，只要 DNS 的基礎穩固，後面衍生的資訊安全問題將會大幅減少，且在資訊安全的策略尚將更彈性與靈活，並同時保有更佳投資報酬率「更安全」:舉例而言，一個良好的 DNS 可有助於資訊安全的管理與維護，而藉由自動化的 DNS 管理，可有助於管理人員在資訊安全系統的維護與管理上更加便利。因此，在以 DNS 作為基本網路安全管理的基礎上，例如詐騙、釣魚網站以及惡意連結等安全問題，皆可於第一時間即進行防護與阻斷。同時，DNS 亦可有效過濾和處裡多數的資訊系統安全警示，使管理人員可將時間與精力花費於真正有需求的資安問題的解決

[95] 同前註。
[96] 同前註。

上。Infoblox[97]提出的方案是透過 DNS 防火牆、進階 DNS 防護技術，搭配整合的裝置與中央管理軟體，提供簡易的 DNS 管理與安全防護，可協助企業補強安全部署中的最弱環節；在抵禦 DNS 攻擊之餘，更可搭配整體資安部署，進而有能力對抗不斷改變與演進的網路攻擊，保護企業的智慧資產與敏感資訊等[98]，達到輕量化、但比一般伺服器更安全的硬體平臺與 OS 系統；透過單鍵快速成立 DNSSEC，簡化以往繁雜的 DNSSEC 程序。

全球知名德國科隆 OX 軟體股份有限公司（OX Software GmbH）發行之白皮書 1.0（Whitepaper Version1.0），亦針對 5G 以及 DNS 間未來關係提出討論與發表觀點。

OX 認為，傳統上，物聯網設備非常容易遭受攻擊與破壞，並且容易受到惡意軟體的感染或 DDoS 攻擊，因此，基於 5G 核心網路虛擬化之性質，若物聯網設備間的端對端通訊未擁有安全性，則將會造成隱私以及攔截等潛在資安問題。而在 5G 網路架構中，幾乎所有網路通訊皆無法脫離 DNS，DNS 可謂於用戶端機器扮演著控制的重要角色與功能。[99]

5G 網路結構低延遲的特性無法以既有 DNS 來滿足，因此若要使 DNS 查詢返回的速度符合 5G 低延遲特性，則 DNS 系統服務必須利用邊緣運算方可解決問題。值得注意的是，OX 對於 DNS 在 5G 網路的使用方式，正好回應了 ICANN 對於 DNS 是否仍適用於 5G 超高速、低延遲場景之疑慮。[100]

針對未來 DNS 在 5G 網路架構所扮演之資安防護功能，OX 除了指出既有的 DOT 與 DOH 為 DNS 基本防護功能外，未來將還須於 DNS 解析器以及權威伺服器中進行加密。再者，DNS 應用程序

[97] Infoblox 是一家具備全方位 DNS 管理與安全技術與解決方案的公司，在全球知名資通訊產業研究機構 IDC（國際數據資訊)的 DNS 相關管理市場研究中，以 50%的全球市佔率居冠。
[98] 達友科技，〈 DNS 安全防護方案〉，<https://www.docutek.com.tw/solution.php?pk=21>
[99] Ox software GmbH, " OX Whitepaper DNS in a 5G Network New Requirements and Demands" ,*WHITEPAPER VERSION 1.0*,p.5 -6
[100] *Id*.p.6-7

級加密方為確保行動設備與其他服務間之通訊部不被任意截取、監視或修改。[101]

OX 對於 5G DNS 架構一共提出四項建議要件，分別為低延遲（Low Latency）、高度本地化（ High Localized）、加密（Encryption）以及虛擬化、協調與控制平面功能（Virtualization、Orchestration&Control Plane Functionality）。意即，DNS 在 5G 網路架構中必須為邊緣運算 DNS（edge DNS）；DNS 伺服器必須將客戶端子網訊息傳遞至內容傳遞網路（Content Delivery Network, CDN），以避免緩存碎片；利用 DNS 加密方式確保安全；DNS 服務必須朝真正的虛擬網路功能（Virtualized Network Function, VNF），或是理想情況下為容器化網路功能/雲原生功能（Container Network Function, or Cloud-Native Network Function, CNF）發展，並且配置協調與控制平面功能。[102]如此一來，透過上述四要件，可構成一符合資安需求之下世代網際網路系統。

微軟是以建構 Azure Private DNS 作為企業建置私網的解決方案。DNS 負責轉譯（或將服務名稱解析）為 IP 位址，而 Azure DNS 為網域的主機服務，並使用 Microsoft Azure 基礎結構來提供域名解析。因此，Azure DNS 不只支援網際網路對向 DNS 網域，同時也支援私人 DNS 區域（zone）。Azure 私人 DNS 可為虛擬網路提供可靠且安全的 DNS 服務，其可管理及解析虛擬網路中的功能變數名稱，而不需要設定自訂的DNS解決方案。 進一步言之，藉由使用私人DNS 區域，企業可以在部署期間使用該企業的自訂功能變數名稱，而非 Azure 提供的名稱。另外，使用自訂功能變數名稱可協助企業量身打造該企業的虛擬網路架構，以最符合該企業的需求，為虛擬網路內的虛擬機器，以及為已連線的虛擬網路，提供命名解決方案。此外，企業還可利用水平分割檢視來設

[101] Ox software GmbH, " OX Whitepaper DNS in a 5G Network New Requirements and Demands" ,*WHITEPAPER VERSION 1.0*,p.9
[102] *Id*.p.11

定區域名稱，使私人與公用 DNS 區域能夠共用名稱[103]。

再者，若要從企業的虛擬網路解析私人 DNS 區域的記錄，則必須將虛擬網路連結至該區域。而連結的虛擬網路具有完整存取權，且可解析在私人區域中發佈的所有 DNS 記錄。此外，也可以在虛擬網路連結上啟用自動註冊。因此，當在虛擬網路連結上啟用自動註冊時，該虛擬網路中虛擬機器的 DNS 記錄會在私人區域中註冊。而當啟用自動註冊時，Azure DNS 將會在每次建立虛擬機器時更新區域記錄、變更其「IP 位址」或「已刪除」[104]。

Azure DN 的功能包括: 若虛擬網路連結至已啟用自動註冊的私人區域，為此虛擬網路中的虛擬機器進行自動註冊；針對已連結到私人區域的多個虛擬網路，支援正向 DNS 解析；在虛擬網路範圍內支援反向 DNS 查詢[105]。

總的來說，DNS 過去長久以來一直為網際網路系統的域名扮演了重要的角色，而在快速發展的 5G 網路或是萬物聯網的下世代網路情境中，DNS 為物聯網設備帶來了更多的資安需求。在 5G 網路背景下，DNS 有朝著邊緣化、但又講求安全、穩定透明的趨勢。目前國際上業者所提出針對 DNS 安全的資安防護系統開發原則，一是優化既有 DNS 防護機制，例如 OX 提出再針對伺服器進行加密、Infoblox 簡化 DNSSEC 執行步驟等。二是針對企業未來可能的私人網路需求創建一符合資安需求的網路環境，開發出各自的 DNS 資安防護系統，像是對於企業內部網路中建置私有 DNS（Private DNS）情境，微軟提出一套作為切分服務類型的客製化網路配置，兼顧私有 DNS 系統建置以及資安建構。簡言之，未來若以 DNS 編碼機制作為資源管理的關鍵，在強化 DNS 安全性部分，可透過強化既有的 DNS 加密方式，例如 DNSSEC 與 5G 網路

[103] Microsoft，〈什麼是 Azure Private DNS?〉，04/9，2021，<https://docs.microsoft.com/zh-tw/azure/dns/private-dns-overview>
[104] 同前註。
[105] 同前註。

架構串聯以及整合加強資安防護，盡量將 DNS 部署於網路架構邊緣，朝著縮短大量連網裝置群播認證時間流程的目標發展。

第二節　國際網路安全政策與法規研析

研究團隊於前節主要探討下世代網路的發展以及可能發生的資安議題，然而，無論下世代網路是否如 ITU Network 2030 的願景發展，世界各國當前的資安政策，也各反映了該國對於未來網路、社會、經濟發展面向的思考。於本節藉由對先進國家資安政策的分析，可瞭解當前各國資安政策與未來需求的差異性，進而提出具前瞻性的建議。

一、美國

美國的資通安全核心政策，係以強化國家關鍵基礎設施的安全性，並鼓勵創造一個有效率、創新和經濟繁榮的網路環境，希望得以促進安全、保障、商業機密、隱私和公民自由。依據 2013 年 2 月 12 日所發布的第 13636 號行政命令（Executive Order, EO），美國國家標準技術研究所（National Institute of Standards and Technology, NIST）授命需訂立一套可供聯邦各單位採用的網路安全框架，並於同（2013）年 8 月首度發布「網路安全框架」（NIST Cybersecurity Framework, CSF），藉此強化國家網路安全與推動資安政策。該框架遵循第 13636 號行政命令之要求進行訂定，要求包含：確立關鍵基礎設施領域之安全標準與指南，以及能衡量實施績效之指引，並於關鍵基礎設施部門、利害關係人提供技術中立之指導；透過特定部門和標準組織之未來合作，進行議題定錨、並實現以新興科技解決組織差異。

基此，NIST 於 2014 年 2 月 12 日發布「改善關鍵基礎設施網路安全框架」1.0 版本，並於年底美國政府公佈網路安全強化法（Cybersecurity Enhancement Act）。川普於 2017 年公布第 13800 號命令[106]，命令表示為強化聯邦網路與關鍵基礎設施之資安防護體系

[106]Trump whitehouse, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, available at https://trumpwhitehouse.archives.gov/presidential-

（Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure ），所有聯邦機構須採用網路安全框架（以下稱作CSF），已有包含義大利、以色列、匈牙利等國採用，NIST與CSF在國際資安政策發展中地位重要。2018年4月16日，NIST匯集已採用CSF的政府單位、民間企業所回饋的意見，發布CSF的1.1版本，該版本較前版本有大幅度的調修，主要強化身分驗證與識別、資安風險的自我評估、管控供應鏈的網路安全以及弱點察覺的四大面向 。以下將以NIST CSF 1.1為骨幹，並依序說明由NIST發布與關鍵基礎設施與基礎網路相關之網路安全規範、特別出版物（Special publication, SP）等其他網路規範。

(一) 網路安全框架（NIST CSF 1.1）

美國網路安全框架之目的，除強化美國關鍵基礎設施的網路安全，亦可提供不同產業領域使用，各產業可進一步參考 CSF 的架構設計，依照自身的需求量身訂做合適之網路安全框架。CSF是以風險為基礎，並由框架核心（Framework Core）、框架設定檔（Framework Profiles）與框架實施層級（Implementation Tiers）組成。由功能面分析，「框架核心」可視為網路安全防護檢核表；「框架設定檔」可視為網路安全的落實程度；「框架實施層級」則可以視為對於網路安全現況的敘述[107] 。分述如下：

1. 框架核心（Framework Core）

框架核心能協助企業檢視其所有的資安防護，例如企業自身的資安現況，是否按照框架核心所列出的各個項目進行檢視。關於框架核心所列出的資安檢核項目，主要可分為功能（Function）、類別（Category）以及子類別（Subcategory）[108]。

actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (Last visited：May, 17, 2021)

[107] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecirity Version 1.1*, (April. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf(Last visited: May,17,2021)

[108] *Id*. at 3-4.

NIST 針對框架核心所列出的檢核項目，也列出針對檢核項目裡的子類別的參考資訊（Informative References），提供企業根據特定的標準和指南的內容，規劃與執行其所需的資安相關的工作[109]。關於框架核心所列檢核項目，依功能主要可分為 5 大面向，包括識別（Identify）、保護（Protect）、偵測（Detect）、回應（Respond）與復原（Recover）。此 5 大面向可視為針對企業遭受攻擊的各個階段所採取的措施，包括資安檢核前（識別和保護）、資安檢核中（偵測）與資安檢核後（回應和復原）須採取的資安措施，以下說明：

(1) 識別（Identify）：了解組織，並管理系統、人員、資產、數據等網路安全風險，並能夠進行風險管理的識別。
(2) 保護（Protect）：制定並實行適當的保護措施，確保能夠為網路安全提供服務。
(3) 偵測（Detect）：制定並實行相關偵測行為，確保能夠識別網路安全事件的發生 。
(4) 回應（Respond）：制定並執行因應攻擊的適當策略，確保能夠對於偵測到的網路安全事件採取必要措施 。
(5) 復原（Recover）：制定並執行適當的復原行為，以恢復從網路安全事件而受損的任何功能或是服務 。

2. 框架設定檔（Framework Profiles）

框架設定檔主要作用有助於將其 5 大功能（辨識、保護、偵測、回應與復原）及其所涵蓋的類別和次類別，分別對應至組織的特定要求、目標、風險容忍度和組織的資源 ，簡言之，即是將企業需求與資源與框架核心的預期成果做連結。

3. 框架實施層級（Implementation Tiers）

框架實施層級指出在不同階段時期，企業或組織如何看待網路安全風險，以及如何執行適當的風險管理流程。框架實施層級

[109] *Id*. at 6-7.

一共分為 4 個層級，由低至高依序為第一層：部分實行（Partial）；第二層：風險已知（Risk informed）；第三層：措施可重複執行（Repeatable）；第四層：完全適應（Adaptive）。每一層級均包含三個部分，包括風險管理流程（Risk Management Process）、綜合風險管理規劃（Integrated Risk Management）以及外部參與（External Participation），階段性實施內容詳參表 3-3。

表 3- 3、NIST 網路安全框架框架實施層級

實施層級	第一層 部分實行	第二層 風險已知	第三層 措施可重複執行	第四層 完全適應
風險管理流程	臨時、被動、非正式網安風險管理規範	已獲管理階層同意批准，尚未確立網安風險管理範圍	已獲管理階層正式批准，並依企業策略與新型態威脅隨時更新	根據過去和目前的網路安全情況，適時調整其網路安全的措施
綜合風險規劃	低，網安資訊來源無法共享	尚未訂定管理辦法，無法重複評估網路安全風險	具體定義「風險」，並了解風險管理策略、流程和程序，按計畫實施和審查。各風險管理角色應盡責監控網路安全風險，並對組織全體進行風險溝通	制定風險策略、流程和程序，明白當前企業組織與網路風險之關係以識別潛在風險，並預估各部門之風險承受能力
外部參與	無法與利害關係人共享網安情資	已了解內外部關係並建立自身網路安全資訊，卻未進行情資共享，且未採取行動	定期與外部對象合作以補充內部資訊、與對方共享，並採取正式協議與監控行動	建立良好之內外部風險情資分享與風險分析機制，並採取正式/非正式之行動

資料來源：本計畫製作

(二) CISA 5G 策略（CISA 5G Strategy）

CISA 5G 策略（CISA 5G Strategy）詳細介紹了 5G 基礎設施的開發和部署方法，該策略可促進安全且有彈性的 5G 基礎設施，進而提升美國的國家安全、資料完整性、技術創新以及經濟機會。

為評估 5G 基礎設施可能面對的風險與制定保護策略，2019 年 5 月，包括美國在內的全球三十多國政府官員於布拉格共同參與由捷克主辦的 5G 資安會議（Prague 5G Security Conference），討論5G網路部署的安全準則。該會議結論經捷克政府彙整為「布拉格提案」（The Prague Proposals），確立了不同類別的建議，包括政策、技術、經濟和安全、隱私及韌性（Resilience）等面向，提供世界各國在建構5G基礎設施方面之資安建議。隨後，美國根據上述「布拉格提案」，於 2020 年 3 月制定「國家安全 5G 策略」（National Strategy to Secure 5G），確定了四項主要工作，包括（1）促進國內 5G 部署，（2）評估風險並辨識 5G 基礎設施的核心安全原則，（3）提出美國在發展和部署全球性的5G基礎設施時所可能遇到的經濟與國家安全風險，以及（4）推動可信賴的 5G 全球發展和部署，以最大程度地提高 5G 基礎設施的安全性。

針對關鍵基礎設施的發展與佈建，美國國土安全部網路安全暨基礎安全局（Cybersecurity and Infrastructure Security Agency, CISA）於 2020 年 8 月發布「CISA 5G 策略」，建立了五項策略提案（Strategic Initiatives），這些計畫即源於「國家安全 5G 策略」中定義的四項主要工作，並以三個核心能力為指引，包括風險管理（Risk Management）、利益相關者參與（Stakeholder Engagement）和技術協助（Technical Assistance），藉此確保有適當的政策、法律和安全框架來充分利用 5G 技術，同時管理其重大風險，達到增進國土安全、資料完整性、技術創新與經濟發展機會。其策略提案和核心能力分述如下：

1. 5G 策略提案（5G Strategic Initiatives）

(1) 強調網路安全性與彈性，支持 5G 網路政策與標準之發展

5G 政策和標準的制定是保護未來 5G 通訊基礎設施的基礎，塑造相關政策和標準的實體將成為全球領導者，並協助 5G 技術的安全部署和商業化。基此，為了防止惡意行為者影

響5G網路的設計和架構，從一開始就以安全性和彈性對其設計和實施至關重要。具體作法為：

- 擴大政府、產業5G工作小組和標準機構的協作。
- 與值得信賴的市場領導者合作，增加5G標準的貢獻。
- 支持國際5G安全和彈性相關政策或框架之發展工作。

(2) 擴大5G網路供應鏈風險態勢感知，推廣安全措施

雖然某些5G設備可能來自受信任的供應商，倘若與惡意行為者合作製造，仍可能危及資訊與資料傳輸的安全性，是以在不受信任的元件、供應商、設備和網路之間，5G供應鏈的安全不斷受到威脅。故應注意：

- 聯邦政府內ICT供應鏈合作，統一5G供應鏈的風險管理工作流（workstreams）。
- 制定共同框架，以評估、排定優先順位和溝通5G供應鏈之風險。
- 創造客製化對外宣傳資料，促進供應鏈風險管理策略。

(3) 與利益相關者合作，加強與保護現有之5G基礎設施

在5G基礎設施發展成熟之前，將與現有的4G LTE基礎設施和核心網路共同運作，雖然5G的架構設計更加安全，但其規範和協定源於過去的網路，其中可能遺留漏洞。這些既有漏洞與未識別的新風險，需要產業和政府合作增強安全功能，以支持安全的5G部署。具體作法如下：

- 與國家實驗室和技術中心合作，評估現有的關鍵5G元件並識別安全漏洞。
- 直接參與以促進關鍵基礎設施部門和州、地方、部及領土（State, Local, Tribal and Territorial, SLTT）等區域中5G部署的安全性和彈性。
- 協調聯邦政府與國際夥伴合作並推廣5G部署的最佳實踐。

(4) 鼓勵5G網路市場創新，培育可信賴之5G網路供應商，隨

著 5G 的部署，重點是確保受國家影響的實體不會主導 5G 市場，建議如下：

- 與聯邦跨部門夥伴合作，建立聚焦5G新興技術的研發計畫。
- 分析和報告不受信任的 5G 元件供應商的長期風險。
- 與聯邦相關獎項競賽計畫合作，以影響和確立5G創新挑戰。

(5) 分析潛在 5G 網路案例並共享風險管理資訊

5G 技術的大容量將可支援一系列新設備和功能，由於有可能在網路上連接數十億臺設備，也稱為巨量多機器型態通訊（mMTC），因此將需要更高的安全性，以保護連接的設備免受潛在威脅和安全漏洞的影響。實行方案如下：

- 在真實和虛擬環境中鑑定、優先排序和評估潛在的 5G 應用個案。
- 發展和提供5G技術支援，以解決利益相關者的使用案例。
- 善用產業專業知識和分析來發展資訊資料，促進5G支持的物聯網設備之最佳安全實踐。

2. 核心能力（Core Competencies）

(1) 風險管理：透過識別、分析、確認優先級別和管理風險等方式來促進安全和有彈性的 5G 部署。

(2) 利益相關者參與：積極讓聯邦、州、地方之不同地區、產業、協會、學術單位、非營利組織和國際合作夥伴參與，以應對 5G 挑戰。

(3) 技術援助：更新和開發指導工具，為利益相關者在5G安全部署的規劃、治理、執行和技術層面予以支持。

3. 關鍵基礎設施指南

美國有 16 個關鍵的基礎設施部門，其資產、系統和網路在實體或虛擬上皆對美國至關重要，若這些設施無法運作或遭到破壞，

將對國家安全和經濟、公共衛生造成破壞性影響。基此，CISA 發布了「必要關鍵基礎設施勞動力指南」（Guidance on the Essential Critical Infrastructure Workforce），旨在保障關鍵基礎設施的正常運行，並加強和維護關鍵基礎設施的安全性和彈性。其中，針對資通訊部門，CISA 指出，通訊產業已從主要提供語音服務發展為使用地面、衛星和無線傳輸系統的多元競爭且相互關聯的行業。同時多數通訊基礎設施的所有者和業者為私部門，係負責保護該部門基礎設施和資產的主要實體。因此私部門被鼓勵與聯邦政府合作，以利預測和應對部門運轉中斷的情況，並了解它們可能如何影響國家領導層在危機時期的溝通能力，以及對於其他部門的衝擊。此外，在與通訊部門合作提供網路上，儘管資訊部門本身即具有一定程度的彈性，其相互依存和相互關聯的結構仍為協調公私部門的準備帶來挑戰。

(三) 其他網路安全規範

除了 CSF 之外，NIST 亦於 1990 年推出特殊出版物 SP 系列。NIST SP800 係依據 2014 年《聯邦資訊安全現代化法》（Federal Information Security Modernization Act of 2014, FISMA 2014）所開發，該系列旨在支持美國聯邦政府對於資訊系統的安全和隱私需求，包括相關的指南、建議、技術規範和 NIST 網路安全活動的年度報告。

在使用上，NIST SP 800 系列需在獲得聯邦官員的批准下應用於國家安全系統，聯邦政府保有是否採用此系列的權力，可以透過法規或政策要求政府機構遵守。NIST SP 800 系列可能超出美國法規和政策的範圍，除非出於合約義務（如外包商），非聯邦政府的組織得以自願決定是否實施；不過，其他負有監督責任的非聯邦組織也可以要求將此系列落實在特定的使用社群。NIST SP 800 系列涵蓋的內容龐大，且持續更新，過往涉及安全部署 DNS（SP 800-81-2）和 IPv6（SP 800-119）的相關指南、安全內容自動化協

定（SCAP）的技術規範（SP 800-126），以及無線區域網路安全規範（SP 800-153）、行動應用程式安全性（SP 800-163）等。以下針對網路層的 IPv6、DNS、WLAN、零信任原則、應用層的 IoT、行動應用程式進行說明。

1. IPv6（NIST SP 800 -119）

由於 IPv4 位址分配已經耗盡，採用 IPv6 是唯一能夠長遠解決 IP 位址短缺的方案，可以預期商用 IPv6 將被廣泛使用，由此組織將不得不更改其網路基礎設施和系統以部署 IPv6。是以，NIST 發布 SP 800 -119 文件，協助聯邦機構了解其在使用 IPv6 協定期間可能存在的安全風險，並提供指導以幫助安全部署 IPv6。

(1) IPv6 安全風險

NIST SP 800 -119 指出，關於 IPv6 之部署，組織可能面臨的一般風險如下：

- 攻擊者社群對 IPv6 的使用：攻擊者社群正在適應 IPv6 環境，對連接網路的所有組織構成嚴重風險。如果組織的安全控制尚未監控 IPv6 訊務，則現有的安全控制系統可能無法檢測進出客戶端設備的 IPv6 訊務。此風險的緩解措施是重新配置或部署安全控制，使其可同時識別 IPv4 和 IPv6。
- 在現有 IPv4 網路上未經授權部署 IPv6：由於網路正在積極部署 IPv6，大多數操作系統都支持 IPv6，並且通常默認啟用 IPv6，這使組織暴露於它可能無法檢測到的漏洞。
- IPv6 中存在的漏洞，包括所有新系統中固有的「零日」（Zero Day）漏洞。
- IPv4／IPv6 雙操作增加之複雜性：雙協定會增加環境的複雜性，兩種協定意味著可能出錯的情況翻倍，安裝新設備或更改現有設備所需的配置數量翻倍，管理員需要對兩種協定保持相同的覆蓋水準以降低風險。

- IPv6 安全產品和流程不成熟，要獲得 IPv4 的多年操作經驗和實際部署的解決方案作為參考還需要時間。
- 可能缺乏供應商支持。

(2) IPv6 安全主題

IETF 在制定 IPv6 標準時將安全性視為重要的設計準則，在其安全設計中，IPsec 係 IPv6 特有的新發展，其提供強力、最新的保密性和完整性保護、存取控制（access control）、回放偵測（access control）、金鑰管理（key management）和針對 IPv4 的同級實體身份驗證（peer-entity authentication），解決了 IPv4 缺乏保密性和完整性的問題。

2. DNS 安全部署指南（NIST SP 800-81-2）

DNS（Domain name system, DNS）是網際網路架構中用來轉換域名（domain name, DN）與網路協定（IPv4 或 IPv6）的系統。DNS 會透過域名伺服器（domain name server）及解析器（resolver）執行域名資料庫（domain name repository）查詢以及域名解析（name resolution）功能，做 IP 與 DN 的對映（mapping）。簡言之，當用戶需要接取某網路，用戶所屬轄區（zone）110之 DNS 會進行查詢，若暫存資料（cache）、資料庫中均未有已註冊之 DN，則 DNS 系統會循樹狀階層架構進行域名查詢（query）。

基此，（1）DNS 的主機環境（Hosting Environment）：DNS 資料庫、系統平臺、域名伺服器與解析器軟體、硬體設施；（2）DNS 資料交換程序（transaction）：查詢與回應、轄區傳送（zone transfer）、DN/IP 資料動態更新、DNS 轄區變更通知（DNS NOTIFY）[111]；（3）安全程序：演算法與金鑰規格選擇、金鑰管理、公鑰基本設定等均屬 DNS 資訊安全範疇。

[110] 此處的轄區（zone）係指在網域中有一臺（或以上）的 DNS，該轄區內的 DNS 屬同一域名，被視為子域（subdomain），同樣具主從關係，區分為主伺服器（master server）與子伺服器（slave server）。一個轄域被視為一個獨立運作之實體（standalone administrative entity）。

[111] 係指主域名伺服器若進行轄區資料變更，子域名伺服器需同樣進行資料變更之程序。

NIST-800-81-2 文件指出，由於 DNS 是大眾可接取的公開資訊資源，維護 DNS 資料機密性（confidentiality）不是 DNS 安全的考量。DNS 首要安全目標在於資料的完整性（integrity）與來源的真實性（authentication），須確保域名（domain name, DN）資訊的真實性、並維護域名資料於傳輸途中（in transit）的完整性。DNS 與其他平臺、軟體和網路層級上（network-level）其實具有同等的脆弱性，而 DNS 屬於全球網路的基礎設施系統，又多了一層特殊性[112]：

(1) 沒有完善定義的系統邊界，參與實體（entity）不限於區域或網路拓樸規則。

(2) 沒有資料機密性的需求，故能被任何地區或關聯性之實體所接取。

基此特性，傳統網路層級的威脅像是偽裝（masquerading）和訊息竄改（message tampering），將會對在資料傳輸、持有資料之完整性上面又造成全然不同的功能性影響[113]：

(1) 假冒 DNS 節點（node）身份的偽裝者（masquerader）可以拒絕對該節點所服務的域（domain）的網路資源（Internet resource）接取。此拒絕接取的範圍不僅針對一組有限的使用者。

(2) 偽裝者或系統入侵者可提供假的 DNS 訊息，藉此汙染 DNS 節點提供給 DNS 子集的暫存（cache）資料，例如拒絕提供給企業用戶的網路存取。

(3) 破壞權威 DNS 資料查詢完整性、或破壞累積許多歷史查詢暫存資料，可能會破壞 DNS 鏈接訊息的檢索過程。易導致權威 DNS 拒絕域名解析，或將使用者誤導至有害、非法網

[112] NIST, Secure Domain Name System (DNS) Deployment Guide,pp ES1-3,available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf (Last visited, May,26,2021)

[113] *Id.*

路資源。

(4) 若DNS系統託管的域名解析資料違反DNS命名規則要求，恐導致DNS系統工作量增加或拒絕服務。

針對 DNS 造成的功能性影響，文件列舉相對應 DNS 部署的指引建議，希望透過本指引能在 DNS 系統的效能表現與資訊完整性上取得平衡，並建議如何保護 DNS 域名伺服器（DNS Name Server）。對於 DNS 部署的建議包括：

(1) 實施適當的系統與網路安全控制，例如操作系統和應用程序修補（patching）、程序隔離（process isolating）以及網路容錯（tolerance）。

(2) 保護 DNS 資料交換程序（transaction），例如 DNS 更新域名解析資料和涉及企業控制的 DNS 節點資料的複製，應使用基於共享機密的特定身份驗證代碼（hash-based message authentication code）來保護交易。

(3) 使用基於非對稱密碼的數位簽章（digital signatures）維護全球網際網路中任何 DNS 節點的域名查詢與回應。

於 DNS 域名伺服器部分，則針對權威伺服器與快取伺服器在 DNS 擴充協定（ DNS Security Extensions, SEC）的部署提供查核之建議。

3. 無線區域網路安全規範（NIST SP 800-153）

無線區域網路（Wireless Local Area Networks, WLANs）為於有限地理區域內的各種可無線連網的資通訊裝置，透過無線通訊技術（Radio Communications）交換數據。每一個 WLAN 的安全性基本上取決於每一個 WLAN 的組成元件，包括客戶端設備、接取熱點（Access Point, AP）以及無線交換器（Wireless Switches）。以網路的安全性而言，相較於其他同類型的網路，WLAN 主要以便利性為主，因此其易於使用的特性，使其安全性較低隨著 WLAN 風險的不斷增加，如何防範針對 WLAN 的攻擊和其他類型

的網路攻擊，也變得更加重要。NIST SP 800-153 保護無線區域網路準則（Guidelines for Securing Wireless Local Area Networks, WLANs）針對 WLAN 的安全性，包括兩大面向：WLAN 的安全設置（WLAN Security Configuration），以及 WLAN 的安全監控（WLAN Security Monitoring）。

(1) WLAN 的安全設置 (WLAN Security Configuration)

NIST 認為規劃與建立 WLAN 的安全性時，不僅要考慮 WLAN 本身的安全性，也需要考慮其如何影響其他網路的安全。由於 WLAN 的網路系統為特定區域內網路，亦可連接至其他網路，針對特定區域外的客戶端設備連網之情況，應將 WLAN 分為供外部和內部使用兩種模式，並且只允許客戶端設備連接特定供外部使用之 WLAN，且外部和內部使用的 WLAN 不應彼此互通。另外，針對同時連接有線網路、WLAN，以及多個無線網路裝置，例如藍芽、手機等的雙連接（dual connected）連網情況，應明確說明如何允許或是禁止何種雙連接的情況。在網路安全的建立上，應針對 WLAN 客戶端設備使用雙聯接，以及同時連接到多個無線網路的裝置進行規範。

(2) WLAN 的安全監控（WLAN Security Monitoring）

依據 NIST SP 800-153 文件所述， WLAN 的網路安全目標與其他類型網路大致相同。相較於一般網路，WLAN 相對容易被攔截傳輸，並偽裝為一個真實的連網裝置或設備，從中插入或更改傳輸內容。例如有線網路，攻擊者為了監視有線網路上的流量，其必須能夠連接有線網路，或是從遠端破壞網路的系統。倘若是針對 WLAN，攻擊者只需要於無線傳輸範圍內即可進行攻擊與侵害。有些攻擊者甚至可以利用高度敏銳的定向天線（directional antennas），即可將有效攻擊範圍擴大至 WLAN 的標準傳輸範圍之外。

關於 WLAN 遭受的攻擊型態，可分為主動攻擊（Active attack）與被動攻擊（Passive attack）兩種模式。主動攻擊為未經授權的一方，將會主動出現、更改或是中斷 WLAN 的傳輸，例如偽裝（Masquerading）、重複（Replay）、竄改訊息（Message modification）、阻斷攻擊（Denial of service, DoS）；被動攻擊則為未經授權的一方，僅監控 WLAN 的傳輸，而攻擊者不會主動出現、更改或是中斷 WLAN 的傳輸，例如竊聽（Eavesdropping）。

4. 零信任原則（NIST SP 800- 207）

零信任架構（Zero Trust Architecture, ZTA）是一種基於零信任原則的企業網路安全架構，旨在防範資料外洩並限制企業內部的橫向移動（lateral movement）。該架構是一種專注於資源保護的網路安全典範，其前提是所有授權皆必須經過評估，不再有絕對信任的使用者。傳統上，在區分安全性等級時，往往係以「內」與「外」來區隔是否信任，一般的企業或機構網路通常著重於外圍防禦，一旦進入內部網路，經過身份驗證的使用者就能夠存取大量資源。因此，未經授權的橫向移動一直是聯邦機構面臨的最大挑戰之一。在零信任概念中，裝置不再有信賴與不信賴的邊界，例如將不再因內網或外網之別而有信任或不信任的情況，也不再有絕對信任的使用者，而是依據不同的信任判斷依據，進而決定相關權限。

(1) 零信任基本原則：

SP800-207 文件由 NIST 正式發布於 2020 年 8 月，要求任何資源在存取前都要檢查使用者是否有權限，並總結了以下七大原則：

- 所有的資料來源與運算服務都應當作是資源。
- 不論任何網路位置的通訊裝置皆應受到保護。
- 對於個別企業資源的存取要求，應該要以每次連線為基

礎去許可。

- 資源的存取應該要基於客戶端識別、應用服務，以及要求存取資安可觀察到的狀態，以及可能包括的行為或環境屬性，去動態決定。
- 企業監控與衡量所有擁有與相關資訊資產的正確性與安全狀態。
- 在允許存取之前，所有的資源的身分鑑別與授權機制，都要是依監控結果動態決定，並且嚴格落實。
- 企業應盡可能收集有關資訊資產、網路架構、骨幹，以及通訊的現況，並用這些資訊來增進安全狀態。

(2) 以零信任看待網路：

NIST SP 800- 207 建議實施 ZTA 的企業，其內部網路除了根據上述原則，亦應參考以下假設進行開發：

- 整個企業專用網路不被視為隱性信任區域。資源存取應該始終視同攻擊者存在於企業網路中，以最安全可行的方式進行通訊。
- 網路上的設備可能非由企業擁有或配置。
- 所有資源皆非固然可信。在向企業請求資源授予之前，每個資產都必須通過 政策落實點（Policy Enforcement, Point, PEP） 評估其安全狀況。
- 並非所有企業資源都存於企業擁有的基礎設施上。企業擁有或管理的資產可能需要利用區域（即非企業）網路進行基本連接和網路服務。
- 企業不可完全信任其區域網路連接。
- 在企業和非企業基礎設施之間移動的資產和工作流應該具有一致的安全策略和狀態。

5. 行動應用程式的安全性（NIST SP 800-163）

行動應用程式（Mobile applications or apps）為智慧裝置以

及未來達到物聯網、P2M 中重要介面，卻也為接受服務的組織或是用戶帶來安全風險，應用程式（Applications, App）漏洞/脆弱度（vulnerability）可能被用來竊取訊息、控制用戶的設備、消耗硬體資源等。

APP 漏洞可因開發人員有意或無意形成，APP 設計或為強化應用程式的功能性，降低應用程式的安全性，以減少成本和縮短 APP 上架的時間，造成 APP 漏洞 。APP 漏洞造成的風險等級，取決於多種影響因素，其中包括 APP 可取得的數據。另外，仰賴無線網路技術，包括例如 WI-FI、蜂巢式網路（cellular）與藍芽等進行數據傳輸的應用程式，也很可能將具有很高的風險，因為其被視為在技術上可作為遠端使用的操控媒介（Vector）。儘管此類 APP 因其傳輸數據性質被視為低風險應用，但若被刻意利用，也將會產生重要影響。為了減少與行動應用程式相關的潛在風險，應採取軟體認證程序，以確保軟體免受漏洞侵害，提升安全信任，不論漏洞為有意或無意，能於事前進行防範 。在 NIST SP 800-163 審查行動應用程式的安全性（Vetting the Security of Mobile Applications）中，從應用程式安全的要求（App Security Requirements）、審查流程（App Vetting Process）、測試以及漏洞的分類（App Testing and Vulnerability Classifiers）、審查注意事項（App Vetting Considerations），一直到應用程式的審查系統（App Vetting Systems）。每階段依據符合一般性或特殊性組織之安全要求標準為前提，按審查流程與特定工具，進行應用程式的安全性檢核。

6. 物聯網設備的安全性（NIST SP 800-213）

2020 年 12 月，NIST 發布了 SP 800-213 草案文件，其諮詢階段結束於 2021 年 2 月 26 日。該草案旨在促進物聯網網路安全，它與 NIST 內部報告之 NISTIR 8228 及 NISTIR 8259 系列相互參照，主要為聯邦機構提供總體指導，並由設備的角度考慮系統的安全

性，提出聯邦機構在採購物聯網設備時需要考慮的具體問題。依據 NIST SP 800-213 建議，伴隨物聯網發展，機構在部署物聯網設備時應詢問下列具體問題：

(1) 該物聯網設備所帶來的好處是什麼？如何利用它？
(2) 需收集哪些數據？
(3) 數據將藉由哪些技術儲存？
(4) 數據將在哪些地理區域共享和／或儲存？
(5) 來自物聯網設備的數據將與哪些第三方共享和／或儲存？
(6) 該設備是否會干擾其他操作或系統功能？
(7) 物聯網設備是否會給機構帶來不可接受的風險或使其不符合網路安全要求？
(8) 物聯網設備是否有已知的安全和／或隱私漏洞？
(9) 在採取安全控制時，物聯網設備是否存在可預見的挑戰？

另外，此草案也有助於應對 2020 年《物聯網網路安全法》（IoT Cybersecurity Improvement Act of 2020）要求，即提供法律指定的物聯網設備採購、獲取或使用指南，為聯邦政府建立最低安全標準及相關指引。根據該法案要求，聯邦政府應為以政府資金購買之物聯網設備制定標準，如果當使用政府機關所採購或獲取的物聯網設備，未遵守NIST制定的標準或指引，則不得續簽採購、獲取或使用該設備之契約。

二、新加坡

國際電信聯盟（International Telecommunication Union，ITU）發布之全球網路安全指數（Global Cybersecurity Index, GCI）係從網路安全法令、技術部署、組織化、建置能力及國際合作等方面衡量各國網路安全的成熟度。依據 2018 年網路安全指數報告（2018 Global Cybersecurity Index (v3)）指出，全球 GCI 排名前十名之國家，新加坡即排名第 6 名，更是亞太地區排名第 1 名之國家，尤其在網路安全法規

制定方面最為成熟[114]，顯示新加坡在網路安全防護的決心與完備性。

新加坡最早自 2005 年開始，陸續成立網路安全主責機關並推動多項資安政策，其中 2015 年成立隸屬新加坡總理辦公室的網路安全局（Cyber Security Agency of Singapore, CSA），專責新加坡網路安全，包括保護關鍵資訊基礎設施（Critical Information Infrastructures, CII）、處理大規模網路攻擊事件、制定網路安全法規、政策與準則、負責國際網路安全協同合作事宜，及跨部門與跨產業的網路安全處理機關，充分展現網路安全即國家安全之意識[115]。隨著資通訊科技逐步推進新加坡邁向智慧國家的同時，也產生越來越多網路威脅，基此，新加坡總理李顯龍於 2016 年正式發布 CSA 擬定之國家級網路安全策略（Singapore Cybersecurity Strategy）（下稱「2016 年網路安全策略」），此份 2016 年網路安全策略揭櫫未來新加坡的最高資安指導原則，主要提出 4 個關鍵網路安全支柱，分別是：1.建置彈性的關鍵資訊基礎設施（Critical Information Infrastructures, CII）、2.創造更安全的網路空間、3.發展充滿活力的網路安全生態系統、4.強化國際合作夥伴關係[116]。

其中在建置彈性 CII 部分，新加坡政府將與 CII 營運商以及網路安全社群（cybersecurity community）合作，亦從 4 個面向著手強化 CII 之網路安全：

1. 建立基礎服務的保護：實施 CII 保護計畫，強化 CII 組織的網路風險意識，並且將透過增加安全設計（Security-by-Design）準則以解決 CII 上游與供應鏈的網路安全問題。
2. 提升回應網路威脅的能力：透過建立更多的國家網路安全事件應變團隊（National Cyber Incident Response Teams, NCIRT）、強化災難恢復計畫（Disaster Recovery Plans）以及業務持續營

[114] ITU, *Global Cybersecurity Index 2018*, pp.16.28,(2018), available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf(Last visited:Apr. 19, 2020)
[115] 黃彥棻，〔資安周報第 45 期〕新加坡用總理高度揭露國家資安戰略，臺灣呢?， iThome，2016 年 10 月 19 日，https://www.ithome.com.tw/news/109141（最後瀏覽日：2021 年 4 月 17 日）。
[116] CSA, *Singapore's Cybersecurity Strategy*, pp.4-5, (2016), available at https://www.csa.gov.sg/-/media/csa/documents/publications/singaporecybersecuritystrategy.pdf (Last visited：Apr, 17, 2020)

運計畫（Business Continuity Plans, BCP）。

3. 加強網路安全治理以及立法架構：透過制定網路安全法，要求 CII 所有人及營運商確保其系統與網路安全，並且促進與 CSA 合作並由 CSA 提供網路安全資訊，允許 CSA 與監理部門以及受影響方密切合作，及時解決網路安全事件。
4. 使政府系統更加安全：藉由分配政府資通訊科技經費至網路安全領域，加強政府機關的網路情境意識（cyber situational awareness）與網路安全事件之管理[117]。

對此，為落實新加坡網路安全戰略，新加坡政府於 2018 年 3 月通過網路安全法（Cybersecurity Act），該法旨在強化關鍵資訊基礎設施抵禦網路攻擊的防護、授權 CSA 預防並回應網路安全威脅與事件、網路安全資訊的共享機制、為網路安全服務提供商建立輕度管制的架構[118]，提升新加坡 CII 網路安全能量。網路安全法中明確規範 CII 之所有人之權利義務，包括 CII 之所有人須提供 CII 之相關資訊給予網路安全專員、CII 之網路安全事件回報義務、定期進行 CII 網路安全稽核與風險評估，以及 CII 所有人亦可向 CSA 提出申訴等，同時，該法授予 CSA 官員多項權力，包括發布確保 CII 所有人於防護 CII 網路安全應採取之措施準則與執行標準、調查及預防網路安全事故之權力、舉辦網路安全演習等，此外，該法亦針對網路安全服務提供商及個人建立網路安全服務執照要求機制，規範任何人不得在無執照下執行須具備執照之網路安全服務[119]。

此外，基於網路安全法規定，CSA 網路安全專員[120]得發布對於 CII 所有人為確保 CII 網路安全所為之措施準則，強化 CII 之所有人網路安全防護之意識。基此，CSA 依據網路安全法於 2018 年發布「關鍵資訊

---

[117] *Id*. at 8-9.
[118] CSA, Cybersecurity Act, available at https://www.csa.gov.sg/legislation/cybersecurity-act (Last visited：May. 3. 2021)
[119] *Id*.
[120] 依據網路安全法規定，部長可委任公職人員或由部長負責之法定機構中的公務人員擔任網路安全專員。主責新加坡國家整體網路安全，包含 CII 之網路安全維護。

基礎設施網路安全實踐準則」（Cybersecurity Code of Practice for Critical Information Infrastructure）（下稱「CII 實踐準則」）[121]，該 CII 實踐準則適用範圍涵蓋所有產業之 CII，主要規範 CII 之所有人在確保其 CII 之網路安全所必須實施之最低限度保護政策，CII 實踐準則中規定多項 CII 之所有人應遵循之責任與事項，包括：要求 CII 所有人須遵守至少每兩年進行 CII 獨立之網路安全稽核、建立網路安全風險管理框架及網路安全防護之政策標準及指導方針、針對 CII 進行脆弱性評估與滲透測試、制定網路安全事件應變計畫並建立網路事件應變小組（Cyber Incident Response Team, CIRT）架構、制定網路安全意識計畫與網路安全資訊共享程序、制定「業務持續營運計畫」（Business Continuity Plan, BCP）與「災難復原計畫」（Disaster Recovery Plan, DRP），以及參與網路安全演習等。此外，對於 CII 之所有人與供應商之雙方契約中需簽訂網路安全要求，避免供應商存取、處理、儲存、聯繫與操作 CII 之相關網路安全風險。同時，該 CII 實踐準則附件 A（ANNEX A），也針對營運技術系統（OT System）之 CII 所有人訂定相關網路安全要求[122]。

OT 系統已成為日常生活和經濟的科技基礎，如依靠 OT 系統調節交通號誌和鐵路網路，為電網供電以及同步監測感測器，提供供水與其他基本服務。但隨著近年資訊技術（IT）和 OT 系統之間的連結日益緊密，OT 系統之 CII 所有人面臨日益嚴重的網路威脅。因此 2019 年 10 月，新加坡政府發布 OT 系統網路安全總體規劃（Singapore's Operational Technology Cybersecurity Masterplan 2019）（下稱「OT 網路安全總體規劃」），該規劃旨在提升基本部門與跨部門網路安全性與網路威脅應變能力，適用範圍與對象為工業控制系統（Industrial Control

[121] 第一版「關鍵資訊基礎設施網路安全實踐準則」於 2018 年 9 月公布，後針對部分條文進行增修並補充附錄 A（ANNEX A），因此增修後之第二版「關鍵資訊基礎設施網路安全實踐準則」於 2019 年 12 月生效。本文引用之內容為第二版增修後的版本。

[122] CSA, *Codes of Practice Standards of Performance*, available at https://www.csa.gov.sg/-/media/csa/documents/legislation_cop/cybersecurity-code-of-practice-cii-dec-2019.pdf (Lsat visited：Apr, 22, 2021)

Systems, ICS）之 OT 系統以及 OT 系統之 CII 所有人[123]。為增加 OT 系統的網路安全，OT 網路安全總體規劃將透過執行 4 個關鍵重點，強化人、過程以及技術等面向之網路安全性。4 個關鍵重點分別為[124]：

1. 強化 OT 系統的網路安全訓練：由 CSA 學院[125]提供之中級至高級網路安全培訓課程，CSA 學院提供不同專業範疇之課程與處理不同威脅以及攻擊向量（attack vectors）之科技平臺，並提供與培訓者實際日常網路安全工作的訓練環境。藉由網路安全人才的訓練，CSA 學院每年培訓約 70 名至 100 名的 OT 網路安全專家，建立更多安全且具應變能力的 OT 群體（OT community）[126]。
2. 建立 OT 網路安全共享與分析中心：CSA 與亞太地區全球彈性聯盟（Global Resilience Federation Asia Pacific, GRFAPAC）合作，於 2019 年 10 月啟動 OT 網路安全資訊共享與分析中心（OT Cybersecurity Information Sharing and Analysis Center, OT-ISAC）。OT-ISAC 成員來自政府、CII 和 OT 等行業，OT-ISAC 推動成員進行知識交流並採取基本的 OT 網路安全最佳實踐和基準。同時，透過參與研討會或會議，OT 網路專業人士可以隨時瞭解 OT 環境中快速演變的威脅和緩解措施。此外，OT-ISAC 還可提供來自網路情報供應商有關 OT 產業營運的網路事件資訊，同時，亦利用遍佈五大洲的 7,000 多個組織的經驗和專業知識，與新加坡 OT 網路安全利益關係人分享可行的網路情報[127]。
3. 加強 OT 網路安全政策與流程：依據網路安全法規定，CSA 網路安全專員針對 CII 之所有人發布 CII 實踐準則。同時，2019 年 11 月新增一份附件（ANNEX A），提供 OT 系統之 CII 所有人應

[123] CSA, *Singapore's Operational Technology Cybersecurity Masterplan 2019*, pp.1,14-16, (Oct. 01, 2019), available at https://www.csa.gov.sg/-/media/csa/documents/publications/ot_masterplan/csa_ot_masterplan.pdf (Lsat visited：May, 5, 2021)
[124] *Id.* at 3
[125] 於 2017 年成立，旨在為提升政府與 CII 部門抵禦網路威脅的準備、應變以及能力。
[126] CSA, *supra* note 123, at 30-31.
[127] *Id.* at 32-33

遵守之網路安全準則。該份附件聚焦於 OT 系統的網路段（network segment）、修補程式管理（patch management）、偵測與持續監控等面向之網路安全要求，協助 OT 系統之 CII 所有人具備有效且能緩和新興網路威脅的能力[128]。

4. 採用創新技術提供系統彈性：為解決 OT 網路安全解決方案的不足，OT 網路安全總體規劃將推動發展新加坡 OT 產業的創新解決方案，協助終端使用者改善網路安全，並發展創新的網路安全解決方案。CSA 於 2018 年推出共同創新（Co-innovation）以及發展概念驗證（POC）計畫，支持透過種子基金促進計畫與解決方案的產生[129]。

此外，OT 網路安全總體規劃也鼓勵 OT 設備製造商與服務提供者在開發階段實施網路安全，使產品與系統內建強大的網路安全措施。OT 網路安全總體規劃將作為新加玻致力為 OT 系統之 CII 所有人建立具有彈性與安全網路環境之戰略藍圖[130]。

除 CII 與 OT 系統之保護外，數位與智慧化程度越來越高，網路空間的安全也成為新加坡政府注重的一環，基此，新加坡於 2020 年 10 月發布「2020 年更安全的網路空間總體規劃」（Singapore's Safer Cyberspace Masterplan 2020）（下稱「2020 年網路安全總體規劃」），該份網路安全總體規劃主要依據 2016 年網路安全策略第 2 支柱創造更安全之網路空間為基礎，提出三項重點策略[131]，主要從三方面著手：保障核心數位基礎設施的安全、保障網路空間活動的安全、增強民眾網路安全意識與應用能力。

1. 保障核心數位基礎建設的安全：新加坡政府將透過安全設計（Security-by-Design）、採取脆弱性評估（Vulnerability

[128] *Id.* at 32-33
[129] *Id.* at 36-37
[130] CSA, *Singapore's Operational Technology Cybersecurity Masterplan 2019*, available at https://www.csa.gov.sg/news/publications/ot-cybersecurity-masterplan (Lsat visited：May, 6, 2021)
[131] CSA, *Singapore's Safer Cyberspace Masterplan 2020*, p.15, (Oct. 06, 2020), available at https://www.csa.gov.sg/-/media/csa/documents/publications/safer-cyberspace-masterplan-2020.pdf (Lasted visited：May. 25, 2021)

assessments）與威脅獵捕（Threat Hunting）等防護策略保障網際網路架構。同時，提出5G網路安全計畫，提供電信網路安全訓練與提升5G網路安全技能與知識的實驗場域。此外，更新多層雲端安全性（Multi-Tier Cloud Security, MTCS）標準，提供雲端服務提供者或使用雲端服務之企業雲端服務安全性參考標準[132]。再者，藉由提供智慧裝置之網路安全標籤機制[133]（Cybersecurity Labelling Scheme），幫助消費者輕鬆評估智慧設備提供之網路安全級別，同時，鼓勵企業利用國家數位身份（National Digital Identity, NDI）如myInfo與SingPass Login作為企業服務客戶之身份驗證機制，保障企業應用程式安全等[134]。

2. 保障網路空間活動的安全：透過建立資料收集與分析資訊的網路融合平臺（Cyber Fusion Platform），使CSA得以優先篩選網路資訊，警告即將發生的惡意網路活動，增強國家惡意網路活動的偵測與分析能力。同時，CSA將建立物聯網威脅分析平臺（IoT Threat Analytics Platform），使CSA得以將全球物聯網威脅的資訊進行分析。此外，建立網路衛生入口（Cyber Hygiene Portal），該入口將設置在CSA的網頁，並提供網路安全指南、工具包以及網路健康查閱工具，使企業使用者去評估他們的域名、信箱以及網路的健康狀況，促使企業免於網路攻擊。再者，CSA將為安全即服務（Security-as-a-Service, SaaS）解決方案設計一個體系結構，為使用者提高網路安全性，保護使用者免於網路威脅[135]。

3. 增強民眾網路安全意識與應用能力：為企業領導者、企業雇員、

[132] Microsoft Build, 新加坡多層雲端安全性（MTCS）標準，https://docs.microsoft.com/zh-tw/compliance/regulatory/offering-mtcs-singapore（最後瀏覽日：2021年5月25日）。
[133] 係新加坡CSA制定的網路安全計畫，根據管制產品符合的條件可申請四種等級標籤(Level 1~4)，由「製造商/開發商」註冊申請。https://www.intertek-twn.com/FrontEnd/newseventsview.aspx?lang=C&no=1962（最後瀏覽日：2021年5月26日）。
[134] CSA, *supra* note 131, at 18-29.
[135] *Id.* at 30-41.

資安長（CISOs）與網路安全團隊等量身打造專門之資源與工具包，如 CSA 將與英國國家網路安全中心（NCSC）合作推出測試網路能力的新工具「Exercise-in-a-box」（EiaBSG），打造一個安全的環境提供企業在其中得以測試其回應各種網路攻擊之能力，使企業面對網路的惡意攻擊具備更好的應對能力。再者，CSA 透過其 GoSafeOnline 社區擴展計畫（GoSafeOnline Community Outreach Programme），針對民眾於數位領域之活動提供網路安全建議，包括舉辦國家網路安全宣導活動、舉辦在職成年人與年長者網路安全推廣社區活動或會議，以及深入校園為學生舉辦網路安全講座等。此外，新加坡政府也將在 2021 年 4 月提出 SG 網路安全信任標誌（SG Cyber Safe Trustmark），企業用此標誌證明其已預先設置網路安全措施，客戶可依據標誌之級別選擇想要交易之企業[136]。

新加坡政府持續於今（2021）年發布與制定網路安全政策，今年 3 月，新加坡通訊及新聞部（Ministry of Communications and Information, MCI）宣布正在制定 CII 供應鏈計畫（CII Supply Chain Programme），預計提供 CSA、CII 之所有人及其供應商，管理供應鏈之網路安全風險的建議流程與措施。另一方面，於今年 3 月啟動 SG 網路安全計畫（SG Cyber Safe Programme），SG 網路安全計畫是 2020 年網路安全總體規劃的一部份，旨在提升新加坡的總體網路安全水平[137]，該計畫將推出多項網路安全措施與工具，包括針對企業領導者、技術團隊與員工提供網路安全工具包（Cybersecurity Toolkits），使企業領導者與員工深入了解網路安全問題與威脅，以及企業自我評估其網路安全狀況工具（Tools for Enterprises to Self-Assess their Cybersecurity Posture），如「Exercise-in-a-box」（EiaBSG）等工具，使企業擁有可演練網路安全

[136] *Id*. at 42-51.
[137] CSA, Speech by Dr Janil Puthucheary, Senior Minister of State, Ministry of Communications and Information at the MCI Committee of Supply Debate 2021, (Mar.02, 2021), available at https://www.csa.gov.sg/news/speeches/mci-cos-2021-sms-speech (Lasted visited：May. 27. 2021)

事件之工具。另外，CSA 也將推出 SG 網路安全信任標誌等[138]，保護企業與消費端網路安全。

大抵而言，新加坡不間斷推動網路安全相關政策與法規調適，從 CII、網路空間的安全、到整個網路安全生態系統等領域著手，全面性保護新加坡之網路安全。此外，亦透過與國際合作，建立全球網路安全網，積極打造有利新加坡發展智慧國家之網路安全環境。

此外，隨著新加坡逐漸朝向智慧國家邁進，各式物聯網的應用也將越來越多元，其中，物聯網資料保護與網路安全管理成為當務之急。為此，新加坡資通訊媒體發展管理局（Infocomm Media Development Authority of Singapore, IMDA）於 2020 年 3 月 13 日發布物聯網網路安全指南（Internet of Things Cyber Security Guide，以下簡稱「物聯網安全指南」）。此份物聯網安全指南由新加坡 IMDA 與新加坡 CSA 共同制定並完成公眾諮詢，以協助企業及其供應商在採購、開發、實施及維護物聯網系統時，具有標準指引得解決網路安全問題[139]。

物聯網安全指南主要聚焦於系統層面的安全建議，提供物聯網開發者（IoT developers）、物聯網供應者（IoT providers）以及物聯網使用者（IoT users）於物聯網系統實施（implementation）或營運（operational）階段的網路安全基準建議（baseline security recommendations）。物聯網安全指南亦說明物聯網開發者、供應者與使用者在物聯網系統生命週期之業務範圍，物聯網開發者主要參與開發階段之設計、開發、部署、整合（integrate）和測試等。物聯網供應者則參與營運階段之營運、支援（support）、維護、更新與退役等。物聯網使用者主要參與實施和營運階段。值得注意的是，在物聯網系統的整個生命週期內，隨著新功能特徵的導入，可能會出現多種實施和營

[138] CSA, SG Cyber Safe Programme, available at https://www.csa.gov.sg/programmes/sgcybersafe (Lasted visited：May. 28. 2021)

[139] Info-communications Media Development Authority, Internet of Things(IoT) Cyber Security Guide, https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf (Lasted visited：Oct. 9. 2021)

運階段週期[140]。

此份物聯網安全指南以新加坡資訊技術標準委員會（Information Technology Standards Committee, ITSC）TR 64「2018 年智慧國家物聯網安全指南」（Guidelines IoT security for smart nation）（下稱：TR 64）[141]中的概念為基礎，提供網路安全相關基礎概念、威脅建模清單（threat modelling checklist）與供應商自我揭露清單（vendor disclosure checklist）[142]。

依據 TR 64 中提出的四項物聯網安全設計原則，包括預設安全（Secure by defaults）、嚴謹防禦（Rigour in defence）、問責性（Accountability）及韌性（Resiliency）[143]，物聯網安全指南就各原則設定各項安全建議步驟，為物聯網使用者與開發者提供物聯網實施與營運階段的安全基準建議，使用者與開發者可採取這些安全步驟，確保物聯網系統的核心安全級別。各項物聯網安全設計原則下之安全建議步驟如下：

1. 提供物聯網使用者及開發者在實施（implementation）階段的安全基準建議[144]：
   (1) 預設安全：
      A. 採用強大的密碼學：透過強大的加密功能確保物聯網之間的數據交換安全性，物聯網安全指南建議產業允許使用密碼技術並將最佳實踐方式適當的落實在物聯網系統。

---

[140] *Id* at 4.
[141] TR 64 介紹物聯網（IoT）系統的基本安全概念和用語，並展示其應用。同時介紹識別與緩解 IoT 系統威脅和漏洞的整體方法與提供關於如何對物聯網進行威脅建模。此外，還確定四個基本的安全設計原則，以及說明相關的應用。還提供如何分類物聯網安全需求及其在支援安全需求識別方面的使用性。https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Internet-of-Things (Lasted visited：Oct. 13. 2021)
[142] IMDA, *supra* note 139.
[143] Info-communications Media Development Authority, Internet of Things(IoT) Cyber Security Guide Annex A Foundational Concepts, https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide-Annex-A.pdf (Lasted visited：Oct. 12. 2021)
[144] IMDA, *supra* note 139, at 7-9.

B. 保護具影響性的數據：衝擊性數據包括密鑰、憑證、代碼、韌體（firmware）、個人資料、輸入/指令及傳感數據（sensing data）等，存取具影響性之數據應保證或驗證數據真實來源，並防止數據被竄改、修改或向未經授權者揭露。物聯網安全指南建議應檢查具影響性數據的真實性，並防止未經授權者揭露或修改。所有與物聯網裝置傳輸的敏感通訊都應被加密。

(2) 嚴謹防禦：

A. 進行威脅建模（Threat modelling）：威脅建模有助於識別系統的資產、系統資產的安全需求及系統資產可能面臨的威脅。因此，有限的資源則可明確集中用於需要保護的內容。威脅建模將可能暴露的攻擊面最小化，並減輕其餘的漏洞。物聯網安全指南建議實施階段初期應採用威脅建模，並且說明明確的營運環境內物聯網設備的預期用途。

B. 建立信任根（Root-of-Trust）：信任根提供了防止竄改的模組，用於儲存與保護裝置的密鑰，並為其他安全機制建立穩固的基礎，透過信任鏈實現更高的安全保證。物聯網安全指南建議信任根應該由關鍵系統組件建立與使用，例如物聯網閘道器和物聯網平臺，因閘道器與平臺可能主導（host）敏感數據並執行具影響性的營運。

C. 部署安全傳輸協議：系統間傳輸資料時使用傳輸協議，同時確保配置正確的傳輸協議安全版本，保護資料有效的傳輸。物聯網安全指南建議盡可能使用經驗證的傳輸協議並適當的啟動安全控制。

(3) 問責性：

A. 實施適當的存取控制：在系統的整個生命週期中，存取系統資源時應受到控制以及管理，最小化惡意行為者的

機會。預設（default）密碼與脆弱的密碼成為常被利用的漏洞。多重身分驗證（Multi-Factor Authentication, MFA）提供發起端（initiators）身分更高的保證，加強問責性及減少錯誤。物聯網安全指南建議無論是網路（cyber）與實體，對於裝置、網路（networks）以及資料都必須實施適當的存取控制。

B. 提供審計軌跡（audit trails）：即使適當的實施存取控制措施，故意濫用、繞過限制與錯誤配置仍是潛在風險，因此擁有審計軌跡是重要的。物聯網安全指南建議所有試圖存取敏感資料與更改系統資源應適當被監控與紀錄（logged）。

(4) 韌性：

A. 防止資源耗盡：物聯網系統易受資源耗盡攻擊，攻擊者以及受損裝置將持續向物聯網設備/網路/系統發送請求，進而耗盡系統資源及影響系統的使用性。物聯網安全指南建議系統應採取機制，防止如 DDoS 的惡意攻擊。

2. 提供物聯網使用者及物聯網供應者在營運（operational）階段的安全基準建議[145]：

(1) 預設安全：

A. 使用穩固的憑證：脆弱的憑證如使用者的識別以及密碼一直被認為是易受攻擊的漏洞。物聯網安全指南建議避免使用預設的憑證，整個系統應使用強而有力的密碼，並強化密碼複雜度與強度以及遵守國際最佳實踐。

(2) 嚴謹防禦：

A. 區分物聯網與企業網路：單一個被入侵（compromised）的裝置容易使攻擊者進入企業的系

[145] *Id* at 9-10.

統。物聯網安全指南建議網路段是必須要部署的，使物聯網裝置分屬不同網路，可以適當的與其他企業的系統以及網路做區分。防火牆與惡意軟體緩解的解決方案應盡可能地在每一個網路實施。

(3) 問責性：

A. 建立適當的裝置管理：所有連結裝置可能暴露風險並被惡意行為者利用，使網路攻擊入侵整個物聯網系統。被盜的裝置可能使用逆向工程竄改，進而針對整個物聯網系統。過時且未修補程式的防火牆或軟體都被納入惡意行為者已知的可利用漏洞。因此，連結裝置的適當管理是確保整個系統安全的關鍵。物聯網安全指南建議適當的裝置管理包括應建立防火牆與軟體的更新與補充，在整個營運的生命週期中盤點連結裝置、軟體與防火牆的版本，並持續更新，嚴格執行存取控制。物聯網使用者與物聯網供應者應訂閱 IMDA、CSA 官方發布的通知與建議，掌握物聯網與 ICT 系統的最新漏洞與攻擊。

(4) 韌性：

A. 具備修復力：在物聯網資產具一定價值時，物聯網系統將成為攻擊目標。當更多複雜的攻擊工具被開發，攻擊者就會找到入侵系統的方法。因此，應做好從攻擊後恢復的準備，尤其當攻擊者入侵物聯網系統導致人與系統之影響。物聯網安全指南建議採取定期系統資料備份，以及定期的災害修復演練。

B. 進行定期評估：物聯網系統是動態且複雜的系統，由於威脅亦不斷的在變化，因此定期進行滲透測試或漏洞評估降低安全風險。物聯網安全指南建議定期進行物聯網系統的滲透測試或漏洞評估。同時，威脅建模也應被作為漏洞評估的一部分。

此外，物聯網安全報告亦提供威脅建模清單（threat modelling checklist）建議，以作為系統開發者威脅建模的指引，檢視並確保威脅建模過程是否具系統性且正常的運作，同時，威脅建模則用於分析與發現系統漏洞與威脅，並將威脅進行優先排序，再以合適的風險減緩技術解決安全問題。另一方面，物聯網安全報告提供供應商自我揭露清單（vendor disclosure checklist）建議，用以界定物聯網供應者應注意的安全功能與服務，使物聯網使用者在採購時，得以評估與比較不同供應者提供的物聯網解決方案與系統的安全性[146]。

新加坡政府發布物聯網安全指南，係以提供業者得以確認物聯網系統的安全性與降低系統帶來可能的威脅與漏洞，同時，涵蓋物聯網供應者及使用者可能面臨如物聯網安全設計基本原則、用於識別資產的安全影響類別、從網路與物理角度列舉威脅類別、物聯網常見的攻擊類別、系統與設備等不同生命週期的威脅因素以及威脅評估等實際問題。基此，IMDA 鼓勵企業與供應商採用物聯網安全指南，並於設計與開發物聯網系統階段即考量系統的網路安全，始於源頭確保業務免於網路安全威脅與可能帶來的損害[147]。

三、歐盟

2011 年，歐盟啟用新一代的關鍵資訊基礎設施保護計畫（Critical Information Infrastructure Protection, CIIP），並於 2013 年針對網路安全推動綜合性立法計畫，由執委會以及歐盟外交和安全高級代表於同年 2 月提出網路與資訊系統安全指令建議（on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union）；同年，歐盟為了確保網路安全，延引 2016 年公布之網路與資訊系統安全指令

[146] *Id* at 11-17.
[147] IMDA, IMDA Launches IoT Cyber Security Guide to Help Enterprise Users and Vendors Secure IoT Systems, https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2020/IMDA-Launches-IoT-Cyber-Security-Guide-to-Help-Enterprise-Users-and-Vendors-Secure-IoT-Systems (Lasted visited：Oct. 12. 2021)

（Directive on Security of Network and Information Systems, NIS Directive），頒布新的網路安全計畫，名為「開放、安全與可靠的網路空間」(The cybersecurity strategy – An Open, Safe and Secure Cyberspace)，表現出對於網路安全問題的預防、應對以及處理的重視。

至 2020 年，歐盟執委會藉由展望 2020 計畫（Horizon 2020），投入逾 3800 萬歐元，支持多項創新計畫，保護關鍵基礎設施免受網路的威脅，使城市更加智慧和安全[148]；2020 年 12 月歐盟執委會針對歐盟未來 10 年的數位發展，提出「歐盟數位十年網路安全戰略」（The EU's Cybersecurity Strategy for the Digital Decade），以支持塑造歐盟的數位未來（Shaping Europe's Digital Future）、歐洲復甦計畫（Recovery Plan for Europe）和歐洲安全聯盟（EU Security Union Strategy），使歐盟可加強共同抵擋網路攻擊以及網路安全問題之應變與處理能力，確保歐盟公民與企業皆能在可信賴的網路安全環境中[149]。

(一) 網路與資訊系統安全指令

歐盟網路與資訊系統安全指令（The Directive on security of network and information systems, NIS Directive）(下稱 NIS 指令)不僅為歐盟數位單一市場(European digital single market)發展的重要項目之一，亦為歐盟第一個綜合性的網路安全立法，旨在提升歐盟關鍵基礎設施的整體網路安全，並確保達成歐盟具備統一、高標準的網路與資訊系統安全之基本法律框架的目標。

由於網路資訊及系統透過網際網路進行，因此在促進歐盟境內商品、服務和人員的跨境流動，扮演了重要的角色。而具備上述跨境性質的網路資訊及系統，對於歐盟的運作至關重要。在上述條件下，NIS 指令可有助於確保網路資訊及系統的跨境流動與

[148] 國際通傳產業動態觀測，〈歐盟提撥 3,800 萬歐元以保護關鍵基礎設施免受網路威脅〉，08/24，2020，<https://intlfocus.ncc.gov.tw/xcdoc/cont?xsmsid=0J210565885111070723&sid=0K237522717263495777>

[149] Stli，〈歐盟執委會提出《歐盟數位十年網路安全戰略》〉，01/2021，<https://stli.iii.org.tw/article-detail.aspx?no=55&tp=1&i=180&d=8602>

安全[150]。

NIS 指令立法目的為希望透過該指令的規範，以期能夠實現歐盟內部共同的網路及資訊系統的高度安全，改善歐盟內部的運作。NIS 指令定義的網路與資訊系統安全，意指在可信任且健全的網路以及資訊系統情況下，得以確保其網路與資訊系統安全得以阻止破壞其儲存、傳輸、處理之數據，或者該相關服務提供或是透過該網路及資訊系統存取之機密性、完整性以及可用性[151]。

NIS 指令規範的對象為各成員國之關鍵基礎服務營運商（operators of essential services）及數位服務供應商。而被認定的重要部門包括能源、運輸、銀行業、金融市場基礎設施、健康照護部門、關鍵基礎設施以及數位基礎設施等。而 NIS 指令內容涵蓋以下面向如下[152]：

1. 歐盟各會員國必須制定各自的網路與資訊安全政策：即要求歐盟會員國皆須制定一網路及資訊系統安全的國家政策(即 NIS 政策)，做為實現和維護網路及資訊系統安全的框架。歐盟要求其會員國制定之國家政策共分為 7 大項目。包括，一、網路及資訊系統安全的國家政策與優先事項；二、達成國家網路及資訊系統安全政策之目標以及優先事項的管理框架，包括政府機關與其他相關行為者的角色與責任；三、對於網路及資訊安全的預防、回應及恢復相關措施，包括公司部門間合作的認定標準；四、確立與網路及資訊系統安全的國家政策相關的教育、資安意識的提升以及培訓計畫；五、與網路及資訊系統安全的國家政策相關的研究與發展計畫；六、鑑別風險的風險評估計畫；七、各會員國需盤點並確認境內的關

[150] Enisa, "DIRECTiVE(EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concering measures for a high level of security of network and information systems across the Union ", *Official Journal of the European Union*,(2016), p.1
[151] *Id*. p.13-14
[152] *Id*. p.2-30

鍵基礎服務營運商，並建立一份清單。

2. 加強歐盟會員國間的網路與資訊安全的合作策略以及跨境合作：旨在建立一個合作小組，以支持並促進成員國間的策略合作與資訊交流，並建立二者間的信任與信心，確保國家主管機關以及單一聯絡點能履行其職能，且電腦安全事故應變小組能夠進行跨域合作。進一步言之，各成員國必須在不影響部門法規管理的前提下，指名一個國家單一聯絡點，負責協調與網路及資訊安全相關的問題，以及歐盟層級的跨境合作。而歐盟成員國應指名一個或多個負責網路以及資訊系統安全的國家主管機關以及一個國家單一聯絡點。而歐盟會員國也可指名一個或多個現有機關。若成員國僅指名一主管機關，則同時該主管機關亦應為國家單一聯絡點。
3. 建立一個電腦安全事故應變小組：係透過建立電腦安全事故應變小組，針對國家網路與資訊安全事件進行偵測，並向相關利害關係人提供網路與資訊安全風險以及事件的預警、通知以及訊息傳播等，並且透過電腦安全事故應變小組，針對網路與資訊安全風險事件提供風險事件的因應及分析等。另外，亦透過電腦安全事故應變小組提供歐盟各會員國交換資安風險或資安事件之相關資訊的平臺。
4. 建立關鍵基礎服務營運商（operators of essential services）以及數位服務供應商的安全及要求：係針對被納入的監管對象（關鍵基礎服務營運商以及數位服務供應商）提出其應盡之職責以及對於其在網路與資訊安全的要求與規範。

在 NIS 指令中，對於關鍵基礎服務營運商的認定標準主要包含以下 3 個要件，分別為一、提供可維持社會重要或經濟活動之

基本服務；二、仰賴網路或資訊系統供應之服務；三、該服務的提供易受到破壞影響者。除了對於關鍵基礎服務營運商的認定標準有規定之外，NIS 指令亦將數位市場中的數位服務供應商納入監管對象。數位服務供應商涵蓋範圍包括線上市場、搜尋引擎以及提供雲端服務的數位服務提供商，並且具有跨境性質。

NIS 針對上述兩者的規範以及要求，主要有以下三點，包括:一、應當採取適當措施管理資訊以及網路安全風險；二、應對於資訊以及網路安全事件採取適當的預防措施以及將資訊以及網路安全事件的影響最小化，確保關鍵基礎服務營運商以及數位服務供應商可持續提供服務；三、關鍵基礎服務營運商以及數位服務供應商應當向該國主管機關以及電腦安全事故應變小組即時通報具有重大影響的資訊以及網路安全事件。

就本指令對於數位服務供應商的規範，亦談到需於數位服務供應商有義務於規畫資訊以及網路安全的措施以及資訊及網路安全事件發生發出通知，並須將其系統以及設施的安全性、事件的處理與反應、業務管理的持續、資安漏洞的監測、稽核以及測試等國際標準因素納入考量。

另外，為避免對於關鍵基礎服務營運商及數位服務供應商造成過重的財政及行政負擔，NIS 指令規定其規範應與資訊以及網路的風險相稱，並將實施措施的技術列為考量。而歐盟為了鼓勵相關領域中微型[153]及小型[154]數位服務提供商的發展，對於微型及小型數位服務提供商的規範則排除於規定之外。

整體而言，在上述兩者的監管上，NIS 指令提及對於關鍵基礎設施營運商以及數位服務提供商之監管程度差別。由於關鍵基礎設施營運商提供之服務，往往為維持關鍵社會及經濟活動的重

[153] 根據歐盟執委會（European Commission）的建議，微型企業係指員工人數為 10 人以下，且年營業額或資產總額在 200 萬歐元以下的企業。

[154] 根據歐盟執委會（European Commission）的建議，小型企業係指員工人數為 10-50 人之間，且年營業額或資產總額在 200 萬至 1000 萬歐元的企業。

心，因此其遭受風險程度亦高於數位服務提供商。有鑑於此，NIS 指令認為對於關鍵基礎設施營運商的監管程度應高於數位服務供應商。而對於數位服務供應商則採取較為寬鬆的要求，管理網路以及資訊安全的風險。更進一步言之，由於數位服務供應商具備跨境性質，因此，應就歐盟層級採取更為統一之作法，且實施之條款應促進相關措施的規範與實施。

5. 建立不同程度的網路以及資訊安全通報制度：係指針對歐盟會員國關鍵基礎設施營運商以及數位服務提供商對於網路以及資訊安全事件的通報機制加以說明與區別。例如，對於關鍵基礎設施營運商而言，向主管機關或電腦安全事故應變小組即時通報網路以及資訊系統安全事件之基準，為對其提供之服務之持續具重大影響者。因此，判定資訊以及網路安全事件是否產生重大影響之考慮因素為下列 3 點，包括：(1) 受關鍵基礎服務中斷影響的使用者數量；(2) 資安事件的持續時間；(3) 事件所受影響區域的地理分布。

對於數位服務供應商而言，向主管機關或電腦安全事故應變小組即時通報網路以及資訊系統安全事件之基準，為對其提供之服務為具實質影響者。因此，判定資訊以及網路安全事件是否產生重大影響之考慮因素為下列 5 點，包括 (1) 受影響的使用者數量，尤其是本身服務係仰賴該服務的使用者；(2) 資安事件的持續時間；(3) 事件所受影響區域的地理分布；(4) 提供服務受阻的程度；(5) 對經濟及社會活動的影響程度。

綜觀上述 NIS 指所涵蓋 5 大面向，可以看出歐盟對於網路及資訊系統安全的重視，以及對於歐盟內部市場的運作之重要性。由於歐盟過去於關鍵基礎服務營運商以及數位服務供應商仍缺乏於網路以及資訊安全系統的規範及要求，且亦無法透過歐盟層級的方式建立一個全面且有效的通用合作與規範機制。因此，NIS

指令的頒布可有效應對有關網路以及資訊安全的挑戰，並在歐盟層級上透過建立、規劃關於資安規範與要求的最低標準、資訊的交流與合作，以及針對關鍵基礎服務營運商以及數位服務供應商的共同安全要求與規範，促進在歐盟會員國的網路以及資訊安全的資安防護以及應對能力。

(二) 下一代網路與資訊系統安全指令（NIS 2）

1. NIS 2 指令背景

如同前述所及，2016 年歐盟公布了網路與資訊系統安全指令（The Directive on security of network and information systems, NIS Directive）(下稱 NIS 指令)，其不僅為歐盟數位單一市場(European digital single market)發展的重要項目之一，亦為歐盟第一個綜合性的網路安全立法，旨在提升歐盟關鍵基礎設施的整體網路安全，以確保歐盟實現統一、高標準的網路與資訊系統安全之基本法律框架的目標。然而，歐盟卻在實際的執行上面臨了許多困境，造成歐盟內部市場於不同層級上規管的分散，無法一致且統一。

另一方面，隨著數位化與科技的迅速發展，網路威脅與攻擊日趨嚴重，既有的 NIS 指令已無法符合當前以及未來歐盟的網路安全發展，例如一、網路攻擊為全球成長最為快速的犯罪形式之一。根據目前最新預測，到今（2021）年全球勒索軟體造成的損害將高達 200 億美元，為 2015 年的 57 倍。進一步言之，企業將以平均每 11 秒遭受一次勒索軟體攻擊，遠高於 2016 年的平均每 40 秒遭受一次勒索軟體攻擊；二、隨著網路攻擊的增加，全球網路安全的支出亦持續增加。目前全球網路安全市場的市值約 1500 億美元，經預測未來於 2023 年將增至 2080 億美元，並於 2026 年增至 4000 億美元；三、隨著全球新冠肺炎的大流行，加速了全球社會的數位化轉型的同時，卻也加劇數位鴻溝等問題，導致全球網路安全

事件快速增加。歐洲刑警組織亦揭示，歐盟會員國間的惡意網路活動正逐漸增加，網路安全問題儼然已成為歐盟面臨的共同問題；四、隨著物聯網相關技術的發展，預計至 2024 年將投入 223 億臺物聯網設備作為使用，使歐盟重新思考在網路安全領域日益嚴峻的挑戰下，應如何加強對於其公民以及企業的保護，以免於受到網路威脅與攻擊[155]。

綜上，歐盟執委會(European Commission) 於 2020 年 12 月 16 日在公布了歐盟數位十年網路安全戰略（The EU's Cybersecurity Strategy for the digital decade）的同時，為要因應未來日益嚴重的威脅以及網路攻擊的增長，亦提出 NIS 指令的修正草案（Revised Directive on Security of Network and Information Systems, NIS 2 Directive），引入更嚴格的監管措施以及更加嚴格的執法要求，例如整個歐盟的統一制裁，以及提議擴大 NIS 2 規管的範圍，以取代原有的 NIS 指令，進而加強安全要求，並進一步解決資訊與通訊科技(Information and Communications Technology, ICT)供應鏈的安全問題以及同時有效要求更多部門和其他機構等採取措施，以提高歐盟的網路安全水準[156]。

2. NIS 2 內容概要

2016 年頒布的 NIS 指令要求歐盟會員國確保關鍵基礎設施和服務的供應商，採取適當的安全措施管理網路風險並在發生事件時能有保持彈性並因應。因此，其涵蓋四大目標，包含管理網路安全的風險、防範網路攻擊、檢測網路安全事件以及減少網路安全事件的影響[157]。

---

[155] European Parliament, BRIEFING EU Legislation in Progress :The NIS 2 Directive,pp.1-2, available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf (Last visited: Oct.23,2021)

[156] Id.at 1-9.

[157] REDSCAN, *NIS2: what organisations need to know about proposed changes to the NIS Directive*, available at https://www.redscan.com/news/nis2-what-organisations-need-to-know/ (Last visited: Oct.23, 2021)

NIS 2 為了因應近年來的網路安全風險以及未來的挑戰(包括 5G 技術的安全)，以優化 NIS 指令的不足，分別於能力強化(Greater capabilities)、合作（Cooperation）、網路安全風險風險管理 (Cybersecurity risk management)提出新的管理原則，並進一步擴大規管的範圍，內容整理如下[158]:

(1) 能力強化

既有的NIS指令旨在提高歐盟會員國網路安全能力。NIS 2 則提出以下兩項新的方針，包含一、頒布更加嚴格的監管措施和執法措施；二、制定行政處罰規定，包括對於違反網路安全風險管理和通報義務之罰款。

(2) 合作

既有的 NIS 指令旨在加強歐盟層面的合作。而 NIS 2 指令則提出三大改善方針，包括一、建立歐洲網路危機聯絡的組織網路(European Cyber crises liaison organisation network , EU- CyCLONe)，以從歐盟層面協調管理大規模網路安全事件和危機；二、加強歐盟會員國當局間的資訊共享與合作，以加強合作小組的作用；三、建立針對全歐盟新發現漏洞之漏洞披露協調機制。

(3) 網路安全風險管理

既有的 NIS 指令提出基本服務營運商（OES）和數位服務提供商 (DSP)必須採取風險管理，並將重大事件通知其國家當局。NIS 2 指令則提出四大新的方針，包括；一、透過一系列重點措施加強安全要求，包含事件響應和危機管理、漏洞處理和披露、網路安全測試以及有效使用加密；二、加強關鍵資訊與通訊科技(ICT)供應鏈的網路安全；三、企業管理階層對遵守網路安全風險管理措施

[158] European Commission, *Revised Directive on Security of Network and Information Systems(NIS2)*,available at https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2 (Last visited: Oct.23, 2021)

之責任；四、簡化事件通報之義務，並對通報流程、內容和時間表做出更精確的規定。

(4) 範圍

NIS 2 除了從強化能力、合作以及網路安全風險管理面提出新的管理原則，更進一步調整並擴大其規管的範圍。例如，既有的 NIS 指令僅涵蓋衛生保健(Healthcare)、運輸(Transport)、銀行和金融市場基礎設施（Banking and Financial Market Infrastructure）以及數位基礎設施(Digital Infrastructure)、水的供應(Water Supply)、能源(Energy)以及數位服務提供商(Digital Service Providers)。

NIS 2 則擴大其涵蓋的範圍，例如新增公共電子通訊網路或服務的提供商（Providers of Public Electronic Communications Networks or Services）；數位服務，例如社交網路服務平臺和數據中心服務(Digital Services Such As Social Networking Services Platforms and DATA Centre Services) ；廢水和廢物管理(Waste Water and Waste Management)；某些關鍵產品的製造，例如製藥、醫療器械和化學品(Manufacturing of Certain Critical Products such as Pharmaceuticals, Medical Devices, Chemicals)；郵政和快遞服務(Portal and Couriers Services) ；食物(Food)以及公共行政(Public Administration)等。

整體而言，NIS 2 指令的目標是希望能使其規範能影響更廣且更全面，因此，NIS 2 指令除了調整並擴大其規管的範圍外，亦提出:監管措施與制裁，包括對國家當局更嚴格的監管措施以及更嚴格的執法要求，並旨在協調歐盟會員國的制裁制度；更強的安全要求之新的措施，包括事件響應和危機管理、漏洞處理和披露、網路安全測試和加密的有效使用；資訊共享與合作，加強當前 NIS 合作小組在製定新興技術和新趨勢政策方面的作用，並透過建立歐洲網路危機聯絡組織網

路（EU-CyCLONE），增加歐會員國當局之間的訊息共享與合作，並加強營運合作，於歐盟層面對大規模網路安全事件和危機進行協調管理；漏洞披露，建立了一個框架，並用於協調整個歐盟新發現漏洞之漏洞披露，並創建歐盟註冊表；更安全的供應鏈關係，透過要求個別企業解決供應鏈和供應商關係中的網路安全風險，以解決供應鏈的安全問題，並且亦加強歐洲層面 ICT 網路安全[159]。

目前，歐盟執委會已於 2020 年 7 月 7 日啟動了關於修訂 NIS 指令的公眾諮詢，以收集各界對於其實施和未來潛在變化影響之意見。諮詢已於 2020 年 10 月 2 日結束[160]，未來的進展值得我們繼續觀察。

(三) 歐盟數位十年網路安全戰略

2020 年 12 月 16 日，歐盟執委會公布了歐盟數位十年網路安全戰略（The EU's Cybersecurity Strategy for the digital decade），作為與塑造歐洲的數位未來（Shaping Europe's Digital Future）、 歐洲復甦計畫（the Commission's Recovery Plan for Europe）、2020 到 2025 年歐洲安全聯盟（EU Security Union Strategy 2020-2025）、歐盟外交與安全政策的全球戰略（the Global Strategy for the EU's Foreign and Security Policy）以及歐洲高峰會 2019-2024 戰略（The European Council Strategic Agenda 2019-2024）呼應的重要推動戰略[161]。

歐盟數位十年網路安全戰略不僅為歐盟過去網路安全戰略的延續，亦與歐盟執委會主席於 2019 年 9 月在歐洲議會發表年度咨

[159] REDSCAN, *NIS2: what organisations need to know about proposed changes to the NIS Directive*, available at https://www.redscan.com/news/nis2-what-organisations-need-to-know/ (Last visited: Oct.23, 2021)

[160] europarl.europa.eu, *REVIEW OF THE DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS*, available at https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive (Last visited: Oct.23, 2021)

[161] European Commision, "The EU's Cybersecurity Strategy for the digital decade", JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL"(2020),p.4

文演說時首次提出歐洲數位十年（Europe's Digital Decade）相呼應。

過去的網路安全戰略以建立開放、可靠與安全的網路為核心，藉以實現達到網路韌性（Achieving cyber resilience）、徹底減少網路犯罪（Drastically reducing cybercrime）、針對歐盟安全暨防禦政策（Common Security and Defence Policy, CSDP），發展網路防護政策與能力、對網路安全發展出企業性和技術性資源（Developing the industrial and technological resources for cyber-security）以及為歐盟建立一個完整的國際網路空間政策和促進歐盟核心價值等五項目標。[162]然而，由於網路以及資訊系統科技的快速發展，越來越多的與網路相關之關鍵基礎設施處於集中狀態，進而導致關鍵基礎設施遭受的攻擊將造成更加嚴重的後果，而這樣的後果並非所有機構或是企業皆足以應付網路以及資訊安全所帶來的挑戰。因此，歐盟數位十年網路安全戰略旨在解決過去網路安全戰略無法因應現今網路安全發展態勢之不足，並藉此建立一個更安全的網路世界，促進歐盟數位經濟的發展。

因此，歐盟數位十年網路安全戰略從監管、投資與政策面提出三大主軸，包括: 1.韌性、技術主權和領導（Resilience, Technological Sovereignty and Leadership）；2.建立防禦、嚇阻和應變能力（Building Operational Capacity to Prevent , Deter and Respond）；3.透過加強合作促進全球開放網路空間（Advancing a Global and Open Cyberspace）[163]。

1. 韌性、技術主權和領導涵蓋以下幾項目標，包括[164]：
   (1) 彈性的關鍵基礎設施和服務（Resilient infrastructure and critical services）: 為依據網路與資訊系統安全指令

[162] 科技法律研究所，〈為了確保網路安全，歐盟頒佈新的網路安全計畫〉，07，2013，<tli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=6261>
[163] European Commision, "The EU's Cybersecurity Strategy for the digital decade", JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL"(2020)p.5,13,19
[164] Id.p.6-14

（Directive on Security of Network and Information Systems, NIS Directiv 而修訂更嚴格的監管措施，以調整國家監管、執行以及主管機關的能力，減少歐盟內部市場的不一致，進而改善網路與資訊系統的安全，使國家關鍵基礎設施服務能保有網路彈性，並能在科技日新月異、資安事件層出不窮的情況下，不受資安威脅與攻擊。

(2) 建立一歐洲網路安全盾牌（Building a European Cyber Shield）：為歐盟創建一個由人工智慧（AI）主導之資安監控中心（AI –enabled Security Operation Centres），以及時避免網路攻擊。

(3) 超級安全的通訊基礎設施（An ultra-secure communication infrastructure）：歐盟衛星通訊是太空計畫的一環，其將提供安全且具成本效益的太空通訊能力，以確保歐盟及其會員國具有安全的通訊基礎設施之營運。再者，歐盟會員國亦與歐盟執委會達成共識，部署量子通訊基礎設施（Quantum Communication Infrastructure, QCI），為歐盟會員國的公部門提供一種全新超安全的加密方式傳遞機密訊息，以抵禦網路攻擊。因此，量子通訊基礎設施將涵蓋兩大重點，包括 1.現有的地面光纖通訊網路，可進行跨國連接；2. 承接前述，其可連接太空衛星之範圍遍及整個歐盟地區（包括其海外領土）。因此，透過建構上述超級安全的通訊基礎設施，可開發和部署一更加安全的加密新方式，並設計一套保護關鍵基礎通訊和數據的新型式，確保機敏資訊的安全，並保護關鍵基礎設施的安全。

(4) 保護下世代行動寬頻網路（Securing the next generation of broadband mobile networks）：歐盟在歐盟網路與資訊安全局（European Union Agency for Network and Information

Security , ENISA）的支持下，於 2020 年 1 月與歐盟 5G 工具箱（EU 5G Toolbox）共同建立一基於客觀、全面與風險的 5G 網路安全方法，以鞏固其 5G 能力，並建立永續且多元的供應鏈。

(5) 安全的物聯網（An Internet of Secure Things）: 在現今物聯網的蓬勃發展下，網路以及資訊安全漏洞無所不在。因此，歐盟執委會將會考慮採用新規則，改善歐盟內部市場所有聯網產品以及相關服務的網路安全性。因此，歐盟透過新規則制定物聯網設備製造商的新義務，以解決軟體漏洞問題，包括軟體的運作與更新，以及在產品結束使用時，確保已刪除個人和其他相關機敏資訊。

(6) 完善全球網路安全（Greater global Internet security）: 探討 DNS 於全球網路安全環境中之使用情況。歐盟執委會欲針對影響全球 DNS 系統完整性以及可用性的極端情況，建立一應急計畫，並透過與其會員國、ENISA、兩個歐盟 DNS 根伺服器營運商與多方利益相關者（multi-stakeholder）共同合作，以確保全球 DNS 可以正常運作。再者，歐盟執委會亦希望透過公共的歐洲 DNS 解析器服務（a public European DNS resolver service）的開發，建立一安全的網路環境，並且藉由 DNS4EU 計畫，建立一個透明、符合最新安全標準、數據以及隱私保護準的 DNS 環境。

(7) 加強科技供應鏈的存在感（A reinforced presence on the technology supply chain）: 歐盟透過 2021 至 2027 年間多年期財務架構（2021-2027 Multiannual Financial Framework）為網路安全數位轉型提供資金與支持。因此，歐盟得以藉由多年期財務架構的協助，推動其產業策略以及橫跨數位供應鏈上在數位科技以及網路安全的

領導及影響力，包括數據和雲、下世代處理器技術（Next generation processor technologies）、超安全接取（ultra-secure connectivity）以及 6G 網路。另外，歐盟執委會亦透過制定專門的網路安全研究計畫，進行網路安全的研究與創新，並持續透過 ENISA 和 Europel 對網路安全的研究，以及支持在歐盟展望（Horizon Europe）計畫內的網際網路創新者，研究下世代網際網路計畫的軟體以及硬體之開發，以增強通訊技術的隱私保護與安全。

(8) 增強歐盟公民的網路安全技能（A Cyber-skilled EU workforce）：歐盟為了增進公民的勞動力素質，並且培養、吸引以及留住優秀的網路安全人才，並且對網路安全和創新進行投資，以培養抵擋網路安全的實力。因此，歐盟透過修訂的數位教育行動計畫（The Revised Digital Education Action Plan），提高孩童、年輕人以及中小企業（SMEs）對於網路安全的意識，同時鼓勵歐盟女性公民參與科學、科技、工程、數學（STEM）[165]的教育，以提高歐盟公民的數位技能與能力。再者，歐盟各網路安全相關機構或組織，亦應整合資源，相互合作。

2. 建立防禦、嚇阻和應變能力涵蓋以下幾項目標，包括[166]：

(1) 建立一個聯合網路單位（A Joint Cyber Unit）：歐盟執委會以及其會員國合作共同成立一個新的聯合網路單位，作為歐盟境內不同網路安全群體合作的平臺，以對重大跨境網路事件以及威脅進行協調與處置。加強歐盟各機構與會員國針對網路安全事件以及威脅可以進行預防、遏止以及處理等的合作。另外，聯合網路單位不僅並不

[165] STEM 是代表科學(Science) 、 科技(Technology) 、 工程 (Engineering)及數學(Mathematics)各英文譯寫的首字母縮略詞。 推動 STEM 教育是配合全球的教育趨勢，以裝備學生應對社會及 全球因急速的經濟、科學及科技發展所帶來的轉變和挑戰。

[166] European Commision, “The EU’s Cybersecurity Strategy for the digital decade”, JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL(2020)p.14-20

會以一個額外的獨立機構成立，而且亦不會影響會員國國家網路安全機構或歐盟其他參與者的權限。

(2) 解決網路犯罪（Tackling cybercrime）：由於是否能有效回應與處裡網路犯罪為確保網路安全的關鍵因素。因此，歐盟透過與執法部門之間的合作與交流，可查明和起訴犯罪者。例如，歐洲刑警組織（European Union Agency for Law Enforcement Cooperation, Europol）已和 ENISA 建立合作關係，共同打擊犯罪。另外，針對 DNS 的網路議題，歐盟也將針對 DNS 涉及之議題處裡之。

(3) 歐盟網路安全外交工具箱（EU cyber diplomacy toolbox）：透過歐盟網路安全外交工具箱，對於影響甚大的網路攻擊，例如影響關鍵基礎設施、供應鏈、民主機制等的網路攻擊，進行預防、遏止、應付以及處理。

(4) 提升網路安全防護能力（Boosting cyber defence capabilities）:歐盟應持續致力於最新網路安全防禦能力的發展，尤其是關鍵技術的開發和運用，例如人工智慧、加密以及量子運算，並進一步鼓勵歐盟會員國充分運用常設合作結構（Permanent Structured. Cooperation, PESCO）和歐洲防衛基金（European Defence Fund; EDF）。

3. 透過加強合作促進全球開放網路空間（Advancing a Global and Open Cyberspace），包括[167]:

(1) 促進歐盟在網路安全的標準、規範以及架構的領先地位（EU leadership on standards, normsand frameworks in cyberspace：歐盟須確保其在網路安全的國際標準中的領導地位以及影響力，以確保第三國推行的標準與歐盟的價值觀相違。因此，在人工智慧、雲、量子運算

[167] *Id*.p.20-24

（quantum computing）以及量子通訊（quantum communication）的快速發展下，歐盟應致力於制定符合歐盟價值的新興科技技術和往寄望路體系結構面的標準，確保網際網路標準可維持全球性與開放性；並同時確保新興技術仍以人為本且注重隱私；並且亦可合法、安全與符合倫理道德。

(2) 與合作夥伴以及多方利益相關群體的合作（Cooperation with partners and the multi-stakeholder community）：歐盟需加強及擴大與其他區域組織以及第三國的網路對話，並促進交流以及合作；歐盟應針對共同關注之網路安全議題，尋求共同立場以及達成共識。

(3) 加強全球對於網路安全的抵禦能力（Strengthening global capacities to increase global resilience）：整體而言，歐盟應協助其合作夥伴增強網路安全能量，促進全球的網路安全發展，建構網路安全的抵禦能力，並對於網路犯罪得以調查以及起訴，同時應付及處裡網路安全所造成的威脅等。

總的來說，歐盟數位十年網路安全戰略為歐盟針對未來 10 年推動的數位政策之一。而這項歐盟數位十年網路安全戰略之目的在於解決過去網路安全戰略無法因應現今網路安全發展態勢之不足，並藉此建立一個更安全的網路世界，促進歐盟數位經濟的發展。因此，歐盟數位十年網路安全戰略以監管、投資與政策為主軸，透過韌性、技術主權和領導；建立防禦、嚇阻和應變能力；加強合作促進全球開放網路空間來實現歐盟網路安全的健全環境。

(四) 歐盟 GDPR 對於 WHOIS 資料庫的影響

由於雲端運算、物聯網、大數據等資訊科技的快速發展，使科技為個人資料保護帶來了相較以往更多的衝擊與影響，歐盟個人資料保護規則（the EU General Data Protection Regulation,

GDPR)，對個資保護採取了相當嚴格的規定，包括對於有關個人資料的蒐集、儲存以及利用。在 GDPR 的規範下，國際上對於 ICANN 的 WHOIS（全球域名註冊查詢系統）資料庫管理上，採取資料公開的態度開始有所質疑，進而影響到 ICANN 的 WHOIS 資料庫系統運作。因此，若從長遠的角度，本計畫進行 DNS 編碼政策研析，勢必須考慮若介接至外網，會與 WHOIS、GDPR 以及 ISO 規定之相容度。

WHOIS 為全球域名註冊的查詢系統，結構上如同目錄，內容包含了全球網域名稱的聯絡人與網域技術設定的相關資料。在歐盟 GDPR 尚未實施前，於 WHOIS 可查詢網域名稱相關聯絡人的公開資料，例如電子信箱、電話號碼以及真實地址等。亦即，除了國家或地區的頂級域名（Country Code Top-Level Domain, ccTLD）對於要公開的資料有各自的規範外，由 ICANN 管理的通用頂級域名（Generic Top-Level Domain, gTLD）必須公開域名聯絡人的姓名、地址、電話以及電子信箱。

然而，隨著 GDPR 的正式實施，國際組織 ICANN 早已多次被歐盟資料保護相關單位警告違法，惟 ICANN 雖認為 WHOIS 有改革的需求，惟其社群內各利害關係團體對於如何改革 WHOIS 始終無法達成共識，使 ICANN 組織、gTLD 註冊管理機構與受理註冊機構均可能面臨違反 GDPR 的巨額罰款。

因此 ICANN 轄下負責制定 gTLD 政策的通用域名支援組織（General Names Supporting Organization, GNSO）理事會，於 ICANN62 會議期間決議成立通用頂級域名註冊資料臨時條款（EPDP on the Temporary Specification for gTLD Registration Data, EPDP)。由 EPDP 工作小組於 2018 年 8 月著手進行，並於 2019 年 2 月完成第一階段的執行工作，並於同年 5 月由 ICANN 董事會決議通過大部分的條款內容。爾後同年 5 月 20 日，ICANN 全面實施 gTLD 註冊目錄中繼政策（Interim Registration Data Policy for

gTLDs），遂開始階段式實施新 RDS 政策(即新 WHOIS 政策)做法。

針對 ICANN 因應 GDPR 實施後對於 WHOIS 的改革，ICANN 在資料蒐集、儲存與利用相關規定，受理註冊機構應向註冊人蒐集的資料、受理註冊機構應傳輸至註冊管理機構的資料以及註冊管理機構及受理註冊機構應傳輸至資料代管方的資料，提出建議。其中對於受個資保護影響爭議最劇的一項建議，即受理註冊機構應蒐集的註冊人資料，例如域名註冊人所屬的組織、傳真號碼、技術人員聯絡資料（例如姓名、電話、電子郵件信箱）等資訊，均以選擇性填寫。因此，註冊人可以有權選擇不提供上述相關涉及個人的聯絡資訊，且過去 WHOIS 蒐集的註冊人管理人員（admin）資料完全取消，不應再予以蒐集。意即，WHOIS 的註冊目錄未來將更新其功能，其註冊目錄服務僅能揭露註冊人的所在國家與州/省，且未來也將以匿名電子郵件信箱或網路表格取代註冊人的電子郵件信箱，同時該匿名電子郵件信箱不得與有可與註冊人連結之單一特殊性。

EPDP 第一階段的工作告一段落後，第二階段的工作已於 2019 年 5 月展開。第二階段工作主旨為建立標準化存取模式（Standardized Access Mode, SAM)，意即過往所謂的統一存取模式（Unified Access Model, UAM）。該工作階段的主要目標係以針對具合理事由的揭露要求，提供相關的註冊資料欄位，建立標準化機制。並且，後續也會處裡例如存取模式可能牽涉的法律問題；如何限制或分類使用者；揭露/存取資料的流程方式；如何處理使用者的驗證(Accreditation)/認證（Authentication）等。

另外，EPDP 也針對第一階段尚未有共識且未解決的問題，於第二階段進行後續的處理。例如，是否區分註冊人為法人或自然人；公開註冊資料中是否顯示附屬/驗證 privacy/proxy 服務提供商；是否揭露註冊人所在城市等資訊。

綜觀 EDPD 兩階段的工作內容，第一階段的任務主要為評估

通用頂級域名（gTLD）註冊數據（即 WHOIS 數據）的規範，確保其符合歐盟 GDPR 的規範。第二階段主要是制定標準化訪問非公開註冊數據系統的政策。

由於考慮本計畫在推動 DNS 編碼以及往後可能介接至 WHOIS 時，須考慮相關機制均需符合 ISO27701 以及歐盟 GDPR 的規範，方可建立一網路切片與 DNS 物聯網的編碼機制，以符合各項國際上對於資訊安全與個資的保護要求。

四、我國

我國為資通訊產業主力國家，政府長期以來在大型國家政策推動上，亦相當著力於促進新世代行動寬頻與網路創新應用服務蓬勃發展，因此，針對下世代網路的發展，我國在整體資通安全法制上可先由我國資安法制及電信管理法制等面向加以探討。

(一) 資通安全管理法

資通安全管理法（以下簡稱資安法）是我國整體資安維護的基礎法制，主要目的在於，由政府提供資源，整合民間及產業力量，提升全民資通安全意識，以提升我國資通安全環境，政府也應建立資通安全軟硬體技術規範、相關服務與審驗機制之發展。資安法的規範對象為公務機關及特定非公務機關，公務機關原則上即指政府各部門，而特定非公務機關則主要指關鍵基礎設施提供者。

研究團隊認為，在下世代電信網路的想像下，電信業者在通訊建設的角色上，即便於未來資訊社會的發展，也仍將持續扮演不可或缺的角色，其關鍵基礎設施提供者的重要性也將更為提升。依據資安法第 16 條規定，關鍵基礎設施提供者需向主管機關提出資通安全維護計畫，以確保其資安能力；並依據資安法第 18 條，因應可能發生的資通安全事件，訂定通報及應變機制。

ITU 所提出之下世代網路願景中，電信產業不僅提供傳統電

信網路服務，更將與創新垂直應用整合，因此對國家與社會之影響，比傳統電信網路更為深遠，電信網路做為國家重要關鍵基礎設施，未來仍必然受資安法的規範，以維護、監督關鍵基礎設施的資通安全。而在未來的資安議題關注的焦點，也非僅指如4G或5G 網路的特定技術服務，而係電信產業整體營運、人員以及組織等部分均需有相應的資安準備，換言之，對於電信產業關鍵基礎設施的思維，將會從現在偏向技術面的重心，轉向以服務敏感性、重要性來評估。

故未來，例如資安法施行細則第 6 條列出 13 款事項，要求業者必須記載於資通安全維護計畫中，後續的執行與實施狀況，並需接受目的事業主管機關的稽核，也必須改善缺失與不足之處，可說是對於業者事業營運整體性的資安維護要求，也將隨著網路架構更加朝以服務為本（Services Based）而改進。

(二) 電信管理法

「電信管理法」為我國通訊傳播產業管制的新法規基礎，其對於電信事業之資安亦有相應之規範。電信管理法於第 15 條明訂「...使用電信資源...之電信事業...應訂定資通安全維護計畫...」，並於第37條至第45條規範有關電信網路管理及安全維護等事項，將資通安全責任列為業者重要義務。未來主管機關即能據此督促電信業者善盡資安防護責任。

與此同時，電信管理法由於大幅度解除電信事業管制，隨著創新服務與新網路技術的發展，電信市場結構也將面臨調整。相較於電信法，電信管理法大幅降低市場進入門檻，允許電信業者有更大的營運空間與其他產業進行業務合作，例如新進業者可租用既有業者之網路基礎設施，並整合自身之設備提供新型態服務。因此，對於下世代網路技術發展而言，電信管理法的通過可促成更多前瞻的垂直應用服務的業者與電信業者合作，並利用創新網路架構提供服務，不同垂直應用業者與電信業者的合作、或甚至

垂直應用業者成為新電信業者，將使資通安全管理更加複雜，因為不同的業者所應受管制的程度也不同，未來在資通安全管理上將需要更為細緻化的規範。

其次，當前垂直應用的推展與網路切片的應用，已可初步觀察到如本章第一節的討論，異質網路的整合、多元的服務與資料交互傳遞的需求，均使網路架構更為複雜，不僅於網路建設時便應確保符合安全標準，甚至在未來的營運上，也必須持續不斷的針對網路安全加以關注與更新。

第三節　下世代電信號碼管理系統安全及跨網互通安全策略

一、下世代電信號碼管理系統建置需求

由前述章節可瞭解到，ITU 所提出的 Network 2030 已擘劃出下世代網路的基本圖像，以及國際間如何因應新形態網路技術與網路拓樸所提出的前瞻政策框架與技術規範。於電信網路號碼層面，當未來網路環境將持續朝著基礎設施逐漸 IP 化、AI 化，物聯裝置、路由設備移動性（mobility）增加、固網、行網、乃至太空網路透過技術整合的方向發展，故在網路識別碼層面上，無論是在既有的 E.164 與 E.212 編碼的持續使用與強化，或是新型態編碼如 NDN（Named Data Network）、DOA（Digital Object Architecture）/DOI（Digital Object Identifier） 的提出，其需求與功能均為了因應未來網路特性持續演進。其中，屬於網路識別碼的域名系統（Domain Name System, DNS） 編碼曾被國際電信聯盟 （International Telecommunication Union, ITU）、ICANN（The Internet Corporation for Assigned Names and Numbers）等國際標準組織認為因應未來網路需求的選擇。

本計畫選擇 DNS 編碼作為下世代電信號碼管理系統之原因，其一為網際網路運作的關鍵基礎，具備極大的編碼命名空間；其二為 DNS 所具備的相容性，於基礎建設普及程度高，其三也是主要的原因，在於 DNS 在 DN/IP 的轉換機制是以身份資料為中心的運作邏輯，包括域名之識別/解析、存儲、註冊，與過去 ITU-T X.1255 文件曾定義過身分管理資訊框架（Framework for discovery of identity management information）相近，故可因應 5G 虛擬化網路的資源管理需求，同時也可因應物聯網之大量裝置識別，設計自動化編碼與管理機制。然而 DNS 機制的運作低延遲的性能優點，亦造成其原始通訊安全性較低，因此在未來網路規模擴大以及各項網路服務越加多元後，將面臨更多的安全威脅。因此，在重視 5G 網路安全之同

時，亦須強化 DNS 的系統安全，以利於完備未來以 DNS 運作為基礎的整體網路環境。

故本計畫聚焦在觀測 DNS 安全性需求，其一在於預防潛在之資安漏洞受到利用，致使重要資料被竊取，為此，需對 DNS 的查詢與回應加上安全防護，保護 DNS 主機之間的資料傳遞，並驗證資料來源與資訊內容的可信度。就整個資訊安全管理系統（Information Security Management System, ISMS）層面，對於組織安全防護的審視與流程改進方面，本章擬參考 ISO 27001 資安認證標準關於資安防護的指引框架及控制措施。ISO 27001 給予明確的管理流程，其計畫、執行、查核、行動之程序可提供本章建立資安稽核機制之參照，透過識別系統威脅及建立量測機制，制定風險處理和改善措施，以強化資安防護、保護資訊資產，並且適用於各類型產業；而為因應針對 DNS 系統之技術開發、維護、安全應用至智慧化與物聯網應用的產業層面，本章則參考其他技術與工業控制系統標準，例如 IEC62443 ，藉由工業自動化和控制系統安全規範協助資產所有者、系統整合商、產品供應商進行檢核查驗及風險管理，達成系統所需的安全等級要求。等作說明。

在敘明 DNS 系統安全如何防範外部攻擊，避免功能運作遭到癱瘓，之前，本計畫先針對觀測 DNS 管理系統建置之整體網路環境的資訊安全需求進行檢視：透過 3GPP 於 2018 年發布之 TS 33.501 v.17.2.1 與 TS 33.811 文件，盤點 5G 網路系統、5G 網路切片的潛在風險為先。

基此，本計畫將從既有網路與下世代網路安全需求差異出發，研析 5G 網路、5G 網路切片、接著說明 DNS 現階段的資安需求與相應的解決方案。再者，為因應下世代號碼管理系統開發建置、以及未來之應用之資訊安全管理系統導入，本計畫將參考現行國際資安稽核標準機制，例如 ISO 27001 以及 IEC 62443，與 IEEE 的 DNS 稽核框架，以瞭解未來此 DNS 編碼機制於兩項國際標準之適用範圍，

進而劃定稽核範圍、識別資安風險、評估資安風險、產出稽核計畫並訂定稽核程序，研擬出適用於下世代電信網路號碼稽核指引框架。針對本計畫產出之指引與稽核框架，範圍初步劃定為因應未來物聯網垂直應用之驗證，如 5G 網路及 5G 網路切片支援智慧製造場景。

綜言之，就 5G 網路、5G 切片及未來的物聯網、智慧製造應用場景，建立相關風險分析、風險說明、監控與改進之指引與稽核框架，提供政府機關與企業在對供應鏈或委外廠商管理時參考，並列入合約要求。

二、既有網路與下世代網路安全需求差異

雖然短期內既有網路尚未全面拓展至固網、行網與太空網路連接的立體通訊環境、全息投影技術應用亦尚未成熟，但現階段5G技術與人工智慧、物聯網應用已日趨顯著，物聯裝置的大規模成長將使得網路節點增加十倍至百倍，但也由於裝置數量大量增加，未來將伴隨新型態網路安全隱憂。在垂直應用場域層面，包括智慧城市、智慧製造、智慧醫療、智慧交通、擴增實境（Augmented Reality, AR）、虛擬實境（Virtual Reality, VR）等皆是未來物聯網技術產業發展之潛在方向；企業不論於智慧製造的自動化系統、遠端操控、AR/VR 應用等，對於資料傳輸、存儲、安全的需求也將隨著5G網路性能隨之提升。

換言之，5G 時代的資安問題將不再侷限於消費者隱私和個資風險，更對於企業經營甚至政府機構之資料治理（data governance）產生重要影響。5G時代的網路功能虛擬化（NFV）與軟體定義網路（SDN）技術，5G核心網路已有「IP化」趨勢；加上多邊緣運算系統的發展、DNS 很有可能作為無線接取（wireless access）控制的重要樞紐，本來發生於資訊網路之風險也將連帶影響到電信網路，故以往於網際網路討論的資安問題，未來也可能成為電信網路之資安問題。如何識別潛在的資安威脅、建立相應之防護機制逐漸受到各國重視，包括歐盟、美國、英國、日本等陸續提出 5G 資安報告，

研擬 5G/B5G 資安規範及配套措施，以確保健全的數位發展環境。

其實無論是 5G 或 B5G 資訊安全，皆建立於 4G 資訊安全之基礎，惟 5G 之網路與技術特性是 4G 時代並未產生，基此，本計畫依序說明 5G 網路、5G 網路切片技術安全需求，並針對解決方案做初步分析。

(一) 5G 網路安全

針對 5G 網路安全之技術需求，3GPP 技術規格-服務與系統第三小組（Technical Specification Groups- Services &Systems Aspects, TSG-SA3）於 2018 年發布之 TS 33.501 v.17.2.1 文件（下稱 33.501 文件），歷經 R15、R16 多次變更申請（Change Request, CR），於今（2021）年 7 月發布最新的 R17 變更申請文件。33.501 文件之規範內容主要針對 5G 系統之網路安全架構，以及 5G 系統執行的安全程序訂定技術標準，並提供相應之 5G 資安場景作為補充說明。

於網路安全架構層面，5G 系統包括 5G 核心網路、5G 新無線電（New Radio, NR），33.501 文件將 5G 系統分為傳輸層（Transport Stratum）、所屬層（Home Stratum）與服務層（Serving Stratum）及應用層（Application Stratum）詳見圖 3-4。

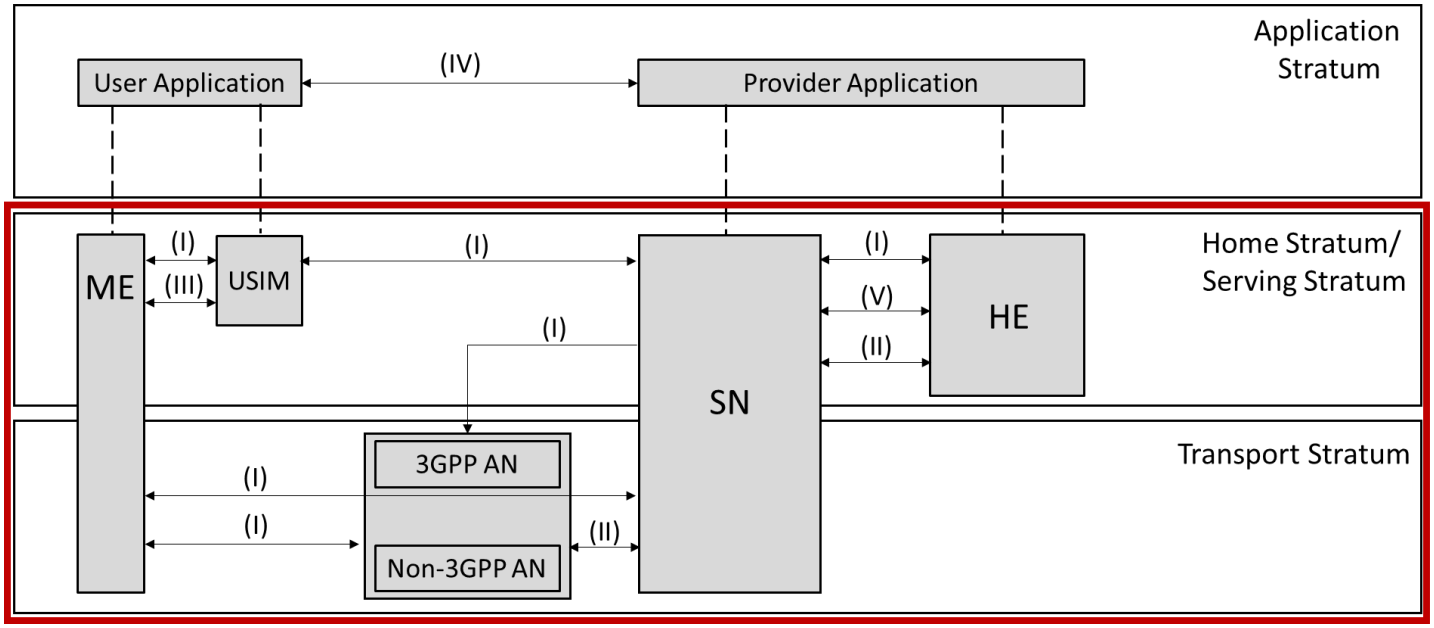


圖 3- 4、整體安全架構圖

資料來源：3GPP, TS 33.501

架構圖中各層均有所屬之功能元件與負責功能，各元件係於3GPP其他技術文件定義；亦有功能元件的部署是跨越層級，但隸屬於同一系統範圍，例如屬於5G核心網路的部分功能元件，像是用戶平面功能（User Plane Function, UPF）被配置在傳輸層，部分像是接取和移動性管理功能（Access and Mobility Management Function, AMF）、網路存儲功能（Network Repository Function, NRF）、安全邊緣保護代理（Secure Edge Protection Proxy, SEPP）等元件被配置於服務層，其他系統範圍之對照詳見表 3-4。

表 3- 4、5G 網路系統範圍對照說明

英文簡稱	英文全稱	中文	說明
ME	Mobile Equipment	移動裝置	即使用者移動終端裝置
USIM	Universal Subscriber Identity Module	通用使用者識別模	包含IMSI（或SUPI[168]），及其他身分驗證

[168] Subscription User Permanent Identifier 之簡稱，為 5G 永久使用者標示，其類似於 LTE 中的 IMSI，為保護 SUPI，將由 SUPI 產生 SUCI(Subscription Concealed User Identifier)，形成公鑰，達到基礎的使用者身份保護。

英文簡稱	英文全稱	中文	說明
		組	工具。
AN	Access Network	接取網路	使用者裝置可接取的網路。
SN	Serving Network	服務網路	屬於使用者裝置的網路
HE	Home Environment	所屬環境	包含使用者配置檔案、識別符號和訂閱資訊之資料庫，即使用者訂閱之網路。

參考資料：本計畫整理

另一方面，33.501 文件根據架構中各功能元件之運作模式，定義出 6 種安全特性，稱作安全域（security domain），包括：

A. 網路接取安全（Network access security）：使終端裝置（User Equipment, UE）可通過認證，安全接取網路服務。
B. 網路域安全（Network domain security）：使網路節點能夠安全地交換信令資料（Signaling Data）和使用者平面資料（User Plane Data）的一系列功能。
C. 使用者域安全（Use domain security）：確保使用者接取移動裝置和移動服務的一系列功能。
D. 應用域安全（Application domain security）：確保使用者與服務提供者之間的訊息能安全地傳遞的一系列功能。（不在此文件討論範圍）
E. 基於服務體系架構安全（SBA domain security）：SBA 域中的一系列功能，包括網路功能註冊、發現和授權，以及對 SBA 介面的保護。
F. 可見與可配置之安全性（Visibility and configurability of security）：告知使用者一系列安全功能有在運行。

如何實現上述各功能元件之安全需求，以及功能元件運作之安全，為文件內容之兩大核心。所有的功能元件皆通用之安全需求為：緩解降階攻擊（Bidding Down Attack）；服務網路與訂閱認

證；使用者裝置授權；服務網路向歸屬網路取得授權；允許未經認證之緊急服務。

除了各功能元件本身之安全需求，功能元件運作之安全可分為：UE 至 3GPP 定義下之 5G 網路系統、UE 至非 3GPP 定義之 5G 核心網路接取、以及其他如互連（internetworking）、跨多個服務網路、網路切片管理安全、網路切片程序等安全程序討論。

若從下世代電信網路號碼之功能觀之，依據不同的使用技術及服務需求的不同劃分為實體層與邏輯層，實體層可以提供高級通訊功能，達到低延遲、高頻寬、高覆蓋率和大規模連接；邏輯層則透過網路虛擬化和網路切片來支持多樣化、高效能和低成本的服務。基此，5G 網路安全性研究可以分為兩個面向：一是實體層安全性（5G 實體層），藉由各項實體技術提供加密、認證、密鑰分發和管理等功能，即根據 3GPP 於實現 5G 安全所定義之金鑰階層管理框架；二是邏輯層安全性（包括 5G 虛擬層、服務層以及應用層），聚焦於網路功能虛擬化（NFV）和軟體定義網路（SDN）之安全性，例如認證憑據儲存和處理功能（Authentication Server Function, AUSF）、認證和金鑰協議（Authentication and Key Agreement, AKA）、等虛擬功能元件，在資安威脅或攻擊產生時進行安全性隔離，此外亦以及確保切片間通訊之安全性、配置錯誤、虛擬化威脅、虛擬機監控程序劫持等，提高 5G 整體之安全結構。換言之，在 5G 認證安全機制中，可透過 AUS 支持 5G-AKA 機制，經由本地網路完成最終身分認證，由此改善 4G 認證安全機制的弱點，亦是往後提升 5G 安全性之關鍵。

在實體層上，由於無線通訊的開放性所引起的竊聽攻擊和未授權存取是兩個主要挑戰，可透過加密和授權機制解決。在邏輯層上，對實體資源進行虛擬化和切片以支援服務，則存在三個主要的安全挑戰：一是共享資源引起的資料外洩；二是硬體、軟體和協議的漏洞；三是外部安全威脅，如阻斷攻擊（DoS）、分散式

阻斷攻擊（DDoS）和中間人攻擊（MITM）等外部攻擊。

總的來說，5G 系統在架構設計上具備強大擴充彈性功能，得以因應未來各種潛在新興應用服務，例如導入接取網路之控制與傳輸平面分離，並以服務為根基的核心網路架構（Service-based Architecture, SBA），採用網路切片以及邊緣運算的設置模式的特性。在資安防護上，5G 網路安全應建立統一的身分驗證框架與可供識別和追蹤機敏資訊的隱私保護機制，以確保跨通訊技術移動，此外，透過5G網路切片可隔離並優化安全性，進而防堵網路威脅滲透至其他網路切片，確保受到攻擊時網路能將損害降至最低。

所謂網路切片，為一個提供特定網路能力和網路特徵的邏輯網路，而網路切片實體（Network Slice Instance）是由一群網路功能實體集合（Network Function Instances）與所需資源（如計算、儲存與網路資源）組成，是構成網路切片之組成要件[169]。5G 網路切片為 5G 網路原生之特性，可以透過共享相同的 5G 基礎設施來提供差異化服務，相對而言也能做到隔離威脅的功能，然而網路切片技術之安全性與潛在威脅也須同步掌握。為掌握5G網路與行動網路的網路切片管理等的安全問題，本計畫將以 3GPP TR 33.811 v15.0.0 文件（下稱：33.811 文件）[170]為基礎，探討國際組織就網路切片安全性管理提出的潛在威脅、安全需求與解決方案標準。並以電機電子工程師學會（Institute of Electrical and Electronic Engineers, IEEE）發布的「5G 網路切片：安全性概述」文件為輔，檢視整體網路切片在生命週期可能會遭遇的潛在安全威脅與安全需求。

[169] 3GPP, *3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;System architecture for the 5G System (5GS);Stage 2, (Release 17),* TS 23.501 v17.2.0(2021-09), https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-h20.zip (last visited：Oct. 4, 2021)

[170] 3GPP, *3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of 5G network slicing management (Release 15),* TR 33.811 v15.0.0, https://www.3gpp.org/ftp/Specs/archive/33_series/33.811/33811-f00.zip (last visited：Aug. 31,2021)

(二) 5G 網路切片安全

3GPP 於 33.811 文件提出 4 項關於網路切片安全管理的關鍵議題，以及 5 種解決方案。前述的 4 個關鍵議題分別提出潛在的切片風險與攻擊，簡述如下：

1. 未經授權存取管理揭露（exposure）介面：管理介面安全管理不當，將造成攻擊者在未經授權下存取（access）網路管理功能，並透過創建特殊（significant）網路資源的網路切片實體或以大量網路切片實體進而耗盡網路資源癱瘓網路，或修改其他客戶的網路切片實體配置，使其服務級別（Service Level Agreement, SLA）失效等[171]。
2. 保護網路切片實體的監控（supervision）與報表（Reporting）：須確保網路切片實體的監控或性能報表完整性，監控或性能報表若遭到竄改則將引起不必要或不適當的網路切片實體修改等，導致網路資源消耗或改變正在運作的切片。同時攻擊者可以竊聽監控與報告數據的傳輸，選取正在運作的網路切片實體進行敏感資訊的攻擊[172]。
3. 保護網路切片子網模版（Network Slice Subnet Template）：網路切片實體的營運（on-boarding）與創建過程中須使用到網路切片子網模版，因此，須確保網路切片子網模版的完整性，在營運、傳輸以及儲存過程中竄改網路切片子網模版，將導致網路切片的實體創件不正確或不成功。此外，若網路切片子網模版得以明碼的方式（in clear text）存取，則攻擊者可取得有關網路切片實體的敏感資料，進而使用敏感資料攻擊正在運作的網路切片實體[173]。
4. 不安全的網路切片性能（capability）協商過程：當通訊服

[171] *Id* at 8-9.
[172] *Id* at 9.
[173] *Id* at 9-10.

務客戶要求客製化之網路切片，並期望由其管理網路切片的模式產生將有潛在風險。針對網路切片性能與特性應以標準化的方式與客戶安全協商，確保協商程式的安全並使安全程式標準化。因為，若網路切片沒有以標準化的方式進行安全保護，切片管理將有可能受到惡意攻擊，例如：發動中間人攻擊修改和降級切片性能[174]。

另一方面，33.811 文件也針對前述 4 種關鍵議題的潛在風險提出 5 種解決方案，簡述如下：

1. 管理揭露（exposure）介面的安全程序：在營運商信任領域內（trust domain），由營運商的安全政策決定保護介面；在營運商信任領域外，則須執行通訊服務管理功能（Communication Service Management Function, CSMF）與網路切片管理功能（Network Slice Management Function, NSMF）間的相互認證、傳輸層安全性協定（Transport Layer Security, TLS）相關之安全性檔案（profiles）、針對通訊服務管理功能（Communication Service Management Function, CSMF）的切片管理服務要求的授權等安全解決方案[175]。
2. 基於授權存取管理功能的 OAuth（開放授權）：提供一個通用的授權程式。因為營運商信任領域內的管理功能需要消耗（consume）其他管理功能所提供的服務[176]。
3. 網路切片子網模版的完整性保護：假定網路切片子網模版以特定格式（e.g XML）創建，在網路切片子網模版的傳輸、營運以及儲存的過程中，以數位簽章（digital signatures）提供完整性保護[177]。

[174] *Id* at 10.
[175] *Id* at 11.
[176] *Id* at 12-13.
[177] *Id* at 13-15.

4. 網路切片子網模版的機密性保護：假定網路切片子網模版以特定格式（e.g XML）創建，在網路切片子網模版的傳輸、營運（on-boarding）以及儲存的過程中，以加密（encryption）提供機密性保護[178]。
5. 網路切片間管理功能的安全性程序：當行動網路營運商細分網路切片並對應至其信任領域內的管理功能或在一信任領域內之管理功能需要消耗其他管理功能提供的服務時，應提供網路切片管理服務消費者（network slicing management service consumer）以及相關製造者一個安全程序。如：網路或傳輸層的保護，所有網路切片管理功能應支援以及執行 TLS。此外，網路切片管理功能間的授權，網路切片管理服務消費者應受到授權始可存取服務，通常會使用開放授權（Open Authorization, OAuth）[179]作為授權機制[180]。

除網路切片本身在安全管理層面問題外，也需瞭解網路切片之生命週期可能產生的威脅與相對應的安全需求，方能掌握每一階段網路切片的安全性。本計畫亦參考 IEEE 提出的「5G 網路切片：安全性概述」，概述 5G 網路切片在生命週期安全（life-cycle security）中，四個階段分別存在的威脅與安全性要求[181]：

1. 準備階段

   準備階段的主要攻擊點是網路切片模板（network slice template），假如網路切片模板設計不當、遭到篡改或執行不當，便會影響由此構建的所有切片，構成威脅。除了強大的主動式攻擊可能破壞模板完整性外，內容暴露也可能

[178] *Id* at 15-17.
[179] 開放授權（OAuth）是一種開放標準，允許使用者讓第三方存取該使用者在網站上儲存的私密資源（如相片、影片、聯絡人），而無需將使用者名稱和密碼提供給第三方。
[180] 3GPP, *supra* note 170 at 17.
[181] IEEE Access，Vol 8., available at https://ieeexplore.ieee.org/abstract/document/9099823

造成敏感資訊外洩。具體的緩解技術包括可預防模板被探測的機制，如藉由密碼協議（cryptographic protocols）提高網路切片模板在傳輸和儲存上的機密性、完整性和真實性（authenticity），以及運用即時安全分析（real-time security analysis）驗證網路切片模板的正確性。

2. 安裝、配置與啟動階段

第二階段的主要威脅包括在啟動之前或啟動期間製造假切片或更改切片配置，此階段的攻擊點為應用程式介面（Application Programming Interface, API），入侵者可能干擾切片的安裝、配置或啟動。具體的緩解技術包括經由存取和操作權限以完善 API 的安全保護機制，例如使用傳輸層安全性協定（Transport Layer Security, TLS）[182]於雙向身份驗證，或透過開放授權（Open Authorization, OAuth）[183]進行服務請求之授權。此外，第一階段提到的一般加密技術和即時安全分析在第二階段仍然有用。

3. 運行階段

此階段面臨最多種類的威脅，包括阻斷服務（DoS）、性能攻擊、資料和隱私外洩，而 API 仍然是此階段的主要攻擊點。此外，與管理相關的威脅，例如未經授權的配置更改，也會在運行時持續產生新的威脅。雖然前一階段的緩解技術在此階段仍然有效，此階段更加強調對網路切片進行真實性和完整性的驗證，具體的緩解技術主要以切片隔離防止分散式阻斷服務（DDoS）攻擊。

4. 退役階段

[182] 傳輸層安全性協定（TLS）是一種安全協定，目的是為網際網路通訊提供安全及資料完整性保障。許多應用程式及網站，如 Google、Facebook、Wikipedia 等皆以此協定來建立安全連線，傳送資料，目前已成為安全通訊的工業標準。

[183] 開放授權（OAuth）是一種開放標準，允許使用者讓第三方存取該使用者在網站上儲存的私密資源（如相片、影片、聯絡人），而無需將使用者名稱和密碼提供給第三方。

在切片退役期間的主要威脅為在退役期間處理不當導致的敏感資料暴露，第二個威脅則是不適當地消耗資源所引起的DoS攻擊。具體的緩解技術包括將敏感資料銷毀，以及網路功能和資源的釋放（de-allocation），避免它們一直處於忙碌狀態。

5G 網路切片允許 5G 基礎設施高度靈活運用，並提供各項差異化服務，因此，如何確保差異化服務的提供是安全可信賴的，網路切片的安全性成為非常重要的一環。本計畫在觀察 33.811 文件與「5G 網路切片：安全性概述」文件後，首先認為網路切片的安全管理不僅僅關注於運作中的網路切片，而是應自網路切片的創建、營運與退役去做觀察，每一階段均存在一定的威脅與安全需求，因此，透過兩份文件可以初步綜覽網路切片在每個階段的潛在風險與安全性。再者，本計畫觀測兩份文件後認為，網路切片管理介面存取將成為首要解決的網路切片安全問題，如 33.811 文件提到未經授權而存取網路功能管理，將引發攻擊者攻擊網路切片實體進而消耗網路資源；而「5G 網路切片：安全性概述」文件亦指出在網路切片安裝、啟動及運行 2 個階段，API 將成為攻擊者的主要攻擊弱點，兩份文件均顯示攻擊者若未經授權隨意連結存取網路管理功能介面或是 API，終將引起攻擊者透過該攻擊點進而竄改網路切片的資訊與功能。為此，本計畫建議網路切片的安全管理須強化存取網路管理功能介面或是 API 間的安全防護機制，透過 TLS 或是 OAuth 授權機制保護網路切片端到端的安全性。

另一方面，33.811 文件也提到，由於網路切片實體的創建與運作需要使用到網路切片子網模版，因此確保網路切片之安全性，即應先確保網路切片子網模版的完整性與安全性。為此，本計畫建議網路切片子網模版可使用數位簽章或加密的方式，保護網路切片子網的完整性與機密性。

(三) 物聯網與智慧製造資訊安全現況與需求

根據拓墣產業研究院於 2021 年研究調查，因應技術成熟與應用場景更趨多元的網路背景下，至 2025 年全球的連接設備數有望達到 750 億個，將產生近 75ZB 數據量。隨著設備數與數據量增加，物聯網生態圈與供應鏈各節點的資安風險也隨之提升，攻擊層出不窮，其手法工具亦持續翻新，以及更多資安漏洞被發現。

鑒於勒索軟體和相關駭客攻擊事件頻傳，加諸數據量上升帶來關鍵基礎設施資安疑慮和數據風險，以及可預期更嚴格的 IoT 資安法規，全球物聯網資安市場將持續保有強勁的發展動能。

觀察物聯網垂直領域，製造業隨無人工廠設立、自動化普及與智動化升級，未來越權存取、遇駭造成的操作中斷將產生更龐大之經濟損失；此外，隨智慧醫療發展，加諸醫院相對開放的空間特性，醫療業的資安更加著重軟硬整合，且資安與人身安全關聯性強對其發展具舉足輕重，故現行 IoT 資安將以製造業與醫療業為最關鍵的垂直應用領域。

目前常見的 IoT 重大安全挑戰包括：弱密碼、密碼缺乏更新、數據保護不足、設備管理不佳等，迄今仍未能有效克服。

此外，雲端物聯網平臺雖然因為能有效處理運用收集的資料和共享資源而備受企業青睞，然而，龐大的數據也成為攻擊者的頭號目標之一。因此，現行資安防護對各大雲端服務供應商（Cloud Service Provider, CSP）而言，不僅是基礎配備，也成為強化其自身產品服務競爭力的手段。例如，Microsoft 推出的 AWS 平臺，其著重點在於「稽核」和「監控」兩大面向；Azure Sphere 具備硬體信任根（root）、縱深防禦等 7 個屬性，並放眼異地／居家辦公模式，提供企業遠端 IT（Remote IT, RIT）、家用 IT（Home IT, HIT）需求；Google 則運用其運用其數位平臺與智慧裝置之整合，特別著眼於加密金鑰市場，並考量以其平臺技術延伸至發展智慧家庭生態圈。

而從資安廠商來看，趨勢科技以網路與端點兩大部分瞄準 IoT 和未來 5G 專網資安商機，Check Point 是聚焦在對影子物聯網（Shadow IoT）裝置的搜索與防護。綜觀各類廠商策略，前端的軟硬體整合、單點的身分驗證，以及場域的影子物聯網為其既有持續強化的防護重點，進而隨自身業務而有多元發展。影子物聯網即是 Check Point 調查使用之概念，為影子物聯網裝置（Shadow IoT Devices）的網路環境，被稱作影子，係因該裝置在組織內部的 IT 團隊不知情情形下對外聯網，且因其老舊，或存在無法修補的資安漏洞；或是企業裝置來自不同供應商、類型龐雜，企業對此類影子裝置的風險控管能力有限[184]。透過 AI 巡檢與擴大服務範圍，以及串聯全產業的資安防護，也頗有從單一設備到全場域乃擴散至上下游趨勢，加諸系統層級的防護亦將建立制度，預料整合式的平臺與解決方案將更受青睞。

表 3- 5、物聯網生態圈各節點資安風險

物聯網生態圈節點	主要特性	潛在風險與威脅
網路與行動 App	• 封閉/開放平臺 • 高數據量處理	• 缺少滲透測試 • 不安全的使用者或第三方授權
雲端設備	• 公共雲、私人雲、混合雲	• Code、管理政策
通訊系統	• 2G/3G/4G/5G • LPWAN • Wi-Fi、Bluetooth	• 不安全通訊
閘道與邊緣裝置	• 多元通訊協議 • 時間敏感網路	• 拒絕服務/分散式阻斷服務 • 無法或不安全更新 • 單純的硬體設計

[184]Yahoo!新聞， Check Point: 90%公司有不安全的影子物聯網裝置，2020/7/31，https://tw.news.yahoo.com/check-point-90-%E5%85%AC%E5%8F%B8%E6%9C%89%E4%B8%8D%E5%AE%89%E5%85%A8%E7%9A%84%E5%BD%B1%E5%AD%90%E7%89%A9%E8%81%AF%E7%B6%B2%E8%A3%9D%E7%BD%AE-160452338.html(瀏覽日期：109 年 11 月 10 日)

物聯網生態圈節點	主要特性	潛在風險與威脅
感測器	• 低功耗 • 窄頻寬 • 資源受限的裝置設備	• 設計錯誤 • 軟、韌體執行錯誤 • 無法更新
產生數據	• 敏感型：影像、位置、個資等 • 技術型：環境測量、運行報告等	• 使用者習性 • 管理政策 • 資料儲存

資料來源：thales；拓墣產業研究院整理，2021/10

而在智慧製造與關鍵基礎設施智慧化方面，先進國家為因應數位轉型多朝能源轉型如智慧電網等應用面發展的同時，也頻繁遭受資安的攻擊與威脅。舉例而言，英國在 2020 年有超過 86%關鍵國家基礎設施（Critical National Infrastructure）其營運技術（Operational Technique）與工控系統（Industrial Control System, ICS）受到網路攻擊，且經檢視有 3 成以上政府組織使用的是 10 年以上舊版 OT 系統；2021 年 5 月美國最大成品油管道營運商 Colonial Pipeline 亦遭駭，癱瘓美東輸油系統，導致美國進入緊急狀態。近幾個月海內外大廠諸如 Sierra Wireless、宏碁、仁寶、日月光集團等紛紛傳出遭勒索軟體攻擊等 IT 災情，對其生產線、伺服器運作產生一定程度影響。

其實智慧製造的環境與物聯設備息息相關，因為整體而言物聯網設備仍是駭客較易入侵，且使用者疏於防護的一環，不僅居家環境如此，近年製造業積極投入數位轉型以打造智慧工廠，在 IT 與 OT 環境越顯複雜的趨勢下，加諸停工成本高，亦成 IoT 資安攻擊首選。

趨勢科技報告調查美國、德國、日本共 500 名製造業的 IT 和 OT 人員，逾 6 成在 2020 年皆經歷過資安事件，其中分別有 75%造成系統停擺、43%停擺時間超過 4 天。在資安防護措施各國則

略有不同，例如日本首重設備備份、美國較關注外圍防火牆和惡意軟體防護，德國則著眼設備本身備份、USB 儲存與入侵防護(IPS)。

趨勢科技在 2021 年 3 月底發布的智慧工廠資安報告中，其重點除了上述提及的區域別調查外，透過對此 3 個製造業大國與工業 4.0 先驅者見微知著，一定程度上也描繪出智慧工廠資安現況與挑戰。歸納該報告，智慧工廠中 OT 端相較 IT 端最大問題在於：「資產可視不落實」、「安全目標難訂定」與「風險威脅未識別」。這些瓶頸源頭來自營運現場的物聯網設備過於繁雜，隨著數位轉型過程 IT 與 OT 漸不同步且後者往往老舊，或影子物聯網設備管控不落實，僅靠內部防堵效果仍有限，如圖 3-5 所示。

因此，扣除掉人為因素，法制端的標準規範對智慧工廠來說也成為落實資安準則，諸如 NIST CSF、ISO 27001 等未來都可能是打進大廠供應鏈的基本要求。綜上所述，短、中期倘相關市場動能與趨勢維持，相較同樣飽受駭客攻擊的醫療與家庭場域，製造業的 IoT 資安產品服務將更受矚目，並朝向外掛、非侵入式(Agentless)且最低限度影響營運的產品設計為發展主軸。

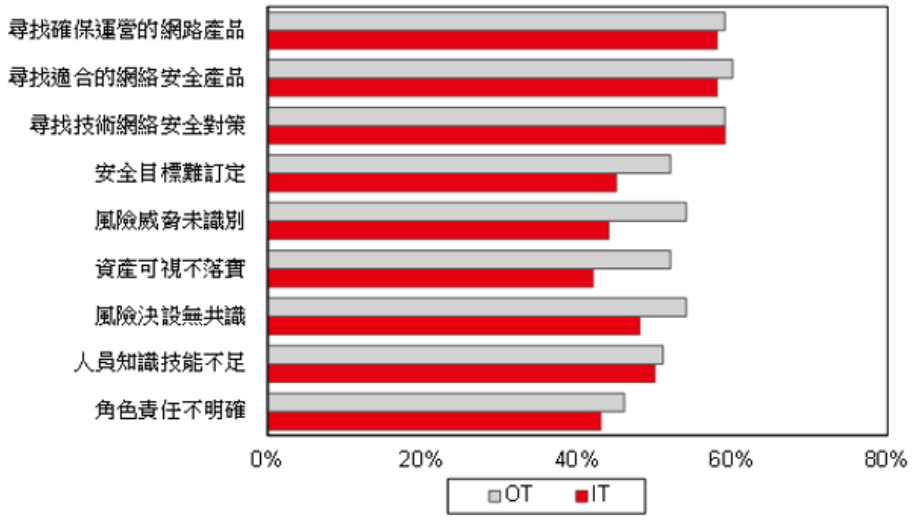


圖 3- 5、美國、德國、日本製造業面臨的 IT、OT 資安挑戰
資料來源：趨勢科技；拓墣產業研究院整理，2021/10

綜合上述物聯網與智慧製造應用場景現況，可整理出以下困境與需求：

1. 硬體品質參差不齊，連接穩定度不足：物聯網應用環境大多部署數十至數百個感測器、通訊設備、電力設備等裝置，相關硬體之準確度、可靠度、使用壽命等，並非全部都能達到理想狀態。物聯網設備需由有線或無線通訊協定將數據傳送到雲端，而通訊連接穩定度則視操作環境而定。大部分出現故障情況之案例，在使用初期時一切裝置皆正常，但運行一段時間後硬體即出現零星故障狀態，久而久之系統便被棄之不用。另外，物聯網操作環境所使用之感測器與相關設備眾多，各廠商設計之硬體通訊協定不一定能相容，增加後續操作及維修更換困難。若整套系統皆採用同一廠商之設備，則後續營運維修也必須依賴該廠商，反而讓整套物聯網服務被"廠商"綁架，對使用者而言並不方便。
2. 製造業思維領頭聯網服務不符需求：物聯網計畫在建置之初，大多把所有可感測之項目全部規劃進去。以農業為例，感測項目可包括土壤溫濕度、空氣溫濕度、光照、二氧化碳濃度、含氧量、含氮量、氨含量等。然實作後發現，許多項目監測值對農民而言並無太大意義，即使是遠端監控功能，除非農田範圍非常廣，需要遠端控制才能即時防止災害損傷，不然對於小農而言，並不太需要這些功能來協助日常作業。所以，當物聯網廠商開始收取後續服務費用時，許多偵測功能便被取消。
3. 物聯網運行需要成本，然使用者負擔意願視效益而定：物聯網應用環境建置之初，需要裝設多種軟硬體，安裝成本高，花費數十至數百萬元建設初期環境之案例所在多有。政府為了鼓勵廠商發展物聯網環境，多半會對計

畫給予財務補貼。系統開始運行後，物聯網環境中所蒐集之數據量呈倍數成長，若使用者對即時數據品質要求提升，相關網路、雲端、在地傳輸設備等勢必需要定期升級。因此，物聯網環境後續維護及營運仍需要持續投入成本，才能讓物聯網環境維持應有的水準。若物聯網設備並未帶來預期效益，使用者未必願意繼續負擔物聯網成本。

4. 物聯網服務商水準不齊，未能提供客戶最佳解決方案：目前提供物聯網方案之廠商多以 IT 專業為主，然物聯網應用領域多元，涵蓋各行各業，這些廠商不見得每次都能提出最佳方案，最常見到的案例即物聯網廠商所提供的服務與客戶需求有偏差，無法確切替客戶解決問題。

此外，隨著數據蒐集數量增加，對軟硬體設備規格需求也相對提升，若物聯網服務商規模不大，提供後續高規格服務的量能不足，未來也將難以持續提供符合客戶所需之服務。基此，未來可能的企業解決方案為：

1. 提升物聯網各硬體元件可靠度及通訊品質：物聯網應用並非僅靠單一通訊系統，而是由各種不同品牌之軟硬體共同建置完成。應用環境若有任一部份品質較為低劣，都會影響整體物聯網之使用效益。在提供物聯網服務之前，必須提升硬體穩定度，才能降低系統操作之不便。
2. 提供彈性收費方案取代設備採購：物聯網建置與服務費用之收費方案必須提供大幅彈性，無論是硬體、軟體、維運服務等，以租賃、分級等方案形式取代一次性設備採購合約，並針對蒐集數據可供外界使用與否提供相關補貼，降低使用者財務負擔，提高使用意願。
3. 將物聯網數據轉化為有用的資訊：針對蒐集之數據，提供以 AI、雲端計算等數位工具分析而成之資訊，讓資訊

能夠協助使用者提高收益、降低成本、提升生活品質，才能使物聯網應用產生應有之效益。

三、現行國際資安稽核標準機制與我國資安體系之關聯性

我國為落實全國之資安意識與防護思維，於 2016 年成立行政院資通安全處（下簡稱院資安處），共歷經 5 階段、各為期 4 年之重大資通安全計畫或方案185；透過資通安全分級與管理機制的規劃、建立與導入，至資安情資共享的階段性策略目標，持續提升我國資安完備度。

於法制層面，我國已於 2019 年正式施行「資通安全管理法」以及 6 項子法[186]。資通安全管理法及其子法於規範上相較於過去僅屬於行政命令，整體位階提升，並增加適用範圍至特定非公務機關[187]（「關鍵基礎設施提供者」、「公營事業及政府捐助之財團法人」屬之），藉此強化對外發生法規範圍為之整體效力[188]。

於政策管理上，該法則明定資訊安全責任分級、資安事件通報、情資分享、資安計畫稽核與獎懲辦法等管理機制，確立資安法制化之基礎，並持續針對我國資通訊政策進行法規調適，和我國資通訊環境與數位經濟發展與時俱進。

時至 2021 年，院資安處以「打造堅韌安全之智慧國家」為願景，從「吸納全球高階人才、培植自主創研能量」、「推動公私協同治理、提升關鍵設施韌性」、「善用智慧前瞻科技、主動抵禦潛在威脅」及「建構安全智慧聯網、提升民間防護能量」等四個面向著手，並配合六大核心戰略產業之「資安卓越產業」規劃持續推動資安產

---

185 行政院資通安全會報，國家資通安全方展方案（110-113 年），2021 年，頁 23。

186 子法包括：〈資通安全管理法施行細則〉、〈資通安全責任等級分級辦法〉、〈資通安全事件等級分級辦法〉、〈特定非公務機關資通安全維護計畫實施情形稽核辦法〉、〈資通安全情資分享辦法〉、〈公務機關所屬人員資通安全事項獎懲辦法〉。

187 〈資通安全法〉第 3 條之第 6 項，亦可見 https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297（瀏覽日期：2021 年 10 月 19 日）。

188 林宜隆、楊書豪，〈行政院資通安全管理法六大子法介紹及適法機關落實法遵之探討〉，2019 臺灣網際網路研討會，2019 年，亦可見 https://tanet2019.nsysu.edu.tw/assets/TANET2019_thesis/D3_005.pdf（瀏覽日期：2021 年 10 月 19 日）。

業，作為「智慧國家方案」與「5+2 產業創新」等大型數位經濟計畫之發展基礎[189]。於「推動公私協同治理、提升關鍵設施韌性」方面，政府延續第 5 期發展方案建立之資安聯防體系機構之建置成果，強化政府管理跨領域情資、提升各領域資安整體素質。

綜上所述，我國目前已有 5G 技術應用與智慧聯網產業創新的願景，在法制面花近 20 年逐漸走向完備之時，將有賴從政策面協助觀測我國發展趨勢，為因應我國現階段產業環境需求，進行法制層面調整。

由於我國資通安全政策與管理法制面的建立係參考美國國家標準暨技術研究院（National Institute of Standard and Technology, NIST）之網路安全架構（Cyber Security Framework），以及 ISO27001 之資訊安全管理系統（Information Security Management System, ISMS）概念所制定。 然而暫時沒有針對近幾年蓬勃發展的物聯網相關垂直領域應用發展企業，這種屬於非傳統智慧製造的企業組織，此類組織的稽核相關指引之產生。

換言之，研究團隊意識到既有的資通安全管理法制層上對於(1)類智慧製造企業組織(2)未來網路系統環境在稽核相關要素的缺乏，故選擇研析 ISO27001:2013、IEC62443 國際稽核標準，以及未來萬物聯網路環境下重要的網路元件 DNS 由 IEEE 提出的稽核系統框架，瞭解其異同，以提前擘劃安全智慧聯網產業環境相關資安稽核指引與相關策略。

(一) ISO27001:2013

ISO 27001 是由國際標準組織（International Organization for Standardization）以及國際電工委員會（International Eletrio Commission, IEC）共同發佈的資安管理標準，此標準已在國際上被廣泛使用，旨在提醒在建構及管理整個資訊安全管理系統

[189] 同註 185。

（ISMS）時，必須注意且不可忽略的層面，並藉由規劃（Plan）、執行（Do）、審查（Check）及改善（Act）的循證方式（簡稱PDCA）來確保系統持續運作並且預防資安事件發生或是降低遭受損失的風險。在 ISO 系列標準中，27000 為整個系列的概觀，適用於 ISMS 範圍、名詞和定義；此外，其中有兩個標準可提供驗證，分別為 ISO 27001 及 ISO 27006，ISO27001 適用於一般企業、ISO 27006 則適用於驗證機構。

ISO27001 是以「風險」為基礎的方法論，定義資訊安全政策、程序以及選擇適當的控制措施來管理風險。在 ISO27001:2013 規範內，除本文要求之外，還包括 14 個控制目標；在依據不同控制目標需求下，區分為 114 個控制措施，內容放於「附錄 A（規定）控制目標與控制措施」（Annex A (normative) Reference control objectives and controls），其條文對應於 ISO27002，係作為組織導入 ISMS 執行稽核實務時的檢核參考項目，用於建立資訊安全管理系統並且進行審核，以確保組織的資訊安全管理系統有持續性的運作，當審核通過，就代表獲得 ISO27001 認證。

以下簡單說明 IEC/ISO27001:2013 之章節與架構。其章節如表 3-6。

表 3- 6、IEC/ISO27001: 2013 章節架構

0.	簡介（Introduction）
1.	適用範圍（Scope）
2.	引用標準（Normative references）
3.	用語釋義（Teams and Definitions）
4.	組織全景（Contest of the organization）
5.	領導作為（Leadership）
6.	規劃（Planning）

7.	支援作業（Support）
8.	導入實施（Operation）
9.	績效評估（Performance evaluation）
10.	持續改善（Improvement）

資料來源：IEC/ISO27001: 2013

首先，第 0 節簡介說明 ISO27001 之 PDCA 原則，確保資訊之機密性、完整性、可用性，並透過管理風險給予關注方信心，且考量 ISMS 與管理系統之相容與整合。

第 1 節列出 ISO27001 之驗證範圍規範，該要求為：

- 建立、實作維持及持續改善組織範圍內的資訊安全管理系統。
- 符合組織需求之資訊安全風險評鑑與處理。
- 為一般性要求，適用各類組織，無論其形態、規模與性質。
- 不得排除本標準之中第 4 節至第 10 節所規定之任何要求事項。

第 2 節「引用標準」、第 3 節「用語釋義」明確說明相關定義出自 ISO27000。第 4 節起至第 10 節則配合 PDCA 循環羅列各節所需檢核之標準。如圖 3-6。

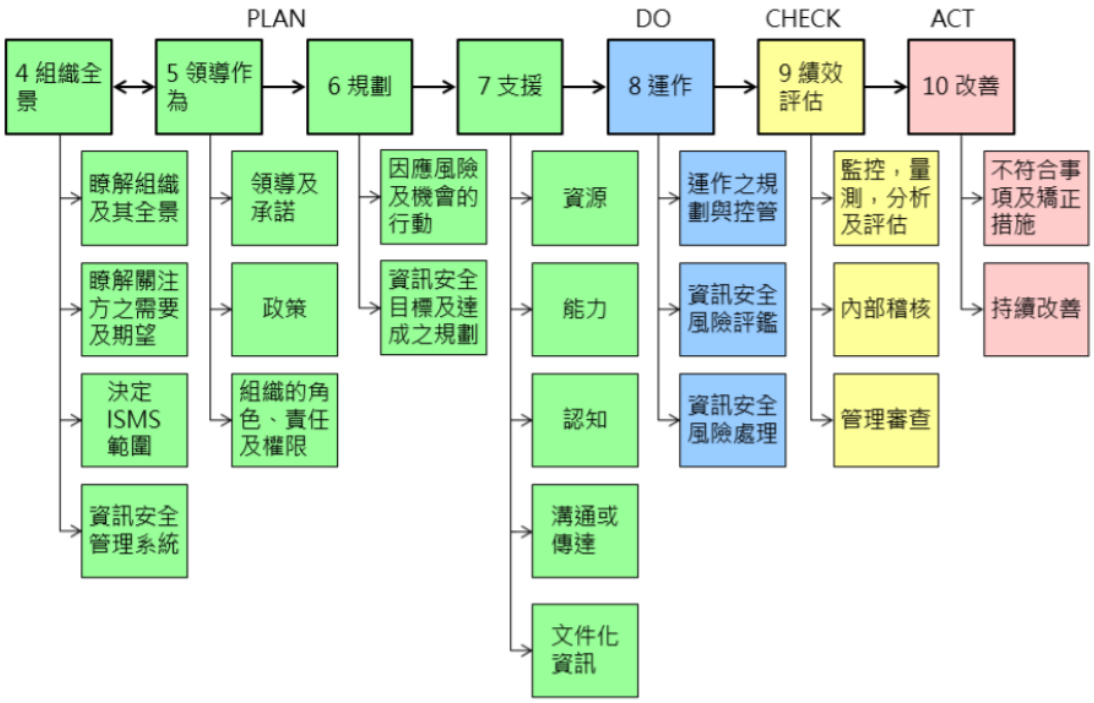


圖 3- 6、ISO27001 與 PDCA 循環

資料來源：BSI

從稽核實務面而論，企業藉由內部稽核，或請第三方驗證機構進行 ISMS 之「績效評估」，確保組織是否依資通安全計畫所規劃，讓 ISMS 整合至組織並能有效運作；內部稽核與第三方驗證機構之區別僅在稽核成員之不同，其稽核步驟雷同。內部稽核中，依據資通安全計畫指派之負責人員組成稽核組並制定稽核計畫（audit programme），以稽核 ISO27001 逐項條文均符合組織需求；為讓評估具可衡量性，需依控制措施項目製作檢核表（checklist），稽核人員將依據稽核原則判定其是否具程度輕微或嚴重的「不符合事項」而開立缺失，透過內稽小組成員之觀察與佐證，產出「稽核報告」、並制定「缺失改善計畫」，以確保 ISMS 之持續改善。在完成第一次 PDCA 的循環後，組織即可憑上述文件資料向國際機構驗證以獲得初始驗證，並於次年追蹤前年之缺失是否改善，再進行次年度之稽核計畫，持續滾動調整組織的資訊安全策略目標。針對 ISO27001 條文項目原則之摘要，以及參考

各國資安政策框架、稽核實務經驗、應配合之重點行動，摘要如下表 3-7：

表 3- 7、IEC/ISO27001: 2013 條文項目原則之摘要

項目	原則	重點行動
4.1 了解組織及其全景	組織應決定「內部及外部議題」，與其目的有關且影響達成其資訊安全管理系統預期成果能力者。	進行組織之「處境及背景分析」，分析產出結果之議題，以決定風險管理之優先順序。
4.2 瞭解關注各方之需要及期望	組織應決定與資訊安全管理系統有關之關注各方，此等關注各方對資訊安全之要求事項。	明列組織內部之管理、非管理成員；組織外部之客戶、中央目的事業主管機關、供應商等。
4.3 決定資訊安全管理系統範圍	組織應決定資訊安全管理系統的邊界與適用性來建立範圍，範圍應以文件化資訊方式提供使用。	劃定 IT 部門（最小範圍）、資訊機房與核心作業系統，宜涵蓋 4.1、4.2 所重視之「內外部議題」與「利害關係人」的資訊安全考量納入範圍。
5.1 領導及承諾	最高管理階層應確保下列事項，展現對資訊安全管理系統之領導及承諾： ● 建立與組織策略方向相同之資訊安全政策及資訊安全目標。 ●確保 ISMS 要求事項整合至組織流程及所需資源之可取得。 ●確保 ISMS 重要性之傳達、並	制定資訊安全管理政策，確保 ISMS 導入的目標設定之達成能落實資安政策與願景。

項目	原則	重點行動
	達預期成果。 ●為促進 ISMS 有效性進行人員指導、支援、宣導、持續改進展現其權力。	
5.2 政策	最高階管理階層應建立資訊安全政策，其政策宜切合組織目標、滿足資訊安全相關要求與承諾，須提供文件化資訊，向全組織或關注各方溝通。	同 5.1。
5.3 組織角色、責任及授權	最高階管理階層應確保資訊安全相關角色的責任與授權加以指派與溝通，以及確保 ISMS 之有效性與可衡量性。	同 5.1。
第 6 節 Planning 規劃		
6.1 因應風險及機會之行動	規劃 ISMS 時應考量 4.1 之議題，與 4.2 要求事項，以及決定應被提出的風險與機會，以確保 ISMS 能達成預定成效，預防、降低非預期影響。組織應規劃風險與機會的處理措施，及如何將措施整合入 ISMS 流程並執行，並評估措施之有效性。	依據組織策略目標與資安需求重點，決定 ISMS 範圍，並盤點 ISMS 範圍內之「資訊資產」。
6.1.2 資訊安全風險評鑑	需建立與維護風險準則，確保重複執行的評鑑能產生一致、有效，並可比較之結果；以及可識別風險（威脅、弱點及風險擁有者）、分析風險（可能性、衝擊性及風險等級）、評估風險（風險處理順序）。	制定風險評鑑計畫，訂定可衡量之年度目標；依風險量測結果計算系統範圍內之資訊資產的風險值，以確定該資產之風險等級。

項目	原則	重點行動
6.1.3 資訊安全風險處理	需選擇適切的風險處理選項，決定選擇的控制措施，釐清排除項目，產生適用性聲明書（State of Applicability, SOA），規劃風險處理計畫，進行風險處理計畫與殘餘風險的核准。	依據風險等級制定風險處理計畫。
6.2 資訊安全目標及其達成之規劃	當規劃如何達成資安目標時，組織應決定待辦事項、所需資源、負責人員、完成時間、結果之評估方式。此外應建立資訊安全目標，其目標應與資訊安全政策一致、為可量測的（如可執行時）、且考量資訊安全要求，以及風險評鑑與處理的結果，並加以溝通與適當更新內容。	透過組織內部之負責人員小組定期檢視 ISMS 制度是否有需改善，例如量測目標是否有期間之限制、目標特性是否符合組織文化等。
第 7 節 Support 支援作業		
7.1 資源	組織應決定提供 PDCA 所需之資源	組織編列專責資安人員、提供相關資安設備之採購預算，採取將資安政策落實至實際工作環境之行為。
7.2 能力	決定所需能力並確保有能力，採取措施，證明能力證據	組織制定教育訓練管理作業程序，進行年度教育訓練。
7.3 認知	確保組織執行工作人員應了解 ISMS 政策、個人對 ISMS 有效性的貢獻、及違反 ISMS 規定之後果	組織透過內、外部稽核人員之觀察、訪談與佐證文件確認其是否有正確之

項目	原則	重點行動
		資安認知。
7.4 傳達	組織應決定有關內外部溝通的需求，包含事項、時機、對象、應執行者、過程。	組織制定情資分享或事故通報流程及相關程序書。
7.5 文件化資訊	-	同 7.4。
7.5.概述	組織應保存對組織 ISMS 系統有效性之文件化資訊。	同 7.4。
7.5.2 制定與修訂	組織應制定文件化資訊格式、編號、語言、版本、存在方式、審查。	同 7.4。
7.5.3 文件化資訊的管制	組織應於分發、存取、儲存、更新、銷毀，以及外部文件化資訊應加以適切低識別與管制。	同 7.4。
第 8 節 Operation 運作		
8.1 運作規劃與控制	組織應規劃、實作及控制達成之 ISMS 要求事項過程、實作 6.1 所決定之行動、達成 6.2 之目標。	-
8.2 資訊安全風險評鑑	組織應於規劃期間、提議或發生重大變更，考量 6.1.2 中建立準則，執行風險評鑑，並保留文件化資訊。	組織實際執行風險評鑑計畫。
8.3 資訊安全風險處理	實作 6.1.3 之風險處理計畫，並保留文件化資訊。	組織實際執行風險處理計畫。
第 9 節 Performance evaluation 績效評估		
9.1 監控、量測、分析與評估	● 決定項目、決定方法、執行時機、執行人員。 ● 監視與量測結果應分析與評估時機。 ● 分析與評估結果執行人員。	組織內部負責人員召開管理審查會議。
9.2 內部稽核	組織是否依規劃期間遵循 ISMS 要求	組織成員定期組成

項目	原則	重點行動
	事項、是否有效實作、維持 ISMS，並保存文件化資訊做稽核證據。	內稽小組，進行年度內部稽核作業程序。
9.3 管理審查	最高管理階層於規劃期間審查組織 ISMS 之合宜性、適切性與有效性，審查項目包括： ●前次管審跟催。 ●內外部議題的變更。 ●績效回饋，包含下列趨勢：不符合事項與矯正措施；監視與量測結果；稽核結果，以及資訊安全目標符合度。 ●利害相關團體回饋。 ●風險評鑑結果與風險處理計畫狀態，以及持續改善的機會。	組織內部負責人員定期召開管理審查會議。
第 10 節 Improvement 矯正措施、持續改善		
10.1 不符合事項與矯正措施	矯正措施需消除不符合的原因，以防止再發生。	組織進行內、外部稽核作業，稽核方發現缺失並開出矯正缺失單，稽核方須針對缺失進行根因分析（root cause），提出暫時性對策、永久性對策以要求要求受稽方改善之。
10.2 持續改善	組織 ISMS 之合宜性、適切性與有效	組織進行內、外部稽核作業，持續追

項目	原則	重點行動
	性。	蹤措施處理進度。

資料來源：ISO:27001:2013、TTC 稽核實務，本計畫綜合整理。

(二) IEC62443

IEC62443 為針對工業自動化與控制系統的安全規範，原本被命名為 ISA 99，由國際自動化學會（International Society for Automation, ISA）所創立，後經審核再透過美國國家標準協會（American National Standards Institute, ANSI）發布，之後被國際電工委員會（International Eletronic Committee, IEC）納入，並由 IEC 內部委員會修訂並發布，因此有 ISA/IEC 62443 兩種名稱（以下簡稱 IEC 62443）。

IEC 62443 由國際標準（International Standard, IS）、技術報告（Technical Report, TR）、技術規範（Technical Standard, TS）三種文件類型組成，總共分為 4 個部分：

- 第 1 部分是概述（General），包含了一般或基本的概念、模組及專有名詞，也包括 ICS 的安全規律。
- 第 2 部分為政策與程序（Policies & Procedures），是透過組織內有效的工業自動化控制系統（Industrial Automation Control System, IACS）安全計畫，來解決並維護 IACS 安全問題。
- 第 3 部分為系統（System），即討論 IACS 系統技術設計與風險、安全需求及等級評估。
- 第 4 部份為元件（Component），是製造商的產品開發與系統控制，以達到產品的安全技術要求。

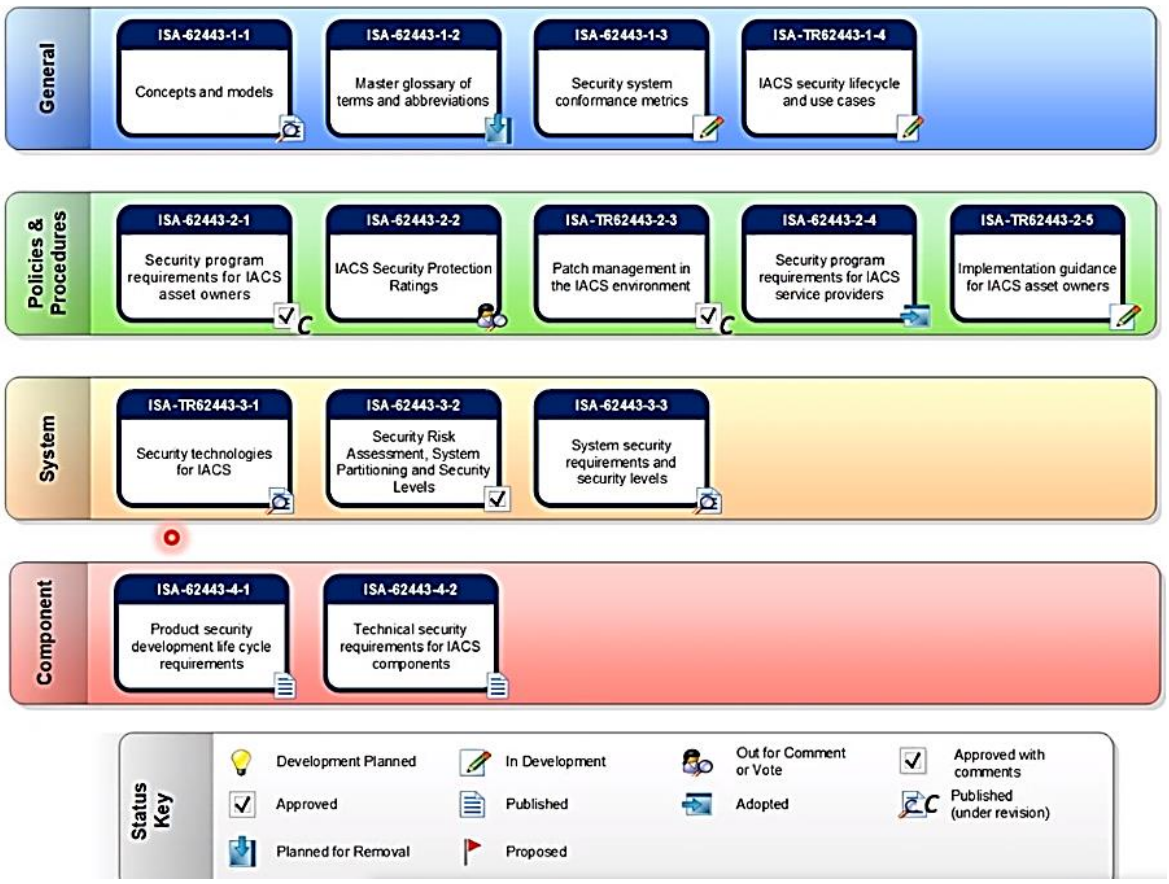


圖 3- 7、ISA/IEC 62443 架構圖與進度

資料來源：MIC，取自行政院院資安處，原始資料來自 IEC62443-3-3

如圖 3-7 所示，IEC62443 各部分之文件有不同的進度，部分文件尚在撰寫或意見徵詢並未正式發行。目前已發行之 IS 為 IEC62443-4-1：產品生命週期開發安全需求標準（Product security development life cycle requirements）、IEC62443-4-2：IACS 元件技術安全需求（Technical security requirements for IACS components）；已發布刻正修改者為 IEC62443-2-1：IACS 資產擁有者建立安全計畫需求（Security program requirements for IACS asset owners）；已發布刻正檢視者為 IEC62443-3-3：系統安全與需求等級（System security requirements and security levels, IS）。以下即針對 IEC62443 目標與規範群體，配合上圖文件進行概述。

1. IEC62443 的目標與規範群體

IEC 62443 的目標和規範群體記載於 IEC 62443-4-2。IEC

62443-4-2 的 IACS 規範群體是資產所有者（asset owner）、系統整合商（system integrator）、產品供應商（product supplier）以及適當的認證機構（compliance authorities）。認證機構包括政府機構和監管機構，他們有法定權力進行審計，以驗證是否符合相關法律和法規[190]。

系統整合商將使用本文件規範來協助他們採購符合 IACS 解決方案的控制系統元件，亦即通過 IEC 62443 規範的系統元件。協助的形式是幫助系統整合商指定他們所需的各個元件的適當安全能力等級。系統整合商的主要標準是 IEC 62443-2-1、IEC 62443-2-4、IEC 62443-3-2 和 IEC 62443-3-3，這些標準提供了安全管理系統的組織和操作要求，並指導他們定義系統的「安全區域」，以及決定這些區域的目標安全能力等級（Security Level- Target, SL-T）。SL-T 通常是透過風險評估來訂定，一旦定義了每個區域的 SL-T，就可以使用提供必要安全能力的元件來實現每個區域的 SL-T。

產品供應商將使用 IEC 62443-4-2 來了解控制系統元件的特定安全能力等級（Security Level - Component, SL-C）的要求。SL-C 係指元件或系統在正確配置時能提供的安全級別，當元件本身可能不提供所需的能力，但可能被設計成與更高層次的實體整合，從而受益於該實體的能力。舉例而言，嵌入式設備本身可能不用維護用戶目錄，但能與系統範圍內的身份驗證和授權服務做整合，故整體而言仍可以滿足組織提供個別用戶身份驗證、授權和管理能力的需求。本文件將規範產品供應商哪些需求可以分配，哪些需求應該是元件中的原生需求。

按照 IEC 62443-4-1 第 8 章中的定義，產品供應商將提供有關如何將元件正確地整合到系統中，以滿足特定 SL-T。SL-T 和 SL-

[190] IEC, Security for industrial automation and control systems－Part, 4-2: Technical security requirements for IACS components (IEC 62443-4-2) , ed.1, Feb., 2019, p.15.

C 的級別計算方式，係根據元件要求（Component requirement, CR）、系統要求（System Requirement, SR）、基礎要求（Foundational Requirements, FR）、加強要求（Requirement Enhancement, RE）等項目進行計算。CR 係源自 IEC 62443-3-3 中所定義之SR，而SR是從IEC 62443-1-1中定義的FR所衍生出來；CR本身還可以包括一組RE，透過CR和RE的組合，將決定一個元件的能力等級，可作為組織用來評估一個正在開發的目標系統，其所欲達到的目標安全級別（SL-T）[191]。在 IEC62443-3-3 有針對安全性級別（SL）要求探討四個等級的對策，威脅由高至低分別為：

- SL4：針對高度高級威脅對策。
- SL3：複雜威脅的對策。
- SL2：中度威脅的對策。
- SL1：基本威脅的對策。

根據SL的級別，對於基本功能需求（FR）會有不同系統要求（SR）以及加強要求（RE）的檢核項目。FR 是作為衡量控制系統能力（即 SL-C）的 7 項基本要求詳參表 3-8，搭配 4 種對策層級，將產生 28 種檢測項目組合。

[191] IEC, Industrial communication networks- Network and system security －Part 3-3: System security requirements and security levels, (IEC 62443-3-3) , ed.1, Aug., 2013, p.14..

表 3- 8、IEC62443-1-1 基本功能需求分類

基本功能需求	功能需求分類
FR1	識別和認證控制（Identification and authentication control, IAC）
FR2	使用控制（Use Control, UC）
FR3	系統完整性（System integrity, SI）
FR4	資料機密性（Data confidentiality, DC）
FR5	受限制的資料流（Restricted data flow, RDF）
FR6	及時回應事件（Timely response to events, TRE）
FR7	資源可用性（Resource availability, RA）

資料來源：IEC62443-1-1，本計畫整理。

2. IEC62443 的稽核機制

IEC62443 關於管理的內容主要在 IEC62443-2-1、IEC62443-2-4；IEC62443-2-1 將 IACS 的適用範圍稱做網路安全管理系統（CyberSecurity Management System, CSMS），由於涉及到營運技術（Operating Technique, OT），故針對 OT 實體工作範圍之環境的安全進行定義，其安全計畫要素（Security Program Elements, SPE）如下：

- SPE1：組織安全措施（Organizational Security measures）
- SPE2：型態管理（Configuration Management）
- SPE3：網路和通訊安全性（Network and Communications Security）
- SPE4：組件安全性（Component Security）
- SPE5：數據保護（Protection of data）
- SPE6：使用訪問/存取控制（User access control）
- SPE7：事件和事件管理（Event and incident management）
- SPE8：系統完整性和可用性（System integrity and

availability）

從組織體系結構的角度來看，劃定適用的工作範圍需要回答類似於以下問題：

- 將涉及哪些計算機系統和網路？
- 是否包括 SCADA 系統和工控配電監視系統？
- 生產線是否包括與生產無關的計算機系統？
- 是否包括製造執行系統（MES）？
- 是否包括其他特殊工控機器管理系統和 SIS 系統？
- 是否包括機器人系統？
- 是否包括與供應商、分包商或建立重要克復的緊急聯繫資訊？

從功能角度來看，工作範圍可分為以下兩類：

(1) 直接風險管理活動：這些活動涉及風險的評估，溝通和優先及。例如，指定本地網路安全所有者，收集和維護資安清單，開發和維護網路體系結構，完成內部或外部審核以及在業務部門或公司基礎上報告這些結果。

(2) 風險管理相關項目：這些是在減少風險管理活動確定的風險的基礎上資助的活動。這些間接風險管理解決方案採用的形勢是時間有限的項目以及正在進行的服務的開發和部署。

於實務面，將根據上述工作範圍決定稽核範圍以及 IEC62443 場域驗證重點，依場域驗證重點制定安全計畫，藉此評估申請者的場域生產流程是否符合標準的安全要求。關於安全計畫之要求則記載於 IEC62443-2-4，詳參表 3-9 。

表 3- 9、IEC 62443-2-4 安全計畫（SP）要求

SP 類別	需求 ID	描述
解決方案人員(Solution Staffing)	SP.01.XX	與服務提供商將人員分配給自動化解決方案相關的活動有關要求。
保證(Assurance)	SP.02.XX	與確保執行自動化解決方案安全政策有關的要求。
架構(Architecture)	SP.03.XX	與自動化解決方案的設計有關的要求。
無線(Wireless)通訊	SP.04.XX	自動化解決方案中與無線使用有關的要求。
安全儀表系統(System Instrumented System,SIS)	SP.05.XX	有關將 SIS 整合到自動化解決方案中的要求。
型態管理(Configuration management ,CM)	SP.06.XX	與自動化解決方案的組構/配置控制有關的要求。
遠距/遠端訪問/存取(Remote access)	SP.07.XX	與遠距//遠端訪問/存取自動化解決方案有關的要求。
事件管理(Event Management)	SP.08.XX	自動化解決方案中與事件處理相關的要求。
帳戶管理(Account management)	SP.09.XX	自動化解決方案中與用戶帳戶管理相關的要求。
惡意軟體防護(Malware protection)	SP.10.XX	有關在自動化解決方案中使用反惡意軟體的要求。
修補/補丁管理(Patch Management)	SP.11.XX	與核准和安裝軟體修補/補丁程序的安全性相關要求。
備份/還原(Backup/Restore)	SP.12.XX	與備份和還原的安全方面有關的要求。

資料來源：IEC62443-2-4，本計畫整理

(1) SP01 解決方案人員（Solution Staffing）

包括應建立人員管理職能（培訓/維護手冊）、指派組織中高層的人負責安全（管理政策），並確保擁有符合資格的技術人員（培訓/技術手冊），進行人員背景調查（服務提供者、外包廠商），釐清組織架構圖（分工、角色）及人事職位異動政策、程序、表格（紀錄文件）。

(2) SP02 保證（Assurance）

- 透過網域安全評估、威脅分析和安全測試，確保病變是自動化解決方案元件是否有足夠的安全性。
- 網路安全評估（如風險評估差距分析、威脅分析或漏洞評估）。
- 元件安全開發工具，如安全要求、安全測試結果。
- 服務提供者必須具有強化解決方案的有文件紀錄的過程。

(3) SP03 架構（Architecture）：場域及解決方案的網路安全架構強化要求。

- 描述它如何規劃、實現、批准的網路分段體系架構。
- 網路架構圖及網路設備安全控制、設定、檢查機制（已批准的網路架構及其網路安全設備的配置策略/程序/檢查表）。
- 網路安全漏洞處理的政策/程序，包括組織中負責這些策略/程序的人員（按角色/職位）。
- 網域設備校時，確保同步網路時間來源安全。
- 如何減少解決方案中使用的元件/設備的攻擊面，以及確保在維護過程中保留減少的攻擊面（安全評估差距分析及改善紀錄）。
- 網路安全。

- 描述如何阻止維護和工程工作站（包括手持設備）或無法繞過控制系統使用者和網路存取控制。（如設計文件、使用者手冊、安全手冊、強化指南等）。
- 應有能力確保使用最少的許可權管理服務提供者負責的網路設備。
- 識別並配置、強化用於保護網路設備管理中使用的數據的加密機制。
- 應有能力確保加密用於保護用於管理網路（例如密碼、配置資料）數據。
- 數據安全及敏感數據保護。
- 應有能力確保並驗證自動化解決方案配置中的所有控制操作和數據流（例如工作站和控制器之間），包括配置更改，是否有效。
- 應由授權使用者發起或批准，以及通過已批准的連接在批准的方向傳輸。
- 識別資料流程、命令串流、下載（例如工程模組的控制器配置/程式設計功能）和用於保護它們的安全控制，以及用於配置安全性的策略/過程/檢查表。
- 記錄如何識別資產擁有者的敏感數據，以及如何確定敏感數據的安全要求。

(4) SP04 無線（Wireless）通訊

- 必須描述如何記錄其無線網路和連結，並保持該文件最新。
- 必須識別用於保護其無線設備的身份驗證和訪問控制機制。
- 確保對無線設備的訪問受到安全和工業自動化業界普遍接受的身份驗證和訪問控制機制的保護。

(5) SP05 安全儀表系統（System Instrumented System, SIS）：整合到自動化解決方案中的要求。

- 應有能力驗證是否已對自動化解決方案中使用的 SIS 通訊進行安全體系結構審查和安全風險評估。
- 服務提供者應有能力確保自動化解決方案外部的通訊（包括遠端存取通訊）不會干擾 SIS 的操作。
- 服務提供者應有能力確保 SIS 外部的應用程式（例如控制系統應用程式）不能參與、中斷或以其他方式干擾對安全功能至關重要的 SIS 通訊。

(6) SP06 型態管理（Configuration management, CM）

- 服務提供者應有能力提供自動化解決方案的準確邏輯和物理基礎架構圖紙/文件，包括其網路設備、內部介面和外部介面。文件和圖紙應作為自動化解決方案的準確表示進行維護。
- 圖紙/描述應清楚地標誌可連接到設備的內部和外部介面（如交換機、路由器、防火牆、網路介面卡）。
- 服務提供者應能夠驗證用於控制和檢測的有線和無線設備是否已正確配置其批准的值。

(7) SP07 型態管理（Configuration management, CM）：遠端管理。

- 服務提供者必須識別已批准在其解決方案中使用的遠端訪問應用程式，或其選擇和批准它們的方式，並顯示它們已被普遍接受。
- 服務提供者應能夠提供有關自動化解決方案中使用的遠端存取應用程式的安裝、配置、操作和終止的詳細說明。
- 服務提供者應能夠驗證用於控制和檢測的有線和無線設備是否已正確配置其批准的值。

- 服務提供者應有能力向資產擁有者提供有關所有建議的遠端訪問連接的資訊。

(8) SP08 事件管理（Event Management）

- 服務提供者應具有處理影響自動化解決方案的網路安全事件的能力，包括檢測網路安全危害和事件，向資產擁有者報告網路安全事件，回饋網路安全危害和事件，包括支援事件回應團隊。
- 服務提供者應能夠確保將自動化解決方案配置為所有與安全相關的事件（包括用戶活動和帳戶管理活動）寫入資產擁有者指定的天數保留審核日誌。
- 服務提供者應有能力確保自動化解決方案配置為相關資產擁有者的要求紀錄和通知操作員的流程相關事件，其事件類型包括狀態更改/操作條件更改/配置更改。

(9) SP09 帳戶管理（Account management）

- 服務提供者應有能力確保自動化解決方案支援，使用單個整合數據庫（可分發或冗餘），用於定義和管理使用者和服務帳戶，限制對帳戶的管理授權使用者，分散存取此資料庫以管理帳戶，分散實施帳戶配置（如密碼）在此資料庫中定義的操作系統許可權和訪問控制清單。
- 服務提供者應有能力確保為使用者創建和維護唯一帳戶。

(10)SP10 惡意軟體防護（Malware protection）

- 服務提供者應有能力向資產擁有者提供為自動化解決方案測試和驗證的惡意軟體保護機制的正確安裝、配置和更新的有文件的說明。
- 服務提供者應有能力確保惡意軟體保護機制已按照服務提供者的批准程式正確安裝/更新和正確配置，惡意

軟體定義檔安裝在與資產擁有者商定的期間內，惡意軟體配置保持更新。

(11)SP11 修補/補丁管理（Patch Management）

- 服務提供者應有能力向資產擁有者提供文件，說明如何評估和批准其負責的自動化解決方案軟體的安全修補程式。
- 服務提供者應有能力向描述安全修補程式/更新的資產擁有者提供文件。每個修補程式的描述應在其製造商發布修補程式後約定的時程內提供給資產擁有者，並應包括適用於服務提供者負責的自動化解決方案元件的安全修補程式，每個修補程式的批准狀態/生命週期狀態。

(12)SP12 備份/還原（Backup/Restore）

- 服務提供者應有能力為自動化解決方案的建議備份過程提供文件，該過程包括但不限於有關如何對自動化解決方案進行完整備份的說明。
- 服務提供者應能夠向資產擁有者提供有文件化的說明，以便將自動化解決方案及其元件恢復正常運行。
- 服務提供者應有能力向資產擁有者提供文件，說明如何控制和安全地管理可行動備份軟體。

由 IEC62443 的安全計畫中 12 個要素可知，其所檢核之項目更圍繞在「核心系統」的要素進行檢核設計，且基於注重上下游供應鏈與分包廠商複雜的 OT 環境考量，在利害關係人上的區分層次更為細緻。與 IEC62443 相較，ISO27001 是很好的 IT 管理體系標準跟框架，但在實作上的指導方針較為缺乏，雖然有附錄的控制措施項目與控制目標，卻沒有實作細節。組織可透過 ISMS 編定完善的組織、應變流程及標準作業流程（Standard Operational Procedure, SOP），雖然不適合營運科技（Operating Technique, OT）

的環境，但能強化 IT 網路安全管理，提供良好的基礎。

(三) DNS 網路安全框架核心

IEEE 於 2017 年出版之《域名系統安全管理》（DNS Security Management）一書中，參考 NIST 網路安全框架（NIST CSF 1.1）的架構設計，提出了適用於 DNS 的框架核心（Framework Core）──「DNS 網路安全框架核心」（Cybersecurity Framework Core DNS Example）。此框架核心係採用風險基礎方法（Risk-Based Approach），並依照 DNS 需求所量身訂做，該框架核心參照 NIST 網路安全框架的架構設計，將所列資安檢核項目分為識別（Identify）、保護（Protect）、偵測（Detect）、回應（Respond）與復原（Recover）之 5 大功能（Function），且再下分 22 項類別（Category）以及 98 項子類別（Subcategory）。該框架核心之檢核項目及檢核重點詳參下表：

表 3- 10、DNS 網路安全框架核心檢核項目

功能	類別	子類別	檢核重點
識別（ID）	資產管理（AM）	ID. AM 1-6	使組織能夠實現商業目標的資料、人員、設備、系統和設施，按照其對商業目標和組織風險策略的相對重要性進行識別和管理。
	商業環境（BE）	ID. BE 1-5	了解組織的使命、目標、利益相關者和活動並確定其優先順序； 該資訊用於告知網路安全角色、責任和風險管理決策。
	治理（GV）	ID. GV 1-4	了解管理和監控組織的規範、法律、風險、環境和營運要求之相關政策、程序和流程，並為網路安全風險之管理提供資訊。

功能	類別	子類別	檢核重點
	風險評估（RA）	ID.RA 1-6	了解與組織營運（包括使命、功能、形象或聲譽）、組織資產和個人相關的網路安全風險。
	風險管理策略（RM）	ID.RM 1-3	建立組織的優先事項、限制、風險耐受力和假設並用於支持營運風險決策。
保護（PR）	存取控制（AC）	PR.AC 1-5	對資產和相關設施的存取僅限於授權使用者、流程或設備，以及授權活動和交易。
	意識與訓練（AT）	PR.AT 1-5	組織人員和合作夥伴接受網路安全意識教育，接受充分培訓以履行與相關政策、程序和協議一致的資訊安全相關義務和責任。
	資料安全（DS）	PR.DS 1-7	資訊和記錄（資料）按照組織的風險策略進行管理，以保護資訊的機密性、完整性和可用性。
	資訊防護程序（IP）	PR.IP 1-12	維護安全策略（處理目的、範圍、角色、責任、管理承諾和組織實體之間的協調）、流程和程序，並用於管理資訊系統和資產的保護。
	維護（MA）	PR.MA 1-2	按照政策和程序進行工業控制和資訊系統元件的維護和維修。
	保護技術（PR）	PR.PT 1-4	管理技術安全解決方案以確保系統和資產的安全性和彈性，符合相關政策、程序和協議。

功能	類別	子類別	檢核重點
偵測（DE）	異常事件（AE）	DE.AE 1-5	及時偵測到異常活動並了解事件的潛在影響。
	安全持續監控（CM）	DE.CM 1-8	以離散的時間間隔監控資訊系統和資產，以識別網路安全事件並驗證保護措施的有效性。
	偵測過程（DP）	DE.DP 1-5	維護和測試偵測過程和程序，以確保能及時和充分了解異常事件。
回應（RS）	回應規劃（RP）	RS.RP 1	執行和維護回應流程和程序，以確保及時回應偵測到的網路安全事件。
	溝通（CO）	RS.CO 1-5	內部和外部利益相關者酌情協調回應活動。
	分析（AN）	RS.AN 1-4	執行分析以確保充分回應並支持復原活動。
	減緩（MI）	RS.MI 1-3	執行活動以防止事件擴大、減輕其影響並根除事件。
	改善（IM）	RS.IM 1-2	透過整合從當前和先前的偵測／回應活動中汲取的經驗，改進組織回應活動。
復原（RC）	復原規劃（RP）	RC.RP 1	執行和維護復原流程和程序，以確保及時恢復受網路安全事件影響的系統或資產。
	改善（IM）	RC.IM 1-2	將汲取的經驗納入未來的活動，以改進復原計畫和流程。

功能	類別	子類別	檢核重點
	溝通（CO）	RC.CO 1-3	復原活動與內部和外部各方協調，例如協調中心（coordinating centers）、網路服務供應商、攻擊系統的所有者、受害者、其他電腦資安事件應變小組（Computer Security Incident Response Team, CSIRT）和供應商。

資料來源：IEEE，DNS Security Management，本計畫整理

此框架核心為各項檢核項目提出與 DNS 有關的潛在安全事件，並提供相關參考文件，例如產業標準、指南和實踐基準等，主要參考文件包括資訊系統稽核與控制協會（Information Systems Audit and Control Association, ISACA）之「資訊及相關技術控制目標」（Control Objectives for Information and Related Technology, COBIT）、ISO/IEC 27001、ISA/IEC 62443，以及美國國家標準技術研究所（National Institute of Standards and Technology, NIST）所擬訂的聯邦資訊系統與組織之安全與隱私控制建議書（NIST SP 800-53A Rev.4）。以下特別列出依據 IEC62443、但未依據 ISO27001 控制措施，可作為本計畫所擬定之資安框架未來可用之檢核項目參考：

1. 商業環境（Business Environment）
   (1) 確認組織在關鍵基礎設施及其產業部門中的定位（ID.BE-2）：根據關鍵程度（criticality）對 DNS 元件進行分類和優先級別排序，以在 DNS 伺服器遭到入侵，或終端使用者被重定向（redirect）到外部惡意網站時，為緊急應對計畫做好準備；定義組織可能面對之 DNS 伺服器故障或外部 DNS 供應商漏洞等緊急事件。
   (2) 建立組織使命、目標和活動的優先級別（ID.BE-3）：

在商業流程定義中顧及 DNS 的資訊安全和由此產生的風險、緊要性評估（criticality assessment）以及資訊保護需求。

2. 治理（Governance）

應以風險管理流程治理網路安全風險（ID.GV-4），即將 DNS 含括在組織的風險管理流程中，由管理層批准並發布給內部員工和相關外部員工，並提供培訓。

3. 風險評估（Risk Assessment）

(1) 辨識與記錄內部及外部威脅（ID.RA-3）：

監控、記錄並追蹤偵測到和回報的 DNS 解析器和伺服器軟體應用程式漏洞；記錄與個人問題、人為錯誤以及自然和非自然災害相關的威脅；監控、記錄和追蹤偵測到和回報的外部 DNS 伺服器和應用程式漏洞。

(2) 辨識潛在的商業衝擊和可能性（ID.RA-4）：

對於每個已識別的威脅和漏洞，記錄威脅發生時的相關商業衝擊；同時對於每個已識別的威脅和漏洞，記錄其發生的可能性。

(3) 辨識並確定風險回應的優先級別（ID.RA-6）：

定義並記錄識別出的每個風險的回應程序。

4. 風險管理策略（Risk Management Strategy）

(1) 風險管理流程由組織利益相關者建立、管理和同意（ID.RM-1）：

根據其發生的可能性和相關商業衝擊評估每個已識別威脅和漏洞的風險。

(2) 確定並明確表達組織風險承受能力（ID.RM-2）：

定義確定和記錄組織風險（包括 DNS）的流程並達成共識。

(3) 組織對風險的承受能力取決於其在關鍵基礎設施和產業部門特定風險分析中的角色（ID.RM-3）：
定義組織對每個已識別 DNS 風險的風險耐受力並達成共識。

5. 資料安全（Data Security）
應保護靜態資料（data at rest）（PR.DS-1），包括：一、保護 DNS 元件硬體，強化操作系統、核心（kernel）和軟體；二、實施存取控制串列（Access Control Lists, ACLs）和交易密鑰，以保護權威 DNS 資料免受更新和區域傳輸影響；三、定義存取控制串列（Access Control Lists, ACLs）以掌控存取和交易資料受到加密；四、使用 DNSSEC 驗證 DNS 資料傳送；五、異地儲存的 DNS 配置和記錄資料必須通過加密進行安全傳輸；六、監控漏洞源並部署影響靜態資料的供應商補丁；七、定期審核 DNS 元件存取記錄和執行功能與角色和責任保持一致。

6. 異常事件（Anomalies and Events）
(1) 為使用者和系統建立和管理網路運作和預期資料流的基準（DE.AE-1）：
持續性監控和追蹤 DNS 流量，以及包括 CPU、HD、記憶體、I/O 等 DNS 伺服器重要資訊。
(2) 從多重來源和感測器聚集和連結 DNS 事件資料（DE.AE-3）：
將 DNS 事件資料安全地傳輸到更廣泛的網路安全事件資訊系統，以協助故障排除。
(3) 確定事件影響（DE.AE-4）：
確定 DNS 事件的影響以排序緩解工作的優先級別。
(4) 建立事件警報門檻（DE.AE-5）：

制定事件回應計畫以定義潛在事件和相應的回應計畫；定期審查、批准和更新事件回應計畫；並在監控系統中建立門檻和警報，以偵測和報告潛在的安全事件。

7. 安全持續監控（Security Continuous Monitoring）
   (1) 監控網路以偵測潛在的網路安全事件（DE.CM-1）：
   監控 DNS 流量以及 DNS 伺服器重要資訊（CPU、HD、記憶體、I/O），以偵測異常使用及潛在網路安全事件。
   (2) 監控物理環境以偵測潛在網路安全事件（DE.CM-2）：
   包括：一、監控物理存取控制和 DNS 元件所在的物理環境，以偵測潛在事件；二、存取關鍵基礎設施（包括 DNS 伺服器）需要使用徽章存取權限（badge-in access）；三、審查存取記錄；四、部署監控系統以偵測尾隨（tailgating）、未授權人員進入，以及審查資產的物理轉移。
   (3) 監控未授權人員、連接、設備和軟體（DE.CM-7）：
   監控安全區域中出現未授權人員的發生率；且任何此類違規事件都應根據事件回應計畫通知並進行調查。
8. 回應─溝通（Respond-Communication）
   (1) 與利益相關者的協調與回應計畫一致（RS.CO-4）：
   根據事件回應計畫將 DNS 安全事件回應資訊傳達給適當的利益相關者。
   (2) 與外部的利益相關者進行自願性資訊共享，以實現更廣泛的網路安全態勢感知（RS.CO-5）：
   將 DNS 安全事件回應資訊傳達給外部的利益相關者，以促進整體產業對攻擊的認識和建立有效的防禦措施。
9. 回應─改善（Respond-Improvements）

應更新回應策略（RS.IM-2），即適當審查和更新安全事件的回應策略。

10. 復原─改善（Recover-Improvements）
    (1) 汲取經驗併入復原計畫（RC.IM-1）：汲取安全事件經驗以更新復原計畫。
    (2) 更新復原策略（RC.IM-2）：從事件復原分析對復原策略進行審查和更新。
11. 復原─溝通（Recover-Communication）
    (1) 管理公共關係（RC.CO-1）：
    與客戶和一般公眾溝通，以傳達安全事件、回應和復原狀態以及計畫行動的相關資訊。
    (2) 修復事件後的聲望（RC.CO-2）：
    提供有意義的資訊（包括已採取的復原措施）有助於修復聲望，同時也必須採取具體復原行動。

此份框架顯示 DNS 做為核心系統在導入稽核管理機制的步驟，與 ISO27001 組織稽核概念相通，不過從 5、6、7 點特別針對 DNS 域名解析、資料儲存的運作機制進行設計。

四、下世代跨網互通安全策略

(一) 非 3GPP 網路跨網互通環境安全

在未來異質網路共存的場景，實行跨網互通的 5G/B5G 網路除了支援 5GNR、也須向下相容既有的行動通訊技術如 4G LTE 或連結 WLAN、有線網路與衛星網路的連接。由於各種無線電通訊終端裝置如手機、小型衛星地面終端設備（Very Small Aperture Terminal, VSAT）的推廣與普及，推測無線通訊將成為異質網路近期的發展主力。在 WLAN 部分，就可能會由不同覆蓋範圍與功率的大、小型基地臺相互連接，網路範圍將同時連結 3GPP 標準定義之蜂巢式網路與非 3GPP 標準定義之熱點覆蓋部署等。

因此，5G 核心網路（簡稱 5GC）跨網互通安全也納入具備終端裝置（UE）連結非 3GPP 接取網路（non-3GPP access network），例如 WLAN、有線網路（wireline network）的安全性考量。其實不論非 3GPP 接取網路的類型為何，5GC 原先就具備一定程度的安全防護功能，其透過網際網路金鑰交換（Internet Key Exchange v2, IKEv2），產生一或多組 IPsec ESP（Encapsulating Security Payload）建立安全關聯（Security Association, SA），做為身分認證機制[192]。

基本上金鑰交換認證具有階層性，第一階段為初始認證，是確定所有裝置為提供行動網路服務接取，第二階段為外部數據網路（data network）認證，是透過與使用者裝置中的元件模組（即 USIM）核對憑證（credential），才能進行安全存取，並使用憑證來接取數據網路。故非 3GPP 接取網路同樣也需完成第一階段金鑰認證，才能被視為「可信任的非 3GPP 接取網路」（Trusted Non-3GPP Access Network, TNAN）。

在 TNAN 認證過程中，負責產生（initiate）與接收（receive）IKEv2 金鑰者分別對應到 UE 與 5GC 中非 3GPP 互連功能介面（Non-3GPP InterWorking Function, N3IWF），由 UE 產生金鑰，N3IWF 做出回應（respond），再傳遞給 AMF 產生金鑰進行交換[193]。一般而言，無論在漫遊（roaming）或非漫遊情境，均有特定的網路營運商依據公眾陸上行動網路（Public Land Mobile Network, PLMN）的網路政策，決定非 3GPP 接取網路是否屬於 TNAN；而 UE 的信任架構也已預先配置（pre-configured）且符合 TS.23.501 文件技術標準，即使（在同一個 TNAN 中）支援多重 DN 時，也需同樣保持信任關係[194]。

---

[192] 由 Microsoft 和 Cisco 開發的新一版安全協定，與其他協定不同是需要建立安全關聯。

[193] 3GPP, *3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;*Security Architecture and procedures for 5G System;Stage 2, (Release 17), TS 33.501 v17.2.1 https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-h21.zip(last visited：Oct. 4, 2021), p.113.

[194] *Id.*

以下就 TNAN 中 WLAN 互連、有線網路互連、以及 non-TNAN 互連進行說明：

1. 與 WLAN 互連

在 WLAN 與 5GC 的互連上，雖然 UE 並不支援 5GC 的網路連接儲存（Network Attached Storage, NAS）註冊，這些不支援的裝置（簡稱 N5CW）得以藉由可信任的 WLAN 的互連功能介面（Trusted WLAN Interworking Function , TWIF）提供 5G NAS 協定堆疊（protocol stack）給 5GC 中的 AMF 元件，5NCW 透過適用於 UTMS[195] 驗證與金鑰協議之延伸驗證通訊協定方法（Extension Authentication Protocol for UMTSAuthentication and Key Agreement, EAP-AKA）[196]，並提供網路接取身分（Network Access Identity ,NAI）給 WLAN，執行 WLAN 接取與 5GC 的連接[197]。

2. 與有線網路互連

在有線網路（wireline network）與 5GC 的互連上，要支援 5G 系統與固網之整合，須具備兩種家用閘道器（Residential Gateway, RG），一是 5G 家用閘道器（5G- Residential Gateway, 5G-RG），另一個是固定-無線家用閘道器（Fixed Wireless Residential Gateway, FN-RG）。5G-RG 可同時透過 5G 有線接取網路（Wireline access network, W-5GAN）與固定－無線接取網路（Fixed Wireless Access, FWA）連結至 5GC，但 FN-RG 僅能透過 W-5GAN 來連接。

(1) 5G-RG 認證

5G-RG 的認證需具備同時支援 5G 無線接取網路（即 5G-RAN）的金鑰認證（5G-AKA）與有線接取網路（即 W-5GAN）的金鑰認證（即 EAP-AKA）的能力，並須通過 3GPP 家用網路（home

[195] 通用行動通訊系統（Universal Mobile Telecommunications System, UMTS），為 3G 技術的技術標準，由 GSM 衍生出來的規格標準，此處特別指驗證與作業階段金鑰方配的 EAP 機制，用來驗證 UMTS 用戶識別模組(USIM)。

[196] EAP 是 5G 特有的認證架構，可以封裝各種認證協定。

[197] 3GPP, *supra note* at.*193*, p.121

network）認證。

若連結 5G-RAN，5G-AKA 的認證方式與 UE 連網的認證機制相同；若連結 W-5GAN，則須用 EAP-5G 認證方式封裝 NAS 訊息，其認證過程係透過 W-AGF 代表 5G-RG 選擇對應的 AMF 以傳遞 UE 的註冊需求（Registration Request），經過各元件金鑰提取（derive）機制傳至 AUSF，由 AUSF 做 UE 身分認證的最終決定，再依循原路徑傳遞錨定金鑰（anchor key）將已封裝 NAS 訊息的安全模式指令（Security Mode Command, SMC）回傳給 UE 完成金鑰交換[198]。換言之，5G-RG 在家用 Wi-Fi 無線連網情境上，與 5G 行動網路認證機制相同，若以整合有線網路的方式連網，將循 EAP-AKA 的金鑰交換機制接取 5GC。

(2) FN-RG 認證

FN-RG 的認證方法透過寬頻聯盟（BroadBand Forum, BBF）或美國有線電視實驗室（CableLabs），由於認證方法不屬於 3GPP 範疇，由 W-AGF 代表 FN-RG 產生註冊需求給 AMF。接下來的步驟與 5G-RG 不同處在於，AMF 將註冊需求傳給 AUSF 後，會再傳給統一數據管理（Unified Data Management, UDM）元件做最終身分驗證，驗證機制是將 FN-RG 的用戶隱藏識別碼（subscription concealed identifier, SUCI）對映資料檔（profile）中的用戶永久識別碼（subscription permanent identifier, SUPI）。認證信令回傳的過程中，AUSF 不提供認證、也不產生金鑰，最終由 AMF 傳遞「接受註冊」的訊息給 W-AGF，其中訊息包括 5G 全球唯一臨時識別碼（5G Global Temporary UE Identity, 5G-GUTI）與其他指標[199]。換言之，FN-RG 在接取 Wi-Fi 無線連網情境上，已經假設在網路營運層面有線網路與 5G 網路營運商對於 W-5GAN 和 PLMN 網路管理取得信任關係，故其驗證方式不須透過金鑰交換與家用網路

[198] *Id.*, pp.124-125.
[199] *Id.*, pp.125-127.

認證。

(3) 連結 5G-RG 和 FN-RG 的 UE 認證

UE 裝置連結家用閘道器的認證部分，則可以透過 N3IWF 或可信任的非 3GPP 閘道器功能（Trusted Non-3GPP Gateway Function, TNGF）

進行，相關規定均定義於 TS 23.502 文件中。

3. 與不信任的非 3GPP 網路互連

當 UE 連接非 TNAN 時，使用稱作「EAP-5G」的特定供應商（vendor- specific）EAP 認證機制，利用擴充的 EAP 類型，和既有的 3GPP 供應商 ID（Vendor-Id）[200]封裝 NAS 訊息，以便進行 UE 和 N3IWF 介面的認證。因此，UE 僅需透過前述的 IKE 初始金鑰交換認證，與 N3IWF 介面建立 IPsec 安全關聯後，確保已加密的 IKE 訊息的完整性。換言之，非 TNAN 認證過程原則上是對加密金鑰的完整性（integrity）進行驗證。

其實 5GC 本身即具備統一的認證架構，不僅可以降低電信業者投資與營運成本，也提供靈活多樣的安全憑證管理，與傳統行動網路安全技術相較更為安全。

然而，隨者網路互通程度越高，攻擊型態反而因大數據技術分析而更難預測，大量流通於網路世界的數據與重要資訊可能會受到嚴重侵害 5G 網路雖提高本身的安全性與相容性，然而各個網路節點的安全性並未同步的提升，像是 UE 裝置安全等級的差異、或雲端化網路的集中部署均有可能成為潛在的安全漏洞。

推究「零信任網路」近年不斷受到重視與討論，其原因在現階段網路環境中，進階持續性威脅（Advanced Persistent Threat, APT）的頻繁攻擊。由於近年存取方式之改變，因疫情產生的遠端工作，加上自攜裝置（By Your Own Device, BYOD）與雲端運

[200] 該供應商 ID 註冊於 IANA 下的 SMI 私人企業註冊碼註冊機構（SMI Private Enterprise Code registry）；SMI 為結構管理資訊（Structure Management Information）的簡稱。

算資源服務日益普及，APT 不直接攻擊核心母系統，利用信任之帳號存取或子系統存取所引發之漏洞，啟動後門監聽功能間接滲透至核心系統，組織邊界的模糊也造就影子物聯網資安威脅。據資安廠商 Positive Technologies 之資安研究團隊報告所示，新的 APT 駭侵團體長期以系統化方式攻擊俄羅斯、美國、印度、尼泊爾、臺灣、日本等政府機關、能源、航空宇其他製造業，80%為資料竊取行為，包括客戶、上下游廠商等利害關係人之機敏資料，或取得重要伺服器與基礎設施之控制權 。基此，自美國 NIST 提出 SP800-207 零信任架構規範起，美國國防資訊局（Defense Information Systems Agency，DISA）亦開始推動相關指引。此外，眾多資安廠商也因應此趨勢提供零信任平臺與相關安全可視化、自動化的資安產品。

不過，零信任架構之建立並未有固定的做法，需導入資訊與網路安全系統管理的組織，應以落實組織資安政策的需求為優先考量點，來訂定相關存取控制與網路安全控制措施並執行稽核作業，方能對組織風險處理規劃上產生實質助益。

臺灣科技大學教授查士朝博士強調，「零信任」架構中仍存在「信任」關係，而是不純粹信任內外「網路邊界」作為安全的憑藉；從 NIST 的角度看待零信任網路環境的核心元件如圖 3-8，重點在經過「資訊存取控制」政策落實點（Policy Enforcement Point, PEP）進行權限檢查，並透過政策決策點（Policy Decision Point, PDP）判斷是否有權限執行，此處需考量多面向的資訊，包括圖中左右兩側的資訊，例如：身分管理、活動紀錄、持續診斷與風險減輕 CDM 系統、PKI 等進行存取決策。

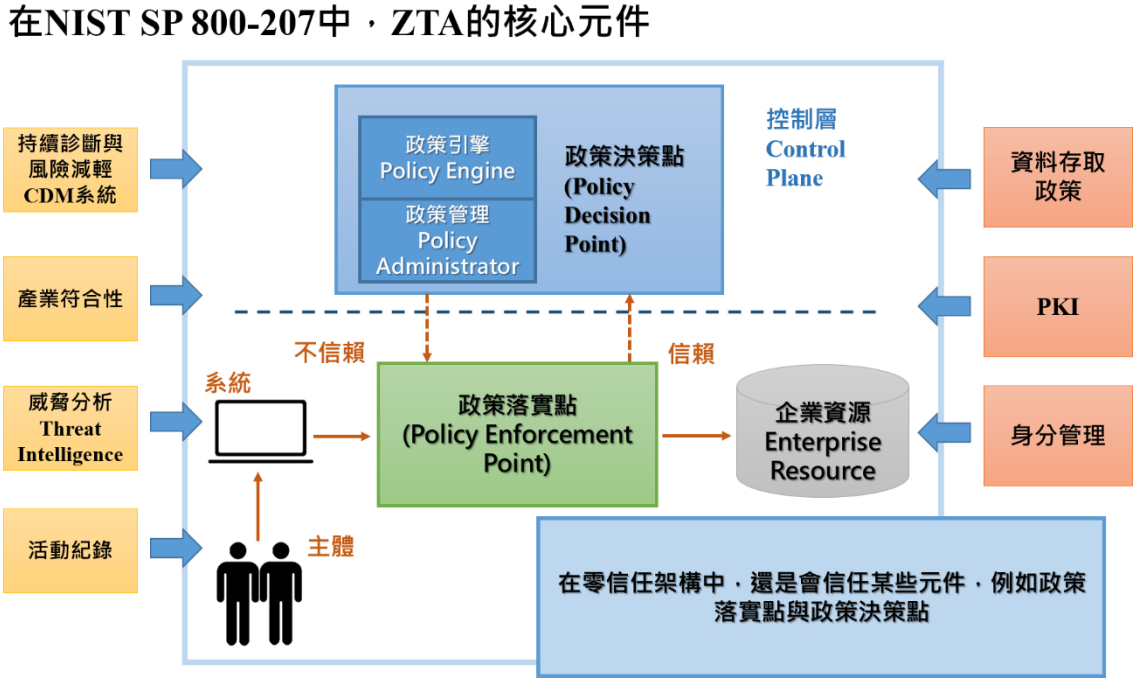


圖 3- 8、NIST SP 800-207 零信任架構與核心元件關聯圖
資料來源：iThome，2021 年臺灣資安大會，查士朝簡報。

簡言之，在零信任架構下，企業組織依然可以信任某些核心的邏輯元件，也就是所謂的 PEP 與 PDP，從存取控制概念來看，則可以分為「可存取資源識別」、「使用者層級的存取控制」、「存取控制加入對風險的考量」。舉上述跨網互通環境資安的例子，即是 5GC 核心網路元件與邊緣網路元件之間所建立的信任機制，可以因需求被組織列為 PEP 與 PDP 的考量項目。

(二) 因應下世代跨網互通安全建立稽核框架

基於上述既有網路與下世代網路落差、國際稽核標準與框架比較、跨網互通環境安全與零信任架構等背景分析。研究團隊認為，可以提取 NIST 零信任原則與零信任網路概念，結合既有的國際標準來進行資安風險管理稽核指引的框架。

1. 稽核策略目標：NIST 零信任概念

針對 NIST 零信任的幾項重點策略，作為稽核框架的原則：

- 企業資安策略：

- 盡可能收集有關資訊資產、網路架構、骨幹及通訊現況
- 企業宜監控、衡量所有擁有與相關資訊資產的正確性與安全狀態。

• 企業網路架構：

- 專用網路不被視為隱性信任區域，資源存取應視同攻擊者存在企業網路中。
- 並非所有企業資源都存於企業擁有的基礎設施，企業所屬資產管理會需要利用外部網路進行連接和網路服務。

• 企業資訊資產：

- 每項資產都必須通過政策落實點（Policy Enforcement Point, PEP）評估。
- 網路上顯示的設備可能並非由企業擁有或配置。

• 企業營運：

- 企業內外部基礎設施之間移動資產與工作流（work flow）之安全策略需保持一致。
- 資源存取上允許存取前所有資源的身分識別與授權均依監控結果動態決定。

2. 稽核框架建立原則：以 ISO27001 為章節骨幹，IEC62443 於涉及系統之章節內容補充，IEEE DNS 框架作為作為參考控制措施

基於 ISO 與 IEC 稽核框架均以「風險管理」為重點，故章節架構安排以 ISO27001 為骨幹，結合 IEC62443 重視的系統元件之監控防護評估，以及其他涉及系統之章節補充；條列原則將會參考 IEEE DNS 框架之運用，擇要放入參考控制措施，整體框架與關聯如圖 3-9 及表 3-11 為章節安排，由於本計畫階段主要集中於政策與策略之擬定，故放入擬增加 IEC62443 用語、部分 NIST 零信任原則的子項目作為結合之範例。

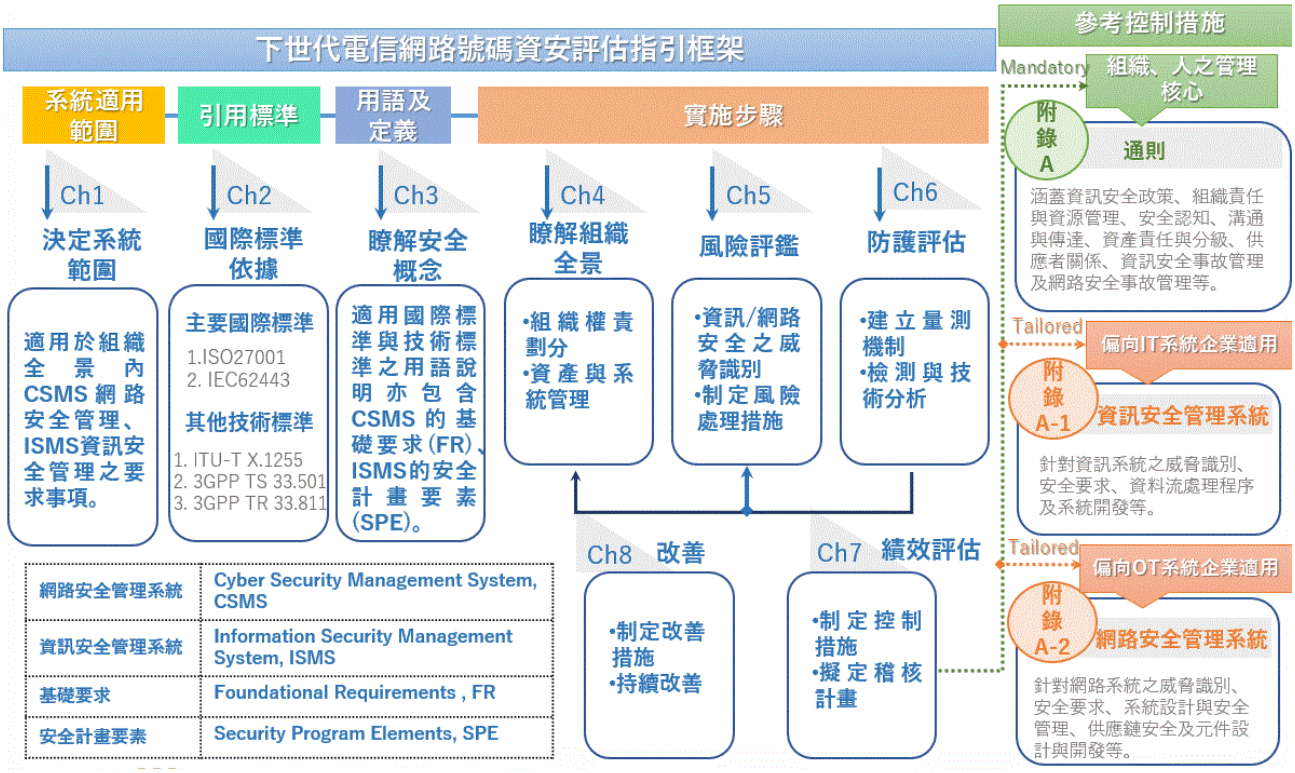


圖 3- 9、下世代電信網路號碼資安評估指引整體架構

資料來源：本計畫整理

表 3- 11、下世代電信網路號碼資安評估指引框架章節安排

第 1 章 適用範圍（Scope） ■ 本框架適用於組織全景內網路安全系統、資訊安全管理系統之要求事項
第 2 章 引用標準（Normative references） ■ 下列標準因本標準所引用，成為本標準之一部分（待持續增修）。 ➢ ISO:27001:2013 ➢ IEC 62443-2-2 ➢ IEC 62443-4-1
第 3 章 用語釋義（Teams and Definitions） ■ 網路安全管理系統（Cybersecurity Management System, CSMS）

■ 資訊安全管理系統（Information Security Management System, ISMS）

■ 基礎要求（Fundamental Requirements, FR）

note: 參考附錄 A-2

■ 安全計畫要素（Safe Plan Elements, SPE）

note: 參考附錄 A-2

第 4 章 組織全景（Contest of the organization）

■ 政策

- 企業宜盡可能收集有關資訊資產、網路架構、骨幹及通訊現況
- 企業宜監控、衡量所擁有資訊資產相關之正確性與安全狀態
- 企業內外部基礎設施之間移動資產與工作流（work flow）之安全策略需保持一致

第 5 章 風險評鑑（Risk Assessment）

■因應風險及機會之行動

- 每項資訊資產都必須依政策落實點（Policy Enforcement Point, PEP）評估決定政策決策點（Policy Decision Point ）

note:網路上顯示的設備可能並非由企業擁有或配置

note:參考 IEC62443-2-2 相關規範

- 須依組織需求訂定核心系統之風險識別、風險處理、風險評估之風險管理計畫。

note:參考 IEEE DNS Security Management 相關規範

第 6 章 防護評估（Security Assessment）

■組織安全目標及其達成之規劃

➢ 每項資訊資產都必須依第 5 章之 PEP 規劃下之政策決策點（Policy Decision Point）執行安全稽核計畫。 ➢ 資源存取上允許存取前所有資源的身分識別與授權均依監控結果動態決定 ➢ 針對本框架之適用範圍，須依第 5 章訂定之風險管理計畫進行資安威脅識別、資產保護、資安事件之偵測、回應與復原層級項目制定稽核計畫。 *note:參考 IEEE DNS Security Management 相關規範*
第 7 章 績效評估（Support） ■網路安全管理系統控制措施 *note: 參考附錄 A-2*
第 8 章 持續改善（Improvement）

資料來源：本計畫整理

1. 框架使用方法：

(1) 理解本框架架構與使用重點

- 第 1 章將 OT 與 IT 的系統範圍皆納入考量，預計條文會增加 OT 與 IT 系統之間關聯性釐清之文字。
- 第 2 章以 ISO、IEC 國際標準作為組織管理、系統環境管理為核心；而為具體控制措施之制定，將會引用其他相關技術標準。
- 實施步驟為第 4 至第 8 章，依據實際稽核導入的步驟。
- 參考控制措施部分，為因應數位轉型企業本身產業別、企業型態的不同，因此在 OT 環境與 IT 環境比重上不同的差異，故針對 ISO27001 的參考控制措施附錄 A 進行改良，細分為「通則」、附錄 A-1 「網路安全管理系統」、附錄 A-2「資訊安全管理系統」，在稽核計畫起動時，稽核小組可以依據組織企業環境之需求，揀選著重於附錄 A-1 或附錄 A-2 的控制措施。

(2) 理解框架適用對象

- 由於落實資安意識與全民資安防護，框架條文基本上會囊括原

則性、具體須注意事項（note）等文字內容，故適用對象係為以「DNS 號碼管理系統」為核心系統雛型，應用於智慧聯網企業等垂直領域業者，但可同時為政府機構、第三方稽核機構作為原則性指引的基礎標準，此基礎標準為類似的核心系統於系統開發、系統驗證、系統營運等生命週期中資訊安全風險評估之最低標準。

(三) 政府機構使用框架策略說明

此稽核框架設計主體對象雖然為智慧聯網企業等垂直領域業者，然政府機構為協助推動國家大型資通訊政策落實與資安法制調適，故本框架放在政策推動角度，希望能不與各部門的資安推行計畫產生扞格為原則，考量作為技術面：包括資安檢測工具、檢測平臺開發環境，法制面：強化利害關係人的情資共享體系、提升資安意識的補充架構。故研究團隊參考智慧國家方案的推動主軸，將下世代電信網路號碼管理稽核框架之使用目的訂定為「**建構跨部門、跨域資料之共通基礎，以 DNS 編碼管理系統作為核心，完備下世代資料治理之推動架構**」。

本框架之資安標的係以數位基盤之先進網路技術驗證（即 DNS 編碼系統管理）的下世代網路情境與技術之系統環境進行策略性的擬定，為落實資安風險預防的概念、也是所有稽核作業最為模糊之處，係為「**瞭解與定義組織內外部環境**」以及對「**利害關係人（關注方）重視的議題**」進行界定。結合國家政策面的規模看待我國資通安全整體環境政策之議題，可歸納出「網路資源識別」、「5G 虛擬化網路資源管理」、「商用物聯網應用管理」三大議題，分別對應到，數位治理、數位基盤、數位創新三大推動主軸，參考如圖 3-10。

- 數位治理策略：落實資安制度導入、建構資料治理生態系（對應網路資源識別議題）
- 數位基盤策略：異質網路安全維護，推動寬頻普及應用（對

應 5G 虛擬化網路資源管理）

- 數位創新策略：提供智慧化、運用物聯網企業之參考措施，鼓勵數位轉型（對應商用物聯網應用管理議題）

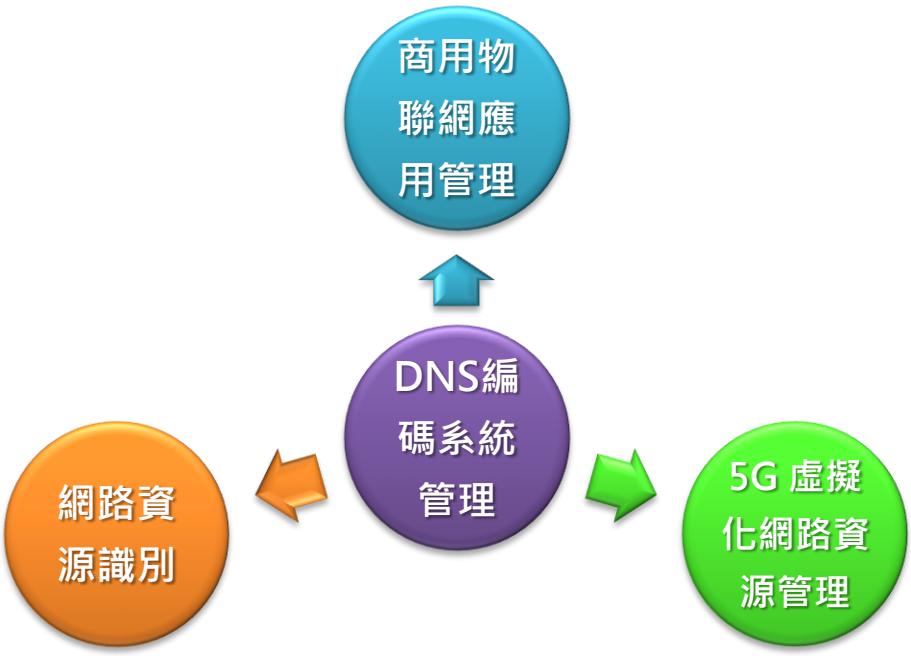


圖 3- 10、下世代電信號碼管理政策關聯議題

資料來源：本計畫整理

在定義完三大議題後，即針對各項議題中，各利害關係方所關注的項目（或痛點）進行通盤性檢視，檢視原則以「風險管理」角度訂定安全等級，此處的安全等級預計將會扣連資安框架中的風險評鑑政策條文。簡言之，**檢視原則：(1)在三大議題下，以 DNS 號碼管理的需求程度決定安全等級，(2)並考量政府機構、電信營運商、網通及物聯設備供應商、垂直領域業者彼此互為利害關係方，對彼此之要求（詳參圖 3-11）。首先是外部議題：**

- **政府機構要求**
  - 電信營運商：維護數位關鍵基礎設施之安全。
  - 網通及物聯設備供應商：設備產品是否合規。
  - 垂直領域業者：場域是否符合服務安全規範。

- **電信營運商要求**
  - 政府機構：維持電信資源分配與管理之公平性。
  - 網通及物聯設備供應商：提供之具安全、可靠之設備產品。
  - 垂直領域業者：**確保前瞻技術應用如網路切片、專用網路安全。**
- **網通及物聯設備供應商要求**
  - 政府機構：能透過 IPv6 商用、創新應用政策之推廣，促進 IPv6 實質應用。
  - 電信營運商：**確保前瞻技術應用下設備營運環境之安全性。**
  - 垂直領域業者：**確保前瞻技術應用下設備營運環境之安全性。**
- **垂直領域業者要求**
  - 政府機構：推動明確之專用網路政策或規則以遵循。
  - 電信營運商：確保前瞻技術如網路切片系統之安全性；跨網互通傳輸封包加密之安全、機密數據之儲存安全。
  - 網通及物聯設備供應商：設備產品、系統簡化與整合；專網設備之安全性。

內部議題部分，則會因為創新應用服務的推廣策略、企業市場競爭而有所變化，依據現階段評估為：

- **政府機構：開放資料與物聯網管理應用。**
- **電信營運商：網路切片市場**
- **網通及物聯設備供應商：空中編程（Over-the-air, OTA）市場**
- **垂直領域業者：物聯應用市場**

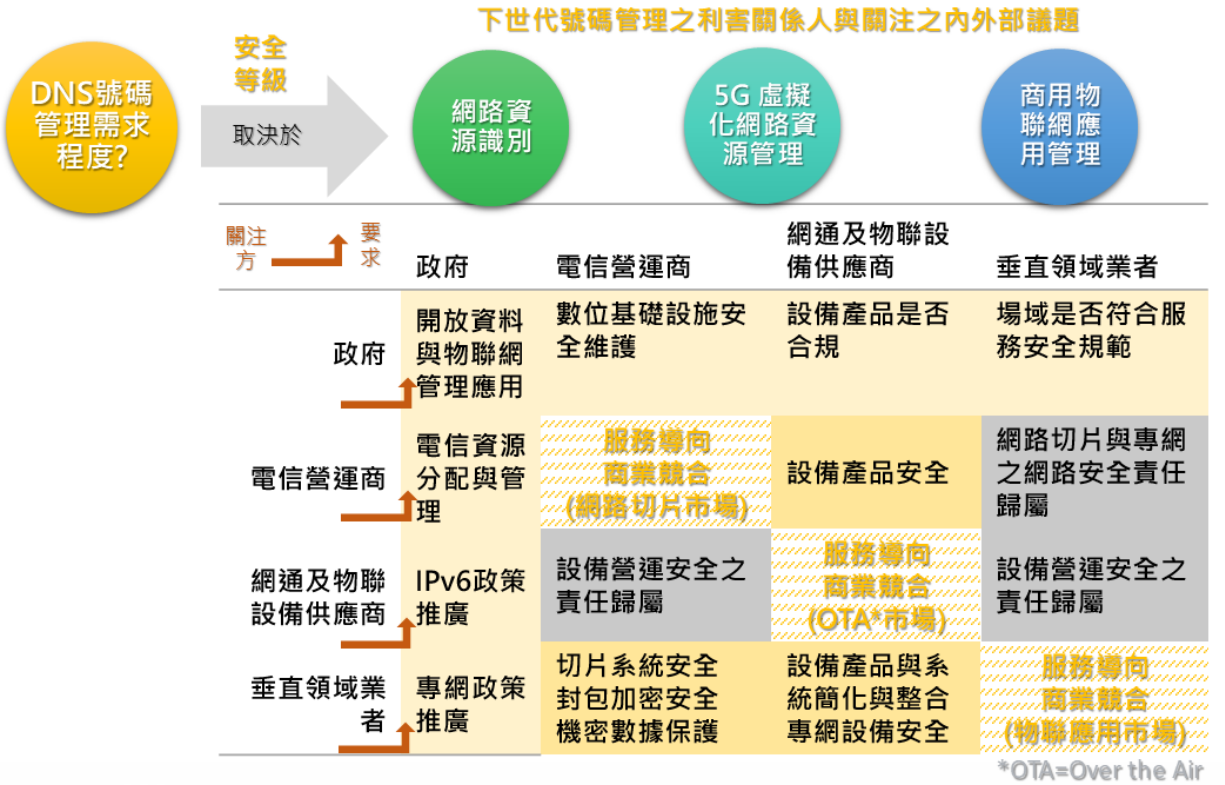


圖 3- 11、關注方對應 DNS 號碼管理議題之要求

資料來源：本計畫整理

根據圖 3-11 表格，則可初步提供欲進行資安風險等級建立之組織進行外部議題的錨定，另一方面，也得以瞭解利害關係方內部議題，以進行風險規劃。

第四節　小結

在 ITU 提出下世代電信網路（Network 2030）的願景下，網路的技術與結構朝向具有更高度異質網路整合發展，同時，也更能重新切片組合以面對各種應用服務需求。由於在下世代網路效能提升的同時，因技術缺陷或網路攻擊恐導致的資訊安全風險與經濟損失將會較以往更為嚴重、涉及層面更為廣泛。研究團隊透過重新識別既有網路各層級之安全需求與下世代網路之差異，接著敘明先進國家目前整體資通安全規範的實施重點，瞭解各國網路安全策略走向，作為建立下世代電信號碼資安稽核機制、電信網路號碼安全管理系統及跨網互通安全策略之基礎。

一、觀測既有網路與下世代網路資安需求差異與國際策略

於下世代網路需求上，本計畫歸納出「多邊緣接取網路」、「關鍵基礎設施」、「路由定址與通訊協定」三層安全需求。在建置多邊緣接取網路時，該網路需要具備高度獨立性與即時備援性能；在關鍵基礎設施建置上，未來虛擬網路環境、硬體軟體化、連網規模提升情況下，若能源、廠房等重要設施一旦防護失靈，將形成巨大經濟損失，故須重視全面性的網路防護。而路由定址與通訊協定，則須考量在多種裝置與應用軟體、網路互連情境下，要加強對資料流的識別；亦須注意內部網路資料流通的安全性。

目前網路技術演進上逐步朝著以「服務」為本的系統架構。以 5G 技術發展為例，在行動通訊領域中已具備下世代網路的許多特徵，透過軟體定義網路（SDN）結合網路切片技術與邊緣運算（MEC）組成的核心網路架構，有望可在專用網段中同時實現超寬頻（eMBB）、巨量連結（mMTC）與超低延遲（URLLC）等應用服務場景。然而，相較下世代網路塑造出的多重接取、多重技術應用環境，仍欠缺對於異質網路整合、跨網路層級資料傳遞等相對複雜化的部分。故以資安層面而論，單就 5G 背景下的網路架構、切片技術、IPv6、DNS 各網路節點的資訊安全需求，均已看到各別的資安防護技術之提出，但於實務

面尚未用「零信任網路」思維加以整合到整個網路系統環境，以面對將來更趨多樣化、範圍更廣的網路攻擊型態。

先進國家在因應下世代網路資安需求的做法上，各國依據國情各有所側重，但均不脫離「制定、導入資安管理框架」、「因應技術發展強化關鍵基礎設施防護體制」、「與利害關係人情資共享、提倡國際合作」三大面向。

歐盟以「監管」、「投資」、「政策」為三大主軸，設立較為前瞻的資安願景；資安戰略則是以技術為導向，期望發展 AI 資安監控中心、部署量子通訊基礎設施，因應下世代寬頻網路與物聯網安全需求，於 ICT 產業供應鏈引入更嚴格的資安規範；美國資安防護的起手式則是由聯邦體系帶動民間產業所建立的資安框架推行，隨著技術與政策變遷，頒布特殊技術文件予聯邦單位實行；現階段美國將持續推行資安框架、著重強化 5G 資安防護。

新加坡則以邁向更安全網路空間為願景，制定三個長期耕耘之目標：一是「持續更新網路安全策略」、二是「建立彈性資訊關鍵基礎設施」、三是「發展網路安全生態系統」。其實新加坡在資安概念上走得比較前面，相較另外兩國只針對 CI（關鍵基礎設施）提出政策，進一步在 CI 概念上提出 CII（關鍵「資訊」基礎設施），制定雲端安全性標準，關注網路技術發展與數位經濟面向，於物聯網安全則針對開發、供應者、使用者、物聯系統實施或營運各階段提出網路安全基準建議，加強各階段之問責性。

雖然歐盟、美國、新加坡各國針對下世代網路的願景法規調適尚在討論階段，但從各國提出之未來政策與願景，以及電信技術與市場演進，推導出各國未來資安管控重點皆因應所謂廣義的「萬物聯網」環境做通盤性的計畫，重點歸納為三項：

- 以風險管理為基礎，建構資安框架，由公到私之階段性導入
- 針對產品供應鏈之安全管理與人員管理，訂定資安義務要求
- 強調設備或系統於開發初期即納入安全技術考量

二、以「零信任概念」建立下世代電信號碼稽核機制

基於上述國際資訊安全需求趨勢的探析可知，在未來萬物聯網的環境，各種終端裝置均有可能因為用戶的使用行為而成為「影子物聯網」的一環。影子物聯網的每個潛在的物聯節點，都有可能提高駭客越權存取、後門程式入侵的風險，造成資料喪失完整、可用、機密性以及連帶的經濟損失。研究團隊認為，應以個人資料的隱私安全保護作為目標，針對組織內部關鍵系統去建構實質意義上的零信任網路環境。進一步言之，如何確保資料擁有者（owner）與身分（ID）、域名（DN）、IP 位址的唯一性、以及其在資料流通時的對映關係（mapping）具不可否認性（non-repudiation），將會是建構下世代網路資訊安全環境的核心策略。

以下世代電信號碼的角度來說，電信號碼、IPv6 與 DNS，並非屬於取代關係，而是跨越應用層、電信層的互動關係。換言之，在網路技術的持續變革中，電信號碼仍為電信網路中識別終端裝置的基礎，但隨著與不同網路層級的應用服務的需求、以及不同網路交互傳遞資料的需求，均會與屬於網際網路的 DNS 系統產生互動的關係。該互動關係即為下世代電信網路號碼的機制運作雛形，其所涉及的資安議題也在這個複雜的系統整合與運作中產生。

基此，研究團隊依原生於網路應用層，得以跨網互連的 DNS 作為資料管理的核心系統，參照國際稽核與技術標準，提煉出適用於下世代萬物聯網系統環境下的DN/IP資料管理稽核框架，並對此提供政府在既有的資通安全管理法架構之下，做為跨部門資料流通的基本方針。

三、以利害關係方所關注之議題擬定跨網互通策略

如前所述，研究團隊初步擬定之資安框架，將作為橋接跨部門、跨域資料之共通基礎，透過以 DNS 編碼管理系統作為核心，完備下世代網路電信號碼管理之推動策略。

在下世代網路電信號碼管理的願景下，DNS 編碼管理系統所構築

的議題將會扣合行政院大型資通訊政策之擘劃方向，在政府數位治理、數位基礎設施、數位創新應用服務三大主軸議題，分別為「網路資源識別」、「5G 虛擬化網路資源管理」與「商用物聯網應用管理」。

為落實資安領域零信任概念之整合應用，研究團隊已結合國際稽核標準概念，於策略擬定初期，識別出下世代網路環境中以 DNS 編碼管理系統為核心業務系統的組織（即關注方），其利害關係方於上述三大主軸下分別重視的內外部議題為何(詳參圖 3-12)。研究團隊歸納出（1）政府、（2）電信營運商、（3）網通及物聯設備商、（4）垂直領域業者彼此互為彼此的利害關係方。透過此 4 種角色分別期望利害關係方能提供何種幫助、面臨何種困境，以確認其跨網互通之議題痛點，研究盤點如下圖。舉例而言，在「網路資源識別」層面，政府（關注方，第 2 列、第 1 欄）要求政府（第 1 列、第 2 欄），能夠「開放資料與物聯網應用」（第 2 列、第 2 欄）。

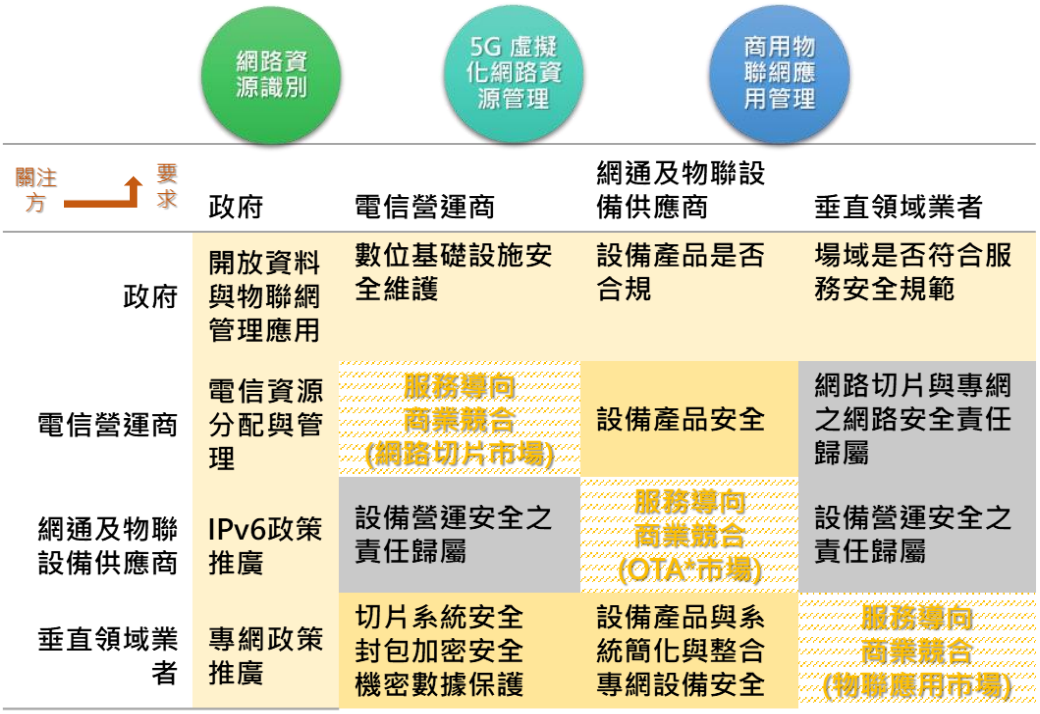


圖 3- 12、下世代電信號碼安全管理議題背景分析

資料來源：本計畫整理

其中，有三處為利害關係人之痛點與關注議題。在 5G 虛擬化網路資源管理與商用物連網管理議題上，網通及物聯設備供應商，對電信營運商（第 4 列、第 2 欄）、垂直領域業者（第 4 列、第 5 欄）分別產生「設備營運安全」的要求，然而對電信營運商與垂直領域業者而言，設備營運安全之責任歸屬、責任範疇均未強制以契約約束，或有明確的管理規則；相同情形亦發生於電信營運商要求垂直領域業者（第 3 列、第 5 欄）負起「網路切片與專網之網路安全」之責任歸屬上。藉由上表所羅列之議題，瞭解各利害關係方得以依循組織對於內外部議題的風險權重，進行 DNS 編碼管理系統安全等級的劃定與風險評估作業。

第四章　下世代電信網路號碼驗證機制

第一節　下世代電信網路號碼系統評估

第五代行動通訊技術（5th generation mobile networks, 5G）引領物聯網（Internet of Things, IoT）產業革新，設備及裝置的類型亦更趨多元。相較傳統 IoT 之應用大多係在特定空間中，裝設實體感測器（如溫度、濕度、壓力感測器等）並定時回傳數據資料，以進行遠端監控、分析及提供服務， 5G 增強型行動寬頻（Enhanced Mobile Broadband, eMBB）、超可靠及低延遲通訊（Ultra-Reliable and Low Latency Communications, URLLC）及大規模機器型通訊 （Massive Machine Type Communications, mMTC）之應用場景，實現多樣化物聯網服務，增加更多對移動性 IoT 設備之需求，注重數據資料即時傳輸能力，並帶動相關產業及應用服務如雨後春筍蓬勃發展。根據數據分析公司 Statista 預估，全球 IoT 設備使用數量將從 2020 年的 87.4 億臺，大幅躍升至 2030 年的 254 億臺[201]，管理 IoT 設備將花費更多人力、時間，如何有效識別及自動配置 IoT 設備成為關注焦點，另外國際間對 IoT 設備之電信網路編碼方式亦有多方討論。

我國行動物聯網服務之編碼原則，係交通部依國際電信聯盟（International Telecommunication Union, ITU）E.164 規約訂定之「電信網路編碼計畫」，以 040 字頭為第一類電信事業物聯網服務接取碼，提供予行動物聯網服務使用，並由國家通訊傳播委員會核配予電信業者，業者應確保門號僅用於機器通訊服務（Machine-Type Communication）。由於物聯網服務以數據資料傳輸為主，所需門號數量龐大，故採最大容量之 15 碼編碼，由國碼、區碼及用戶號碼 3 部分組成（範例 :國碼 886+40+BCDEF+GHIJK），每一門號具唯一性，管理原則採「號碼申

[201] Statista (2021/10/19), “Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030” Retrieved from https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (2021/11/26)

配」、「號碼收費」及「號碼收回」三大機制併行之方式。[202]

惟推動行動電話系統共通標準的 GSM 協會（Groupe Speciale Mobile Association, GSMA）於 2015 年發布「E.164 regulatory exceptions for IoT connected services 」，其中提到 E.164 部分規定並不適用於物聯網服務，例如：號碼可攜服務及緊急電話服務等，同時 GSMA 亦建議監管機關應從物聯網之應用方式著手訂定相關管理制度，而非使用之號碼範圍。[203]此外，E.164 編碼著重於用戶之語音及話務服務管理，在 IP 化 5G 網路架構下，IoT 設備連網後之識別以網域名稱（Domain name）及位址（IPv4 或 IPv6）為主，E.164 已非識別 IoT 設備之必要選項。爰此，研究團隊研析國際文獻資料，探討 IoT 設備編碼及管理之可能解決方案。

在 2015 年 11 月由網際網路工程任務組（Internet Engineering Task Force, IETF）舉辦之 IETF 94 中，韓國學者發表「DNS Name Autoconfiguration for Internet of Things Devices」，[204]其中探討如何在沒有網路管理者介入的情況下，以 IoT 設備的類型及產品型號自動配置網域名稱系統（Domain Name System, DNS）之名稱，應用情境包含辦公室、智慧電表、商場或公路網等，透過此 DNS 名稱，可輕易識別及管理個別 IoT 設備。該 DNS 名稱為：unique_id.device_model.device_category.Location.domain_name，包含具唯一性的識別符號（unique_id）、產品的型號或製造商名稱（device_model）、設備類型（device_category）、設備所在處（location）及使用之網域名稱（domain_name）。

此外，網際網路網域名稱及位址指配機構（Internet Corporation for

[202] 中華民國交通部，「電信網路編碼計畫」。檢自 https://www.motc.gov.tw/uploaddowndoc?file=mlaw/201611221609390.pdf&filedisplay=%E9%9B%BB%E4%BF%A1%E7%B6%B2%E8%B7%AF%E7%B7%A8%E7%A2%BC%E8%A8%88%E7%95%AB.pdf&flag=doc (2021/10/31)

[203] GSMA(2015/01) “E.164 - regulatory exceptions for IoT connected services” Retrieved from https://www.gsma.com/iot/wp-content/uploads/2017/11/E.164position.pdf （2021/10/27）

[204] Jaehoon Paul Jeong, Sejun Lee, Jung-Soo Park(2015/10) “DNS Name Autoconfiguration for Internet of Things Devices”Retrieved from https://datatracker.ietf.org/doc/draft-jeong-6man-iot-dns-autoconf/ （2021/11/29）

Assigned Names and Numbers, ICANN）於 2017 年 11 月之 ICANN 60 中發表「DOA over DNS Prototype」，展示以 DNS 作為物聯網識別之可行性。數位物件架構（Digital Object Architecture, DOA）之設計目的，係透過彈性的命名管理系統（Handle System）建立持久性之識別碼。ICANN 提出，若能滿足可加入如持久性錨點等不只一個識別碼之命名空間，命名規約與 Handle System 相似，同時能建立如 DOA 資源記錄（Resource Record, RR）類型之 DNS RR 數據資料，即可以 DNS 建立 DOA 類型之持久性識別碼。簡言之，即係在 DNS 上執行 DOA RR 類型之數位物件架構及命名管理。[205]ICANN 亦於 2020 年發布備忘錄說明其對「5G Technology」及 ITU「Network 2030」之立場。

綜整國際相關實證後，研究團隊提出以 DNS 提供另一種為 IoT 設備編碼的可能性，通過連接 IMEI 及域名構建獨一無二之 DNS 編碼，並擬定驗證情境及平臺系統規格，以進行下世代電信網路號碼編碼機制之概念性驗證（Proof of Concept, PoC）。

一、5G 網路技術及系統架構

雲端原生（Clould Native）技術使 5G 網路架構產生兩項革新，一係將控制平面（Control Plane, CP）功能分為多個獨立的網路服務，以軟體化、模塊化及服務化的方式建構網路；二係將控制平面及使用者平面（User Plane, UP）分開，因此可靈活地將使用者平面部署於核心網路，亦或部署於更靠近用戶端之接入網。同時，透過網路功能虛擬化（Network Functions Virtualization, NFV）及軟體定義網路（Software-Defined Networking, SDN）技術，在雲化的 5G 核心網路基礎上，彈性地依不同需求建構邏輯隔離之網路切片，支援端對端隔離之用戶服務，提供跨領域協作之機會，為消費者及企業提供創新應用，並能即時、高效地連結多元且大量的 IoT 設備。依據 ITU-R 定義，5G 之三大應用場景（Usage Scenarios）如圖 4-1 所示，說明如下：

[205] Alain Durand(2017/10),” DOA over DNS” Retrieved from https://tools.ietf.org/pdf/draft-durand-doa-over-dns-03.pdf (2021/11/30）

1. 增強型行動寬頻（Enhanced Mobile Broadband, eMBB）
   5G 網路資料傳輸速度可達每秒 1 gbps（gigabits per second），是 4G 網路資料傳輸速度的 10 至 100 倍。
2. 超可靠及低延遲通訊（Ultra-Reliable and Low Latency Communications, URLLC）
   指無線接取網路應滿足可靠性 99.999%、移動性中斷時間 0ms、控制平面時延 10ms 及使用者平面時延 0.5ms。換言之，5G 網路提供低延遲和高可靠之訊息交換能力，以支援物聯網協作需求，例如無人駕駛、智慧工廠及遠距醫療等高度精密、高度安全及高準確度之應用，相關應用對於數據傳輸量、遲延性和可靠性要求非常嚴格。
3. 大規模機器型通訊（Massive Machine Type Communications, mMTC）
   5G 網路提供更高連結和高密度的訊息控制能力，聯網密度達到每平方公里 100 萬臺設備，支援及滿足更多 IoT 設備之連結，並提供物與物之間快速溝通，有助於連結大量感測器，以智慧城市為例，滿足不同環境中各種設施、公共及個人設備之連網需求。

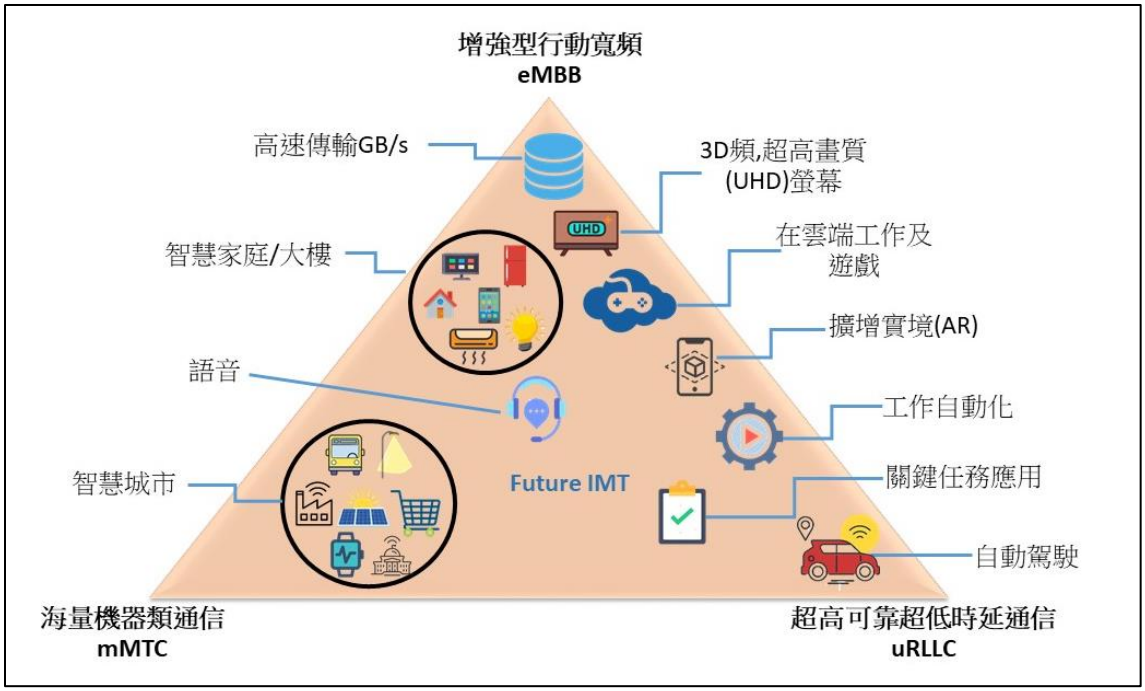


圖 4-1、ITU 的 5G 三大應用場景

資料來源：本計畫製作

針對 5G 核心網路架構，3GPP TS23.501 描述了基於服務系統及基於參考點系統之 2 種網路功能（Network Function, NF）存取及溝通介面。[206]

1. 服務系統：控制平面之網路功能（例如：接取及移動管理功能）允許其他授權的網路功能存取服務，必須包含點對點參考點介面。（如圖 4-2 服務系統架構圖）
2. 參考點系統：任兩個網路功能（例如：接取及移動管理功能和會話管理功能）之間由點對點參考點（例如： N11）提供互動、存取及溝通介面。當控制平面和使用者平面、5G 核心網路（5G Core Network, 5GC）與無線或外部網路連接時，亦係基於點對點參考點。（如圖 4-3 參考點系統架構圖）

[206] 3rd Generation Partnership Project(2021/09)"Technical Specification Group Services and System Aspects;System architecture for the 5G System (5GS) Stage 2"TS 23.501 V17.2.0

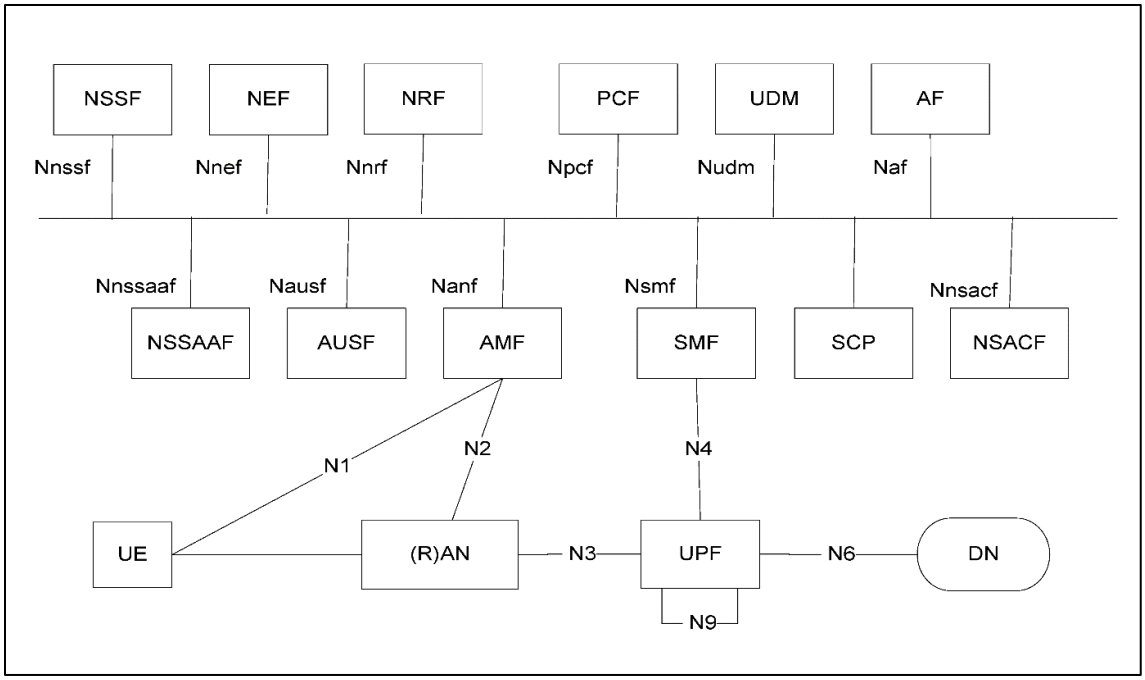


圖 4- 2、服務系統架構圖

資料來源：3GPP TS 23.501 V17.2.0

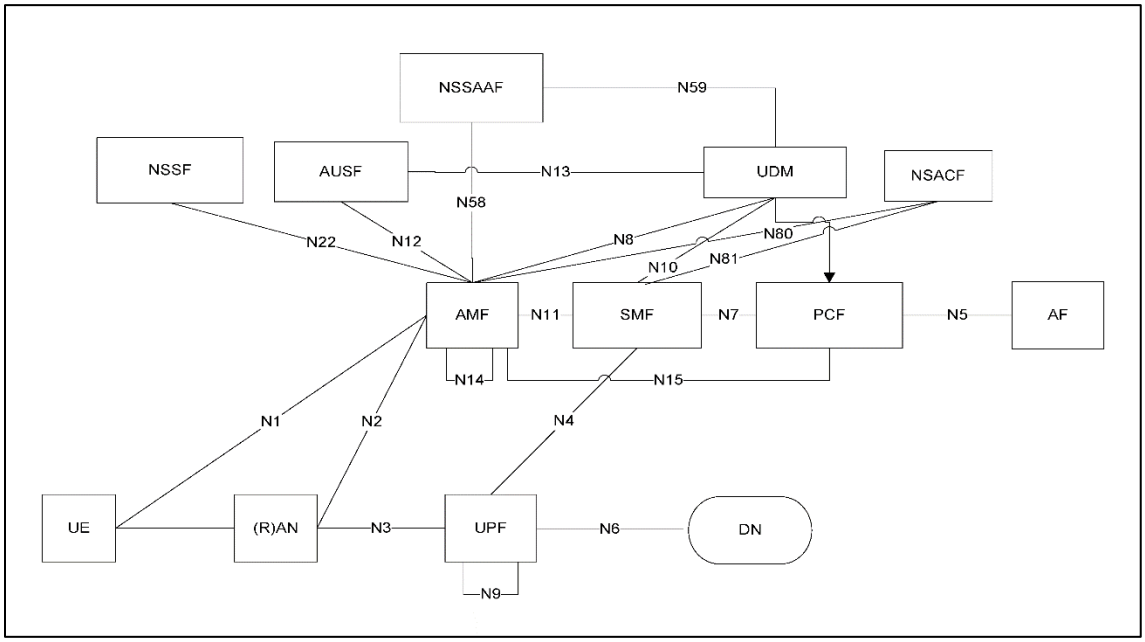


圖 4- 3、參考點系統架構圖

資料來源：3GPP TS 23.501 V17.2.0

彙整 5G 核心網路元件功能介紹如表 4-1：

表 4- 1、5G 核心網路元件功能

網路元件	功能介紹
認證伺服器功能（Authentication Server Function , AUSF）	負責鑑權、決定是否進行 UE 認證，包含 EAP 身份驗證伺服器功能及密鑰儲存，實現 3GPP 及非 3GPP 之接入認證。
存取與移動管理功能 (Access and Mobility Management Function, AMF)。	提供 UE 和 SMF 連結管理之傳輸通道，為 UE 接入提供驗證、註冊、鑑權、移動性管理和連接管理功能，是終端及無線核心網路控制平面之接入點。
資料網路（Data Network, DN）	提供以資料為中心的服務（如業者服務、接入第三方服務應用）的網路。
網路曝光功能（Network Exposure Function, NEF）	提供第三方或非 3GPP 環境 5G 核心網路功能，在 AF 存取 5G 核心節點時提供安全性，可視為代理應用程式介面（Application Programming Interface, API）聚合點或到核心網路的轉換器
網路資料庫功能（Network Repository Function, NRF）	為不同的網路功能提供註冊、登記及監測服務，以實現自動化管理，並使不同的網路功能互相發現、透過 API 通訊。
網路切片選擇功能（Network Slice Selection Function, NSSF）	管理網路切片相關資訊，根據 UE 的訂閱選擇網路切片及 AMF。
特定於網路切片和 SNPN 身份驗	特定用於網路切片的認證和授

網路元件	功能介紹
證和授權功能（Network Slice-specific and SNPN Authentication and Authorization Function, NSSAAF）	權。
政策控制功能（Policy Control Function, PCF）	與 4G 現有的政策與計費控制規則功能（Policy and Charging Rules Function, PCRF）相似，主要管理 5G 核心網路中的各流程的服務品質（Quality of Service, QoS）。
連結管理功能 (Session Management Function, SMF)	負責建立和管理連結，分配和管理 UE 的 IP 位址。
統一資料管理功能（Unified Data Management, UDM）	儲存使用者資料、網路服務配置檔及網路接入政策，在使用者初始連接時，通過 UDM 的資料驗證使用者資訊。
統一資料庫 (Unified Data Repository, UDR)。	承載與資料管理相關的主數據庫，可儲存、檢索、訂閱、管理應用程式資料。
使用者平面功能（User Plane Function, UPF）	允許多種部署位置以降低 5G 延遲性，可部署於核心網路、靠近用戶端，或兩者間的任何位置。負責在無線接入網、網際網路和外部資料網路互連，路由和轉發封包，處理使用者平面的 QoS，檢查封包和執行政策與計費控制 (PCC, Policy and Charging Control) 規則，報告流量使用情形等。

網路元件	功能介紹
應用功能（Application Function, AF）	與其他 5G 核心網路控制平面的網路功能互動，可由業者或可信的第三方針對不同應用提供服務。
終端裝置（User Equipment, UE）	使用者終端設備
無線接入網路（Radio Access Network, (R)AN）	無線存取網路實體，即基地臺端

資料來源：本計畫製作

二、網路切片技術（Network Slicing）

利用虛擬化技術將網路資源切分為多個不同之網路切片，每個網路切片可視為一個獨立之 5G 核心網路，IoT 設備依其訂閱接入相應之網路切片以進行資料傳輸。網路切片技術使網路資源得依使用者需求及其訂閱之服務調整，增加網路應用靈活性，同時減少建置硬體設備、網路的成本及時間。端對端網路切片之範圍從 UE 經 5G 核心網路到網際網路通訊協定骨幹網路（IP Backbone），並可依 IoT 設備的網路切片服務（Network Slice Selection Assistance Information, NSSAI）訂閱項目，由 5G 核心網路的 NSSF 網元提供對應之切片服務。其部署方式共有三種，說明如下：

1. 網路切片共用實體資源，但在邏輯上完全隔離，每個切片均有完整的控制平面及使用者面功能。UE 可連結多個獨立網路切片，並可在每個核心網路訂閱獨立的網路切片。
2. 網路切片共用部分控制平面功能，可共用行動性管理之控制平面功能，而業務的控制和轉發功能為各切片之獨立功能，以實現切片的特定服務。
3. 網路切片共用所有的控制平面功能由，而使用者面功能為切片專有。

5G 三大應用場景對網路傳輸速度、設備數量、高可靠及低

延遲等有不同等級的需求。當業者建置 5G 網路時，透過 5G 關鍵的雲端運算、軟體定義網路（Software-Defined Networking, SDN）以及網路功能虛擬化（Network Functions Virtualization, NFV）等技術，依場景將網路資源切分為多個不同虛擬邏輯網路，以提供不同的應用服務情境。參考 GSMA 介紹網路切片之不同應用場景與環境如圖 4-4 所示，5G 及網路切片技術有助於電信業者打造多元化、客製化與彈性化的網路部署方式，帶來潛在服務商機。[207]

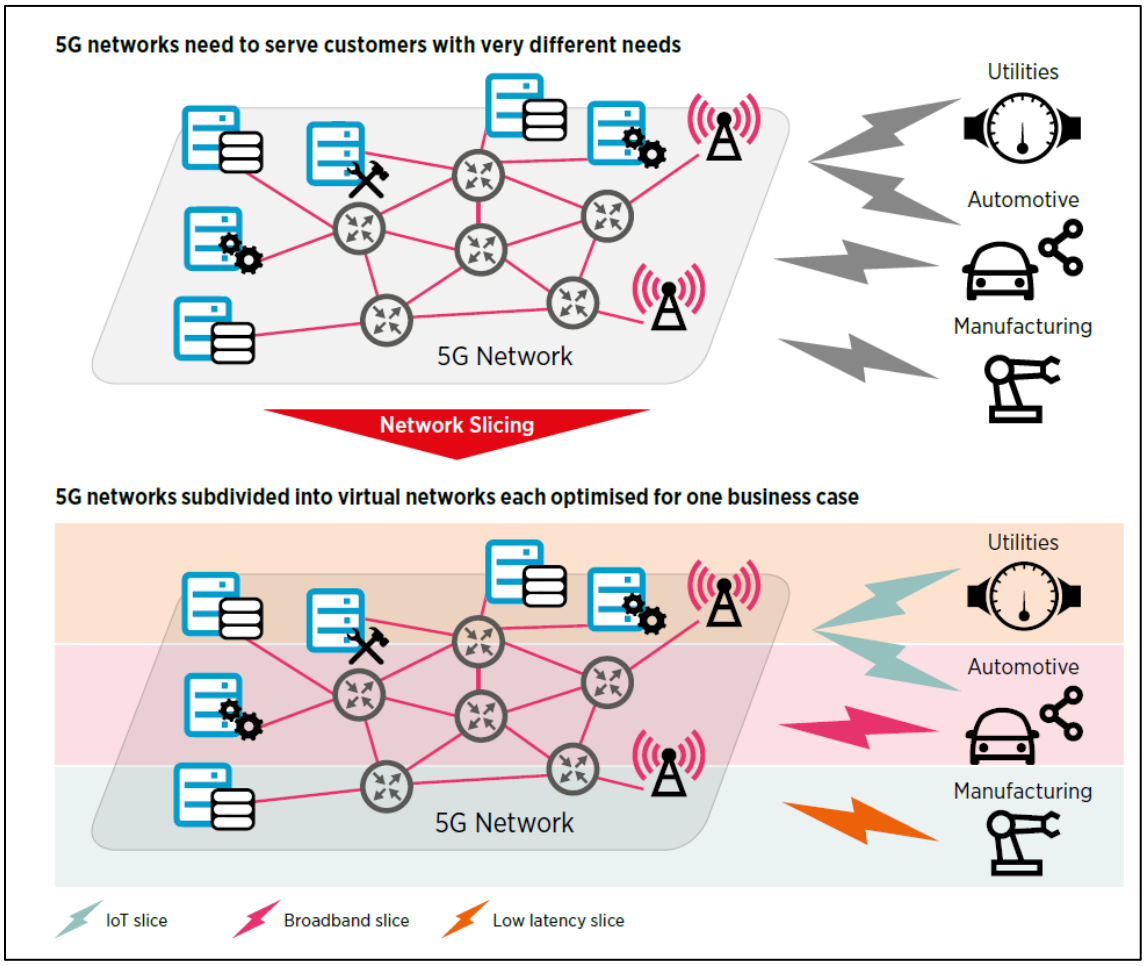


圖 4- 4、5G 網路切片架構示意

資料來源：GMSA

[207] GSMA (2017/07) ” An Introduction to Network Slicing” Retrieved from https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf (2021/10/27)

本計畫有關網路切片之編碼構想來自於 3GPP TS 23.003，5G 核心網路網元的 NSSF 依用戶訂閱配置不同網路切片，並給予不同的 S-NSSAI（Single Network Slice Selection Assistance Information，網路切片選擇輔助訊息）。208電信業者透過此配置提供差異化的網路切片服務，套用 DNS 編碼規格可採用以下格式：

[nssf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org]

在 3GPP 的 DNS 編碼原則中，< >內為變數，NSSAI 由 S-NSSAI 構成，UE 發送以協助選擇特定網路切片，NSSAI 值可隨網路切片特性另行編碼。舉例一：如用戶所訂閱的 NSSAI 為專供低延遲的車聯網服務，其對應網路切片服務代碼為 v2x，套用此編碼範例為：[v2x.nssf.5gc.mnc01.mcc999.3gppnetwork.org]（依 ITU-T 標準，測試使用 mnc001.mcc999）

舉例二：如用戶訂閱大頻寬服務以用於虛擬實境，其對應網路切片服務代碼為 embb，套用此編碼範例為：

[embb.nssf.5gc.mnc01.mcc999.3gppnetwork.org]

三、多重接取邊緣運算技術（Multi-access Edge Computing, MEC）

為實現 5G 技術低延遲特性，ETSI 提出以行動邊緣運算技術（Mobile Edge Computing）滿足 5G 場景要求。邊緣運算為雲端運算之進化，將資源移動到離需要方更近的位置，也就是將裝載著應用程式的主機從集中式資料中心移動到網路邊緣、更靠近用戶端，以符合 5G 網路低延遲和頻寬效率之需要。2017 年 ETSI MEC ISG 將原來的行動邊緣運算技術（Mobile Edge Computing）更名為多重接取邊緣運算技術（Multi-access Edge Computing）。 因應需求差異，MEC 運算平臺可部署於不同位置，包含無線網路節點（Radio Node）、匯流聚合節點（Aggregation Point）及核心網路端（Core Network）。摘要說明 MEC 之部署情境：

[208] 3rd Generation Partnership Project (2021/09) ” Technical Specification Group Core Network and Terminals;Numbering, addressing and identification”, 3GPP TS 23.003 V17.3.0

• 通用型 MEC

MEC 主機之實體位置，從基地臺附近到中央資料網路之間，根據操作、性能或安全等需求靈活地部署在不同的位置，其共同點係藉由使用者平面（User Plane Function, UPF）將流量引導至目標 MEC 應用程式及網路。電信業者可依技術及服務選擇數據網路及 UPF 部署之位置及資源，協調 MEC 主機及其應用程式，動態決定 MEC 主機位置。圖 4-5 說明 MEC 實體位置之部署方式。[209]

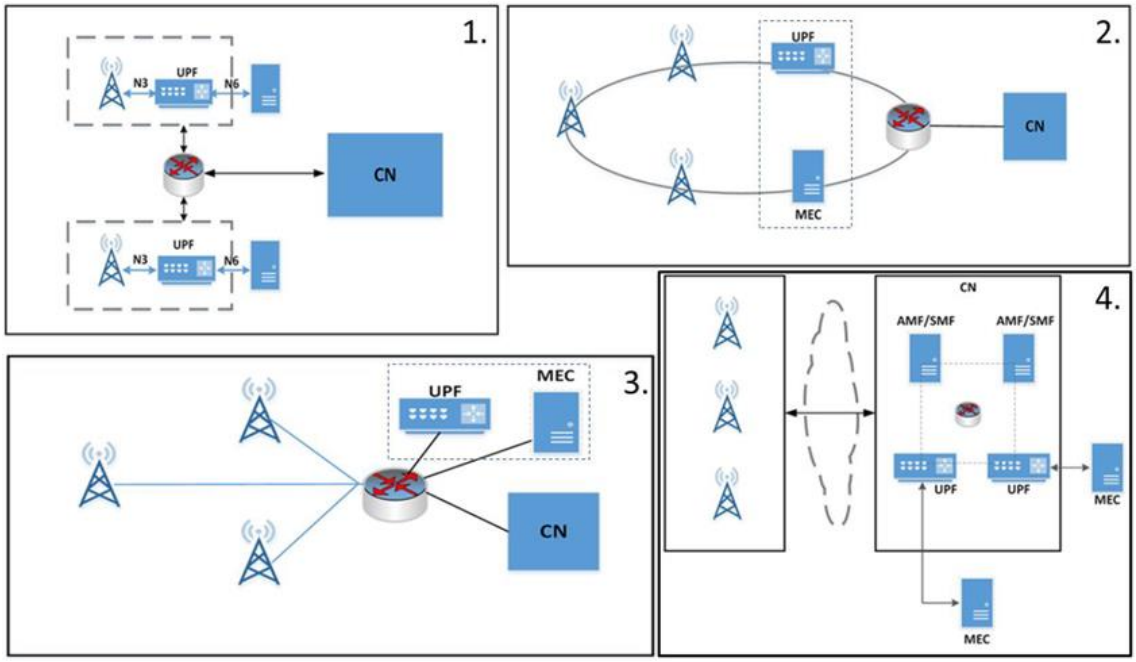


圖 4- 5、MEC 實體部署的範例

資料來源：ETSI White Paper No. 28

依圖 4-5 中編號說明部署情形如下：

a. MEC 和本地 UPF 與基地臺搭配。

b. MEC 與傳輸節點搭配，可能是本地 UPF。

c. MEC 和本地 UPF 搭配一個網路匯聚點。

[209] ETSI (2018/06) “ETSI White Paper No. 28 MEC in 5G Networks,” 1st edition

d. MEC 與核網功能並置（即在同一資料中心）。

- 分散式 MEC

MEC 架構在網路邊緣以減少端到端之延遲，其主機包含虛擬化基礎架構及運行應用程序或服務的運算平臺。一個 MEC 系統係由分佈在網路邊緣並透過底層網路連接的多個 MEC 主機組成，UE 通常會連接至最近的 MEC 主機，但從最佳服務品質（Quality of Service, QoS）及體驗品質（Quality of Experience, QoE）來看，最靠近的 MEC 主機可能並非最佳選擇。

為選擇提供最佳服務之 MEC 主機，不僅需考量 MEC 主機與用戶設備之間的距離，還需評估底層網路之流量負載，及 MEC 主機運算資源之使用情形。例如在大型活動中，同一服務區域內之大量 UE 均向最靠近之 MEC 主機請求服務，其主機可能過載並需要將部分服務移轉至相鄰 MEC 主機，以平衡流量和運算的負載。因此，電信業者或 MEC 服務業者希望 MEC 主機之間可優化及分配服務，使用戶設備得查詢鄰近 MEC 主機提供的相同服務信息，選擇負載較少的主機繼續提供服務。此外，如果 UE 是行動電話或便攜式裝置時，因為 UE 會在不同 MEC 主機之服務區域間移動，將觸發 UE 或 MEC 移動性管理，將現有服務無縫轉移至新的 MEC 主機。

另一個分散式 MEC 之使用案例，可參考 ETSI GS MEC 030 中描述之 V2X 應用。[210]智慧運輸系統 (Intelligent Transportation System, ITS) 業者部署不同的 MEC 系統，透過不同業者的網路提供全國範圍的 V2X 服務。V2X 服務亦可能由同一國家或不同國家的不同網路業者提供，車輛行駛時會穿越不同 MEC 主機的服務區域，甚至可能會穿越不同 PLMN 的 MEC 系統，在這種操作條件

[210] ETSI (2020/04) Retrieved from "Multi-access Edge Computing (MEC); V2X Information Service API"https://www.etsi.org/deliver/etsi_gs/MEC/001_099/030/02.01.01_60/gs_MEC030v020101p.pdf ,P10（2021/10/27）

下，需保持客戶端到服務器間之連續性。

除了持續引領 MEC 技術發展的 ETSI MEC ISG 國際組織，致力於制定與實現全球性行動電話系統規範的 3GPP 標準化機構在制定 5G 行動網路的架構標準中，也特別提及 5G 網路需要能支援 MEC 技術相關功能。本計畫參考 ETSI 的 MEC 技術文件（如表 4-2 說明），研析目前國際上針對 DNS 技術支援 5G 通訊網路的解決方案，以擬定開發場域平臺系統規格。

表 4- 2、ETSI MEC 技術標準

技術項目	技術文件	內容摘述
多重接取邊緣運算（MEC）	New ETSI White Paper on Enhanced DNS Support in Distributed MEC Environment	說明 MEC 環境中支援 DNS 架構，並適當設計 DNS 與 MEC SLA 的部署。另外，也說明在 3GPP 5G 網路架構下，MEC 環境下的 DNS 網路部署等規範。
	ETSI GR MEC 024	說明網路切片及多重接取邊緣運算的架構規範，並透過實際應用案例說明一個網路切片中如何支援多個應用場景，以及網路切片與多重接取邊緣運算如何能達到最有效率部署。

資料來源：本計畫製作

四、網域名稱系統（Domain Name System, DNS）

DNS 技術為一種主從式網路架構（Client-Server Model, C/S 架構），用以查詢及對映網域名稱及 IP 位址。DNS 在行動核心網路裡依據用途功能不同部署於兩個地方，一是部署在行動網路的無線通訊網域中，當無線網路與核心網接取時，進行核心網域內的定位、用戶資料認證、

核心網路元件間認證、動態主機設定通訊協定（Dynamic Host Configuration Protocol, DHCP）解析及核心網路引入長期演進語音承載（Voice over Long-Term Evolution, VoLTE）等功能，稱之為 Gn DNS（DNS for Gn interface）；二是部署在網際網路中，DNS 提供設備裝置接取外部網路使用，透過內容傳遞網路（Content Delivery Network,CDN）或 IP 反解使設備裝置連接到外部網路，稱之為 Gi DNS（DNS for Gi interface），DNS 之電信網路角色，如圖 4-6 所示。

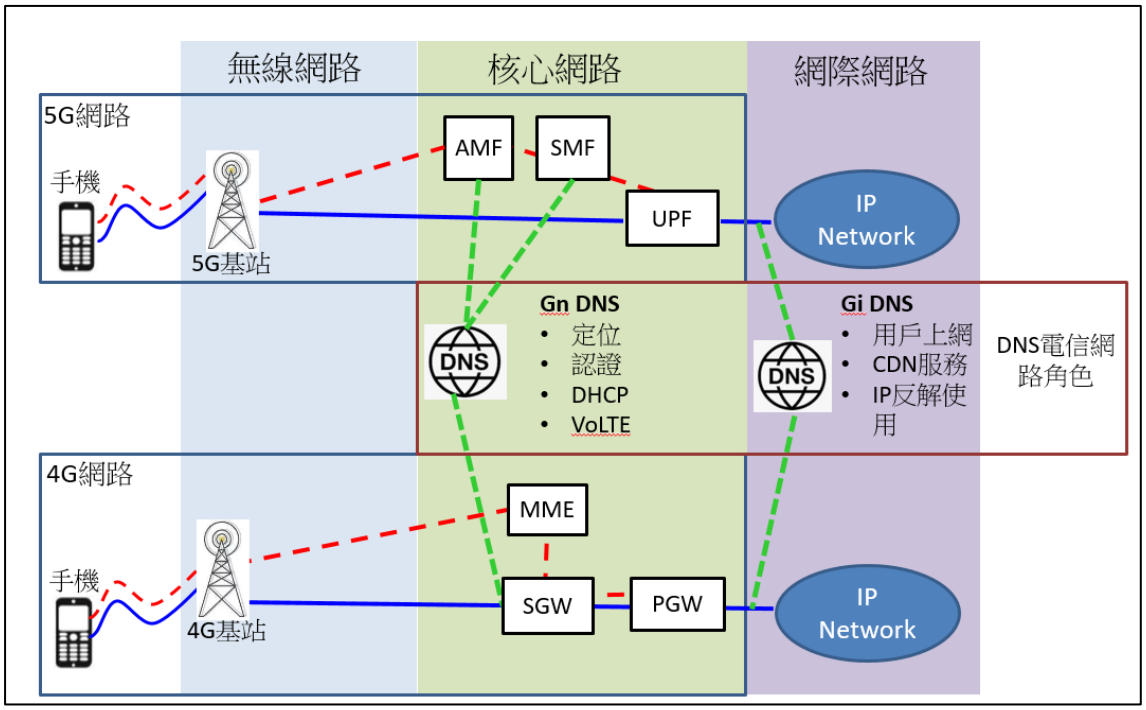


圖 4- 6、行動網路 DNS 之部署與角色

資料來源：本計畫製作

現行行動網路中的 Gn DNS，作用於核心網元間的主機名或域名解析工作，現以 UE 的兩種使用場景，分述說明 Gn DNS 於 3G 至 5G 不同時期之行動網路運作機制。第一種使用場景是當 UE 接入行動網路時，UE 將所設置的存取點名稱（Access Point Name, APN）或 DNN（Data Network Name，在 3GPP Release 15 中，APN 已經以 DNN 名稱

取代）[211]上報至行動網路中，行動網路再將 APN 或 DNN 資訊送至 DNS 做查詢，並依據不同的 APN 或 DNN 選擇不同的路由上網，如表 4-3 說明。

表 4- 3、當 UE 註冊時 Gn DNS 解析 APN 或 DNN 之註冊流程

Gn DNS 使用場景一:當 UE 註冊（UE Attached）時，依據 UE 提供的 APN 或 DNN 資訊，解析連網需求。		
3G	SGSN 依 UE（User Equipment）的 APN 選擇不同的 GGSN，之後 GGSN 會分配 UE IP 以建立 PDP context（GTPv1）連網。	Gn DNS 解析行動網路網元之流程如圖 4-7 步驟 1、2、3
4G	S-GW 依 UE 的 APN 選擇不同 P-GW，P-GW 分配 UE IP 建立 EPS Bearer（GTPv2）連網。	
5G	AMF 依 UE 的 DNN 選擇不同 SMF，之後 SMF 會分配 UE IP 以建立 IP Bearer（GTPv2）。	

資料來源：本計畫製作

[211] ETSI (2018/07) “Digital cellular telecommunications system (Phase 2+) (GSM);Universal Mobile Telecommunications System(UMTS);Numbering, addressing and identification”(3GPP TS 23.003 version 15.4.0 Release 15) Retrieved from https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/15.04.00_60/ts_123003v150400p.pdf , P37（2021/10/27）

第二種使用場景如表 4-4 說明，是當 UE 移動時，提供由舊服務區網元更換到新服務區網元之 DNS 解析，能讓移動中的用戶連網不中斷。

表 4- 4、當 UE 移動中 Gn DNS 解析行動網路網元之流程

Gn DNS 使用場景二: 當 UE 移動（UE Moves）時，提供服務接續的 DNS 解析，能讓移動中的用戶連網不中斷		
3G	用戶移動中更換到新的 SGSN 服務區域時，透過 Gn DNS 查到舊 SGSN IP，使用戶可以持續連網不斷線使用。	Gn DNS 解析行動網路網元之流程如圖 4-7 步驟 6、7、8
4G	用戶由來源 SGW 下的 eNB 移動到目的端 t-S-GW 下的 t-eNB 服務區域時，t-S-GW 會透過 Gn DNS 查到來源 S-GW 的對應 IP，之後 t-S-GW 通知 P-GW 將用戶的連線由來源 S-GW 切換至 t-S-GW，以保持 UE 可以持續連網不斷線。	
5G	用戶由來源 AMF 下的 gNB 移動到目的端 t-AMF 下的 t-gNB 服務區域時，t-AMF 會透過 Gn DNS 查到 AMF 的對應 IP，之後 t-AMF 通知 SMF 將用戶的連線由來源 AMF 切換至 t-AMF，以保持 UE 可以持續連網不斷線。	

資料來源：本計畫製作

如圖 4-7 所示，從 3G 至 5G 用戶連網訊息係由不同網元產生，並以 RADIUS 協議傳送至 AAA 資料庫（Authentication, Authorization, and Accounting）中作為計費或認證使用。

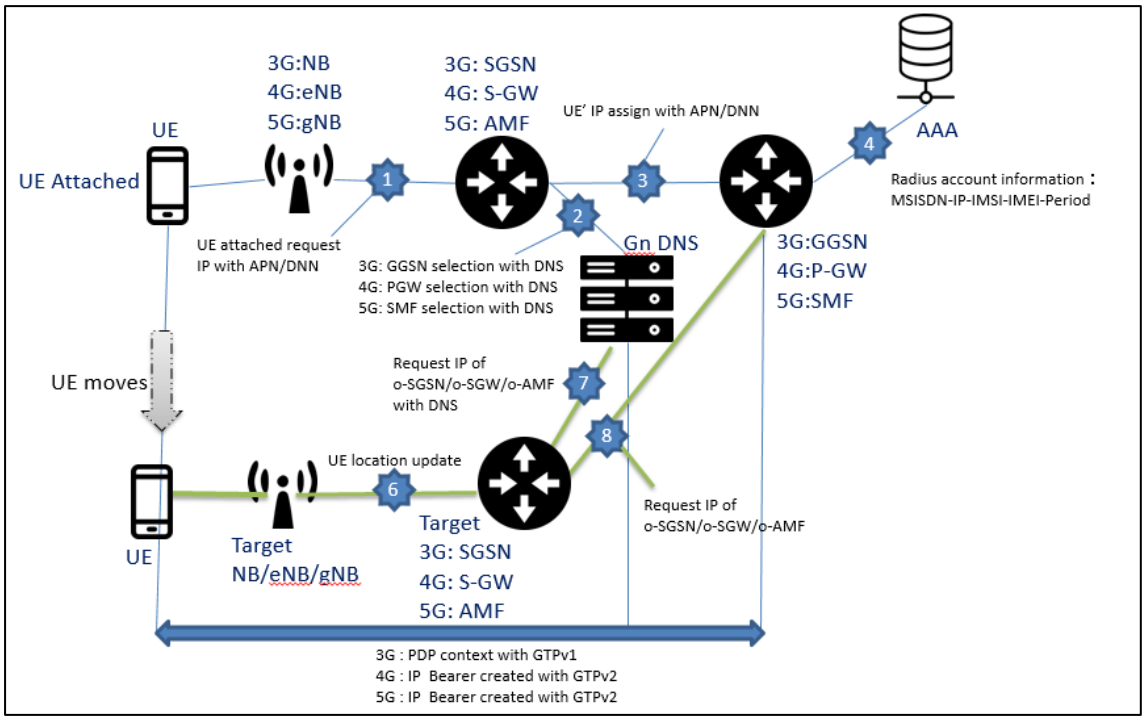


圖 4- 7、Gn DNS 解析行動網路網元之流程圖

資料來源：本計畫製作

圖 4-7 之名詞相關說明如下：

- UE （User Equipment 終端裝置）：裝有符合 3GPP Sim 卡的聯網裝置。
- APN （Access Point Name，存取點名稱）：定義 3G/4G 行動裝置行動數據連線的網路路徑。
- NB （Node BaseStation，節點基站）：3G 基站。
- t-NB （target Node BaseStation，目的端節點基站）：UE 移動時的目的端 3G 基站。
- SGSN （Serving General Package Radio Service support node，GPRS 服務支援節點）：3G 網路的數據封包轉送節點。

- t-SGSN（target Serving GPRS Support Node，目的端的服務 GPRS 支援節點）：UE 移動時的目的端的 3G 網路的數據封包轉送節點。
- GGSN（Gateway GPRS Support Node，GPRS 支援節點轉發閘道）：提供 3G 網路配發 IP 及數據封包轉發功能。
- eNB（Evolved Node BaseStation，演進節點基站）：4G 基站。
- S-GW（Serving Gateway，服務閘道）：4G 網路的數據封包轉送節點。
- t-S-SW（target Serving Gateway，目的端的服務閘道）：UE 移動時目的端的 4G 網路的數據封包轉送節點。
- P-GW（Packet Data Network Gateway，封包數據網路閘道）：提供 4G 網路配發 IP 及數據封包轉發功能。
- DNN（Data Network Name，資料網路名稱）：定義 5G 行動裝置行動數據連線的網路路徑
- gNB（Next Generation Node BaseStation，次世代節點基站）：5G 基站。
- AMF（Access and Mobility Management Function，存取與移動管理功能）：5G 網路的認證及數據封包轉送節點。
- t-AMF（target source Access and Mobility Management Function，目的端的接取和移動性管理功能）：UE 移動時目的端的 5G 網路的認證及數據封包轉送節點。
- SMF（Session Management Function，連結管理功能）：提供 5G 網路配發 IP 及數據封包路由控制功能。

1. 行動網網域的 DNS 編碼

行動網網域裡早有以 DNS 技術網域命名概念的編碼規則，運用於電信網路網域的 IP 網路交換，依據行動業者網路策略選擇路由及網元，所定義的 DNS 命名網域編碼規則，如 GSMA IR.67 指引裡說明在行動網域的各行動業者編碼規範整理如表 4-5 所示。[212]

表 4- 5、GSMA IR.67 指引行動網域裡子網域（sub-domain）定義

行動核心網	行動網域裡子網域定義
3G	mnc<MNC>.mcc<MCC>.gprs
4G	epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
5G	5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
備註	MNC 定義為 2 碼，MCC 定義為 3 碼，其中<>裡填入的是變數值，依據電信業者不同所填入。 舉例: 5gc.mnc01.mcc999.3gppnetwork.org

資料來源：本計畫製作

2. 行動網路中各應用場景編碼

3GPP TS29.060 中定義行動網路的 Gn DNS 無線通訊網域，[213] 當無線網路與核心網接取時，Gn DNS 除了進行核心網域內的定位與、用戶接入網路解析、核心網路元件間認證與網元域名解析等功能，行動網路在不同時代也依需求將 DNS 編碼命名特性加入了地理涵蓋位置資訊，運用在各種應用場景下對映的完整網域名稱（Fully Qualified Domain Name, FQDN）解析，整理如表 4-6 說明，表中由<>所填入的值為依據行動網路定義的變數值：

[212] GSMA(2020/06) “DNS Guidelines for Service Providers and GRX and IPX Providers” Retrieved from https://www.gsma.com/newsroom/wp-content/uploads//IR.67-v16.0.pdf,P.20 (2021/10/27)

[213] 3rd Generation Partnership Project (2019/06) “Technical Specification Group Core Network and Terminals;General Packet Radio Service （GPRS）;GPRS Tunnelling Protocol （GTP）across the Gn and Gp interface” Retrieved fromhttps://www.3gpp.org/ftp//Specs/archive/29_series/29.060/29060-f50.zip P.26(2021/10/27)

表 4- 6、行動網路 Gn DNS 的 FQDN 解析運用

運用場景	核心網路 Gn DNS 的 FQDN 運用	說明
3G APN 設定	<APN>.mnc<NMC>.mcc<MCC>.gprs	3G 行動網路裡 APN（Access Point Name，接入點名稱）運用
3G RAI 設定	rac<RAC>.lac<LAC>.mnc<MNC>.mcc<MCC>.gprs LAC 表示是縣市：例如臺北市，RAC 表示基站所在行政區域，例如萬華區	Routing Area Identity， 表示有地理上涵蓋位置的 3G 行動網路
4G APN 設定	<APN>.epc.mnc<NMC>.mcc<MCC>.3gppnetwork.org	4G 行動網路裡 APN 運用
4G TAI 設定	tac<TAC>.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org TAC 表示是縣市行政區：例如臺北市萬華區	Tracking Area identity，有地理上涵蓋位置的 4G 行動網路
5G DNN 設定	<DNN>.epc.mnc<NMC>.mcc<MCC>.3gppnetwork.org	5G 行動網路的 DNN （Data Network Name，數據網絡名稱）
5G TAI 設定	tac<TAC>.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org TAC 表示是縣市行政區：例如臺北市萬華區	地理上涵蓋位置的 5G 行動網路

資料來源：本計畫製作

第二節　實測驗證平臺之規劃

一、驗證目的

IoT 設備通訊需經「識別」及「定址」,「識別碼」(Identifier)在特定環境中可唯一地識別出單一 IoT 設備之元件(Entity),網域名稱、IP 位址和電話號碼等均為識別碼。[214]由於物聯網服務著重於連網裝置與應用程式之間自動傳送數據的通訊服務,適合以封包交換(Packet switch)的方式傳送數據資料,少有以電路交換(Circuit switch)方式傳送語音或簡訊之情形。

觀察 5G 行動通訊之演進,IP 已成為軟體定義網路、網路功能虛擬化及行動邊緣運算等 5G 關鍵技術之基礎,增加更多網際網路(應用層)之應用情境,因 DNS 命名的彈性與其高普及之基礎建設,具有因應未來網路需求之潛力,考量 IP 化電信網路環境及自動化之大量物聯網裝置,本計畫參考 ETIS 所發佈之 MEC 技術文件及 ICANN 於 2020 年提出之「5G Technology」建議,以 DNS 技術建立具彈性、即時性、可有效管理及識別物聯網裝置之編碼機制,作為下世代電信網路編碼之解決方案,並設計概念驗證(Proof of Concept, PoC)情境,驗證 IoT 設備自動配置號碼與管理號碼之機制,並自主開發資料管理系統及平臺。

本計畫 PoC 場域建置於 5G 專網環境、不連結至公眾網路,並使用符合 3GPP R15 標準之設備,以驗證 DNS 編碼技術之適用性。本機制將為 IoT 設備生成一組包含 IoT 設備國際行動裝置辨識碼(International Mobile Equipment Identity, IMEI)、基站名稱、區域名稱及其使用之網路切片服務之完整網域名稱(Fully Qualified Domain Name, FQDN)。其概念為 IoT 設備透過 5G 基地臺(Next Generation Node B, gNB)連接至 5G 核心網路(Core Network),一旦 IoT 設備連接與認證成功,將被分配到一組 IPv4 及 IPv6 位址,及一組 DNS 編碼。另為使管理者可以快速

[214] AIOTI (2018/02) " Identifiers in Internet of Things (IoT)", Version 1.0, Retrieved from https://euagenda.eu/upload/publications/identifiers-in-internet-of-things-iot.pdf ((2021/10/27)

了解 IP 與 DNS 之間的關係與變化，以及系統環境之執行效能，特別設計 Dashboard 平臺讓管理者可以快速了解執行情形，同時也易於管理、監控及查詢資訊。

二、實測驗證平臺之 5G 網路環境

(一) 5G 網路環境

本計畫使用符合 3GPP R15 版本之 gNB Based 5G SA 模擬器（以下簡稱 5G 模擬器），模擬 5G 核心網路與 5G 基地臺之標準行為，為 IoT 設備註冊及配發 IP。圖 4-8 說明本計畫 5G 模擬器所具有之 5G 核心網路元件功能，包含政策控制功能（PCF）、統一資料管理功能（UDM）、認證伺服器功能（AUSF）、存取與移動管理功能 (AMF) 、連結管理功能 (SMF)、使用者平面功能（UPF）及資料網路功能（DN）等網路功能元件。

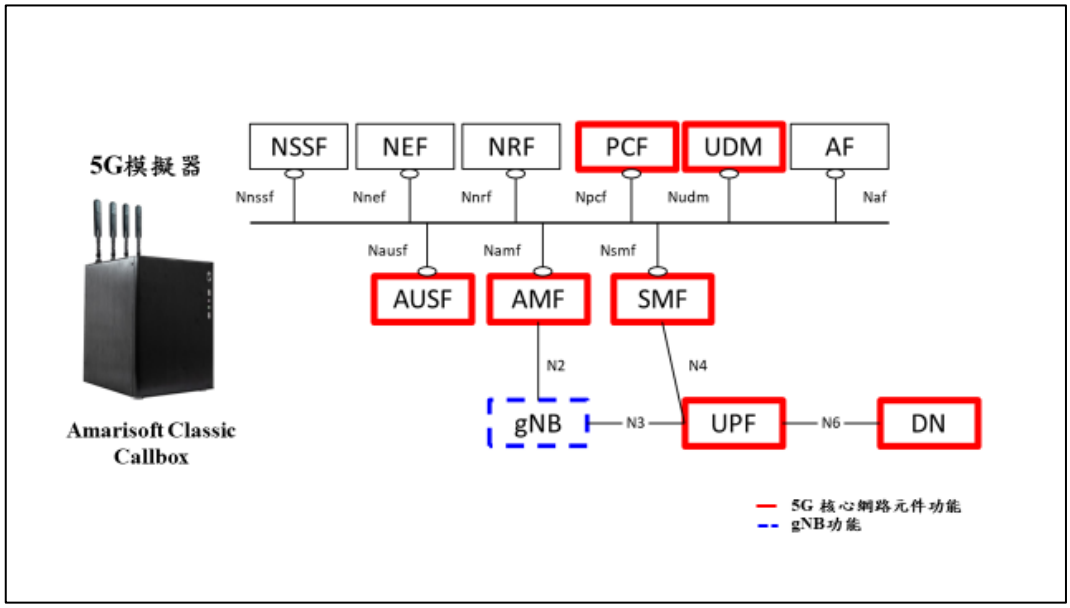


圖 4- 8、5G 模擬器所包含之網路功能元件

資料來源：本計畫製作

5G 模擬器（Emulator）之 5G 核心網路具基礎 5G 連線所需功能，惟不具 UDP 介面，故缺乏 AAA 計費功能（Accounting）之原

生支援，因此研究團隊參考 3GPP TS 29.561 有關 RADIUS accounting update 之說明（如圖 4-9 所示），以 5G 模擬器所開放之 API 開發 RADIUS Server 元件，以 Log Generator 加上 RADIUS 之方式蒐集 AMF 及 gNB 資料，使 5G 模擬器具備 RADIUS 協定支援功能，過濾 AAA 資料（Authentication, Authorization, and Accounting）後與用戶連網訊息（如：DNN、Cell ID、IMSI、IMEI、IP）一起透過 RADIUS 協定封包發送給 DNS，再由 DNS 自動編碼生成 IoT 設備之 A Record 或 AAAA Record。[215]（圖 4-9 中之 DN-AAA 為第三方認證網元，可以透過 RADIUS 協議與 SMF 交換 authentication, authorization, accounting 訊息。）

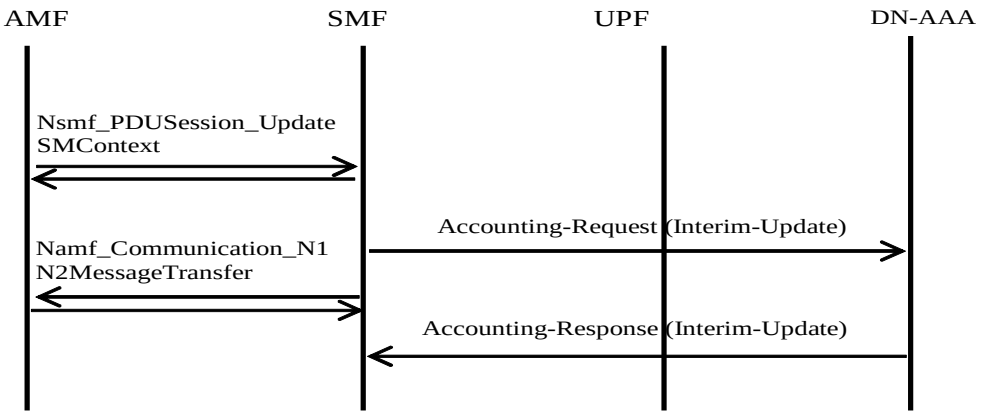


圖 4- 9、RADIUS accounting update

資料來源：3GPP TS 29.561

[215] 3rd Generation Partnership Project (2021/09) ” Technical Specification Group Core Network and Terminals;5G System; Interworking between 5G Network and external Data Networks;Stage 3”, 3GPP TS 29.561 V17.3.1, P23-31

PoC 實測驗證場域所使用之 5G 模擬器功能分述如表 4-7：

表 4- 7、PoC 實測驗證場域採用 5G 模擬器功能說明

項次	5G 模擬器功能	說明
1	5G 模擬器符合 3GPP 標準行為	5G 模擬器是依據 3GPP R15 開發，並與基於高通晶片之多款不同商用終端設備對接過，評估可符合本案的研析國際組織 3GPP 所發佈的等相關標準規範需求。
2	5G 模擬器可實現網路切片功能	5G 網路切片得要在 SA 架構發展下，才能夠充分發揮其功能及加以付諸實現效益。但是傳統商用核心網路與基地臺可實現 5G SA 架構並提供網路切片功能的產品須等到 2021 年年底才有商轉產品，所以考量時效性及成本而採用 5G 模擬器。
3	5G 模擬器可提供細部訊息	本案案研究時須得到多項細部訊息以方便後續解析，例如 gNB、5GC、UE IMSI、IMEI 與即時配發之 IP 位址、連線斷線時間等解析資料，，5G 模擬器原設計初衷即為測試需求，開放使用者深入詳細研究至單一封包的程度，也可透過大量原生 API 獲得以上所述細部訊息。
4	5G 模擬器採用全軟體實作，提供高彈性可自行導入第三方軟體	5G 模擬器採用全軟體實作，基於 Linux 開放環境提供包含 5GC 以及 gNB 網路元件皆由軟體程式相關服務，同時仰賴於其作業系統為 Linux 系統，便可輕易在 5G 模擬器設備中開發、安裝與執行本案所需之客製化程式，順利將本案所需 5G 網路資訊導出產生 DNS Record

資料來源：本計畫製作

就實測驗證用途與目的而言，本計畫選用之gNB Based 5G SA模擬器符合 3GPP 5G 標準行為，其 5G 核心網路及 gNB 功能符合 PoC 需求，惟其功能與電信級別之商用環境確有區隔，以下簡單具體說明 5G 模擬器與真實環境之差異：

1. 電信級別之商用真實環境較測試環境設定複雜，本實驗場域僅考慮 IoT 設備及實驗場域需求設定 5G 模擬器，商用真實環境需考量物與人交互作用之設定。
2. 電信級別之商用真實環境對硬體、軟體配置之容量與效能要求較測試環境嚴格，本實驗場域僅探討並取用 5G 模擬器之 5GC 與網路切片基礎功能設定，5G 模擬器採用全軟體實作，硬體效能無法達到實際 5G 商轉產品的能力。
3. 電信級別之商用真實環境較測試環境需要更多的資訊安全考量，PoC 實驗場域係為封閉式企業專網環境，不與公共網路連結。
4. 5G 模擬器設計用途為測試 5G、LTE、LTE-M 和 NB-IoT 設備的解決方案，符合 3GPP 標準的 eNB 和 EPC，以進行功能和效能性測試。
5. 5G 商轉產品為符合電信級商用需求，Latency 需達到 <10ms，5G 模擬器無此設計。
6. 5G 電信級商用設備需保證在 17 秒內可以將備援服務正確啟動備援機制，實證場域的測試環境僅有單一臺 5G 模擬器，無備援功能。

(二) 網路切片設定

PoC 之網路切片設定係依據 3GPP TS 23.501 定義之切片/服務類型（Slice/Service Type, SST ）參數規格如圖 4-10 所示，依序設定 IoT 設備 SST 參數如表 4-8，以模擬支援 5G 應用之網路切片服

務類型。[216]5G 模擬器雖支援網路切片相關參數設定，但不包含依 SST 值分配不同 IP 網段，故研究團隊將網路切片 SST 參數與 DNN 參數視為聯合參數，依不同的 SST 與 DNN 組合配發不同的 IP 網段，使不同網段間之 IoT 設備使用網路隔離之網路切片功能。

Slice/Service type	SST value	Characteristics.
eMBB	1	Slice suitable for the handling of 5G enhanced Mobile Broadband.
URLLC	2	Slice suitable for the handling of ultra- reliable low latency communications.
MIoT	3	Slice suitable for the handling of massive IoT.

圖 4- 10、3GPP TS 23.501 所定義之 SST 參數規格

資料來源：3GPP TS 23.501

表 4- 8、網路切片 SST 參數設定

	IoT_1	IoT_2	IoT_3	IoT_4	IoT_5
DNN	internet1	internet2	internet3	internet4	internet5
IMEI	355979860003363	355979860003702	355979860003728	355979860003785	359047100170495
NSSAI	eMBB	eMBB	URLLC	MIOT	MIOT
SST	1	1	2	3	3
Template	AR/VR 8K Videos	AR/VR 8K Videos	Factory Automatic Machines	Smart City Sensors	Smart City Sensors

資料來源：本計畫製作

(三) MEC 架構設計

ETSI MEC 003 說明 MEC 係指在靠近網路邊緣或接近網路邊緣的虛擬設備中執行行動邊緣運算功能，其框架包含行動邊緣運算主機（如行動邊緣平臺、行動邊緣應用程式及虛擬化基礎設施）、行動邊緣系統層管理、行動邊緣主機層管理及與外部相關（例如

[216] 3rd Generation Partnership Project (2021-09) “Technical Specification Group Services and System Aspects;System architecture for the 5G System (5GS)” TS 23.501 V17.2.0, P216

網路層）之實體設備，其功能元件間存在點對點之參考點溝通介面（如圖 4-11）。依據 MEC 參考點之定義，處理功能方面之參考點為 Mp（如 Mp1），處理平臺之開通、告警及網管系統等管理方面之參考點為 Mm（如 Mm5），而處理與外部實體相關之參考點為 Mx（如 Mx1）。本計畫 MEC 架構設計參考行動邊緣平臺（Mobile edge platform）之概念，將實體之 MEC 伺服器切分成不同虛擬機器（Virtual Machine, VM）以安裝 DNS 應用程式及管理平臺。在行動邊緣平臺中，具有流量控制（Traffic Rules Control）、DNS 處理（DNS Handling）及註冊服務（Service Registry）三個功能區塊，[217]本計畫以 Edge DNS 模組作為 DNS 處理功能區塊，當 DNS 自 5G 模擬器取得用戶連網訊息（如 Start/Stop time、MSISDN、IP、IMSI、IMEI、Cell ID）後，可自動編碼生成 A Record 及 AAAA Record，再將相關資訊傳送至管理平臺。

[217] ETSI, GS MEC 003 (2016/03) “Mobile Edge Computing (MEC);Framework and Reference Architecture”, P9

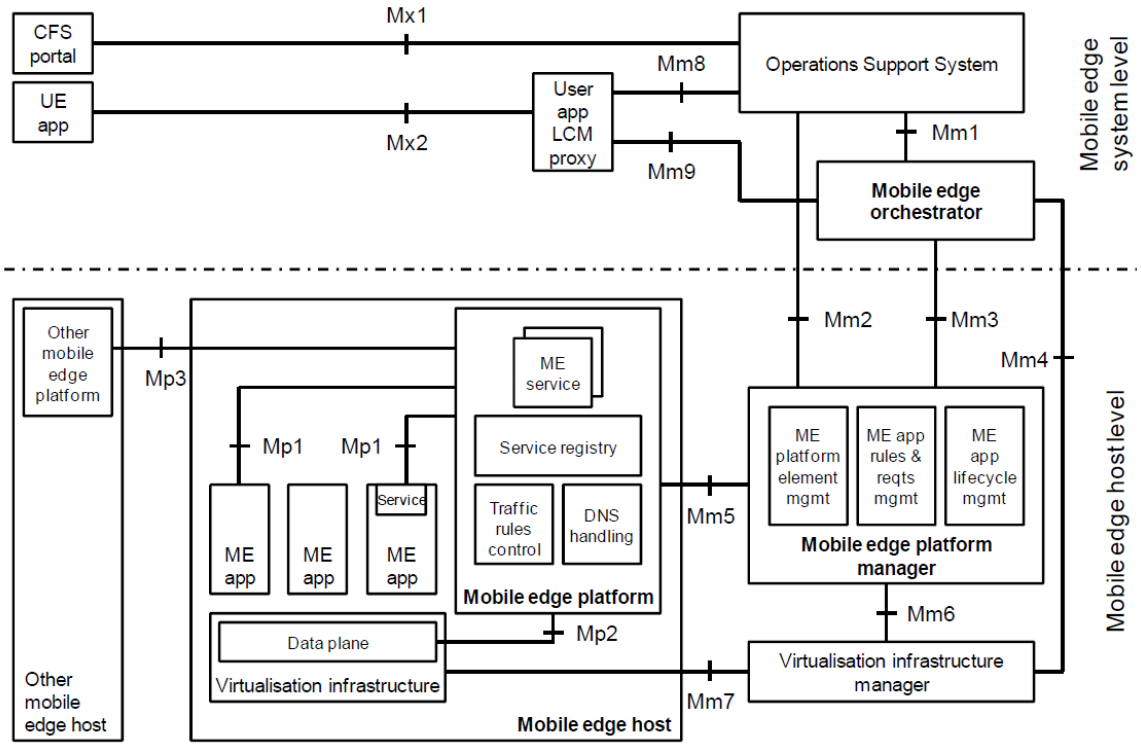


圖 4- 11、MEC 架構

資料來源：ETSI GS MEC 003 MEC

參考 ICANN「5G Technology」中提及對低延遲敏感之 5G 應用，應盡可能將 DNS 部署於邊緣數據中心附近。所謂邊緣運算即係指在網路的邊緣進行資料處理，使之更接近需要方，將 DNS 部署在網路邊緣可減少端到端之延遲，當 IoT 設備移動時，它可能需要不時地被定向到更靠近它的邊緣數據中心，[218]利用 MEC 架構下 Edge DNS 的概念進行 IoT 設備管理，因 IoT 設備距離近，比起讓 IoT 設備連回核心網路的 Gn DNS，執行解析效率更快、降低延遲性，故將本計畫之 DNS 及管理平臺部署於靠近基站的位置。

由於基站無線傳輸技術的進步，使得 UE 到 3G 至 5G 核心網路的封包來回往返時間（Round trip time, RTT）縮短，影響 RTT 的因素有四個：物理距離、伺服器的響應時間、傳輸媒介及區域

[218] ICANN Office of the Chief Technology Officer,(2020/01/23)" 5G Technology", P5

性的網路流量，當伺服器更靠近 UE 的時候，可縮短 RTT。[219]在「5G Technology」中亦提及 5G 的目標之一係將延遲性縮短到 10ms 或 5ms RTT 以下，並建議將 DNS 之部署盡量靠近本地端且利用分散式的快取系統提高 DNS 的效率、降低延遲性。[220]另參考 NGMN「Pre-Commercial Networks Trials Major Conclusions」有關延遲性之測試，NGMN 測試發現 UE 到無線電存取網路（Radio Access Network, RAN）的 RTT 小於等於 8ms，而從 UE 到新無線電節點（New Radio Node）再到 4G 核心網路或 5G 核心網路及應用伺服器之間的距離如果是 200 公里，其 RTT 小於等於 10ms 至 15 ms，其測試結果顯示核心網路到 RAN 之間的距離對端對端的延遲性起關鍵作用，亦顯示了 MEC 之必要性。[221]研究團隊另整理中華電信、台灣大哥大、遠傳及台灣之星 RTT 量測值如表 4-9，因臺灣地小，從基站至核心網路的距離約在 170 公里之內。如為腹地廣大之陸地國家，其核心網路至基站距離可達 600 公里、RTT 亦會增加，將 MEC 設在靠近基站的位置可有效降低延遲性。

表 4- 9、行動網路傳輸延遲比較

項次	行動網路傳輸情境	網路延遲
1	UE 連至 5G 基站旁的 MEC	<1ms
2	UE 連至 5G 核心網	RTT<15ms
3	UE 連至 4G 核心網	RTT<25ms
4	UE 連至 3G 核心網	RTT<45ms

資料來源：本計畫製作

三、實測驗證平臺之編碼原則

對於大量連結之物聯網裝置，以手動配置 DNS 名稱繁瑣耗時，如可自動配置為人類可讀之 DNS 名稱，對於物聯網裝置之管理有很大助

[219] Adam Novotný (2021/06/29) “What is RTT (Round-Trip Time) and How to Reduce it?” Retrieved from https://www.stormit.cloud/post/what-is-round-trip-time-rtt-meaning-calculation
[220] ICANN Office of the Chief Technology Officer,(2020/01/23)” 5G Technology”, P6
[221] NGMN (2021/2/17) “Pre-Commercial Networks Trials Major Conclusions” Retrieved from https://ngmn.org/wp-content/uploads/210406-NGMN-PrecomNW_Trials_Major_Conclusions-v2.pdf, P12-P14 (2021/12/02)

益。假設每個 IoT 設備均有一出廠配置，具有製造商 ID、設備型號 ID 及型號資訊等（例如:車輛、路邊裝置、智能電視或智能冰箱），這個出廠配置可被設備讀取並與域名連接以建構其 DNS 編碼，DNS 編碼應有其獨特之識別（例如：唯一的 ID 或序列號），以與其他設備區分。[222]

本計畫截取遠端認證撥接使用者服務（Remote Authentication Dial In User Service, RADIUS）協議傳送之用戶連網訊息及 AAA 資訊組成 DNS 編碼欄位，用戶連網訊息欄位中包含具 unique_id、device_model、device_category、Location 及 domain_name 等元素之欄位，如表 4-10 所列，用於 PoC 實測驗證場域之 DNS 自動編碼欄位。其中 unique_id 是設備的唯一識別碼，以保證其唯一性之 DNS 名稱，以 ASCII 字符表示，為英文字母或數字，在本 PoC 中以 IMEI 作為唯一識別碼，並可展示 device_model 及 device_category 等設備型號及類型特性。此外，當 IoT 設備的 DNS 名稱包含位置資訊，可以讓用戶輕鬆的識別設備的物理位置，在本次 PoC 中，DNS 名稱包含基地臺及域名兩個級別的位置資訊。

此外，如車輛、智慧型手機及無人載具等 IoT 設備具有移動性，允許 IoT 設備跨域移動，為了處理移動中 IoT 設備之 DNS 編碼，當 IoT 設備移動到新的區域時，就會生成新的 DNS 編碼並在指定的 DNS 伺服器上註冊。[223]

[222] J. Jeong (2021/08)" DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks"

[223] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound (1997/04) "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136 Retrieved from https://www.rfc-editor.org/rfc/rfc2136

表 4- 10、PoC 實測驗證場域之 DNS 編碼組成欄位

名稱	說明
DNN	DNN 為網路接入技術，當 IoT 終端設備出網時，裝置上網時必須核配一個參數，換言之，DNN 決定了裝置通過哪種接入方式訪問網絡。
Cell ID	基地臺之識別碼。
IMSI	IMSI 是每個用戶所屬系統的識別碼，當手機裝入 SIM 卡及開機後，SIM 卡中會讀取用戶所在地點，當用戶所在地點與本地網路系統（Home Location Register, HLR）不同時，訊息會傳送到本地網路系統，系統就開啟漫遊模式，進入另一個外地網路系統（VLR）。
MSISDN	移動臺國際用戶識別碼（Mobile Subscriber International ISDN number, MSISDN）是行動用戶的 ISDN 門號，是用戶呼叫公眾行動電話網路的一組識別行動用戶的號碼，可由此號碼辨別用戶所屬國家及電信業者。
IMEI	IMEI 是每個 IoT 設備獨屬的號碼，該組號碼一般會顯示在設備裝置機身上與外包裝上，同時也存在於設備裝置的記憶體中。
IP	網路層分配 IoT 設備的 IP。

資料來源：本計畫製作

(一) DNS 編碼規則碼長規範

依據 RFC 1123 有關 DNS 編碼規則之定義，[224]每一級域名之長度以 63 個字元為限，域名總長度不得超過 255 個字元，將地理位置資訊欄位加入域名，即可經由 DNS 識別 IoT 設備安裝於哪一個基站的服務範圍內，並可應用在不同的 IoT 場域中。

(二) IoT 設備的唯一標示規範

依據 GSMA 定義每個 IoT 設備必須擁有自己獨一無二的 TAC

[224] Internet Engineering Task Force (1989/10) “Requirements for Internet Hosts -- Application and Support”, P12, RFC1123 Retrieved from https://tools.ietf.org/html/rfc1123

碼，[225]因 IMEI 的號碼擁有不會重複的唯一性。本實驗場域採用 GSMA 的定議採用 IMEI 欄位作為 IoT 設備號碼，達成不會重複的唯一性的功能。IMEI 由 15-17 個數字組成，前八碼稱 TAC 表示裝置的品牌和型號，第 9 位開始到 14 位則是生產序號，第 15 號以後則是驗證碼。

(三) 地區與地域標示

依據 3GPP TS 29.561 定義，[226]當 SMF 分配裝置 IP 後可以透過 RADIUS 協議將 IP、IMEI、Cell ID 等資料傳出，Cell ID 及 Domain 同屬表示 UE 的地理位置，分大區域對應的 Domain 如臺北、高雄地方，小區域對應的 Cell ID，表示 UE 所在位置之基站。

(四) 5G 核心網路之 DNS 編碼

根據 GSMA IR.67 指引，[227]用於 5GC 架構中提供網元相關節點 FQDN 解析，由 3GPP TS 23.003 定義細部資訊，說明電信業者使用 5G 範圍之 DNS 定義與規範。

本計畫之編碼機制針對個別 IoT 設備配發一組 FQDN，格式如下：

<IMEI>.<Cell.ID>.<Domain_ID>.<sst>.nssf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

透過 FQDN，管理者可輕易識別出個別裝置廠牌、型號、網路切片特性及其所在位置，以達管理之效，以下詳細說明：

1. IMEI：為國際行動裝置辨識碼（International Mobile Equipment Identity, IMEI）。

---

[225] GSMA (2019/04) “IMEI Allocation and Approval Process” Retrieved from https://www.gsma.com/newsroom/wp-content/uploads//TS.06-v16.0.pdf ,P4 (2021/10/27)

[226] 3rd Generation Partnership Project (2020/06) “Technical Specification Group Core Network and Terminals;Interworking between the Public Land Mobile Network （PLMN）supporting packet based services andPacket Data Networks （PDN）” Retrieved from https://www.3gpp.org/ftp//Specs/archive/29_series/29.061/29061-f60.zip , P80 (2021/10/25)

[227] GSMA (2020/06) “DNS Guidelines for Service Providers and GRX and IPX Providers” Retrieved from https://www.gsma.com/newsroom/wp-content/uploads//IR.67-v16.0.pdf , P20 (2021/10/25)

2. Cell_ID：為基地臺之識別碼（例如臺北市中正區博愛路x號）。
3. Domain_ID：代表基地臺所在之地理位置（例如臺灣西部北區，新竹頭前溪以北至宜蘭礁溪）。
4. MNC：行動裝置之網路代碼（Mobile Network Code, MNC），是電信業者的編碼，例如中華電信為 011。
5. MCC：則為該裝置之國家代碼（Mobile Country Code, MCC），是電信業者所屬國家的代碼，例如臺灣為 466。
6. sst：為裝置所屬之服務切片類型（Service/Slice Type, SST），例如 sst=1 表示 eMBB，sst=2 表示 URLLC，sst =3 表次 MIOT。

PoC 驗證中 FQDN 資訊係由 IoT 設備傳送給 5G 模擬器，節錄 3GPP TS 23.502 R15 有關 IoT 設備建立連線時，其 FQDN 資訊來源如圖 4-12，另節錄圖 4-12 之步驟 1 及步驟 3 傳送資訊如下：[228]

● 步驟 1：PDU 會話建立請求（PDU Session Establishment Request）。

從 UE 到 AMF 傳送 NAS Message (S-NSSAI(s), DNN, PDU Session ID, Request type, Old PDU Session ID, N1 SM container

● 步驟 3：Nsmf_PDUSession_CreateSMContext 请求（Nsmf_PDUSession_CreateSMContextRequest）。

從 AMF 到 SMF 傳送 Nsmf_PDUSession_CreateSMContext Request (SUPI, DNN, S-NSSAI(s), PDU Session ID, AMF ID, Request Type, PCF ID, Priority Access, N1 SM container (PDU Session Establishment Request), User location information, Access Type, PEI, GPSI, UE presence in LADN service area, Subscription For PDU Session Status Notification, DNN Selection Mode, Trace Requirements) Nsmf_PDUSession_UpdateSMContext Request (SUPI, DNN, S-NSSAI(s), SM Context ID, AMF ID, Request Type, N1 SM container

[228] 3rd Generation Partnership Project (2021-09) ”Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS)”, 3GPP TS 23.502 V15.15.0, P66-68

(PDU Session Establishment Request), User location information, Access Type, RAT type, PEI)

依步驟 1 及步驟 3 說明，IoT 設備註冊時會傳送 SUPI、DNN、NSSAI、IMEI 及 User locatio information 等資訊至 SMF。[229]應用在 PoC 驗證中，NSSAI 為 IoT 設備訂閱之網路切片 SST，User location information 為 Cell_ID，而本次 PoC 的 Domain_ID 由 DNS 自動生成。

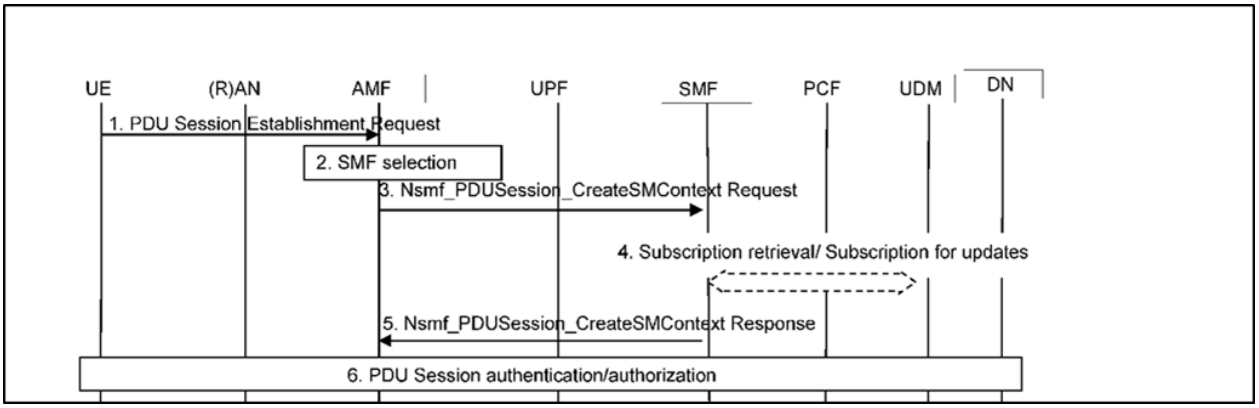


圖 4- 12、IoT 設備建立連線時之 FQDN 資訊來源

資料來源：3GPP TS 23.502 v15

四、實測驗證平臺之系統架構

(一) 功能邏輯架構

本次 PoC 實證 5G 場域下，當有大量 IoT 設備（UE）連網時，如何利用 DNN 與 NSSAI 網路切片參數做切片管理，並於 5G 模擬器中開發 Raidus Server 功能，使 5G 模擬器之核心網路具備 SMF 於 UE 註冊認證後，傳送 UE 的 AAA 資訊到第三方應用之機制，再利用 DNS 自動編碼生成 UE 之 A Record 或 AAAA Record，並藉由本計畫自行設計與開發之 RESTful API 將相關資訊傳遞到 Dashboard 主機以即時生成相關畫面。以下多重接取邊緣運算層、

[229] 3rd Generation Partnership Project (2021-09) "Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS)", 3GPP TS 23.502 V15.15.0, P65

無線接取層、終端設備及系統管理分述功能邏輯架構。

1. 多重接取邊緣運算層

本計畫 PoC 實測驗證場域採用一臺 Amarisoft Classic Callbox5G 模擬器，為一具有 3GPP 標準之 gNB Based 5G SA 模擬器，提供 5G 核心網功能打造實驗場域，可模擬 5G 基地臺（gNB）與核心網路（5GC）之標準行為，並支援網路切片功能，以符合本案 PoC 實證場域計畫目的，另外部署兩臺 MECS-6110 伺服器並於上面安裝 Edge DNS Server 與 DNS 編碼程式，分別為 DNS_1 與 DNS_2。

2. 無線接取層

配合 5G 核心網（5GC）功能配置之 5G 基地臺，提供符合 3GPP 5G gNB 相關無線接取層之標準介接。本計畫之 5G 模擬器提供 3 個符合 3GPP gNB 規範之 5G Cells，3 個 Cells 劃分為 2 個 Domain，配置 Cell_1 與 Cell_2 屬於 Domain_1，另配置 Cell_3 屬於 Domain_2。

3. 終端設備

IoT 終端裝置（UE）透過無線接取層接入多重接取邊緣運算層。本計畫提供 5 組 IoT 終端設備，依順序編號為 IoT_1、IoT_2、IoT_3、IoT_4 及 IoT_5。

4. 系統管理

使用一臺 MECS-6110 伺服器，上面安裝 Web Server 與平臺管理資料庫，提供 PoC 實測驗證場域的 DNS 編碼管理與監控功能。

依據本 PoC 規劃之功能邏輯架構，IoT 設備將透過 5G gNB 的基站天線（Cells）接入 5G 核心網之使用者平面和控制平面，再由 5G 核心網路提供 IoT 設備註冊、連接及認證網路等功能，IoT 設備將依所在位置連結至不同 Domain 中的 Cell。PoC 相關功能架構請參考圖 4-13。

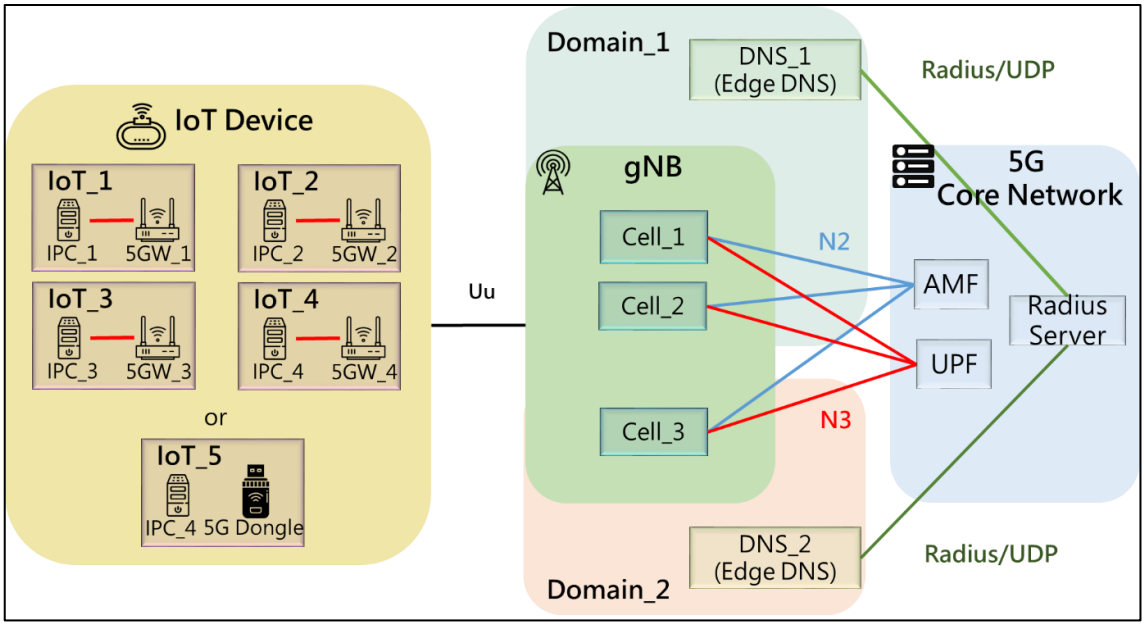


圖 4- 13、功能邏輯架構圖

資料來源：本計畫製作

當 IoT 設備連線到 5GC 的 AMF 進行註冊時，AMF 將設備裡 IMSI、IMEI 及 DNN 設定配發 IP 位址，並透過 RADIUS 協議將 DNN、Cell ID、IMSI、MSISDN、IMEI、IP、SST 等資料，依據設備所在 Domain 傳送給 DNS_1 或 DNS_2， DNS 收到資料後自動生成 A /AAAA Record。5GC 與 DNS 間採用之標準，係依據 3GPP TS 29.561 技術文件以 RADIUS Accounting 訊息內容，將 SMF 與 DN-AAA（DN-AAA 為第三方認證網元，可以透過 RADIUS 協議與 SMF 交換 authentication, authorization, and accounting 訊息）網元之用戶資訊及 AAA 資訊傳送給 DNS，作 DNS 自動編碼之應用。

(二) 硬體架構

PoC 實測驗證平臺之硬體設備，依其功能、廠牌、型號、數量資訊整理如表 4-11。

表 4- 11、PoC 實測驗證場域之硬體設備列表

項次	設備功能	廠牌	型號	數量	PoC 實測驗證平臺之架構部署關係說明
1	伺服器	凌華科技股份有限公司	MECS-6110	3 臺	兩臺伺服器運用於多重接取邊緣運算層，一臺伺服器運用於系統管理
2	IoT 裝置	凌華科技股份有限公司	MXE-211-M2G	4 臺	終端設備
3	網路交換器	HPE Aruba	Aruba 2930F	1 臺	於多重接取邊緣運算層裡作連接三臺 MEC 伺服器之用
4	5G 核心網路模擬設備	Amarisoft	Amarisoft Classic Callbox	1 臺	gNB Based 5G R15 SA 模擬器，無線接取層及 5G 核心網路
5	5G 閘道器	新漢股份有限公司	DTA1164 W /5G SA/NSA Gateway	4 臺	終端設備之 5G 無線模組
6	5G 行動網卡	皇鋒通訊股份有限公司	APAL TRIBUTO 5G Dongle	1 個	終端設備之 5G 無線模組

資料來源：本計畫製作

本計畫設計 2 種 IoT 設備之 5G 連網情境，第 1 種情境是 IoT 設備利用 5G 閘道器（5G Gateway）連網，例如：多個智慧電表連結至 5G Gateway 再連結至 gNB 之情形。驗測中係以工業主機（Industrial PC, IPC）加上 5G Gateway 之方式組成 IoT 終端設備，如圖 4-14 硬體設備架構圖中 IoT 設備編號 IoT_1（IPC_1+5GW_1）、IoT_2（IPC_2+5GW_2）、IoT_3（IPC_3+5GW_3）及 IoT_4（IPC_4+5GW_4）所示，IPC 透過乙太網路線連至 5G Gateway，每一個 5G Gateway 均安裝 5G SIM 卡，透過 5G 無線網路連至 5G

模擬器的基站天線，使 IoT 設備藉由 gNB 接入 5G 核心網。

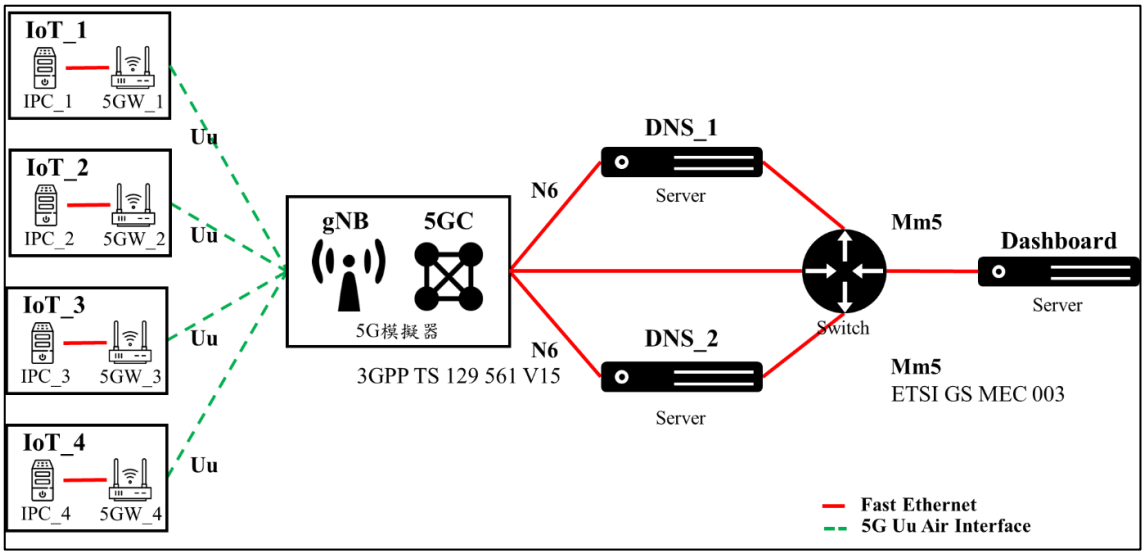


圖 4- 14、硬體設備架構圖（以 5G Gateway 連線）

資料來源：本計畫製作

第 2 種情境則是 IoT 設備透過 5G 行動網卡（5G Dongle）連網，例如：智慧工廠 AGV 機器人原生具備 5G 通訊模組，透過本機內 5G 通訊模組直接與 gNB 建立 5G 連線。驗測中以 IPC 加上 5G Dongle 之方式，組成 IoT 終端設備，如圖 4-15 中編號 IoT_5（IPC_4+5G Dongle）所示，IPC 直接透過 USB 介面獲得 5G 連線功能，於 5G Dongle 內插入 5G 網路 SIM 卡，由 5G Dongle 自動與 gNB 接入 5G 核心網完成註冊與 IP 配發流程，即可使 IPC 獲得 5G 網路存取能力。在後續情境測中，將與 IoT_1、IoT_2、IoT_3 一同進行測試，以驗證系統平臺同時處理 2 種連網情境之能力。

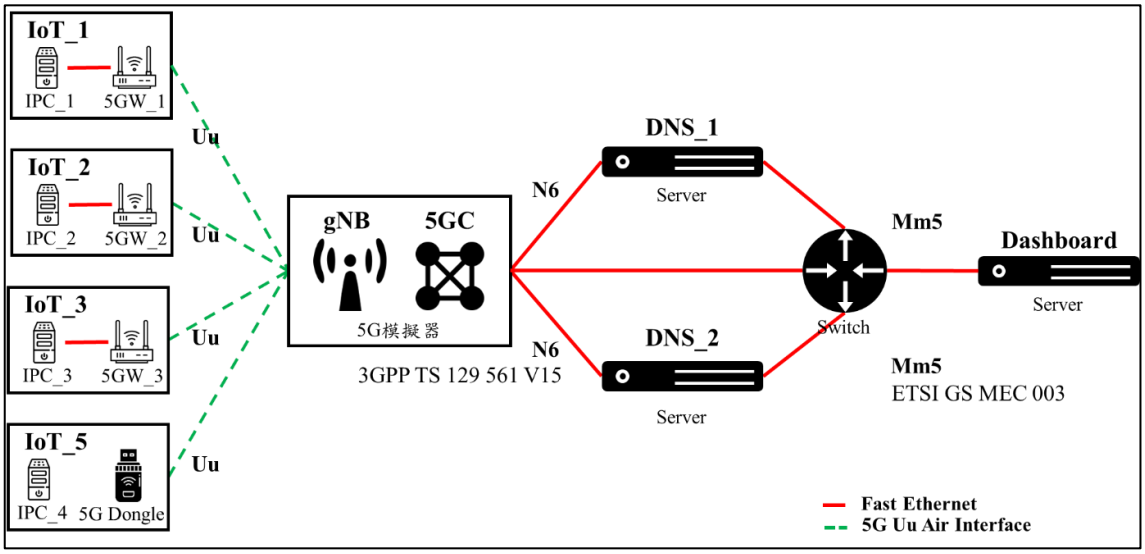


圖 4- 15、硬體設備架構圖（以 5G Dongle 連線）

資料來源：本計畫製作

IoT 終端設備透過 5G 基站連接 5G 核心網路與網際網路，一旦連接與 5G 認證成功，IoT 終端設備會被分配到一組 IP 位址，這組 IP 位址也會依前述編碼規則分配到一組 DNS 名稱。在 IoT 終端設備移動過程中，5G 核心網路會隨時管理 IoT 終端設備的 IP 位址，管理原則包含動態分配與記住所分配的 IP 位址，圖 4-16、圖 4-17 為 PoC 實測驗證場域的 UE 註冊流程。

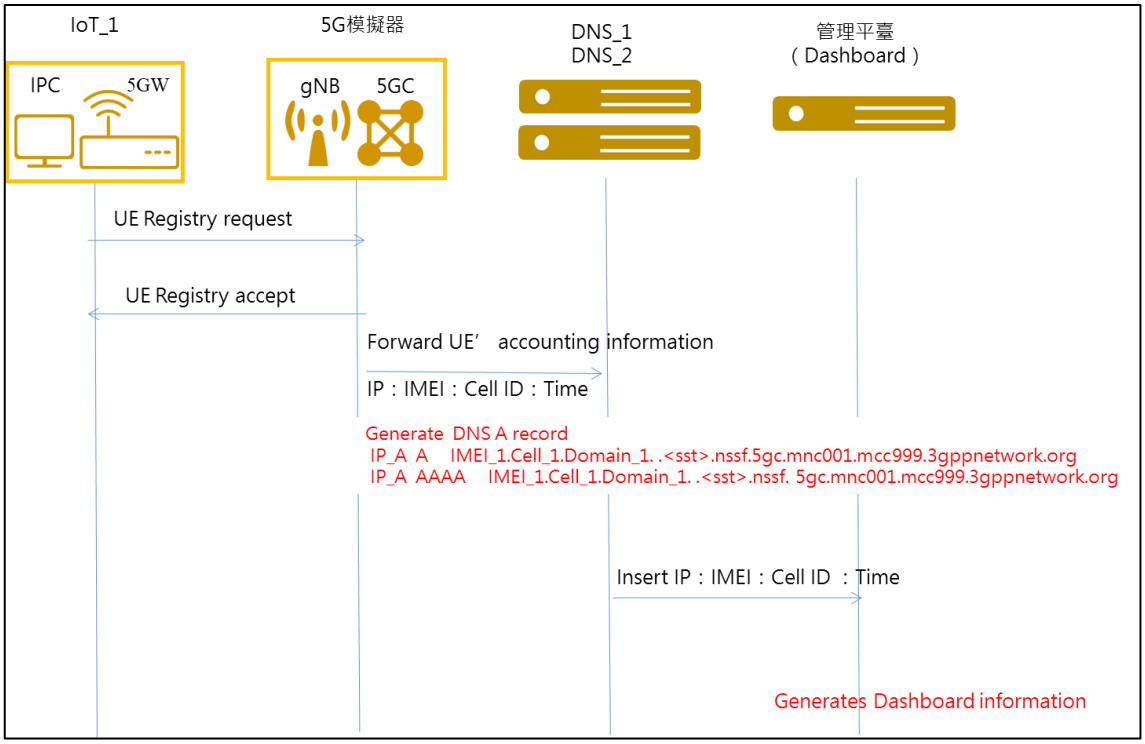


圖 4- 16、 PoC 實測驗證場域的 UE 註冊流程圖(以 5G Gateway 連線)

資料來源：本計畫製作

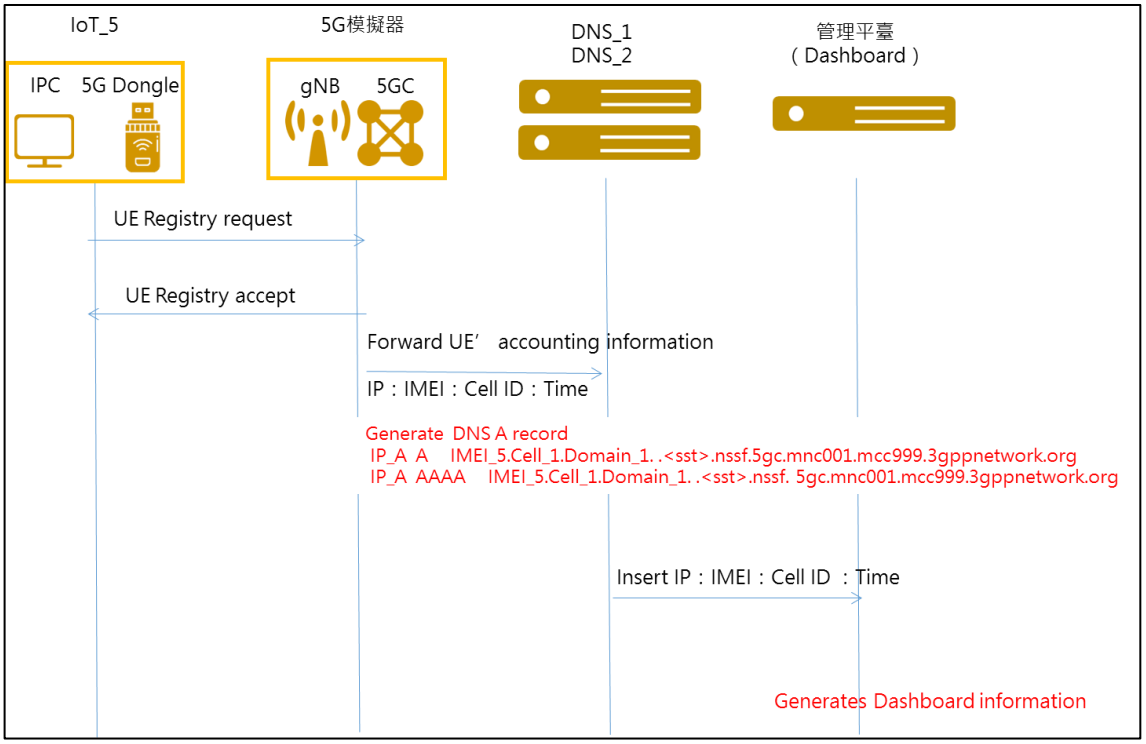


圖 4- 17、 PoC 實測驗證場域的 UE 註冊流程圖（以 5G Dongle 連線）

資料來源：本計畫製作

(三) 實測驗證平臺之軟體規劃與程式開發

PoC 實測驗證平臺環境包含 3 臺伺服器，其中 2 臺用於 DNS Server，1 臺用於場域展示及管理平臺 Dashboard，伺服器的作業系統與所需要的軟體執行環境架構如圖 4-18 所示：

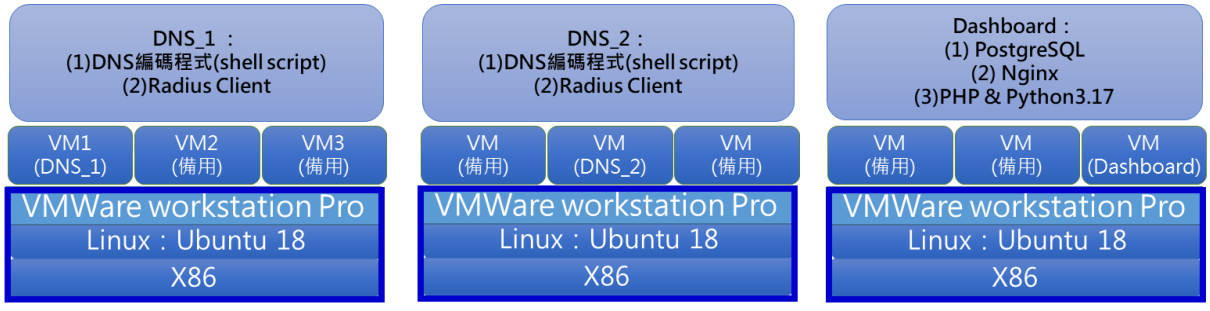


圖 4- 18、伺服器系統軟體架構圖

資料來源：本計畫製作

本案開發 4 個客製化軟體，用於將註冊資訊傳送到 DNS 伺服器，以進行 DNS 編碼程式解析，並將 IP 及域名資訊寫到 DNS 伺服器上，最後由程式管理平臺（Dashboard）到 DNS 伺服器上截取資訊，以圖形化介面（Graphical User Interface, GUI）呈現。4 個客製化軟體說明如下：

1. Edge DNS Server 系統軟體

在 PoC 實測驗證場域之伺服器上安裝 BIND（Berkeley Internet Name Domain）9.4 版本以上之 DNS Server 系統軟體，支援 DNS split、minimal response 及 RPZ（Response policy zone），並具備以下功能：

(1) 網域名稱系統（Domain Name System, DNS）：在網際網路中，機器（如電腦、手機等設備）使用被稱為 IP 位址的數字相互通訊，而域名則是人可閱讀的識別碼，輸入域名即可連結至正確的網路位置。DNS 係對映域名及 IP 位址之分散式資料庫，無論輸入域名或 IP 位址，均可查詢到相應之主機。

(2) DNS 查詢方式：分為遞迴式（Recursive）及交談式（Iterative）兩種。DNS 用戶端向 DNS Server 之查詢以遞迴式為主，用戶端將封包送出查詢，直到得到正確名稱；而 DNS Server 間之查詢以交談式為主。

(3) 資源記錄（Resource Record, RR）類型：

- 主機記錄（Host Address, A）： A 記錄用於解析主機之網域名稱，並將其對映到主機實體之 IP 位址。
- 別名記錄（Canonical Name, CNAME）：CNAME 為別名的標準名稱記錄，用於將某個別名連結至另一個正式的或標準的網域名稱記錄。
- IPv6 主機記錄（AAAA）：與 A 記錄對應，解析主機網域名稱並將其對映到 IPv6 位址。
- 服務位置記錄（Service, SRV）：用於識別或指定提供特定服務的伺服器。

- 域名伺服器記錄（Name Server, NS）：決定使用哪個 DNS Server 進行通訊及解析。
- NAPTR 記錄（Naming Authority Pointer, NAPTR）：用於支援 ENUM 查詢，將電話號碼對映到 DNS 系統。
- 指標記錄（Pointer, PTR）：於反向查詢時提供網域名稱，係將 IP 位址對映到主機 FQDN。

2. DNS 編碼程式

本計畫在兩臺伺服器上安裝 DNS Server 並以 Ubuntu 內建 Shell script 方式編譯，使用 daemon 的方式每 60 秒讀取 5G 模擬器的 CSV 格式中的 RADIUS information，讀取後在 /var/named/chroot/etc/named.conf 下，自動生成 FQDN：<IMEI>.<Cell.ID>.<Domain_ID>.<sst>.nssf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org。

在 DNS Server 中，由多個資源記錄組成一個網域名稱之區域檔案（Zone File），用以解析及反向解析 DNS 名稱，A Record 及 AAAA Record 即為資源記錄一種，可將 DNS 的網域名稱對映到 IPv4 或 IPv6 位址。[230]當取得兩種 IP 格式的其中一種後，DNS 編碼程式將自動生成 FQDN 以及與 UE 對應之 DNS A Record 及 AAAA Record，形成 IoT 設備的 IP 與 DN 的配對關係，達成下世代電信號碼分配與設備對應。

DNS 編碼程式邏輯與判讀處理原則，連動管理平臺（Dashboard）之開發條件及判讀如下：

(1) 如果 DNS 編碼程式無法讀取 RADIUS information 或是讀取失敗以及 DNS FQDN 無法寫入，便產生 error message，寫入 /var/log/messages，並透過 syslog 送往 Dashboard 主機顯示在螢幕上。

[230] TWNIC" DNS 資源紀錄(Resource Record)介紹", Retrieved from http://dns-learning.twnic.net.tw/bind/intro6.html（2021/11/29）

(2) 若生成 FQDN 成功，便產生 successful message，寫入 /var/log/messages，並透過 syslog 送往 Dashboard 主機顯示在螢幕上。

(3) 當收到 RADIUS information 為 UE account start，生成 FQDN 後，透過 PostgreSQL insert 語言將 5G Gateway 的 IP、IMEI、IMSI、Cell_ID、Domain_ID、Time 送往 Dashboard 主機。

(4) 當收到 RADIUS information 為 UE account stop，便刪除原來 FQDN 紀錄，透過 PostgreSQL delete 語言將 5G Gateway 的 IP、IMEI、IMSI、Cell_ID、Domain_ID、Time 送往 Dashboard 主機。

3. 場域展示及管理平臺（Dashboard）

在伺服器上安裝 Web Server 與資料庫，當 DNS 收到 5G 模擬器的資料後，會透過 RESTful API 向 Dashboard 傳送 IoT 設備之註冊訊息，以將資料寫入 Dashboard 的 PostgreSQL 資料庫。PostgreSQL 資料庫儲存平臺相關資訊包含 DNS Log、System Log 與 IoT 設備移動所產生的 Log。Dashboard 以 GUI 方式顯示 IoT 設備的 Registry Start/Stop time、MSISDN、IP、IMSI、IMEI、Cell ID、SST 等用戶連網訊息。Web Server 伺服器透過 Python 提取資料庫資料，使用者可透過 Web-based GUI 操作介面瀏覽以下功能：

- 提供查詢功能列，查詢與顯示特定裝置之位置與歷史軌跡。
- 可即時顯示裝置之 DNS Name 及其使用之 IP 位址。
- 提供系統列顯示系統狀態。
- 提供實驗場域無線網路環境 System Log。
- Dashboard 的主要頁面如圖 4-19、圖 4-20 及圖 4-21。

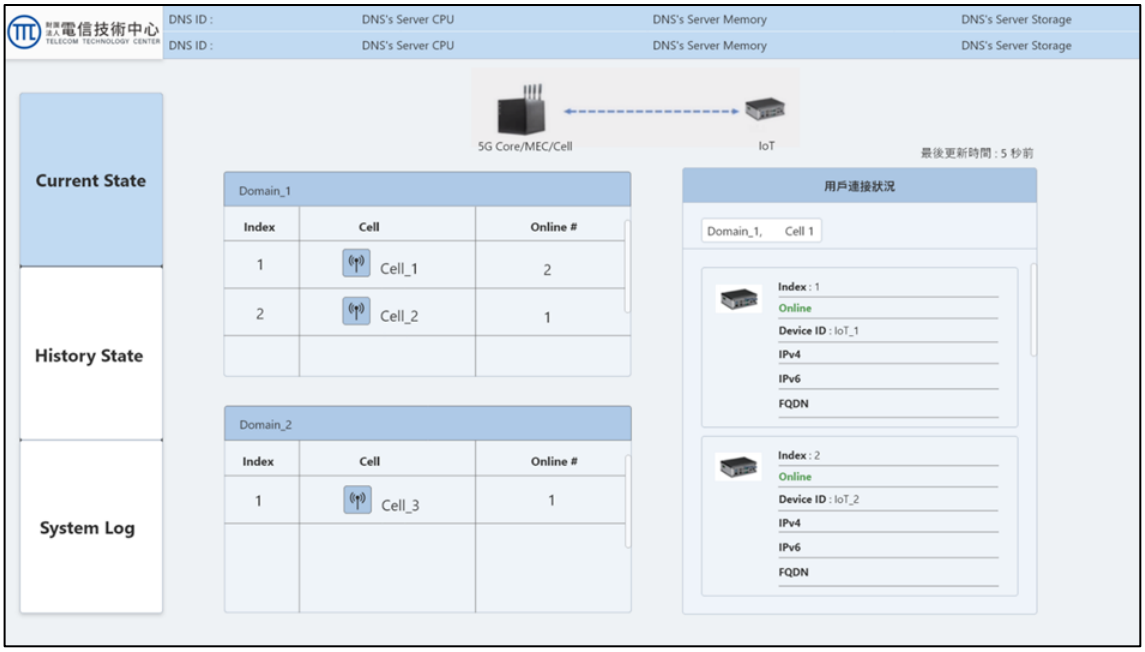


圖 4- 19、PoC 場域 Dashboard 首頁示意圖

資料來源：本計畫製作

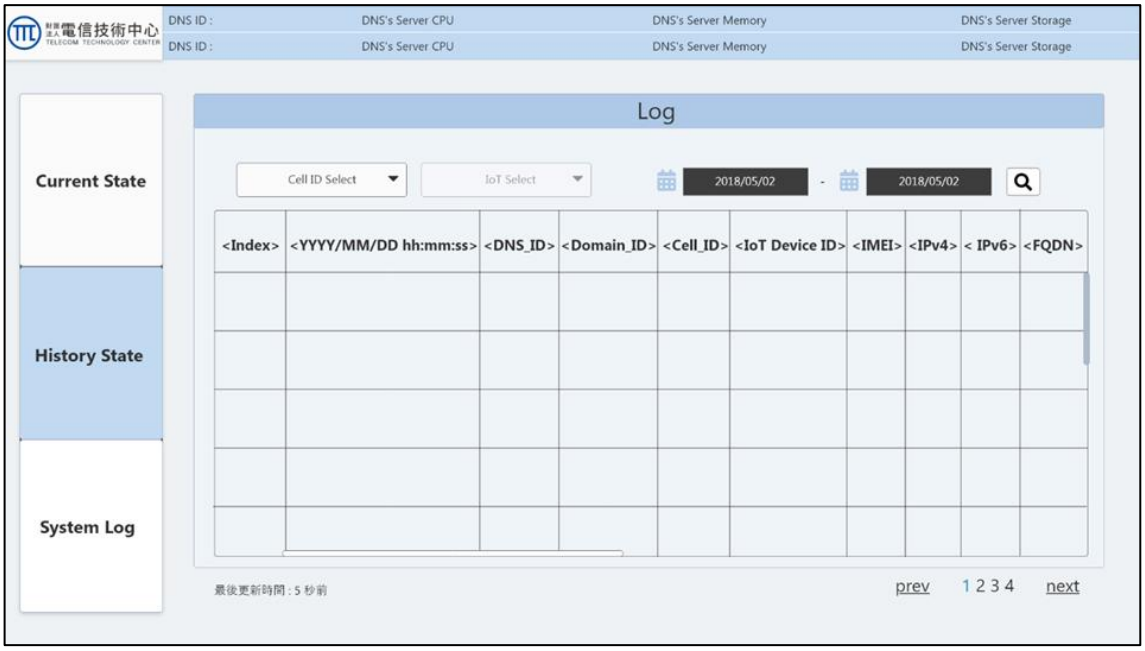


圖 4- 20、PoC 場域 Dashboard 歷史資料示意圖

資料來源：本計畫製作

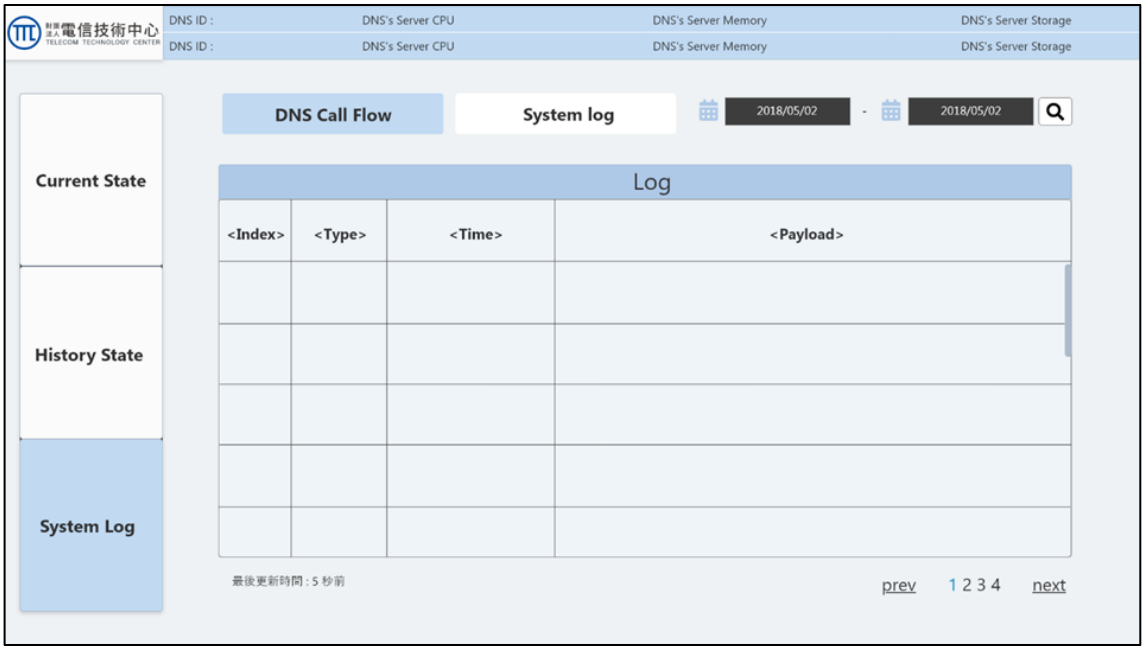


圖 4- 21、PoC 場域 Dashboard System Log 示意圖

資料來源：本計畫製作

4. 遠端認證撥接使用者服務（Remote Authentication Dial In User Service, RADIUS）傳送功能

   本 PoC 依前述之編碼機制及功能架構，分別在 2 臺伺服器上安裝 Edge DNS Server 系統軟體、DNS 編碼程式，及在 1 臺伺服器上安裝場域展示用 Dashboard，並於 5G 模擬器上開發 RADIUS 傳送功能，依據 3GPP TS_129561V15 以 RADIUS 協議向 DNS 發送 IoT 設備之 AAA accounting information，以將 5G UE 註冊等相關資訊，傳送到 DNS 伺服器。

   5G 模擬器中 5G Log Analyzer 內具備 API Server 模組以及 RADIUS Server 模組。API Server 模組主要用於定期性觸發 5G 模擬器對外開放溝通的系統 API，並獲取 5G 模擬器中基地臺與核心網路之運行紀錄，並從紀錄日誌中撈取包含 IoT 設備之相關資訊，如：UE 註冊所獲得 IP 位址、IMSI 資訊、IMEI 資訊、UE 連接之基地臺的 Cell ID、UE 上線或離線時

間與目前狀態等資訊。而 RADIUS Server 模組則是負責與 DNS Server 建立連線，並將 API Server 所獲得並分析出的資訊即時傳送給 DNS Server 以建立 DNS Record，其 RADIUS 傳送運作流程如下及如圖 4-22 所示。：

(1) 啟動 5G Log Analyzer。

(2) 確認 5G Log Analyzer 中 API Server 以及 RADIUS Server 是否能分別正常連接至 5G 網路模擬器以及 DNS 伺服器。

(3) API Server 週期性發送獲取 log 資訊之 API Request。

(4) API Server 收到 API Response 後，分析 Log 資訊內容，並依照範例之 csv 格式整合產生 DNS Record 之資訊並提供給 RADIUS Server。

(5) RADIUS Server 收到來自 API Server 的 csv 格式輸入後，立即將資訊透過 RADIUS 連線發送給 DNS Server。

(6) 持續重複 3-5 流程。

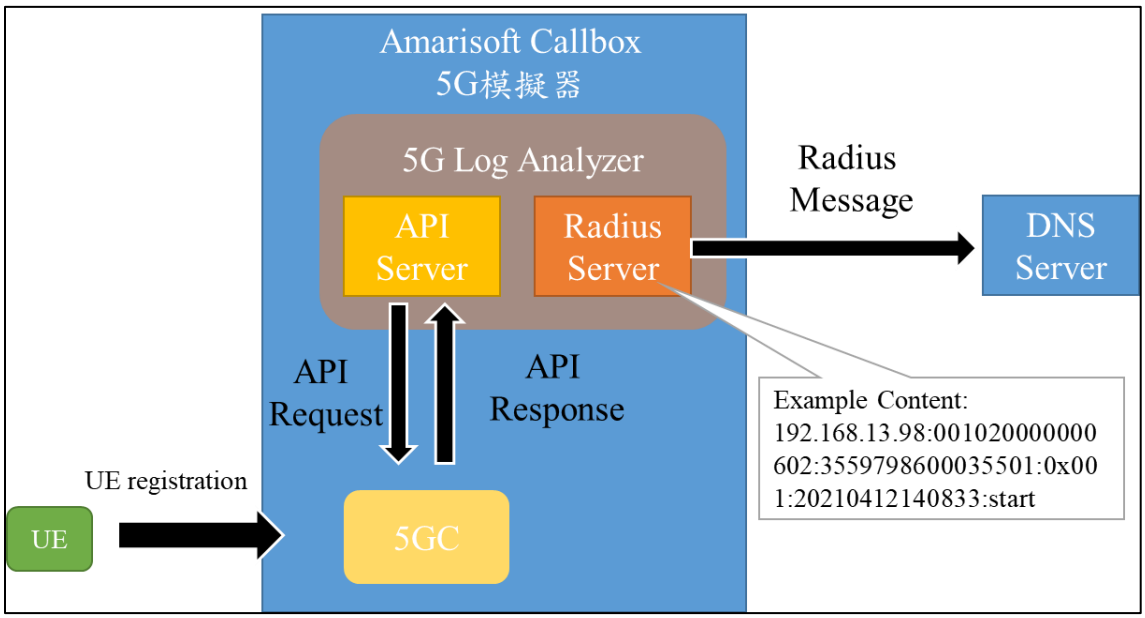


圖 4- 22、5G 模擬器對 RADIUS 傳送運作流程圖

資料來源：本計畫製作

彙整 PoC 實測驗證系統平臺軟體及自主設計開發程式如表 4-12。

表 4- 12、PoC 場域軟體列表

項次	軟體名稱	功能說明	數量
1	Edge DNS Server 系統軟體	DNS 安裝與設定	2 套
2	DNS 編碼程式	自動生成與 5G UE 對應 DNS A/AAAA Record	2 套
3	Dashboard	場域展示用網站，顯示各設備狀態與展示運作流程	1 套
4	RADIUS 資料傳送	將 UE 設備註冊資料，傳送到 DNS	1 套
5	MEC 伺服器系統軟體	1. Ubuntu 2. PostgreSQL 3. Nginx	1 式

資料來源：本計畫製作

第三節　電信號碼分配與設備對應之測試項目及測試結果

一、驗證設計

本驗證設計物聯網裝置以兩種方式接取 5G 網路，連網方式一係透過 5G Gateway 作為裝置與網路連結之中介，為物聯網應用廠商常用連網方式之一，例如智慧電表；另一連網方式係透過 5G Dongle 讓裝置直接接取 5G 網路，例如智慧工廠之無人搬運車（Automated Guided Vehicle, AGV）或機器人。本驗證包含以下三大項技術程序：

1. 物聯網裝置利用 5G Gateway 接取 5G 網路，並在同域不同基站以及跨域不同基站間移動，驗證編碼系統註冊及自動編碼能力。
2. 物聯網裝置利用 5G Dongle 接取 5G 網路，並在同域不同基站以及跨域不同基站間移動，驗證編碼系統註冊及自動編碼能力。
3. 驗證編碼系統為大量物聯網裝置註冊及自動編碼之能力。

二、基本驗證項目

PoC 實測驗證平臺系統之基本驗證項目，包含系統邏輯元件之介接測試、連線及信令測試。UE 透過 5G gNB 連線至 5GC，過程包括無線頻段取得、UE 註冊、UE 離線及 UE 接入 5G 網路等基本驗證測試，如表 4-13 彙整。

表 4- 13、基本驗證項目彙整表

項次	測試內容	預期結果	測試結果
1	5G radio band scanning	UE 可掃描搜尋到 5G N78 頻段之無線電廣播訊號	UE 掃描搜尋到 5G 模擬器，其掃描結果包含 99901 之 5G 網路訊號
2	UE attached with successful	UE 註冊至 5G 網路成功	UE 註冊成功，UE 成功接收到 5G 模擬器所發送之 Registration Accept 訊息
3	UE attached with failure	UE 註冊至 5G 網路失敗	將 UE 資訊移除後，使 UE 註冊遭拒，UE 收到 5G 模擬器所發送之 Registration reject 訊息
4	UE de-attached with successful case	UE 從 5G 網路離線成功	關閉 5G Gateway 功能與電源，5G Gateway 依照 3GPP 標準流程傳送 Deregistration request，內容包含 5G Gateway 註冊所獲得之 5G-GUTI 參數並接收到 gNB 發送之 RRC release
5	UE integrity protection	UE 發送之控制封包具備完整性資安保護	SecurityModeCommand 訊息中指定之完整性保護演算法為 5G NIA1，與 NAS 層訊息皆包含依據訊息內容雜湊之 MAC-I 值，且註冊過程中未出現 Integrity check failed 之訊息
6	UE data traffic interoperability	UE 可正常透過 5G 網路與其他設備聯通	UE 可取得 5GC 所配發之 IPv4 位址，並順利使用 Ping 工具與其他設備聯通，5G Gateway 接收到 Google DNS 回覆之 ICMP Echo Response 證明具備資料平面互通性

項次	測試內容	預期結果	測試結果
7	Network slicing access privileges	gNB 與 5GC 建立 NG 協定連線時，只有設定合法 network slicing 的 gNB 才能成功建立連線	gNB 與 5GC 建立 NG 協定連線時，只有設定合法 network slicing 的 gNB 才會成功建立連線並回覆 NG setup response 訊息

資料來源：本計畫製作

三、情境測試項目

情境測試項目主要係藉由設定 IoT 設備不同之連網及使用情形，驗證當 IoT 設備在不同 Domain 之間移動時，IoT 設備的 IP 會自動取得 IP 位址，同時 DNS 伺服器會同步動態更改 A Record 及 AAAA Record，並與其他 Domain 上的 DNS 伺服器交換 FQDN 資訊，達到 IoT 設備在專網間的互相通訊與辨識，自動配置（Autoconfig）與管理專網號碼。

當完成 IoT 設備在不同 Cell 之間移動進行自動註冊後，將繼續 IoT 設備在不同 Cell 之間持續移動，觀察 log 變化情形，另外採用程式模擬方式產生大量靜態 IoT 設備，檢視其支援大量設備自動註冊的能力。

IoT 設備初始參數設定如表 4-14：

表 4- 14、IoT 設備初始參數

	IoT_1	IoT _2	IoT _3	IoT _4	IoT_5
DNN	internet1	internet2	internet3	internet4	internet5
IMEI	355979860003363	355979860003702	355979860003728	355979860003785	359047100170495
NSSAI	eMBB	eMBB	URLLC	MIOT	MIOT
SST	1	1	2	3	3
Template	AR/VR 8K Videos	AR/VR 8K Videos	Factory Automatic Machines	Smart City Sensors	Smart City Sensors
Throughput	1Gbps/1Gbps	1Gbps/1Gbps	500Mbps/500 Mbps	1Mbps/1Mbps	1Mbps/1Mbps

資料來源：本計畫製作

(一) 情境一

IoT 環境中，如溫溼度感測或是空氣品質偵測等傳統設備，並不具備 5G 連線能力，可以 5G Gateway 作為裝置與網路連結之中介進行5G連網，為物聯網應用廠商常使用之連網方式。情境一採用 MXE-211-M2G 設備與 DTA1164W 5G SA/NSA Gateway 組成 IoT 終端設備，場域中共有 4 組 IoT 終端設備，依序為 IoT_1、IoT_2、IoT_3、IoT_4。

1. 同域測試

當 IoT 設備與 5GW_1 從 Cell_1 移動到 Cell_2，觀察 IP 與域名變化，同域測試內容及預期結果如表 4-15 ，IP 註冊與 DNS 動態管理流程及說明如圖 4-23 所示。

表 4- 15、同域測試

項次	測試內容	預期結果
1	5G 模擬器及 DNS 間的編碼核配與管理	5G 模擬器可以透過 Raius 協議將 IP:IMSI:IMEI:Cell ID 資訊傳給 DNS
2	Device 取得 IP（IPv4/IPv6）與 DNS mapping	5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致
3	DNS 編碼核配與管理	DNS 可以依據 5G 模擬器產生之 RADIUS 內容自動產出 A/AAAA Record
4	多個 Device 註冊 DNS 與核配編碼	比對各 5G 模擬器及 DNS：Device IP、IMSI、IMEI 及 Cell ID 結果一致

資料來源：本計畫製作

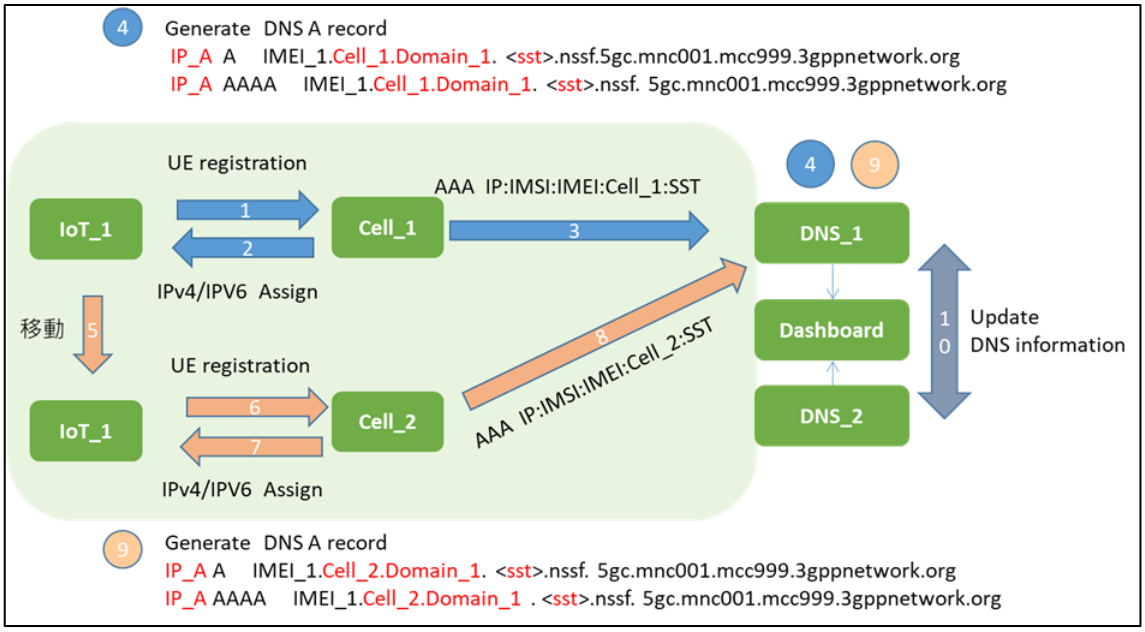


圖 4- 23、同域移動之 IP 註冊與 DNS 動態管理流程

資料來源：本計畫製作

(1) 測試步驟

同域測試步驟如表 4-16 說明：

表 4- 16、同域移動之 IP 註冊與 DNS 動態管理流程

步驟	流程	說明
1	UE 註冊	IoT 連線到 Cell_1，並進行註冊
2	配發 IPv4/IPV6 位址	5G 模擬器配發 IP 給 IoT
3	傳送註冊資訊至 DNS	傳送[IP:IMSI:IMEI:Cell_1:SST]等資訊至 DNS
4	Generate DNS A/AAAA Record	DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record
5	UE 移動	IoT 從 Cell_1 移動至 Cell_2，同為 Domain_1
6	UE registration	IoT 連線到 Cell_2，並進行註冊
7	配發 IPv4/IPV6 位址	5G 模擬器配發 IP 給 IoT，因為是同一 Domain，使用原來的 IP
8	傳送註冊資訊至 DNS	5G 模擬器傳送 [IP:IMSI:IMEI:Cell_2:SST]等資訊至 DNS
9	Generate DNS A/AAAA Record	DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record
10	DNS 與 Dashboard 更新資料	Dashboard 取得更新的 DNS A/AAAA Record 資訊

資料來源：本計畫製作

(2) 同域移動設備參數內容

完成步驟 1 到步驟 4 後進入系統檢視 IoT 設備參數異動，如圖 4-24 所示：

		IoT_1	IoT_2	IoT_3	IoT_4
	DNN	internet1	internet2	internet3	internet4
	IMEI	355979860003363	355979860003702	355979860003728	355979860003785
	NSSAI	eMBB	eMBB	URLLC	MIOT
	SST	1	1	2	3
	Template	AR/VR 8K Videos	AR/VR 8K Videos	Factory Automatic Machines	Smart City Sensors
	Throughput	1Gbps/1Gbps	1Gbps/1Gbps	500Mbps/500Mbps	1Mbps/1Mbps
步驟1,2	Service IP IPv4 (DHCP)	10.10.11.3	10.10.12.3	10.10.13.3	10.10.14.3
	Service IP IPv6 (DHCP)	10:10:11:3:200:ff:fe00:0	10:10:12:2:200:ff:fe00:0	10:10:13:2:200:ff:fe00:0	10:10:14:2:200:ff:fe00:0
步驟3,4	DN	355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003785.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org

圖 4- 24、IoT 設備註冊 IP 以及自動註冊 DN 後之參數

資料來源：本計畫製作

IoT 在同域的不同 Cell 移動時（步驟 5），DNN 與 IP 不更換，DN 會更改 Cell 名稱。完成步驟 6 到步驟 10 後進入系統檢視 IoT 設備參數之異動情形，如圖 4-25 所示：

		IoT_1	IoT_2	IoT_3	IoT_4
	DNN	internet1	internet2	internet3	internet4
	IMEI	355979860003363	355979860003702	355979860003728	355979860003785
	NSSAI	eMBB	eMBB	URLLC	MIOT
	SST	1	1	2	3
	Template	AR/VR 8K Videos	AR/VR 8K Videos	Factory Automatic Machines	Smart City Sensors
	Throughput	1Gbps/1Gbps	1Gbps/1Gbps	500Mbps/500Mbps	1Mbps/1Mbps
步驟6,7	Service IP IPv4 (DHCP)	10.10.11.3	10.10.12.3	10.10.13.3	10.10.14.3
	Service IP IPv6 (DHCP)	10:10:11:3:200:ff:fe00:0	10:10:12:2:200:ff:fe00:0	10:10:13:2:200:ff:fe00:0	10:10:14:2:200:ff:fe00:0
步驟8-10	DN	355979860003363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003785.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org

圖 4- 25、IoT 設備在同域的不同 Cell 移動後之參數

資料來源：本計畫製作

(3) 同域測試結果

彙整同域測試之預期結果及測試後結果對照說明如表 4-17。

表 4- 17、同域移動測試結果

項次	測試內容	預期結果	測試結果
1	5G 模擬器及 DNS 間的編碼核配與管理	5G 模擬器可以透過 RADIUS 協議將 IP:IMSI:IMEI:Cell ID 資訊傳給 DNS	於步驟 3 以及 9，5G 模擬器會透過 RADIUS 協議將 IP:IMSI:IMEI:Cell ID:SST 資訊傳給 DNS。
2	Device 取得 IP (IPv4/IPv6)與 DNS mapping	5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致	IoT 終端設備於步驟 1、2 以及步驟 5、6、7 完成註冊後，自動取得 IP 位置。 檢視 5G 模擬器與 DNS 系統上所看到的 IP 資訊一致。
3	DNS 編碼核配與管理	DNS 可以依據 5G 模擬器產生 RADIUS 內容自動產出 A/AAAA Record	於步驟 4、9，DNS 透過 RADIUS 協議得到的 IP:IMSI:IMEI:Cell ID:SST 資訊，自動產生 A/AAAA Record。
4	多個 Device 註冊 DNS 與核配編碼	比對各 5G 模擬器及 DNS：Device IP、IMSI、IMEI 及 Cell ID 結果一致	於 Dashboard 檢視各 IoT 終端設備的 IP、IMSI、IMEI 及 Cell ID 的資訊，與 5G 模擬器傳送的資料一致。

資料來源：本計畫製作

如圖 4-26，從 Dashboard 確認註冊後，4 臺 IoT 設備在 Cell_1 的位置：

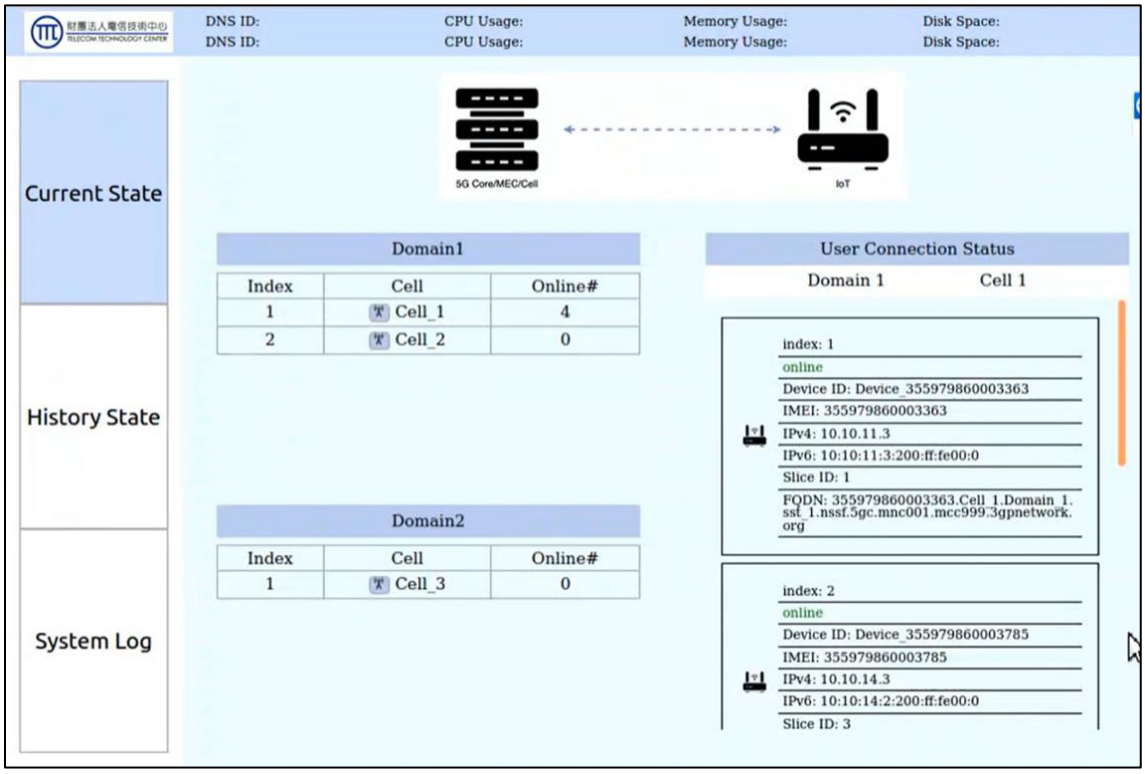


圖 4- 26、IoT 設備註冊後之 Dashboard 畫面

資料來源：本計畫製作

如圖 4- 27，從 Dashboard 可確認，同域內 4 臺 IoT 設備移動從 Cell_1 至 Cell_2 的位置：

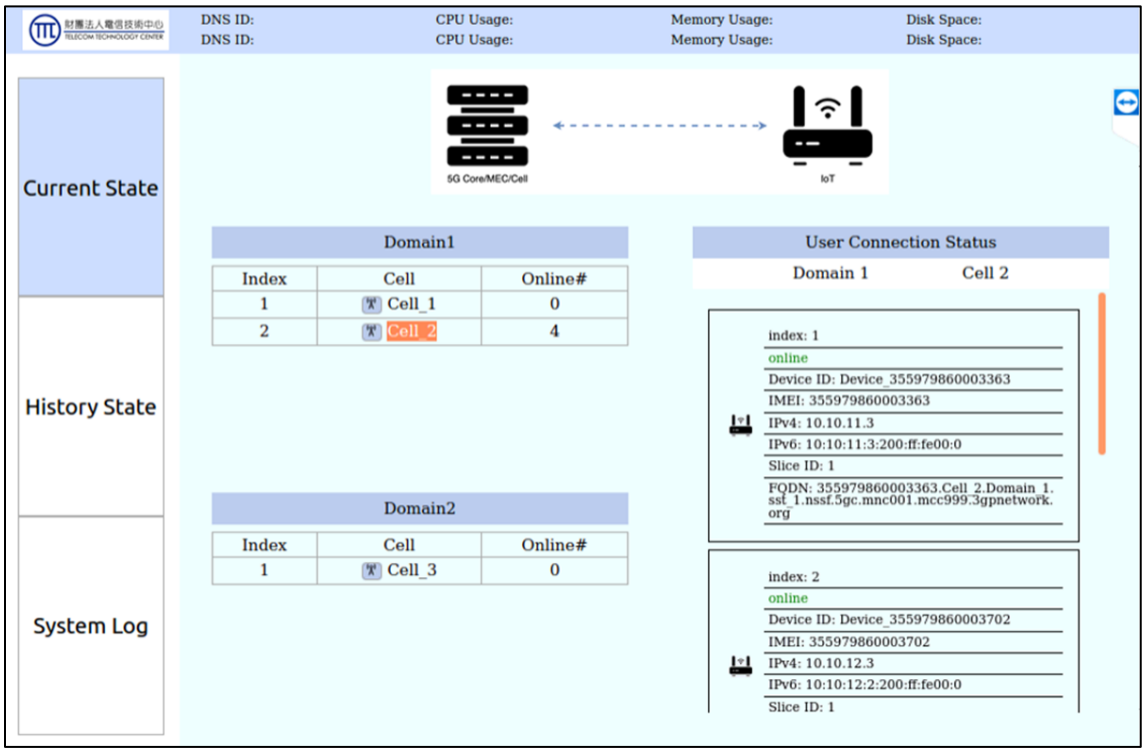


圖 4- 27、IoT 設備同域移動後之 Dashboard 畫面

資料來源：本計畫製作

從 Dashboard 下載資料中截取 IoT 設備註冊後自動編碼產生 FQDN 之 System Log 如表 4-18：

表 4- 18、IoT 設備註冊後之 Dashboard System Log

Datetime	Payload	Type
2021/11/1 14:07	Device_355979860003363 is attached on Cell_1 with FQDN 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 14:07	Device_355979860003702 is attached on Cell_1 with FQDN 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 14:08	Device_355979860003728 is attached on Cell_1 with FQDN 355979860003728.Cell_1.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 14:08	Device_355979860003785 is attached on Cell_1 with FQDN 355979860003785.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO

資料來源：本計畫製作

2. 跨域測試

當 IoT 設備與 5GW_1 從 Cell_1 移動到 Cell_3，觀察 IP 與域名變化， 跨域測試內容及預期結果如表 4-19，其 IP 註冊與 DNS 動態管理流程如圖 4-28：

表 4- 19、跨域測試

項次	測試內容	預期結果
1	5G 模擬器及 DNS 間的編碼核配與管理	5G 模擬器可以透過 Raius 協議將 IP:IMSI:IMEI:Cell ID 資訊傳給 DNS
2	跨網域 Device 取得 IP（IPv4/IPv6）與 DNS mapping	5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致
3	跨網域 Device 的 DNS 編碼核配與管理	DNS 可以依據 5G 模擬器產生 RADIUS 內容自動產出 A/AAAA Record

資料來源：本計畫製作

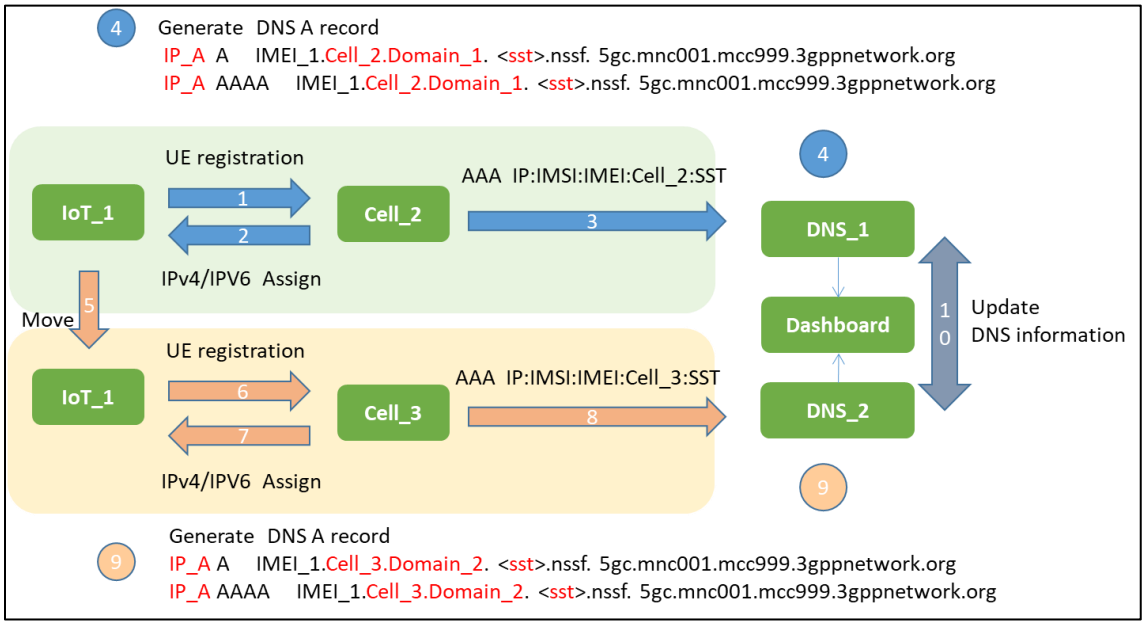


圖 4- 28、跨域移動之 IP 註冊與 DNS 動態管理流程

資料來源：本計畫製作

(1) 測試步驟

跨域測試步驟如表 4-20 說明：

表 4- 20、跨域移動之 IP 註冊與 DNS 動態管理流程

步驟	流程	說明
1	UE 註冊	IoT 連線到 Cell_2，並進行註冊
2	配發 IPv4/IPV6 位址	5G 模擬器配發 IP 給 IoT
3	傳送註冊資訊至 DNS	5G 模擬器傳送 [IP:IMSI:IMEI:Cell_1:SST]等資訊至 DNS
4	Generate DNS A/AAAA Record	DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record
5	UE 移動	IoT 從 Cell_2 移動至 Cell_3，從 Domain_1 移動至 Domain_2
6	UE registration	IoT 連線到 Cell_3，並進行註冊
7	配發 IPv4/IPV6 位址	5G 模擬器配發 IP 給 IoT
8	傳送註冊資訊至 DNS	5G 模擬器傳送 [IP:IMSI:IMEI:Cell_3:SST]等資訊至 DNS
9	Generate DNS A/AAAA Record	DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record
10	DNS 與 Dashboard 更新資料	Dashboard 取得更新的 DNS A/AAAA Record 資訊

資料來源：本計畫製作

(2) 跨域移動設備參數內容

步驟 1 到步驟 4 之註冊流程與同域測試相同，相關參數請參考前圖 4-24。當 IoT 設備跨域移動時（步驟 5），DNN 不變，註冊時將得到新的 IP，同時也會更改 DN 的 Cell 與 Domain 名稱，完成步驟 6 到步驟 10 後進入系統檢視 IoT 設備參數之異動情形，如圖 4-29 所示：

		IoT_1	IoT_2	IoT_3	IoT_4
	DNN	internet1	internet2	internet3	internet4
	IMEI	355979860003363	355979860003702	355979860003728	355979860003785
	NSSAI	eMBB	eMBB	URLLC	MIOT
	SST	1	1	2	3
	Template	AR/VR 8K Videos	AR/VR 8K Videos	Factory Automatic Machines	Smart City Sensors
	Throughput	1Gbps/1Gbps	1Gbps/1Gbps	500Mbps/500Mbps	1Mbps/1Mbps
步驟 6,7	Service IP IPv4 (DHCP)	10.10.11.4	10.10.12.4	10.10.13.4	10.10.14.4
	Service IP IPv6 (DHCP)	10:10:11:4:200:ff:fe00:0	10:10:12:3:200:ff:fe00:0	10:10:13:3:200:ff:fe00:0	10:10:14:3:200:ff:fe00:0
步驟 8-10	DN	355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003785.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org

圖 4- 29、IoT 設備跨域移動後之參數

資料來源：本計畫製作

(3) 跨域測試結果

彙整跨域測試之預期結果及測試後結果對照說明如表 4-21。

表 4- 21、跨域移動測試結果

項次	測試內容	預期結果	測試結果
1	5G 模擬器及 DNS 間的編碼核配與管理	5G 模擬器可以透過 RADIUS 協議將 IP:IMSI:IMEI:Cell ID 資訊傳給 DNS	於步驟 3 以及 9，5G 模擬器會透過 RADIUS 協議將 IP:IMSI:IMEI:Cell ID:SST 資訊傳給 DNS。
2	Device 取得 IP (IPv4/IPv6)與 DNS mapping	5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致	IoT 終端設備於步驟 1、2 以及步驟 5、6、7 完成註冊後，自動取得 IP 位置。檢視 5G 模擬器與 DNS 系統上所看到的 IP 資訊一致。
3	DNS 編碼核配與管理	DNS 可以依據 5G 模擬器產生 RADIUS 內容自動產出 A/AAAA Record	於步驟 4、9，DNS 透過 RADIUS 協議得到的 IP:IMSI:IMEI:Cell ID:SST 資訊，自動產生 A/AAAA Record。

資料來源：本計畫製作

如圖 4-30，從 Dashboard 確認 4 臺 IoT 設備在 Cell_2 的位置：

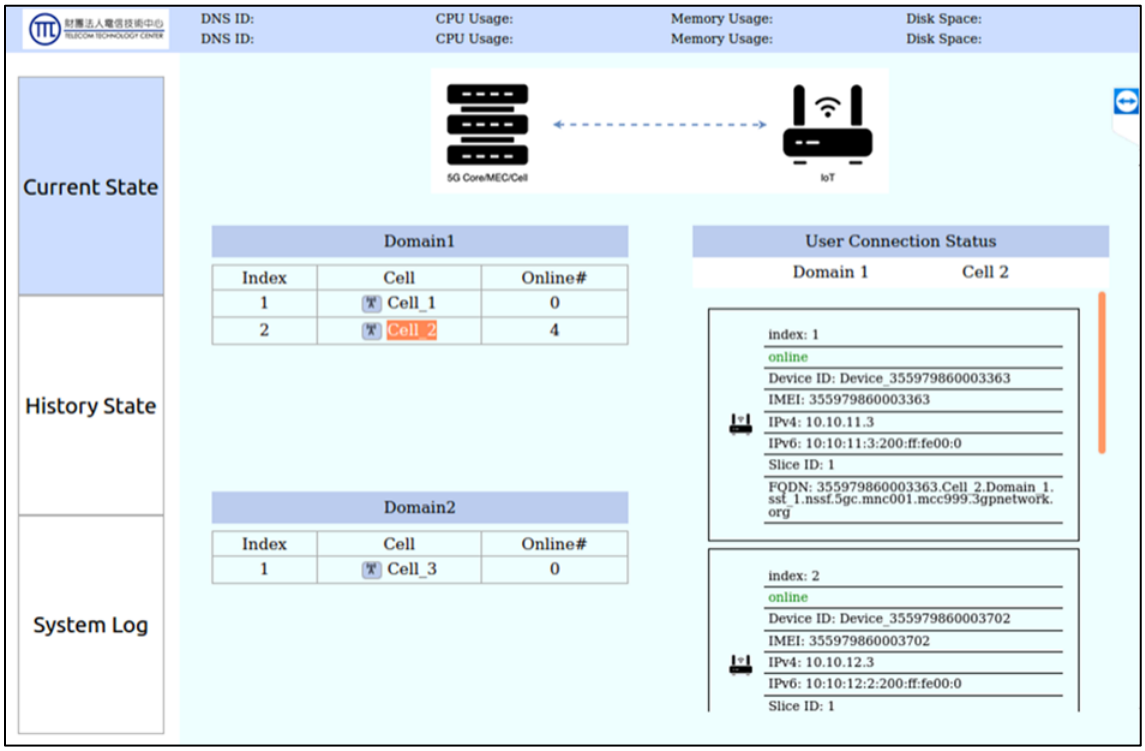


圖 4- 30、IoT 設備跨域移動測試前之 Dashboard 畫面

資料來源：本計畫製作

如圖 4-31，經過跨域移動測試後，4 臺 IoT 設備從 Cell_2 移動至 Cell_3 的位置：

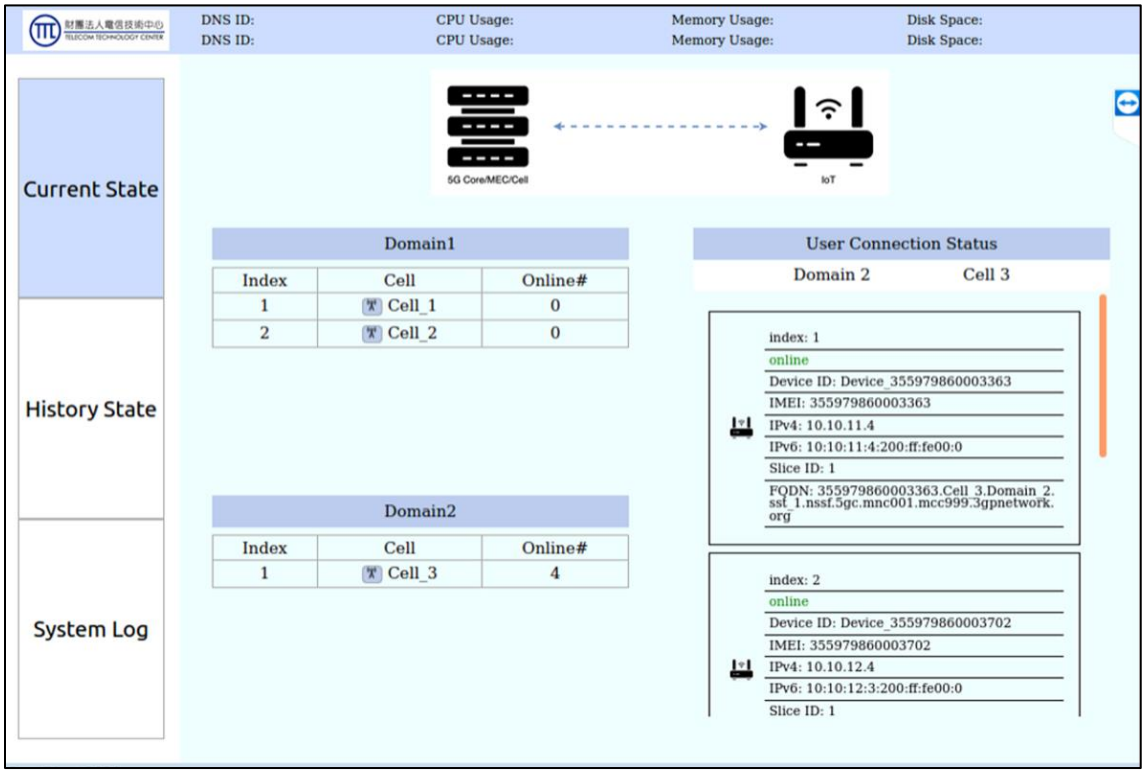


圖 4- 31、IoT 設備跨域移動測試後之 Dashboard 畫面

資料來源：本計畫製作

從 Dashboard 下載資料中截取 IoT 設備跨域移動測試後自動編碼產生 FQDN 之 System Log 如表 4-22：

表 4- 22、IoT 設備跨域移動測試後之 Dashboard System Log

Datetime	Payload	Type
2021/11/1 14:14	Device_355979860003363 is detached from Cell_2	INFO
2021/11/1 14:14	Device_355979860003702 is detached from Cell_2	INFO
2021/11/1 14:14	Device_355979860003728 is detached from Cell_2	INFO
2021/11/1 14:14	Device_355979860003785 is detached from Cell_2	INFO
2021/11/1 14:19	Device_355979860003702 is attached on Cell_3 with FQDN 355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 14:19	Device_355979860003363 is attached on Cell_3 with FQDN 355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 14:19	Device_355979860003728 is attached on Cell_3 with FQDN 355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 14:19	Device_355979860003785 is attached on Cell_3 with FQDN 355979860003785.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO

資料來源：本計畫製作

3. 大量物聯網裝置測試

完成 IoT 終端設備在不同 Cell 之間移動進行自動註冊後，繼續讓 IoT 終端設備在不同 Cell 之間持續移動，觀察 log 變化情形，另外採用程式模擬方式產生大量靜態物聯網裝置，檢視其支援大量設備自動註冊的能力。

(1) 測試項目一

產生大量設備的 RADIUS 資料，傳送到 DNS Server，驗證系統具備大量設備自動編碼能力，測試項目如表 4-23，註冊流程如圖 4-32。

表 4- 23、大量 IoT 終端設備測試項目一

項次	測試內容	預期結果
1	模擬程式產生大量物聯網裝置資料	可從 Dashboard 顯示物聯網裝置數量以及展示物聯網裝置資訊
2	DNS 編碼核配與管理	DNS 可以依據 RADIUS 內容自動產出 A/AAAA Record

資料來源：本計畫製作

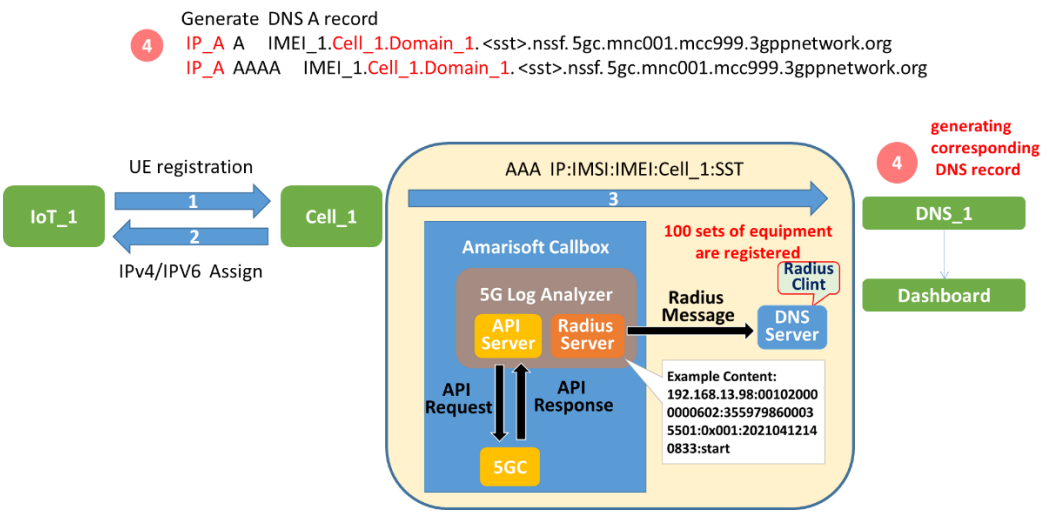


圖 4- 32、大量 IoT 終端設備註冊並產生 RADIUS 資料流程

資料來源：本計畫製作

A. 測試步驟

測試步驟如表 4-24 說明：

表 4- 24、大量物聯網裝置測試項目一之 IP 註冊與 DNS 動態管理

步驟	流程	說明
1	UE 註冊	使用模擬程式產生大量 RADIUS 資料
2	Generate DNS A/AAAA Record	DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record
3	DNS 與 Dashboard 更新資料	Dashboard 取得更新的 DNS A/AAAA Record 資訊

資料來源：本計畫製作

B. IoT 終端設備參數內容

透過自主開發之程式產生 100 臺 IoT 終端設備的 RADIUS 資料，傳送到 DNS Server，IoT 終端設備參數設計如表 4-25：

表 4- 25、IoT 終端設備參數

Name	IP_CAM	Power_ Meter	Temp_Meter	Smart_ Parking	Smart_Lamps
DNN	IP_CAM	Power_Meter	Temp_Meter	Smart_Parking	Smart_Lamps
TAC（IMEI 前 8 碼）	45678123	34567812	23456781	12345678	72345678
NSSAI	eMBB	MIOT			
SST	1	3			
Template	High quality Video	Smart City sensor			
Throughput	100Mbps/100 Mbps	1Mbps/1Mbps			
Zone	nssf.5gc.mnc001.mcc999.3gppnetwork.org				
Service IP IPv4	10.100.11.18	10.100.12.18	10.100.13.18	10.100.14.18	10.100.15.18
Service IP IPv6	10:10:11:18:200:ff:fe00:0	10:10:12:18:200:ff:fe00:0	10:10:13:18:200:ff:fe00:0	10:10:14:18:200:ff:fe00:0	10:10:15:18:200:ff:fe00:0

資料來源：本計畫製作

C. 測試結果

執行完模擬程式之後，100 個 IoT 終端設備自動註冊，可從 Dashboard 顯示在 Cell_1 有 29 個上線設備，Cell_2 有 31 個上線設備，Cell_3 有 40 個上線設備，並可檢視每個 IoT 終端設備的資訊。測試結果說明如表 4-26：

表 4- 26、100 臺 IoT 終端設備註冊測試結果

項次	測試內容	預期結果	測試結果
1	模擬程式產生大量物聯網裝置資料	可從 Dashboard 顯示物聯網裝置數量以及展示物聯網裝置資訊	於 Dashboard 上顯示 100 台的 IoT 終端設備資訊
2	DNS 編碼核配與管理	DNS 可以依據 RADIUS 內容自動產出 A/AAAA Record	DNS 自動產出 A/AAAA Record

資料來源：本計畫製作

如圖 4-33、圖 4-34，從 Dashboard 可確認 IoT 終端設備自動註冊後，設備所在位置及 System Log：

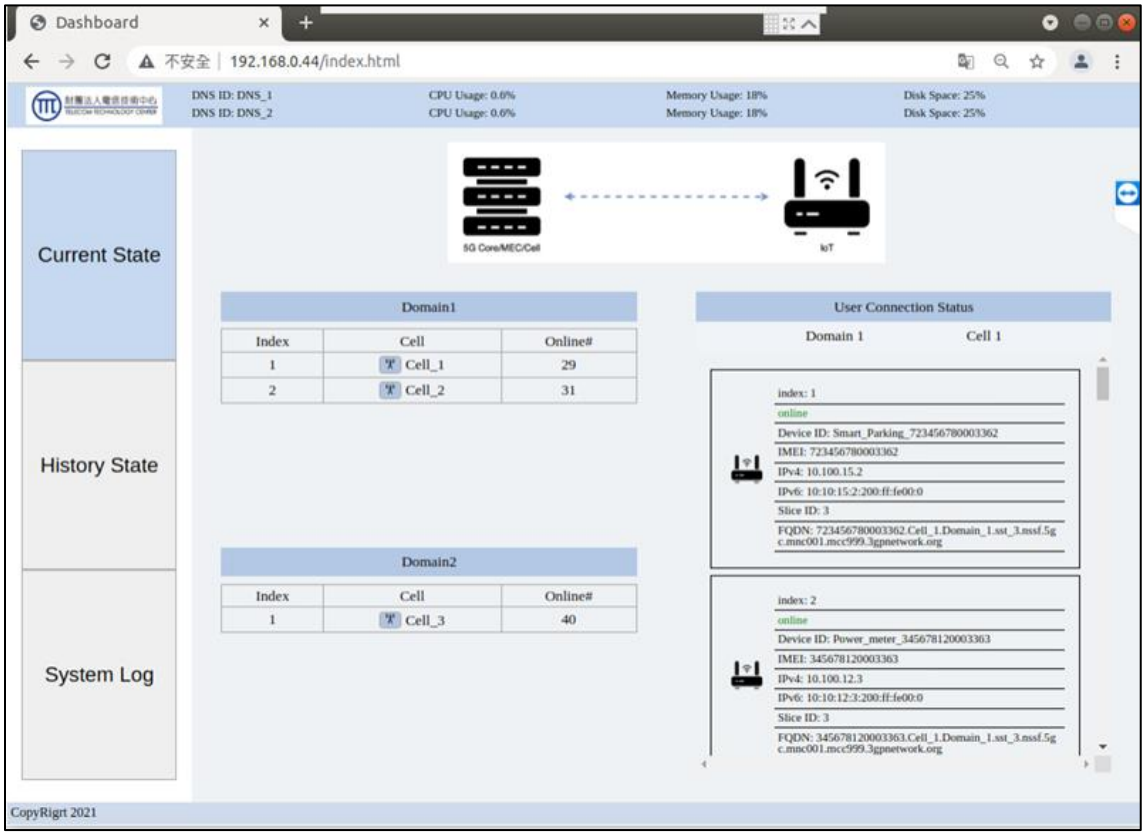


圖 4- 33、100 個 IoT 終端設備自動註冊展示畫面

資料來源：本計畫製作

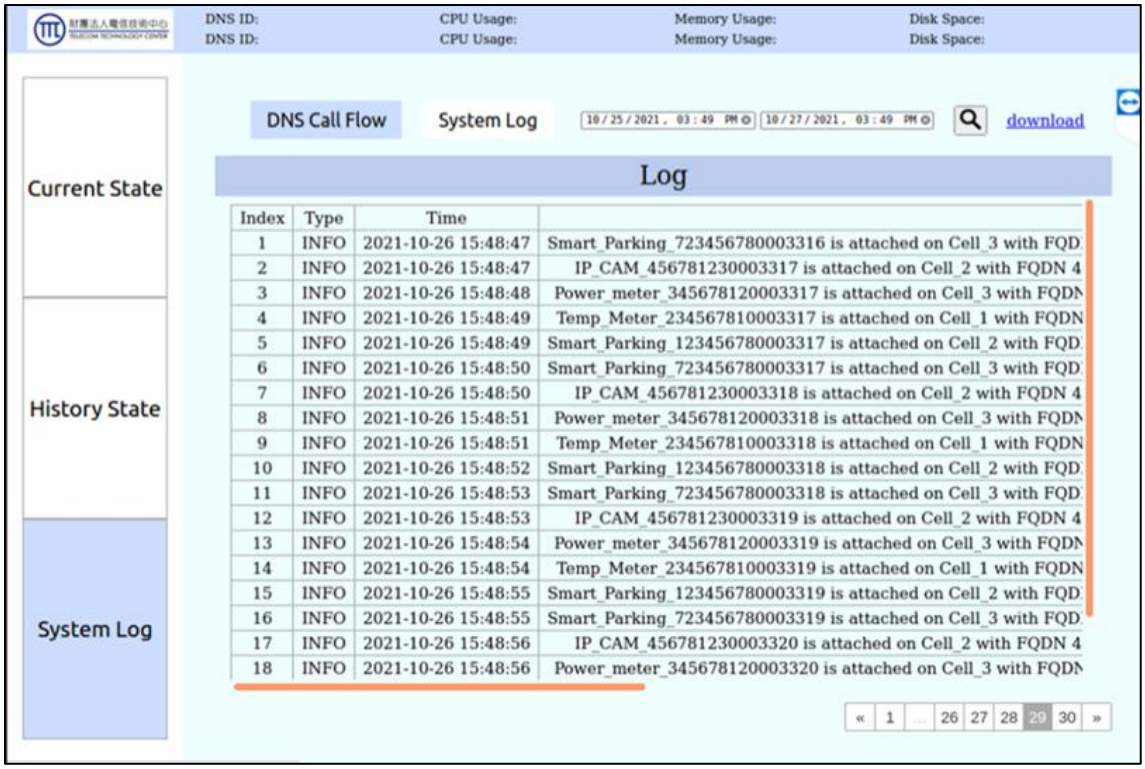


圖 4- 34、100 臺 IoT 自動註冊 System Log

資料來源：本計畫製作

從 Dashboard 下載資料中，節錄 100 臺 IoT 終端設備裝置自動註冊後自動編碼產生 FQDN 之 System Log 如表 4-27：

表 4- 27、100 臺 IoT 終端設備註冊後之 Dashboard System Log

Datetime	Payload	Type
2021/10/26 12:10	IP_CAM_456781230003361 is attached on Cell_3 with FQDN 456781230003361.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Power_meter_345678120003361 is attached on Cell_1 with FQDN 345678120003361.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Temp_Meter_234567810003361 is attached on Cell_2 with FQDN 234567810003361.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Smart_Parking_723456780003361 is attached on Cell_1 with FQDN 723456780003361.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Smart_Parking_123456780003361 is attached on Cell_3 with FQDN 123456780003361.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	IP_CAM_456781230003362 is attached on Cell_3 with FQDN 456781230003362.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Power_meter_345678120003362 is attached on Cell_1 with FQDN 345678120003362.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Temp_Meter_234567810003362 is attached on Cell_2 with FQDN 234567810003362.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Smart_Parking_123456780003362 is attached on Cell_3 with FQDN	INFO

Datetime	Payload	Type
	123456780003362.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	
2021/10/26 12:10	Smart_Parking_723456780003362 is attached on Cell_1 with FQDN 723456780003362.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Power_meter_345678120003363 is attached on Cell_1 with FQDN 345678120003363.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	IP_CAM_456781230003363 is attached on Cell_3 with FQDN 456781230003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Temp_Meter_234567810003363 is attached on Cell_2 with FQDN 234567810003363.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Smart_Parking_123456780003363 is attached on Cell_3 with FQDN 123456780003363.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Smart_Parking_723456780003363 is attached on Cell_1 with FQDN 723456780003363.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	IP_CAM_456781230003364 is attached on Cell_3 with FQDN 456781230003364.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Power_meter_345678120003364 is attached on Cell_1 with FQDN 345678120003364.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Smart_Parking_123456780003364 is attached on Cell_3 with FQDN 123456780003364.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO

Datetime	Payload	Type
2021/10/26 12:10	Temp_Meter_234567810003364 is attached on Cell_2 with FQDN 234567810003364.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Smart_Parking_723456780003364 is attached on Cell_1 with FQDN 723456780003364.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Power_meter_345678120003365 is attached on Cell_1 with FQDN 345678120003365.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	IP_CAM_456781230003365 is attached on Cell_3 with FQDN 456781230003365.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Temp_Meter_234567810003365 is attached on Cell_2 with FQDN 234567810003365.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 12:10	Smart_Parking_123456780003365 is attached on Cell_3 with FQDN 123456780003365.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO

資料來源：本計畫製作

(2) 測試項目二

20 分鐘內，4 臺 IoT 終端設備在不同 Cell 與 Domain 間移動，log 須呈現移動後之變化，測試項目如表 4-28，移動流程如圖 4-35。

表 4- 28、大量 IoT 終端設備測試項目二

項次	測試內容	預期結果
1	物聯網裝置於 20 分鐘內移動	可從 System Log 中檢視物聯網裝置移動軌跡
2	DNS 編碼核配與管理	DNS 可以依據移動軌跡自動產出 A/AAAA Record

資料來源：本計畫製作

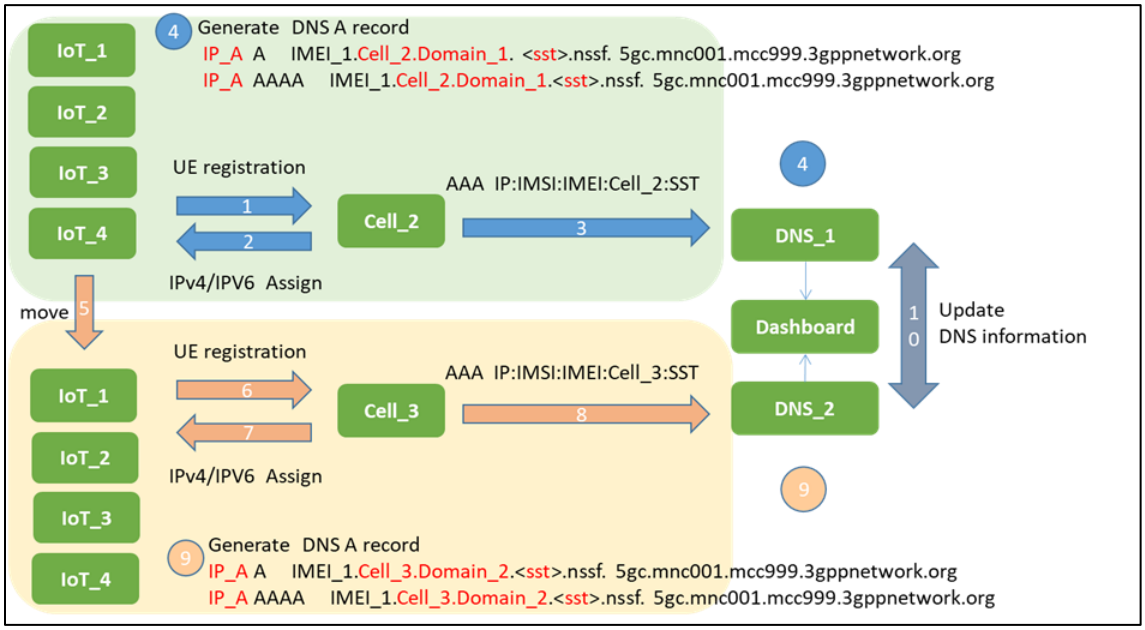


圖 4- 35、大量 IoT 終端設備跨域移動之 IP 註冊與 DNS 動態管理流程

資料來源：本計畫製作

A. 測試步驟

測試步驟如表 4-29 說明：

表 4- 29、大量 IoT 終端設備測試項目二之 IP 註冊與 DNS 動態管理

步驟	流程	說明
1	UE 持續移動	IoT 在 Cell_1、Cell_2 與 Cell_3 之間移動
2	Generate DNS A/AAAA Record	DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record
3	DNS 與 Dashboard 更新資料	Dashboard 取得更新的 DNS A/AAAA Record 資訊

資料來源：本計畫製作

B. 測試結果

測試後，可從 Dashboard 的 System Log 中檢視 4 個 IoT 終端設備持續移動之軌跡，彙整持續移動測試之預期結果及測試後結果對照說明如表 4-30，System Log 如圖 4-36。

表 4- 30、IoT 終端設備持續移動之測試結果

項次	測試內容	預期結果	測試結果
1	物聯網裝置於 20 分鐘內移動	可從 System Log 中檢視物聯網裝置移動軌跡	從 Dashboard 的 System Log 中可以展示連網裝置移動軌跡
2	DNS 編碼核配與管理	DNS 可以依據移動軌跡自動產出 A/AAAA Record	DNS 自動產出 A /AAAA Record

資料來源：本計畫製作

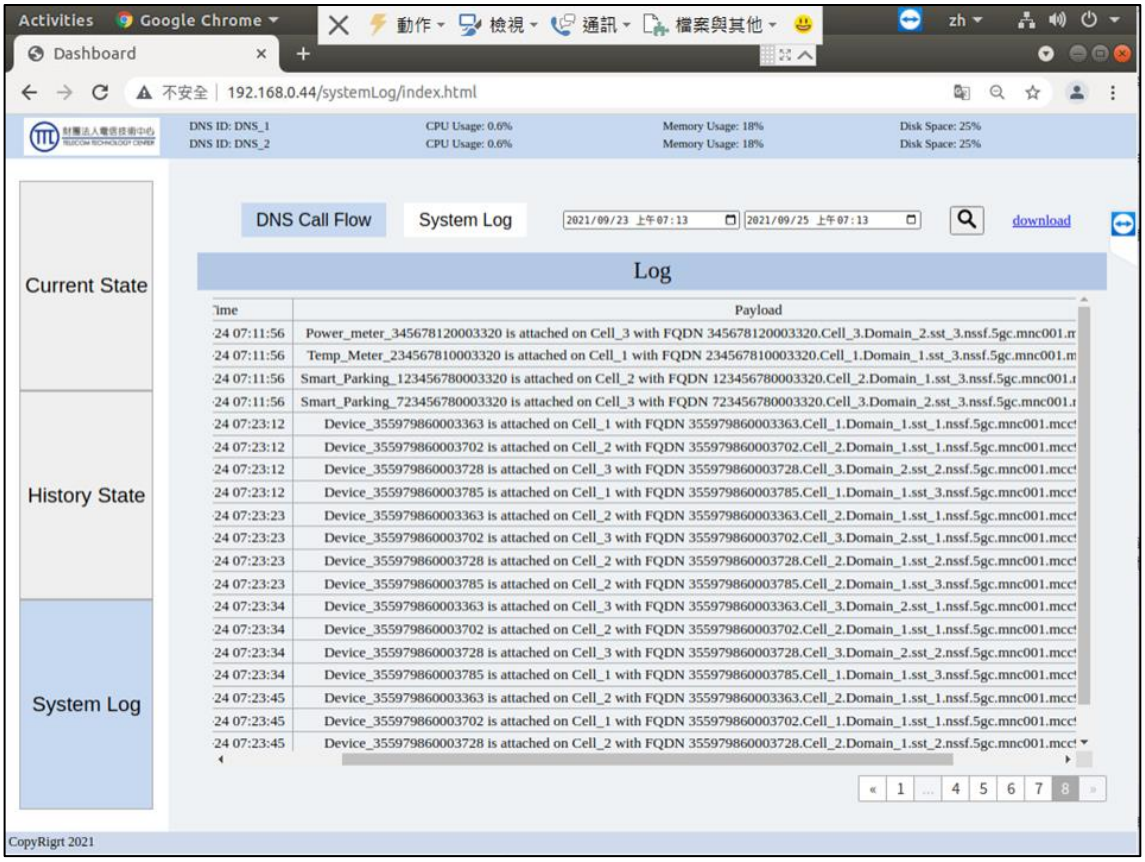


圖 4- 36、IoT 終端設備持續移動 Dashboard System Log

資料來源：本計畫製作

從 Dashboard 下載資料中，節錄 IoT 終端設備持續移動後自動編碼產生 FQDN 之 System Log 如表 4-31：

表 4- 31、IoT 終端設備持續移動之 Dashboard System Log

Datetime	Payload	Type
2021/10/26 16:20	Device_355979860003702 is attached on Cell_1 with FQDN 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:20	Device_355979860003363 is attached on Cell_1 with FQDN 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:20	Device_355979860003728 is attached on Cell_1 with FQDN 355979860003728.Cell_1.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:20	Device_355979860003363 is detached from Cell_1	INFO
2021/10/26 16:20	Device_355979860003702 is detached from Cell_1	INFO
2021/10/26 16:20	Device_355979860003728 is detached from Cell_1	INFO
2021/10/26 16:24	Device_355979860003363 is attached on Cell_1 with FQDN 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:24	Device_355979860003702 is attached on Cell_1 with FQDN 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:24	Device_355979860003728 is attached on Cell_1 with FQDN 355979860003728.Cell_1.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:25	Device_355979860003785 is attached on Cell_1 with FQDN 355979860003785.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO

Datetime	Payload	Type
2021/10/26 16:26	Device_355979860003363 is attached on Cell_2 with FQDN 355979860003363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:26	Device_355979860003785 is attached on Cell_2 with FQDN 355979860003785.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:26	Device_355979860003728 is attached on Cell_2 with FQDN 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:26	Device_355979860003702 is attached on Cell_2 with FQDN 355979860003702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:27	Device_355979860003363 is detached from Cell_2	INFO
2021/10/26 16:30	Device_355979860003702 is detached from Cell_2	INFO
2021/10/26 16:30	Device_355979860003728 is detached from Cell_2	INFO
2021/10/26 16:30	Device_355979860003785 is detached from Cell_2	INFO
2021/10/26 16:31	Device_355979860003363 is attached on Cell_3 with FQDN 355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:31	Device_355979860003702 is attached on Cell_3 with FQDN 355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:31	Device_355979860003728 is attached on Cell_3 with FQDN 355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:31	Device_355979860003785 is attached on Cell_3 with FQDN	INFO

Datetime	Payload	Type
	355979860003785.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	
2021/10/26 16:32	Device_355979860003363 is detached from Cell_3	INFO
2021/10/26 16:32	Device_355979860003728 is detached from Cell_3	INFO
2021/10/26 16:32	Device_355979860003785 is detached from Cell_3	INFO
2021/10/26 16:32	Device_355979860003702 is detached from Cell_3	INFO
2021/10/26 16:34	Device_355979860003363 is attached on Cell_1 with FQDN 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:35	Device_355979860003702 is attached on Cell_1 with FQDN 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:35	Device_355979860003728 is attached on Cell_1 with FQDN 355979860003728.Cell_1.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:36	Device_355979860003785 is attached on Cell_1 with FQDN 355979860003785.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:37	Device_355979860003363 is detached from Cell_1	INFO
2021/10/26 16:37	Device_355979860003702 is detached from Cell_1	INFO
2021/10/26 16:37	Device_355979860003785 is detached from Cell_1	INFO
2021/10/26 16:37	Device_355979860003728 is detached from Cell_1	INFO
2021/10/26 16:40	Device_355979860003363 is attached on Cell_3 with FQDN 355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO

Datetime	Payload	Type
2021/10/26 16:40	Device_355979860003728 is attached on Cell_3 with FQDN 355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:40	Device_355979860003702 is attached on Cell_3 with FQDN 355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:40	Device_355979860003785 is attached on Cell_3 with FQDN 355979860003785.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:42	Device_355979860003702 is detached from Cell_3	INFO
2021/10/26 16:42	Device_355979860003728 is detached from Cell_3	INFO
2021/10/26 16:42	Device_355979860003363 is detached from Cell_3	INFO
2021/10/26 16:42	Device_355979860003785 is detached from Cell_3	INFO
2021/10/26 16:43	Device_355979860003363 is attached on Cell_2 with FQDN 355979860003363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:43	Device_355979860003702 is attached on Cell_2 with FQDN 355979860003702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:43	Device_355979860003728 is attached on Cell_2 with FQDN 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/10/26 16:44	Device_355979860003785 is attached on Cell_2 with FQDN 355979860003785.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO

資料來源：本計畫製作

(二) 情境二

IoT 環境中，如智慧工廠之無人搬運車（Automated Guided Vehicle, AGV）或機器人，IoT 設備可安裝 5G SIM 卡或是安裝 5G Dongle 連上 5G 網路。

在情境二中，採用 MXE-211-M2G 設備安裝 5G Dongle 作為 1 組 IoT 終端設備，編號為 IoT_5，測試 IoT 設備安裝 5G Dongle 連網之情形，此外，亦採用 MXE-211-M2G 設備與 DTA1164W 5G SA/NSA Gateway 組成 3 組 IoT 終端設備，以測試 DNS 編碼機制具有同時因應兩種不同連網方式之能力，場域中共有 4 組 IoT 終端設備，依序為 IoT_1、IoT_2、IoT_3、IoT_5。

1. 同域測試

當 IoT 設備與 5G Dongle 從 Cell_1 移動到 Cell_2，觀察 IP 與域名變化。同域測試內容及預期結果如表 4-32，IP 註冊與 DNS 動態管理流程及說明如圖 4-37 所示。

表 4- 32、同域測試

項次	測試內容	預期結果
1	5G 模擬器及 DNS 間的編碼核配與管理	5G 模擬器可以透過 Raius 協議將 IP:IMSI:IMEI:Cell ID 資訊傳給 DNS
2	Device 取得 IP（IPv4/IPv6）與 DNS mapping	5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致
3	DNS 編碼核配與管理	DNS 可以依據 5G 模擬器產生 RADIUS 內容自動產出 A/AAAA Record
4	多個 Device 註冊 DNS 與核配編碼	比對各 5G 模擬器及 DNS：Device IP、IMSI、IMEI 及 Cell ID 結果一致

資料來源：本計畫製作

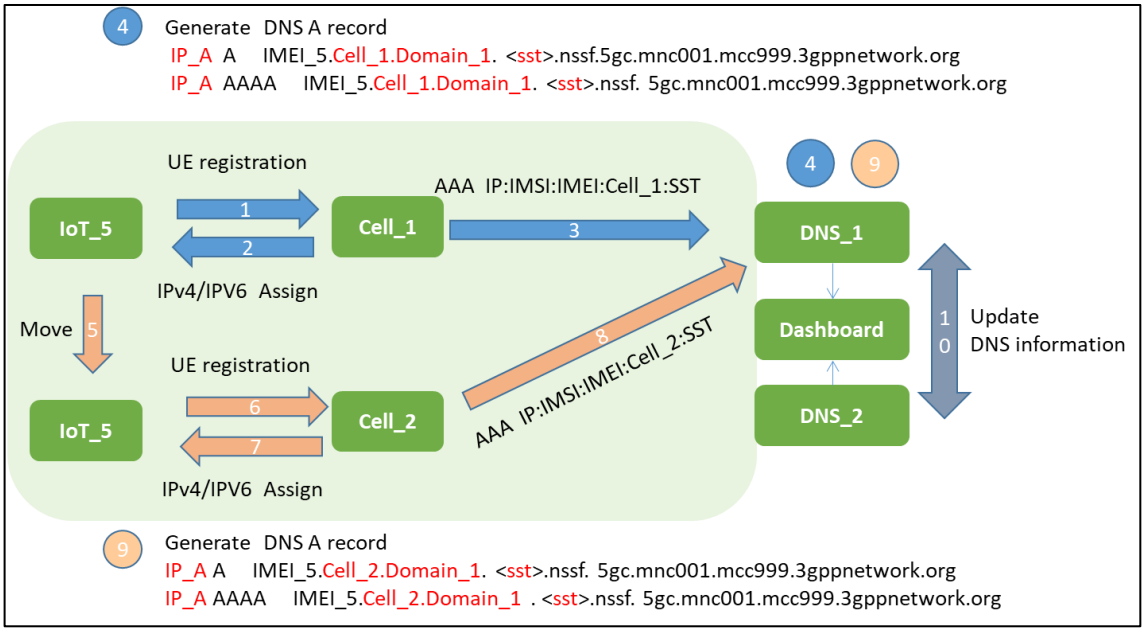


圖 4- 37、同域移動之 IP 註冊與 DNS 動態管理流程

資料來源：本計畫製作

(1) 測試步驟

同域測試步驟如表 4-33 說明：

表 4- 33、同域移動之 IP 註冊與 DNS 動態管理流程

步驟	流程	說明
1	UE 註冊	IoT 連線到 Cell_1，並進行註冊
2	配發 IPv4/IPV6 位址	5G 模擬器配發 IP 給 IoT
3	傳送註冊資訊至 DNS	傳送[IP:IMSI:IMEI:Cell_1:SST]等資訊至 DNS
4	Generate DNS A/AAAA Record	DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record
5	UE 移動	IoT 從 Cell_1 移動至 Cell_2，同為 Domain_1
6	UE registration	IoT 連線到 Cell_2，並進行註冊
7	配發 IPv4/IPV6 位址	5G 模擬器配發 IP 給 IoT，因為是同一 Domain，使用原來的 IP
8	傳送註冊資訊至 DNS	5G 模擬器傳送 [IP:IMSI:IMEI:Cell_2:SST]等資訊至 DNS
9	Generate DNS A/AAAA Record	DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record
10	DNS 與 Dashboard 更新資料	Dashboard 取得更新的 DNS A/AAAA Record 資訊

資料來源：本計畫製作

(2) 同域移動設備參數內容

完成步驟 1 到步驟 4 後進入系統檢視 IoT 終端設備參數異動，如圖 4-38 所示：

		IoT_1	IoT_2	IoT_3	IoT_5
	DNN	internet1	internet2	internet3	internet5
	IMEI	355979860003363	355979860003702	355979860003728	359047100170495
	NSSAI	eMBB	eMBB	URLLC	MIOT
	SST	1	1	2	3
	Template	AR/VR 8K Videos	AR/VR 8K Videos	Factory Automatic Machines	Smart City Sensors
	Throughput	1Gbps/1Gbps	1Gbps/1Gbps	500Mbps/500Mbps	1Mbps/1Mbps
步驟 1,2	Service IP IPv4 (DHCP)	10.10.11.8	10.10.12.6	10.10.13.6	10.10.11.7
步驟 1,2	Service IP IPv6 (DHCP)	10:10:11:8:200:ff:fe00:0	10:10:12:4:200:ff:fe00:0	10:10:13:4:200:ff:fe00:0	10:10:11:7:200:ff:fe00:0
步驟 3,4	DN	355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org	359047100170495.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org

圖 4- 38、IoT 終端設備註冊 IP 以及自動註冊 DN 後之參數

資料來源：本計畫製作

IoT 在同域的不同 Cell 移動時（步驟 5），DNN 與 IP 不更換，DN 會更改 Cell 名稱。完成步驟 6 到步驟 10 後進入系統檢視 IoT 終端設備參數之異動情形，如圖 4-39 所示：

		IoT_1	IoT_2	IoT_3	IoT_5
	DNN	internet1	internet2	internet3	internet5
	IMEI	355979860003363	355979860003702	355979860003728	359047100170495
	NSSAI	eMBB	eMBB	URLLC	MIOT
	SST	1	1	2	3
	Template	AR/VR 8K Videos	AR/VR 8K Videos	Factory Automatic Machines	Smart City Sensors
	Throughput	1Gbps/1Gbps	1Gbps/1Gbps	500Mbps/500Mbps	1Mbps/1Mbps
步驟 6,7	Service IP IPv4 (DHCP)	10.10.11.8	10.10.12.6	10.10.13.6	10.10.11.7
	Service IP IPv6 (DHCP)	10:10:11:8:200:ff:fe00:0	10:10:12:4:200:ff:fe00:0	10:10:13:4:200:ff:fe00:0	10:10:11:7:200:ff:fe00:0
步驟 8-10	DN	355979860003363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org	359047100170495.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org

圖 4- 39、IoT 終端設備在同域的不同 Cell 移動後之參數

資料來源：本計畫製作

(3) 同域測試結果

彙整同域測試之預期結果及測試後結果對照說明如表 4-34。

表 4- 34、同域移動測試結果

項次	測試內容	預期結果	測試結果
1	5G 模擬器及 DNS 間的編碼核配與管理	5G 模擬器可以透過 RADIUS 協議將 IP:IMSI: IMEI:Cell ID 資訊傳給 DNS	於步驟 3 以及 9，5G 模擬器會透過 RADIUS 協議將 IP:IMSI:IMEI:Cell ID:SST 資訊傳給 DNS。
2	Device 取得 IP (IPv4/IPv6) 與 DNS mapping	5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致	IoT 終端設備於步驟 1、2 以及步驟 5、6、7 完成註冊後，自動取得 IP 位置。 檢視 5G 模擬器與 DNS 系統上所看到的 IP 資訊一致。
3	DNS 編碼核配與管理	DNS 可以依據 5G 模擬器產生 RADIUS 內容自動產出 A/AAAA Record	於步驟 4、9，DNS 透過 RADIUS 協議得到的 IP:IMSI:IMEI:Cell ID:SST 資訊，自動產生 A/AAAA Record。
4	多個 Device 註冊 DNS 與核配編碼	比對各 5G 模擬器及 DNS：Device IP、IMSI、IMEI 及 Cell ID 結果一致	於 Dashboard 檢視各 IoT 終端設備的 IP、IMSI、IMEI 及 Cell ID 的資訊，與 5G 模擬器傳送的資料一致。

資料來源：本計畫製作

如圖 4-40，從 Dashboard 可確認，4 臺 IoT 終端設備註冊後在 Cell_1 的位置，其中使用 5G Dongle 之 IoT 終端設備之 IMEI 為 359047100170495：

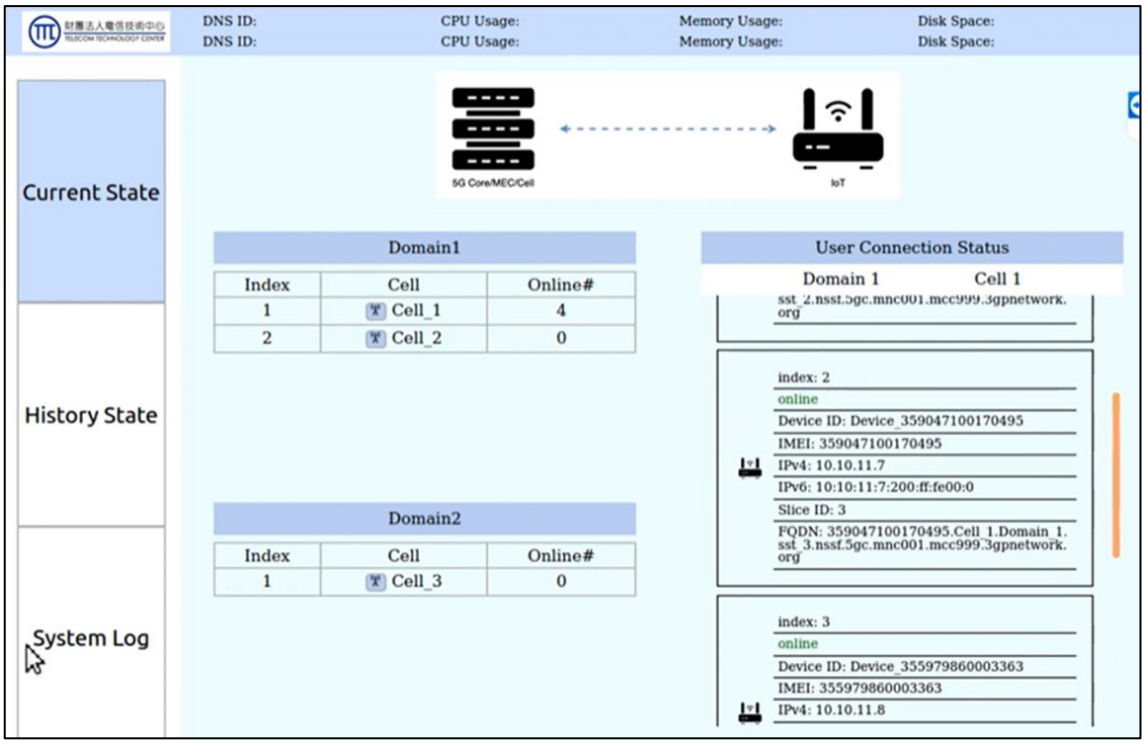


圖 4- 40、IoT 終端設備同域移動之 Dashboard 畫面

資料來源：本計畫製作

如圖 4-41，在同域內，4 臺 IoT 終端設備移動至 Cell_2 的位置：

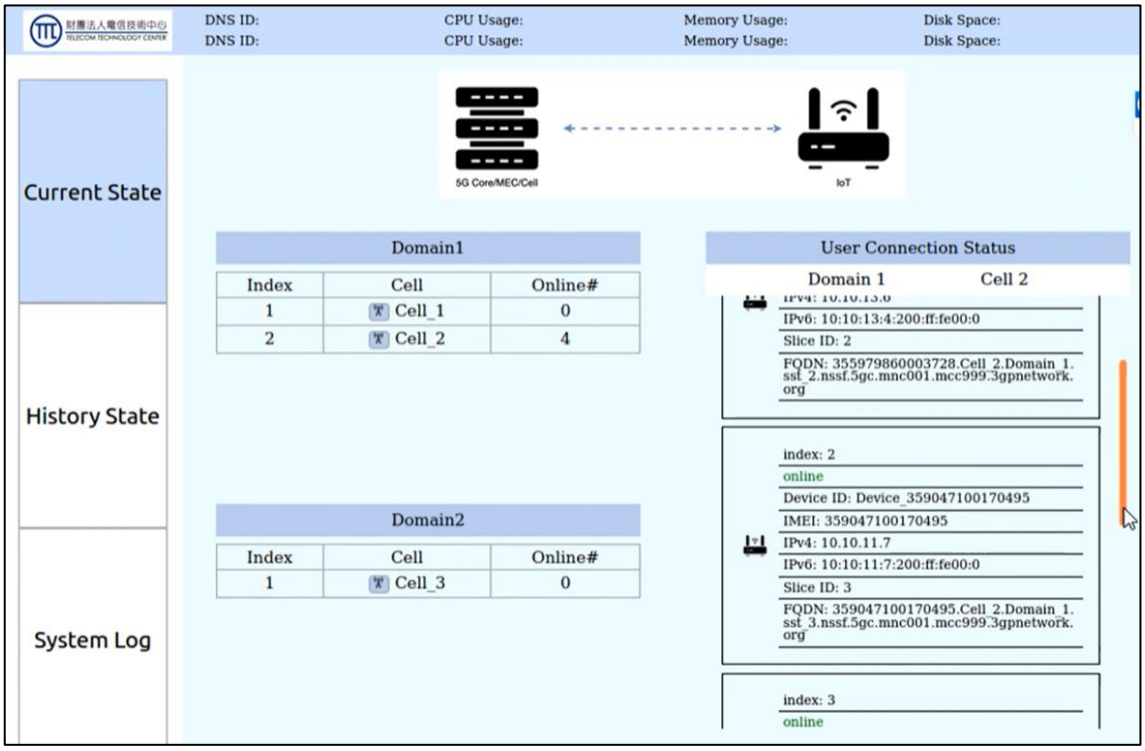


圖 4- 41、IoT 終端設備同域移動之 Dashboard 畫面

資料來源：本計畫製作

從 Dashboard 下載資料中截取 IoT 終端設備註冊後自動編碼產生 FQDN 之 System Log 如表 4-35。

表 4- 35、IoT 終端設備註冊後之 Dashboard System Log

Datetime	Payload	Type
2021/11/1 14:50	Device_359047100170495 is attached on Cell_1 with FQDN 359047100170495.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 14:53	Device_355979860003728 is attached on Cell_1 with FQDN 355979860003728.Cell_1.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 14:53	Device_355979860003702 is attached on Cell_1 with FQDN 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 14:53	Device_355979860003363 is attached on Cell_1 with FQDN 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 15:01	Device_359047100170495 is attached on Cell_2 with FQDN 359047100170495.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 15:01	Device_355979860003363 is attached on Cell_2 with FQDN 355979860003363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 15:01	Device_355979860003728 is attached on Cell_2 with FQDN 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 15:01	Device_355979860003702 is attached on Cell_2 with FQDN 355979860003702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO

資料來源：本計畫製作

2. 跨域測試

當 IoT 終端設備從 Cell_1 移動到 Cell_3，觀察 IP 與域名變化，跨域測試內容及預期結果如表 4-36，其 IP 註冊與 DNS 動態管理流程如圖 4-42：

表 4- 36、跨域測試

項次	測試內容	預期結果
1	5G 模擬器及 DNS 間的編碼核配與管理	5G 模擬器可以透過 Raius 協議將 IP:IMSI:IMEI:Cell ID 資訊傳給 DNS
2	跨網域 Device 取得 IP（IPv4/IPv6）與 DNS mapping	5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致
3	跨網域 Device 的 DNS 編碼核配與管理	DNS 可以依據 5G 模擬器產生 RADIUS 內容自動產出 A/AAAA Record

資料來源：本計畫製作

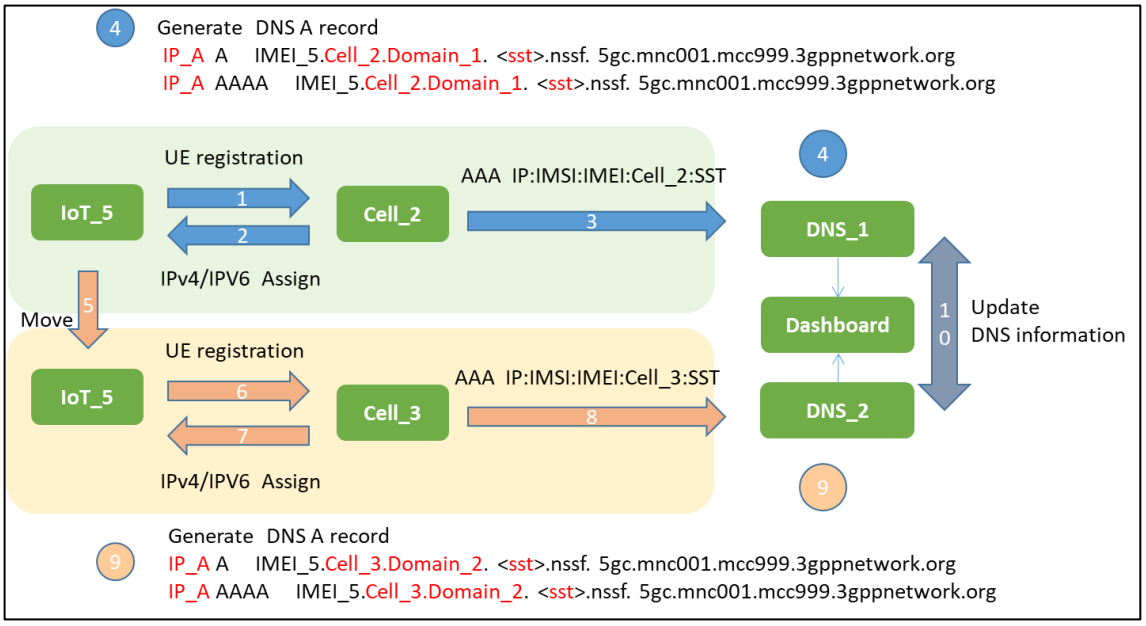


圖 4- 42、跨域移動之 IP 註冊與 DNS 動態管理流程

資料來源：本計畫製作

3. 測試步驟

跨域測試步驟如表 4-37 說明：

表 4- 37、跨域移動之 IP 註冊與 DNS 動態管理流程

步驟	流程	說明
1	UE 註冊	IoT 連線到 Cell_2，並進行註冊
2	配發 IPv4/IPV6 位址	5G 模擬器配發 IP 給 IoT
3	傳送註冊資訊至 DNS	5G 模擬器傳送 [IP:IMSI:IMEI:Cell_1:SST]等資訊至 DNS
4	Generate DNS A/AAAA Record	DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record
5	UE 移動	IoT 從 Cell_2 移動至 Cell_3，從 Domain_1 移動至 Domain_2
6	UE registration	IoT 連線到 Cell_3，並進行註冊
7	配發 IPv4/IPV6 位址	5G 模擬器配發 IP 給 IoT
8	傳送註冊資訊至 DNS	5G 模擬器傳送 [IP:IMSI:IMEI:Cell_3:SST]等資訊至 DNS
9	Generate DNS A/AAAA Record	DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record
10	DNS 與 Dashboard 更新資料	Dashboard 取得更新的 DNS A/AAAA Record 資訊

資料來源：本計畫製作

(1) 跨域移動設備參數內容

步驟 1 到步驟 4 之註冊流程與同域測試相同，相關參數請參考圖 4-38。當 IoT 終端設備跨域移動時（步驟 5），DNN 不變，註冊時將得到新的 IP，同時也會更改 DN 的 Cell 與 Domain 名稱，完成步驟 6 到步驟 10 後進入系統檢視 IoT 終端設備參數之異動情形，如圖 4-43 所示：

		IoT_1	IoT_2	IoT_3	IoT_5
	DNN	internet1	internet2	internet3	internet5
	IMEI	355979860003363	355979860003702	355979860003728	359047100170495
	NSSAI	eMBB	eMBB	URLLC	MIOT
	SST	1	1	2	3
	Template	AR/VR 8K Videos	AR/VR 8K Videos	Factory Automatic Machines	Smart City Sensors
	Throughput	1Gbps/1Gbps	1Gbps/1Gbps	500Mbps/500Mbps	1Mbps/1Mbps
步驟 6,7	Service IP IPv4 (DHCP)	10.10.11.10	10.10.12.7	10.10.13.7	10.10.11.9
	Service IP IPv6 (DHCP)	10:10:11:a:200:ff:fe00:0	10:10:12:5:200:ff:fe00:0	10:10:13:7:200:ff:fe00:0	10:10:11:9:200:ff:fe00:0
步驟 8-10	DN	355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org	355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org	359047100170495.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org

圖 4- 43、IoT 終端設備跨域移動後之參數

資料來源：本計畫製作

(2) 跨域測試結果

彙整跨域測試之預期結果及測試後結果對照說明如表 4-38。

表 4- 38、跨域移動測試結果

項次	測試內容	預期結果	測試結果
1	5G 模擬器及 DNS 間的編碼核配與管理	5G 模擬器可以透過 RADIUS 協議將 IP:IMSI:IMEI:Cell ID 資訊傳給 DNS	於步驟 3 以及 9，5G 模擬器會透過 RADIUS 協議將 IP:IMSI:IMEI:Cell ID:SST 資訊傳給 DNS。
2	Device 取得 IP（IPv4/IPv6）與 DNS mapping	5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致	IoT 終端設備於步驟 1、2 以及步驟 5、6、7 完成註冊後，自動取得 IP 位置。 檢視 5G 模擬器與 DNS 系統上所看到的 IP 資訊一致。
3	DNS 編碼核配與管理	DNS 可以依據 5G 模擬器產生 RADIUS 內容自動產出 A/AAAA Record	於步驟 4、9，DNS 透過 RADIUS 協議得到的 IP:IMSI:IMEI:Cell ID:SST 資訊，自動產生 A/AAAA Record。

資料來源：本計畫製作

如圖 4-44，從 Dashboard 可確認 4 臺 IoT 終端設備在 Cell_2 的位置：

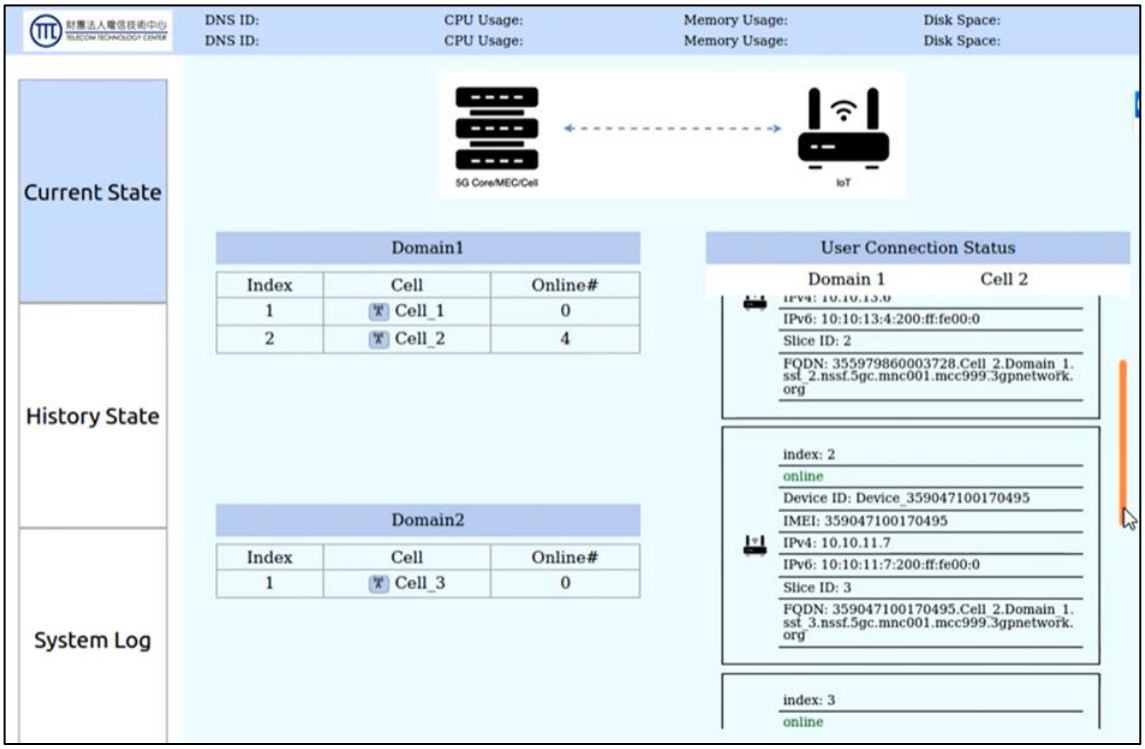


圖 4- 44、IoT 終端設備跨域移動測試前之 Dashboard 畫面

資料來源：本計畫製作

如圖 4-45，經過跨域移動測試後，4 臺 IoT 終端設備移動至 Cell_3 的位置：

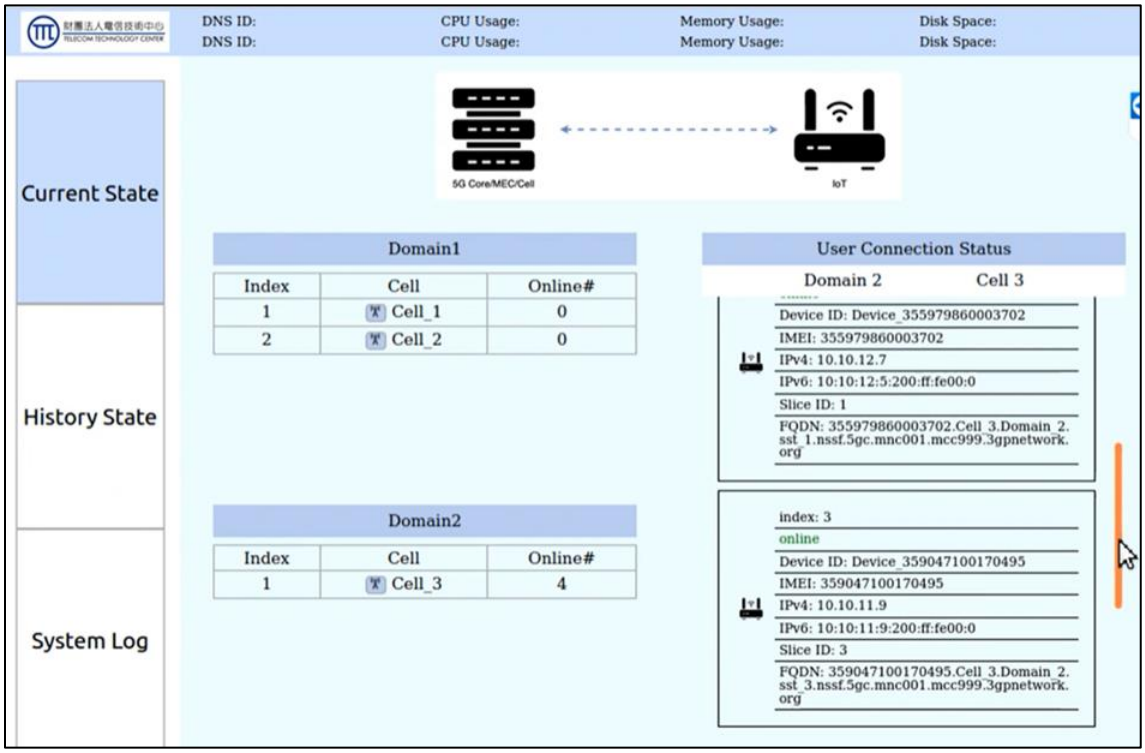


圖 4- 45、IoT 終端設備跨域移動測試後之 Dashboard 畫面

資料來源：本計畫製作

從 Dashboard 下載資料中截取 IoT 終端設備跨域移動測試後自動編碼產生 FQDN 之 System Log 如表 4-39：

表 4- 39、IoT 終端設備跨域移動測試後之 Dashboard System Log

Datetime	Payload	Type
2021/11/1 15:06	Device_355979860003363 is detached from Cell_2	INFO
2021/11/1 15:06	Device_355979860003702 is detached from Cell_2	INFO
2021/11/1 15:06	Device_355979860003728 is detached from Cell_2	INFO
2021/11/1 15:06	Device_359047100170495 is detached from Cell_2	INFO
2021/11/1 15:20	Device_359047100170495 is attached on Cell_3 with FQDN 359047100170495.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 15:22	Device_355979860003363 is attached on Cell_3 with FQDN 355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 15:22	Device_355979860003702 is attached on Cell_3 with FQDN 355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO
2021/11/1 15:22	Device_355979860003728 is attached on Cell_3 with FQDN 355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org	INFO

資料來源：本計畫製作

第四節　小結

我國採用 E.164 以 SIM 卡及門號提供物聯網服務，惟面對大量連結之物聯網裝置，以手動核配裝置門號繁瑣耗時，缺乏對 IoT 設備之識別及定址，亦無法確認 SIM 卡是否被確實用於物聯網服務。為解決 IoT 設備識別與管理問題，研究團隊參考 ICANN 發表之「5G Technology」，

建議以 DN 命名及 IP 轉換解析機制強化對 IoT 設備之辨識性，並透過概念性驗證（Proof of Concept, PoC）檢視 DNS 編碼機制在 IP 化、雲端化的下世代電信網路環境中，是否具備管理大量、多元物聯網服務之能力，得益於網路應用層之開放性及擴增號碼功能，使用 DNS 自動命名及管理系統可滿足大量物聯網裝置編碼需要，並強化管理需求及安全性。

一、驗證成果

本驗證設計物聯網裝置以兩種方式接取 5G 網路，連網方式一係透過 5G Gateway 作為裝置與網路連結之中介，此為物聯網應用廠商常用連網方式之一；另一連網方式係透過 5G Dongle 讓裝置直接接取 5G 網路。包含以下三大項技術程序驗證：

1. 物聯網裝置利用 5G Gateway 接取 5G 網路，並在同域不同基站以及跨域不同基站間移動，驗證編碼系統註冊及自動編碼能力。
2. 物聯網裝置利用 5G Dongle 接取 5G 網路，並在同域不同基站以及跨域不同基站間移動，驗證編碼系統註冊及自動編碼能力。
3. 驗證編碼系統為大量物聯網裝置註冊及自動編碼之能力。

PoC 系統環境以 5G 模擬器（emulator）支援 5G SA 核心網路及 gNB 功能，IoT 設備連線到 5G 核心網路註冊並配發 IP 位址，再透過自主開發之 RADIUS Server 元件，將用戶連網資訊依 RADIUS 協定傳送給本計畫開發之 DNS 編碼程式，DNS 編碼程式收到資料後自動生成 A Record 或 AAAA Record，完成 DNS 自動編碼完整網域名稱（Fully Qualified Domain Name, FQDN）之應用，FQDN 連接 IMEI 及域名以構建物聯網裝置獨一無二的 DNS 編碼。彙整本計畫驗證成果及效益如表 4-40，詳細內容於後文中說明。

表 4- 40、PoC 實測驗證成果彙整表

下世代電信網路號碼技術研析及管理實測驗證	
驗證成果	1. DNS 編碼機制可用於管理固定式 IoT 設備及跨域移動之 IoT 設備編碼，並可依 IPv4 或 IPv6 配發 DNS A Record 或 AAAA Record。 2. DNS 編碼機制及管理平臺可同時為大量 IoT 設備產生相應之 FQDN。 3. 以 DNS 編碼機制管理 IoT 設備，可藉由設備之 IMEI 碼產生唯一識別碼，並可識別設備之廠牌及型號。 4. 以 DNS 編碼機制管理 IoT 設備，可藉由 Cell_ID 及 Domain_ID 資訊，追蹤 IoT 設備之位置。 5. 使用 Dashboard 查詢功能列及 System Log，可快速找到特定 IoT 設備。 6. 使用 Dashboard 查詢功能列及 System Log，可快速查閱連線至特定 Cell 或 Domain 下之 IoT 設備。 7. 可利用 5G 網路切片技術，提供不同應用服務情境。

資料來源：本計畫製作

在 IP 網路架構之上，邊緣運算、網路虛擬化及網路切片等 5G 技術實現增強型移動寬頻（eMBB）、超低延遲可靠通訊（uRLLC）及大 規模機器型通訊（mMTC）三大應用服務，建構「萬物互聯」之榮景，物聯網之管理方式亦在國際間引起關注與討論，目前以 E.164 規管物聯網服務，需解決號碼指配給「物」之後如何識別「物」及如何避免指配給「物」之門號被移作他用之問題。如將 DNS 編碼機制應用於 IoT 設備之管理，將為 IoT 設備提供唯一識別碼，並可透過網路切片功能或結合 5G 設備識別器（5G-Equipment Identity Register, 5G-EIR）功能，當 IoT 設備在 AMF 註冊時，確認 IoT 設備之識別碼，[231]以避免非 IoT 設

[231] ETSI (2018-10) "5G;5G System;Equipment Identity Register Services;Stage 3" (ETSI TS 129 511 V15.1.0,P7

備使用物聯網服務。

現階段我國依 E.164 編碼核配 040 開頭之號碼供物聯網服務設備使用，並限制不得用於語音服務，然目前並無機制可驗證一組 040 號碼是否確實用於物聯網裝置或設備，參考國內各家電信業者物聯網管理介面，其功能包含門號開通服務、流量使用率及月租費資訊，但無法得知 IoT 設備之廠牌型號。DNS 編碼機制透過 IP 對應、自動生成 FQDN，因包含 IMEI，可直接識別 IoT 設備之廠牌型號及其代表之特性，例如：環控監測、照明、無人載具，且因 IMEI 資料係共用 GSMA 之資料庫，不會產生混淆之疑慮，同時 IMEI 屬於去識別化資料，使用 IMEI 統計分析亦不涉及個資問題。

此外，當討論物聯網管理時，連網方式之殊異、通訊結構之質變、異質網路之聚合，亦為須納入考量之重點，得益於 DNS 分層樹狀結構命名方式，可在既有的統一標準上架設新應用。目前我國電信業者在 4G 或 5G 網路均有 PGW/SMF 的 RADIUS 服務，會將用戶連網取得 IP 後之 AAA 資訊，傳送至因應金融監督管理委員會金融科技白皮書所成立之 TWID 身分識別中心，[232]提供多元身分識別、信物管理、電子文件簽署及資料共享等服務，此平臺廣泛應用於關貿署、健保署及國稅局以做手機實名認證。未來電信業者或相關服務供應商只要在 PGW/SMF 多指定一組 IP 傳送至 DNS 做 AAA 認證，不須更改其電信網路架構及設定，可降低建置成本並提高業者使用本機制之接受度。

本計畫經 PoC 實證以 DNS 技術管理及識別 IoT 設備為可行之解決方案。在 5G 專網環境下，例如：企業專網或智慧園區，大量 IoT 設備連網後，無論是固定式或移動式設備，在同域或跨域不同基站間移動，可透過 5G 核心網路進行 UE 認證、配發 IPv4 或 IPv6 位址及分配網路切片服務，並利用部署於邊緣之 DNS 完成設備的自動編碼，並能以 Dashboard 儲存、管理、查詢相關 log 資料。

[232] MobileID Retrieved from https://www.twca.com.tw/product/c0cf07bd-25ab-42d8-a1bd-3e6e71950113 (2021/10/22)

二、驗證結果說明

本計畫參考國際組織 ITU、3GPP、GSMA、ICANN 及 ETSI 等發佈之電信技術，綜整研析下世代電信網路號碼驗證機制，驗證以 DNS 自動編碼的機制與方法，可套用在不同的 IoT 設備情景運用及達成 IoT 設備管理，PoC 實測驗證成果效益說明如下：

1. 利用部署於邊緣之 DNS 降低網路延遲，本計畫之 DNS 及 Dashboard 均部署於基站旁，因 DNS 靠近基站，查詢所需時間短、網路延遲低。
2. DNS 編碼使用 IMEI 及 Cell_ID 資訊提高 IoT 設備管理之可讀性，IMEI 前八碼可識別 IoT 設備，Cell_ID 可確認設備的位置，管理更方便並可延伸連結 MEC 多重接取邊緣運算中 Firewall 的管理、Network slicing 的路由調配及 QoS 設定。
3. 本案 PoC 實測驗證場域連接專網環境下的基站，只有網域管理者知道 Cell_ID 實際地理位置，對於 Cell_ID 資訊隱密層級高。
4. 現行物聯網使用門號 040 管理機制，實務上在用戶申辦門號後，管理者並不清楚是否用於 IoT 設備，以 IMEI 管理可以在用戶使用非 IoT 設備時發出告警，若結合 5G-EIR 功能，UE 註冊時 AMF 會比對 IMEI 是否為黑/白名單）功能，可以設定黑名單阻止用戶使用非 IoT 設備連網。
5. 考量現階段我國使用 040 門號規管 IoT 設備，如將 DNS 編碼應用於管理使用 040 號碼之物聯網裝置，可以用以下格式呈現：

   <040xxxxxxxxxx>.<IMEI>.<Cell_ID>.<Domain_ID>.<sst>.nssf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
6. 管理上可以取代 5G EIR 功能，如果 IMEI 是屬於非 IoT 設備，例如手機或是 5G Gateway，就予以阻擋，如果 IoT 設備不屬於 sst=3 的 MIoT 物聯網切片也予以阻擋。

7. 使用者如果有直接連結 IoT 設備需求，未來物聯網管理平臺實際應用上可以開發將網址轉為 QR cord（Quick Response Code，快速回應圖碼）的功能，使用者只要使用手機掃描便可以直接接入 IoT 設備，不須繁雜手續。
8. 將技術規劃及 PoC 具體成果發表於國際組織（或社群），以強化我國與國際專業人士交流互動，提高國際聲量。

另綜整驗證範圍如下：

(一) 本計畫 PoC 實測驗證平臺之自動編碼適用於專網環境，例如企業私網之內部管理

IoT 設備的自動化編碼管理適用於企業私網及具有網路切片的5G應用環境，考量資安因素，本機制不適用於跨不同企業及不同網路切片間之交互連結。實務上，亦不建議讓外部用戶連結至 IoT 設備以避免造成資安破口，結合本計畫 PoC 實測驗證平臺的 IoT 自動編碼，建議之資訊安全配套措施舉例說明如下：

1. 網際網路的外部用戶需連到 IoT 管理平臺查詢 IoT 設備狀態，透過IoT管理平臺提供IoT設備訊息，而非直接與IoT設備接取訊息。
2. 企業私網及網路切片內部的 IoT 設備，為單向傳送訊息內容，且需於IoT管理平臺集中管理，例如:工廠內的自動化設備只能由中控中心管理。
3. 使用不同網路切片服務的 IoT 設備不交互連結，例如: 車聯網與行車中心的網路連線，例如 OTA（空中下載技術，Over-the-Air）的韌體更新及車輛定位只能由行車中心單向管理；而車聯網 V2X 的自動控制及車輛資料收集由行車系統及邊緣運算完成；用戶車內的連網裝置不與任何車內元件直接產生連結。

(二) Gn DNS 網元隔離的資安需求

IoT 設備連網的網段與 Gn DNS 網段不能相通， 3GPP 規範之 Gn DNS 功能專用於核心網域內的定位、用戶接入網路解析、核心網路元件間認證及網元域名解析工作，與 IoT 設備連至網際網路所產生 DNS 解析為不同網段，IoT 設備無法透過網際網路 DNS 解析 FQDN 進行互相辨識，僅提供管理人員辨識 IoT 設備管理使用。參考 GSMA IR.67 指引，Gn DNS 需與連線至網際網路的 DNS（Gi DNS）分離進行實體隔離，所有 IoT 設備及網際網路連網都無法連線至 Gn DNS，以保證 Gn DNS 安全。

(三) DNS 編碼的隱私安全管理

本計畫 PoC 實測驗證平臺的 IoT 自動編碼格式為：

[IMEI.Cell_ID.Domain_ID.sst.nssf.5gc.mnc01.mcc999.3gppnetwork.org]

IMEI 係具有唯一性的設備識別碼，和 MSISDN 用戶門號與 IMSI 用戶識別碼不同，IMEI 無法直接與用戶個人訊息連結，而 Cell ID 及 Domain 為企業私網或電信業者自訂之欄位及配置，與 IMEI 搭配無法直接識別使用者身分，保障用戶資訊。使用 IMEI 編碼雖方便管理，惟 IMEI 碼與產品名稱對應資料非公開資訊，須向 GSMA 取得授權並購買 IMEI 資料庫，方能取得 IMEI 的產品對應表。此外，本 PoC 實測驗證之 DNS 編碼機制無法辨別 IMEI 之合法性，應規管 IMEI 以避免使用偽造之 IMEI 引發號碼重覆或無法識別裝置，影響管理。

(四) IoT 設備需位於基站涵蓋區並直接與基站進行無線訊號連網

本 PoC 實測場域範圍是依據 3GPP 定義，當 UE 位於基站涵蓋區，進行實證測試。如果 IoT 設備無法以行動網路連網，例如 IoT 設備使用 Wi-Fi 連線至 5G 無線分享器，再透過 5G 無線分享器進行連網，依本計畫編碼原則無法直接識別透過 Wi-Fi 連網之 IoT 設備，但可以透過連結外部 DHCP Proxy 認證設備，讀取裝置的

MAC 碼，MAC 碼如同 IMEI 碼係具唯一性之設備識別碼，可按本計畫編碼原則識別使用 5G Wi-Fi 連網的 IoT 設備。

(五) 不適用於非 IP 的 IoT 間通訊

本案編碼方式係基於 IoT 的 DN 與 IP 對應，不適用於以訊息佇列遙測傳輸（Message Queuing Telemetry Transport, MQTT）之機器對機器（Machine to Machine, M2M）間的通訊連結。在非 IP 層協議上，IoT 設備是否有域名或 IP 不影響 IoT 之間的通訊，其機制與技術不同於以 DN 與 IP 的 DNS 編碼制機基礎。

三、下階段 PoS 規劃

本計畫將延續今年概念驗證（Proof of Concept, PoC）成果規劃服務驗證（Proof of Service，PoS）情境並建置 5G 專網環境下之實測驗證場域(如圖 4-46)，研析以 DNS 編碼機制及管理平臺結合智慧運輸系統（Intelligent Transportation System, ITS）應用之適用性及可行性，以整合 ITS 管理環境。

參考交通部高速公路局有關智慧運輸系統之網頁，我國智慧運輸資料收集系統包含車輛偵測器，天候偵測器、影像事件偵測系統、壅塞回堵偵測、閉路電視攝影機、自動車牌辨識器，將所收集資料具體應用於掌握高速公路路況、預測行車時間及休息站之停車管理等，並可藉由手機 APP 或藍芽推播訊息、資訊發布設施（如：路徑導引標誌及旅行時間標誌）與交控管制設施（如：匝道儀控號誌、天候資訊可變標誌及車道管制號誌）等方式，將資訊即時傳遞予用路人，以增進行車安全、降低交通擁擠及提升運輸效率。[233]

本計畫參考我國現有之 ITS 應用方式，驗證以 DNS 編碼機制整合管理系統，以統一管理智慧交通運輸工具、道路基礎設施及物聯網感測器。在服務情境之設計上，規劃於 5G 專網切片環境下，驗證 DNS 編

[233] 交通部高速公路局智慧運輸系統網站，檢自 https://transport-curation.nat.gov.tw/museum-ITS2020/index.html (2021/11/04)

碼機制部署於智慧交通之基礎設施流量、停車及相關應用 IoT 設備管理服務，為物聯網裝置、感測器配發 IP，並藉由 IP 註冊情形掌握運作情形，於裝置出現異常時發出告警通知，並可透過 FQDN 之 Cell_ID 及 Domain_ID 追蹤移動式 IoT 設備之位置。此外，將評估以網路切片服務將網路資源切分為多個不同虛擬邏輯網路之方式，同時滿足不同 IoT 設備對 5G 增強型移動寬頻（eMBB）、超低延遲可靠通訊（uRLLC）及大規模機器型通訊（mMTC）之不同需求，並能透過 IMEI 直接辨識物聯網物件，以套用不同 QoS 規則。

為改善人、車、路之互動關係，並增進運輸系統之安全及效率，規劃 PoS 應用情境如以下說明：

1. 聯網基礎設施：接收包含道路、交通號誌及路燈資訊，掌握街道活動。
2. 車輛追蹤：連結車輛 IoT 及定位裝置，協助交通管理。
3. 規劃智慧路徑：引導車輛接收即時交通資訊，規劃最佳路徑，緩解壅擠。
4. 停車：識別停車位利用情形，使停車更輕鬆、更高效。

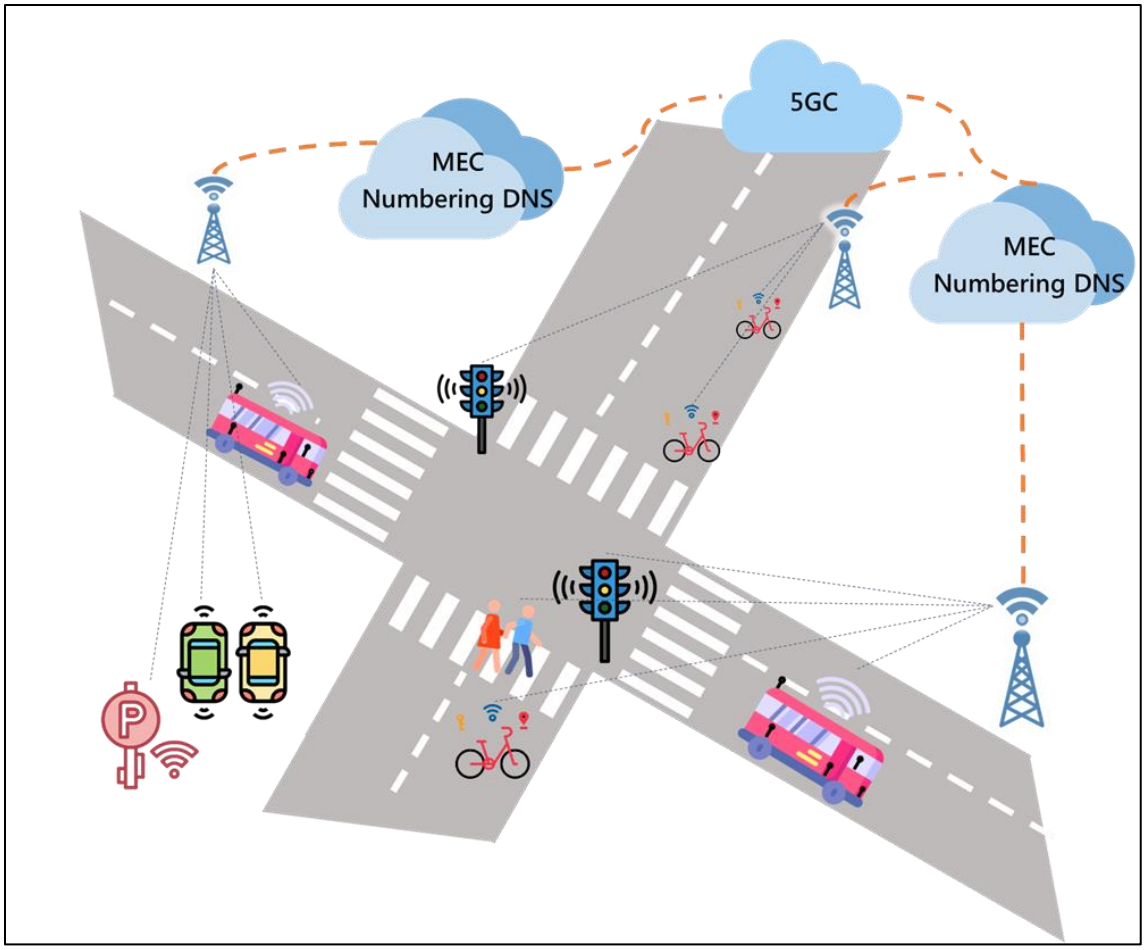


圖 4- 46、PoS 情境規劃

資料來源：本計畫製作

第五章 下世代電信網路號碼人才培育

第一節 計畫背景及目標

隨著第五代行動通訊在全球進入商用階段，各種創新應用服務也將趨動產業升級，而我國行政院也於 2019 年 5 月核定「臺灣 5G 行動計畫」，訂定 5G 發展目標與具體推動措施，並積極培育 5G 跨域人才，藉由推動學界研究 5G 前瞻通訊技術能量外，並鼓勵學界與法人、產業界等共同合作進行研發，發展符合產業需求的技術方案，培育 5G/B5G 技術之頂尖研發人才及 5G 跨域應用人才，以掌握行動通訊技術與標準發展趨勢，並厚植未來學研界與產業發展。

有鑑於此，人才培育結合本計畫電信編碼標準研究，透過觀測國際電信號碼機制發展及各國政策發展趨勢，並評估 5G 切片開發場域平臺系統規格、擬定DNS（Domain Name System）號碼驗證機制，研析過程透過加強與國內單位及國際合作，及實際參與相關國際組織，綜整將國際會議及交流成果挹注到研究分項中，並將會議交流及研究成果分享及擴散至相關產業界，以促進我國 5G IoT 與網路切片相關產業技術與國際接軌，以協助國內產業及早因應及市場布局，進而提升我國相關產業自主研發能力。此外，本計畫透過技術及實證研究成果，與國際組織及社群進行交流，並達成參與相關國際標準制訂工作及可擔任該等組織重要幹部之專業人才之目標。

為達成「培育參與相關國際標準制訂工作及可擔任該等組織重要幹部之專業人才」之目標，本計畫依 4 年期程推動人才培育工作，而今年為人才培育先導期，並依據計畫徵求書之要求盤點國際下世代電信號碼相關會議及活動，研提參與策略及效益；邀請下世代電信號碼相關領域專家學者與本計畫成員共同組成專業團隊，共同參與國際相關會議及活動，並培養 3 位專業人才分別參於會議提交成果報告；另外，辦理下世代電信號碼專家交流會至少 3 場，邀請相關領域專家產學研者參與討論，建立交流平臺溝通及分享專業新知及心得。本計畫目標如下：

1. 國際會議及交流之培育成果
2. 強化技術能量及累積國際組織影響力
3. 人才培育短、中、長期參與策略及效益

第二節　計畫架構及研究流程

本計畫今年度人才培育為先導期，並依據計畫徵求書之要求，首先盤點國際下世代電信號碼相關組織，分析與下世代電信網路號碼相關之組織、社群及其運作模式，接著由本計畫 3 位專家學者及本計畫成員共同參與國際組織會議及活動，並與相關社群交流，提出鎖定參與國際組織之工作小組及議題等。再者，為蓄積下世代電信網路號碼技術能量，計畫團隊透過參與國際會議，將其蒐集相關資訊回饋於本計畫研究中。另外，本計畫辦理經驗分享會，訪談具參與國際標準組織經驗之國內專家學者及辦理國際會議會前諮詢會，以蒐集研提參與策略及效益，綜整提出培育我國具備參與相關國際標準制定工作及可擔任該等組織重要幹部之專家學者短、中、長期參與策略及效益。計畫架構如圖 5-1 所示：

1. 強化國際鏈結：
- 盤點下世代電信號碼相關國際標準組織，分析其組織、社群及運作模式，提出參與國際組織之工作小組及議題等。
- 參與國際組織相關會議及活動，以建立國際交流。
- 參與國際組織社群，以掌握國際下世代電信號碼相關發展趨勢及增進互動與交流。

2. 蓄積技術能量：
- 計畫團隊研析下世代電信號碼機制及各國政策發展、研析下世代電信網路號碼資安相關議題、規劃及建立電信網路號碼驗證機制等，並將研究產出發表至 ICANN 72 會議，以促進國際組織社群討論及關注相關議題之機會。

3. 提升國際參與能量：
- 經驗傳承及分享會：邀請曾參與或擔任國際相關組織幹部之專業人士，進行經驗分享交流，以建立經驗傳承管道，作為

專業團隊學習標竿。

- 座談會：為擴散國際電信號碼新知與發展，專家學者於座談會中，透過與產官學研專業人士直接討論，以建立國內技術與產業互動交流平臺，促進我國技術與產業能量升級，協助國內產業及早思考因應策略並進行市場布局。

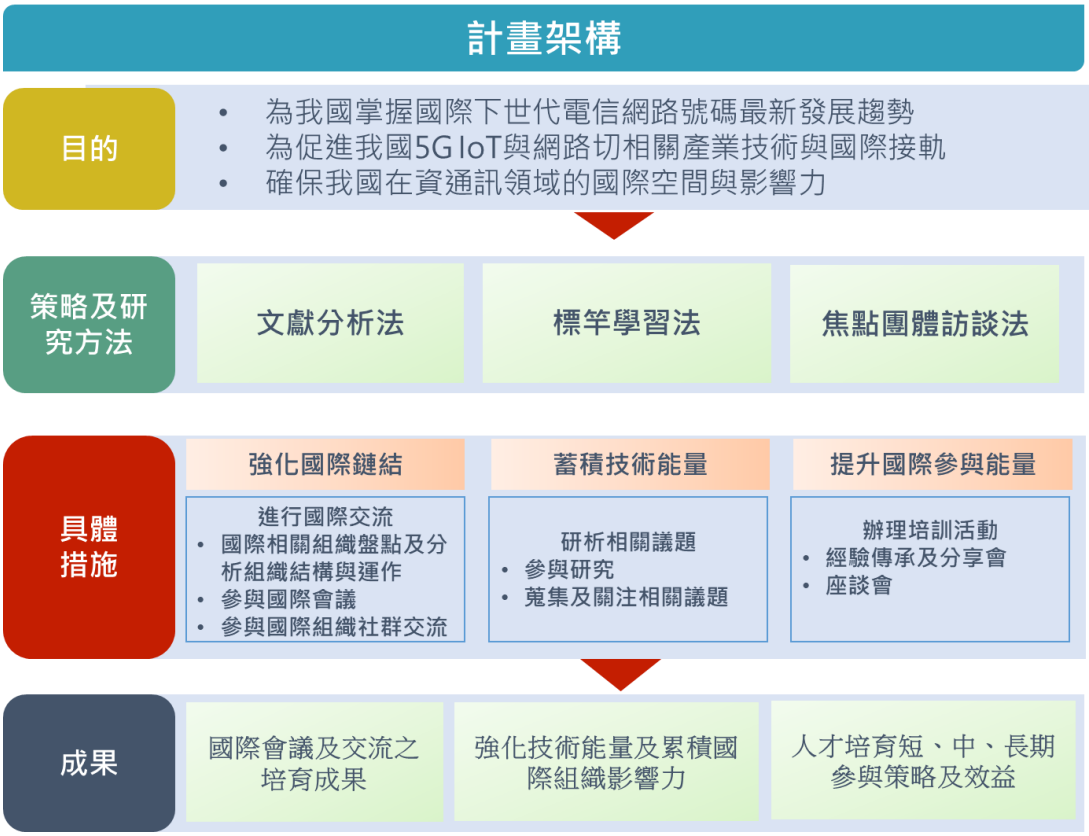


圖 5- 1、計畫架構圖

資料來源：本計畫製作

今年度計畫目標「國際會議及交流之培育成果」、「強化技術能量及累積國際組織影響力」及「人才培育短、中、長期參與策略及效益」，依計畫徵求書之要求擬定策略及研究方法，再串連這些工作項目的成果產出報告，研究方法說明如下：

1. 文獻分析法：文獻分析是指根據研究目的或議題，透過蒐集、分析、歸納與研究有關國際組織運作架構、國際下世代電信

號碼相關技術報告等文獻資料，全面地掌握所要研究問題的一種方法。為了解國際在下世代電信號碼機制及相關組織運作方式，本計畫以文獻分析法，先盤點國際下世代電信號碼相關會議及活動，並分析相關國際組織運作及社群運作討論。另外，透過專家團隊共同參與相關國際組織會議及社群，觀察國際對於下世代電信網路編碼議題趨勢，以強化及推動本計畫於該議題之研究、交流及掌握最新技術發展。

2. 標竿學習法：標竿分析（Benchmark），或稱作基準化分析法，源自企業組織針對欲研究之目標主體，與市場上具代表性/競爭性之事業體之最佳目標主體進行比較分析，從而得出可衡量（measurable）、可評估（evaluable）之基準（值）（standard）或指標（indicator），用以優化目標主體、提升企業組織能力的一種方法。本計畫為培養參與相關國際標準制訂工作及可擔任該等組織重要幹部之專業人才，因此透過標竿學習法，先行邀請曾擔任國際組織幹部及曾經制定過國際標準之專家學者，提供專業團隊規劃及執行方向，作為本計畫今年及未來人才培育參考及學習參考。
3. 焦點團體訪談法：焦點團體訪談法是常用的研究方法，透過主持人帶領下，邀請同質背景的成員，針對特定主題彼此溝通討論、意見交流及腦力激盪後得出建議與觀點。本計畫將安排3場座談會，透過辦理座談會之形式，邀請在產、官、學等不同領域的電信專家學者，蒐集國內各主管機關、電信業者、物聯網業者及專家學者之意見，就下世代電信網路號碼技術及國際發展趨勢，提供國內市場之建議。

透過文獻分析法、標竿學習法及焦點團體訪談法，綜整相關資料及各界之建議，以作「國際會議及交流之培育成果」、「強化技術能量及累積國際組織影響力」、「人才培育短、中、長期參策略及效益」之依據。

第三節　執行內容與成果

一、國際會議及交流之培育成果

本計畫核心架構係以國際5G前瞻技術趨勢、資通訊安全之政策走向，致力於5G網路切片技術之專網編碼系統之開發、建置與概念性測試，並將 DNS 系統與 5G 網路切片技術融合、跨場域編碼互通相關研究彙整成最終成果。計畫目的為透過研究分析及實證，制訂5G物聯網設備之未來管理方案，以協助我國產業因應國際科技發展的趨勢並且超前部署，提升我國相關產業自主研發能力，並對於我國發展新興科技提供實質貢獻。有鑑於此，本計畫所參與之國際會議及交流，主要蒐集國際在下世代電信編碼議題發展趨勢及討論面向，並將國際會議參與成果，回饋到計畫中。

(一)　國際組織會議分析及參與策略

本計畫盤點與下世代電信號碼相關之國際組織會議及活動，綜整發現 ITU、IETF 及 ICANN 成立背景與宗旨，及對編碼議題之探討趨勢與本計畫研究主題相符，惟參與 ITU 需向成員國遞送申請書，而我國國際處境特殊，無法直接以中華民國身分加入ITU，因此針對參與該組織及擔任該組織之重要幹部，面臨與其他國家不同的挑戰與困難。

除此之外，該組織須是由公司或單位加入或參與，而本計畫主要是透過參與國際會議及活動方式，以培養專家學者。基此，本計畫將聚焦參與可透過個人身分及非政府組織參與的 IETF 及 ICANN 組織會議及活動，並強化與「網際網路工程任務組」（Internet Engineering Task Force, IETF）及 ICANN「識別碼研究、運作及安全部門」（Identifier Research, Operations, and Security，簡稱 IROS）等組織之連結，研提參與策略及效益，以培養參與相關國際標準制定工作及可擔任該等組織重要幹部之專家學者，進而掌握國際下世代電信網路號碼發展趨勢，促進我國 5G IoT 與網路

切片相關產業技術與國際接軌，確保我國在資通訊領域的國際空間與影響力。

IETF 與本計畫議題關聯性高，其組織架構並非採取會員制度，而是以個人名義皆可參與或發表文件，參與對象以個人為主，而不是國家、公司或團體，經評估後於該組織擔任國際組織幹部之可行性較高，因此今年度安排 2 名專家學者分別參與 IETF111 及 IETF112 兩場會議，以強化國際鏈結及掌握國際相關議題趨勢；另外，考量 ICANN 近年來有與本計畫相關之 DNS 編碼議題，因此本計畫除參加 ICANN 會議，亦積極加強與 ICANN IROS 日常的交流互動，建立議程設定及政策倡議的管道。

為培育我國具備參與相關國際標準制訂工作及可擔任該等組織重要幹部之專業人才，因此將根據盤點結果，分析 IETF 及 ICANN 組織運作及工作小組，以作為今年及未來參與的指南。

1. IETF 組織及運作：網際網路工程任務組(Internet Engineering Task Force，IETF)為技術性國際非政府組織，其主要致力於網際網路標準制定，以確保全球網際網路皆能以相同的語言進行互通互聯。IETF 每年舉辦 3 場國際會議，提供設備商、學生及對網際網路有興趣者參與，就網際網路標準及通訊協定相關議題進行討論。2004 年 IETF 發布 RFC393「IETF 任務宣言」(A Mission Statement for the IETF)，該 RFC 揭示了 IETF 的使命、使命宣言的必要性、目標、研究與研發之間的平衡關係、任務和程序說明、所有權歸屬等。IETF 有別於傳統意義上的標準制定組織，IETF 的參與者都是志願人員，透過每年召開的三次 IETF 會議來完成該組織的如下使命：
   - 鑑定網際網路之運行與技術問題，並提出解決方案。
   - 詳細說明網際網路協定之發展或用途，解決相應問題。
   - 向 IESG 提出針對網際網路協定標準及用途之建議。
   - 促進向網際網路社群推廣 IETF 的技術研究成果。

- 為網際網路使用者、研究人員、電信業者、設備商及管理者等提供訊息交流的論壇。

雖然 IETF 不具有實體法人格，然而由於許多網際網路技術議題皆於該組織討論，並且透過技術人員實作及討論後，制定出技術標準(RFC)，因此該組織所公布的技術標準越來越具有影響力。

IETF 為有效解決網際網路技術問題，並制定多數人可以接受的標準，IETF 工作小組(Working Group)成員需精確掌握並界定議題範圍，經反覆討論各種方案的可行性及相容性，或評估與其他方案合作討論尋求可行性方案，最後提出新的標準及通訊協定。

IETF 每年舉辦三次會議，對於參與會議的參加者無資格上的限制，並針對網際網路協定等相關議題進行討論。例如，IETF 110 中有五場與 DNS 相關的會議，並已針對物聯網設備的 DNS 名稱自動配置提出了草案。IETF 七大領域請參閱表 5-1 包括 ART(Applications and Real-Time Area)、GEN(General Area)、INT(Internet Area)、OPS(Ops & Management Area)、RTG(Routing Area)、SEC(Security Area)及 TSV(Transport)，有 130 餘個工作小組分屬其中，每個領域設置 2 名 Directors，Directors 與 IETF 主席組成 IESG(Internet Engineering Steering Group)，共同處理業務及標準審查。與本案相關之領域為 INT(Internet)、RAI(Real-time Applications & Infrastructure)及 RTG(Routing)領域，今年度專家學者及計畫研究團隊參與及觀察 4 個工作領域的會議及先前發布的草案，並從 4 個工作領域中鎖定 1 至 2 個工作小組，作為未來積極參與 Mailing lists 及議題設定的目標。

表 5- 1、IETF 工作領域表

工作領域 (WG Area)	縮寫	研究及討論議題
Applications and Real-Time Area	ART	主要研究範圍有三類： 語音、視訊、即時訊息方式傳遞，或即時性應用和服務，且對通訊延遲具敏感性的通訊協議和架構。 非即時傳送的應用程式，如 HTTP、電子郵件和 FTP 等應用的協議和架構。 構建模組，如 URI 語法、身份驗證機制、資料格式和編解碼器等。
General Area	GEN	支援、更新和維護 IETF 標準等工作。
Internet Area	INT	主要研究 IP 層（IPv4 和 IPv6)相關議題，如 IPv4 耗盡、IP 版本間融合、DNS、DHCP、主機和路由器配置、裝置移動性、標識符號和定位符號分離、VPN 和偽線（pseudowires）等各種鏈路層技術。
Ops & Management Area	OPS	研究網路管理及網路維運議題，例如 DNS 維運、IPv6 維運、維運安全和路由維運等內容。
Routing Area	RTG	研究透過維持現有路由協議的可延展性和穩定性、路由擴充和錯誤修復等，以確保網路路由系統可持續良好運行。
Security Area	SEC	研究安全服務議題，例如完整性、身份驗證、不可否認性、機密性和訪問控制。
Transport	TSV	該領域主要涵蓋範圍如下： 網路資料傳輸之技術議題，如端到端資料傳輸機制，以支援應用和服務潛在可能交換大流量及高頻寬需求。檢測網路中的擁塞，並對網路擁塞進

工作領域 (WG Area)	縮寫	研究及討論議題
		行反應機制處理，如網路傳輸控制協議（TCP、SCTP、MPTCP 和 DCCP）中的異常流量控制。

資料來源：本計畫整理

IETF 每次會議議題都是在工作小組已有初步共識、討論度最高及重要的技術標準草案，而召開會議後再由會議主席決議該技術標準草案是否需送交 IESG 審定(共同處理業務及標準審查小組)，IESG 係由工作小組區域董事(Area Directors)及 IETF 主席共同組成，開會決定技術草案是否成為技術標準文件。換言之，IETF 社群交流與互動的意義為建立議程設定及標準擬定之重要溝通管道之一。透過蒐集 IETF 每日 Mailing lists 中之會議議程及工作小組討論議題，進而瞭解目前國際組織在電信網路編碼研究的趨勢，以強化本計畫與 IETF 會議議程之連結。IETF 標準制定流程如圖 5-2 所示。

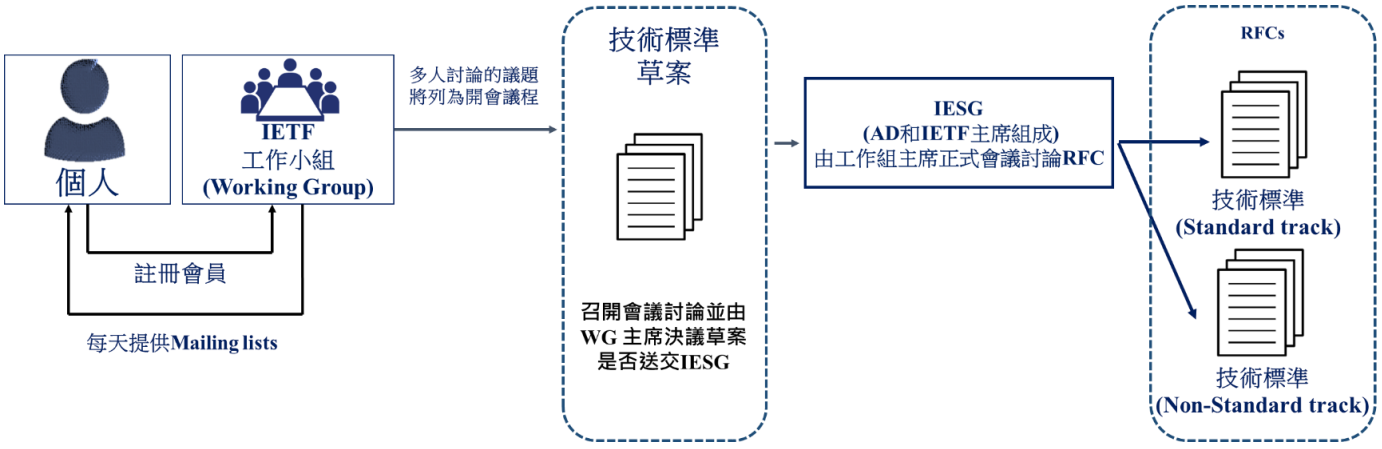


圖 5- 2、IETF 標準制定流程

資料來源：本計畫製作

2. ICANN 組織及運作： ICANN 是一個全球性的、以民意為導向、非營利性的組織，1998 年成立於美國加州。ICANN 集合了全球網路界商業、技術及學術各領域專家，負責協調網路運作、制定網路治理政策，以確保網路穩定性、安全性與韌性。ICANN 職掌範圍包含「通訊協定參數及通訊埠」（Protocol Parameters and Port）之協調、「網域名稱系統」（Domain Name System，簡稱 DNS）之管理、IP 位址之分配暨指派，以及「根伺服器系統」（Root Server System）之管理。ICANN 的使命是維護全球網路「獨特識別碼系統」（Unique Identifier System）的安全與穩定。具體而言，ICANN 的任務包含：
   - 協調分發 DNS「根區」（Root Zone）中的網域，並協助發展、執行「通用頂級網域」（Generic Top-Level Domains，簡稱「gTLD」）及以下第二級網域的相關政策。
   - 協助 DNS 根伺服器系統的維運、發展及協作。
   - 協調分發最頂級的 IP 及自治系統號碼。
   - 與相關組織合作，依其他網路協定標準訂定組織要求，提供註冊管理機構必要的網路功能。

惟須注意 ICANN 並不會監管網際網路所傳遞的內容，無法阻止垃圾郵件發送，也不負責處理網際網路存取相關事宜，但會透過協調網際網路命名系統，對網際網路的擴展發揮著重要影響。

ICANN 強調由全球「多方利益共同體」（Multi-Stakeholders）參與，如圖 5-3，多方利益共同體包含政府部門、民間企業、網路社群以及個人使用者等；其依由下而上的共識決策為基礎，制定全球網域管理政策。



圖 5- 3、ICANN 多方利益共同體組成圖

資料來源：本計畫製作

為確保所有人均平等參與政策制定之決策過程，ICANN 制定出細緻的治理流程；各社群不但參與 ICANN 技術決策，也監督並參與 ICANN 組織的營運規劃。ICANN 社群團體大致分為兩類，ICANN 組織架構如圖 5-4 所示：

- 「支援組織」（Supporting Organization，簡稱「SO」）：ICANN 的支援組織功能非常重要，其主要功能是就網路技術管理領域，提出政策建議或發起工作小組。支援組織分別為網路位址支持組織（Address Supporting Organization, ASO）、國碼頂級域名支持組織（Country Code Names Supporting Organization, ccNSO）及通用頂級域名支持組織（Generic Names Supporting Organization, GNSO）。
- 「諮詢委員會」（Advisory Committee，簡稱「AC」）：諮詢委員會針對包括政府事務（GAC）、根伺服器安全（RSSAC）、網路安全（SSAC）領域提出政策建議，其中較特別的是 ALAC，其代表廣大的一般網際網路個人使用者。

ICANN 組織如圖 5-4，董事會係由 16 位具投票權之董事組成，其中 8 位董事由「提名委員會」（Nominating Committee，簡稱「NomCom」）選出，ASO、GNSO、ccNSO 各推選 2 位，

ALAC 推選 1 位，ICANN 組織執行長則為當然董事。另有不具投票權之聯絡人 4 位。



圖 5- 4、ICANN 組織圖

資料來源：ICANN[234]

ICANN 每年舉辦三次全球性實體會議，依《ICANN 章程》所定義之五大地理區235（亞/澳/大洋洲、非洲、歐洲、拉丁與加勒比海美洲、北美洲）輪流舉辦。ICANN 每場會議均有不同形態與任務。大致說明如下：

- 第一場會議為「社群論壇」（Community Forum），通常在 2 月或 3 月舉行，為期六天；會議始於星期六，終於星期四。社群論壇會議結構包含 SO 與 AC 之內部工作、跨

[234] ICANN, Beginner's Guide to Participating in ICANN, 2013. https://www.icann.org/resources/files/participating-2013-11-08-en（最後瀏覽日：2021/5/23）

[235] ICANN，ICANN Geographic Regions，https://meetings.icann.org/en/regions（最後瀏覽日：2021/5/23）

社群互動，以及針對社群感興趣議題召開全體會議。

- 第二場為「政策論壇」（Policy Forum），通常在 6 月舉行，為期四天；會議始於星期一，終於星期四。政策論壇著重於 AC 與 SO 內部的政策制訂工作及區域外展活動。政策論壇通常比額外兩場會議規模較小，且議程較為精簡，並不會召開公眾論壇與 ICANN 董事會會議。政策論壇是 ICANN 政策制定流程工作小組推動相關工作之重要管道。
- 第三場為 ICANN「年度大會」（Annual General Meeting，簡稱「AGM」），通常在10月或11月舉行，為期六天。年度大會會議結構包含 AC 與 SO 相關工作以及跨社群間之互動，惟整體重點是向全球受眾展示出 ICANN 工作成果，並且擴充更多的會議時間做為教育培訓課程。此外，年度大會同時也是 ICANN 董事會新成員就任會議。

(二) 國際會議參與成果

盤點及蒐集ICANN、IETF及ITU等與本計畫關聯性高議題，今年度參與相關會議，分別為 ICANN 71 政策論壇、ICANN 72 年度大會、IETF 111、IETF 112 及 ITU Digital World，其透過會議參與發現目前國際對於下世代電信網路編碼著重在物聯網唯一識別碼號碼議題。依據 ITU Digital World 論壇提到，未來 5G 網路趨勢將朝向 AI 化、自動化及大量物聯網應用，因此物聯網唯一識別碼的編碼研究重要性逐漸受到重視。今年會議參與內容及參與成果說明如下。

1. ICANN 71 虛擬會議：CANN 71 會議為「政策論壇」（Policy Forum），原定於2021年6月14日至17日在荷蘭海牙舉行，但今年正逢國際新冠肺炎流行之際，因考量 ICANN 社群、董事會與工作人員之健康與安全，因此改為虛擬會議方式召開。

ICANN 71 政策論壇是 ICANN 政策制定工作小組在推動政策相關工作中，蒐集會員資訊的重要管道之一，該場會議著重於諮詢委員會與支援組織的政策制訂工作，故會議議程較多為政策制定及跨社群討論，而會議主題主要為網路監管發展、ICANN 在網際網路治理生態系統中的角色，以及討論網域註冊商之運作方式等。依據 ICANN 71 會議議程，專家學者參與「DNS 安全」、「各國監管政策對 ICANN 政策的影響」、「科技新知」、「DNS 濫用」及社群討論等會議，希冀從參與會議中，蒐集 5G 與 DNS 相關資訊及國際發展趨勢，以強化研究研析能量，詳細會議參與場次之參與理由及效益如表 5-2 所示。

表 5- 2、ICANN 71 會議參與及效益表

會議名稱	中文名稱	參與理由及效益
DNSSEC and Security Workshop (1 of 2)	DNS 資安與安全研討會 (1 of 2)	1. 本場會議講述 DNS 資安及安全相關議題及政策發展方向。 2. 透過參與該會議，蒐集 DNS 資安及網路安全資訊，以作為本計畫後續研究之參考。
DNSSEC and Security Workshop (2 of 2)	DNS 資安與安全研討會(2 of 2)	
Plenary Session: Impact of Regulatory Developments on ICANN Policy Topics	全體會議：各國監管政策對 ICANN 政策的影響	1. 本場會議講述從各國國內法(例如 GDPR)在 ICANN 各項政策之影響，及後續可能進展的方向，進而推測未來國際網際網路政策發展趨勢。 2. 希冀透過 DNS 相關資安議題及會議討論內容，作為後續網路運作（無論是固定網路、行動網路或是物聯網）相關稽核規範制定之參考。

會議名稱	中文名稱	參與理由及效益
Tech Day (1 of 2)	科技新知(1 of 2)	1. 透過技術性議題的分享，可獲悉與網域名稱產業（註冊業務、DNS、網路安全等）相關技術新知。 2. 透過會議的召開，結識更多各專業領域的著名專家，擴展技術人際脈絡。
Tech Day (2 of 2)	科技新知(2 of 2)	
GNSO - CPH DNS Abuse Work Group Community Update	GNSO - CPH DNS 濫用工作小組會議	透過 GNSO 締約方對 DNS 濫用行為的研析與應對行為報告，藉此了解 ICANN 部分社群對 DNS 濫用行為的相關規範制定方向與採取措施，以做為未來相關場域規範、限制與濫用行為認定之參考。
SSAC Public Meeting	網路安全穩定諮詢委員會公開討論會議	透過「安全與穩定諮詢委員會」（SSAC）與公眾的互動和對談，進一步了解該社群特性與參與社群的成員的行業屬性，以此做為我國未來啟動新型態網路建設在組建網路安全與「服務提供層級」（Service Level）維持相關的機制時，可有一足供參照且持續運作之對象。
The Post-Pandemic Future of ICANN Public Meetings	後疫情下未來 ICANN 會議舉行方式討論會議	1. 該議程討論下次 ICANN 會議的形式及討論議程。 2. 希冀透過參加該會議，提前掌握 ICANN72 會議主軸，以利

會議名稱	中文名稱	參與理由及效益
		本計畫提前準備研究及相關事宜。

資料來源：本計畫製作

2. ICANN 72 虛擬會議：ICANN 72 會議為 ICANN「年度大會」（Annual General Meeting，簡稱「AGM」），會議結構包含 AC 與 SO 相關工作以及跨社群間之互動，惟整體重點是向全球展示出 ICANN 工作成果，並且擴充更多的會議時間做為教育培訓課程，同時也是 ICANN 董事會新成員就任會議。本次會議除了延續 ICANN 71 參與 DNSSEC、SSAC 外，本次參與 3 場 Tech Day，並由本計畫顧問國立宜蘭大學資訊工程學系陳麒元副教授，發表行動裝置應用 DNS 作為識別機制的「概念驗證」（PoC），希冀透過今年研究成果，進行國際交流及互動，ICANN 72 會議如表 5-3。

表 5- 3、ICANN 72 會議參與及效益表

會議名稱	中文名稱	參與理由及效益
Introducing the DNS Security Facilitation Initiative - Technical Study Group (DSFI-TSG)	介紹促進 DNS 安全-技術研究組	1. 簡介工作小組成立目的。 2. 說明網際網路生態系與 DNS 間的緊密關聯。 3. 說明 DNS 惡意攻擊的樣態與可能的解決方案。 4. 此場會議介紹促進 DNS 安全-技術研究組（DSFI-TSG）之工作。
SSAC Public Meeting	網路安全穩定諮詢委員會公開討論會議	1. 向公眾簡介社群成立目標與宗旨。 2. 公布社群研究成果。 3. 社群進行中及預計研討的工作項目說明。

會議名稱	中文名稱	參與理由及效益
		4. 藉由 SSAC 成員及公眾分享內容中，了解 SSAC 社群成員與外界互動的模式，進一步提供評估參與該社群的相關策略。
Tech Day (1 of 3)	科技新知（1 of 3）(1 of 3)	透過技術性議題的分享，可獲悉與網域名稱產業（註冊業務、DNS、網路安全等）相關之技術新知。 透過會議的召開，結識更多各專業領域的著名專家，擴展技術人際脈絡。
Tech Day (2 of 3)	科技新知（2 of 3）(2 of 3)	
Tech Day (3 of 3)	科技新知（3 of 3）(3 of 3)	
Joint Meeting: ICANN Board and SSAC	ICANN 董事與網路安全穩定諮詢委員會公開討論會議	1. 就社群關注議題與政策和 ICANN 董事會溝通。 2. 社群成員直接向 ICANN 董事會表達意見的機會。
DNSSEC and Security Workshop(1 of 3)	DNS 資安與安全研討會（1 of 3）(1 of 3)	藉由與會講者的經驗分享與運作實績呈現，可提供本專案場域實驗小組更多 DNS 相關安全技術導入參考，讓整體場域實驗更加完整及具前瞻性。
DNSSEC and Security Workshop(2 of 3)	DNS 資安與安全研討會（2 of 3）(2 of 3)	
DNSSEC and Security Workshop(3 of 3)	DNS 資安與安全研討會（3 of 3）(3 of 3)	

資料來源：本計畫製作

3. ICANN 會議成果：今年度參與 ICANN 兩場會議中，主要會議成果有蒐研與本計畫相關議題，本計畫主要是透過物聯網裝置設備上的 IMEI 碼作為唯一識別碼，並透過 5G 核心網的 Radius 轉換為 DNS，本實驗概念的目的，主要是提供下世代電信網路在大量物聯網裝置、AI 化及自動化下，建立自動化及好管理的物聯網設備編碼機制，試圖取代 E.164 物聯網號碼之可行性驗證。此外，在 DNS 系統下的資安稽核機制，也是本計畫分項二的研議焦點，因此本次會議積極蒐集與本實驗相關議題及討論，並且發表今年度 PoC 研究成果，透過會議上的討論及交流，精進本實驗架構。

今年度參與 ICANN 71 及 72 兩場會議，會議中有 3 場會議內容提供本案持續研析，其 3 場會議內容及與本計畫關係說明如表 5-4。

表 5- 4、ICANN 會議報告與本計畫關係說明表

報告名稱	報告內容	與本計畫關聯性
歐盟網路安全原則性措施之指令草案（NIS2）	NIS2 草案核心，歐盟希望各成員國均能加入網路安全（Cybersecurity）的協防架構中，各成員國應要求其境內管理網域名稱系統（Domain Name System，簡稱 DNS）之機構，致力於維護其註冊資料之正確、紀錄 DNS 登記人之聯絡資訊、公布非屬個人資料之資訊，如遇正當請求	NIS2 草案專注於打擊網路犯罪，希望 ICANN 旗下的域名發放與登記單位能夠配合執法單位提供可疑違法人士之個人資料，雖然與電信號碼相關之主題較為無關，但確是網際網路界未來重要的國際趨勢，ICANN 對於歐盟的各草案之意見以及未來之因應措施，也會影響整個 DNS 生態系，是以應列

報告名稱	報告內容	與本計畫關聯性
	時應立刻提供相關資訊。	為重點觀察之國際趨勢。
網路犯罪公約（Convention on Cybercrime）	網路犯罪公約定義網路犯罪（Cybercrime）之內容以及規模、各國防治網路犯罪（Cybercrime）應採取之措施，其中第83條要求各國應訂定法律，要求網域名稱登記機構有協助執法機關調查並提供資料之義務。	網路犯罪公約對於ICANN旗下的域名發放與登記單位就註冊人之資料蒐集與利用等，未來將有具體義務誕生，應持續觀察此類議題。
零接觸通用 IoT 裝置識別（Zero-Touch Universal IoT Device Identity）	零接觸通用 IoT 裝置識別是使用以 PKI 為基礎之裝置識別，透過使用者購買具備預先配置通用識別的裝置或安全元件（允許 CA 在初期就參與供應鏈）做為識別策略，其具有諸多安全特性。	該研究與本計畫都探討IoT 識別方式，該研究優點在於探討如何在IoT安全情境下進行裝置識別，因此該研究可為本實驗要探討的裝置安全提供研究參考。

資料來源：本計畫製作

NIS2 草案核心，歐盟希望各成員國均能加入網路安全（Cybersecurity）的協防架構中，各成員國應要求其境內管理網域名稱系統（Domain Name System，簡稱 DNS）之機構，致力於維護其註冊資料之正確、紀錄 DNS 登記人之聯絡資訊、公布非屬個人資料之資訊，如遇正當請求時應立刻提供相關資訊。

NIS2 草案有三大綱領為：成員國固有能力、風險管理、合作與資訊交流；其中以「風險管理」與 DNS 營運商最為相關。

DNS 系統與 NIS2 指令認為網路的完整性仰賴一個可靠、強韌且安全的 DNS 系統，是故 DNS 系統扮演的角色至為重要，並歸為 NIS2 所定義的關鍵設施；DNS 解析鏈上所有的服務供應商皆屬適用對象，包括根域名伺服器、頂級域名伺服器、權威名稱伺服器及遞迴解析器。

為求執行上的一致性，全部的 DNS 服務供應商與頂級網域名稱皆自動納為適用對象；另外採用單一管轄權制度，故 DNS 服務供應商必須根據其主要場所（Main Establishment）在歐盟境內所位處之國家採行 NIS2；在歐盟境內未設立有主要場所者，則須指派一名代表於歐盟。NIS2 採取的安全規範水平適用於各個部門，但單一部門內亦可討論其專屬做法；問責性歸屬之層級為各類關鍵設施的上級管轄單位。關於各域名註冊資料納入規管範圍如表 5-5 所述。

表 5- 5、網域名稱註冊資料與 NIS2 指令草案規管範圍表

項次	網域名稱註冊資料與 NIS2 指令
鑑於註冊管理機構應遵守規範，NIS2 基於以下理由，將域名註冊資料納入規管範圍	
1	為維護 DNS 的安全穩定與系統韌性，應維持資料之正確及完整，並保障合法取得性。
2	註冊資料的及時取得性與 DNS 濫用的防治直接相關。
相關規範明文於 NIS2 第 23 條（Article 23），TLD 註冊管理機構為其對象	
1	應蒐集並維護域名註冊資料的正確性及完整性。
2	應納入得識別／聯繫域名持有人及「聯絡窗口」（Contact Point）之資料。
3	不得無故延宕非個人資料之揭露。

項次	網域名稱註冊資料與 NIS2 指令
4	不得無故延宕註冊資料請求之回應。
5	特定資料之請求者，若驗證結果符合合法請求之目的，則應予以揭露。
6	註冊資料的及時取得性與 DNS 濫用的防治直接相關。歐盟之目的希望註冊管理機構相關方，應針對 NIS2 的規範擬定因應政策及指引，尤透過 ICANN 內部延伸擬定為佳，藉此補足 ICANN 長期以來在 WHOIS 資料政策上所取得成果。此外，為確保歐盟單一市場的運作一致性，歐盟願意採納經產業或 ICANN 制定之「指引準則」（Guideline）。

資料來源：本計畫製作

《網路犯罪公約》係歐洲理事會針對「經電腦進行之特定犯罪行為」所擬定的刑事司法公約，除了持續針對如智慧型手機等新型裝置增訂指引內容（Guidance Notes）外，近期也提出籌備中的《強化合作及電子證據披露做法之網路犯罪公約第二增訂草案》（2nd Additional Protocol to the Budapest Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence）。

《網路犯罪公約》截止目前已有 66 個簽署方及 11 個觀察國。此公約的實踐情形由歐洲理事會網路犯罪公約委員會（Cybercrime Convention Committee，TCY）進行追蹤評估，並由歐洲理事會網路犯罪防治計畫辦公室（Cybercrime Programme Office，C-PROC）負責能力建構工作。

另外是「零接觸通用 IoT 裝置識別安全性策略」，本篇透過實證研究，針對 IoT 識別對安全性帶來之挑戰進行說明及提出解決方案。主要探討內容為哪些「識別挑戰」（Identity Challenge）會阻擾 IoT 之安全性？使用以 PKI 為基礎之裝置識別，做為識別策略，其具有諸多安全特性，其安全性策略及說明如表 5-6。

表 5- 6、零接觸通用 IoT 裝置識別安全性策略說明表

安全性策略	說明
「端對端」（End to End，簡稱 E2E）訊息安全（E2E Message Security）	● 在訊息中介進行簽章／加密。 ● 防止中介受到侵害的好方式。
傳輸驗證（Transport Authentication）	● 使用 TLS[236]相互驗證的裝置憑證。 ● 比「私鑰分割」（Shared Secrets）、API Tokens 更具安全性。
網路驗證（Network Authentication）	● 使用 EAP-TLS[237]驗證的裝置憑證。 ● 允許精細的網路造訪，比預先「共享金鑰」（Pre-shared Key）更佳。

資料來源：Ash Wilson（Valimail）

然現階段無法完全採納上述安全策略的主要原因在於「互通性」（Interoperability）及成本問題如下表 5-7。

表 5- 7、零接觸通用 IoT 裝置識別互通性安全性策略說明表

安全性策略	問題
認證中心（Certification Authority）	● 建立、營運、維護、保護成本高。 ● 小型企業難以接觸。 ● 在應用程式／組織導入 CA 或 PKI，需引入額外的「命名空間」（Namespace）。當有多個命名空間時，CA 可以確保在其命名空間內識別碼的一致性，但無法避免另外的 CA 使用相同的實體名稱。

[236] Transport Layer Security，即「傳輸層安全性」。

[237] EAP-TLS 是 IETF 的一個開放標準，使用 TLS 協定來驗證客戶端網路，以允許客戶端加入該網路。EAP-TLS 在無線廠商之間得到很好的支持，其能夠提供良好的安全保證。EAP-TLS 使用 PKI 來保護 RADIUS 認證伺服器的通訊，不過因為 EAP-TLS 配置困難而很少被使用。

安全性策略	問題
	● 需將所有內容加載至同一 CA，以避免識別碼衝突。
訊息安全 （Message Security）	● 用於尋找證書的專有 API 整合。
傳輸驗證及網路驗證	● 需要分配「信任錨」（Trust Anchors，簡稱「TA」）。 ● 撤銷需要 OCSP[238]或 CRL[239]。 ● 特別對於小型組織來說難以做到。

資料來源：Ash Wilson（Valimail）

該實驗透過「網路驗證」（Network Authentication），並在「通用識別」（Universal Identity）理想狀態，使用者購買具備預先配置通用識別的裝置或安全元件（允許 CA 在初期就參與供應鏈），以支援不同網路及網路提供商間之「漫遊」（Roaming），用於會計、退款之顧客識別碼，並使用更易於撤銷的 OCSP／CRL；另外該篇文章也討論到命名空間的重要性，認為 Binding 命名空間缺乏，透過「雲端安全聯盟」（Cloud Security Alliance，簡稱 CSA）IoT 識別及造訪管理之結論指南以定義 IoT 裝置的通用命名空間，挑戰是應用程式設計者僅定義一個全新的命名空間。另外文章假設如只使用 DNS 而不新建一個命名空間呢？

DANE 的使用：解決現況及通用識別之間存有的兩個問題，一是缺乏用於客戶端識別的命名空間、憑證及信任錨的可尋性，採用 CA 發行的用戶端 ID 佈建 EAP-TLS，以做為移至 DNS-bound 客戶端識別的方式，在不改變 TLS 的情況下支援新的協定。而在是否可以在 RADIUS 伺服器中動態管理 CA 證書的同時執行

[238] 即「線上憑證狀態協定」（Online Certificate Status Protocol）。
[239] 即「憑證吊銷列表」（Certificate Revocation List）。

DNS 名稱 bindings 成為一項挑戰，講者表示，在過程中有一些方式可以在 TLS 以外的地方進行驗證，其 PoC 如圖 5-5 至圖 5-7。

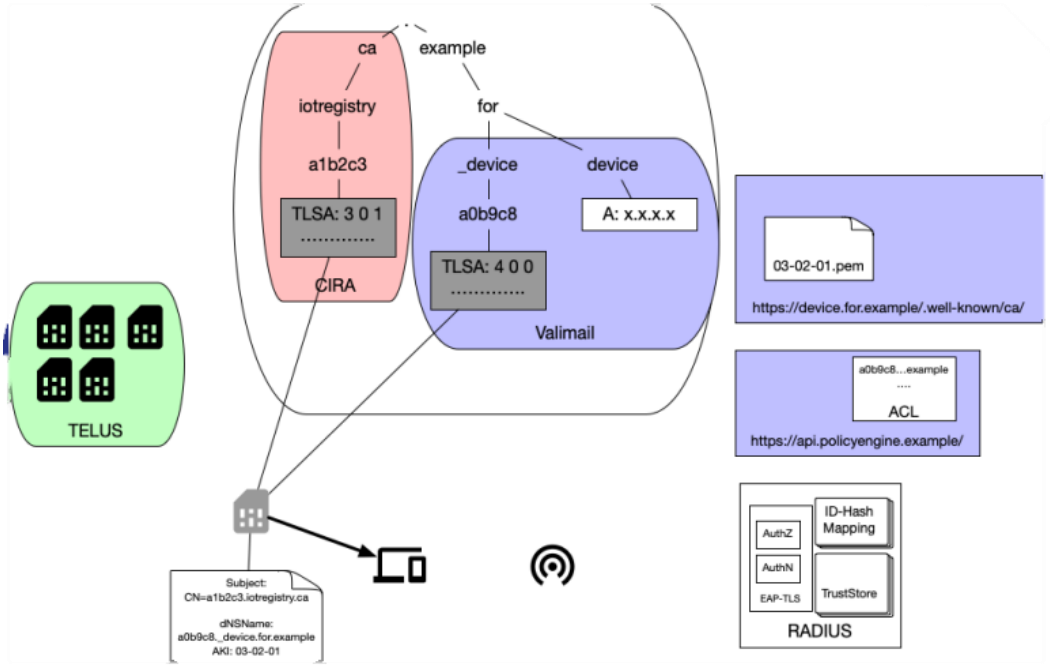


圖 5- 5、零接觸通用 IoT 裝置識別之識別發行流程圖

資料來源：Ash Wilson（Valimail）

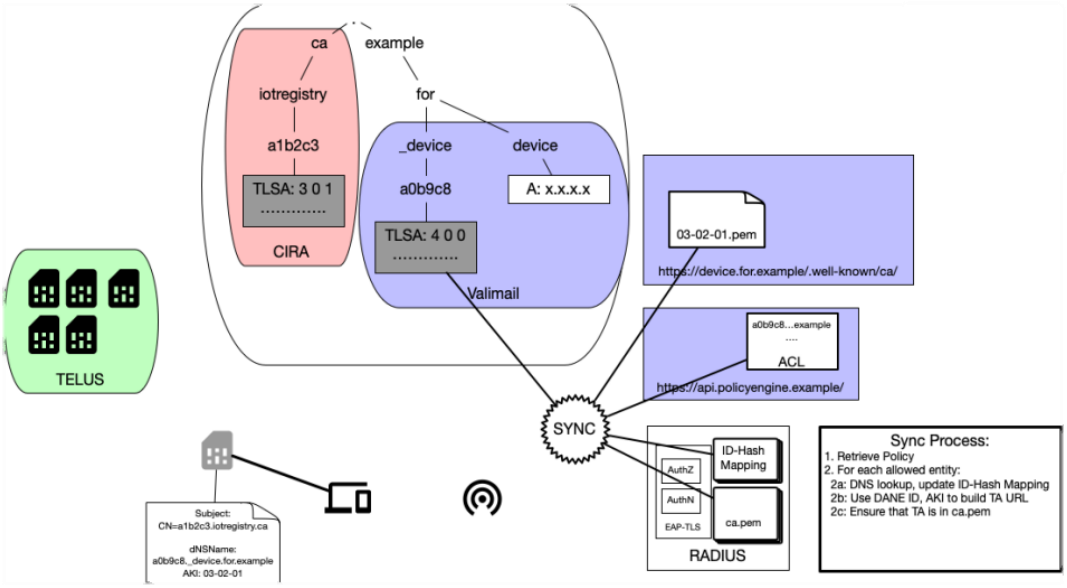


圖 5- 6、零接觸通用 IoT 裝置識別之信任認證圖

資料來源：Ash Wilson（Valimail）

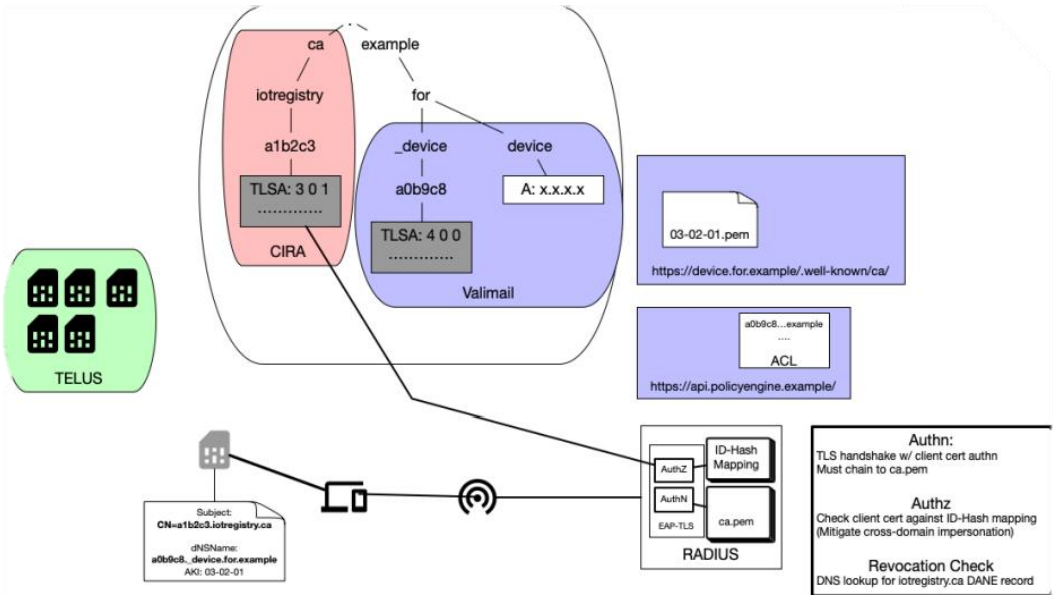


圖 5- 7、零接觸通用 IoT 裝置識別之驗證及授權圖

資料來源：Ash Wilson（Valimail）

除參與國際會議所獲得與本計畫相關資料外，由於今年度本計畫透過書信及電洽方式，試圖與 ICANN 技術長辦公室進行技術交流，然而經過多次嘗試未果，因此本計畫轉換方式，與 ICANN GNSO 聯繫，希冀能在 ICANN 72 會議的 Tech Day 發表成果，而歷經多次針對本計畫議題及 DNS 技術進行交流後，最終 GNSO 同意安排時段讓本計畫發表 PoC 成果。

本次成果發表係由本計畫人才培育之專家學者，國立宜蘭大學陳麒元副教授進行報告，以本計畫分項三 PoC 實驗為主題，說明透過在 5G 網路切片環境下，核心網路以 Radius 協議將 APN、Cell ID、IMSI、MSISDN、IMEI、IP 等資料傳送至 Gn DNS 進行 IoT 設備編碼。並說明實驗設計兩個不同場域，並將設備裝置移動性需求、相同的完整網域名稱連接到不同的 IP 地址及 DNS 基礎運行，透過完整網域名稱(FQDN)可以查詢 IP 地址並連接到不同應用指標，作為 5G 物聯網 DNS 編碼技術，並作為管理 5G 物聯網管理方式。

陳教授最後提到透過 PoC 過程，已驗證 DNS 自動編碼之機制與方法，可運用於最新 5G 網路切片環境，並以有效方式管理 IoT 裝置。

團隊下階段規劃在實際 5G 網路環境，導入電信服務情境進行服務驗證（PoS）。本次的內容，獲得與會者的熱烈迴響，紛紛提問，從提問的內容也可看出陳教授的實驗的確是準確擊中目前某些 IoT 裝置運作的盲點，與會者提問概略整理如下：

a. 實驗目標的 IoT 裝置是什麼？（實際應用／商業化後係有哪些裝置會使用本技術下去實際運作？）
b. DNS A 紀錄及 AAAA 紀錄的 TTL 設定值是甚麼？
c. 在 ZONE 有這麼多更新時，是如何管理 DNS 的授權啟動紀錄值的？
d. 這些名稱將會用在哪裡？請說明隱私保護規劃／考量。
e. 上述 DNS 都是否在私人網路上運作？
f. 若 IoT 裝置在工業網路情境下不會移動／移轉的話，那變換行動通訊基地臺的意義是什麼？

因時間有限，針對相關提問回應，講者於會後提供書面資料給主辦團隊，提供大家參考。

今年參與兩場 ICANN 會議，並由 3 位專家學者及研究團隊共同參加，專家學者建議組建含官學研的團隊，以及鎖定特定國際組織社群，以利集中資源投入能量。

4. IETF 111 虛擬會議：IETF111 虛擬會議於 2021 年 7 月 26 日至 7 月 30 日舉行，共計 5 日。此次會議由「瞻博網路」（Juniper）、CISCO、ICANN 等單位贊助主辦，為因應新型冠狀病毒疫情影響，以「全球遠端參與形式」舉行，共計 1,411 名遠端參與者。

由於 IETF 主要負責網際網路標準的研究發展和制定，例如網際網路上使用的通訊協定(protocols)、程序 (procedures)和慣例

(conventions)等的制定，其組織架構，與本計畫議題關聯性高，並非採取會員制度，而是以個人名義皆可參與或發表文件，參與對象以個人為主，而不是國家、公司或團體，經評估後於該組織擔任國際組織幹部之可行性較高，因此今年度安排2名專家學者分別參與 IETF111 及 IETF112 兩場會議，以強化國際鏈結及掌握國際相關議題趨勢。

IETF111 議程安排主要為「網際網路工程任務小組」（Internet Engineering Task Force，簡稱「IETF」）及「網際網路研究任務小組」（Internet Research Task Force，簡稱「IRTF」）各工作小組進行中「草案」（Draft）目前進展及未來規劃，同時包含社交活動 Newcomers' Coffee Break 及 IETF 全體大會，請參見表 5-8。

表 5- 8、IETF 111 會議參與及效益表

會議名稱	中文名稱	參與理由及效益
ACM/IRTF Applied Networking Research Workshop New Internet Protocols & Practical Congestion Control	ACM/IRTF 應用網路研究研討會 新的網路協議和實用的擁塞管制	透過應用網路研究研討會，掌握目前國際在網際網路的討論及研究主軸。
IRTF Open Meeting	IRTF 公開會議	參與本工作小組的討論，除了有機會獲取與本專案相關草稿工作進程外，也可了解該小組作業文化。
Domain Name System Operations	域名系統操作	
DANE AutheNtication for Iot Service Hardening	用於物聯網服務強化的 DANE 身份驗證	
Newcomers' Coffee Break	Newcomers' Coffee Break	藉由新進成員活動，多方面了解 IETF 生態及領域社群。

會議名稱	中文名稱	參與理由及效益
Extensions for Scalable DNS Service Discovery	可擴充 DNS 服務發現的延伸	參與本工作小組的討論，除了有機會獲取與本專案相關草稿工作進程外，也可了解該小組作業文化。
ACM/IRTF Applied Networking Research Workshop Privacy & Applications	ACM/IRTF 應用網路研究研討會 隱私與應用	透過應用網路研究研討會，掌握目前國際在網際網路的討論及研究主軸。
IETF Plenary	IETF 全體會議	藉由參與 IETF 全體大會，了解其重要核心成員對整體組織的領導方向及評估各領域議題的側重方向，以提供專案成員擘劃未來專案主軸。
DNS PRIVate Exchange	DNS 私有交換	DNS 傳輸交換隱私工作小組（Dprive）主要工作是保障 DNS 訊息交換間的機密性及找尋可能性的解決方案並評估工作小組所提供的技術方案應對各種 DNS 監控攻擊的有效性。 參與本工作小組的討論，除了有機會獲取與本專案相關草稿工作進程外，也可了解該小組作業文化。
Deterministic Networking	確定性網路	

資料來源：本計畫製作

5. IETF 112 虛擬會議：IETF112 虛擬會議於 2021 年 11 月 8 日至 11 月 12 日舉行，共計 5 日。該場會議由 Ericsson、CISCO、Akamai 等單位贊助辦理，由於本次會議仍是新型冠狀病毒疫情影響之際，因此以「全球遠端參與形式」舉行。

IETF112 延續 IETF111 參與議程，本次安排參與「網路上 IPv6 的限制資源節點」（IPv6 over Networks of Resource-constrained Nodes）、「運營和管理領域工作組與 OpsAWG / OpsAREA 接合」（Operations and Management Area Working GroupCombined OpsAWG / OpsAREA）、「DNS 私有交換」（DNS PRIVate Exchange）等議程，會議參與場次及效益請參見表 5-9。

表 5- 9、IETF 112 會議參與及效益表

會議名稱	中文名稱	參與理由及效益
IETF Plenary	IETF 全體會議	透過參與 IETF 全體大會，了解 IETF 整體組織的領導方向及評估各領域議題的重點，以提供專案成員擘劃未來專案主軸。
IPv6 over Networks of Resource-constrained Nodes	網路上 IPv6 的限制資源節點	參與此場會議可知該工作小組各草稿之工作進展及重點，例如：「無線個人區域網路」（WPAN）與「低功率廣域網路」（LPWAN）中相關「標頭資料壓縮」（Header Compression）技術及「原生性短位址」（Native Short Address，簡稱「NSA」）在物聯網（IoT）應用與 NSA 的特性。

會議名稱	中文名稱	參與理由及效益
Operations and Management Area Working Group Combined OpsAWG / OpsAREA	運營和管理領域工作組與 OpsAWG / OpsAREA 接合	參與此工作小組之討論，可獲得與本專案相關草稿之工作進程。
IRTF Open Meeting	IRTF 公開會議	透過參與 IRTF 公開會議可知目前 IRTF 各項工作進程及發展狀況。
Deterministic Networking	確定性網路	確定性網路 (DetNet) 工作小組專注於在第 2 層橋接及第 3 層路由段上運行之確定性數據路徑，這些路徑可以提供延遲、丟失以及數據封包延遲變化和高可靠性的界限。參與此場會議可知該工作小組目前各草稿技術發展進程。
DNS PRIVate Exchange	DNS 私有交換	DNS 傳輸交換隱私工作小組（Dprive）主要工作係保障 DNS 訊息交換間之機密性及找尋可能之解決方案，並評估工作小組所提供之技術方案應對各種 DNS 監控攻擊的有效性。
Domain Name System Operations	域名系統操作	此工作小組主要工作為 DNS 軟體開發、服務運作及管理製作相關的工作指引。 目前沒有與專案（直接）相關之技術文件討論，但仍建議參

會議名稱	中文名稱	參與理由及效益
		與本議程以了解目前技術規劃方向。
IOT Operations	物聯網運營	此工作小組係負責討論物聯網相關設備運作問題，尤其是設備的啟動與生命週期的管理；因為與物聯網相關的 IETF 工作小組很多，本工作小組也希望在討論各種物聯網相關的技術組合時能發揮積極的作用。

資料來源：本計畫製作

6. IETF 參與建議：我國為全球移動資通訊及物聯網設備的主要設計及生產地，網際網路服務供應商（ISP）及設備製造商，除應積極參與 IETF 現場或線上會議，以俾了解網路協定及服務的最新資訊，更應主動參與 IETF 工作小組的討論（以現場或遠端形式參與），提出相關建議，使學、產相關研究成果能納入網際網路的協定，以提升我國資通訊產業的競爭力。本次會議的相關建議及草案，對我國進一步了解目前技術前端的研究與方向有實質幫助，而相關的建議如下：

- 鎖定 IETF 參與及討論主題：參與 IETF 兩次會議，在本計畫研究下，觀察出目前 IETF 探討的議題仍主要針對網路通訊、物聯網、路由通訊、無線網路、DNS 安全、IRTF 等領域，在相互關係上，每個領域都有其重要性與獨特性。針對本計畫下世代電信網路號碼技術並未觀測出 IETF 有開始討論的工作小組或草案，換言之，雖然 ITU Network 2030 提出下世代電信網路特徵之一係電信網路及網際網路日漸融合，但截至目前觀察，IETF 並未針對該議題開始討論。事實上，本計畫認為並不是尚未開始討論，就沒有討論或是延續該議題之

必要，反之亦然，本計畫評估「物聯網唯一識別碼自動配置」、「電信網路與網際網路介接」、「DNS 系統安全」等議題將是未來下世代電信網路號碼技術下熱門及制定國際標準之方向，事實上該研究方向仍會隨著國際技術發展有所變更，但可確定有助於標準制定及國際互動交流方向之議題。

- 配合參與 IETF Mailing list 討論，建立對相關研究議題之交流：針對上述鎖定「物聯網唯一識別碼自動配置」、「電信網路與網際網路介接」、「DNS 系統安全」等議題作為未來在 IETF 制定技術標準前期應積極參與 IETF 電子郵件討論之群組，IETF 各個工作小組都有 IETF 電子郵件討論群組，群組內討論範圍涉及網際網路協定的早期規劃直至最後徵求意見稿的定案，且會議中報告的草案，大多已於電子郵件討論群組中取得一定程度之共識後，才於會議中進行宣讀報告。我國政府相關部門、國內廠商及網際網路服務供應商應當積極參與各電子郵件討論群組，了解未來網際網路協定或架構的趨勢，積極提出對我國發展有利的相關意見等，讓我國資通訊的相關發展得以在國際上處於領先地位。

(三) 國際組織交流成果

本計畫今年度 ICANN IROS 及 IETF 等國際組織進行交流，其交流執行過程及成果說明如下。

在與 ICANN IROS 進行多次的書信交流部分，主要針對與本計畫相關議題詢問 ICANN IROS 是否有相關研究，以及 ICANN 針對 5G 技術發展趨勢等相關意見。ICANN IROS 表示針對 5G 技術相關研究部份，ICANN 於 2020 年發布一篇 IROS-004 《5G Technology》，近期內並計劃更新該報告。

此外，ICANN 表示在《5G Technology》中提到的「延遲」議題上，目前並沒有衍生或對此議題有繼續著墨的計畫；而在「網路切片」和「新標識符號」這兩個議題，ICANN IROS 表示有發

表了IROS-017《NEW IP》及ISG NIN(Industry Specification Groups Non-IP Networking/非 IP 相關網路連接產業規範小組)報告，ICANN正在撰寫一篇關於非IP的報告，並已於2021年7月更新。

在近期與ICANN IROS交流中，其提供以下幾篇與本計畫相關報告，其內容及摘要如下：

- IROS-026《Non-IP Networking (NIN)》：該報告是與歐洲電信標準協會(ETSI)合作完成。該報告針對下世代電信網路中的網路虛擬化技術下，將非 IP 網路作為 TCP/IP 協議替代方案之可行性；由於TCP/IP協議恐不適合下世代電信網路，特別是在網路虛擬化的情況下，因此該篇報告說明透過每個數據封包包含資料源和目的地，以及中間路由器如何轉發數據包等資料，應簡化IP數據封包。
- IROS-017《New IP》：New IP，係以一個可以定義新網路資料封包格式的資料介面（data plane）技術，讓資料封包格式在傳輸架構上允許點對點不一致，且在不用安裝轉譯裝置的情形下向後相容（backward compatibility）。進一步言之，New IP 可破除既有資料封包的嚴格結構，像是發訊點使用IPv4、接收點為 MPLS 格式此種不對稱位址（asymmetric address）的傳輸機制，將不需要透過通道進行傳輸，僅需建置能解讀New IP格式的路由設備。若聚焦於電信編碼機制方面，語音封包（standalone packet）的位址類型包含 IPv4、IPv6或MPLS的值，則封包需自帶IPv4、IPv6或MPLS編碼規則，以因應多種通訊協定網路互連的情境。
- IROS-004《5G Technology》：隨著科技快速發展與物聯網時代來臨，下一波的連網設備將不再侷限於電腦與行動電話等智慧型手持裝置，機器與機器之間的通訊將成為常態。然而此一趨勢將要面臨的一個重要問題是，「針對 5G 超高速、低延遲的應用場景，既有的 DNS 是否仍適用於 5G？」，對

此問題，ICANN 於 2020 年 1 月提出「5G Technology」報告，該報告提出在 5G 技術中網路部署與資源配置擁有更大的彈性，若優化 DNS 設計架構及整體運作，有助於彌補 DNS 遞迴式查詢設計導致之傳輸延遲，而讓整體 5G 網路實現最佳化的應用場景特性。

本計畫之ICANN IROS交流工作項目，係透過長期參與ICANN會議的單位網路中文資訊股份有限公司協助建立與ICANN IROS互動交流的管道，然後在幾次與ICANN IROS交流過程中，感受到ICANN IRSO交流意願及討論積極性較低，本計畫團隊有嘗試提供初步研究成果內容與ICANN IROS討論，然而仍無獲得回覆。以下是網路中文及本計畫綜整之執行困境：

- 書信交流降低議題討論意願：由於受到疫情影響，無法參與實體會議，而僅能用書信或 Skype 等通訊軟體互動，然而書信及 Skype 等互動無形中增加 ICANN 人員工作負擔，導致降低回覆及交流之意願。根據網路中文過去的經驗，召開實體會議時，當面的討論及交流較有助於對議題之完整傳達，以及提升交流之意願，換言之，書信交流確實降低溝通之有效性。
- 下世代電信網路議題與 ICANN 研究領域較無直接關係：透過書信交流及參與 ICANN 71 成果來看，ICANN 主要是負責網際網路名稱與數字位址分配之機構，雖然 ICANN IROS 是 ICANN 的技術部門，但其研究領域不外乎網際網路名稱，在下世代電信網路相關議題並沒有主動涉略，然而依據網路中文分析，在 ICANN「one world, one internet」的宗旨下亦會關注 5G 技術發展，然而在現階段技術仍在發展的同時，並不會積極研究5G技術(如網路虛擬化、網路切片)等相關衍生性議題。

有鑑於疫情關係，近期ICANN 72確定仍是召開虛擬會議，換言之，現階段與ICANN IROS交流困境將無法因召開實體會議親自互動

交流下而獲得好轉。

本計畫觀察ICANN IROS會與研究單位或國際相關組織合作，透過會議或於國際相關組織發表議題，進行合作或交流，因此，本計畫於ICANN 72會議的Tech Day發表一場「電信網路號碼裝置DNS自動配置」，透過實質產出及研究成果，與ICANN IROS及ICANN針對5G及下世代電信網路號碼議題建立討論及互動的基石，並希望藉由在ICANN 72發表論文，能與國際各界針對本計畫議題討論與回饋，除蓄積本計畫研究能量外，透過發表相關議題，以作為我國資通訊政策倡議之橋梁。

本次在Tech Day發表之研究成果，利用DNS作為物聯網識別碼並設計概念性驗證（PoC），透過自動分配DNS識別碼管理物聯網裝置。經由DNS識別碼機制，5G固定和行動物聯網裝置能高效取得識別碼，未來也可將此編碼系統應用於最新的5G專網切片環境並有效管理大量的物聯網裝置。例如藉由引導車輛接收即時交通資訊規劃智慧交通路徑，以緩解擁擠路況。此次研究成果發表獲得來自不同國家政府、學術及網路社群等專業領域與會者的熱烈討論及迴響，TTC也期待透過此次發表建立國際交流管道、加強國際鏈結，並確保我國在資通訊領域的國際空間與影響力。

另外，在與IETF交流部分，IETF Guide Program計畫係透過IETF資深參與者帶領新進者（參與實體會議五次以下）方式，以協助新人縮短成為活躍成員(active member)的時間。該計畫主要具體目標為了解 IETF及技術標準開發過程的相關知識、給予具主動學習意願之參與者即時回饋及培育IETF新一代活躍成員等。

本次IETF專家交流是透過IETF Guide Program指導員計畫，依據指導員的專長、研究領域協助本計畫媒合到目前任職於美國加州大學洛杉磯分校(University of California, Los Angeles)的IETF資深會員Dr. Zhang，Dr. Zhang為IETF前期會議的21位成員之一，參加IETF已有34年資歷。其主要研究物聯網、TCP/IP及命名資料網路 (Named Data

Networking，簡稱NDN)等相關研究，近期投入研究命名資料網路、網路協議架構設計(Network Protocol Designs)、下世代網際網路及物聯網安全等相關研究，其指導員專長與本計畫具有高度關聯性。

本次交流主要分為兩部份，第一為參與IETF社群及會議指南，第二為下世代電信網路號碼相關議題。會議結束後，Dr. Zhang另外回饋與本計畫議題相關資訊，其交流成果及回饋：

- 下世代電信網路號碼相關議題：有關下世代電信網路號碼透過網域名稱系統（Domain Name System，簡稱DNS）命名須考量到安全系統，事實上這個問題不是無法解決，而是過去在DNS安全系統和提出解決方案的討論不夠充分，若能有妥適的解決方案，則該方案才能得到良好的運作。此外，下世代物聯網編碼除了透過IMSI、OID作為唯一識別碼外，NDN也是國際上在討論用來作為物聯網編碼的規則，透過NDN命名直接通訊，不需轉換成地址，做物聯網更簡便，並可把安全性直接加入通訊中，提升其便利性及效率。另外，有關近年國際上在討論New IP的議題，Dr. Zhang認為物聯網關鍵問題在於經雲端運算所產生的通訊安全議題，而非New IP議題，之所以New IP被討論是基於商業考量，但若回歸到研究及技術層面上，則會較著重物聯網雲端運算之通訊安全。
- IETF會議指南：IETF為一個開放的組織，鼓勵該領域工程師及相關研究人員透過組織會議及社群交流互動，並提出相關解決方案，過去實體會議時，透過會後的互動及交流過程中，成員們可以獲得豐富的收穫。最近受到疫情影響，採用虛擬會議辦理，不可否認虛擬會議影響討論及交流的機會，然而本次IETF 111的Newcomers' Coffee Break是模擬會場環境，希冀能透過該模式，讓新進成員能有私下交流的機會。

- 回饋：目前IETF社群中，針對物聯網及物聯網定址相關討論主要有T2T RG工作小組、6LO工作小組和DNSSE工作小組，另外IETF最近有新成立「物聯網理事會」(Internet-of-Things Directorate)，該組織主要是跨IETF社群、跨外部組織的工作小組，以討論非物聯網協議工作中遇到的物聯網相關議題，建議研究過程中可多利用這些社群及資源。

二、強化技術能量及累積國際組織影響力

(一) 研究參與

為了蓄積本計畫的技術能量及提升專家學者之專業知識，專家學者分別參與本計畫研究工作及蒐集國際相關資訊，並透過參與國際會議中所蒐集的資料及重要議題，作為本計畫參考依據。有關專家學者參與及負責計畫工作內容如圖 5-8 所示。

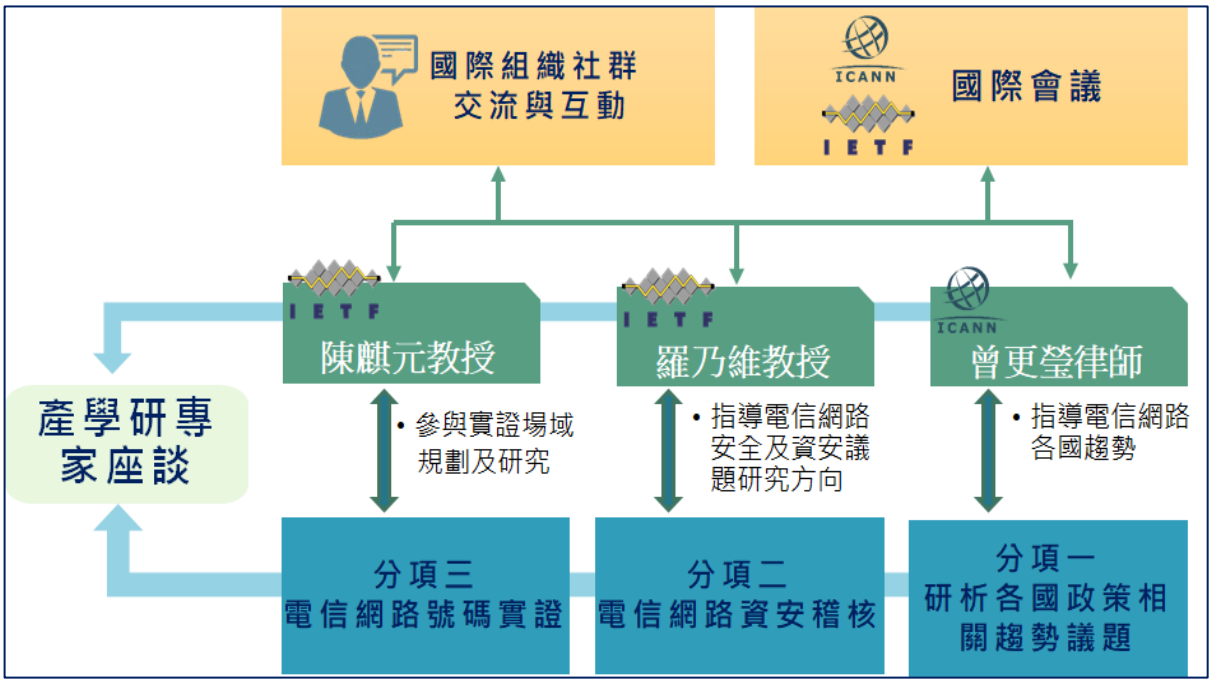


圖 5- 8、計畫參與分配架構

資料來源：本計畫製作

1. 參與觀測國際下世代電信號碼機制及各國政策發展研究

- 研究工作：下世代電信號碼技術及政策議題較為前瞻，且目

前國際著名組織 ITU、ICANN 仍不斷提出新興議題，國際建立及制定相關技術標準及政策預估仍須等待下世代電信號碼技術成熟，然而為超前部署下世代電信號碼技術與標準發展，本計畫借重曾更瑩律師在網際網路法律及電信法規等專業，研析網路分裂議題上 ICANN 與成員國可能主張的電信號碼方向，提供本計畫方向及建議。

- 蒐集及掌握國際相關趨勢：曾更瑩律師曾參與過 ICANN 相關會議，對該組織討論議題較為熟悉，因此本計畫由曾更瑩律師協助掌握及蒐集 ICANN 與成員國對下世代電信號碼之主張及最新趨勢，以作為本計畫參考依據。

2. 參與下世代電信號碼資安稽核研究

- 研究工作：有鑑於下世代電信網路議題衍生電信號碼資安稽核機制、系統安全及跨網互通安全議題等新興資安議題，本計畫由羅乃維教授參與下世代電信號碼資安稽核研析項目，借重羅乃維教授在雲端計算與安全、網路安全及資訊安全等專業，提供本計畫研析方向及建議。
- 蒐集及掌握國際相關趨勢：由於下世代電信號碼資安稽核屬於前瞻性議題，因此相關的標準規範國際組織也處於起草規劃階段，有鑑於羅乃維教授長期致力於研究資訊安全及網路安全等議題，對其相關議題熟悉且掌握其脈絡，因此本計畫請羅乃維教授協助掌握及蒐集國際下世代電信號碼最新趨勢，並提供本計畫研析方向建議，以作為本計畫參考依據。

3. 參與下世代電信網路號碼驗證機制研究

- 研究工作：有鑑於目前國際尚未有具體的電信網路號碼編碼機制，本計畫由陳麒元副教授參與下世代電信網路號碼驗證機制，借重陳麒元副教授在行動通訊、量子通訊之專業，協助依據現有的國際技術標準，評估行動物聯網 DNS 核配及

編碼方式、DNS 網路核配技術、DNS 編碼機制及 IoT 裝置 IP 自動核配驗證技術等。

- 蒐集及掌握國際相關趨勢：由於目前國際尚未有具體的電信網路號碼編碼機制，因此由陳麒元副教授協助掌握及蒐集國際下世代電信號碼最新趨勢，以作為本計畫參考依據。

(二) 座談會

為擴散國際電信號碼新知與發展，及建立我國技術與產業雙向交流平臺，促進我國技術與產業升級能量，及協助國內產業及早因應策略並進行市場布局，本計畫辦理三場座談會，座談會上安排專家學者擔任主持人，除藉由培育專家學者，希冀專家學者透過參與國際會議所獲得之新知及趨勢，能與參與座談會之專家學者、產業代表及各界代表分享，促進國內產學研技術交流，及擴散國際電信號碼新知與發展，進而提升我國技術與產業升級能量。

本次座談會主要有三個主題，分別為「下世代電信網路號碼與物聯網編碼趨勢」、「下世代電信號碼政策及資安機制」及「下世代電信網路號碼研究及 DNS 編碼技術概念性驗證成果」，這三場探討問題及交流成果如下表 5-10。

表 5- 10、 座談會議題及結論綜整表

座談會討論主題	綜整結論
第一場座談會	
從國際下世代電信網路號碼發展趨勢來看，對我國相關電信號碼規劃及使用上的可能影響為何？	● 在下世代電信網路發展趨勢下，應考量網路切片或網路虛擬化下的編碼機制。 ● 從我國電信編碼的發展來看，確實沒有針對物聯網設備的編碼機制或演算法，目前物聯網產品、

座談會討論主題	綜整結論
	各廠商通常有自己的標識和編碼方式，是否需建立設備的唯一性識別號碼機制，取決於法規對於物聯網產品的監管機制；若規劃未來採用新電信編碼制度，可能對既有用戶(含行動與固網市話)造成衝擊，例如新舊號碼(用戶) 如何互撥？是否需建置轉換平臺？業者既有設備是否能支援？等影響，建議研究單位及主管機關將其納入研究。 ● 未來可思考 ENUM/DNS 的特性來做電信號碼的規劃，可在既有的服務號碼不受影響下，新服務的號碼以較長的碼長配置或搭配更有彈性的接取碼指配，提升 E.164 號碼使用的容量及效率。
我國物聯網及電信產業應用及發展趨勢為何？	● 未來我國電信產業及物聯網發展將朝 5G 企業專網應用發展為主。 ● 短期或中期而言，4G 或 5G 仍會使用 2G、3G 電路交換核心網路提供 CSFB 語音服務，所以傳統的 E.164（MSISDN） 及 E.212（IMSI）均會存在，但 E.164（MSISDN）未來可能在沒有電路交換的核心 網路後逐漸消失。 ● 未來可思考 ENUM/DNS 的特性來

座談會討論主題	綜整結論
	做電信號碼的規劃，可在既有的服務號碼不受影響下，新服務的號碼以較長的碼長配置或搭配更有彈性的接取碼指配，提升 E.164 號碼使用的容量及效率。 ● 預期物聯網市場將在 AI、監控、企業專網服務、通訊、雲端科技、智慧醫療等應用領域持續發光發熱。 ● 預估在疫情過後，物聯網在軟體與服務等智慧應用領域將會出現顯著成長。
非 3GPP 標準下之 IoT 裝置(如透過 Wi-Fi 連線到 5G Gateway)，是否規劃編碼應用範圍？	● 物聯網編碼方式應考慮連接公眾電信網路（固定通訊網路或行動通訊網路），在網際網路上應用的物聯網服務，其使用之網域名稱與位址（IPv4 或 IPv6）的編製格式與現行網際網路上的各種應用服務須一致。 ● 物聯網應用廠商以 Gateway 作為連接中介，包括 Wi-Fi 及非 IP 應用（例如：藍牙），建議需探討兩者是否皆需納入監管及如何監管。最重要的是在法規上需清楚定義監管邊界，才可談如何及運用何種號碼方法來監管。 ● 非 3GPP 標準 IoT 裝置如透過 Wi-

座談會討論主題	綜整結論
	Fi 連線到支援 E.212 及 E.164 編碼機制之 5G Gateway 使用服務，行動網路僅能就前述 5G Gateway 之 E.212 及 E.164 編碼進行身分驗證、識別、提供服務及通訊監察，無法識別及管理經 Wi-Fi 接取之個別 IoT 裝置。 ● 未來若有新型態編碼規則，應能納入 3GPP 標準依循 3GPP 標準使用行動網路之 IoT 裝置，以確保 IoT 裝置 DNS 編碼可順利運行於行動網路（含跨境漫遊）。
物聯網應用的編碼需求與可用方案為何？是否有建立統一標準編碼之必要？ DNS 編碼是否能作為下世代物聯網設備編碼之解決方案？	● 基於電信網路與非電信網路都可以通用、大量查詢可以分散計算環境及可以快速分配與確認 ID 唯一性等理由，DNS 會是一個很好的建議方案。 ● 考量未來監管及資安需求，統一標準編碼有其必要性 ● 可將 DNS 編碼作為下世代物聯網設備編碼之解決方案列為考量，不過仍需參考國際標準做法。 ● 國外有 4G 業者擁有不需 MSISDN 的物聯網裝置，這些物聯網裝置經配對方式配對到號碼以控管 API。5G 牽涉到更多的物聯網，包括固網或行動裝置都希望可納

座談會討論主題	綜整結論
	入到同一 5G 平臺提供服務。因平臺集中更好控管，所以在制定規範時，建議可參照國外或者 3GPP 針對不同連接裝置的控管方式。 ● 未來產業趨勢將「電腦化」，而如何與其「溝通」則將是一重大課題。鑑此，將須制訂符合國內法規的統一標準制度，並尋求世界各業者與廠家共識以因應未來的電腦（物）互聯溝通使用。
第二場座談會	
針對國際下世代電信網路號碼技術發展趨勢，在5G技術發展下我國電信網路的通訊安全、裝置安全面臨之可能威脅與挑戰為何？	● 在電信管理法第5條，提供電信服務，且有與他電信事業進行互連協商或申請裁決、申請核配第 56 條規定以外之無線電頻率、申請核配設置公眾電信網路之識別碼或信號點碼及申請核配用戶號碼行為之一者，應向主管機關辦理電信事業之登記，其中申請核配設置公眾電信網路之識別碼、信號點碼及申請核配用戶號碼，為目前討論之編碼原則標的，換言之，在決定識別碼的範圍時，主管機關應有對應的管理措施。 ● 再者，有關E.164、E.212、DNS、NDN 等編碼，目前電信管理法分為兩種管制模式，一是「電信號

座談會討論主題	綜整結論
	碼核配及管理辦法」及電信管理法第 71 條，需由法人組織辦理，換言之，上述編碼規管力道較強。第二種是「網際網路位址及頂級網域名稱註冊管理業務監督辦法」，為公私協力治理的方式，兩種規範之規管強度不同，而未來是否會有第三種管制方式及何種管制模式，提供後續議題討論。 ● 另外，過去 DNS、NDN 域名的名稱本身可能具有意義(或是具有商標名稱)，因此涉及到智財權的爭議，建議將該議題納入研究方向。 ● 最後建議從資安角度，觀察歐盟近期更新 NIS2 修訂草案，歐盟將 DNS 納入政府監管及查詢措施，這部份建議可納入研究議題。
我國下世代電信網路號碼技術發展下之政策建議為何？	● 更加關注相關國際組織(ITU、IANA(PTI)、ICANN)在該議題的討論，以利作為我國下世代電信網路號碼技術發展之政策參考。
下世代電信網路安全與稽核重點探討：跨網互通(切片內網、外網)、OT、工控系統、IoT 物聯網應用場景的資安需求下，建議的	● 跨網互通，外網到內網仍需要縱深防禦及避免單點失效造成營運中斷，外網相關資安防禦設備、內網區隔及備援機制等，可採用

座談會討論主題	綜整結論
稽核重點為何？	識別、偵測、防護、應變四個構面去思考，並在設備部署事前、事中、事後階段建立管理制度。 ● OT 及工控系統可依照業務屬性做適當區隔，OT Gateway 端的防禦機制及偵測、OT 設備白名單機制、降低非授權軟體使用，從 OT 設備制定設備資安檢查清單，如惡意程式檢測，推行實驗室資安設備檢測標章機制，OT 設備部署前再執行資安測試確認，測試通過後再移轉至營運區降低風險，定期設備資安檢測配合軟體白名單機制可大幅度降低營運衝擊。 ● 網路切片應有其對應安全分級與對應級別之安全的網路隔離、分片隔離、功能隔離以及資源隔離。 ● 網路切片所存取之 Network Function 應具有存取權限限制、服務之間的認證與授權、過濾以及 SCP(Service Communication Proxy)。 ● 網路切片應設有存取限制、對應切片的身分驗證、切片資源分配限制、流量規則與政策。
不同網路需求下之資安稽核概念	● 先行概述資安稽核概念之間的目

座談會討論主題	綜整結論
援用：ISMS 與 I(A)CS、SCDA 之間的關聯、管理概念是否可相容與交互應用？可如何引用適用？	的及差異，首先 ISMS 的核心精神是 PDCA 循環檢核及改善的過程(Plan-Do-Check-Action)，其目的是改善流程及管理品質；而 IACS(Industrial Automation and Control Systems/工業自動化和控制系統)目的是確保工業控制設施的各種運作具有可用性和安全性；SDCA(Standardize-Do-Check-Action)則是標準化和維持穩定運作的流程；PDCA 是使企業管理效能不斷提升的驅動力；SDCA 則是防止企業管理效能下滑的制動力；IACS 則是確保整體企業運轉的可靠性及安全性，這三者可以組成穩定(IACS)-改進(PDCA)-維持(SDCA) 的工作循環，可以讓企業不斷穩定地向上提升。沒有標準化措施，企業就無法維持在較高的管理效能。
第三場座談會	
下世代電信網路具有網路虛擬化及網路切片等特性，對物聯網編碼使用產生影響為何？	● 有影響： (1) 5G 專網是促進數位轉型以及運作更有效率的方式。 (2) 德國在 2020 年就開始討論 5G 專網的 IoT 聯網設備應如何管理及編碼，進而對提供 IMSI 作為管理

座談會討論主題	綜整結論
	機制議題提出討論。 ● 無影響：網路虛擬化及網路切片對物聯網編碼使用應無影響，3GPP 及 GSMA 標準已制定網路切片之編碼計畫，提供端到端網路切片識別之用途。
固行網融合的趨勢對電信編碼機制需求及影響為何？	● 現行固、行網分開的架構所提供的服務一樣，使用相同的電信編碼機制需求。因此，不影響目前的電信編碼。 ● 目前國內電信編碼仍具備識別服務及費率的功能，若未來國內出現新型態固行網融合的服務及計費，才有新的編碼需求。
在網路虛擬化及網路切片的管理上，是否需依據服務的重要性制定一致的電信號碼編碼規則(例如涉及關鍵設施)？	● 3GPP 及 GSMA 標準已依據服務重要性制定一致性之網路切片(eMBB、URLLC、MIoT 及 V2X)及服務 QoS (5QI)等編碼計畫，應無需針對網路虛擬化及網路切片管理再另訂一致的電信號碼編碼規則。 ● 關鍵基礎建設可以視為是不同專網場域，也就是不同網路切片，建議在涉及關鍵基礎設施部分可考慮規劃建立電信號碼編碼規則。
DNS 編碼註冊、分配及存儲系統	● 目前我國相關法規並未對網域名

座談會討論主題	綜整結論
之管理上是否納入關鍵基礎設施(CI)管制？在管理上如何依據其重要性，以選擇由主管機關管制、公私協力或業者自律？	稱系統的運作與管理上有細部的法規限制。 ● 建議組成 DNS 營運機構組織或是協會，透過行業的自律及稽核機制，健全整體 DNS 的解析環境

資料來源：本計畫製作

(三) 經驗傳承及分享

本計畫為使研究團隊(專家學者及研究人員)熟悉 ICANN 及 IETF 等國際組織運作、掌握國際組織討論議題及熟識國際組織人員，因此邀請曾擔任或參與國際組織之重要幹部，辦理 3 場經驗分享會議，經驗分享會議講師及主題如表 5-11，除了將經驗傳承外，希冀透過經驗分享會講授國際組織相關專業知識及建立資源鏈結。

表 5- 11、經驗分享會主題場次表

主講人	經歷	主題
沈信雄	電信政策國際會議參與經驗	電信編碼技術發展趨勢暨國際會議經驗談
	號碼網域管理業務經驗	
吳國維	中華電信股份有限公司董事	ICANN 組織參與實務經驗分享與討論
	前 NII 產業發展協進會執行長	
	前 Public Interest Registry 董事	
黃勝雄	臺灣網路資訊中心(TWNIC)執行長	IETF 組織參與及國際電信編碼趨勢
	亞太網路資訊中心(APNIC)董事	

主講人	經歷	主題
	亞太網路治理論壇委員	
	亞洲(.asia)頂級網域註冊管理局諮詢委員	

資料來源: 本計畫製作

三場經驗分享會依據講者的經驗及熟悉的國際組織，講授的內容有所差異，但主要經驗分享會講述題綱著重 4 點：

- 講述目前國際下世代電信號碼機制發展趨勢及關注議題，以利掌握國際在電信號碼議題之研析方向。
- 國際電信號碼相關會議參與經驗及如何主導國際標準制定之策略。
- 對於政府於此領域投入人才培育規劃之看法或建議。
- 培育出我國具備參與相關國際標準制定工作及可擔任該等組織重要幹部之專家學者所提升的能力及策略。

依據上述講述內容，本計畫綜整成果如表 5-12。

表 5- 12、經驗分享會內容綜整表

項次	內容
國際電信號碼相關會議參與經驗及如何主導國際標準制定之策略	1. ICANN 參與策略： • 依據參與 ICANN 的經驗，應先多聽多看多參與會議，並熟悉及熟讀組織的相關規章、實際參與了解會議如何操作、與各國代表交流，將會議內容帶回來，討論我們能深入組織的機會。 • 多參與 ICANN 會議及社群交流，並積極投入社群會議，有助於獲得國際組織成員支持。

項次	內容
	• 建議參與 ICANN 組織或交流時，仍是以政策或網際網路治理相關問題為主。 2. IETF 參與策略： • 從現實面來看，臺灣在資通訊產業很強，廠商在設計能力很強，但他們在國際標準制定無太多涉略，此外國內學界也未將發表 IETF 的 RFC 作為升等的績效，因此建議國家政策應調適，並設計政策誘因，以利推動及鼓勵廠商、學研單位參與 IETF。 • 根據過往發表 IETF RFC 的經驗，制訂國際標準不太可能是單一國家或單位提出想法、聚集相關利害關係人、爭取支持、界定反對者有哪些、突顯問題顯著性，相關利害關係人需要一起合作，方能順利制訂出具利害關係人支持的 RFC。 • ICANN 若有實際技術問題時，會諮詢或參考 IETF 草案或文獻，因此若要討論技術或進行技術交流，建議仍是回到 IETF。
對於政府於此領域投入人才培育規劃之看法或建議	1. ITU 會議通常皆需查看護照，持臺灣護照無法進入會議會場。另外參加 ITU 的方式，若是以個人名義，或是有些會議場次對與會人員資格要求無特別規範，是可以參與會議的，並不是特別困難，但這樣的方式並不是所謂的進入 ITU 組織。 2. IETF 政治介入相對難度低，所以考量技術與可落實性，IETF 相對來說是可多加參與的國際組織；另外，人才培育規劃的藍圖部分比

項次	內容
	較薄弱，不能僅依靠單一部會，因此建議人才培育可與外界技術單位、國外技術單位合作才能有較好的成效。
培育出我國具備參與相關國際標準制定工作及可擔任該等組織重要幹部之專家學者所提升的能力及策略	1. 選定人才培育的人選是成功的第一步，不論參與 IETF 或 ICANN 基本上都是志願性質、無給職的工作，因此若與人才培育的專家學者生涯規劃及工作領域相關，則能有提升專家學者專業能力之機會。 2. 建議鎖定 IETF 與本計畫主題相關社群參與，方能深入參與及建立社群互動。

資料來源：本計畫製作

三、人才培育短、中、長期參與策略及效益

本年度計畫透過參與 ICANN、IETF 等 4 場國際組織會議、7 場培訓課程(含 3 場經驗分享會及 4 場會前培訓會議)、3 場座談會及多次與國際組織交流，提升我國專家學者對國際下世代電信網路號碼討論議題的認識，此外本計畫透過曾擔任國際組織幹部者之建議及相關量化數據，作為本計畫擬定培養我國參與國際標準制定工作及可擔任該等組織重要幹部人才之策略方向、執行內容及績效指標。

(一) 短期策略及效益

1. 組建產官學研專業團隊

依據今年度執行成果及專家學者建議，為有效延續本案的技術能量及政策效益，未來應組建一個由官、學研共同組成的專業團隊。專業團隊應有政府部門之常任事務官，以利掌握政府政策及議題發展方向，並且在專家學者與國際組織交流互動時，扮演政策溝通之掌舵者角色，除此之外，若有常任事務官參與本計畫，可避免其技術能量及研究成果掌握在研究團隊，導致其研究能量

無法傳承及延續。

組建產官學研專業團隊之目的及分工如圖 5-9 說明：

- 法人/產業等單位：由於法人或法人主要可透過了解產業趨勢，以扮演政府政策及擔任政府智庫之角色，此外，官方代表若參與較具有敏感性之會議時，可藉由法人/產業單位，消弭具政治敏感性之會議，換言之，法人單位除了協助政府機關研究相關議題外，還可協助政府機關執行高度政治化之議題，與國際組織或國外團體交流時較具有彈性。
- 政府單位：組建產官學研專業團隊中，主要政策決策者為政府機關，因此在專業團隊中政府單位是專案執行的掌舵者，以及透過常設事務官作為技術決策、指導及政府政策目標之橋梁。此外，由於政府部門的業務輪調及人力流動相較學研單位較低，而考量下世代電信網路號碼技術強調能量及技術積累，透過蓄積技術能量、累積歷年成果，方有助於政府政策目標之達成，因此建議需納入政府固定事務官加入團隊研究。
- 學術單位：學術單位之角色及功能主要在技術(實作)及學術研究方面，由於下世代電信網路號碼技術議題較為前瞻及創新，需透過技術實作及學術研究匯聚研究能量，除此之外，本計畫考量國際組織(如IETF)參與需長期投入及向下扎根，否則計畫結束後，過去累積之能量或是在國際組織培養之能量就無法延續，實屬可惜，因此透過培養莘莘學子參與國際組織，有助於延續我國投入國際標準組織之參與能量。



圖 5- 9、組建專業團隊架構圖

資料來源：本計畫製作

在標準組織活動之參與需依賴技術團隊的堅強研發能量為後盾，因此需有學研機構例如財團法人形式的研究機構的專業人員，以作為研究及政策智庫之角色，透過雙方合作相互支援的團隊，針對下世代電信網路號碼議題及制定標準進行充分討論並與各國際組織討論與表達意見，以專業化的形象提升本團隊在國際標準組織的影響力與能見度。

此外，團隊的工作主要分為兩大項，分別為與技術相關之研究及標準活動參與，兩者工作內容相輔相成並相互合作。

2. 提升技術能量

在研究團隊技術能量累積之策略上，依據技術發展的趨勢選擇或調整參與的標準組織。今(110)年度著重參與 ICANN 及 IETF，未來持續觀測國際組織在下世代電信網路及物聯網編碼議題的國際標準制定單位，需滾動式調整參與目標。

本計畫目標在培養參與相關國際標準制定工作及可擔任該等組織重要幹部之專家學者，因此依據前述針對 ICANN 及 IETF 兩個不同性質的國際組織，評估不同目標。其主要策略及國際技術交流能量為：

(1)培養參與IETF國際標準制定工作：IETF為技術性國際組織，因此該組織以培養參與相關國際標準制定工作為目標。根據

第一年參與IETF評估，目前「物聯網唯一識別碼自動配置」、「電信網路與網際網路介接」、「DNS系統安全」等議題為未來下世代電信網路號碼技術下熱門及制定國際標準之方向，事實上該研究方向仍會隨著國際技術發展有所變更，但至少確定有助於標準制定及國際互動交流方向之議題。在鎖定及觀察下世代電信網路號碼相關技術標準議題後，專業團隊在第二年進行技術研究、技術提案、成果發表以及會議或Mailing lists討論與意見表達工作。同時要熟悉國際標準化之運作過程與建立人脈，並同步將最新技術趨勢、產業發展策略及市場重要訊息攜回專業團隊內部討論，取得共識，使專家學者能充分代表官方立場後續參與及推動我國資訊外交之政策原則。如上所述，國際標準組織參與團隊，主要負責兩項工作。第一項為標準相關之技術研發工作，包含撰寫國際標準會議技術貢獻、參與技術貢獻議題之討論、協助技術貢獻提案分析評估，並依實際需求參與國際標準組織會議。

(2) 培養ICANN幹部：ICANN為政治性之國際組織，該組織主要為全球網路順暢運作及協調管理的重要網路國際組織，以多方利益共同體(multi-stakeholders)的參與模式，由下而上、匯集及採納所有不同社群意見制定政策[240]。ICANN社群及支援組織眾多，而本計畫研議及分析各社群，鎖定培養未來擔任ICANN GAC副主席、ALAC諮詢委員、SSAC 委員。挑選這3個社群之理由及策略如下。

- ICANN GAC副主席：政府諮詢委員會GAC的成員主要來自世界各國/地區政府之代表，而出席GAC會議成員也包含各種全球性組織，例如國際電信聯盟(ITU)、經濟合作與發展組織(OECD)，因此鎖定參與該委員會之目的為了解各國在

[240] TWNIC，ICANN 組織簡介（二），台網中心電子報，2017 年 8 月，http://www.myhome.net.tw/2017_08/p08.htm（最後瀏覽日：2021/11/10）

公共政策問題上向ICANN提供之建議內容，並透過與該成員國互動，掌握各國及各國際組織在下世代電信網路號碼技術之立場。爭取擔任ICANN GAC副主席之效益除能代表我國爭取及遊說對我國有利之法規或議題之外，也有機會透過該職位與國際其他政治性組織交流。

依據ICANN GAC運作原則GAC副主席係由選舉產生，任期一年，可連選連任，而副主席條件為應盡可能適當體現成員在地域和發展方面的多樣性[241]，據此規劃爭取擔任ICANN GAC副主席之策略。該策略為派選一位具有政府官員代表身分之人選，並且積極參與ICANN每年年會，以及積極在每次工作小組會議出席及發表意見，進而建立在GAC的話語權及建立人脈。此外，在選舉副主席期間，可積極拜訪他國代表，以了解其他國家代表需支持之議題，建立議題結盟之機會，爭取其他國家代表之支持。

- ALAC諮詢委員：ALAC是類似於ICANN的民意機構，ALAC之職責是考量及維護網際網路個人用戶的利益，以及關注用戶的意見及社群觀點，參與該組織委員主要目的是政治性考量，由於GAC副主席一職需要由來自世界各國/地區政府之代表選舉產生，而我國國情特殊，在國際上受到中國大陸打壓或阻擾情形屢見不鮮，為爭取參與國際組織及維護我國在國際上影響力及話語權，建議長期及積極爭取ALAC諮詢委員，該社群委員由15名成員組成，其中10名直接由各區域網際網路用戶投票產生，而非由來自世界各國/地區政府之代表選舉產生，在此情況下，可以透過鼓勵及動員網際網路用戶支持我國專業人員。

  依據ICANN ALAC程序規則，ALAC由15名成員組成諮

[241] ICANN, About the GAC- Operating Principles. https://gac.icann.org/operating-principles/operating-principles?language_id=11（最後瀏覽日：2021/11/08）

詢委員會，其中10名諮詢委員是每一ICANN區域選取2名。此外，訪談網路中文股份有限公司說到，由於ICANN等國際組織對於女權保障意識日漸升高，雖然沒有明文規定委員會兩性比例，但據此規劃爭取擔任ALAC諮詢委員之策略，人選建議為女性，並且建議具有法律或律師背景，此外該人選應積極參與ICANN每年年會，以及積極在每次工作小組會議出席及發表意見，以獲得ALAC利益相關者的認同。

- SSAC 委員：SSAC網路安全穩定諮詢委員會，根據《ICANN章程》第12.2(b)條明文，SSAC會針對網路名稱與位址分配系統之安全性、完整性事宜，向ICANN社群與ICANN董事會提出建議，此外，SSAC也會參與網際網路命名和地址分配服務的安全威脅、風險分析進行評估，以確保網際網路域名之營運、管理與註冊的穩定與安全等。[242]

SSAC共33名委員，任期三年，得連選連任，且得無限制連任。於ICANN董事會中，具無投票權一席。SSAC委員申請流程如圖5-10，而選任期間通常在每年4月至6月，可由志願者自行向SSAC申請或是由SSAC成員推薦，候選人須在兩周內繳交相關資料及文件，SSAC成員審核通過後，會進行面試，面試通過後會送交ICANN董事會決議任命。然而，若未獲選者，自申請後的12個月內不得再次申請。

[242] ICANN, Security and Stability Advisory Committee(SSAC). https://www-icann-org.translate.goog/groups/ssac?_x_tr_sl=en&_x_tr_tl=zh-TW&_x_tr_hl=zh-TW&_x_tr_pto=nui,sc（最後瀏覽日：2021/11/08）

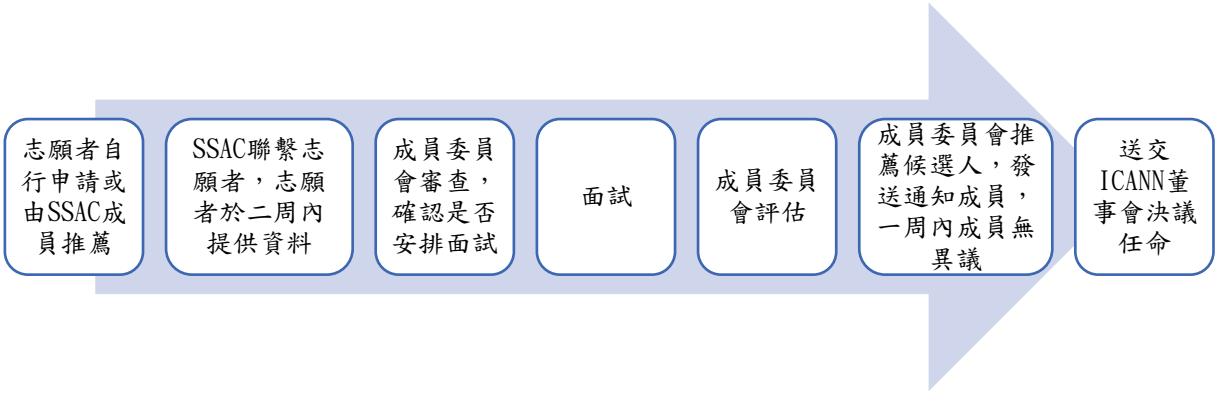


圖 5- 10、SSAC 委員申請流程

資料來源：本計畫製作

第二年之策略為爭取參與社群事務及在社群提出技術討論(Mailing lists)，因此第二年培訓課程辦理重點為「國際標準編寫原則」，將第二年的研究成果編寫為IETF技術標準草案，並且透過INT社群的Mailing lists進行討論，換言之，該課程辦理的主要目的，是可實際產出一篇技術草案，並將研究產出之成果與國際組織社群進行交流。

此外，由於適逢COVID-19疫情流行之際，線上虛擬會議有可能成為主流，然而透過今年參與虛擬會議發現，現在虛擬會議之參與策略及演講方式與實體會議具有差異，為使專家學者能掌握虛擬會議參與者的共鳴及建立交流互動，第二年也將安排「會議參與策略實務」課程，以因應未來可能再次參與ICANN線上虛擬會議成果發表之情形。此外課程培訓將另外安排國際談判及會議禮儀，例如「雙語協商與談判」，今年度訪談交通部鄧添來前司長，根據其經驗國際協商與談判之情境多元，必須不斷訓練及模擬多種情境，除此之外，我國國際地位屢次受到中國大陸打壓或阻擾，中國大陸官方經常透過正式國際會議或是私下請他國遊說之方式，干擾我國代表在國際組織之參與，因此，我國專業人員代表更應該在平時加強協商與談判技巧。

(二) 中期策略及效益

1. 擴大國際組織社群參與

第三年人才培育除延續先前組建官學研專業團隊外，為延續下世代電信網路號碼技術能量，第三年將著重納入學界人才。根據今(110)年本計畫參與兩次 IETF 發現，我國除本計畫研究團隊及 TWNIC 之外，僅有少數學生及業界工程師參與，換言之，臺灣目前較沒有技術能量或是參與 IETF 標準制定的人員與能量。訪談友訊科技股份有限公司劉明翰處長表示，臺灣目前資通訊產業對於制定 Layer 層或是網際網路相關技術標準較不具備誘因，通常產業都是按照已制定的國際標準生產相關網通設備。另外訪談 NII 產業發展協進會前執行長吳國維表示，臺灣學界因參與 IETF 無法併入升等之績效，導致我國學界長期沒有投入在 IETF 技術標準制定。

倘若我國政府希冀透過推動培育 5G 跨域人才，培育 5G/B5G 技術之頂尖研發人才及 5G 跨域應用人才，以利厚植未來學研界與產業發展，參與 IETF 國際組織及交流討論是掌握行動通訊技術與標準發展趨勢、早日佈局之關鍵參與方式，因此本計畫第三年預計辦理 IETF 相關實務程式競賽或是研習營，主要參與對象鎖定學界及學生，鼓勵學生投入參與 IETF 會議，此外 IETF 定期辦理 Hackathon， Hackathon 可鼓勵開發人員透過實作方式開發實用程序、解決方案等，以展示 IETF 標準實際實現的方式，而在參與 Hackathon 的過程中，學生可與其他國家的專家學者、工程師共同合作及討論解決方案，進而擴大交流互動及技術累積的能量。

2. 強化技術能量

(1) 國際技術交流合作：

技術交流及互動是強化及累積技術實力或人脈建立的方式之一，然而訪談 IETF 資深研究員 Dr. Zhang 表示，觀察到亞洲地區的研

究人員或是學生，欠缺交流及互動的能力，因此第三年人才培育的重點也將著重在強化國際技術交流，透過強化 Mailing list 交流，在 Mailing list 積極發言及發表技術相關討論內容，並爭取國際不同研究單位在同一領域及議題的合作，建立一個跨國的研究小組，作為互動及交流的實質成果目標。

(2) 辦理實作研習等活動：

為配合擴大國際組織社群參與之策略，第三年培訓課程除延續「國際標準編寫」、「會議參與策略實務」及「雙語協商與談判」以強化國際標準制定及技術能量外，第三年將著重在辦理 IETF 程式競賽或研習營，其主要目的為鼓勵大專院校學生參與及瞭解 IETF，希冀學生能於在校時培養參與技術標準與程式競賽之興趣，並使 IETF Hackathon 作為學生挑戰自我及發揮技術實力的殿堂。本計畫第三年延續前年度在 Mailing list 參與討論之相關議題，並結合議題辦理 IETF 程式競賽或研習營，透過實作將下世代電信網路擬制定之技術標準作為研究技術實作之可行性評估。

(三) 長期策略及效益

1. 增進國際參與

為因應未來國際政治環境、國際資通訊發展，本計畫僅提供框架性執行內容。若依據歷年執行成果、投入長期資金、選定具有意願及生涯規劃相符之人員、有固定研究團隊參與，第四年執行內容將延續前幾年人才培育執行成果，著重爭取擔任國際組織幹部及爭取與其他國際成員共同參與技術標準草案，並且鎖定在尋求與國際合作發表技術標準研究成果。

- 爭取擔任國際組織幹部：持續爭取擔任 ICANN ALAC 委員或 ICANN GAC 副主席一職，並盤點歷年所累積的資源(各國人脈、所建立的聯盟及共同支持的議題)，並強化所累積之資源，遊說及動員利益關係人支持我國專家學者。

- 爭取與其他國際成員共同參與技術標準草案：綜整研究團隊歷年在 IETF Mailing lists 討論議題，及觀察國際上對網際網路技術之發展，並爭取與其他國際成員共同參與技術標準草案，希冀透過與國際成員共同制定或參與技術標準草案，能快速掌握未來下世代電信網路號碼技術標準，進而促進我國產業能即早因應技術標準。

2. 深化技術能量

為增進國際組織社群參與之策略，第四年培訓課程除延續「會議參與策略實務」及「雙贏協商與談判」外，將辦理「進階國際標準撰寫」課程，深化我國撰寫技術標準之能量，並藉由辦理課程，鼓勵及增進專家學者撰寫國際技術標準能力。

第四節　小結

下世代電信網路號碼技術仍處於發展階段，針對電信物聯網環境編碼方式仍有多方討論。傳統公眾電信網路（PSTN）乃以採用 ITU E.164 編碼標準為主，具備國際通用、容易記憶及穩定性高等優點；而在網際網路領域，國際間則是採用 ICANN 所定義的 DN 編碼，其優點為擴充彈性大、可呈現直覺判讀訊息、利於異質網路間互通。此兩種編碼方式都行之有年，具備不可取代的優點和特性，預期將會是下世代電信編碼兩大主流技術，因此各國皆持續關注 ITU 及 ICANN 相關議題之發展；此外，「物聯網唯一識別碼自動配置」、「電信網路與網際網路介接」、「DNS 系統安全」及「網路切片編碼」等議題是新興技術發展下同步產生的議題，因此參與 ICANN、IETF 等國際組織，尋求與國際單位或組織合作研究及制定技術標準的機會，有助提升我國技術能量及促進國際參與，並協助國內產業及早因應以進行市場布局。

一、人才培育之重要性

下世代電信網路是以硬體及軟體結合的全新技術架構，電信網路

採用許多原本網際網路的技術，因此網路需要運用大量的虛擬開發及整合測試，網際網路與電信網路之間的界線正逐漸消失，依據 Network 2030 的觀點，在該趨勢之下，如果沒有跨行業、跨部門的合作，未來的網路技術部署無法協調發展，並將導致網路性能、故障、孤立、阻礙數位發展、降低生產力及破壞消費者信心等[243]。因此該報告建議，產、官、學研應該建立跨夥伴的合作架構，以統合未來網路技術發展資源及設施。

為對應下世代嶄新的電信環境，未來將會出現相對應的新型人才需求，因此，培育相關電信編碼人才的重要性同樣不言而喻。為滿足5G產業發展需求下的5G技術與應用人才，透過參與國際會議及與各國專家學者交流之成果回饋於本計畫各研究分項，並分享及擴散至相關產業界，以促進我國 5G IoT 與網路切片相關產業技術與國際接軌，並協助國內產業及早因應及進行市場布局，進而提升我國相關產業自主研發能力。

二、規劃與執行成果

為深入了解相關國際組織針對 5G/B5G 及網路切片進行的電信號碼編碼研究（Telephone Numbering Plan），本計畫今年度由 3 位專家學者及研究團隊成員組成專業團隊，如圖 5-11 之國際會議參與回饋流程圖所示，透過研究團隊參與 IETF、ICANN 等有關 5G/B5G 及新興無線通訊之國際組織會議及活動，並將參與國際會議所蒐集到的資料及重要議題作為本計畫研究參考。

[243] Network 2030 A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyon, ,2019. https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/White_Paper.pdf（最後瀏覽日：2021/9/6）

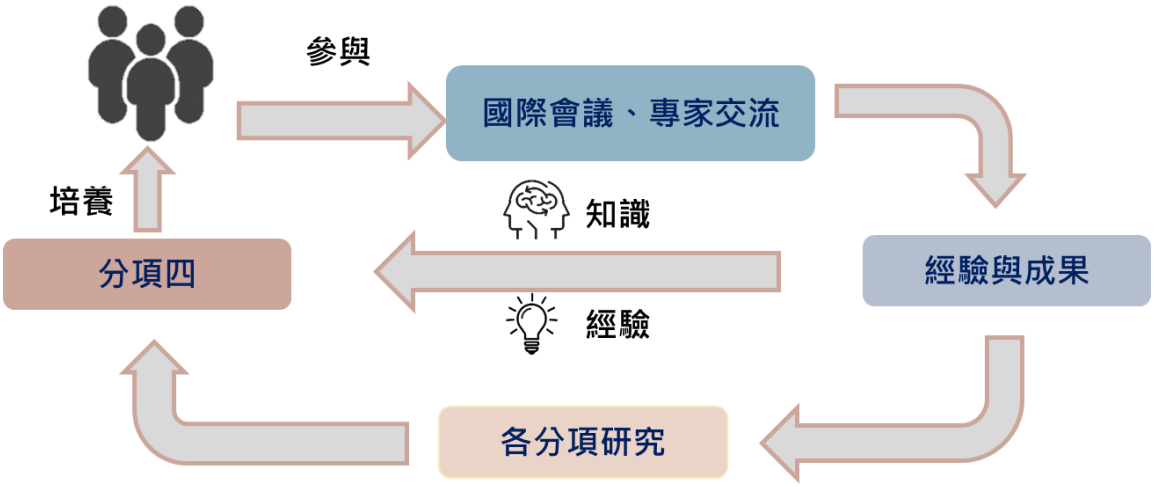


圖 5- 11、國際會議參與回饋流程圖

資料來源：本計畫製作

今年(2021)透過曾更瑩律師指導各國下世代電信網路號碼技術及政策發展趨勢，並將國際會議參與成果回饋及投入本計畫分項一「下世代電信網路號碼技術及政策」、羅乃維教授指導電信網路安全及資安議題研究方向，並將國際會議參與成果回饋及投入分項二「下世代電信網路號碼資安稽核」及陳麒元副教授參與實證場域規劃及研究，協助指導分項三「下世代電信網路號碼驗證機制」。

另外，本計畫已辦理主題分別為「下世代電信網路號碼與物聯網編碼趨勢」、「下世代電信號碼政策及資安機制」及「下世代電信網路號碼研究及DNS編碼技術概念性驗證成果」3場座談會，會議邀請產、官、學研交流經驗及推廣國際會議的相關新知。

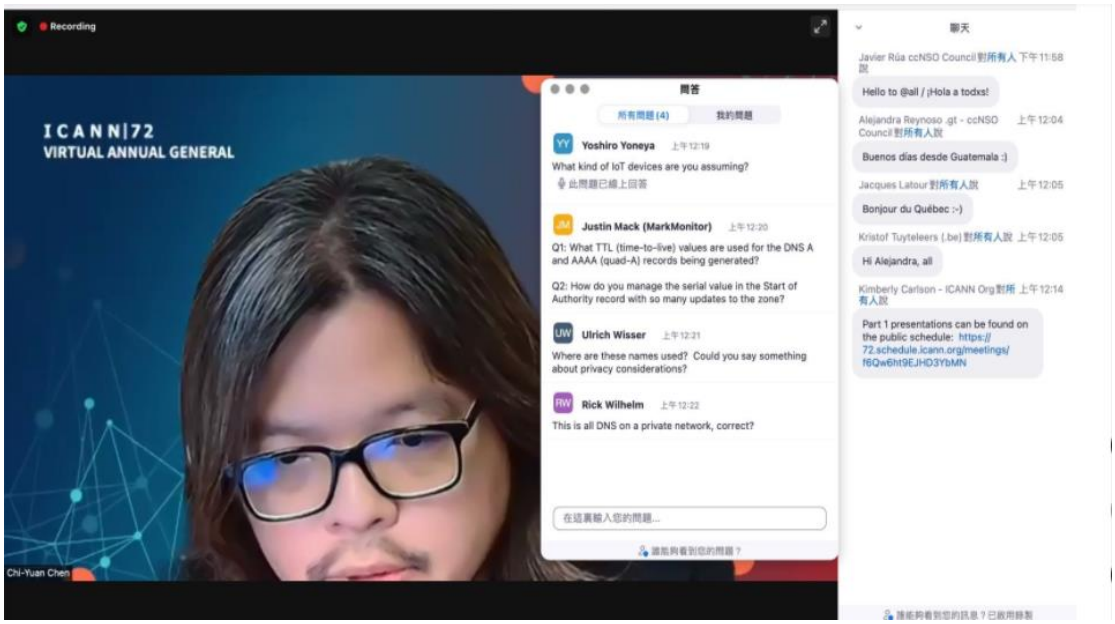


圖 5- 12、ICANN 72 會議成果發表

資料來源：本計畫製作

此外，為將本計畫分項三 PoC 研究成果與國際組織交流及討論，並使 DNS 物聯網編碼技術在國際組織倡議及推廣，今年度請 3 位人才培育專家學者之一—國立宜蘭大學陳麒元副教授至 ICANN 72 的 Tech Day 發表「PoC of DNS identifier」（DNS 識別碼的概念性驗證），成果發表會如圖 5-12。本次成果發表會，提出 DNS 識別碼自動命名及定址的物聯網設備，使下世代電信網路環境可自動化、大量及多元管理物聯網設備。此次成果發表在簡報結束後，有許多與會專家學者針對本實驗之設備、環境等提問，初步在國際交流上取得重大進展。

承上述，今年度人才培育在參與國際會議、辦理座談會、經驗分享會及會前諮詢會議上皆分別取得質化及量化的實質成果。在會議辦理方面，今年度辦理 3 場座談會，共計 178 人次參與，並辦理 3 場經驗分享會及 4 場 ICANN 與 IETF 會前諮詢會議，在國際會議參與及國際組織交流上，今年度共參與 5 場國際會議，包含 ICANN 71、ICANN 72、IETF 111、IETF 112 及 ITU Digital World，並辦理一場 IETF 交流會議及與 ICANN IROS 進行多次書信交流，其人才培育成果質化及量化請參

閱表 5-13。為提升我國專家學者對國際下世代電信網路號碼討論議題的認識，並掌握培養我國參與國際標準制定工作及可擔任該等組織重要幹部之策略。

表 5- 13、人才培育成果質化與量化綜整表

項目	質化成果	量化成果
國際會議	ICANN 71、ICANN 72：本次參與ICANN 71及72成果包含獲取新知、會議交流及挖掘未來參與社群。 • 獲取國際新技術及規範新知：參與2場ICANN會議，其中「歐盟網路安全原則性措施之指令草案（NIS2）」、「網路犯罪公約（Convention on Cybercrime）」、「零接觸通用IoT裝置識別（Zero-Touch Universal IoT Device Identity）」等3篇報告為與本計畫內容相關之國際發展新知。 • 會議交流：本計畫成果在ICANN 72 Tech Day發表「PoC of DNS identifier」（DNS識別碼的概念性驗證），展示DNS識別碼機制；簡報結束後有許多專家學者針對本實驗之設備、環境等進行討論及交流。	共參與5場次國際會議
	IETF 111、IETF 112：本次參與IETF 111、IETF 112，由於IETF為技術性的國際組織，討論議題專業且技術性高，本次參與成果為提出參與建議及鎖定議題及工作小組。 • 本計畫與物聯網編碼有關，因此鎖定參與IETF INT領域之工作小組。 • 積極參與IETF Mailing list討論：由於IETF 會議僅是報告每個工作領域或工作小組之技術草案進度，因此報告時間大約5分鐘，透過參與會議獲得新知有限，未來若長期且先行在Mailing lists討	

項目	質化成果	量化成果
	論，除了可增進交流互動外，較有助於獲取新知。	
	ITU Digital World：本次參與「未來5G網路及標準發展會議(5G: fueling digital transformation today - or tomorrow?)」及「未來網際網路、有線網路及無線網路發展趨勢(Wired, wireless, worldwide: what's next for networks?)」，透過本次會議掌握目前下世代電信網路號碼技術發展，未來電信探討面向為：(1) 5G網路趨勢將朝向AI化、自動化及大量物聯網應用(2) 低軌衛星發展可能有助於弭平數位落差，因此未來國際將著重發展低軌衛星。	
國際交流	1. IETF交流會議：本年度IETF交流會議對象為美國加州大學洛杉磯分校(University of California, Los Angeles)的IETF資深會員Dr. Zhang，會議成果為： • Dr. Zhang提出在物聯網編碼技術上，NDN也是國際上在討論用來作為物聯網編碼之規則，透過NDN命名直接通訊，不需轉換成地址，做物聯網更簡便，並可把安全性直接加入通訊中，提升其便利性及效率。 • IETF最近有新成立「物聯網理事會」(Internet-of-Things Directorate)，該組織主要是跨IETF社群、跨外部組織的工作小組，以討論非物聯網協議工作中遇到的物聯網相關議題，建議研究過程中可多利用這些社群及資源。 2. ICANN IROS書信交流：與ICANN IROS之交流中，其提供幾篇與本計畫相關之報告，分別為《Non-IP Networking (NIN)》、《New IP》、《5G	IETF交流會議1場次及ICANN IROS書信交流

項目	質化成果	量化成果
	Technology》。	
座談會	今年度分別針對電信網路號碼及物聯網編碼、電信號碼政策及資安機制及 DNS 編碼技術及成果等議題辦理3場座談會。為推廣新知及協助國內廠商進行市場布局，3場次內容包含： ・IETF 國際組織及技術標準制訂介紹 ・下世代電信網路號碼趨勢 ・DNS 物聯網編碼技術及實測說明	座談會共計辦理3場次，共計178人次參與
計畫研究	本計畫今年邀請國立臺灣科技大學資管系羅乃維教授、國立宜蘭大學資訊工程系陳麒元副教授、理律律師事務所曾更瑩律師3位專家學者，透過參與國際會議及活動提供未來制訂技術標準方向、參與ICANN及爭取幹部一職之建議及指導分項三PoC實證驗證，其成果說明如下： ・ 透過參與IETF及研究發現「物聯網唯一識別碼自動配置」、「電信網路與網際網路介接」、「DNS系統安全」等議題將是未來下世代電信網路號碼技術下熱門及制定國際標準之方向。 ・ 建議人才培育對象應由政府部門的常任事務官、學界的學者、財團法人等三方組建專業團隊，學界主要是進行技術研究，法人單位主要是政策法規研究及政府智庫的角色，透過學界及法人單位代表政府機關參與國際會議。而希冀將政府官員納入團隊，主要是由於常任事務官變動及更替的頻率相對不高，透過政府主導，有利於掌握國際參與的議題主軸，且較能累積長期努力的成果。 ・ 協助計畫研究團隊PoC實證驗證，並於ICANN 72	培育專家學者3位

項目	質化成果	量化成果
	發表「PoC of DNS identifier」（DNS識別碼的概念性驗證），展示以DNS識別碼機制解決物聯網裝置使用E.164難以管理及識別物聯網裝置的問題。	
經驗分享會	本計畫邀請曾擔任相關國際組織之重要幹部者，談論主題包含「電信編碼技術發展趨勢暨國際會議經驗談」、「ICANN組織參與實務經驗分享與討論」、「IETF組織參與及國際電信編碼趨勢」，其成果及建議如下： • 依據黃勝雄執行長制訂IETF技術標準經驗，預計歷時4年，此外該制訂技術標準為跨國、跨單位投入資源，因此建議若要培育或是規劃制訂相關技術標準，應挹注長期資金及有跨國或固定的研究團隊參與。 • 依據吳國維前執行長長期參與ICANN經驗，ICANN屬性為政治性國際組織，若有實際技術問題時，會諮詢或參考IETF草案或文獻，若要討論技術或技術交流，建議仍是回到IETF。此外，建議參與ICANN組織或交流時，仍是以政策或網際網路治理相關問題為主。	辦理經驗分享會3場次
會前諮詢會議	辦理4場參與國際會議前的主題培訓，以利專業團隊在參與國際會議或活動前，得掌握參與目的、關注之議題及政策倡議之方向等。	辦理會前諮詢會議4場次

資料來源：本計畫製作

三、未來推動策略及效益

本計畫人才培育之目標是培養參與相關國際標準制定工作及可擔任該等組織重要幹部之專業人才，以確保我國在資通訊領域的國際空間及影響力。為達該目標，本計畫今年透過實質參與的經驗及訪談曾參與國際組織或擔任幹部的專家學者，提具短、中、長期人才培育四年期程的策略方向、執行內容及績效指標等建議方案，盼有效延續本案的技術能量及政策效益，並作為未來主管機關參考依據。短、中、長期策略規劃期程共計四年，第一年是今年的人才培育先導期，透過參與會議鎖定制定國際標準的技術議題、鎖定擔任 ICANN ALAC、GAC、SSAC 該等組織的幹部位置、強化與 IETF INT 的社群互動交流等。第二年除延續第一年執行成果外，應組建官學研的專業團隊，共同就技術面、政策面進行討論，凝聚技術能量，此外應加強辦理實務培訓課程，例如國際技術標準撰寫實務、雙贏協商及談判等課程。第三年應積極爭取擔任國際組織幹部及爭取國際技術合作，因此模擬國際會議及 IETF 實作程式競賽或研習營將為第三年的重點；第四年為強化技術能量及優化目前規劃執行策略，首先應盤點三年所累積的人脈及技術資源，並從盤點結果強化技術或人脈能量，爭取 ICANN 幹部席位或 IETF 技術標準制定工作。

為達成本計畫提具之人才培育預期目標，本計畫評估政府應每年持續編列預算予主管機關，委由具穩定資通訊能量之研究團隊整合願意長期投入參與國際組織活動之專業人員，並積極參與國際標準組織內之固定工作群組，以逐步累積參與貢獻度及國際人脈，為我國在國際資通訊領域爭取更多空間和話語權。

針對培養我國參與國際標準制定工作及可擔任該等組織重要幹部，提出以上短、中、長期人才培育提具 4 年期程的策略方向、執行內容及績效指標等建議方案之執行策略方向及 KPI 如表 5-14 規劃所示。

表 5- 14、人才培育短、中、長期參與策略與效益規劃表

項目		第一年 (先導期)	第二年 (短期)	第三年 (中期)	第四年 (長期)
策略方向		蓄積技術能量 鎖定國際參與	提升技術能量 建立國際參與	強化技術能量 擴大國際參與	深化技術能量 增進國際參與
執行內容		鎖定國際組織社群：盤點與本計畫議題相關之國際組織社群 建立參與管道及策略：IETF 及 ICANN 國際組織交流管道	組建專業團隊及參與組織社群：組建專業研究團隊，爭取參與社群事務 提升研究團隊技術能量：持續研究計畫執行，並在社群提出技術討論	擴大國際組織社群參與：爭取社群其他成員支持及合作關係 強化技術能量：與國際組織成員進行技術交流，並尋求合作研究開發機會	增進國際參與：培育可擔任國際組織幹部之專家學者 深化技術能量：尋求國際技術交流合作，並爭取參與國際標準制定
績效指標	人才培育	人才培育成果報告≥1 份	培訓課程>3 場 培育課程資料≥1 份	培育課程≥3 場 IETF 相關活動(研習或程式競賽)≥1 場	培育課程≥3 場 ICANN 相關活動(研習或會議)≥1 場
	國際合作(人員互動及國際交流)	國際會議成果發表≥1 場(篇) 國際組織專家學者交流會議 1 場	參與國際組織社群≥2 個 國際會議成果發表≥1 場(篇)	國際技術交流會≥1 場 國際會議成果發表≥1 場(篇)	國際技術研究成果發表≥1 場(篇) 爭取擔任國際組織幹部

項目		第一年 (先導期)	第二年 (短期)	第三年 (中期)	第四年 (長期)
	研究報告	國際組織(ICANN 及 IETF 等)參與策略報告 1 份	國際組織及社群討論議題分析報告 1 份	分析國際組織及社群電信網路技術討論報告 1 份	我國資通訊領域國際參與及影響力分析報告 1 份

資料來源: 本計畫製作

第六章 研究結論與政策建議

本計畫旨在「超前部署下世代電信編碼之技術與標準發展」、「掌握國際最新技術標準制定情形」及「確保我國科技發展與國際並駕齊驅」，並評估發展情勢對我國政策及產業面之影響。

盱衡國內外對於下世代電信網路號碼技術之整體發展，目前可視仍在「方興未艾、持續發展」時期，本計畫綜整「下世代電信網路號碼技術及政策」、「下世代電信號碼資安稽核」、「下世代電信網路號碼驗證機制」及「下世代電信網路號碼人才培育」之結論，綜整提出政策建議及下世代電信網路號碼與數位經濟發展政策。

第一節　研究結論

一、 下世代電信網路號碼技術及政策

在各層級網路的運作上，命名（naming）、定址（addressing）與識別（identity）機制是網路運作及相互連通的基礎，而在這背後運作的即為號碼機制。無論是電信網路（電信層）或網際網路（應用層），「號碼」所扮演的角色，均在於賦予設備唯一的識別性，並使網路中的其他設備可以透過定址與該設備互連通訊。隨著技術與服務的演進，未來號碼的分配對象，也將各自在電信層及應用層擴展至各種數位資源，並需更為細緻的資源解析管理機制協助其運作。

(一) 電信網路號碼的辨識性需求增加

在電信網路上，號碼原為識別（identity）的用途，透過號碼的編定與分配，可以識別出不同的使用者或是設備；但號碼本身並不具備足夠的辨識性（recognize），亦即我們無法從號碼的外觀得知使用者、設備或服務的屬性；而為了強化號碼（如 E.164）的辨識性，當前係透過「公眾電信網路號碼計畫」將號碼加以分類與分配管理，透過將冠碼及首碼與不同電信服務的對應，使號碼區塊擁有如地理區域（02、03 等地理區域碼）或是服務類型（如

070 網路電話）的辨識。

在數位經濟發展下，通訊服務型態越來越多元，前述 E.164 的辨識性有所限制，尤其加上詐騙電話盛行，民眾每天所接到的電話形形色色；而另一方面，網際網路與電信網路的創新應用也不斷增加，「公眾電信網路號碼計畫」所建立的辨識性已不足因應民眾使用電信號碼的需求。

(二) 網際網路通訊協定（TCP/IP）的開放性降低新電信技術對號碼的需求

當前電信網路最廣泛使用的電信號碼機制為 ITU 與各國協調制定的 E.164、E.212 標準。由於公眾交換電話網路(Public Switch Telephone Network, PSTN)仍為各國最基礎的通訊服務系統，因此各國在號碼議題上的探討，基本上仍將 E.164 號碼視為國家電信資源進行管制。新興電信服務是否需要配發 E.164 號碼，與該服務是否需與既有電信網路互連互通有極大關係；例如網路電話（VoIP）與衛星電話，均應有與電信網路互通之需求，而必須配發 E.164 號碼。

由於網際網路通訊協定 TCP/IP 具有相當大的開放性，在無需配發 E.164 號碼情況下，可從軟體及應用的面向解決網路互通的需求，且網際網路應用服務的多元性及相對低於傳統電信服務的費用，甚至改變了消費者的使用行為，取代了部分基礎語音通訊服務。例如即時通訊軟體(Instant Messaging, IM)，其在無須分配 E.164 號碼下，即可提供文字訊息傳遞及語音通訊。

(三) 應用層跨向電信層的通訊需求增加

從 5G 的技術發展可以觀察到，網路核心架構朝向 IP 化及軟體化，這意味著電信技術將更加縮短網路層與應用層的距離，一方面，E.164、E.212、DN、IP 位址等均可適用於 IP 公眾網路下的物聯網應用，另方面，隨著電信網路架構 IP 化及 VoIP、M2M 技

術之發展，新型態應用服務對於 E.164 之需求性產生了變化。

傳統電話網路以語音服務為基礎，過去「語音」是最便利的通訊溝通媒介；當愈來愈多的電信技術及服務建立在 IP 及數據傳輸的基礎上，愈來愈多的電信服務（例如物聯網、智慧公共安全）是建立在應用層，代表網際網路應用層對於電信網路層的互連通訊需求持續增加，依其服務性質，需與公眾交換電話網路界接時，仍需分配 E.164 號碼。

技術發展使得新型態應用服務可依其需求，選擇 E.164 或是 DN/IP 作為其號碼解決方案，預期將來可能對於既有的 DN/IP 運作機制及國家號碼計畫產生影響。

例如，我國分配 040 號碼予物聯網服務，為了避免業者因提供電信語音服務而受到如通訊監察義務之高度管制措施，而限制物聯網創新發展，因此限制 040 號碼不能提供語音及簡訊服務；時至今日，物聯網應用的類型越來越多，由應用層以語音服務跨向電信層通訊的需求未來將逐漸出現，對於號碼之規劃以及相對應之監管，亦應加以重新檢視。

(四) 網路應用層的號碼機制多元化發展下增加網路資源管理之需求

在網際網路上，IP 位址的辨識性雖然非常低，但透過 DN 命名及 IP 轉換解析機制（即 DNS 系統），不但強化了辨識性，同時得力於網路應用層的開放性，可進一步擴增號碼之功能，因應物聯網大量連網裝置的需求，透過自動命名及管理系統，強化管理需求以及安全性。

除了上述所提，民眾的通訊需求越來越多元，提升號碼辨識性之需求，下世代電信網路號碼技術上的發展，也使網路資源（使用者、設備、資訊、網站等）的型態越來越多元。例如近來元宇宙（metaverse）概念議題，未來趨勢將有更多不同類型的網路資源，並需透過號碼分配機制加以管理。因此，因應下世代電信網路發展的異質性與多元性，其網路互通之需求也越加複雜。

二、 下世代電信網路號碼資安稽核

依據 ITU FG NET 2030[244]所擘劃的願景來看，在未來 10 年的網路環境將比現在更為複雜。在網路效能逐漸提高的同時，將有機會連結萬物，形成多重裝置、多重接取服務並存的多重網路環境。在既有網路與 ITU 所擘劃的未來網路環境相比較可推知，目前多重網路發展的初期將以電信網路層與應用層彼此之間的技術介接與整合為首要發展目標，例如 5G 與 WLAN、有線網路等非 3GPP 網路的跨網互連；在應用服務方面是以物聯網通訊為基礎做為垂直領域的研發方向，但在路由與定址上的跨網互連機制是否因應上述的網路變革而改變，目前尚未有所定論。然而，在通訊網路架構的安全層面，已提前將跨網互通安全技術納入考量。

待網路硬體軟體化、行動通訊元件虛擬化等各方條件成熟，多重網路互連情形下，即使是使用 4G 時代就存在的資安攻擊手法，也會因為（1）網路流量提升（2）網路與通訊服務規模擴大（3）關鍵基礎設施與垂直產業網路化、自動化、智慧化，使駭客攻擊行為衍生出多樣化的攻擊策略與複合的攻擊型態，造成比以往更為龐大的經濟、安全損失，例如進階持續攻擊（Advanced Persistent Threat, APT），不僅限於針對攻擊對象進行單一威脅類型、單一時間點、單一攻擊目標，而是更多及複雜的攻擊型態。

觀測近 2 年國際主要國家如歐盟、新加坡、美國，在因應上述網路環境所做的網路安全政策與法規調適可知，各國除了重視網路本身的安全管理，還對於資通訊科技（Information Communication Technology, ICT）供應鏈、以及物聯網供應鏈安全管理，針對相關人員之管理訂立相關原則或義務、並將設備或系統開發初期之安全性納入考量。在 ICT 供應鏈層面，歐盟於 NIS2 擴大資安規管範圍至數位服務、關鍵製造等智慧化產業；新加坡宣布制定 CII 供應鏈計畫，提升企業領導者、技術

[244] ITU, “FG NET 2030” , https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx.(Lasted visited：Nov. 29. 2021)

團隊與員工的網路安全管理；美國在 NIST 框架基礎上提出強化 5G 供應鏈風險管理策略，積極促成產官學機構與民間關係人參與並提供技術援助。在物聯網供應鏈層面，歐盟規劃將物聯網供應商之個人與機敏資訊保護義務納入網路十年戰略的物聯網安全措施；新加坡依物聯網人員（開發者、供應者、使用者）與系統階段（實施、營運階段）提出對應之安全建議；美國從物聯網設備採購角度考慮系統安全性，作為聯邦機構安全與數據隱私評估標準。

前述先進國家建立網路安全框架、頒布對於網路系統、設備、人員的資通安全需求與操作指南，或要求將其納入組織的風險管理的環節，無非是期望能逐步提升全民資通安全的認知與資通安全能力，以落實國家網路安全總體策略。

綜上所述，本計畫之下世代電信網路號碼驗證機制，其在系統架構技術及管理上應重視網路識別碼、網路通訊品質及既有的核心網路安全性架構與身分認證機制，以確保網路通訊的安全性。

在組織管理角度，應建立於既有的國際稽核標準之上，增加零信任網路概念的指引原則，不再以組織或網路的內部與外部作為安全邊界的區分準則，而須通盤瞭解組織整體的網路、資訊系統環境，以訂立相關資通安全政策，並擬定可以具體落實的資通安全策略。

在政策管理的角度，在資通安全管理法制體系與數位經濟發展的基礎下，對於高風險產業如能源、關鍵製造等逐步網路化、自動化、智慧化，建立共同的風險溝通機制，得以因應新型態垂直產業轉型背景下對於資訊系統、營運系統與環境交互連結的管理需求。

三、 下世代電信網路號碼驗證機制

隨著下世代電信網路號碼技術發展，可預期物聯網裝置數量將快速成長，此外裝置型態也將更加多元，根據市場研究機構 IDC 預估，至 2025 年物聯網裝置數量將超過 4 百億個[245]。依據本計畫分項一結論

[245] International Data Corporate (IDC), "The Growth in Connected IoT Devices Is Expected to Generate 79.4 ZB of Data in 2025," 19 June 2019.（Lasted visited：Nov. 29. 2021）

得知，既有 E.164 編碼主要應用在電信網路層，透過號碼的編定與分配，得以識別使用者或是設備，然而隨著通訊技術、服務型態及物聯網裝置數量的改變，在管理上對於號碼辨識性(recognize)的需求更甚於以往。有鑑於此，本計畫提出除現有的 E.164 編碼外，大量物聯網設備在下世代電信網路及網路切片環境中，具有高辨識性及有效管理之編碼解決方案。

本計畫在擬定下世代電信網路號碼系統驗證機制前，先行蒐集以 IoT 設備自動命名之相關國際文獻，其中 2015 年於 IETF 發表之「DNS Name Autoconfiguration for Internet of Things Devices」[246]，是基於 IP 網路中，IoT 設備在無線或有線網路下透過 DNS 命名進行自動配置，並 IoT 設備之型號等訊息轉譯成 DNS，使物聯網用戶(例如司機、乘客)可以直覺式識別網路中的每個設備裝置，以達到遠端監控之目的；另外，2018 年於 International Conference on Mobile Computing and Ubiquitous Network 發表之「Flexible Name Autoconfiguration for IoT Devices」[247]及 2020 年第八屆無線網路與行動通訊國際會議(International Conference on Wireless Networks and Mobile Communications, WINCOM)發表的「UAV for IoT Communications: Beam Selection Using Matching Game and Network Slicing」[248]，均提出 IoT 設備自動命名及直覺性辨識與管理之概念。綜整國際文獻(如表 6-1)及評估 5G 切片技術，擬定下世代電信網路號碼概念性驗證（Proof of Concept, PoC），透過 DNS 識別碼自動分配予物聯網裝置，以利物聯網裝置更易於直覺辨識及管理。

[246] Jaehoon Paul Jeong, Sejun Lee, Jung-Soo Park, "DNS Name Autoconfiguration for Internet of Things Devices", Oct 14 2015, available at https://datatracker.ietf.org/doc/draft-jeong-6man-iot-dns-autoconf/（Lasted visited：Nov. 29. 2021）

[247] T. Yanase, H. Tanaka, and H. Suzuki, "Flexible name autoconfiguration for iot devices," in Proceedings of The 11th International Conference on Mobile Computing and Ubiquitous Network (ICMU 2018), 2018.

[248] Salma Brihi; Anas Ghamizi; Karim Chakri, " UAV for IoT Communications: Beam Selection Using Matching Game and Network Slicing", Dec. 4 2020, available at https://ieeexplore.ieee.org/document/9272510（Lasted visited：Nov. 29. 2021）

表 6- 1、以 DNS 為 IoT 設備命名之國際文獻

年份	2015	2018	2020
報告名稱	DNS Name Autoconfiguration for Internet of Things Devices	Flexible Name Autoconfiguration for IoT Devices	UAV for IoT Communications: Beam Selection Using Matching Game and Network Slicing
內容摘要	依 IoT 設備資訊自動配置 DNS，用以識別及管理個別 IoT 設備，其 DNS 包含具唯一性的識別符號、產品型號或製造商名稱、設備類型、設備位置及其使用之域名等。	當 IoT 設備分配 IPv6 位址進行通訊，通常會使用如 FQDN 等便於使用者辨識設備之識別碼，該報告提出不更動 IoT 設備規格之情況下，利用 IoT 設備使用之通訊協定獲得資訊並自動生成包含設備位置欄位之 FQDN，另可依需求將 FQDN 更改為更容易識別之 FQDN。	利用 SDN 及 NFV 技術，提出基於網路切片之 5G 邏輯架構，以提供靈活之個性化服務及移動性管理機制，並提出以無人機作為小型蜂窩基站之應用情境，提升及強化網路覆蓋率。

資料來源：本計畫製作

本計畫 PoC 設計 2 種測試情境，一為 IoT 設備移動測試，設備在同域不同基站間及不同域不同基站間移動，以驗證 DNS 編碼可提供 IoT 設備位置資訊；另一測試情境為大量設備註冊及認證測試，驗證 DNS 機制具備因應大量設備連網之能力，並可參照 IMEI 為 IoT 設備依特性編碼，以直覺式辨識不同功能之 IoT 設備，進而提升管理效率。

IoT 設備連網後分配 IP 位址以進行通訊，惟 IP 位址係供機器識別使用，須解析 IP 位址並轉換成如完整網域名稱（Fully-Qualified Domain

Name, FQDN）的方式供人易於理解及識別。當 5G 帶動物聯網應用發展，在大規模機器型通訊（mMTC）應用場景之下，自動配置 FQDN 及 IP 位址將節省許多人力及時間。爰此，本計畫研析以 DNS 為 IoT 設備自動產生 FQDN 及配置 IP，並建立資料管理平臺儲存及查詢歷史軌跡紀錄，以驗證在下世代電信網路環境中，利用 DNS 機制自動編碼及管理之之可行性。此外，PoC 亦將網路切片之參數加入編碼欄位，以符合 5G 依應用服務需要將網路資源切成不同的獨立網段，未來管理上可依 IMEI 及網路切片類型套用不同 QoS 規則，並阻止非物聯網設備連網。

本 PoC 實驗成果於 ICANN 72 「Tech Day」議程中發表”PoC of DNS identifier”專題演講，透過本次會議與各國專家及技術人員共同探討 DNS 編碼之運用方式，將於未來服務驗證（Proof of Service, PoS）階段，作為驗證相關情境之方向，及優化 DNS 自動編碼機制之應用方式。

四、 下世代電信網路號碼人才培育

下世代電信網路號碼在國際實屬前瞻技術議題，目前國際上仍持續討論中。為使我國掌握全球最新技術發展趨勢及確保我國在資通訊領域的國際空間及影響力，規劃培養專業人才積極參與國際標準組織為本計畫人才培育之目標。

本計畫除透過分項一及分項二研析相關技術、政策及資安議題，並將研究成果與國際組織及專家學者交流，希冀能培養參與相關國際標準制定工作及可擔任該等組織重要幹部之專業人才。

有鑑於此，本計畫今年度邀集 3 位專家學者，其分別為國立臺灣科技大學資訊管理系羅乃維教授、國立宜蘭大學資訊工程學系陳麒元副教授及理律律師事務所曾更瑩律師，與本計畫團隊共同參與 ICANN、IETF 及 ITU 共計 5 場國際組織會議，並與 ICANN IROS 及 IETF 交流互動。此外，為傳承國際組織參與經驗，本計畫邀請通傳會沈信雄簡任技正、TWNIC 黃勝雄執行長及 NII 吳國維前執行長，辦理 3 場經驗分享會。另依據參與國際組織會議所獲得資訊及近期國際組織在電信技術相關領域關注議題，研提人才培育短、中、長期參與策略及效益。

最後，本計畫為協助國內產業及早因應及進行市場布局，故辦理 3 場座談會，邀集政府機關相關單位、電信業者及設備商等利害關係人，透過討論交流達到技術擴散之目的，以促進我國下世代 5G IoT 與網路切片相關產業技術與國際接軌。

今年度人才培育成果主要為「人才培育成果」及「人才培育短、中、長期參與策略及效益」:

1. 今年為人才培育先導期，透過今年度參與國際組織之成果，建議未來可依「物聯網唯一識別碼自動配置」、「電信網路與網際網路介接」、「DNS 系統安全」及「網路切片編碼」等議題作為未來制定國際技術標準議題。

2. 本計畫提出 4 年期程的策略方向、執行內容及績效指標等建議方案，建議應組建官學研的專業團隊，透過參與會議鎖定制定國際標準的技術議題、鎖定擔任 ICANN ALAC、GAC、SSAC 該等組織的幹部位置、強化與 IETF INT 的社群互動交流等。

第二節　政策建議

一、 下世代電信網路號碼政策

(一) 號碼政策應以技術中立原則，依服務需求進行號碼之分配管理

在既有 E.164 號碼的基礎下，從基礎服務、識別、辨識、定址、互通等條件，觀察下世代電信網路號碼技術的發展，在接取網路上，新技術（如衛星）首要提供寬頻接取而不提供語音服務，對於納入 E.164 的需求亦不顯著。

本計畫評估，未來無論是新電信技術或是物聯網，編定特別的號碼區塊，應由具體的服務需求而定。例如車聯網服務，編定首碼識別其為車輛；或因人工智慧之發展，未來需辨識非人類對象等，針對特定物聯網類型的需求，考量公共性、而非技術性，以編定新號碼區塊。

(二) 依據國內垂直專網發展需求決定 E.212 號碼取用途徑

E.164 號碼最早使用在固網電話，行動網路技術則採用 E.212 號碼為國際行動用戶識別碼（International Mobile Subscriber Identity, IMSI），為電信業者認證用戶與服務的依據，因此若使用者申請行動電信業者之服務時，業者透過 SIM 卡配有 E.212 號碼與裝置結合，供電信業者識別使用者，並提供行動電話及行動寬頻服務。而在5G技術發展上，除了提供傳統行動寬頻服務外，其技術革新主要在於能提供物聯網所需的超低延遲以及巨量連結的需求，從而，不同類型的物聯網服務，均可透過5G技術建立專用網路。

專用網路係非電信業者之網路，因此網路擁有者並不提供公眾電信服務，從而無法以電信業者身份取得 E.212 號碼，為了讓專網業者能使用 5G 技術，依據 ITU 之規範在 E.212 號碼的使用上有幾種可能的選擇。

首先是僅限專網內部使用，依據 ITU-T E.212 (2016) Amendment 1 (07/18) Appendix III 限定 MCC 為 999，此一途徑因為使用者的專網僅內部連接，概念類似於免執照無線電頻率，故無須通報 ITU-T；另一途徑則依據 ITU-T E.212 (2016) Amendment 3 (12/20) Annex H，使用國際共用的 MCC 號碼 90x，此一途徑可透過企業自身直接向 ITU-T 申請核發；最後則是由國家申請特定的MCC號碼，並以共享的形式提供國內企業使用，例如美國採用共享 MCC 號碼 315 的方式。

在上述三種途徑中，可自由使用MCC=999的途徑最為簡易，本計畫分項三的 PoC 亦是採用此一方式，而在網路使用上限制較多；例如須以國家名義向 ITU 申請，然而因我國國際地位特殊，無法以國家的名義向 ITU 申請額外的號碼資源，因此由國家申請分享的方式有其困難；故而，若國內專網業者未來有與公眾網路串接的需求，我國則需評估透過協助、委託我國企業（設有海外分公司者）代為向 ITU 申請。

(三) 推動網際網路號碼加速 IPv6 推廣與汰除 IPv4 政策

在 IPv4 轉換至 IPv6 的討論上，主要在資源分配上 IPv4 的數量已經分配殆盡，而另一方面，IPv6 在技術運作的改進，使其更能應對網路安全的需求，例如 IPv6 與 IPsec 安全架構搭配，能發揮安全效益且不降低網路效能。然而，推廣 IPv6 的使用，我國長期推動 IPv4 與 IPv6 雙軌並行，雖然能大幅增加 IPv6 的使用性，卻使網路設備中同時混雜 IPv4 與 IPv6，不但無法增加網路的安全性，反而使網路中同時存在 IPv4 與 IPv6 的漏洞，安全性反而比單純使用 IPv4 更差。

整體而言，有國際合作推廣 IPv6 成效初見，然在 IPv6 具有相當普及程度之後，應加速汰除 IPv4 及鼓勵 IPv6 持續創新，無論是歐盟、美國，均由政府提供政策性的資源支持。而我國推動 IPv6 成效優越，但本計畫觀察到，我國在 Covid-19 疫情期間，居家辦公之際許多舊式網路設備繼續被使用，IPv4 設備的網路流量不減反增，顯示 IPv4 的汰除進度並不如預期，我國在 IPv6 的推廣上，需逐漸調整雙軌策略，應轉向鼓勵 IPv4 汰除之策略。

二、 對「公眾電信網路號碼計畫」之建議

觀察下世代電信網路架構下，不論行動通訊或是物聯網通訊仍使用 E.164 編碼規則，在電信層並未出現新取而代之編碼標準。本計畫所觀測之新編碼機制均建立於應用層、IP 網路基礎上，並能辨識或定址更多類型的資訊、物件等。

(一) 因應下世代通訊服務場景分配號碼區塊

在電信管理法思維下，號碼資源分配時，除了辨識發話端所在地理區之外，其他類型的號碼區塊則是以辨識電信業務為主，例如 09 冠碼的行動電信、070 網路電話（特殊二類），以及近來的 040 物聯網號碼（禁止語音通訊）。然而，下世代通訊技術與服務的類型只會增加不會減少，若堅持 E.164 號碼必須維持以冠碼辨

識特定通訊服務類型的原則，我國整體號碼資源雖不至於枯竭，但可推測將造成更多號碼資源的浪費。

因此，在當前網際網路應用普及之際，評估號碼區塊的編定時，應著重於辨識公共服務提供者，並考量將分配區塊縮小，以容納更多元的服務辨識需求。

(二) 考量智慧虛擬碼、網路電話號碼、物聯網號碼之長期檢視規劃

隨著電信網路架構 IP 化及 VoIP、M2M 技術之發展，監理機關開始為新型態應用服務使用 E.164 之需求進行國家號碼計畫之調整；由於號碼編配後再作改變的行政成本將極為巨大，為新服務編配新號碼字頭更須審慎評估。現行公眾電信網路號碼計畫，010～080 智慧虛擬碼、070 網路電話號碼以及 040 物聯網號碼則可配合前項建議進行回收重整，未來則建議以技術中立之概念進行評估、分配管理。

(三) 下世代電信網路資料傳輸之管理政策

在 5G 與物聯網發展下，國外號碼在本國的使用，已不僅限於國外人士於我國進行漫遊通信，各式用途的物聯網裝置，亦可能因為各種需求（如國外專業團隊帶入工作設備），使物聯網裝置的號碼有於我國使用的需求；或另一方面，如衛星通訊此種可跨越國境提供服務的技術，亦可能直接使用國外電信號碼提供給國內使用者。

對於上述情況，研究團隊初步提出建議評估原則：

1. 評估境外號碼進入我國之期間，若為有期限的進出我國，則可予以放寬，若無相對應之期限，則可考慮加以限制。
2. 評估境外號碼進入我國之方式，若進入者僅為號碼，漫遊至我國電信網路，則可予以放寬；若為境外電信服務，則應予管制或限制，或要求境外業者依據我國法令落地。
3. 評估境外號碼進入之數量，如僅為少量，對市場影響甚微，則

可放寬；若有相當數量，影響我國電信服務之運作，則應考慮加以限制。

號碼之使用為國家資源分配之議題，但不同國家的法制與政策有落差，國外的號碼管理與分配政策與我國未必相同，市場條件也未必對等，縱使因技術發展而致使用門檻降低，我國仍應審慎評估，避免損害我國電信服務市場。

三、 下世代電信網路號碼資安稽核策略與跨網互通安全

(一) 強化解析系統的重要性與安全性

數位資源IP化的管理，當前仍以DNS機制為主，然而，DNS的初始設計為 DN/IP 之解析機制，未考慮安全性與隱私需求，其架構不易變動；增強安全性後可能面臨網路效能下降，延遲增加。未來以 DNS 為基礎之管理機制，具有廣泛的基礎設施、軟體整合與網際網路的相容性，需強化其隱私與安全。

假設 DNS 編碼機制成功作為下世代網路號碼管理系統，並廣泛應用於公共服務，將會依據不同的服務型態產生不同程度之管制，並產生相應的政策需求。在管制程度之決定上，本計畫建議，將 DNS 機制依據其所處服務之重要性，決定是否納入關鍵基礎設施（Critical Infrastructure, CI）之管制模式（例如智慧電網）。納入 CI 後，依據產業受管制程度高低，決定採取主管機關管制（如電網）、公私協力（例如 TWNIC）、業者自律(例如企業專網)之管制機制，進而檢視資通安全管理法及相關子法之條文規範與法制框架調整。

(二) 下世代網路架構與跨網需求之資安稽核策略建議

基於下世代電信網路願景，本計畫分析各項技術標準與各國資安政策，推導未來資安管控重點歸納為三項，分別是：

- 以風險管理為基礎，建構資安框架，由公到私之階段性導入
- 針對產品供應鏈之安全管理與人員管理，訂定資安義務要求

- 強調設備或系統於開發初期即納入安全技術考量

在下世代電信網路架構上，E.164、IPv6 與 DN 將形成跨越應用層、電信層的互動關係，隨著不同網路層級的應用服務需求、以及不同網路層級交互傳遞資料的需求，均會與屬於網際網路的 DNS 系統產生互動的關係。基此，研究團隊依原生於網路應用層，得以跨網互連的 DNS 作為資料管理的核心系統，參照國際稽核與技術標準，提出適用於下世代萬物聯網系統環境下的 DN/IP 資料管理稽核框架，並對此提供政府在既有的資通安全管理法架構下，做為跨部門資料流通的基本方針。

在下世代網路電信號碼管理的願景下，DNS 編碼管理系統所構築的議題將會扣合行政院大型資通訊政策之擘劃方向，在政府數位治理、數位基礎設施、數位創新應用服務三大主軸議題，分別為「網路資源識別」、「5G 虛擬化網路資源管理」與「商用物聯網應用管理」，並依據政府、電信業者、專網業者與網通及物聯設備商等利害關係人，盤點、識別出風險管理議題，以做為未來跨網互通策略之進一步分析。

四、 下世代電信網路號碼系統驗證建議

有別於在公眾電信網路通用之 E.164 及 E.212 編碼，主要應用於人與人之通訊與識別，本計畫建立及驗證下世代電信網路號碼系統，目的為提供使用者對物聯網裝置易於直覺式辨識及管理之編碼解決方案，以因應 5G 時代的 IoT 應用場景更加多元，並增加更多對移動性 IoT 設備之需求，例如智慧工廠、無人車、智慧環境監控等應用服務。

5G 網路傳輸除整合 LPWAN 技術，將部署更多 5G 小基站擴大網路覆蓋範圍，推動專網應用以強化企業內部資訊傳輸之安全，在網路受建築物阻擋的區域中提高網路覆蓋及傳輸率。

(一) 可參考的編碼規則建議

因應本計畫今年 PoC 實作需求，本次驗證所設計之編碼規則，

依據其應用場景及網路環境，將裝置所在之基站、區域列為編碼要素之一，模擬 IoT 設備在不同基站間移動時之情境，可即時追蹤 IoT 設備移動至哪一個基站的服務範圍。依據本年度之驗證成果，未來若進行其他服務之驗證，編碼規則可參考以下原則加以制定：

1. 區分網路環境對內與對外需求，決定編碼中的資訊類型

本年度情境為封閉式網路，故在編碼規則設計上，將基站及區域列入，在 DNS 編碼中包含了許多內部的資訊，使內部能方便有效的管理大量 IoT 裝置；然而，經分項二的研析可知，包含於 DNS 編碼的資訊可能成為隱私資料洩漏的環節，因此，在未來需評估網路環境的開放性，制定對內或對外網路環境之編碼格式，對外裝置的編碼必須涵蓋較少的資訊。

2. 評估系統服務需求，決定 DNS 與 IP 的變動對應關係

考量 IPv6 技術演進使 IP 數量趨近於無限，以 DNS 自動編碼解析 IP 位址，利於大量 IoT 裝置快速自動化地配置編碼，而在未來 PoS 規劃上，將更進一步評估服務層面如設備間溝通或與電信業者既有平臺整合等相關應用。IPv6 位址的數量，若足使各裝置擁有獨一的位址，就可透過 DN 的變化記錄在內部管理裝置；反之，若裝置有對外需求，或需被由外部查詢、連線，則 DN 必須固定，以維持完整的外部查詢與對應關係。

3. 遵照 DN 的基本編碼規則，依 IoT 裝置屬性配發固定唯一碼

本計畫場域設定為專網封閉式環境，IoT 裝置單向上傳資訊，不考慮被別人參照或查詢(query)。在 PoS 或實際應用場景，如 IoT 須被參照、查詢或出網，DN 命名須考量具唯一性及不被辨識(不使用具敏感資訊可被判讀之資料欄位，如 MAC, IMEI, IMSI)。

(二) 觀測系統內容與界定稽核範圍

名稱解析系統本身屬於資訊管理系統之一，因此其資安屬於資訊安全管理（ISMS）的一環，透過本次系統驗證，未來可作為

其他單位導入 ISO 或其他資安管理機制與進行資安稽核的參考，由此可觀察出該資訊系統可能的範圍與需求，未來進一步完善稽核機制。

五、 下世代電信網路號碼人才培育短、中、長期參與策略與效益

本計畫透過今年參與國際組織成果及訪談曾參與國際組織或擔任幹部的專家學者可知，持續參與是獲得更大國際影響力，爭取擔任幹部的主要條件。

(一) 短、中、長期人才培育策略方向

今(2021)年是人才培育先導期，透過參與會議鎖定制定國際標準的技術議題、鎖定擔任 ICANN ALAC、GAC、SSAC 該等組織的幹部位置、強化與 IETF INT 的社群互動交流等。第二年（短期）除延續第一年執行成果外，應組建官學研的專業團隊，共同就技術面、政策面進行討論，凝聚技術能量，此外應加強辦理實務培訓課程，例如國際技術標準撰寫實務、雙贏協商及談判等課程。第三年應積極爭取擔任國際組織幹部及爭取國際技術合作，因此模擬國際會議及 IETF 實作程式競賽或研習營將為第三年（中期）的重點；第四年（長期）為強化技術能量及優化目前規劃執行策略，首先應盤點三年所累積的人脈及技術資源，並從盤點結果強化技術或人脈能量，爭取 ICANN 幹部席位或 IETF 技術標準制定。

(二) 選才培訓及參與策略建議

研究團隊透過本年度各項活動與訪談，已可提出國際參與所需之專業能力分析、課程與加強之專業面向與經驗傳承，然而，在人才的培育與參與部分，仍須政府其他政策的配套。

1. 以政策誘因吸引人才投入技術社群討論

由本年度的執行及訪談可知，特別在技術社群性高的 IETF 的參與上，不僅培訓的人才需參與會議，本身也需不斷的投入技術

研發，並與社群持續互動，方能逐步的取得技術標準的影響力。因此，本計畫建議可鎖定學研單位資歷較淺的人才，並給予特定的政策誘因，如學界的升等評比、研發單位的補助等，促使人才願意長期投入特定領域累積能量。

2. 將參與國際會議納入公務體系之培訓需求

若國際組織屬性偏向政策討論，則產官學研界之人才都可參與，惟若於公務體系中，則亦需與其職能加以結合，並加強所需之政策專業知能，強化其國際參與之能力，並與國家政策相互結合，使其更能於國際場合與他國進行政策交流。

第三節　下世代電信網路號碼與數位經濟發展政策

本計畫分析電信技術與服務、網際網路號碼分配等國際標準及主要國家推動 IPv6 之政策的成果發現，總體而言，下世代網路持續朝向全面採用網際網路通訊協定(All-IP)、接取端異質網路技術融合匯流發展的趨勢。

一、 下世代電信網路號碼與數位經濟發展願景

詳言之，首先，在電信號碼層面，從各國編配 E.164 號碼予物聯網服務之政策經驗分析，亦可推論依據 ITU-T E.164 規約編定的公眾電信網路號碼計畫，主要目的仍在維持全球電信網路的互通性，並同時討論如何滿足下世代電信網路對於號碼、命名、定址和識別資源（NNAI）相關需求。

其次，在網際網路層面，由 IPv6 構建出新的網路空間平臺與垂直應用，將會產生更多的技術創新機會，故而如何有效地引導產業及學研界，協同建構並深化 IPv6 規模部署、產業發展和應用創新，為現階段政府可加以關注的重點。

最後，從近來「元宇宙（metaverse）」概念的討論潮流可觀察到，無論各國或各企業對於元宇宙細緻的內涵論述為何，從技術演進的路徑可知，元宇宙的概念基礎必然以無間隙網路串連各種虛擬資源而構

成，故異質網路的接取與互連互通的發展趨勢已如前述；而仍處於初期概念發展者，為數位智慧資產 IP 化（Intellectual Property-to-IP address, IP-to-IP）的過程，本計畫所觀察之網際網路新型態號碼，如 OID、DOA、NDN 等，均以數位資產（資料、文件、檔案等）為號碼分配對象，其數量將更遠超過當前的物聯網。因此，下世代網路將面對更為龐大的號碼管理與分配的需求，對於政策制定機關而言，不僅需考慮號碼之分配，同時亦需開始關注號碼與資源的管理解析機制需求。

二、 下世代電信網路號碼促進數位經濟發展之政策建議

基於上述之分析與觀察，對於下世代電信網路整體政策建議如下：

1. 建立公部門號碼資源解析管理機制

當前，政府在國家數位經濟政策的推動上，以數位轉型及數位創新為主軸，因此在概念上，政府部門需將公部門所持有的各種資料與各種服務加以數位化，並且依據需求將前述的公部門數位資源加以 IP 化或編配電信號碼，以提供民眾接取利用。政府整體將會因數位資源管理的需求，而需設置公部門的號碼解析管理系統，以妥善的維持各種政府數位資源的指向。日前，Facebook 曾發生過其域名解析系統（DNS）因人為操作失誤、當機導致大規模斷網事件，可知當政府或企業單位的數位資源數量達到非常龐大的規模時，便無法以人力進行管理，而需透過資源管理系統加以協助，該系統需以自動化命名（auto-naming），並能因應資源的變動而重新定址（auto-addressing），並需識別（auto-identity）資源的完整性與可用性。

本計畫分項三所建立之號碼管理 PoC 概念驗證，提供命名的規則與系統雛形架構，可為上述建議之具體參考。未來則可視數位資源的型態、服務的特性與目的、處於內部或外部網路等進一步進行調整。

2. 持續關注 NDN 與非 IP 網路的技術發展

在網際網路發展上，號碼機制的運作則與解析系統加以整合，

以強化號碼的識別性。網際網路最基礎的號碼系統為 DNS，但因應網路資源的多樣性，亦有其他編碼機制於不同用途。尤其命名資料網路（Named Data Networking, NDN），革新了 IP 體系結構，轉變為以資料為核心的架構，使當前端對端的傳輸概念，強化為內容分發和網路控制。

非 IP 網路(Non-IP Networking; NIN)則是更有別於傳統 IP 架構的新通訊協定，更大幅度的重新檢視當前 IP 化網路的缺點與改進。然而，相較於其他編碼機制的發展，NIN 的整體面貌上不明確，也難以評估其未來與既有 IP 網路的互動或取代關係，但由於其為歐洲電信標準協會(European Telecommunications Standards Institute, ETSI)下之產業規範研究組（ISG）所提出，仍具有一定程度之業界與議題影響力。

附錄一、參考文獻

壹、 英文文獻

1. 3GPP, *3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;System architecture for the 5G System (5GS);Stage 2, (Release 17)*, TS 23.501 v17.2.0(2021-09). Retrieved from https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-h20.zip (last visited：Oct. 4, 2021)
2. 3GPP, *3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of 5G network slicing management (Release 15),* TR 33.811 v15.0.0. Retrieved from https://www.3gpp.org/ftp/Specs/archive/33_series/33.811/33811-f00.zip (last visited：Aug. 31,2021)
3. 3GPP, *3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;*Security Architecture and procedures for 5G System;Stage 2, (Release 17), TS 33.501 v17.2.1 . Retrieved from https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-h21.zip(last visited：Oct. 4, 2021), p.113.
4. 3rd Generation Partnership Project (2021-09) ”Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS)”, 3GPP TS 23.502 V15.15.0, P65
5. 3rd Generation Partnership Project (2019/06) “Technical Specification Group Core Network and Terminals;General Packet Radio Service （GPRS）;GPRS Tunnelling Protocol （GTP）across the Gn and Gp interface” Retrieved from https://www.3gpp.org/ftp//Specs/archive/29_series/29.060/29060-f50.zip P.26(2021/10/27)
6. 3rd Generation Partnership Project (2020/06) “Technical Specification Group Core Network and Terminals;Interworking between the Public Land Mobile Network （PLMN）supporting packet based services andPacket Data Networks （PDN）”Retrieved from https://www.3gpp.org/ftp//Specs/archive/29_series/29.061/29061-f60.zip , P80 (2021/10/25)

7. 3rd Generation Partnership Project (2021/09) ” Technical Specification Group Core Network and Terminals;Numbering, addressing and identification”, 3GPP TS 23.003 V17.3.0
8. 3rd Generation Partnership Project (2021/09) ” Technical Specification Group Core Network and Terminals;5G System; Interworking between 5G Network and external Data Networks;Stage 3”, 3GPP TS 29.561 V17.3.1, P23-31
9. 3rd Generation Partnership Project (2021-09) “Technical Specification Group Services and System Aspects;System architecture for the 5G System (5GS)” TS 23.501 V17.2.0, P216
10. 3rd Generation Partnership Project (2021-09) ”Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS)”, 3GPP TS 23.502 V15.15.0, P66-68
11. 3rd Generation Partnership Project(2021/09)“Technical Specification Group Services and System Aspects;System architecture for the 5G System (5GS) Stage 2”TS 23.501 V17.2.0
12. Adam Novotný (2021/06/29) “What is RTT (Round-Trip Time) and How to Reduce it?” Retrieved from https://www.stormit.cloud/post/what-is-round-trip-time-rtt-meaning-calculation
13. AIOTI (2018/02) ” Identifiers in Internet of Things （IoT）”, Version 1.0. Retrieved from https://euagenda.eu/upload/publications/identifiers-in-internet-of-things-iot.pdf （(2021/10/27)
14. Alain Durand(2017/10),” DOA over DNS” Retrieved from https://tools.ietf.org/pdf/draft-durand-doa-over-dns-03.pdf (2021/11/30）
15. Alain Durand, "5G Technology",*ICANN Office of the Chief Technology Officer*(2020)p.1-13
16. ATIS, ATIS-0300052(2020-03), Non-Geographic 5XX-NXX Code Assignment Guidelines. Retrieved from https://access.atis.org/apps/group_public/document.php?document_id=51937 (Last visited:Dec. 5, 2021)
17. ATIS, IMSI Assignment and Management Guidelines for
18. ATIS, International Mobile Subscriber Identity (IMSI) Assignment and Management Guidelines and Procedures. Retrieved from https://www.atis.org/wp-content/uploads/2020/10/IMSI-Guidelines-v16.pdf (Last visited:Dec. 5, 2021)
19. BNetzA, Mitteilung Nr. 101/2020. Retrieved from https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachge

biete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/TechnischeNummern/IMSI/Mitteilung101.pdf (Last visited:Dec. 5, 2021)
20. CEPT Electronic Communication Committee, 2010. ECC Report 153 - Numbering and Addressing in Machine-to-Machine (M2M) Communications. Retrieved from https://docdb.cept.org/document/261 (Last visited:Jul. 15, 2021)
21. CEPT Electronic Communication Committee, 2011. ECC Recommendation (11)03 - Numbering and Addressing for Machine To Machine (M2M) Communications. Retrieved from https://docdb.cept.org/document/499 (Last visited:Jul. 15, 2021)
22. CEPT Electronic Communication Committee, 2020. ECC Report 311 - Sub-assignment and number hosting - Implementation models, rights of use and obligations for E.164 numbers across the electronic communications supply chain. Retrieved from https://docdb.cept.org/document/14735 (Last visited:Jul. 15, 2021)
23. Cisco SD-WAN and Cloud Networking, “Cisco SD-WAN: Application Aware Routing”. Retrieved from https://www.youtube.com/watch?v=KR4jqWmcRTk.
24. CN Hu, Numbering plan for M2M and IoT services - A study of United States, Japan, China and Taiwan. Retrieved from https://ieeexplore.ieee.org/document/8354667 (Late visited, May, 26,2021)
25. COMPUTERWORLD, "5G AND FUTURE MOBILE" (2017). Retrieved from https://www.computerworld.com/article/3204594/http-and-dns-in-a-5g-world.html.
26. CSA, *Codes of Practice Standards of Performance*. Retrieved from https://www.csa.gov.sg/-/media/csa/documents/legislation_cop/cybersecurity-code-of-practice-cii-dec-2019.pdf (Lsat visited：Apr, 22, 2021)
27. CSA, Cybersecurity Act. Retrieved from https://www.csa.gov.sg/legislation/cybersecurity-act (Last visited：May. 3. 2021)
28. CSA, SG Cyber Safe Programme. Retrieved from https://www.csa.gov.sg/programmes/sgcybersafe (Lasted visited：May. 28. 2021)
29. CSA, *Singapore’s Cybersecurity Strategy*, pp.4-5, (2016), Retrieved from

https://www.csa.gov.sg/-/media/csa/documents/publications/singaporecybersecuritystrategy.pdf (Last visited：Apr, 17, 2020)

30. CSA, *Singapore's Operational Technology Cybersecurity Masterplan 2019*, pp.1,14-16, (Oct. 01, 2019). Retrieved from https://www.csa.gov.sg/-/media/csa/documents/publications/ot_masterplan/csa_ot_masterplan.pdf (Lsat visited：May, 5, 2021)
31. CSA, *Singapore's Operational Technology Cybersecurity Masterplan 2019*. Retrieved from https://www.csa.gov.sg/news/publications/ot-cybersecurity-masterplan (Lsat visited：May, 6, 2021)
32. CSA, *Singapore's Safer Cyberspace Masterplan 2020*, p.15, (Oct. 06, 2020), Retrieved from https://www.csa.gov.sg/-/media/csa/documents/publications/safer-cyberspace-masterplan-2020.pdf (Lasted visited：May. 25, 2021)。
33. CSA, Speech by Dr Janil Puthucheary, Senior Minister of State, Ministry of Communications and Information at the MCI Committee of Supply Debate 2021, (Mar.02, 2021). Retrieved from https://www.csa.gov.sg/news/speeches/mci-cos-2021-sms-speech (Lasted visited：May. 27. 2021)
34. DSFI-TSG, DNS Security Facilitation Initiative Technical Study Group - Final Report, Oct. 15, 2021. Retrieved from https://community.icann.org/display/DSFI/DSFI+TSG+Final+Report
35. Enisa, "DIRECTiVE(EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concering measures for a high level of security of network and information systems across the Union ", *Official Journal of the European Union*,(2016), p.1
36. ETSI (2018/07) "Digital cellular telecommunications system (Phase 2+) (GSM);Universal Mobile Telecommunications System(UMTS);Numbering, addressing and identification"(3GPP TS 23.003 version 15.4.0 Release 15) Retrieved from https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/15.04.00_60/ts_123003v150400p.pdf , P37（2021/10/27）
37. ETSI (2018-10) "5G;5G System;Equipment Identity Register Services;Stage 3" (ETSI TS 129 511 V15.1.0,P7
38. ETSI (2020/04) Retrieved from "Multi-access Edge Computing (MEC); V2X Information Service API". Retrieved from

https://www.etsi.org/deliver/etsi_gs/MEC/001_099/030/02.01.01_60/gs_MEC030v020101p.pdf ,P10（2021/10/27）
39. ETSI, ETSI launches new group on Non-IP Networking addressing 5G new services. Retrieved from https://www.etsi.org/newsroom/press-releases/1749-2020-04 (Last visited:Dec. 5, 2021)
40. ETSI, GR IP6 006 V1.1.1 (2017-11) - Generic migration steps from IPv4 to IPv6. Retrieved from https://www.etsi.org/deliver/etsi_gr/IP6/001_099/006/01.01.01_60/gr_IP6006v010101p.pdf (Last visited:Dec. 5, 2021)
41. ETSI, GS MEC 003 (2016/03) “Mobile Edge Computing (MEC);Framework and Reference Architecture”, P9
42. ETSI, IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward . Retrieved from https://www.etsi.org/images/files/ETSIWhitePapers/etsi_WP35_IPv6_Best_Practices_Benefits_Transition_Challenges_and_the_Way_Forward.pdf (Late visited, May, 26,2021)
43. ETSI, IPv6 White Paper outlines best practices, challenges, benefits and the way forward. Retrieved from https://www.etsi.org/newsroom/news/1814-2020-08-etsi-ipv6-white-paper-outlines-best-practices-challenges-benefits-and-the-way-forward (Last visited:Dec. 5, 2021)
44. europarl.europa.eu, *REVIEW OF THE DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS. Retrieved from* https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive (Last visited: Oct.23, 2021)
45. European Commision, “The EU’s Cybersecurity Strategy for the digital decade”, JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL”(2020),p.4
46. European Commision, “The EU’s Cybersecurity Strategy for the digital decade”, JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL”(2020)p.5,13,19
47. European Commision, “The EU’s Cybersecurity Strategy for the digital decade”, JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL(2020)p.14-20
48. European Commission, *Revised Directive on Security of Network and Information Systems(NIS2). Retrieved from* https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2 (Last visited: Oct.23, 2021)

49. European Parliament, BRIEFING EU Legislation in Progress :The NIS 2 Directive,pp.1-2. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf (Last visited: Oct.23,2021)
50. Giulio Grassi et al., VANET via Named Data Networking, Retrieved from https://named-data.net/publications/vanet_via_ndn_infocom_nom/ (Last visited:Dec. 5, 2021)
51. Google IPv6 Statistics. Retrieved from https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption (last visited, 2021/5/25).
52. GSMA (2017/07) " An Introduction to Network Slicing" Retrieved from https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf (2021/10/27)
53. GSMA (2019/04) "IMEI Allocation and Approval Process" Retrieved from https://www.gsma.com/newsroom/wp-content/uploads//TS.06-v16.0.pdf ,P4 (2021/10/27)
54. GSMA (2020/06) "DNS Guidelines for Service Providers and GRX and IPX Providers" Retrieved from https://www.gsma.com/newsroom/wp-content/uploads//IR.67-v16.0.pdf , P20 (2021/10/25)
55. GSMA(2015/01) "E.164 - regulatory exceptions for IoT connected services" Retrieved from https://www.gsma.com/iot/wp-content/uploads/2017/11/E.164position.pdf （2021/10/27）
56. GSMA(2020/06) "DNS Guidelines for Service Providers and GRX and IPX Providers" Retrieved from https://www.gsma.com/newsroom/wp-content/uploads//IR.67-v16.0.pdf,P.20 (2021/10/27)
57. GSMA, E.164 - regulatory exceptions for IoT connected services, Retrieved from https://www.gsma.com/iot/iot-knowledgebase/e-164-regulatory-exceptions-iot-connected-services-gsma/ (Last visited:Dec. 5, 2021)
58. Chih-Nan Hu, Shih-Hsiung Lee& Chu-Sing Yang(2017). Numbering plan for M2M and IoT services - A study of United States, Japan, China and Taiwan.IEEE, 2017 International Conference on Information Society (i-Society).
59. Doi: 10.23919/i-Society.2017.8354667

ICANN GNSO - Final Report on the new gTLD Subsequent Procedures Policy Development Process. Retrieved from https://gnso.icann.org/sites/default/files/file/field-file-attach/final-report-newgtld-subsequent-procedures-pdp-20jan21-en.pdf (Last visited:Jul. 15, 2021)

60. ICANN OCTO, Non-IP Networking (NIN). Retrieved from <https://www.icann.org/en/system/files/files/octo-026-12jul21-en.pdf> (Last visited:Dec. 5, 2021)
61. ICANN Office of the Chief Technology Officer ,"5G Technology", Alain Durand,OCTO-004(2020), Retrieved from https://www.icann.org/en/system/files/files/octo-004-23jan20-en.pdf
62. ICANN Office of the Chief Technology Officer," New IP", Alain Durand,OCTO-017 (2020) , Retrieved from <https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf>
63. ICANN Security and Stability Advisory Committee（SSAC）,"The DNS and the Internet of Things: Opportunities, Risks, and Challenges " ,*SAC 105*(2019)p.11
64. ICANN Security and Stability Advisory Committee（SSAC）,"The DNS and the Internet of Things: Opportunities, Risks, and Challenges " ,*SAC 105*(2019)p.14-17
65. ICANN, About the GAC- Operating Principles. Retrieved from <https://gac.icann.org/operating-principles/operating-principles?language_id=11>（Last visited:2021/11/08）
66. ICANN, Beginner's Guide to Participating in ICANN, 2013 . Retrieved from <https://www.icann.org/resources/files/participating-2013-11-08-en>（Last visited:2021/5/23）
67. ICANN, Domain Name System Security Facilitation Initiative Technical Study Group Begins Its Work, July 1, 2020, Retrieved from <https://www.icann.org/en/blogs/details/domain-name-system-security-facilitation-initiative-technical-study-group-begins-its-work-1-7-2020-en
68. ICANN，ICANN Geographic Regions.Retrieved from <https://meetings.icann.org/en/regions>.
69. ICANN, Security and Stability Advisory Committee(SSAC),Retrieved from <https://www-icann-org.translate.goog/groups/ssac?_x_tr_sl=en&_x_tr_tl=zh-TW&_x_tr_hl=zh-TW&_x_tr_pto=nui,sc>（Last visited:2021/11/08）

70. IEC, Industrial communication networks- Network and system security －Part 3-3: System security requirements and security levels, (IEC 62443-3-3) , ed.1, Aug., 2013, p.14..
71. IEC, Security for industrial automation and control systems－Part, 4-2: Technical security requirements for IACS components (IEC 62443-4-2) , ed.1, Feb., 2019, p.15.
72. IEEE Access，Vol 8.. Retrieved from https://ieeexplore.ieee.org/abstract/document/9099823
73. IETF, Enterprise IPv6 Deployment Guidelines. Retrieved from https://tools.ietf.org/html/rfc7381（Late visited: May,26,2021）
74. IMDA, IMDA Launches IoT Cyber Security Guide to Help Enterprise Users and Vendors Secure IoT Systems, https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2020/IMDA-Launches-IoT-Cyber-Security-Guide-to-Help-Enterprise-Users-and-Vendors-Secure-IoT-Systems (Lasted visited：Oct. 12. 2021)
75. Info-communications Media Development Authority, Internet of Things(IoT) Cyber Security Guide. Retrieved from https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf (Lasted visited：Oct. 9. 2021)
76. Info-communications Media Development Authority, Internet of Things(IoT) Cyber Security Guide Annex A Foundational Concepts, Retrieved from https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide-Annex-A.pdf (Lasted visited：Oct. 12. 2021)
77. International Data Corporate (IDC), "The Growth in Connected IoT Devices Is Expected to Generate 79.4 ZB of Data in 2025," 19 June 2019.（Lasted visited：Nov. 29. 2021）
78. Internet Engineering Task Force (1989/10) “Requirements for Internet Hosts -- Application and Support”, P12, RFC1123 Retrieved from https://tools.ietf.org/html/rfc1123
79. ITU, “FG NET 2030” , https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx.(Lasted visited：Nov. 29. 2021)

80. ITU, *Global Cybersecurity Index 2018*, pp.16.28,(2018). Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf(Last visited:Apr. 19, 2020)
81. ITU-T, ITU-T TSAG (Study Period 2017) Temporary Document 789: Action plan related to the Resolutions and Opinion of WTSA-16. Retrieved from https://www.itu.int/md/T17-TSAG-200921-TD-GEN-0789 (Last visited:Jul. 15, 2021)
82. ITU-T, Recommendation E.212 (2016) Amendment 1 (07/18), Retrieved from https://www.itu.int/rec/T-REC-E.212-201807-I!Amd1/en (Last visited:Dec. 5, 2021)
83. ITU-T, Recommendation E.212 (2016) Amendment 3 (12/20). Retrieved from https://www.itu.int/rec/T-REC-E.212-202012-I!Amd3/en (Last visited:Dec. 5, 2021)
84. ITU-T, Recommendation Y.2001 (12/04) - General overview of NGN, Retrieved from https://www.itu.int/rec/T-REC-Y.2001-200412-I/en (Last visited:Dec. 5, 2021)
85. ITU-T, Resolutions and Opinions 2016 editions. Retrieved from https://www.itu.int/pub/T-RES (Last visited:Jul. 15, 2021)
86. ITU-T, Standards Development. Retrieved from https://www.itu.int/en/ITU-T/about/Pages/development.aspx (Last visited:Jul. 15, 2021)
87. ITUT-T, WTSA-20. Retrieved from https://www.itu.int/en/ITU-T/wtsa20/Pages/default.aspx (Last visited:Jul. 15, 2021)
88. J. Jeong (2021/08)" DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks"
89. J. Jeong, DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks. Retrieved from https://www.ietf.org/id/draft-jeong-ipwave-iot-dns-autoconf-11.html (Last visited:Dec. 5, 2021)
90. Jaehoon Paul Jeong, Sejun Lee, Jung-Soo Park(2015/10) "DNS Name Autoconfiguration for Internet of Things Devices"Retrieved from https://datatracker.ietf.org/doc/draft-jeong-6man-iot-dns-autoconf/ （2021/11/29）
91. Jaehoon Paul Jeong, Sejun Lee, Jung-Soo Park, "DNS Name Autoconfiguration for Internet of Things Devices", Oct 14 2015,

available at https://datatracker.ietf.org/doc/draft-jeong-6man-iot-dns-autoconf/（Lasted visited：Nov. 29. 2021）
92. Lixia Zhang et al., Named Data Networking, ACM SIGCOMM Computer Communication Review, Volume 44, Number 3, July 2014.
93. MFA, MulteFire Alliance (MFA) simplifies path to 5G private network deployment for Enterprise, Retrieved from https://www.mfa-tech.org/2021/06/22/mfa-simplifies-path-to-5g-private-network-deployment-for-enterprise/ (Last visited:Dec. 5, 2021)
94. MobileID Retrieved from https://www.twca.com.tw/product/c0cf07bd-25ab-42d8-a1bd-3e6e71950113 (2021/10/22)
95. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecirity Version 1.1*, (April. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf(Last visited: May,17,2021)
96. NDN Project, NDN Technical Report NDN-0043: The Design and Implementation of the NDN Protocol Stack for RIOT-OS, Retrieved from https://named-data.net/publications/techreports/ndn-0043-2-ndn-riot/ (Last visited:Dec. 5, 2021)
97. NDN Project, NDN Testbed, Retrieved from https://named-data.net/ndn-testbed/ (Last visited:Dec. 5, 2021)
98. NDN Project, NFD Developer's Guide (Latest Revision 11), Retrieved from https://named-data.net/publications/techreports/ndn-0021-11-nfd-guide/ (Last visited:Dec. 5, 2021)
99. NDN Project, NFD Overview. Retrieved from https://named-data.net/doc/NFD/0.7.0/overview.html (Last visited:Dec. 5, 2021)
100. ndnSIM Documentation, Introduction. Retrieved from https://ndnsim.net/current/intro.html (Last visited:Dec. 5, 2021)
101. Network 2030 A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyon, ,2019. Retrieved from https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/White_Paper.pdf（Last visited:2021/9/6）
102. NGMN (2021/2/17) "Pre-Commercial Networks Trials Major Conclusions" Retrieved from

https://ngmn.org/wp-content/uploads/210406-NGMN-PrecomNW_Trials_Major_Conclusions-v2.pdf, P12-P14 (2021/12/02)
103. NIST, IPv6 Profile. Retrieved from https://www.nist.gov/publications/nist-ipv6-profile (Last visited:Dec. 5, 2021)
104. NIST, Secure Domain Name System (DNS) Deployment Guide,pp ES1-3. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf
105. NIST, Updates USGv6 Program in Support of New Federal IPv6 Initiatives. Retrieved from https://www.nist.gov/news-events/news/2020/12/nist-updates-usgv6-program-support-new-federal-ipv6-initiatives (Last visited:Dec. 5, 2021)
106. Ox software GmbH, " OX Whitepaper DNS in a 5G Network New Requirements and Demands" ,*WHITEPAPER VERSION 1.0*,p.5
107. Ox software GmbH, " OX Whitepaper DNS in a 5G Network New Requirements and Demands" ,*WHITEPAPER VERSION 1.0*,p.5 -6
108. Ox software GmbH, " OX Whitepaper DNS in a 5G Network New Requirements and Demands" ,*WHITEPAPER VERSION 1.0*,p.9
109. REDSCAN, *NIS2: what organisations need to know about proposed changes to the NIS Directive*. Retrieved from https://www.redscan.com/news/nis2-what-organisations-need-to-know/ (Last visited: Oct.23, 2021)
110. REDSCAN, *NIS2: what organisations need to know about proposed changes to the NIS Directive*. Retrieved from https://www.redscan.com/news/nis2-what-organisations-need-to-know/ (Last visited: Oct.23, 2021)
111. Salma Brihi; Anas Ghamizi; Karim Chakri, ” UAV for IoT Communications: Beam Selection Using Matching Game and Network Slicing”, Dec. 4 2020. Retrieved from https://ieeexplore.ieee.org/document/9272510 （Lasted visited：Nov. 29. 2021）
112. Shared HNI for CBRS Range. Retrieved from https://www.atis.org/wp-content/uploads/2020/10/IMSI-CBRS-Guidelines_v2.pdf (Last visited:Dec. 5, 2021)
113. Statista (2021/10/19), “Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030”. Retrieved from https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (2021/11/26)

114. T. Yanase, H. Tanaka, and H. Suzuki, “Flexible name autoconfiguration for iot devices,” in Proceedings of The 11th International Conference on Mobile Computing and Ubiquitous Network (ICMU 2018), 2018.
115. Trump whitehouse, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Retrieved from https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (Last visited：May, 17, 2021)
116. TWNIC, Taiwan IPv6 Global Ranking: 6. Retrieved from https://ipv6now.twnic.tw/ipv6/index.html (last visited, 2021/5/25).
117. US DoD, Implementation of Internet Protocol Version 6. Retrieved from https://media.defense.gov/2021/Jul/13/2002761414/-1/-1/0/DOD-MEMORANDUM-DEPARTMENT-OF-DEFENSE-IMPLEMENTATION-OF-INTERNET-PROTOCOL-VERSION-6.PDF (Last visited:Dec. 5, 2021)
118. US EOP, Completing the Transition to Internet Protocol Version 6. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf (Last visited:Dec. 5, 2021)
119. US FERC, Internet Protocol Version 6 (IPv6) Policy. Retrieved from https://www.ferc.gov/media/ferc-internet-protocol-version-6-ipv6-policy (Last visited:Dec. 5, 2021)
120. Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound (1997/04) "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136 Retrieved from https://www.rfc-editor.org/rfc/rfc2136
121. Zhiyi Zhang et al.,. NDNoT: A Framework for Named Data Network of Things, ACM Information Centric Networking Conference 2018. Retrieved from https://conferences.sigcomm.org/acm-icn/2018/proceedings/icn18posterdemo-final22.pdf (Last visited:Dec. 5, 2021)
122. 總務省，〈IoT 時代の電気通信番号に関する研究会 報告書〉，7/3，2019，
123. 總務省，〈M2M 等専用番号の創設〉，1/4，2017，<https://www.soumu.go.jp/menu_news/s-news/01kiban06_02000056.html>

貳、 中文文獻

1. DIGITIMES，〈5G 數位轉型製造業應把握這 5 大關鍵〉，11/24，2020，<https://www.digitimes.com.tw/iot/article.asp?cat=158&cat1=20&cat2=&id=0000598842_SMO76GDH50POOE1NJ9B5O>。
2. iThome，〈歐洲的 IPv4 位址正式用罄〉，11/27，2019，<https://www.ithome.com.tw/news/134437>。
3. Microsoft Build,〈新加坡多層雲端安全性（MTCS）標準〉，<https://docs.microsoft.com/zh-tw/compliance/regulatory/offering-mtcs-singapore>。
4. Microsoft，〈什麼是 Azure Private DNS?〉，4/9，2021，<https://docs.microsoft.com/zh-tw/azure/dns/private-dns-overview>。
5. Microsoft Build，〈新加坡多層雲端安全性（MTCS）標準〉<https://docs.microsoft.com/zh-tw/compliance/regulatory/offering-mtcs-singapore>。
6. NCC，行動網路識別碼核配現況，2021/06，< https://www.ncc.gov.tw/chinese/files/14050/行動網路識別碼核配現況.pdf>。
7. NCC，電信網路編碼計畫，2016/12，<http://www.ncc.gov.tw/chinese/files/07060/192_952_070606_1.doc>。
8. NCC NEWS,”一物一號 效率可靠安全的電信級 IoT 簡介電信網路中之 IoT 編碼”，July 2017，p.1-p.6，<https://www.ncc.gov.tw/chinese/files/ebook/154/ebook/NCC%20News10607.pdf >。
9. Semisphere，〈[資安] DNS over HTTPS（DoH）與 DNS over TLS（DoT）〉，6/29，2019，<https://firsemisphere.blogspot.com/2019/06/dns-over-httpsdohdns-over-tlsdot.html>。

10. Stli，〈歐盟執委會提出《歐盟數位十年網路安全戰略》〉，1/2021，<https://stli.iii.org.tw/article-detail.aspx?no=55&tp=1&i=180&d=8602>。
11. TWNIC，〈ICANN 技術長辦公室改名為「識別碼研究、運作及安全部門」〉， 6/27，2020，<https://blog.twnic.tw/2020/06/30/7550/>。
12. TWNIC，ICANN 組織簡介（一），台網中心電子報，2017 年 7 月，< http://www.myhome.net.tw/2017_07/p08.htm >。
13. 人民網，《中國移動互聯網發展報告(2021)》正式發布，2021 年 7 月 22 日，<http://finance.people.com.cn/n1/2021/0722/c1004-32166880.html >。
14. 中華民國交通部，「電信網路編碼計畫」，<https://www.motc.gov.tw/uploaddowndoc?file=mlaw/2016112216093 90.pdf&filedisplay=%E9%9B%BB%E4%BF%A1%E7%B6%B2%E8% B7%AF%E7%B7%A8%E7%A2%BC%E8%A8%88%E7%95%AB.pdf &flag=doc >。
15. 中華人民共和國中央人民政府，中共中央辦公廳國務院辦公廳印發《推進互聯網協議第六版（IPv6）規模部署行動計劃》，2017 年 11 月 26 日，<http://www.gov.cn/zhengce/2017-11/26/content_5242389.htm>。
16. 中華人民共和國中央人民政府，關於加快推進互聯網協議第六版（IPv6）規模部署和應用工作的通知，2021 年 7 月 12 日，<http://www.gov.cn/zhengce/zhengceku/2021-07/23/content_5626963.htm >。
17. 中國信息通訊研究院，物聯網白皮書（2020 年），第 19-20 頁，2020 年 12 月，

<http://www.caict.ac.cn/kxyj/qwfb/bps/202012/P020201215379753410419.pdf >。

18. 行政院（2019 年 5 月 10 日），台灣 5G 行動計畫（2019-2022 年 <https://digi.ey.gov.tw/File/76CD1E43C2424FF8>。
19. 先進國家業 IPV4/IPV6 位址經驗分析報告〉，《九十八年度新一代網際網路協定互通認證計畫期末研究報告附件》，法規政策分類，2009，p.165 <http://www.ipv6.org.tw/docu/elearning8_2009/1009804292b-08.pdf>。
20. 科技法律研究所，〈為了確保網絡安全，歐盟頒佈新的網路安全計畫〉，07，2013，<tli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=6261> 。
21. 科技新報，〈網路安全的第一道防線，就從 DNS 防護做起〉，8/6，2020，<https://technews.tw/2020/08/06/infoblox-dns-security/>。
22. 財團法人臺灣網路資訊中心，〈Native IPv6 連網環境建置及 IPv6 用戶安全防護研析〉，2020。
23. 國立台灣大學計算機及資訊網路中心電子報，〈DNSSC 安全計設簡介〉，9/20，2012，<https://www.cc.ntu.edu.tw/chinese/epaper/0022/20120920_2206.html >。
24. 國立台灣大學計算機及資訊網路中心電子報，〈DNSSC 安全計設簡介〉，9/20，2012，<https://www.cc.ntu.edu.tw/chinese/epaper/0022/20120920_2206.html >。
25. 國家通訊傳播委員會，出席 GSMA 行動 360 系列—數位化社會會議出國報告書，2018 年 11 月，<https://www.ncc.gov.tw/chinese/files/19091/5012_41986_190917_1.pdf >。

26. 國際通傳產業動態觀測，〈歐盟提撥 3,800 萬歐元以保護關鍵基礎設施免受網路威脅〉，8/24，2020。
<https://intlfocus.ncc.gov.tw/xcdoc/cont?xsmsid=0J210565885111070723&sid=0K237522717263495777>。
27. 新世紀智庫論壇第 54 期(2011 年 6 月 30 日)。國際標準化組織(ISO)。
< http://www.taiwanncf.org.tw/ttforum/54/54-18.pdf >。
28. 創泓科技，〈DNS 資訊安全防護的最後一哩路〉，<https://www.uniforce.com.tw/edcontent_d.php?lang=tw&tb=1&id=217>。
29. 經濟部標準檢驗局（2008 年 8 月 15 日）。國際通訊聯盟(ITU)。<https://www.bsmi.gov.tw/wSite/ct?xItem=16648&ctNode=9175&mp=1>。
30. 經濟部標準檢驗局（2009 年 6 月）。產業技術標準活絡及推廣委辦計畫深入國際標準化組織。
<https://www.bsmi.gov.tw/wSite/public/Data/f1352964204876.pdf>。
31. 經濟部標準檢驗局(2009 年 9 月)。深入國際標準化組織。
<http://www.standards.org.tw/CKEdit/upload/21/files/201506080817.pdf >。
32. 黃彥棻，〈新加坡用總理高度揭露國家資安戰略，臺灣呢?〉，《資安周報第 45 期》，iThome，2016 年 10 月 19 日。
33. 資安人，〈DNS 安全防護傘-DNSSEC〉，9/6，2010，<https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=5886>。
34. 達友科技，〈 DNS 安全防護方案〉，<https://www.docutek.com.tw/solution.php?pk=21>。
35. 數位時代，〈5G、純網銀上路，資安風險更棘手？4 大資安趨勢老闆需注意〉，12/13，2019

<https://www.bnext.com.tw/article/55909/trendmicro-estimation2020-cybersecurity>。

36. 駐西班牙台北經濟辦事處，西班牙「Expansión 日報」9 月 24 日報導：行動通訊協會(GSMA)宣布，2021 年在西班牙巴塞隆納舉辦之世界行動通訊大會(MWC)將延至 6 月辦理，2020 年 9 月，< https://www.roc-taiwan.org/es/post/13735.html >。

附錄二、中英文名詞對照

英文全名	英文縮寫	中文名稱
3rd Generation Partnership Project	3GPP	第三代合作夥伴計畫
4th Generation mobile communication	4G	第四代行動通訊系統
5G Core Network	5GC	5G 核心網路
5G Globally Unique Temporary UE Identity	5G-GUTI	5G 全球唯一臨時識別碼
5G New Radio Technology	5G NR	5G 新無線電技術
5G Non-standalone	5G NSA	5G 非獨立組網
5G-Residential Gateway	5G-RG	5G 家用閘道器
5G Standalone	5G SA	5G 獨立組網
Access and Mobility management Function	AMF	存取與行動管理功能
Advanced Persistent Threat	APT	進階持續性威脅
Artificial Intelligence	AI	人工智慧
Access Control List	ACL	存取控制清單
Access Network	AN	存取網路
Access Point	AP	存取點
Access Point Name	APN	存取點名稱
Access Stratum	AS	接取層
American National Standards Institute	ANSI	美國國家標準協會
Authentication Server Function	AUSF	身份驗證伺服器功能
Authentication Center	AuC	驗證中心
Authentication and Key Agreement	AKA	驗證和金鑰協議
Administration And Maintenance	OAM	管理維運系統
Allocation and Retention Priority	ARP	分配和保留優先權
Application Programming Interface	API	應用程序介面

英文全名	英文縮寫	中文名稱
Asymmetrical Digital Subscriber Line	ADSL	非對稱數位用戶迴路
Asynchronous Transfer Mode	ATM	非同步傳輸模式
Augmented Reality	AR	擴增實境
Authentication Header	AH	認證表頭
Automatic Neighbour Relation	ANR	自動建立鄰近基台關係
Border Gateway Protocol	BGP	邊界閘道器通訊協定
Broadcast Control CHannel	BCCH	廣播控制通道
Broadcast Multicast Service Center	MBSC	廣播及群播服務中心
By Your Own Device	BYOD	自攜裝置
Car 2 Car Communication Consortium	C2CCC	車對車通訊協會
Car Connectivity Consortium	CCC	車聯網聯盟
Carrier Aggregation	CA	載波聚合
Carrier Aggregation enhancement	CA enhancement	載波聚合增強
cCll Identification	Cell ID	細胞識別
Cellular Internet of Thing	CIoT	行動物聯網
Cellular Telecommunications Industry Association	CTIA	行動電信產業協會
Cellular-V2X	C-V2X	蜂巢式車對任何物體通訊
Centrulized Unit	CU	中央單元
Certification Authority	CA	驗證機構
Channel Quality Indicator	CQI	通道品質指標
Clear Channel Assessment	CCA	空閒通道評估
Cloud Radio Access Netwrok	C-RAN	雲端無線存取網路
Code Division Multiple Access	CDMA	分碼多重存取
Code Division Multiplexing	CDM	分碼多工
Communication Service Management Function	CSMF	通訊服務管理功能
Content Delivery Network	CDN	內容傳遞網路
Coordinated MultiPoint transmission	CoMP	協同多點傳送
Core Network	CN	核心網路

英文全名	英文縮寫	中文名稱
Country Code Top Level Domain	ccTLD	國家（或地區的）頂級網域
Critical Information Infrastructures	CII	關鍵資訊基礎設施
Critical Information Infrastructure Protection	CIIP	關鍵資訊基礎設施保護計畫
Cybersecurity Framework	CSF	網路安全框架
Cyclic Redundancy Check	CRC	循環冗餘校驗
Dynamic Host Configuration Protocol	DHCP	動態主機配置協定
Data Network	DN	數據網路
Data Network – Authentication, Authorization and Accounting	DN-AAA	數據網路-認證、授權與計費
Data Network Name	DNN	數據網路名稱
Denial of Service	DoS	阻斷攻擊
Directive on security of network and information systems	NIS Direvtive	網路與資訊系統安全指令
Distributed Denial of Service	DDoS	分散式阻斷攻擊
Distributed Unit	DU	分布單元
DNS Security Extensions	DNSSEC	DNS 安全擴展
Domain Name	DN	網域名稱
Domain Name System	DNS	網域名稱系統
Domain Name System Security Facilitation Initiative Technical Study Group	DSFI-TSG	DNS 安全協調技術研究小組
Encapsulating Security Payload Header	ESP	資料封裝加密表頭
enhanced Machine Type Communication	eMTC	增強型機器型態通訊
enhanced Mobile BroadBand	eMBB	增強型行動寬頻
enhanced Multimedia Broadcast Multicast Service	eMBMS	增強型多媒體廣播多播服務
enhanced Narrow Band Internet of Things	eNB-IoT	增強型窄頻段物聯網

英文全名	英文縮寫	中文名稱
enhanced Physical Downlink Control CHannel	ePDCCH	增強型實體下行控制通道
enhancements of VoLTE	eVoLTE	增強版長期演進通話技術
eNode B	eNB	演進基站收發信台
EPS Mobility Management	EMM	進化封包系統移動管理
EPS Session Management	ESM	演進分封系統之會談管理
EU General Data Protection Regulation	EU GDPR	歐盟個人資料保護規則
European Telecommunications Standards Institute	ETSI	歐洲電信標準協會
EUTRA-NR dual connectivity	EN-DC	演進版通用陸地無線存取網路-新無線電技術雙連結
Evolved Multimedia Broadcast Multicast System	eMBMS	演進的多媒體廣播群播服務
Evolved Multimedia Broadcast/Multicast Service	eMBMS	演進多媒體廣播/群播服務
Evolved Node B	eNB	基地台
Evolved Packet Core	EPC	演進分封核心網
Evolved Packet System	EPS	演進的分封系統
Evolved Universal Terrestrial Radio Access Network	EUTRAN	演進版通用陸地無線存取網路
Evolved Vehicle-to-Everything	eV2X	演進車對任何物體通訊
Extension Authentication Protocol for UMTSAuthentication and Key Agreement	EAP-AKA	適用於 UTMS 驗證與金鑰協議之延伸驗證通訊協定方法
Fiber To The Building	FTTB	光纖到大樓
Fiber To The Curb	FTTC	光纖到街角（鄰 / 路邊）
Fiber To The Home	FTTH	光纖到府
Fifth Generation mobile communication	5G	第五代行動通訊
Fixed BroadBand	FBB	固網寬頻
Fixed Wireless Residential Gateway	FN-RG	固定-無線家用閘道器
Frequency Division Duplex	FDD	分頻雙工

英文全名	英文縮寫	中文名稱
Gateway GPRS Support Node	GGSN	GPRS 服務支援節點
General Names Supporting Organization	GNSO	通用域名支援組織
General Packet Radio Service	GPRS	通用封包無線服務
General Top Level Domain	gTLD	通用頂級網域
Global Positioning System	GPS	全球衛星定位系統
Global Resilience Federation Asia Pacific	GRFAPAC	亞太地區全球彈性聯盟
Global System for Mobile Communication	GSM	全球行動通訊系統
Global System for Mobile communications Association	GSMA	全球行動通訊系統協會
GPRS Tunneling Protocol	GTP	分封數據服務隧道協定
Guaranteed Bit Rate	GBR	保證位元率
Heterogeneous Network	HetNet	異質網路
High Speed Downlink Packet Access	HSPDA	高速下行封包存取
High Speed Packet Access	HSPA	高速封包存取
Home Location Register	HLR	本籍位置記錄器
Home Public Land Mobile Network	HPLMN	本地公用陸地移動網路
Home Radio Frequency	home RF	無線電家庭網路
Home Subscriber Server	HSS	本地用戶伺服器
Homogenous Extended Service Set IDentifier	HESSID	同質延伸服務集識別碼
HyperText Transfer Protocol	HTTP	超文本傳輸協定
HyperText Transfer Protocol Secure	HTTPS	超文本傳輸安全協定
Internet Corporation for Assigned Names and Numbers	ICANN	網際網路名稱與數字位址分配機構
Identity	ID	識別
Identifier Research, Operations and Security	IROS	識別碼研究、運作及安全部門
Internet Engineering Task Force	IETF	網際網路工程任務組

英文全名	英文縮寫	中文名稱
Industrial Control Systems	ICS	工業控制系統
Information Security Management System	ISMS	資訊安全管理系統
Infrastructure-to-Infrastructure	I2I	路對路通訊
Infrastructure-to-Vehicle	I2V	路對車通訊
Instant Message Service	IMS	即時訊息服務
Institute of Electrical and Electronics Engineers	IEEE	電機電子工程師學會
Integrated Service Digital Network	ISDN	整合服務數位網路
Interior Gateway Protocols	IGPs	內部閘道協定
Interleaved Frequency Division Multiple Access	IFDMA	交錯式分頻多重存取
International Mobile Subscriber Identity	IMSI	國際行動用戶識別碼
International Mobile Telecommunications-2000	IMT-2000	ITU 第三代行動通訊
International Mobile Telecommunications-2020	IMT-2020	ITU 第五代行動通訊
International Mobile Telecommunications-Advanced	IMT-Advanced	進階型國際行動電信系統
Internet Service Provider	ISP	網際網路服務供應商
International Telecommunication Union	ITU	國際電信聯合會聯盟
International Telecommunication Union - Radiocommunication Sector	ITU-R（Radio）	國際電信聯盟無線分支
International Telecommunication Union - Telecommunication Standardization Sector	ITU-T	國際電信聯合會電信標 準化部門
Internet Content Provider	ICP	網路內容供應商
Internet Control Message Protocol	ICMP	網路控制訊息協定
Internet Data Center	IDC	網路資料中心
International Eletronic Committee	IEC	國際電工委員會

英文全名	英文縮寫	中文名稱
Internet Engineering Task Force	IETF	國際網路工程研究團隊
Internet Key Exchange	IKE	網際網路金鑰交換
internet mode	i-mode	上網模式
Internet Protocol	IP	網際網路通訊協定
Internet Protocol Security	IPSec	網際網路安全協定
Internet Protocol version 4	IPv4	第四版網際網路協定
Internet Protocol version 6	IPv6	第六版網際網路協定
International Society for Automation	ISA	國際自動化學會
International Standard	IS	國際標準
Intrusion-detection system	IDS	入侵檢測系統
ITU Radiocommunication Sector	ITU-R	國際電信聯合會聯盟_無線分支
ITU Telecommunication Development Sector	ITU-D	國際電信聯合會聯盟_電信發展分支
ITU Telecommunication Standardization Sector	ITU-T	國際電信聯合會聯盟_電信標準化分支
International Organization for Standardization	ISO	國際標準組織
Key Performance Indicators	KPI	關鍵績效指標
Licensed-Assisted Access to unlicensed spectrum	LAA	授權頻帶輔助之非授權頻譜存取技術
Local Area Network	LAN	區域網路
Logical Channel	LCH	邏輯通道
Logical Link Control	LLC	邏輯鏈結控制
Long Term Evolution	LTE	長期演進技術
Long Term Evolution_Advanced	LTE-A	進階版長期演進技術
Low Power Wide Area	LPWA	低功耗廣域通訊
LTE+WLAN Aggregation	LWA	LTE 與無線區域網路聚合
LTE-NR Dual Connectivity	EN-DC	長期演進技術與新無線電技術雙連結

英文全名	英文縮寫	中文名稱
LTE-WLAN Aggregation Adaptation Protocol	LWAAP	LTE 與無線區域網路聚合適配協定
LTE-WLAN Radio Level Integration	LWRLI	長期演進技術與無線區域網路之無線層整合
MAC Identification	MID	媒體存取控制識別碼
Machine Type Communication	MTC	機器類型通訊
Machine Type Communication enhancement	MTC enhancement	機器型態通訊增強
Man-in-the-Middle Attack	MITM	中間人攻擊
massive Machine Type Communication	mMTC	大量機器型態通訊
Massive Machine Type Communications	mMTC	巨量設備間通訊
Master eNB	MeNB	主基地台
Maximum Transmission Unit	MTU	最大傳輸單位
Media Access Control	MAC	媒體存取控制
Message Information Block	MIB	訊息資訊塊
Multi-access Edge Computing	MEC	多重接取邊緣運算
micro second	us	微秒
mili second	ms	毫秒
millimeter Wave	mmW	毫米波
Mobile BroadBand	MBB	行動寬頻
Mobile Content Provider	MCP	行動內容供應商
Mobile Number Portability	MNP	行動通訊號碼可攜
Mobile Satellite Service	MSS	衛星行動服務
Mobile Station	MS	行動用戶
Mobile Switching Center	MSC	行動交換中心
Mobile Virtual Network Operator	MVNO	行動虛擬網路業者
Mobile Virtual Private Network	MVPN	行動虛擬私有網路
Mobility Management Element	MME	行動管理單元
Mobility Management Entity	MME	移動性管理實體
Multimedia Broadcast Multicast Service	MBMS	多媒體廣播群播服務

英文全名	英文縮寫	中文名稱
Multimedia Message Service	MMS	多媒體訊息服務
Multiple Input Multiple Output	MIMO	多重輸入多重輸出
Multi-Protocol Label Switching	MPLS	多重通訊協定標籤交換技術
Multi-Tier Cloud Security	MTCS	多層雲端安全性
Named-service transaction	NST	已命名之服務交換
Narrow Band Internet of Things	NB-IoT	窄頻段物聯網
Narrowband Machine to Machine	NB M2M	窄頻段機器對機器通訊
National Communications Commission	NCC	國家通訊傳播委員會
National Digital Identity	NDI	國家數位身份
National Institute of Standards and Technology	NIST	國家標準技術研究所
Network Exposure Function	NEF	網路開放功能
Network Function Virtualization	NFV	網路功能虛擬化
Network Access Identity	NAI	網路接取身分
Network Attached Storeage	NAS	網路連接儲存
Network Address Translation	NAT	網址轉換
Network Slice Selection Assistance Information	NSSAI	網路切片選擇輔助資訊
Network Slice Management Function	NSMF	網路切片管理功能
Network Slice Type	NEST	網路切片類別
Network Slice Selection Function	NSSF	網路切片選擇功能
Network Function	NF	網路功能
Network Function Virtualization	NFV	網路功能虛擬化
Network Management System	NMS	網路管理系統
new generation NB	gNB	新世代基地台
New Radio Multiple Input Multiple Output	NR MIMO	新無線多重輸入多重輸出技術
New Radio Technology	NR	新無線電技術

英文全名	英文縮寫	中文名稱
Next Generation Mobile Network	NGMN	下世代行動網路
Next Generation Mobile Networks Alliance	NGMN Alliance	次世代行動網路聯盟
Non Access Stratum	NAS	非存取層
Non Public Network	NPN	非公眾網路
Non-3GPP Inter Working Function	N3IWF	非 3GPP 互連功能介面
Office of the Chief Technology Officer	OCTO	首席技術官辦公室
Orthogonal Frequency Division Multiplexing	OFDM	正交分頻多工
Orthogonal Frequency Division Multiplexing Access	OFDMA	正交分頻多重存取
Over-The-Air activation	OTA	空中啟動
Open Authorization	OAuth	開放授權
Open Shortest Path First	OSPF	開放式最短路徑優先
Operating Support System	OSS	維運支援系統
Over-the-top Service	OTT	透過網際網路直 接向用戶提供的應用服 務
Packet data network GateWay	P-GW	分封數據網路閘道器
Packet Switching Network	PSN	分封交換網路
Point to Point Protocol	PPP	點對點通訊協定
Power Saving Mode	PSM	省電模式
Primary Cell	PCell	主細胞
Primary Secondary Cell	PSCell	主要次細胞
Private Branch eXchange	PBX	用戶專用交換機
Public Land Mobile Network	PLMN	公眾陸地行動網路公用陸地移動網路
Public Switched Telephone Network	PSTN	公眾交換電信網路
Public Warning System	PWS	公眾示警系統
Policy Control Function	PCF	策略控制功能
Policy and Charging Rules Function	PCRF	策略與計費規則功能

英文全名	英文縮寫	中文名稱
Packet Data Network	PDN	封包數據網路
Packet Data Network Gateway	PDN Gateway, PGW	封包數據網路閘道器
QoS Class Identifier	QCI	服務品質級別指標
Quality of Experience	QoE	使用者經驗
Quality of Service	QoS	服務品質
Quick Response Code	QR code	快速反應條碼
Radio Access Network	RAN	無線存取網路
Radio Access Network Application Par	RANAP	無線存取網路應用端
Radio Access Network slice	RAN slice	無線存取網路切片
Radio Access Notification Area Code	RANAC	無線存取網路通報區域碼
Radio Frequency	RF	無線電頻率
Radio Frequency-IDentification	RFID	無線射頻辨識系統
Radio Resource Control	RRC	無線資源控制
Radio Resource Control Connected	RRC_CONNECTED	無線資源控制連線模式
Radio Resource Control Idle	RRC_IDLE	無線資源控制閒置模式
Regional Internet Registry	RIR	區域網際網路註冊機構
Remote Radio Head	RRH	遠端射頻頭端
Residential Gateway	RG	家用閘道器
Resource Certification	R-PKI	資源公鑰基礎設施
Resource Record Signature	RRSIG	資源紀錄簽章
Routing Area Update	RAU	路由區域更新
Second Generation	2G	第二代行動電話
Secondary Cell	SCell	次細胞
Secondary eNB	SeNB	次基地台
Secondary gNB	SgNB	次新世代基地台
Serving GateWay	S-GW	服務閘道器
Serving GPRS Support Node	SGSN	服務 GPRS 支援節點
Serving Grant interface	SGi	授權服務介面
Short Message Service	SMS	簡訊服務

英文全名	英文縮寫	中文名稱
Signal to Interference plus Noise Ratio	SINR	訊號對干擾加雜訊比
Session Management Function	SMF	會話管理功能
Security operation center	SOC	訊安全監控中心
Signal to Noise Ratio	SNR	訊號雜訊比
Signaling System number 7	SS7	第 7 訊號系統
Simple Network Management Protocol	SNMP	簡單網路管理協定
Software Definition Network	SDN	軟體定義網路
Subscriber Identity Module	SIM	用戶識別模組
Subscription Concealed Identifier	SUCI	用戶隱藏識別碼
Subscription Permanent Identifier	SUPI	用戶永久識別碼
Supervisory Control and Data Acquisition	SCDA	監控與數據採集系統
Synchronous Digital Hierarchy	SDH	同步數位階層
Synchronous Optical NETwork	SONET	同步光纖網路
Software-defined Network	SDN	軟體定義網路
Service-based Architecture	SBA	服務導向架構
SEcurity Anchor Function	SEAF	安全固定功能
Security-as-a-Service	SaaS	安全即服務
Security and Stability Advisory Committee	SSAC	安全及穩定諮詢委員會
Security Edge Protection Proxy	SEPP	安全邊緣保護代理伺服 器
Security Level - Component	SL-C	元件安全能力等級
Security Level - Target	SL-T	目標安全能力等級
Security Mode Command	SMC	安全模式指令
Self-organizing Network	SON	自組織網路
Signaling System Number 7	SS7	第七號信號系統
Special publication	SP	特別出版物
Statement of Applicability	SoA	適用性聲明書
Taiwan Association of Information and Communication Standards	TAICS	台灣資通產業標準協會

英文全名	英文縮寫	中文名稱
Technical Report	TR	技術報告
Technical Standard	TS	技術規範
Telecommunication Standardization Advisory Group	TSAG	電信標準化顧問組
Telecommunication Standardization Bureau	TSB	電信標準化局
The fifth Generation Mobile Network	5G	第 5 代行動網路技術
The fifth Generation Mobile Network Automotive Association	5GAA	第 5 代行動網路汽車協會
The fourth Generation Mobile Network	4G	第 4 代行動網路技術
The third Generation Mobile Network	3G	第 3 代行動網路技術
The Third Generation Partnership Project	3GPP	第 3 代合作夥伴計畫
Time Division - Synchronous Code Division Multiple Access	TD-SCDMA	分時同步分碼多重存取
Time Division Duplex	TDD	分時雙工
Time Division Multiple Acess	TDMA	分時多重存取
Time To Live	TTL	存留時間
Top Level Domain	TLD	頂級網域
Tracking Area	TA	追蹤區
Tracking Area Code	TAC	追蹤區碼
Tracking Area Identity	TAI	追蹤區辨別碼
Tracking Area Update	TAU	追蹤區更新
Transmission Control Protocol/Internet Protocol	TCP/IP	傳輸控制網際網路通訊協定
Transmit	TX	傳送
Transport Layer Security	TLS	傳輸層安全協議
Trusted Non-3GPP Access Network	TNAN	可信任的非 3GPP 接取網路
Trusted Non-3GPP Gateway Function	TNGF	可信任的非 3GPP 閘道器功能

英文全名	英文縮寫	中文名稱
Trusted WLAN Interworking Function	TWIF	可信任的 WLAN 的互連功能介面
Ultra Reliable and Low Latency Communication	URLLC	超高可靠性與低延遲通訊
Ultra Wide Band	UWB	超寬頻系統
UMTS Subscriber Identity Module	USIM	UMTS 用戶識別模組
Universal Mobile Telecommunications System	UMTS	通用移動通訊系統
Unified Data Management	UDM	統一數據管理
Uniform Resource Identifier	URI	統一資源識別碼
Uniform Resource Locator	URL	統一資源定址器
Uniform Resource Name	URN	統一資源名稱
User Equipment	UE	終端裝置
User Plane Function	UPF	用戶平面功能
Universal Integrated Circuit Card	UICC	通用積體電路卡
Vehicle to Everything	V2X	車間普及通訊
Vehicle to Infrastructure	V2I	車對路通訊
Vehicle to Pedestrian	V2P	車對人通訊
Vehicle to Vehicle	V2V	車對車通訊
Virtual Reality	VR	虛擬實境
Virtual Personal Netwark	VPN	虛擬私人網路
Wireless Local Area Networks	WLANs	無線區域網路
Wireline Access Network	W-5GAN	5G 有線接取網路
World Telecommunication Standardization Assembly	WTSA	世界電信標準化全會

ISBN：978-986-531-354-8



GPN：1011002098
定價：1200 元