國家通訊傳播委員會 108 年度補助計畫

「推動 5G 垂直應用場域實證規劃、法規調適暨資安法規整備計畫」之細部計畫二「5G 釋照之先期資通安全法規整備計畫」

期末報告定稿

受補助機關：財團法人電信技術中心

計畫主持人：林家樑 博士

研究期程：108 年 6 月 11 日至 108 年 12 月 31 日

國家通訊傳播委員會 補助計畫

中華民國 109 年 3 月

（本報告內容純係受補助單位之觀點，不應引申為本機關之意見）

國家通訊傳播委員會 108 年度補助計畫

「推動 5G 垂直應用場域實證規劃、法規調適暨資安法規整備計畫」之細部計畫二「5G 釋照之先期資通安全法規整備計畫」

期末報告定稿

受補助機關：財團法人電信技術中心

計畫主持人：林家樑 博士

研究期程：108 年 6 月 11 日至 108 年 12 月 31 日

國家通訊傳播委員會 補助計畫

中華民國 109 年 3 月

（本報告內容純係受補助單位之觀點，不應引申為本機關之意見）

目　　次

目　　次……I
圖　目　次……IV
表　目　次……VII
中英文縮寫對照表（依縮寫開頭字母順序排列）……IX
摘　　要……XXI
第壹章　緒論……1
第一節 計畫緣起……3
第二節 計畫目標……6
第三節 計畫內容……8
第四節 預期效益……12
第五節 計畫執行方法……14
第六節 計畫時程說明……16
第貳章　國際組織針對 5G NSA 網路資通安全要求……18
第一節 第三代合作夥伴計畫組織（3GPP）……18
第二節 歐洲電信標準協會（ETSI）……43
第三節 全球行動通信系統協會（GSMA）……44
第四節 美國國家標準暨技術研究院（NIST）……61
第五節 網際網路工程任務組織（IETF）……69
第六節 下一代行動通信網路（NGMN）……72
第七節 結構化資訊標準促進組織（OASIS）……76
第八節 國際電信聯合會電信標準化部門（ITU-T）……79
第九節 本章總結……82
第參章　全球各主要國家 5G 資通安全維護監理作為或法令以及電信業者相關作為……86

第一節 全球主要國家針對 5G NSA 資通安全監理作為或法令...90
一、 美國 90
二、 歐盟 97
三、 德國 108
四、 英國 111
五、 澳洲 116
六、 日本 119
七、 南韓 122
八、 中國 125
九、 國際布拉格會議之布拉格 5G 資通安全提案 131
第二節 全球主要電信業者針對 5G NSA 網路資通安全相關作為.... 137
一、 美國 142
二、 德國 150
三、 澳洲 153
四、 日本 156
五、 南韓 166
第三節 本章總結 168
第肆章 5G NSA 網路元件、威脅說明及資安相關因應方向 177
第一節 無線電接取網路（RAN） 179
第二節 多重接取邊緣運算（MEC） 188
第三節 傳輸網路（TN） 197
第四節 核心網路 （CN） 202
第五節 本章總結 212
第伍章 「行動寬頻業務管理規則」修正草案 218
第一節 第五代行動通信系統資通安全維護計畫參考框架 220
第二節 意見徵詢會議與業界說明會辦理 256
第陸章 「行動寬頻系統審驗技術規範」修正草案及其相關審驗作業程序.....259

第一節 行動寬頻系統審驗技術規範部分規定修正草案及審驗作業程序 260
第二節 意見徵詢會議辦理 279
第柒章 結論與未來展望 282
第一節 結論 282
第二節 未來展望 290
第捌章 計畫查核說明 294
第一節 Milestone & 計畫整體 End-point 達成情形.....294
第二節 本計畫成果報告說明 296
第玖章 參考文獻 300

附件一 「資通安全維護計畫參考框架」與「行動寬頻系統審驗技術規範」修正草案意見徵詢會與業界說明會徵詢意見與問題彙整紀錄
附件二 「2019 洛杉磯－全球行動通信系統協會世界行動通訊大會（GSMA Mobile World Congress 2019 Los Angeles）」參訪報告
附件三 「2019 歐盟網路安全法國際會議（International Conference on the EU Cybersecurity Act 2019）」參訪報告
附件四 「2019 沖繩開放國際會議（Okinawa open days 2019）」參訪報告
附件五 「5G 垂直應用實證與資安策略國際論壇」紀錄報告

圖　目　次

圖 1-1、本計畫與國家政策關聯性 4
圖 1-2、本計畫目標與執行規劃 7
圖 2-1、3GPP 組織結構 19
圖 2-2、5G 標準制訂機構關連 20
圖 2-3、5G 網路架構與功能簡示 24
圖 2-4、非漫遊情況下之 5G 網路信任模型 27
圖 2-5、漫遊情況下之 5G 網路信任模型 27
圖 2-6、密鑰層級框架 28
圖 2-7、用戶介接狀態切換與移動性示意圖 35
圖 2-8、3GPP SCAS 編撰框架 39
圖 2-9、NESAS 宗旨 45
圖 2-10、NESAS 框架 47
圖 2-11、網路設備安全保障方案流程 50
圖 2-12、NIST CSF 三要素 62
圖 2-13、NIST CSF 框架核心 63
圖 2-14、資通安全維護計畫 17 項應載明事項與 CSF 之對應 64
圖 2-15、NIST CSF 框架核心 22 個類別 65
圖 2-16、NIST CSF 資產管理子類別 65
圖 2-17、NIST CSF 框架實現層級 66
圖 2-18、NIST CSF 框架組態 67
圖 2-19、NIST CSF 框架建立步驟 68
圖 2-20、網路功能虛擬化各介面與標準組織之關係 77
圖 3-1、歐盟 5G 網路安全風險評估活動 102

圖 3-2、德國網路安全戰略 108
圖 3-3、UK 電信安全要求 114
圖 3-4、5G 申請審查基準概要 120
圖 3-5、5G 系統建置之附加條件 121
圖 3-6、南韓「5G+戰略」推動方向 123
圖 3-7、南韓「5G+戰略」推行策略 124
圖 3-8、電信業者預計部署首批 5G 商用網路時程 138
圖 3-9、電信業者 5G 網路安全投資需求 138
圖 3-10、電信業者 5G 網路元件之重要性 139
圖 3-11、電信業者對於防火牆的更新需求 140
圖 3-12、電信業者對於未來 5G 網路安全部署需求 141
圖 3-13、德國電信所採取之網路設備安全保障概述 151
圖 3-14、網路安全五個需知 154
圖 3-15、Docomo CSIRT 組成 157
圖 3-16、NTT SOC 中心 158
圖 4-1、5G 網路四大區塊與對應之資通安全威脅 178
圖 4-2、5G NSA Option 3 之網路架構 179
圖 4-3、5G NSA 之無線電接取網路實體元件架構 182
圖 4-4、MEC 之四種可能的部署場景 189
圖 4-5、5G NSA 之多重接取邊緣運算實體元件架構 190
圖 4-6、5G NSA 之傳輸網路實體元件架構 197
圖 4-7、5G NSA 之傳輸網路示意圖 198
圖 4-8、5G NSA 之核心網路實體元件架構 203
圖 4-9、服務導向之 5G 核心網路功能架構 205

圖 5-1、5G 系統架構圖 222

圖 5-2、資通安全維護計畫風險分析管理 255

表　目　次

表 1-1、工作項目之細項工作項目彙整表 9
表 1-2、本計畫進度甘特圖 16
表 2-1、3GPP 七大聯合標準組織簡介 18
表 2-2、與 5G 架構及安全相關的 3GPP 標準 30
表 2-3、5G 設備安全保證方案 42
表 2-4、5G 網路切片服務品質之標準 5QI 值 57
表 2-5、具有 IMS 支援的 eMBB 特定網路服務切片之 NEST 範例 60
表 2-6、國際組織針對 5G NSA 網路資通安全要求總表 82
表 3-1、各國已商轉 5G 電信業者一覽表 86
表 3-2、南韓「5G +戰略」 123
表 3-3、AT&T 資訊與網路安全客戶參考指南 142
表 3-4、資通安全維護計畫應載明事項與 AT&T 資訊與網路安全客戶參考指南、網路安全參考框架之對應 144
表 3-5、日本各電信業者針對 5G 基地臺安全性之相應對策計畫 161
表 3-6、全球各主要國家 5G 資通安全維護監理作為或法令統整 168
表 3-7、各主要國家電信業者針對 5G NSA 網路資通安全維護比較 172
表 4-1、四大區塊威脅風險總表 212
表 4-2、資通安全維護計畫應載明事項與 ISO 27001 之對應 216
表 5-1、意見徵詢會議與業界說明會列表 256
表 6-1、行動寬頻系統審驗技術規範部分規定修正草案條文與說明 262

表 6-2、資通安全維護計畫應載明事項與行動寬頻系統審驗技術規範部分規定修正草案對照表.....267

表 8-1、本計畫查核點說明 294

表 8-2、本計畫成果報告說明 298

中英文縮寫對照表（依縮寫開頭字母順序排列）

縮寫	英文（原文）	中文
3GPP	3rd Generation Partnership Project	第三代合作夥伴計畫組織
4G	4th Generation Mobile Communication System	第四代行動通信系統
5G	5th Generation Mobile Communication System	第五代行動通信系統
5G CR	Commission Recommendation - Cybersecurity of 5G Networks	5G 網路之網路安全建議書
5G NSA	5G Non-standalone	5G 非獨立組網
5G SA	5G Standalone	5G 獨立組網
5G-ppp	5G Infrastructure Public Private Partnership	5G 基礎設施公私合作聯盟
AES	Advanced Encryption Standard	進階加密標準
AF	Application Function	應用功能
AI	Artificial Intelligence	人工智慧
AKA	Authentication and Key Agreement	身份驗證與密鑰協議
AMF	Access and Mobility Management Function	接取與移動性管理功能
API	Application Programming Interface	應用程式介面
AR	Augmented Reality	擴增實境
ARIB	社団法人電波産業会，Association of Radio Industries and Businesses	日本電波產業會
ARPF	Authentication Credential Repository and Processing Function	身份驗證憑證儲存與處理功能
AS	Access Stratum	接取層
ATIS	Alliance for Telecommunications Industry Solutions	電信行業解決方案聯盟
AUSF	Authentication Server Function	身份驗證伺服器功能

縮寫	英文（原文）	中文
AuC	Authentication Center	驗證中心
BBU	Base Band Unit	基頻單元
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Federal Commissioner for Data Protection and Freedom of Information	聯邦資料保護與資訊自由委員會
BNetzA	Bundesnetzagentur, Federal Network Agency	聯邦網路局
BPI	Business Performance and Innovation	商業表現及發展革新組織
BSI	Bundesamt für Sicherheit in der Informationstechnik，Federal Office for Information Security	聯邦資訊安全辦公室
BSS	Base Station Support System	基地臺支援系統
CAPEX	Capital Expenditure	資本支出
C-RAN	Cloud Radio Access Network	雲端化無線電接取網路
CCAS	China Communications Standards Association	中國通信標準協會
CD	Continuous Delivery	持續遞送
CDN	Content Delivery Network	內容遞送網路
CEPT	European Conference of Postal and Telecommunications	歐洲郵政及電信管理委員會
CHAP	Challenge-handshake Authentication Protocol	挑戰握手鑑別協定
CIA	Confidentiality, Integrity and Availability	機密性、完整性與可用性
CIS	Center for Internet Security	網路安全中心
CISA	Cybersecurity and Infrastructure Seurity Agency	網路安全和基礎設施安全局

縮寫	英文（原文）	中文
COBIT	Control Objectives for Information and Related Technologies	資訊及相關技術之控制目標
CP	Control plane	控制平面
CPRI	Common Public Radio Interface	共用公眾無線電介面
CSA	EU Cybersecurity Act	歐盟網路安全法案
CSF	Framework for Improving Critical Infrastructure Cybersecurity	強化關鍵基礎設施網路安全架構
CSIIF	Cyber Skills Immediate Impact Fund	網路技術即時作用基金
CSIRT	Computer Security Incident Response Team	電腦安全緊急事件應變團隊
CT	Communications Technology	通訊科技
CU	Centralized Unit	中央單元
CUPS	Control/User Plan Separation	控制/用戶平面分離
DCMS	Department for Digital, Culture, Media and Sport	英國數位、文化、媒體暨體育部
DDoS	Distributed Denial-of-service	分散式阻斷服務
DHCP	Dynamic Host Configuration Protocol	動態主機配置協定
DHS	United States Department of Homeland Security	美國國土安全部
DN	Data Network	數據網路
DN-AAA	Data Network – Authentication, Authorization and Accounting	數據網路-認證、授權與計費
DNS	Domain Name System	網域名稱系統
DRB	Data Radio Bearer	數據無線電載送
DSLAM	Digital Subscriber Line Access Mulitplexer	數位用戶線路接取多工器
DSS	Dynamic Spectrum Sharing	動態頻譜共享
DoD	United States Department of Defense	美國國防部
DoS	Denial-of-service	阻斷服務

縮寫	英文（原文）	中文
DU	Distributed Unit	分布單元
EAP	Extensible Authentication Protocol	擴展驗證協議
EC	European Commission	歐盟執行委員會（簡稱歐盟執委會）
eCPRI	Evolved Common Public Radio Interface	演進共用公眾無線電介面
EECC	European Electronic Communications Code	歐盟電子通訊法典
eMBB	Enhanced Mobile Broadband	增強型行動寬頻
eNB	Evolved NodeB	4G 基地臺
ENISA	European Union Agency for Cybersecurity	歐盟網路與資訊安全局
ePrivacy	Directive on Privacy and Electronic communications	隱私及電子通訊指令
EPS	Evolved Packet System	演進版分封系統
eSIM	Embedded Subscriber Identity Module (SIM)	嵌入式用戶身份模組
E-UTRA(N)	Evolved Universal Terrestrial Radio Access (Network)	演進通用地面接取（網路）
ETRI	한국전자통신연구원，Electronics and Telecommunications Research Institute	電子通信研究院
ETSI	European Telecommunications Standards Institute	歐洲電信標準協會
ETSI-ISG	European Telecommunications Standards Institute - Industry Specification Group	歐洲電信標準協會產業規範組
EUCA	International Conference on the EU Cybersecurty Act	歐盟網路安全法案國際會議
FCC	Federal Communications Commission	美國聯邦通訊委員會

縮寫	英文（原文）	中文
Gbps	Gigabit per second	每秒十億位元
GDPR	General Data Protection Regulation	一般資料保護規範
GHz	Giga-hertz	秭赫
gNB	Next generation Node B	5G 基地臺
GPRS	General Package Radio Service	通用封包無線電服務
GRE	Generic Routing Encapsulation	通用路由封包
GPU	Graphics Processing Unit	圖形處理器
GSA	Global Mobile Suppliers Association	全球行動供應商協會
GSM	Global System for Mobile Communications	泛歐數位式行動電話系統
GSMA	Global System for Mobile Communications Association	全球行動通信系統協會
GST	Generic Slice Template	通用切片模板
GTP	General Package Radio Service（GPRS） Tunneling Protocol	通用封包無線電服務（GPRS）洞道協議
GUTI	Globally Unique Temporary Identity	全球唯一臨時識別碼
HSS	Home Subscriber Server	本籍用戶伺服器
HTC	High Tech Computer Corporation	宏達國際電子公司
HTTP	HyperText Transfer Protocol	超文本傳輸協定
HTTPS	HyperText Transfer Protocol Secure	超文本傳輸安全協定
IAB	Internet Architecture Board	網際網路架構委員會
IAT	Independent Audit Team	獨立審核小組
ICP	Internet Content Provider	網際網路內容供應商
ICT	Information and Communications Technology	資訊與通訊科技
IDaaS	Identity-as-a-service	身份即服務
IDC	Internet Data Center	網際網路數據中心

縮寫	英文（原文）	中文
IEC	International Electrotechnical Commission	國際電工委員會
IEEE	Institute of Electrical and Electronics Engineers	電機及電子工程學會
IEEPA	International Emergency Economic Powers Act	國際緊急經濟權力法
IESG	Internet Engineering Steering Group	網際網路工程指導團隊
IETF	Internet Engineering Task Force	網際網路工程任務組織
IMS	IP Multimedia Subsystem	IP 多媒體子系統
IMSI	International Mobile Subscriber	國際行動用戶識別碼
IMSI-catcher	International Mobile Subscriber Identity-catcher	國際行動用戶識別碼擷取器
IMT	International Mobile Telecommunication	國際行動電信
IP	Internet Protocol	網際網路協定
IPsec	Internet Protocol Security	網際網路安全協定
ISA	International Society of Automation	國際自動化學會
ISO	International Organization for Standardization	國際標準組織
ISP	Internet Service Provider	網際網路服務供應商
IT	Information technology	資訊科技
ITU	International Telecommunication Union	國際電信聯合會
ITU-D	International Telecommunication Union - Telecommunication Development Sector	國際電信聯合會電信發展部門
ITU-R	International Telecommunication Union - Radiocommunication Sector	國際電信聯合會無線電通訊部門

縮寫	英文（原文）	中文
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector	國際電信聯合會電信標準化部門
Kbps	Kilobit per second	每秒千位元
KISA	한국인터넷진흥원，Korea Internet and Security Agency	南韓網路振興院
L2TP	Layer 2 Tunneling Protocal	第二層洞道協定
LAN	Local Area Network	區域網路
LI	Lawful Interception	合法監聽
LTE	Long-term Evolution	長期演進技術
Mbps	Megabit per second	每秒百萬位元
MEC	Multi-access Edge Computing	多重接取邊緣運算
METIS	Mobile and Wireless Communications Enablers for the Twenty-Twenty Information Society	2020 年資訊社會之行動無線通訊推廣會
MHz	Mega-hertz	兆赫
MIIT	Ministry of Industry and Information Technology，	工業和信息化部（簡稱工信部）
MME	Mobility Management Entity	移動性管理實體
mMTC	Massive Machine Type Communications	大規模機器型通信
MR	Mixed Reality	混合實境
MSIT	과학기술정보통신부，Ministry of Science and ICT	科學技術資訊通信部
MVNO	Mobile Virtual Network Operator	行動虛擬網路營運者
MWCLA	GSMA Mobile World Congress Los Angeles	洛杉磯－全球行動通信協會世界行動通訊大會
NAS	Non-access Stratum	非接取層
NB-IoT	Narrow Band Internet of Things	窄頻物聯網

縮寫	英文（原文）	中文
NCC	National Communications Commission	國家通訊傳播委員會（簡稱通傳會）
NDS/IP	Network Domain Security Architecture for IP-based Protocol	網際網路協定導向的網域安全架構協定
NEF	Network Exposure Function	網路開放功能
NESAS	Network Equipment Security Assurance Scheme	網路設備安全保障方案
NEST	Network Slice Type	網路切片類別
NF	Network Function	網路功能
NFV	Network Function Virtualization	網路功能虛擬化
NGMN	Next Generation Mobile Networks	下一代行動網路聯盟
NGMN-SCT	Next Generation Mobile Networks - Security Competence Team	下一代行動網路聯盟安全能力小組
NICT	国立研究開発法人情報通信研究機構，National Institute of Information and Communications Technology	日本國立研究開發法人情報通信研究機構
NIS	Directive on Security of Network and Information Systems	網路與資訊系統安全指令
NISC	内閣サイバーセキュリティセンター，National Information Security Center	國家資訊安全中心
NIST	National Institute of Standards and Technology	國家標準暨技術研究院
NMS	Network Management System	網路管理系統
NRF	Network (function) Repository Function	網路（功能）貯藏功能
NS	Network Slicing	網路切片
NSSF	Network Slice Selection Function	網路切片選擇功能
NSSAI	Network Slice Selection Assistance Information	網路切片選擇輔助資訊

縮寫	英文（原文）	中文
NSRI	국가보안기술연구소，National Security Research Institute	國家保安技術研究所
OAM	Operations, administration and maintenance	營運、管理與維護
Ofcom	Office of Communications	通訊管理局
OMB	United States Office of Management and Budget	美國行政管理和預算局
OOD	Okinawa Open Days	沖繩國際開放會議
OPEX	Operating Expense	營運支出
OSS	Operating Support System	維運支援系統
OT	Operating Technology	營運科技
OTT	Over-the-top Service	註釋：透過網際網路直接向用戶提供的應用服務
PAP	Password Authentication Protocol	密碼驗證協定
PCF	Policy Control Function	策略控制功能
PCO	Protocol Configuration Options	協定組態選項
PCRF	Policy and Charging Rules Function	策略與計費規則功能
PDCP	Packet Data Convergence Protocol	封包數據匯聚通訊協定
PDN	Packet Data Network	封包數據網路
PDN Gateway, PGW	Packet Data Network Gateway	封包數據網路閘道器
PDU	Protocol Data Unit	協議數據單元
PLMN	Public Land Mobile Network	公共陸上行動網路
PON	Passive Optical Network	被態光纖網路
QKD	Quantum Key Distribution	量子密鑰分配
QR code	Quick Response Code	快速反應條碼
QRNG	Quantum random number generator	量子隨機數產生器

縮寫	英文（原文）	中文
QoS	Quality of Service	服務品質
QUIC	Quick User Datagram Protocol Internet Connections	快速用戶數據封包協定網路連線
RAN	Radio Access Network	無線電接取網路
RAT	Radio Access Techonology	無線電接取技術
RLC	Radio Link Control	無線電連結控制
RRC	Radio Resource Control	無線電資源控制
RRM	Radio Resource Management	無線電資源管理
RRU	Remote Radio Unit	遠端無線電單元
SAS	Statement on Auditing Standards	審計標準說明書
SBA	Service-based Architecture	服務導向架構
SCAS	SeCurity Assurance Specification	安全保障方案
SDN	Software-defined Network	軟體定義網路
SDO	Standards Development Organization	標準制定組織
SEAF	SEcurity Anchor Function	安全固定功能
SEPP	Security Edge Protection Proxy	安全邊緣保護代理伺服器
SGSN	Serving General Package Radio Service (GPRS) support node	GPRS 服務支援節點
SGW	Serving Gateway	服務閘道器
SIDF	Subscription Identifier De-concealing Function	用戶識別碼去隱藏功能
SIM	Subscriber Identity Module	用戶身份模組
SIP	Session Initiation Protocol	會話初始化協定
SMF	Session Management Function	會話管理功能
SMS	Short message service	簡訊服務
SNS	Social Networking Service	社群網路服務
SOC	Security operation center	資訊安全監控中心

縮寫	英文（原文）	中文
SON	Self-organizing Network	自組織網路
SRB	Signalling Radio Bearer	信號無線電載送
SS7	Signaling System Number 7	第七號信號系統
SSC	Session Service Continuity	會話服務連續性
SUCI	Subscription Concealed Identifier	用戶隱藏識別碼
SUPI	Subscription Permanent Identifier	用戶永久識別碼
TLS	Transport Layer Security	傳輸層安全性協定
TSDSI	Telecommunications Standards Development Society, India	印度電信標準開發協會
TSSR	Telecommunications Sectors Security Reforms	電信部門安全改革法
TTA	한국 정보통신기술협회，Telecommunications Technology Association	南韓電信技術協會
TTC	电信技术委员会，Telecommunication Technology Committee	日本電信技術委員會
TR	Technical Report	技術報告
TS	Technical Specification	技術規範
TSR	Telecoms Security Requirements	電信安全要求
UDR	User Defined Route	用戶定義路由
UDM	Unified Data Management	統一數據管理
UE	User Equipment	用戶設備
UICC	Universal Integrated Circuit Card	通用積體電路卡
UMTS	Universal Mobile Telecommunications System	全球行動通信系統
UP	User plane	用戶平面
UPF	User Plane Function	用戶平面功能

縮寫	英文（原文）	中文
uRLLC	Ultra-reliable low latency communication	超可靠低延遲通訊
USF	Universal Service Fund	普及服務基金
USIM	UMTS Subscriber Identity Module	全球行動通信系統用戶身份模組
V2X	Vehicle-to-everything	車聯網
VIM	Virtual Infrastructure Manager	虛擬基礎設施管理者
VNF	Virtual Network Function	虛擬網路功能
VoLTE	Voice over LTE	透過長期演進技術傳輸之語音
VPN	Virtual Private Network	虛擬私人網路
VR	Virtual Reality	虛擬實境
WDM	Wavelength Division Multiplex	波長多工
Wi-Fi	Wireless Fidelity	無線區域網路
WiMAX	Worldwide Interoperablity for Microwave Access	全球互通微波接取
WLAN	Wireless Local Area Network	無線區域網路
WWRF	Wireless World Research Forum	無線世界研究論壇

資料來源：國家傳播通訊委員會-雙語詞彙、國家傳播通訊委員會-雙語詞彙、本團隊整理

摘　　要

5G 系統具備大頻寬、高容量及低延遲的特性，將促進許多新興服務與創新應用發展，進而推動各領域的產業轉型。為因應多樣化的應用服務，5G 系統在架構設計上將網路功能軟體化與虛擬化，而達到網路功能的快速擴充性與彈性。另外，從運算、儲存及軟體運作的角度來看，5G 系統在整體網路營運及服務提供上納入更多元與廣泛的資訊與通訊技術。這些改變使得 5G 系統面臨更為複雜的資通安全風險與威脅，也為 5G 電信業者在網路部署、維運與服務提供時帶來新的資通安全挑戰。

基於前段說明，為達到促進國家 5G 網路安全、保障消費者權益及健全 5G 產業發展之目的，國家通訊傳播委員會(以下簡稱通傳會）補助財團法人電信技術中心執行「推動 5G 垂直應用場域實證規劃、法規調適暨資安法規整備計畫」之細部計畫二「5G 釋照之先期資通安全法規整備計畫」。本計畫旨在透過研析國際相關組織、各國監理單位及電信業者等有關 5G 網路安全或威脅之標準、指引及報告等文件，並出席相關國際論壇及研討會掌握最新資訊，進而考量我國情境以修訂「行動寬頻業務管理規則」及「行動寬頻系統審驗技術規範」等法規，確保我國 5G 網路安全。

本計畫已研析 3GPP、ETSI、GSMA、NIST、IETF、NGMN、OASIS 及 ITU-T 等 8 個國際組織之相關文獻，也針對美國、歐盟、德國、英國、澳洲、日本、南韓及中國等 8 個主要國家或聯盟監理單位所發佈的 5G 網路安全相關指引或報告進行研析。此外，本計畫也蒐集美國、德國、澳洲、日本與南韓等 5 個國家之電信業者有關 5G 網路安全之規劃與作為。為了獲取 5G 網路安全最新資訊並與向國際專家請益，本計畫共出席包含 2019 GSMA Mobile World Congress Los Angeles、

2019 International Conference on the EU Cybersecurity Act 以及 Okinawa Open Days 2019 等三個國際論壇或研討會，透過參與國際性會議，掌握主要國家之電信監理單位對於 5G 資通安全最新研析、政策及實際作為，以利我國法規制定之參考。本計畫綜整上述各方面之資訊，提出通傳會「行動寬頻業務管理規則」及「行動寬頻系統審驗技術規範」之修正草案。其中，針對「行動寬頻業務管理規則」第 40 條「資通安全維護計畫」，進一步提出「第五代行動通訊資通安全維護計畫參考框架」供 5G 電信業者做為規劃資通安全維護計畫之依據，以期確保 5G 資通安全維護計畫之完整性與可靠性。本計畫也針對「行動寬頻系統審驗技術規範」增訂 5G 資通安全相關之一般性與功能性對應審驗規定，以確認 5G 網路正式提供服務時已具備一定資通安全防護能力。

由於國內將於 2020 年正式進入 5G 網路時代，5G 電信業者必須提交「5G 資通安全維護計畫」取得通傳會審核通過後才能正式提供商業服務。如何針對電信業者提交之「5G 資通安全維護計畫」進行審核及未來實際施作該計畫後之稽核作業程序等都將是通傳會未來重要工作。此外，隨著電信業者引入 5G SA 網路架構及因應持續演進的資通安全威脅或事件，通傳會也須要掌握主要國家之研究單位、電信商、設備商、第三方應用服務商等，對於 5G 資通安全最新研究與實作及政策與實際作為，並針對「5G 資通安全防護計畫」之要求進行滾動式修正。

第壹章　緒論

第五代行動通信系統（5th Generation Mobile Communication System，5G）時代來臨，將使得用戶在使用行動應用服務方面產生巨大改變。從用戶手機服務到自動駕駛應用等各個領域，5G 高速且低延遲特性有助於電信業者拓展新興之垂直應用服務範疇。網路虛擬化、開放性、大量開源軟體採用、與第四代行動通信系統（4th Generation Mobile Communication System，4G）共存等環境，使得面對 5G 網路下之資通安全挑戰更顯嚴峻。

通訊網路是國家最重要的關鍵基礎設施之一，涵蓋民生、社會、經濟甚至國防，因此 5G 網路的設置是我國整體資通安全政策不可或缺的一環，且應層層把關觸及 5G 網路設置中的每一個層面，例如：頻譜規劃、無線電器材管制、通訊設備安全驗證、第三方服務、供應鏈等。基於上述，為促進通訊傳播健全發展及保障人民通訊權益之主要使命，國家通訊傳播委員會（National Communications Commission，NCC，以下簡稱通傳會）監管電信網路與推動 5G 釋照之先期資通安全法規整備責無旁貸。

面對 5G 網路即將商轉，在電信、廣播、媒體、資訊科技（Information Technology，IT）上的整合與發展，在監理資通安全法規、系統設備安全認證、網路及機房安全性管理等，均需要有完備的資通安全維護相關政策、規範以提升用戶、業者、政府整體之資安防護能量，才能有效的降低資通安全威脅與風險。

為健全我國數位經濟之永續發展、保障通信安全及維護用戶權益，本團隊計畫於 109 年 5G 釋照前，協助通傳會完成「行動寬頻業務管理規則」草案第 40 條「資通安全維護計畫」應載明事項之參考框架

及「行動寬頻系統審驗技術規範」草案之資通安全一般審驗規定，以要求 5G 網路設置時，即納入資通安全防護機制，並使未來在 5G 網路營運時具備足夠的資通安全防護能量，確保 5G 網路安全可信賴，進而促進相關垂直應用場域及創新應用服務之發展。

第一節 計畫緣起

國際行動網路標準組織「第三代合作夥伴計畫組織（3rd Generation Partnership Project，3GPP）」已於 2018 年 6 月起階段性制訂完成 5G 網路技術標準規範 [1]，其中美國、歐洲、澳洲、日本、南韓、中國等先進國家亦全力發展 5G 相關技術研究，透過垂直應用服務場域之建置來實證相關技術。開放式行動網路技術日新月異與人性化應用服務之轉變，全球各國將面臨 5G 行動網路資通安全嚴峻挑戰，駭客攻擊行為及不斷提升之資通訊安全風險與威脅，引起全球對於資通訊安全憂慮，須釐清挑戰採取策略以保障國人資通訊安全及維護人民權益。

通訊網路資通安全是我國數位國家、創新經濟的關鍵驅動力量，為國家持續運作之關鍵基石。為提供國人一個安全、人性、強健之寬頻通訊網路，來維繫國家、經濟、社會持續運作，並確保電信業者能以維護人民隱私安全為己任，達成 5G 網路通訊時刻安全有保障之營運目標。根據國家安全會議與行政院 105 年 8 月共同召開資安即國安策略會議，通傳會將遵循總統宣示之「資安即國安」國家策略執行目標，目標「打造安全可信賴的數位國家」[133]，本計畫在通傳會基礎處之監督及指導下，自 108 年 6 月起開始協助通傳會執行「推動 5G 垂直應用場域實證規劃、法規調適暨資安法規整備計畫」之細部計畫二「5G 釋照之先期資安法規整備計畫」，保障 5G 網路資通安全與國人通訊隱私權益。

5G 網路發展與部署為各國競逐的焦點，2019 年 4 月南韓與美國即陸續正式推出 5G 非獨立組網（5G Non-standalone，5G NSA）。2019 年 6 月 [2]，全球行動通信供應商協會（Global Mobile Suppliers Association，GSA）指出，目前全世界已經有 16 個國家推出 5G 網路

商業化服務。我國為了加速 5G 網路基礎建設佈建時程，通傳會將頻譜競標作業提前至 2019 年 12 月舉行，預計在 2020 年我國即能正式邁入 5G 網路服務新時代。



圖 1-1、本計畫與國家政策關聯性

資料來源：行政院科技會報辦公室《臺灣 5G 行動計畫》

政府在推動我國 5G 網路發展政策上，除完成釋照作業外，另一項重要任務是如何發展出健全的資通安全環境、保護消費者權益、維護國家安全與利益。考量 5G 網路結合創新的架構與設計，其面臨之資通安全與國安威脅較以往更嚴峻且多元，5G 資通安全維護計畫的整備是必要的，為加速與完備 5G 網路之資通安全發展，行政院核定並公布《臺灣 5G 行動計畫》（如上圖 1-1）[125]，其中於主軸三即強調「完備 5G 技術核心及資通安全防護能量」，因此，相關配套法規應於 5G 釋照前整備完畢，不只有利於 5G 頻譜競標者有所依循，且敦促 5G 頻譜得標者未來在 5G 網路建置時，必須把 5G 資通安全防護考量納入整體規劃與建設之中。是以，主管機關須針對 5G 網路資通安全之範疇充分掌握與瞭解，而其可能存在的弱點、威脅以及風險亦須要經過詳細的評估，以確保消費者權益與資通安全。

本計畫預計於 2019 年 5G 釋照前，於通傳會指導下，針對電信法授權之「行動寬頻業務管理規則」與「行動寬頻系統審驗技術規範」兩部子法，完成提研資通安全管理建議項目，強制規定未來 5G 頻譜得標者在網路設計規劃階段，即應識別擬設置之 5G 網路相關弱點、風險及威脅等，並研提防護、偵測、應處等作為，同時載明於應提出之資通安全維護計畫，並落實於後續網路建設、營運及相關管理，以具備足夠的資通安全防護能量，確保 5G 網路安全可信賴，保障相關垂直應用場域與創新應用服務之穩定發展。

第二節 計畫目標

本計畫目標為協助通傳會確保我國 5G 網路安全與防護能力，保障 5G 網路安全可信賴，進而促進相關垂直應用場域與相關創新應用服務之發展。因此，極須在 5G 釋照前，盤點與研析 5G 網路相關資通安全議題，並參考國際、區域標準組織及 5G 網路已商轉國家所提之 5G 網路資通安全防護建議，研提我國 5G 網路應具備之資通安全防護要求並納入「行動寬頻業務管理規則」與「行動寬頻系統審驗技術規範」等法規。藉由法規之完備，賦予電信業者具備相關資通安全防護機制之義務，俾確保 5G 網路資通安全。

展望未來，5G 網路架構得力於軟體化系統與開放軟體介面的設計，允許第三方服務提供者透過電信業者的多重接取邊緣運算（Multi-access Edge Computing，MEC），滿足用戶的高速運算需求，強化即時服務體驗，此類創新技術，加深了 5G 網路面臨之資通安全威脅。而隨著 5G 釋照，另一潛在之資通安全危機，即來自於不受信任之第三方系統設備商的問題也日漸浮現，此一問題不僅在我國，國際上對於 5G 網路建設時，如何識別、檢測、驗證第三方設備商之系統設備是否可信賴，亦表達強烈關切，主要原因在於隨著 5G 網路逐漸普及，此類有資通安全疑慮之系統設備也將漸漸進入各國 5G 網路商用市場，各國主管機關若不積極督促與協助電信業者和系統設備商排除不安全之第三方系統設備商，將可能會有國家機密外洩之潛在風險等，而嚴重影響國家安全。

對此，本計畫認為，應隨 5G 技術之演進與網路普及進程，持續精進 5G 相關資通安全政策與規範，進行 5G 網路資通安全管理規範之調適及滾動式修正，同時，5G 網路與垂直應用的發展也將擴大資通安全風險的範疇，通傳會亦需持續掌握國際 5G 標準組織資通安全

技術發展、主要國家 5G 資通安全法制與政策趨勢，並累積資通安全防護能量，使我國 5G 業者能提供安全可信賴的 5G 網路服務予消費者。

本計畫目標與執行規劃如下圖 1-2：

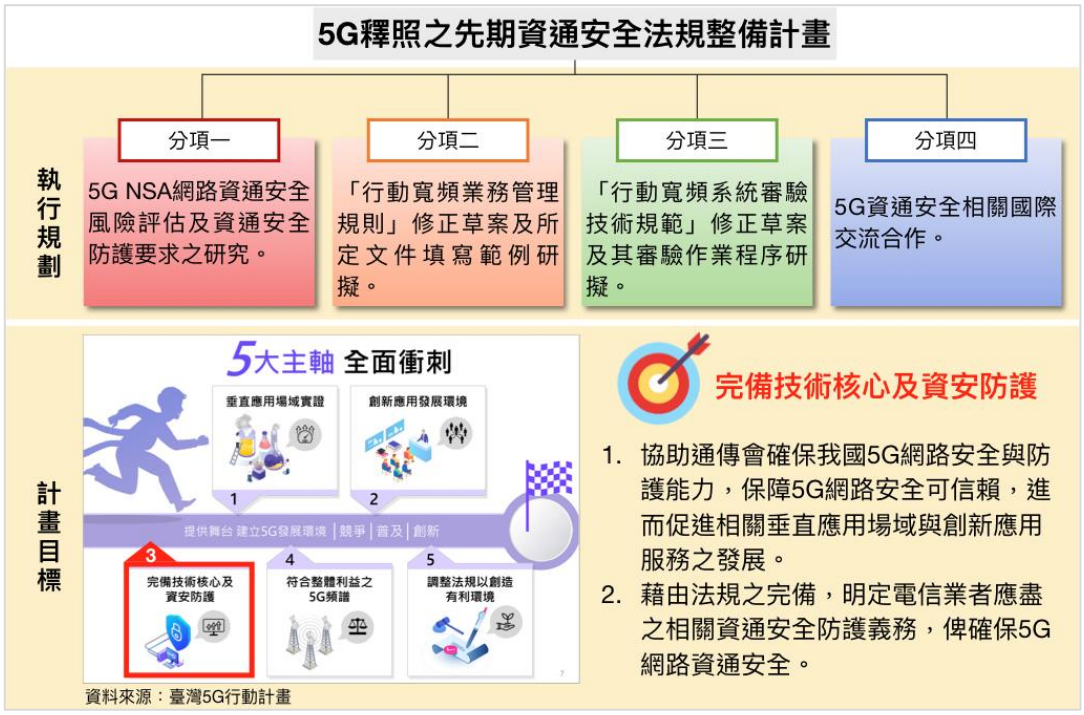


圖 1-2、本計畫目標與執行規劃

資料來源：本團隊整理

第三節 計畫內容

綜觀世界各國就 5G 網路所涉之資通安全及國家安全，皆已展開相關工作。我國亦於 2019 年底至 2020 年初之間釋出第一波 5G 頻率執照，為保障我國 5G 網路安全與穩定，進一步維護未來 5G 垂直應用場域之資通安全，以利新世代行動寬頻與網路創新應用服務蓬勃發展，業者於構築 5G 網路基礎建設時，即應注意符合國際資通安全標準。

5G 網路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，5G 網路可促成更多垂直應用的業者與電信業者合作，並利用 5G 網路提供服務，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，垂直應用的推展將使 5G 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 5G 安全加以關注與更新。

因此，目前配合 5G 釋照時程，本團隊協助通傳會完備電信法授權訂定之「行動寬頻業務管理規則」及「行動寬頻系統審驗技術規範」相關資安要求，據以要求 5G 頻譜得標者設置 5G 網路時，採用符合國際資通安全標準之設施與設備，並納入資通安全防護管理機制，以確保 5G 網路安全可信賴，善盡通訊傳播網路管理者責任。

為配合協助通傳會完備「行動寬頻業務管理規則」與「行動寬頻系統審驗技術規範」之資通安全相關法規調適及 3GPP 5G 標準的釋出時程，本計畫針對 5G NSA 架構進行國際或區域組織；如：3GPP、歐洲電信標準協會（European Telecommunications Standards Institute，

ETSI）、全球行動通信系統協會（Global System for Mobile Communications Association，GSMA）、美國國家標準暨技術研究院（National Institute of Standards and Technology，NIST）等之 5G 網路資通安全相關風險評估及資通安全防護要求之蒐集與研析，並參與國外 5G 資安相關會議汲取經驗與舉辦 5G 資安國際論壇，包含：2019 洛杉磯－全球行動通信系統協會世界行動通訊大會（GSMA Mobile World Congress Los Angeles，MWCLA）、2019 歐盟網路安全法案國際會議（International Conference on the EU Cybersecurty Act，EUCA）、2019 沖繩開放國際會議（Okinawa Open Days，OOD）以及 5G 垂直應用實證與資安策略國際論壇，進一步結合我國目前情勢，協助修訂「行動寬頻業務管理規則」與「行動寬頻系統審驗技術規範」之資通安全相關法規，研提資通安全防護法規調適及資通安全維護計畫應提報內容及撰寫指引等建議內容。針對上述工作項目，本計畫細項工作項目之工作內容如下表 1-1 闡述：

表 1-1、工作項目之細項工作項目彙整表

分項	本計畫	本計畫細項工作項目
1	5G NSA 網路資通安全風險評估及資通安全防護要求研究報告	國際組織針對 5G NSA 網路資通安全要求：研析 3GPP、ETSI、GSMA、NIST 等國際組織有關 5G NSA 網路資通安全相關文獻以及國際組織針對 5G NSA 網路資通安全要求。
		全球各主要國家 5G 資通安全維護監理作為或法令：盤點前揭國際組織提出之 5G NSA 網路資通安全漏洞與相關風險評估。
		全球各主要國家電信業者就 5G NSA 網路資通安全之相關作為：蒐集與研析美國、南韓、日本、歐盟、澳洲等已（即將）商轉 5G 網路國家之 5G NSA 網路資通安全風險評估情形，及其監理機關之相應資通安全防護要求與監理作為或法令。

分項	本計畫	本計畫細項工作項目
		配合國際趨勢進行報告更新：就 9 月份所提之 5G NSA 網路資通安全風險評估及資通安全防護要求研究報告配合國際趨勢進行更新。
2	「行動寬頻業務管理規則」修正草案及所定文件填寫範例研擬	草案第 40 條「資通安全維護計畫」應載明事項之參考框架：彙整我國 5G NSA 網路建置時應考量及評估之資通安全風險議題，研提「行動寬頻業務管理規則」修正草案及所定文件，並填寫範例等資料草案第 40 條「資通安全維護計畫」應載明事項之參考框架。
		召開意見徵詢會議，研議參考框架之適用性及可行性：邀集產、官、學、研及相關利害關係人，召開意見徵詢會議，研議參考框架之適用性及可行性，共同研商適用於我國 5G NSA 網路資通安全風險評估項目。
		舉辦 2 場資通安全維護計畫參考架構業界說明會，於說明會中宣導 5G 通訊架構應具備之資訊安全要求，協助業界瞭解管理規則之要求。
3	「行動寬頻系統審驗技術規範」修正草案及其相關審驗作業程序研擬	研訂資通安全之一般審驗規定及其作業程序：彙整我國 5G NSA 網路建置時應考量及評估之資通安全風險議題，研提「行動寬頻系統審驗技術規範」修正草案及其相關審驗作業程序，並研訂資通安全之一般審驗規定及其作業程序。
		召開意見徵詢會議，研議草案及審驗作業程序之適用性及可行性：邀集產、官、學、研及相關利害關係人，召開意見徵詢會議，研議草案及審驗作業程序之適用性及可行性，共同研商適用於我國 5G NSA 網路資通安全風險評估項目。
		預告草案之外界意見研析及回覆：依通傳會預告之草案，進行外界意見研析及回覆，並評估是否需進行修正。
4		參與國際 5G 資通安全相關活動：參與 ENISA 或 GSMA 等國際組織 5G 資通安全議題重要活動或拜

分項	本計畫	本計畫細項工作項目
	5G 資通安全相關國際交流合作	會已商轉、即將商轉 5G 電信業者、網路安全監理單位等，持續掌握國際 5G 最新資通安全趨勢。
		舉辦 5G 資通安全相關國際論壇：於臺灣舉辦 5G 資通安全論壇，邀請國內外產官學研相關專家學者進行演說及會談。

資料來源：本團隊整理

第四節 預期效益

5G 高頻寬、低延遲的特性將會帶來數位世界的革命，使得社會對於使用通訊網路的依賴大幅廣泛與提升，如從自駕車到全自動化工廠、智慧城市等，將會有許多新興之垂直應用服務展露，這同時也會為國家、人民帶來潛在無比的經濟效益，因此 5G 網路的發展已成為目前全球各國爭相角逐的目標之一，然而 5G 嶄新的架構與設計將會面臨到前所未有的資安挑戰與威脅，而通訊網路為國家之關鍵基礎建設之一，是維繫國家、經濟、社會持續運作的一個重要建設，故確保通訊網路資通安全以保障國家穩定發展、促進經濟持續進步、維護國家安全格外重要，本中心（財團法人電信技術中心）配合國家「國安及資安」策略協助通傳會釐清 5G 網路所帶來之資通安全風險、威脅來研擬相應規範、策略、應對措施以保障人民、業者、國家安全，達到培養足夠之資通安全防護能量來發展出健全的資通安全環境、保護消費者權益、維護國家安全與利益。

本計畫預期產出的主要研究成果與效益如下：

(一)掌握趨勢：掌握國際主要國家 5G 網路建設資通安全防護政策與實際作為

本計畫透過資料蒐集與研讀、線上或實際參與會議，掌握 5G 可能帶來之潛在弱點、風險與威脅，以及國際主要國家之政府以及電信業者對於 5G 資通安全最新政策、規範、監理及實際作為、應對措施，並且結合本國情勢、政策、利益考量，以提供相關之 5G 資安情資，有利後續法規調適之參考。

(二)法規調適：整備 5G 第一階段釋照得標業者 5G 網路建設之資通安全防護的完備性與妥適性

本計畫之執行，將協助通傳會，透過上述全球趨勢掌握，提出「行動寬頻業務管理規則」及「行動寬頻系統審驗技術規範」須增修訂之相關資通安全條文建議，完整呈現 5G 業者自執照競標、事業籌設至網路建設等各階段相關權利義務，並將研提資通安全維護計畫參考框架來引導業者提出 5G 網路之「資通安全維護計畫」，確保未來 5G 頻譜得標者能夠在 5G 設置、營運時有足夠的資通安全防護能力，並隨 5G 網路技術演進及佈建時程，研析國際 5G 資通安全政策發展最新趨勢，並適時進行法規調適。

(三)確保安全：完備 5G 資通安全防護以促進 5G 網路創新應用服務發展

5G 資通安全可以從制度面和管理面以及技術面三個層次闡述，但最重要的內涵就是要做到 Security By Design（預設安全），意指 5G 網路建設之初，就必須納入資通安全防護機制，未來在營運時，也具備足夠的資通安全防護能量，真正做到確保 5G 網路的安全性，也可以進一步做到促進各種垂直應用場域及創新應用服務的發展。成功的垂直場域應用會是 5G 網路發展的重要關鍵，其為涉及國家安全、利益、人民福祉、企業發展之要點。本計畫期望透過掌握趨勢、法規調適能夠確保未來 5G 網路安全可信賴，貫策 Security by Design 之精神，進而促進相關垂直應用場域及數位經濟之永續發展。

第五節 計畫執行方法

本計畫工作項目包含，5G NSA 網路資通安全風險評估及資通安全防護要求研究、「行動寬頻業務管理規則」修正草案及所定文件填寫範例研擬、「行動寬頻系統審驗技術規範」修正草案及其相關審驗作業程序研擬及 5G 資通安全相關國際交流合作。上述研究透過文獻分析、深度訪談、個案研究、參與觀察等方法，加速與完備 5G 之發展，確保 5G 網路資通安全與防護能力。針對 5G 關鍵基礎設施及後續營運所涉資通安全議題進行深入探討，並研提整體資通安全防護及法規調適措施打造 5G 資通安全防護機制，建立 5G 安全防護能量，發展活躍網路社會、推進高值創新經濟、建構富裕數位國家。本計畫依據計畫架構擬定出各研究分項需要釐清的議題，採用適當的研究方法進行，再串連這些工作項目的成果產出研究報告，計畫執行方法分述如下：

(一)文獻分析法

研析 3GPP、ETSI、GSMA、NIST 等國際組織有關 5G NSA 網路資通安全相關文獻。盤點前揭國際組織提出之 5G NSA 網路資通安全漏洞及相關風險評估。蒐集及研析美國、歐盟、澳洲、日本、南韓等已（即將）商轉 5G 網路國家之 5G NSA 網路資通安全風險評估情形，及其監理單位之相應資通安全防護要求。

(二)深度訪談法

依前揭國際相關資訊之研析結果，邀集產、官、學、研及相關利害關係人，共同研商適用於我國 5G NSA 網路資通安全風險評估項目。

(三)個案研究法

彙整我國 5G NSA 網路建置時應考量及評估之資通安全風險議題，並研提「行動寬頻業務管理規則」及「行動寬頻系統審驗技術規範」之修正建議，增訂 5G NSA 網路資通安全防護要求及相關資通安全審驗規定。

(四)參與觀察法

參與 3GPP、ETSI 或 GSMA 等國際組織 5G 資通安全議題重要活動，或拜會已商轉、即將商轉 5G 網路國家之行動通信業者、網路安全相關單位，持續掌握國際 5G 最新資通安全趨勢。

第六節 計畫時程說明

為配合前述研究議題與研究方法之落實推動，本計畫執行期程自108年6月11日至108年12月31日，並於108年9月30日提交期中報告；108年10月31日提交經參考外界意見之①「資通安全維護計畫」應載明事項之參考框架及②「行動寬頻系統審驗技術規範」資通安全審驗規定；108年12月20日提出期末報告，符合通傳會之業務時程需求（如下表 1-2 計畫執行甘特圖）。為確保工作進度及研究品質，執行計畫過程中，本團隊也配合通傳會要求，辦理工作小組會議並提交工作進度報告。

表 1-2、本計畫進度甘特圖

工作項目	108年						
	6月	7月	8月	9月	10月	11月	12月
期中成果報告				▲			
期末成果報告							▲
5G 釋照之先期資通安全法規整備計畫							
5G NSA 網路資通安全風險評估及資通安全防護要求研究							
國際組織針對 5G NSA 網路資通安全要求				▲			
全球各主要國家 5G 資通安全維護監理作為或法令				▲			
全球各主要國家電信業者就 5G NSA 網路資通安全之相關作為				▲			
配合國際趨勢進行報告更新							▲

工作項目	108 年						
	6 月	7 月	8 月	9 月	10 月	11 月	12 月
「行動寬頻業務管理規則」修正草案及所定文件填寫範例研擬							
草案第 40 條「資通安全維護計畫」應載明事項之參考框架					▲		
召開「行動寬頻業務管理規則」修正草案及所定文件填寫範例等資料意見徵詢會議 1 場					▲		
舉辦 2 場資通安全維護計畫參考架構業界說明會							▲
「行動寬頻系統審驗技術規範」修正草案及其相關審驗作業程序研擬							
研訂資通安全之一般審驗規定及其作業程序					▲		
召開「行動寬頻系統審驗技術規範」修正草案及其相關審驗作業程序意見徵詢會議 1 場					▲		
預告草案之外界意見研析及回覆							▲
5G 資通安全相關國際交流合作							
參與國際 5G 資通安全相關活動							▲
舉辦 5G 資通安全相關國際論壇							▲

▲：為各階段之工作查核點。
註 1：期中報告於 108 年 9 月 30 日交付。
註 2：期末報告於 108 年 12 月 20 日交付。

資料來源：本團隊整理

第貳章　國際組織針對 5G NSA 網路資通安全要求

第一節 第三代合作夥伴計畫組織（3GPP）

3GPP [3]由全球七大標準制定組織（Standards Development Organization，SDO）聯合組成，其宗旨是制定和維護全球無線通訊標準。根據全球性需求制定出一套全球通用之統一標準以實現產業標準化。這七個標準制定組織橫跨亞洲、歐洲、北美洲（其相關簡介如下表 2-1），包括日本社團法人電波產業會（社团法人電波産業会，Association of Radio Industries and Businesses，ARIB）、美國電信行業解決方案聯盟（Alliance for Telecommunications Industry Solutions，ATIS）、中國通信標準化協會（China Communications Standards Association，CCSA）、ETSI、印度電信標準開發協會（Telecommunications Standards Development Society, India，TSDSI）、南韓電信技術協會（한국정보통신기술협회，Telecommunications Technology Association，TTA）以及日本電信技術委員會（电信技术委员会，Telecommunication Technology Committee，TTC） [4]。

表 2-1、3GPP 七大聯合標準組織簡介

ARIB	社團法人電波產業會（ARIB）是一個日本的 SDO，內部有 27 為 3GPP 的會員。
atis	電信行業解決方案聯盟（ATIS）是一個位在北美洲的 SDO，45 位 3GPP 的會員分別來自美國電信商 AT&T、Verizon、Sprint 以及 T-Mobile。
CCSA	中國通信標準化協會（CCSA）主要致力於中國的 SDO，擁有 89 位 3GPP 會員。
ETSI	歐洲電信標準協會（ETSI），是歐洲的 SDO，擁有 380 位 3GPP 會員，其中有些會員是來自其他地區。

tsdsi India's Telecom SDO	印度電信標準開發協會（ISDSI）是印度的 SDO，擁有 18 位 3GPP 會員。
TTA	電信技術協會（TTA），是南韓的 SDO，擁有 20 位 3GPP 會員。
TTC Telecommunication Technology Committee	電信技術委員會（TTC），是日本的 SDO，擁有 9 位 3GPP 會員。

資料來源：3GPP、本團隊整理

各組織與 3GPP 相互合作，包括制定總體政策、策略以及技術規範、產業政策等；5G 通訊標準技術的訂定組織，由 16 個工作小組組成(如下圖 2-1)，負責制定終端、基礎設施和系統端到端的標準規範。

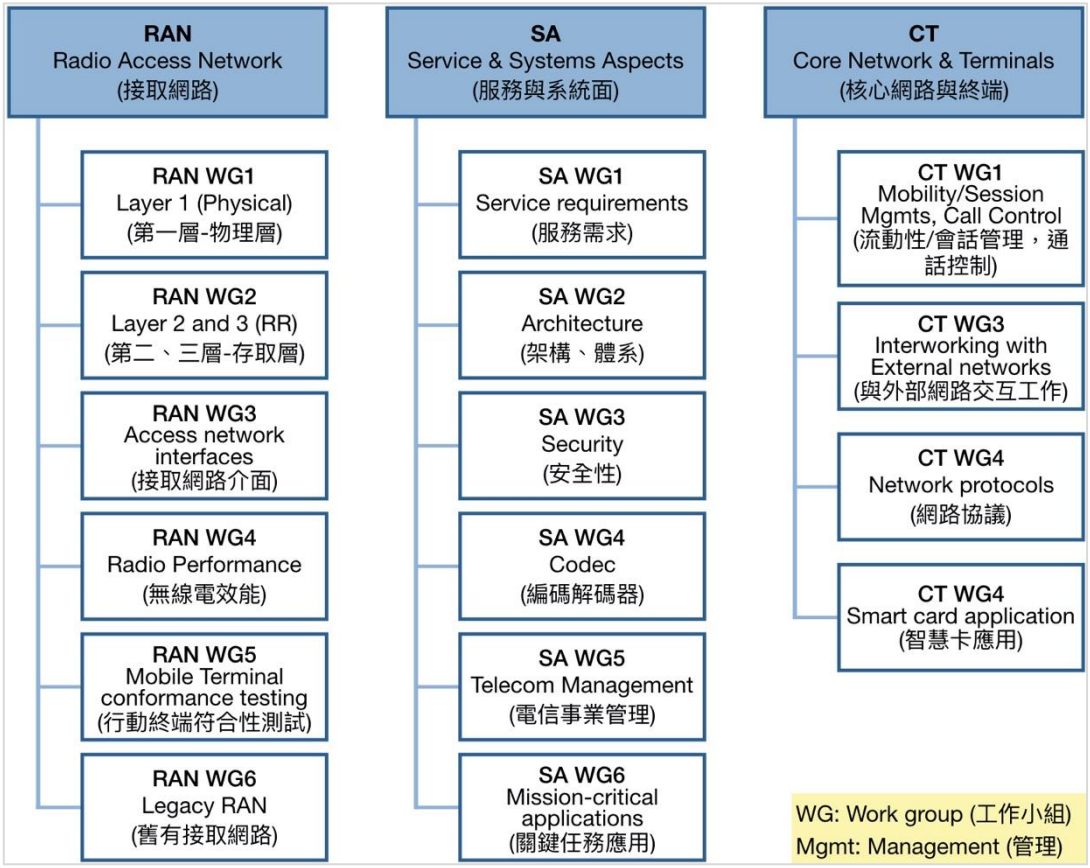


圖 2-1、3GPP 組織結構

資料來源：3GPP、本團隊整理

5G 技術主要依循 3GPP 技術標準制定，除 3GPP 還有其他相關推動組織，如歐盟的 5G-PPP（5G Infrastructure Public Private Partnership，5G 基礎設施公私合作聯盟）、METIS（未來 2020 年資訊社會之行動無線通訊推廣會，Mobile and Wireless Communications Enablers for the Twenty-Twenty Information Society）、無線世界研究論壇（Wireless World Research Forum，WWRF）、南韓 5G 論壇、IMT-2020（International Mobile Telecommunication，國際行動通訊）等各國關鍵資通訊產業力量外，亦與設備商如 Ericsson（愛立信）、Nokia（諾基亞）、Samsung（三星）、研究機構 GSMA、NGMN 及電信業者如 Docomo、Vodafone 等，同時針對異質網路接入也邀請 IEEE（Institute of Electrical and Electronics Engineers，電機電子工程師學會）、WFA（WiFi alliance，Wi-Fi 聯盟）投入對 5G 的研究，各組織之關係簡略如下圖 2-2 所示：

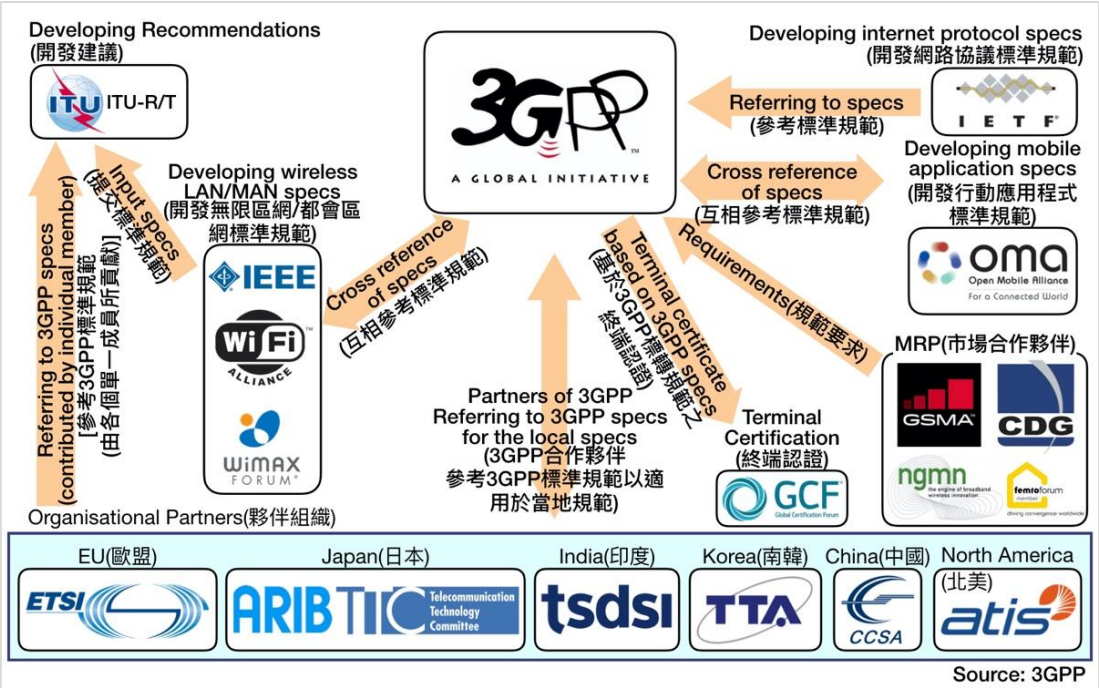


圖 2-2、5G 標準制訂機構關連

資料來源：IMT-2020 PG, 2015、3GPP、本團隊整理

5G 預期會對社會產生廣泛且深遠的影響，為了盡可能地降低任何風險，必須在設計階段就設想未來應用場景所需的安全要求，而不是事到臨頭才開始著手發展安全功能，預防勝於治療，應先提早準備。5G 安全不僅是技術問題，也是一種公共利益，更是一個新的商機，安全議題將涉及 5G 系統的各個方面，從核心網路到網路管理與支援系統的營運，從空中介面到應用程式 API 介面的所有通訊協定，都必須遵守國際標準通過 5G 系統所定義的安全功能和流程機制，具體落實安全且可靠的 5G 服務 [5]。

一、3GPP 之安全焦點

依據 3GPP 安全小組的代表 Stefan Schröder 指出 [5]，由於 5G 網路將帶來物聯網時代，大量裝置的訊息數據傳輸，同時也涉及許多敏感性資料，且虛擬化、軟體化的系統架構也提高了安全風險，因此 5G 網路安全之重點應涵蓋對 5G 各平面所傳遞之訊息安全性強化，如訊息來源驗證（Message Origin Authentication）、訊息的機密性與完整性保護〔Message protection （Integrity /Confidentiality）〕、協同各層強化反偽裝機制（Cross-layer anti-spoofing enforcement）以及訊息內容的授權範圍（Message content authorization），3GPP 制定各個網路功能標準與規範到上述面向上，包含服務註冊與訊息交換過程中的各項程序等。另外，網路系統互通性、網路漫遊服務、跨業者之邊界的安全性亦受到重視。在核心網路的信令在傳遞過程中，逐級跳躍的各個節點亦需要保護其所傳遞之信令是安全的，甚至對於特別敏感之信令要提供端對端的安全（End-to-end Security）。

依據前 3GPP 安全工作組的前主席 Prasad 在 2019 美國 RSA 會議（一國際性 IT 安全研討會）上所做的說明 [6]，針對上述目標進行以下各項工作之相關研究。

(一)主要身份驗證（Primary Authentication）：5G 系統和終端設備相互的身份驗證稱（Mutual Authentication）為主要身份驗證。TS 33.501 [7]除了提供 5G 密鑰機制（5G-AKA）外，還提供異質網路的驗證機制，採常見的 EAP-AKA 機制，以支援如 WLAN 的使用情境。

(二)第二道身份驗證（Secondary Authentication）：第二道身份驗證的目的是要提升用戶的身份驗證能力，使電信業者可以成為一個身份即服務（Identity-as-a-Service，IDaaS）的提供者。

(三)無線電接取網路安全-DU-CU 之分離（RAN Security - DU-CU Split）：在 5G 網路系統中，基地臺可以任意的在邏輯切分為 CU 和 DU 兩個部分，提供靈活的部署選項，TS 33.501 [7]要求啟用機密性保護，使得即使是部署在網路最邊緣的 DU，也無法解開用戶的數據。

(四)強化用戶隱私（Enhanced Subscriber Privacy）：因 IMSI-Catcher 的盛行或者信令攻擊的廣為人知，造成用戶隱私外洩已非罕事，且在 5G 系統中，用戶裝置與網路端均會儲存更多機密性資料，因此 3GPP 在 TS 33.501 [7]提出臨時身份識別碼的解決方案，可以保護或降低用戶的永久識別碼外洩。

(五)網路可視性與組態設定能力（Visibility and Configurability）：5G 系統架構在先天的設計上即開啟加密功能，但此加密安全機制的先天設計僅侷限在網路層（Network layer）中，因此並不能確定加密機制是否存在於更上層的應用層（Application layer）中，故 TS 33.501 [7]要求終端裝置能開放 API 使得加密參數、演算法或流量統計資訊等能被終端裝置上的應用程式所查閱，確認

是否處於有效的加密保護狀態，此為可視性。同時也賦與用戶再其終端裝置上更多的安全功能的組態設定能力。

(六)以服務導向的 5G 核心網路架構（Service Based Architecture）：SBA 為 5G 核心網路的架構，TS 33.501 [7]為其提供安全性保護機制。

(七)強化電信業者之間的安全性〔PLMN(Public land mobile network，公共陸上行動網路）Interconnect Security – SEPP（SEcurity edge Protection Proxy，安全邊緣保護代理伺服器）〕：電信系統中有關 SS7 的密鑰竊取或是路由攻擊以及有關 Diameter 的網路節點偽裝或是信令的來源位置欺騙，這些網路安全事件在近幾年來有見長的趨勢，因此在 5G 跨網連接的安全議題中，SS7 以及 Diameter 的安全性被高度關注，是以在 5G 網路中應使用 SEPP，目的是為加強電信業者之間的互通介面的安全問題。

(八)強化漫遊時本籍網路的控制能力（Increased Home Control）：5G 系統所帶動的物聯網時代將會需要完備網路服務完整覆蓋率，需要盡可能地將網路服務覆蓋零死角，上述需求可能會帶動跨電信業者之漫遊服務情境的增長，尤其未來 5G 小型基地臺的部署，將可能會有跨電信業者合作提供服務的情境出現，因此需要強化網路漫遊時的安全。

(九)與核心網路聯結之 NAS（Non-access Stratum，非接取層）協議發起階段的安全保護（Initial NAS Message Protection）。

(十)5G 與 4G 核心網路之互通安全（5G System – Evolved Packet System Interworking Security）：5G 網路部署初期，要達到網路服務的完整覆蓋並非輕而易舉之事，用戶使用初期，勢必會常有

5G、4G 之跨網路系統介接的情況發生，可能會有降階攻擊（Bidding-down attack）等之網路安全風險，且初期 5G NSA 網路亦是仰賴 4G 架構。

二、3GPP 安全標準及規範

3GPP 已針對前段所述之重點提出部分 5G 網路安全規範，這些規範是承接過去舊有網路系統之安全規範，再考量新的 5G 系統所帶來的風險，並且結合 5G 網路功能（如下圖 2-3 [8]）所提出的規範。

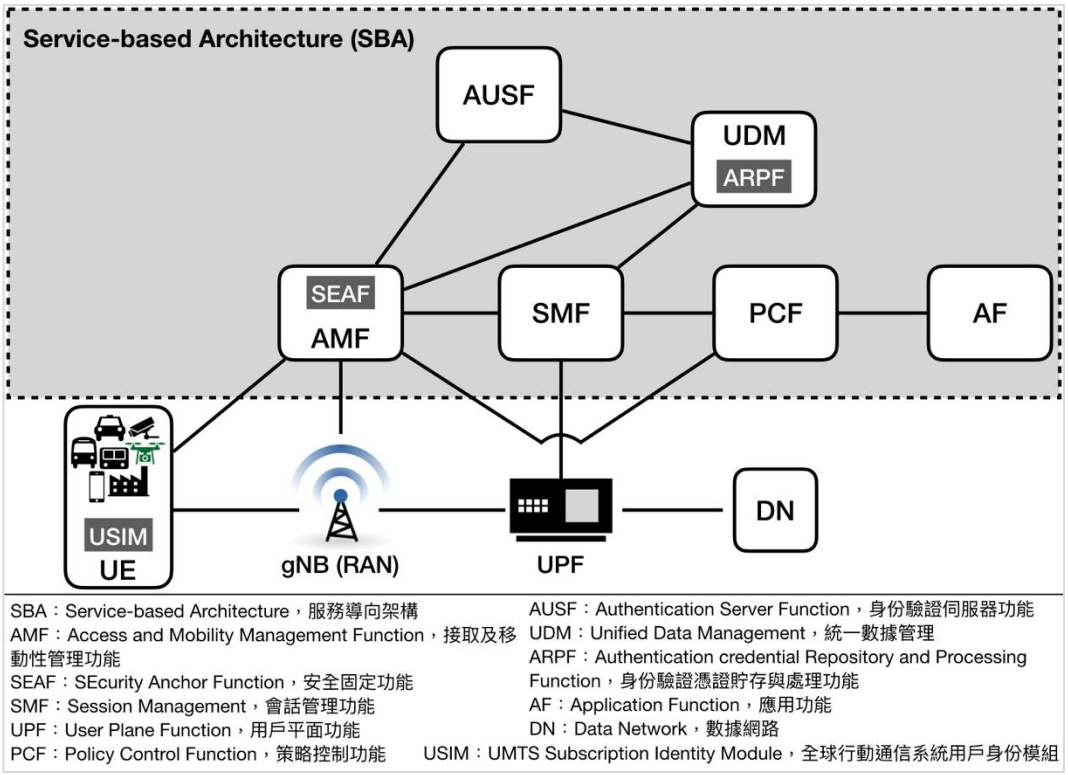


圖 2-3、5G 網路架構與功能簡示

資料來源：Overview of 5G Security in 3GPP、本團隊整理

本計畫整理 3GPP 針對 5G 網路系統所提出的安全規範 [7] [8] [9] [10] [11]，首先 3GPP 提出 5G 網路的信任模型（Trust Model），主要傳達 5G 網路系統架構中各部元件與功能的安全信任等級；第二，提出 5G 網路安全中的密鑰層級框架（Key Hierarchy Framework），表達

出密鑰在整個 5G 網路加密機制中所扮演的角色；第三，建立在信任模型以及密鑰層級框架上，3GPP 針對 5G 網路系統提出相關之安全規範，其內容綜整如下：

(一)5G 網路的信任模型（Trust Model）

從 4G 網路演化至 5G 網路的過程中，整體網路系統的信任關係由二元變為多元化。在過往 3G、4G 網路的系統架構中只有 UE 和電信業者兩個角色，並沒有明確而完整地信任管理體系與概念。5G 網路未來將與垂直場域應用合，將有新的參與者、設備等加入 5G 網路，例如，傳統電信業者通常也是基礎設施與服務的供應者，而在 5G 網路世界中，可能會引入第三方服務提供商的角色。另一方面相較傳統網路的終端用戶，5G 網路的連接裝置除了行動裝置外，還有各式各樣的物聯網設備、交通運輸工具等。因此，5G 網路需要構建新的信任管理體系與概念、研究身份驗證和信任管理機制以定位出各個角色之間的多元信任感。

是以，3GPP 提出了針對 5G 新系統的網路信任模型（Trust model），分為非漫遊情境（如下圖 2-4）與漫遊情境（如下圖 2-5），在這些模型中，安全性會隨著與核心網路的距離增大而遞減。用戶端主要是由 USIM 與 ME（Mobile Equipment，行動裝置）所組成的。另一方面，網路端中的 RAN 被分為 DU 與 CU，兩者組成 gNB，其中由於 DU 可能被部署在不受管制的區域中，因此 DU 不應具備接取用戶通訊資料的權限，而 CU 則會被部署在較安全的受管制的區域中。在核心網路中，AMF 會作為 NAS 信令的完成終止點，與 SEAF 部署在同一位置，SEAF 貯藏最高權限的密鑰（憑證）（Anchor key，固定密鑰）。

在漫遊情境中（如下圖 2-5），用戶本籍網路（Home network）與漫遊的暫訪網路（Visited network）之間是透過 SEPP 來作為互通互作的控制平面連結，以加強其安全性。AUSF 保存用戶端 USIM 所產生的可重複使用驗證密鑰，這個密鑰的使用範圍包含驗證用戶接取有 3GPP 規範的元件與非 3GPP 規範的元件〔如用戶端透過 IEEE 802.11（WLAN）驗證使用〕。ARPF 保存驗證憑證，做為用戶端中 USIM 的對應密鑰，另外用戶數據被保存於 UDR 中，而 UDM 利用保存在 UDR 的用戶數據來執行大多數基本的功能，如產生驗證憑證、用戶資訊、服務等。在空中介面傳輸中，應考量到在用戶平面與控制平面中的主動式攻擊與被動式攻擊，確保數據透過空中介面傳輸的安全性是極為重要的焦點。

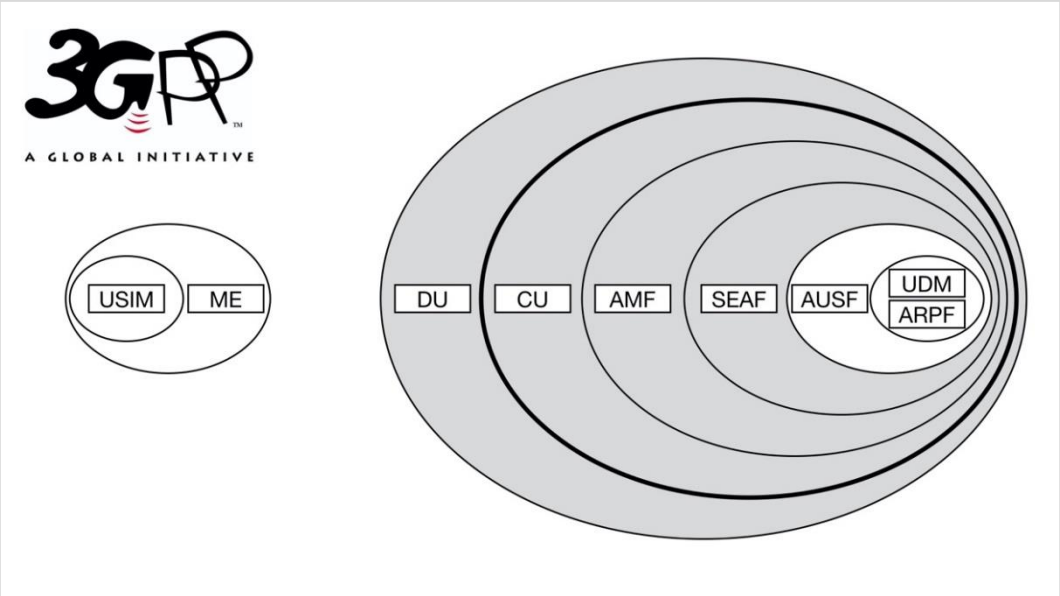


圖 2-4、非漫遊情況下之 5G 網路信任模型

資料來源：3GPP、本團隊整理

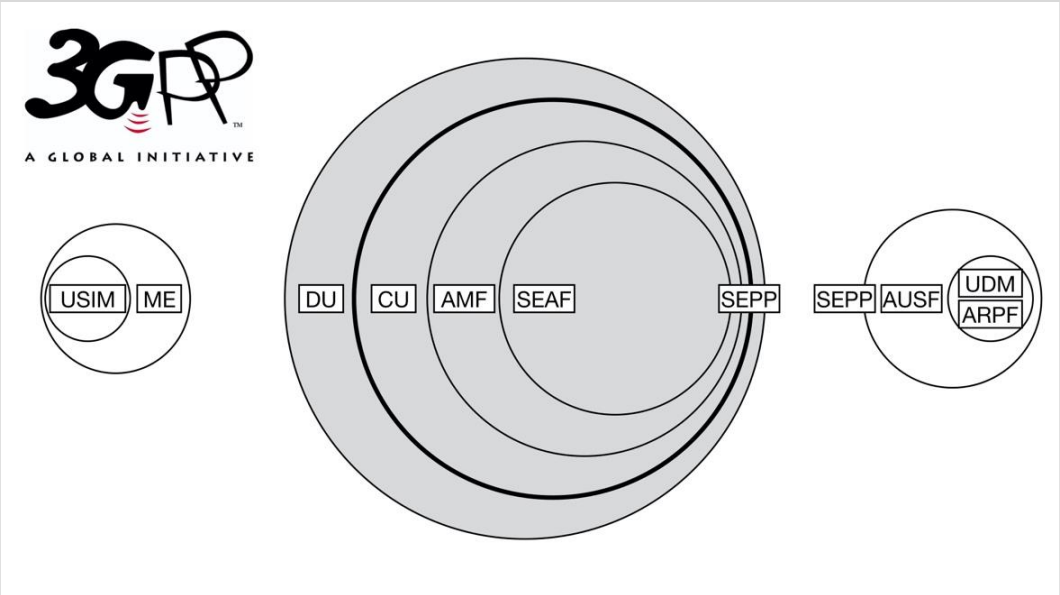


圖 2-5、漫遊情況下之 5G 網路信任模型

資料來源：3GPP、本團隊整理

(二)5G 網路加密機制之密鑰層級框架（Key Hierarchy Framework）

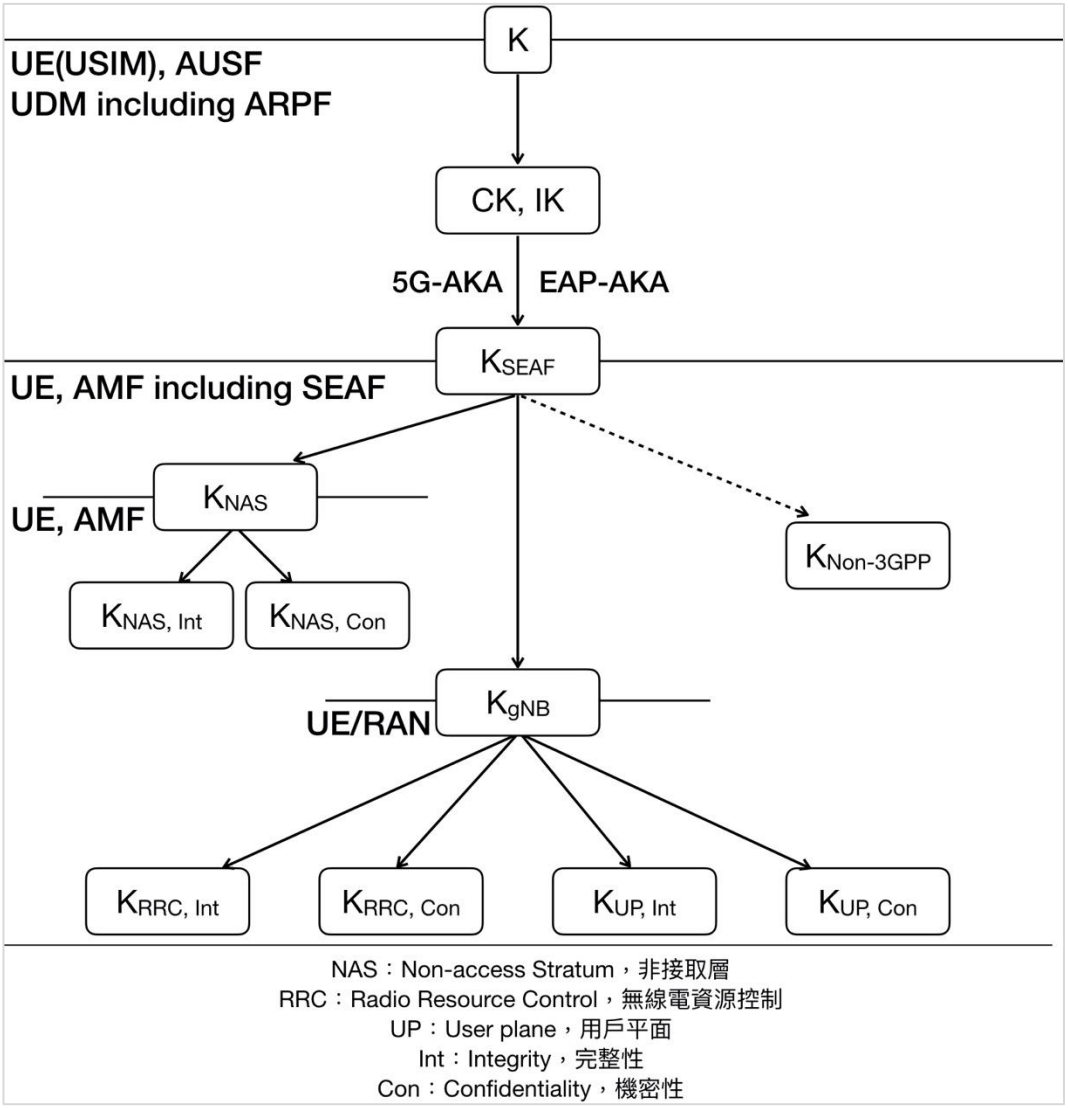


圖 2-6、密鑰層級框架

資料來源：3GPP、Overview of 5G security in 3GPP、3GPP 5G Security 及本團隊整理

傳統加密演算法中，複雜的密鑰生成與分配流程難以確保 5G 網路的高速傳輸與安全防護，而實體層密鑰生成技術的密鑰生成速率受限於無線通訊頻道的容量，這無疑成為 5G 大頻寬數據傳輸的加密技術之一大挑戰。

為了確保 5G 網路的加密機制可以同時符合高速傳輸與安全防護，3GPP TS33.501 [7]為整體 5G 網路安全加密機制中提出密鑰層級框架（Key Hierarchy Framework）（如上圖 2-6）。此份框架展現了密鑰在整個 5G 網路系統中所扮演的角色，框架內容包括密鑰推衍、密鑰功能及密鑰分配。網路系統中的每一支密鑰均會有一支對應密鑰儲存於 UE 中，密鑰的生成是由最初被儲存於用戶端 USIM 中（同時存在於 5G 核心網路 ARPF 中的對應密鑰）的長期密鑰（憑證）（Long-term secret key，K）作為開端，即是安全上下文（Security context）之加密機制密鑰推衍的起源，K 衍生成 CK（Cipher key）與 IK（Integrity key），再根據 5G-AKA 或 EAP-AKA 演算法衍生成 K_{SEAF}（Anchor key，固定密鑰，儲存於 SEAF 中）作為後續 UE 要無線電接取網路驗證的根本密鑰（Root key），下一步 K_{SEAF} 會分成 NAS 與 AS 信令保護分別推衍，NAS 部分會衍生成 NAS 信令的完整性（$K_{NAS, Int}$）與機密性保護密鑰（$K_{NAS, Con}$）；AS 方面，會衍生成 AS 信令的用戶平面完整性（$K_{UP, Int}$）與機密性（$K_{UP, Con}$）保護密鑰，以及 RRC 完整性（$K_{RRC, Int}$）與機密性保護密鑰（$K_{RRC, Con}$），其中用戶平面的完整性保護是一項針對 5G 大量物聯網裝置的加強安全措施；另外，若有網路元件是非 3GPP 所規範的標準，應針對其信令保護 K_{SEAF} 會再多衍生為非 3GPP 規範密鑰（$K_{Non-3GPP}$）。在所有 5G 網路的加密機制中，均應遵循此一框架流程執行。

3GPP 5G 網路安全的目標和 4G 是一致的，就是保證網路和數據的機密性、完整性、可用性（Confidentiality、Integrity、Availability，CIA）。5G 網路安全標準必須包括更多的特性，以應對潛在的新型安全挑戰，並在未來 5G 生命週期中實現網路安全。3GPP 的安全標準化組織（SA WG3）於 2018 年 3 月完成了第一版 5G 網路規範（3GPP TS 33.501）制定 [7]，與 5G 架構及安全相關的 3GPP 標準如下表 2-2 所示。

表 2-2、與 5G 架構及安全相關的 3GPP 標準

架構（Architecture）		
編號	**狀態**	**參考來源**
TR 23.799	已發布	http://www.3gpp.org/DynaReport/23799.htm
TS 23.501	已發布	http://www.3gpp.org/DynaReport/23501.htm
TS 23.502	已發布	http://www.3gpp.org/DynaReport/23502.htm
安全（Security）		
編號	**狀態**	**參考來源**
TR 33.899	已發布並持續修訂	http://www.3gpp.org/DynaReport/33899.htm
TS 33.501	已發布並持續修訂	http://www.3gpp.org/DynaReport/33.501.htm

資料來源：3GPP、本團隊整理

其中標準規範 3GPP TS 33.501（亦被稱為 ETSI TS 133.501，因 ETSI 接受並引用 3GPP 文件為其標準文件）乃是 5G 系統中最廣泛的資通安全重要標準規範之一，該標準規範旨在基於 4G LTE 的安全基礎上，再進一步研究 5G 網路特性並提升新系統的安全性，且對於 4G 安全標準（TS 33.401）發佈後，研提這期間新發現或者具有重大危害之威脅所對應之安全規範。

(三)5G 網路安全相關規範綜整

1. 身份驗證與授權（Authentication and Authorization）：5G 網路揭開了物聯網時代的革命，這使得連網裝置數量將可能呈指數型增長，因此裝置的身份驗證與授權機制將會需要更高大規模的安全防護，TS 33.501 [7]中提到 3GPP 根據 4G 網路提出針對 5G 網路的身份驗證，定義主要身份驗證（Primary Authentication）與第二道身份驗證（Secondary Authentication）：主要身份驗證為必要性措施，用於驗證裝置連結至核心網路的授權，與 4G 身份驗證機制及極為雷同，最主要的差異在於 5G 驗證機制具有嵌入式本籍網路控制功能（Built-in Home Control），這項功能允許本籍網路業者可以得知 UE 在任何網域中是否有進行驗證機制，且可以發出身份驗證要求，意指無論用戶存在任何網域或是意圖跳過身份驗證機制時，本籍網路業者仍可發出身份驗證要求，為網路身份驗證與授權上多一層保障；第二道身份驗證為選擇性措施，只有當主要身份驗證成功執行時，第二道身份驗證才會執行，第二道身份驗證是一項基於 PCO（Protocol Configuration Options，協定組態選項）的驗證機制，用戶在 PCO 中提供 PAP（Password Authentication Protocol，密碼驗證協定）/CHAP（Challenge-handshake Authentication Protocol，挑戰握手鑑別協定）之用戶憑證，3GPP 所規範的第二道身份驗證主要用於接取服務數據網路（Data Network）之驗證，以往 UE 在連接外部數據網路時必須讓用戶輸入帳號密碼來取得權限，而現在有了第二道身份驗證，外部數據網路端可以透過儲存在電信業者內的用戶憑證資料，來達到授權。5G 網路兩種加密驗證機制均支

援 5G-AKA 與 EAP-AKA，5G-AKA 亦規範了 Wi-Fi 協定的加密機制，涵括通訊網路與無線網路的認證，UE 與網路均必須支援此一功能才可以作為初步互相驗證（Mutual Authentication）、後續的服務安全性以及加密程序。

2. 用戶裝置的安全性與資訊隱私（Privacy）：從 3G、4G 網路演變至現今的 5G 網路，甚至是通訊網路以外的各行各業，以及 IMSI-Catcher 的盛行，隱私安全性一直是如火如荼的議題，且 5G 網路中，由於連網設備數量的與安全等級的提升，更複雜加密機制、更多的密鑰與憑證使用、更多的敏感資訊，用戶裝置與網路系統將會儲存與管理比以往更大量的用戶本身的個人（Human）與機器（Machine）的憑證、密鑰與識別資訊等機敏性資料，如果在提供網路服務時讓這些資訊在不安全的情況下傳輸，或是保存在不安全的位置中，這些機密資料可能遭受攻擊者透過硬體、軟體等方法所攔截、竊聽，進而對於用戶本身或是整體電信業者網路的負面影響，因此 3GPP 針對此一威脅提出了用戶憑證儲存在 UE 中的安全規範：(1)用戶憑證的完整性保護、(2)用戶憑證之長期密鑰（K）的機密性保護、(3)對於用戶憑證使用的執行驗證機制，上述三點均必須透過在 UE 上執行部署可防止竄改的硬體元件。

3GPP 在 TS 23.003 [12]中規範了 SUCI（用戶隱藏識別碼）可以用來防止用戶識別碼被竊取，是永久識別碼（Subscription Permanent Identifier，SUPI）的隱藏（Conceal）版本，其執行概念是 UE 利用電信業者提供的公開密鑰（Public Key）以及機率性的非對稱式加密（Probabilistic Asymmetric Encryption）的方法來隱藏識別碼，避免識別碼被顯現並追蹤，在接取本

籍網路(Home network)時，位於 ARPF 中的 SIDF(Subscription Identifier De-concealing Function，用戶識別碼去隱藏功能）會去解除隱藏並取得 SUPI，然而如果在緊急通話的情況下或是電信業者沒有提供公開密鑰時，SUPI 可能不會被隱藏成 SUCI。TS 23.501 [9]與 TS 33.501 [7]中也為 5G 網路系統定義了一種新的 5G 全球唯一臨時識別碼（5G Global Unique Temporary Identifier，5G-GUTI）來最小化 SUPI 與 SUCI 的曝光風險。

3. 用戶裝置與網路之間的用戶平面與控制平面之安全：在 TR 33.899 [13]中敘述到 5G 網路為提供各式多樣化的垂直應用與服務，導入網路切片之概念，將底層實體網路分成多個邏輯網路。這些邏輯網路是相互隔離、獨立管理並且按照需求建立，提供客製化的網路服務，並在切片中利用控制平面與用戶平面來傳送，控制平面為負責傳送控制信令的通道，用戶平面則是傳送用戶資料的通道，上述這樣的網路架構將會使得網路系統中可能會包含許多位於開放環境中的中間節點（Middle nodes），例如異質接取（Heterogeneous access）、NFV 等，因此用戶平面的終端（Termination point）可能會暴露在開放環境中，進而導致其風險提升，萬一完整性保護中的端對端（傳輸層或應用層）的安全協定因效能考量而被排除使用，或是在機密性保護中無啟動加密機制或是使用弱加密演算法進行加密，那麼用戶平面可能遭受到攻擊者的竄改、偽造、攔截或竊聽。另一方面在控制平面中，完整性與機密性保護也扮演著重要的角色。因此根據目前 TS 33.501 [7]與 TS 38.323 [14]所述，在 5G gNB 中使用封包數據匯聚通訊協定（PDCP）用來確保用戶平面與控制平面之安全性，PDCP 使

得終端（Termination point）在較安全的環境中，提供用戶平面與控制平面的完整性與機密性保護，當完整性保護被啟動時，重送保護（Replay Protection）也會同時被啟動，以讓傳輸介面得以安全的完成任務。

根據 TS 33.501 [7]與 TS 23.502 [15]中敘述，當 PDU 在建立新的會話時，SMF 會提供 PDU 之用戶平面安全能力（Security cabability）給予 gNB，安全能力的選擇是由最接近之區域 SMF 來主導，如果用戶平面未對 DRB（Data Radio Bearer，數據無線電載送）啟動完整性/機密性保護，那麼 gNB 與 UE 亦將不會對其啟動完整性/機密性保護。

4. 移動性（Mobility）安全：相較於 4G 網路的移動性管理，5G 網路為提供更多樣化的垂直應用與服務導入網路切片技術，以及為因應大量佈建基地臺而採用 CD-DU 分離架構，根據 TS 33.501 [7]中規範，電信業者可透過考量 gNB 的安全性質，選擇透過 X_n 或是 N_2 切換介面來進行用戶與基地臺間的介接切換（如下圖 2-7）；其中 Xn 切換介面是適用於不涉及 AMF 的切換；而 X_2 切換介面則是適用於涉及 AMF 的切換。

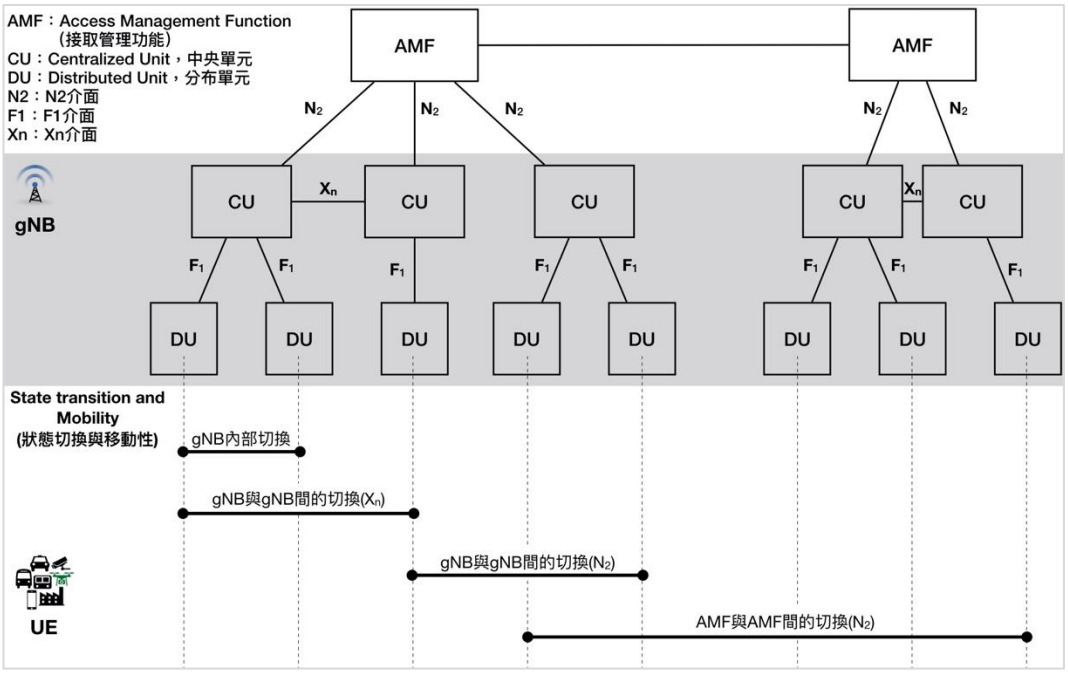


圖 2-7、用戶介接狀態切換與移動性示意圖

資料來源：3GPP、3GPP 5G security、本團隊整理

A. X_n 切換介面：透過 X_n 介面從來源 gNB 切換到目標 gNB 的用戶與基地臺間的介接切換即稱為 Xn 切換，來源 gNB 必須擁有 UE 5G 的安全能力（Security Capability）以啟動來自目標 gNB 要求的切換訊息，如加密與完整性保護機制，目標 gNB 根據預先設定好的切換指令保護機制列表來選擇具有最高優先權的保護機制，被選定的保護機制將會在 UE 中執行，如果 UE 沒有接收到任何被選定的加密或是完整性的保護機制，則 UE 會根據上一次的保護機制來執行切換，再切換指令中，目標 gNB 會將 UE 從來源 gNB 所收到的安全能力資訊傳送到 AMF，AMF 再將所收到的資訊根據已經儲存在內部資料庫的資訊進行比對驗證，如未驗證通過，AMF 會將內部資料庫的資

訊傳送給 gNB 以拒絕連接，並且可能會採取適當的處理措施。

B. N_2 切換介面：透過 N_2 介面從來源 gNB 切換到目標 gNB 的用戶與基地臺間的介接切換（可能包含 AMF 轉換）即稱為 N_2 切換，在 N_2 切換介面中，來源 gNB 擁有 AS 信令的保護機制，這個保護機制被傳送到目標 gNB 供其解密與 RRC 連線建立（RRC Connection Establishment）的完整性驗證。

C. 內部 gNB-CU 切換介面：此切換介面是在 DU-CU 分離時在同一個 gNB-CU 中要切換 DU 的情境下所使用的，因終端（Termination point）相同，所以這個介面不需改變 AS 信令的保護機制，如果 UE 沒有收到新的 AS 保護機制要求，則會繼續執行上一次的保護機制。

5. DU-CU 介面安全：5G 基地臺不同於過往傳統的 4G 架構，為了達到低延遲與多基地臺部署的靈活性，利用 DU-CU 分離的模式來建立，這會導致 DU 與 CU 之間傳輸介面的風險，例如竊聽、攔截等。根據 TS 33.501 [7]、TS 38.470 [16]與 TS 38.472 [17]，5G 基地臺中 DU 與 CU 之間的傳輸介面是透過 F1 來連結並利用 TS 33.210 [18]與 TS 33.310 [19]中規範的 NDS/IP（Network Domain Security Architecture for IP-based Protocol，網際網路協定導向的網域安全架構協定）來保護其安全性，在 F1 間的傳遞訊息包含控制平面與用戶平面，其安全要求必須支援機密性、完整性以及重送保護（Replay protection）的機制，且控制平面與用戶平面的保護機制是互相獨立的，意指可以各自分開設定。

6. 跨網路系統之互相運作安全性（Interworking Security）：5G 網路要全面覆蓋不可能一蹴可幾，用戶裝置必定會在 4G 與 5G 網路系統間作轉換，根據 TS 36.300 [20]所敘，在 5G NSA 網路中主要是利用到 4G-5G 雙連線（EN-DC）的技術，用戶裝置會同時連接到 5G NR 與 4G LTE 訊號，兩者都會連到 4G 核心網路。根據 TS 33.501 所敘 [7]，5G NSA 網路運行時，主基地臺（Master base station，eNB）會計算並且挾帶密鑰（K_{gNB}）與 UE NR 的安全能力（Security Capability）給 gNB，同時 UE 也會生成相同的 K_{gNB}，eMB 會檢查 UE 是否具有 5G NR 的安全能力以及接取 gNB 的權限，gNB 選擇安全機制並且通知 eNB 選擇結果，eNB 再傳送 RRC 連接重組要求（RRC Connection Reconfiguration Request）給 UE 指示其需要設定新的 DRB 或/和 SRB（Signalling Radio Bearer，信號無線電載送）給 gNB 以及計算 K_{gNB}，UE 計算 K_{gNB} 並通知 eNB RRC 已重設完成，eNB 進一步會啟動加解密機制與完整性保護，然後 eNB 再通知 gNB RRC 已重設完成且要求其遵循新的設定結果，近一步也會啟動加解密機制與完整性保護。

7. 跨電信網路之安全性（Inter Operator Network Security）：電信系統中有關 SS7 的密鑰竊取或是路由攻擊以及有關 Diameter 的網路節點偽裝或是信令的來源位置欺騙有日漸增長的趨勢，根據 TS 33.501 中所述 [7]，N_{32} 介面作為跨電信網路之連接橋樑，是透過 IPX（Internetwork Packet Exchange，互相運作封包交換）技術來完成介接，位於 PLMN 中的 SEPP 正是為了強化跨電信網路的安全，SEPP 保護了所有跨 PLMN 中在網路功能交換的服務層資訊（Service layer information）

之安全，意指 SEPP 從網路功能中收到服務層訊息時，會先啟動訊息保護機制再進一步透過 N_{32} 介面傳輸；同樣地，SEPP 從 N_{32} 收到訊息時，會先進行安全驗證機制再傳送到適合的網路功能。SEPP 提供完整性、機密性、以及重送保護的功能，同時相互驗證、授權、加密機制、密鑰管理等亦是 SEPP 的功能之一，除此之外，它也提供拓樸隱藏（Topology hiding）以及偽裝（Spoofing）保護。

8. 網路切片的安全性（Network Slicing Security）：5G 網路具有網路切片（Network slicing）的全新技術，這個技術將會根據不同的網路性質與需求，例如延遲、頻寬、安全性等來畫分成多個虛擬網路，以應對多變的 5G 網路應用需求情境，然而根據 TS 33.501 [7]與 TR 33.899 [13]中在網路切片的基本安全風險考量上，切片的獨立性必須受到重視，如果缺乏切片獨立性，那麼具有接取其中一個切片權限的攻擊者可能也會發動大規模的連帶攻擊，進而連帶影響其他切片，適當的切片獨立性有助於完整性與機密性的保護。此外，在考量獨立性的同時，除切片與切片之間的獨立性外，還必須注意到網路基礎設施與切片的來源獨立性，以將風險最小化。5G UE 具有可同時接取多個網路切片以取得多樣服務的權限，接取的網路也不侷限於僅連接 3GPP 所規範的服務 [7]，當網路切片選擇數據被竄改或是偽裝，那未授權的 UE 可能會使用這些錯誤資訊來連接網路切片並消耗資源。

上述許多安全強化功能都需要在未來 5G SA 架構下才會落實。在 5G NSA 架構中，33.501 規範了 4G eNB 與 5G gNB 之間密鑰推衍

（Key Derivation）的作法 [7]，以利業者可以提早規劃 5G 基地臺的部署。在這情況中 5G gNB 基地臺是受 4G EPC 核心網路所管理，gNB 的密鑰則是由協同工作的 4G eNB 的密鑰所推衍，值得一提的是在此 NSA 架構中用戶的 UP 資料之完整性，因其本質上還是 LTE 架構，一般是無法保證其訊息完整性的。

三、供應鏈風險管理

5G 網路系統供應鏈風險中，各設備之供應、測試及管理等，也在 3GPP 的考量之中，其認為安全保障是確保網路設備達到安全要求的一種方式，同時為確保設備部署遵循安全的開發，除安全的標準化系統和協定之外，還需要確保安全的系統建置，因此，為了使各參與方、相關方對電信網路設備的安全性達成共識，推動電信網路設備製造與營運安全的良性發展，3GPP 制定《安全保障方案（SeCurity Assurance Specification，SCAS）》，目標是為確保網路設備安全上的技術標準，保障基本的網路設備安全，SCAS 編撰框架如下圖 2-8 所示；相關標準如下表 2-4 所示。

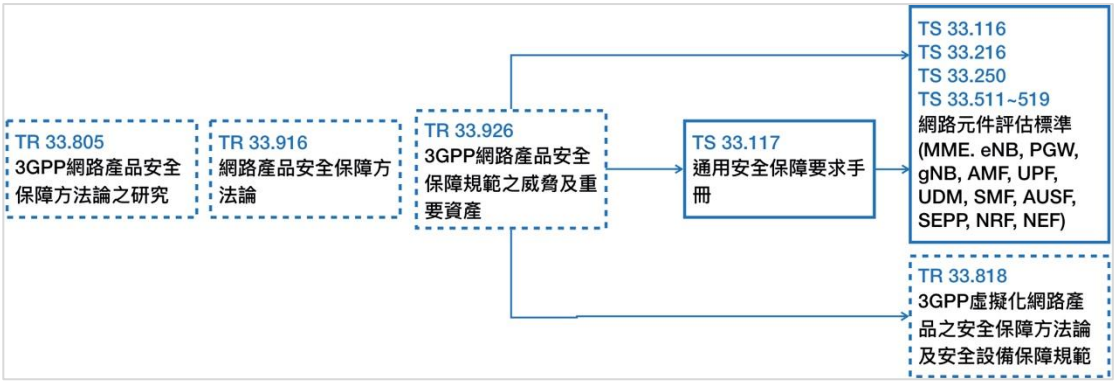


圖 2-8、3GPP SCAS 編撰框架

資料來源：5G 設備安全評測標準解讀、本團隊整理

為確保其定義的各個網路元件之安全性，3GPP 展開安全保障及評估方法研究工作，並編制通用的以及針對各網路元件的安全風險分

析，測試用例及加強措施的技術報告（Technical Report，TR）和技術規範（Technical Specification，TS）。3GPP 認為通用標準中的分級是針對不同的評估規模，不同評估深度和不同評估技術手段來包裝。在通用標準中，不同的等級刻畫了安全評估的實施程度和安全保障不同的水準，其中 3GPP 網路產品的安全評估樣本，評估深度是比較確定的，所以不需要通用標準的評估等級，也不需要通用標準的證書許可過程。以下綜整 SCAS TR 33.805 中載明的方法論 [22]：

1. 網路產品的威脅分析。
2. 對於每一類網路產品採用單一的安全類別和單一的安全評估等級。
3. SCAS 的評估分為：安全一致性測試，基本的滲透測試和增強型之滲透測試。但目前增強的滲透測試還未在 3GPP 的範圍內進行定義。
4. 安全一致性測試：流量管理及保護，對管理面的流量進行機密性和初始化保護，其中測試用例包含所有的網路元件不接收該保護之管理面流量。
5. 基本滲透測試：傳輸介面掃描，要求所有非網路業務需求的傳輸介面都應關閉，測試方式包括對網路設備的所有外部傳輸介面進行掃描。
6. 3GPP 擬定網路設備評估所用的規範：設備商將網路產品提交給評估方。

7. 評估方需要由權威機構來認可：以達到評估方的公信力，在 GSMA 的體系裡面，是由國際實驗室認證聯盟成員基於 ISO 10725 來對某些允許條件的測試實驗室進行認證授權。

8. 評估方基於 3GPP 的規範來進行評估並生成評估報告：基於評估報告，設備商可以自聲明自己的產品通過安全評估，也可以由一些權威認證方來提交證書,說明設備商達成 3GPP 所要求的安全性。

9. 電信業者基於設備商的自我聲明或者是權威認證：來作為設備商產品是否滿足安全需求的依據之一。

TR 33.916 是基於 TR 33.805 確定的方法論技術路線 [23]，描述具體合併替代，包括：如何撰寫一個網路產品的 SCAS 文檔，分些步驟，安全描述，測試用例必須包含這些內容；評估應該由什麼步驟組成，參與分別承擔什麼角色等。TR 33.805 和 TR 33.916 的關係是，TR 33.805 [22]討論幾種可行的方法論，包括通用標準和發展 3GPP 自己的評估方法論，而 TR 33.916 則明確使用 3GPP 自己的方法論，採用方法論的細節進行探討。從安全的角度，TR 33.926 [24]對網路產品的分類所面臨的安全風險，需要保護的關鍵資產等進行識別和描述。從安全的角度，網路產品雖然功能不同，但在安全威脅和安全評估上是有部分共通性，此共性可以形成一些安全評估的最小集合。從安全的考量來說,評估對象包括網路設備本身的核心功能以及相關的傳輸介面，也包括硬體，操作系統等通用的部分，還包括跟管理與維護、本地配置、遠程管理與配置以及營運相關的管理部分。

表 2-3、5G 設備安全保證方案

編號	文件標題
TS 33.517	5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class（安全邊緣保護代理網路設備之 5G 設備安全保證方案）
TS 33.514	5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class（統一數據管理設備之 5G 設備安全保證方案）
TS 33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class（5G 基地臺之設備安全保證方案）
TS 33.513	5G Security Assurance Specification (SCAS); User Plane Function (UPF)（用戶平面功能之 5G 設備安全保證方案）
TS 33.515	5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class（會話管理功能之 5G 設備安全保證方案）
TS 33.518	5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class（網路儲存功能之 5G 設備安全保證方案）
TS 33.519	5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class（網路開放功能之 5G 設備安全保證方案）
TS 33.512	5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)（接取與移動性管理功能之 5G 設備安全保證方案）
TS 33.216	Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class（演進節點 B 之 5G 設備安全保證方案）
TS 33.516	5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class（驗證服務功能之 5G 設備安全保證方案）

資料來源：3GPP

第二節 歐洲電信標準協會（ETSI）

ETSI [25]創建於 1988 年，是歐洲地區性標準制定組織（SDO），成立宗旨是為貫徹歐洲郵政及電信管理委員會（European Conference of Postal and Telecommunications，CEPT）和歐盟執行委員會（European Commission，EC，歐盟執委會）的電信政策，以滿足市場各方面及管制部門的標準化需求，實現開放、統一標準、競爭的歐洲電信市場。ETSI 與 ITU 相比，具有許多差異，首先，ETSI 有很廣泛的公眾性和開放性，不論主管部門、用戶、電信業者或研究單位都可以平等地發表意見，另外，依市場和用戶的需求制定標準，用標準來定義產品，指導生產，針對性和時效性強，也是 ETSI 與 ITU 的不同之處。ITU 為了協調各國，在制定標準時，常常留有許多選項，以便不同國家和地區進行選擇，造成設備標準的統一和互通麻煩，而 ETSI 則針對歐洲市場和世界市場的情況，將一些標準深入細化。

七大 SDO（如表 2-1）共同決定 3GPP 的整體政策和策略，3GPP 亦受 SDO 委託制定通用的技術規範，而各個 SDO 可能會制定國家和地區性的標準，在此過程中需要參考 3GPP 相關標準規範，其中 ETSI 採用 3GPP 標準，並由 ETSI 做日常 3GPP 的維護工作。

第三節 全球行動通信系統協會（GSMA）

GSMA [26]成立於 1995 年，最初成立之主要原因是為了奠定與推廣 GSM（泛歐數位式行動電話系統，Global System for Mobile Communications）行動電話之共通標準，演進至今，其主要工作為協助會員推動新興行動技術之商用化、互通性及研擬相關監理政策，GSMA 會員包括電信業者、電信相關之設備商及網路業者等，主要目的為活絡電信產業之商業發展；在 5G 的工作項目上，GSMA 也將協助電信業者擬定策略、監理框架及研究相關商用及互連之應用發展，以利輔助新世代通訊網路技術的推動 [27]。

5G 網路將會帶動整個上下游供應鏈的發展，會以大量不同的設備供應商加入 5G 產業中，因此對於供應鏈、產品設備風險的議題當中，GSMA 與 3GPP 合作共同提出針對網路元件之《網路設備安全保證方案（Network Equitment Security Assurance Scheme，NESAS）》，適用於電信設備生命週期的安全保障，設備製造商可依循 3GPP 所制定之標準規範（SCAS），設計其產品符合基本安全要求。NESAS 還著重於安全保證方法流程，期望電信業者可透過認證之第三方實驗室，取得各元件之安全認證，此方法可做為未來電信業者採購設備時，對安全性的認定標準。

GSMA 參考 3GPP 所制定之 SCAS 提出網路設備安全保障方案（NESAS），用於網路設備的安全評估。NESAS 引述 SCAS 提出安全基準，對於網路設備需滿足一系列的安全需求，同時證明製造商的開發流程和生命週期管理流程符合安全標準。對於設備供應商來說，NESAS 旨在滿足國際行動通訊網路安全法規的需求，將有助於降低由於各個國家和地區的管制要求以及電信業者的需求差異所導致的

安全需求的差異。對於電信業者來說，NESAS 提供了可行的衡量設備供應商是否落實安全要求的方法。

如下圖 2-9 所示，GSMA 管理、制定並定期修訂整個 NESAS 規範，這項規範包含了設備供應商的開發與產品生命週期之認證、測試實驗室之認證、網路設備之安全性測試評估，GSMA 也制定了爭議解決方案（Dispute resolution）以作為若供應商認證或安全性測試發生爭議時，還是能夠以 NESAS 來解決。

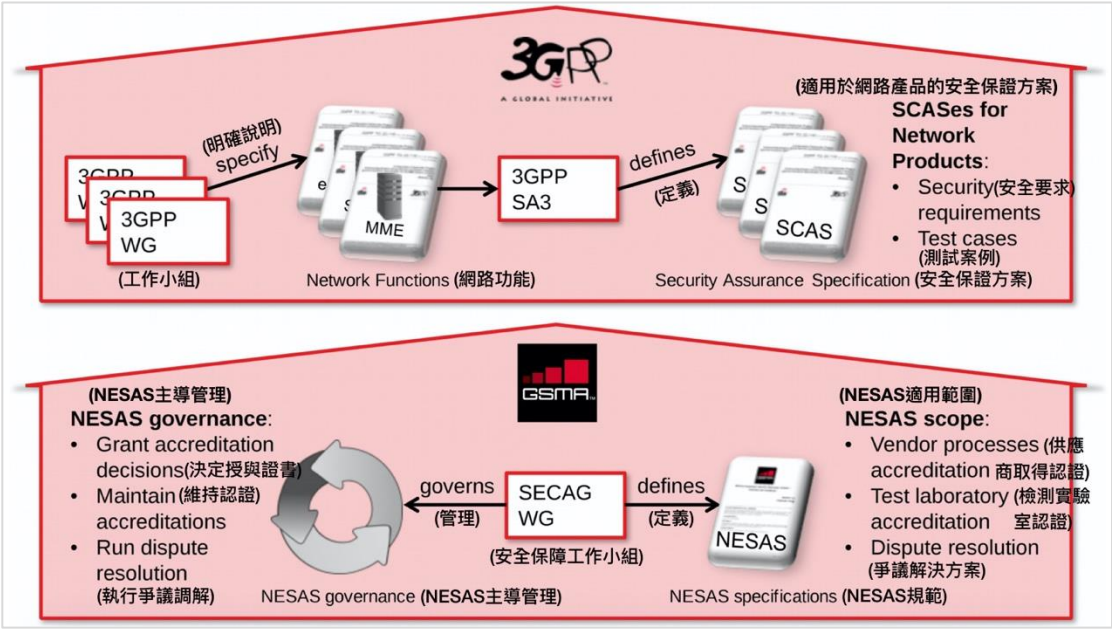


圖 2-9、NESAS 宗旨

資料來源：GSMA Network Equipment Security Assurance Scheme Overview_v0.3、本團隊整理

NESAS 框架包括認證評估和測試評估兩個流程：

(一)認證評估

認證供應商的安全相關開發和產品生命週期過程，向外界宣告此設備供應商確實能夠製造安全的產品；在進行認證時，設備商先定義自己的內部流程（不必公開揭露流程細節），描述如何將安全性

融入到設計、開發、實施和維護過程中，然後藉由外部獨立審查小組（Independent Audit Team，IAT）來執行基於 NESAS 之審核，外部審核員審查設備商所提之流程並確定是否真正落實執行，審核結果會正式記錄在審核報告文檔中。根據 IAT 提供的審核報告，GSMA 將決定是否授予設備設備商通過認證的證書。

(二)測試評估

測試評估實際網路設備的安全性，設備供應商通過認證評估，且被認證為有能力製造安全產品的設備商時，其生產的網路設備必須再透過 NESAS 授權認證合格的實驗室（可為供應商內部實驗室或外部第三方獨立實驗室）來執行產品安全性測試評估，NESAS 引用 3GPP 制定的 SCAS 系列規範作為測試評估的要求，如果通過安全性測試，那這些網路設備的安全性就更具公信力，測試評估報告可以提供給那些即將採購設備的業者參考。

NESAS 框架如下圖 2-10 所示：



圖 2-10、NESAS 框架

資料來源：GSMA NESAS Overview_v0.3

(一)安全測試實驗室的認證

FS. 14 NESAS - Security Test Laboratory Accreditation Requirements and Process（安全測試實驗室認證要求及過程）明述測試實驗室取得合格認證之規範，GSMA 透過 ISO 17025 審查機制來審查實驗室是否具有能力進行基於 SCAS 的網路設備安全性測試所需之相關技能與工具，測試實驗室可為設備供應商本身或第三方單位，安全測試實驗室在獲得 ISO 17025 的認證之後，需向 NESAS 認證委員會提交通過 ISO 17025 認證的證書，認證委員會記錄實驗室的資訊並於評估後向滿足 NESAS 要求的實驗室頒發認證證書，通過的實驗室稱為「NESAS 測試實驗室（NESAS Test Laboratory）」，可執行後續的網路設備產品安全性測試評估。

(二)設備供應商產品開發和生命週期管理流程之認證

依據 FS.15 NESAS - Vendor Development and Product Lifecycle Security Requirements（供應商產品發展與產品生命週期之需求與認證方法）明述認證規範，描述執行稽核和認證的過程。GSMA 指定 IAT 根據此份文件，實施設備供應商產品發展與產品生命週期之認證，並產出審查報告，GSMA 根據其審查報告會決定是否頒發設備供應商安全認可證書。

(三)爭議解決方案

FS. 16 NESAS - Dispute Resolution Process（爭議調解流程）旨在設備商認證、測試實驗室認證、設備測試中，如有發生不符合規定導致未通過，或是執行過程中發生爭議時，這個解決方案基於 NESAS 整體之精神提供了相關的解套，以降低後續再次執行之成本。

(四)網路設備安全評估

根據 3GPP 所制定之 SCAS，包含 TR 33.916, TS 33.116, TS 33.117 等，來對於通過認證之設備商所生產之網路設備進行產品安全性測試評估，並提出測試報告，其中測試僅能由通過認證之測試實驗室執行。

NESAS 定義的網路設備安全保障方案的細部流程 [21]（如下圖 2-11）大概如下：

1. 啟動：設備商提供申請，與 GSMA 指定之審查小組協商審查日期，且與 GSMA 簽訂合約。
2. 審查準備：設備商協商審查範圍，制定議程並向審查小組提交文件。

3. 設備商向審查小組提交文件：審查開始時，供應商和審查小組召開線上或者現場會議，供應商對其提交的資訊進行總體介紹，審查小組可能會指明需要進一步澄清。

4. 審查小組評審文件：審查小組評審設備商所提交的流程是否符合 NESAS 的要求。這個過程中審查小組可能會告訴設備商哪些文件缺失以及提供的資訊所不能滿足的要求，以及雙方協商確定補充文件或修改文件的時間，最後提交完整版文件。

5. 現場審查：審查小組評估包括(1)文件記錄的流程是否被實際應用到供應商的日常營運中；(2)供應商有職員、技能、設備、工作實踐和資源是否有來遵循文件中記錄的流程；(3)員工是否受到充分的流程培訓、理解流程。

6. 結果展示：審查小組向設備商展示其發現，並輸出審查報告，審查小組與供應商就審查報告和審查結果達成一致。

7. 認證：NESAS Accreditation Board（NESAS 認證委員會）接收審查報告，並決定是否授予認證，如果通過認證，則設備商獲得認證證書（Accreditation Certificate），如果設備商不反對，則該證書的副本將在 GSMA 網站上公開。

8. 網路設備安全測試：通過認證之設備供應商將其製造的產品送至通過 NESAS 測試實驗室進行測試，安全測試實驗室依照 SCAS 來評估安全性以後，會將測試報告以及供應商審查報告提供使用業者。

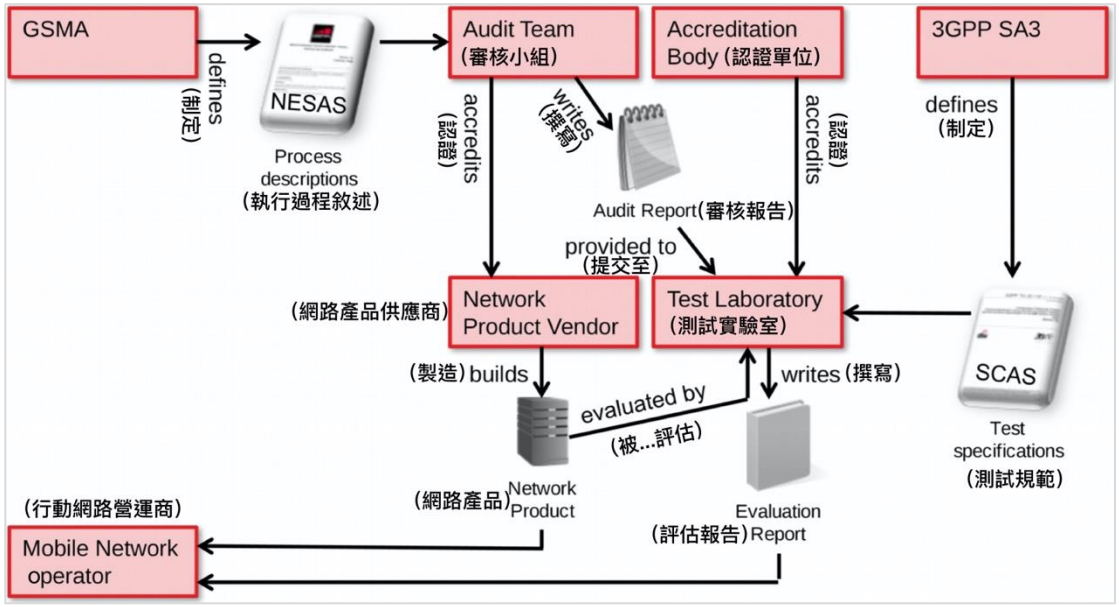


圖 2-11、網路設備安全保障方案流程

資料來源：GSMA Network Equipment Security Assurance Scheme Overview_v0.3、本團隊整理

GSMA 除關注於網路設備安全保障方案 NESAS 外，針對跨電信業者之互連服務，亦提供相關之作業指引，如 GSMA FS.07 SS7 and SIGTRAN Network Security（SS7 信號傳輸網路安全）、GSMA FS.19: Diameter interconnect security（Diameter 互聯安全）；就 5G SA 架構下核心網路之跨業者網路切片安全防護亦有所提及。

網路切片是 3GPP R15 定義的 5G 網路重要特性之一，能夠共享業者之基礎設施，將其構建專用邏輯網路，並使用業者之核心網路功能。雖然 3GPP 已構思了各種網路切片的使用場景，但卻沒有規範網路切片在實際場域的共通屬性，這是因為該項工作並非完全屬於技術性工作，牽涉至各業者之間的商業模式與各樣垂直應用的相異需求。3GPP 只決定技術議題，而技術的市場拓展工作則交由 GSMA，增強從技術到商業化採用這中間的空白。

GSMA 表示將對 5G 提出整體解決策略，以確保垂直應用市場和消費者在 5G 所創造的機會中受益，而 GSMA 所提出之《未來網路計畫（Future Networks Programme）》將指引電信業者在不失可靠性，安全性和可互通性下，降低成本，同時滿足客戶的期望，GSMA 因此在 2018 年 8 月發表《從垂直產業需求到網路切片特性（From Vertical Industry Requirements to Network Slice Characteristics）》報告 [28]，該報告認為應提出通用切片模板（Generic Slice Template，GST）與網路切片類別（Network Slice Type，NEST）來做為行業標準，整體運作模式為電信業者將客戶與網路服務需求映射到 GST 的屬性，並根據服務需求來生成符合需求的屬性數值以建立 NEST。GST 應定義出網路切片在各行各業可以通用的屬性，這些屬性可為供應商，電信業者、第三方服務提供商與切片使用客戶（例如汽車業，工業 4.0 等垂直領域），各方面有共通的溝通基礎，作為參考來理解各方需求，提供切片服務。而更在乎網路基礎設施底層功能之垂直應用領域的客戶、電信業者與他們的漫遊合作夥伴，則可使用 NEST 促進需求理解。GSMA 已經完成了對主要市場的研究，並與潛在的網路切片客戶直接對話，目前正在定義網路切片的服務功能之參數化，使其更具可用與通用。

在前述的基礎上，GSMA 根據 3GPP 之規範文件（Release 15）於 2019 年 3 月發表《通用網路切片模板（Generic Network Slice Template，GST）》指引第一版，並於同年 10 月發表 GST 第二版（此為目前最新版） [29]，報告提出了 5G 網路切片之各種通用屬性，旨在提供一套標準化的網路切片屬性來作為規範網路切片服務應用時應考量之面向及具體標準，這些屬性可分為三種呈現性質；必須呈現、條件呈現（在某些特定狀況下必須呈現）、選擇呈現（可選擇是否呈

現），並根據不同的服務需求調整屬性生成不同的 NEST，每一個 NEST 都有其必須、條件與選擇呈現的屬性數值，以下列出此份指引所提出之網路切片的 35 種屬性：

1. 可用性（Availability）：（GST 第二版尚未明述屬性特質）。
2. 服務範圍（Area of service）：數值為{ sting, string,… }，可填入如臺灣、美國、日本等，屬於選擇呈現屬性。
3. 延遲耐受度（Delay tolerance）：數值為二位元（0 或 1），0 代表不支援，1 代表支援，屬於選擇呈現屬性。
4. 定性通訊（Deterministic communication）
   A. 可用性（Availability）：數值為二位元（0 或 1），0 代表不支援，1 代表支援，屬於選擇呈現屬性。
   B. 週期性（Periodicity）：數值為{ float, float,… }，單位為秒，可填入如運動控制（Motion Control）500×10^{6} 秒，屬於條件呈現屬性。
5. 每一個網路切片之下傳流通量（Downlink throughput per network slice）。
   A. 保證下傳流通量（Guaranteed Downlink throughput）：數值 float，單位為 kbps，可填入如 10 Mbps，屬於選擇呈現屬性。
   B. 最大下傳流通量（Maximum Downlink throughput）：數值為 integer，單位為 kbps，可填入如 10 Gbps，屬於條件呈現屬性。

6. 每一個用戶裝置之下傳流通量(Downlink throughput per UE)。

   A. 每一用戶裝置之保證下傳流通量（Guaranteed Downlink throughput per UE）：數值 integer，單位為 kbps，可填入如雲端遊戲下可達 25000 Kbps，屬於條件呈現屬性。

   B. 每一用戶裝置之最大下傳流通量（Maximum Downlink throughput per UE）：數值為 integer，單位為 kbps，可填入如金牌用戶可達 1000000 Kbps，屬於選擇呈現屬性。

7. 能源效率（Energy efficiency）

   A. 網路切片能源效率（Network Slice Energy Efficiency）：數值 integer，單位為 Bit/Joule（b/j 每焦耳位元），可填入如都市區域 40 b/j，屬於選擇呈現屬性。

   B. 量測的時間架構（Time Frame of the Measurement）：數值為 integer,單位為天,可填入如 7 天量測(每週量測)，屬於條件呈現屬性。

8. 群組通訊支援(Group communication support):數值為 integer，可填入如 0 代表不支援、1 代表單點對多點等，屬於選擇呈現屬性。

9. 隔離層級（Isolation level）

   A. 隔離（Isolation）：數值 integer，，可填入如 0 代表無隔離、1 代表實體隔離（Physical Isolation）、2 代表邏輯隔離（Logical Isolation），屬於選擇呈現屬性。

   B. 實體隔離（Physical Isolation）：數值為 integer，可填入如 0 代表處理程序與執行緒(Process and threads)隔離、

1 代表實體記憶體（Physical Memory）隔離、2 代表實體網路（Physical Network）隔離，屬於條件呈現屬性。

C. 邏輯隔離（Logical Isolation）：數值為 integer，可填入如 0 代表虛擬來源（Virtual Resource）隔離、1 代表網路功能（NF）隔離、2 代表租戶/服務（Tenant/Service）隔離，屬於條件呈現屬性。

10. 基於訊息傳遞之位置（Location based message delivery）：數值為二位元，0 代表不支援、1 代表支援，屬於選擇呈現屬性。

11. 支援之封包最大尺寸（Maximum supported packet size）：數值為 integer，單位為位元組（Bytes），數值可填入如物聯網 40 Bytes，屬於選擇呈現屬性。

12. 任務之關鍵支援（Mission critical support）：數值為二位元，0 代表不具任務關鍵性、1 代表具備任務關鍵性，屬於選擇呈現屬性。

13. 多媒體通訊資源（MMTel support）：數值為二位元，0 代表不支援、1 代表支援，屬於選擇呈現屬性。

14. 窄頻物聯網支援（NB-IoT Support）：數值為二位元，0 代表不支援、1 代表支援，屬於選擇呈現屬性。

15. 網路切片用戶之網路功能（Network Slice Customer network functions）：數值為｛sting, string,…｝，可填入如 UPF、PCF 等，屬於選擇呈現屬性。

16. 連接數（Number of connections）：數值為 integer，可填入 100000 會話（sessions），屬於條件呈現屬性。

17. 終端數（Number of terminals）：數值為 integer，可填入 100000 終端（terminals），屬於條件呈現屬性。

18. 效能監控（Performance monitoring）

    A. 可用性（Availability）：數值{ integer, integer, integer,… }，可填入如服務需求成功率（Service request success rate），屬於選擇呈現屬性。

    B. 監控取樣頻率（Monitering Sample Frequency）：數值為 integer，可填入如 1 代表每秒、2 代表每分鐘、3 代表每小時等，屬於選擇呈現屬性。

19. 效能預測（Performance prediction）

    A. 可用性（Availability）：數值{ integer, integer, integer,… }，可填入如 0 代表流通量（throughput）、1 代表延遲（latency）、3 代表服務需求成功率（Service request success rate），屬於選擇呈現屬性。

    B. 預測頻率（Prediction Frequency）：數值為 integer，可填入如 1 代表每秒、2 代表每分鐘、3 代表每小時，屬於選擇呈現屬性。

20. 位置配置支援（Positioning support）

    A. 可用性（Availability）：數值{ integer, integer, integer,… }，可填入如 1 代表 CID（Cell ID，用戶識別）、2 代表 ECID（Enhanced Cell ID，增強用戶識別）等，屬於選擇呈現屬性。

B. 預測頻率（Prediction Frequency）：數值為 integer，可填入如 1 代表每秒、2 代表每分鐘、3 代表每小時等，屬於選擇呈現屬性。

C. 精準度（Accuracy）：數值為 float，單位為公尺，可填入如正負 1 公尺等，屬於選擇呈現屬性。

21. 無線電譜頻（Radio spectrum）：數值為｛sting, string,…｝，可填入如 n1、n77 等，屬於選擇呈現屬性。

22. 可靠性（Reliability）：（GST 第二版尚未明述屬性特質）。

23. 根本原因調查（Root cause investigation）：數值為 integer，可填入如 0 代表不適用、1 代表被動適用、2 代表主動適用，屬於選擇呈現屬性。

24. 會話與服務連貫性支援（Session and Service Continuity support）：數值為 integer, integer, integer，可填入如 1 代表 SSC mode 1、2 代表 SSC mode 2、3 代表 SSC mode 3，屬於必須呈現屬性。。

25. 網路切片的同時使用（Simultaneous use of the network slice）：數值為 integer，可填入如 0 代表可以與任何網路切片使用、1 代表可以與具有相同 SST 值網路切片使用、2 代表可以與具有相同 SD 值網路切片使用、3 代表不可以任何網路切片使用等，屬於選擇呈現屬性。

26. 切片服務品質參數（Slice quality of service parameters）:數值為｛integer, integer,…｝，可填入如 1, 2, 3, …，需參照 3GPP

TS 23.501 內之 5QI 表（本計畫摘錄部分表格如下表 2-4），屬於必須呈現屬性。

表 2-4、5G 網路切片服務品質之標準 5QI 值

5QI 值	資源屬性	預設優先權	數據封包估計延遲值	數據封包錯誤率	預設最大數據脈衝容量	預設平均時間窗口	應用服務案例
1		20	100ms	10-2	N/A	2000 ms	語音通話
2		40	150ms	10-3	N/A	2000 ms	視訊通話
3		30	50ms	10-3	N/A	2000 ms	直播串流服務、即時遊戲、車聯網…等
4		50	300ms	10-6	N/A	2000 ms	非視訊通話（緩衝串流）
5		10	100ms	10-6	N/A	N/A	IMS 信令傳輸
6		60	300ms	10-6	N/A	N/A	視訊（緩衝串流）、以 TCP 為基礎的服務
7		70	100ms	10-3	N/A	N/A	語音、視訊（直播串流）、互動式遊戲
8		80	300ms	10-6	N/A	N/A	視訊（緩衝串流）、以 TCP 為基礎的服務
9		90	300ms	10-6	N/A	N/A	視訊（緩衝串流）、以 TCP 為基礎的服務

資料來源：3GPP 23.501、Generic Network Slice Template Version 2.0, Global System for Mobile Communications Association (GSMA), 2019-10、本團隊整理

27. 支援非 IP 化流量（Support for non-IP traffic）：數值為二位元，0 代表不支援、1 代表支援，屬於選擇呈現屬性。

28. 裝置速率（Supported device velocity）：數值為 integer，單位為每小時公里（km/h），可填入如 0 代表靜止 0 km/h、1 代表步行 0~10 km/h 等，屬於選擇呈現屬性。

29. 同步性（Synchronicity）

    A. 可用性（Availability）：數值為 integer，可填入如 0 代表不可用、1 代表基地臺與用戶間、2 代表基地臺與各用戶間，屬於選擇呈現屬性。

    B. 精準度（Accuracy）：數值為 float，單位為秒，可填入如 0.0000001 秒，屬於選擇呈現屬性。

30. 終端密度（Terminal density）：數值為 integer，單位為每平方公里之數量（number per km^2），可填入如每平方公里有 10000 臺裝置，屬於選擇呈現屬性。

31. 每一個網路切片之上傳流通量（Uplink throughput per network slice）

    A. 保證上傳流通量（Guaranteed Uplink throughput）：數值 integer，單位為位元組（Bytes），可填入如 10 Mbps，屬於選擇呈現屬性。

    B. 最大上傳流通量（Maximum Uplink throughput）：數值為 integer，單位為位元組（Bytes），可填入如 10 Gbps，屬於條件呈現屬性。

32. 每一個用戶裝置之上傳流通量（Uplink throughput per UE）

A. 每一用戶裝置之保證上傳流通量（Guaranteed Uplink throughput per UE）：數值 integer，單位為 kbps，可填入如虛擬實境下可達 75000 Kbps，屬於條件呈現屬性。

B. 每一用戶裝置之最大上傳流通量（Maximum Uplink throughput per UE）：數值為 integer，單位為 kbps，可填入如金牌用戶可達 1000000 Kbps，屬於選擇呈現屬性。

33. 用戶管理之公開（User management openness）：數值為二位元，0 代表不支援、1 代表支援，屬於選擇呈現屬性。

34. 用戶資料接取（User data access）：數值｛integer, integer, integer,…｝，可填入如 1 代表直接網際網路接取（Direct internet access）、2 代表終止於私人網路（Termination in the private network）、3 代表區域流（Local traffic）無網際網路接取，屬於必須呈現屬性。

35. 車聯網通訊模式（V2X communication mode）：數值｛integer, integer, integer,…｝，可填入如 1 代表 L2TP tunnel（Layer 2 tunneling protocol，第二層洞道協議）洞道、2 代表 GRE（Generic Routing Encapsulation，通用路由封裝）洞道、3 代表 VPN（Virtual Private Network，虛擬私人網路）洞道等，屬於條件呈現屬性。

簡略介紹完 35 種通用屬性後，下表 2-5 舉例具有 IMS 支援的 eMBB 特定網路服務切片需求並依據上述屬性來生成 NEST 範例：

表 2-5、具有 IMS 支援的 eMBB 特定網路服務切片之 NEST 範例

屬性	數值
服務範圍（Area of service）	德國
每一用戶裝置之保證下傳流通量（Guaranteed Downlink throughput per UE）	192Kbps
每一用戶裝置之最大下傳流通量（Maximum Downlink throughput per UE）	50,000 Kbps
多媒體通訊資源（MMTel support）	1
會話與服務連貫性支援（Session and Service Continuity support）	1
切片服務品質參數（Slice quality of service parameters）	1, 2, 5, 6, 7, 8, 9
每一用戶裝置之保證上傳流通量（Guaranteed Uplink throughput per UE）	192Kbps
用戶資料接取（User data access）	0
終端數（Number of terminals）	10,000,000

資料來源：3GPP 23.501、Generic Network Slice Template Version 2.0, Global System for Mobile Communications Association (GSMA), 2019-10、本團隊整理

第四節 美國國家標準暨技術研究院（NIST）

美國為了強化聯邦機構間的合作與協調，2013 年 2 月歐巴馬總統發佈了「改善關鍵基礎設施網路安全（Improving Critical Infrastructure Cybersecurity）」行政命令，該行政命令指出，有鑑於關鍵基礎設施的網路威脅持續增長，成為嚴重的國家安全挑戰之一，為有效防止重要基礎設施網路入侵，需改進網路安全，維護關鍵基礎設施的可靠運作。行政命令同時要求公私部門必須進行網路安全資訊共享，並要求 NIST [30]制定網路安全框架 [31]，以減少關鍵基礎設施的網路風險。網路安全框架應包括一套標準、方法、程序和流程，並應盡可能納入自願協商一致的標準和行業最佳實行做法。本計畫與 NIST 抱持著相同的觀點，資安防護並不是全面防堵，而是要基於風險評估而來 [32] [33]，再選定合適的控制措施。

網路安全框架應提供具有靈活性、可重複性、基於績效和成本效益的方法，包括資訊安全與控制措施，以幫助關鍵基礎設施的所有者和電信業者評估及管理網路風險；且應著重於關鍵基礎設施的跨部門安全標準和準則。NIST 於 2014 年 2 月發佈第一版《強化關鍵基礎設施網路安全架構（Framework for Improving Critical Infrastructure Cybersecurity，CSF）》 [34]，作為各部門制定自身網路安全計畫之參考。CSF 廣泛地被世界各國政府以及相關業者做為網路資安參考依據，截至 2018 年 2 月，已有超過 30%美國本土組織使應該框架，各國包含日本、義大利、以色列、百慕達等，以及國際組織如 ISO（International Organization for Standardization，國際標準組織）、IEC（International Electrotechnical Commission，國際電工委員會） [35]。於 2018 年 4 月，NIST 彙集那些採用 CSF 的企業與單位所回饋的意見，發表 4 年來之重大改版 1.1 版（為目前最新版）。

美國總統川普（Donald Trump）就任後，於 2017 年 5 月發佈「加強聯邦網路和關鍵基礎設施網路安全的總統行政命令（Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure）」，要求各聯邦機構應使用 NIST CSF 或任何後續文件，來管理該機構的網路安全風險 [36]。每個機構負責人應在本命令之日起 90 天內向美國國土安全部（United States Department of Homeland Security，DHS）部長和美國行政管理和預算局（United States Office of Management and Budget，OMB）局長提供風險管理報告；然而對於企業是否採用 CSF 仍是給予選擇權，並非具有強制性的法規。



圖 2-12、NIST CSF 三要素

資料來源：NIST CSF、本團隊整理

NIST CSF 是以風險為基礎所制定的，並由框架核心（Framework Core）、框架實現層級（Framework Implementation Tiers）和框架組態（Framework Profiles）三個要素所組成（如上圖 2-12）；這三要素的意義，分別是資安防護檢核表、落實程度，以及現況的描述，三者環環相扣，相輔相成，參考者可透過資安防護檢核表來檢視其現況與落實程度，以強化其資通安全防護。

(一)框架核心（Framework Core）

包含功能（Function）、類別（Categories）、子類別（Subcategories）和參考資訊（Informative references）如下圖 2-13：



圖 2-13、NIST CSF 框架核心

資料來源：NIST CSF、本團隊整理

1. 功能（function）：辨識（Identify）、保護（Protect）、偵測（Detect）、回應（Respond），以及復原（Recover）五項功能。這五項功能對應組織遭受攻擊的各個階段，分別為事前（識別與防禦措施）、事中（偵測威脅機制）和事後（攻擊因應和災害復原），所需採取之措施及進行探討，並組成網路安全管理的生命週期，藉由這五項功能的要求項目與參考資訊的搭配運用，可使組織順利進行網路安全管理。這五項功能可以分別對應到（如下圖 2-14）本團隊與通傳會共同研析各國際組織、監理機構之資安作為與各國主要電信業者之

5G 網路安全防護策略，並提出第五代行動通信系統資通安全維護計畫參考框架（詳如第伍章）。

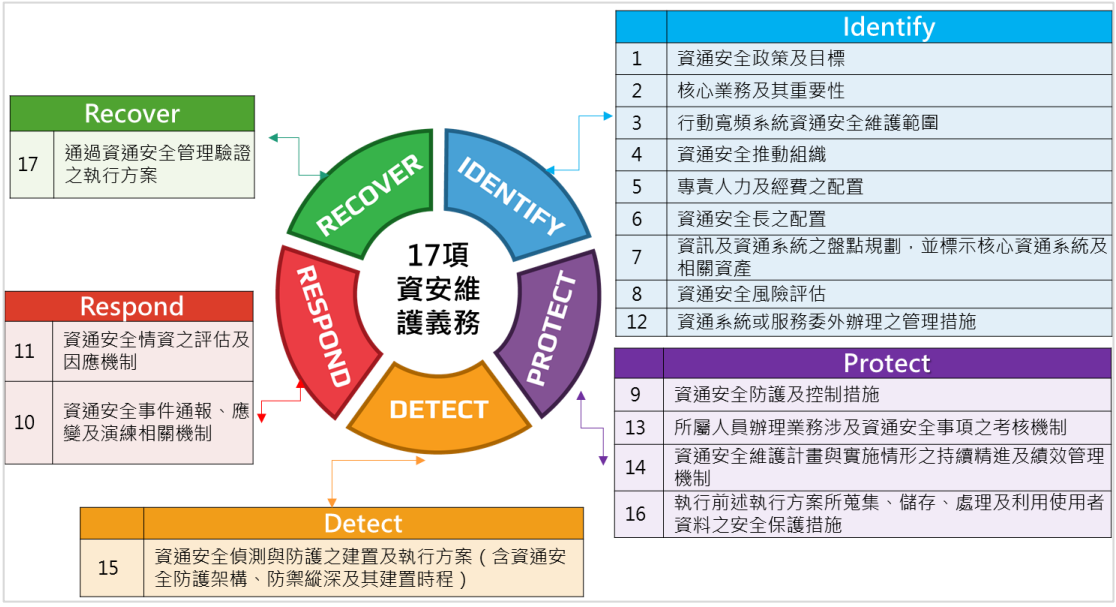


圖 2-14、資通安全維護計畫 17 項應載明事項與 CSF 之對應

資料來源：本團隊整理

2. 類別（categories）：框架核心功能又再細分成多種所需執行的類別，以辨識（Identify）這項功能而言，便區分為下列類別：資產管理（Asset Management）、營運環境（Business Environment）、治理（Governance）、風險評估（Risk Assessment）以及風險管理策略（Risk Management Strategy）如下圖 2-15 所示：



圖 2-15、NIST CSF 框架核心 22 個類別

資料來源：NIST CSF、BSI 整理、本團隊整理

3. 子類別（Subcategories）：各個類別中，均再細分數個子類別，近一步提供更細部的參考框架。以資產管理類別為例，共有 6 個子類別，分別是實體裝置的清查、軟體平臺與應用程式的盤點、資料流量的管理、資訊系統編目列管、資源調度的優先順序，以及與外部合作夥伴之間的所扮演的資安任務等，如下圖 2-16 所示：

Function (功能)	Category (類別)	Subcategory (子類別)
IDENTIFY (ID) (識別)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. 資產管理（ID.AM） 持續識別與管理那些為達到業務目標所運行的數據、人員、設備、系統以及設施，並評估其對於整個組織的目標與風險策略的相對重要性	ID.AM-1: Physical devices and systems within the organization are inventoried 盤點組織內的實體裝置與系統
		ID.AM-2: Software platforms and applications within the organization are inventoried 盤點組織內的軟體平台與應用
		ID.AM-3: Organizational communication and data flows are mapped 定位組織通訊與數據流
		ID.AM-4: External information systems are catalogued 將外部資訊系統分類成冊
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value 依據類別層級、關鍵性、業務價值來衡量資源的重要性（資源如硬體、設備、數據、時間、人員與軟體）。
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established 建立整體公司以及第三利益相關方（如供應商、消費者、合作夥伴）的網路安全相關職位與責任義務

圖 2-16、NIST CSF 資產管理子類別

資料來源：NIST CSF、本團隊整理

4. 參考資訊（Informative references）：包含非營利組織網路安全中心（Center for Internet Security，CIS）指南、資訊及相關技術控制目標（Control Objectives for Information and Related Technologies，COBIT）框架、國際自動化學會（Center for Internet Security，ISA）指南、ISO 27001:2013 及 NIST SP 800-53 [38]；在 NIST 網路安全框架中，從 5 大資安功能類型裡面，再區分「類別」與「子類別」，子類別指的是需做到的事項，組織若要執行這些部分，要根據參考資訊所列出的文件，以便達成子類別的要求。

(二)框架實現層級（Framework Implementation Tiers）

實現層級由低到高，NIST 總共區分為 4 個等級，從最低的層級為部分實施（Partial）、察覺風險（Risk Informed）、察覺風險且可重複實施（Repeatable）、完全適應並實施（Adaptive）四個等級。提供組織如何看待網路安全風險，管理風險的流程之背景訊息（如下圖 2-17）。

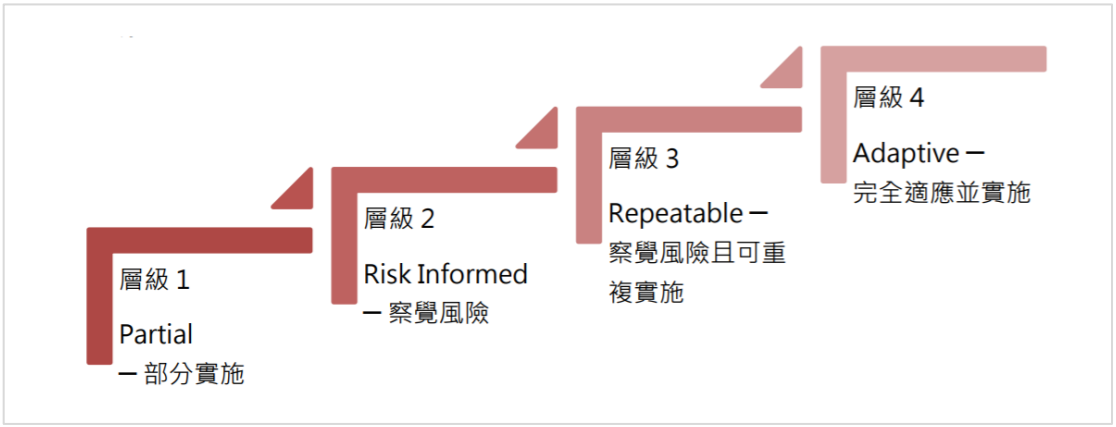


圖 2-17、NIST CSF 框架實現層級

資料來源：NIST、BSI、本團隊整理

(三)框架組態（Framework Profiles）

係組織依照本框架實際操作後所產出的結果，表示組織根據框架類別和子類別中選擇的業務需求，所產生之結果，如下圖 2-18 所示，描述一個在管理階層、業務/過程層和實現/操作層相互協調進行框架實施的過程。

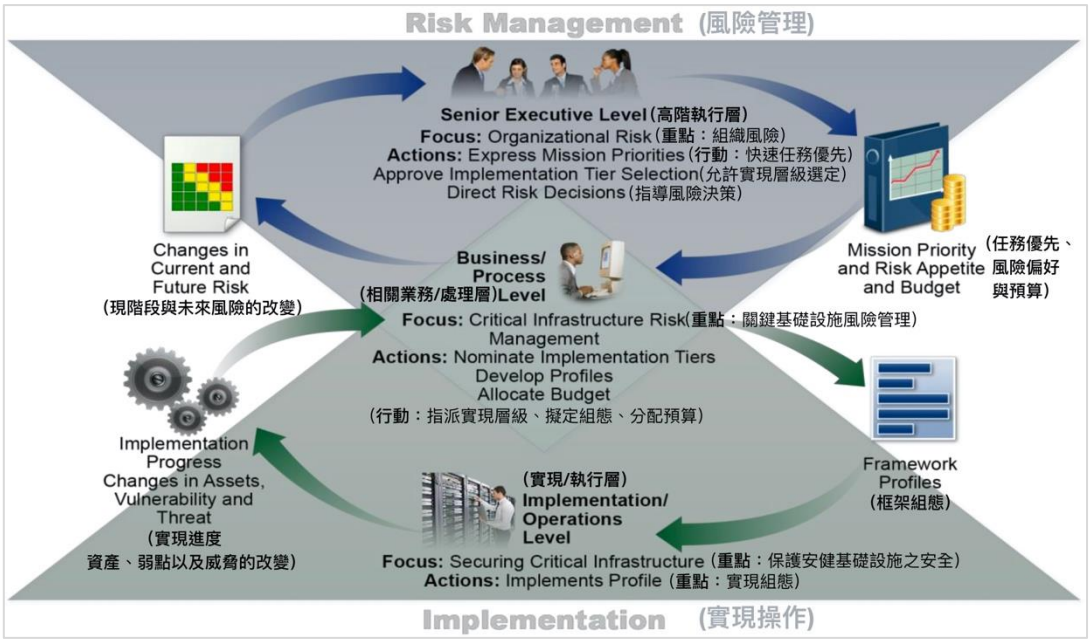


圖 2-18、NIST CSF 框架組態

資料來源：NIST CSF、本團隊整理

如何透過三要素之執行順序及合作關係，建立與實施 NIST CSF 框架，因此，組織在制定一項新的網路安全計畫時，NIST 建議參考以下步驟（如下圖 2-19）進行，並透過不斷地改善與滾動式修正，以強化組織的資訊安全。步驟 1：決定優先順序與範圍、步驟 2：確認目標與方向、步驟 3：建立組織現況的側寫、步驟 4：實施風險評鑑、步驟 5：建立理想目標的側寫、步驟 6：針對差距進行分析及確認優先順序、步驟 7：實施行動計畫；透過以上的實施步驟，組織就可以依據其需要，不斷地重複進行分析與改善其資訊安全。



圖 2-19、NIST CSF 框架建立步驟

資料來源：NIST、BSI、本團隊整理

第五節 網際網路工程任務組織（IETF）

網際網路工程任務組織（Internet Engineering Task Force，IETF）[39]成立於 1985 年，為全球具權威性的網際網路技術標準化組織之一。IETF 始於一項美國聯邦政府支持的計畫，爾後自 1993 年以來，在網際網路協會（Internet Soceity，ISOC）的支持下，IETF 逐步定位為標準制定組織。IETF 是一個大型且公開性的民間標準制定組織，在全球網際網路業界享有網路技術研究的權威，IETF 並沒有正式的入會要求，而是匯集所有與網際網路架構和推動網際網路發展的網路設計者、電信業者、投資者和研究人員所組成的，其中所有的參與人員均是志願性的，故歡迎所有對這個領域有興趣或具影響力的人士參與，此外，其資金來源通常由雇主或贊助商資助。

IETF 主要任務是負責網際網路相關技術規範的研發和制定，負責開發和推廣的網際網路標準，當前全球網際網路的 TCP/IP（傳輸控制通信協定/網際網路通信協定，Transmission Control Protocol/Internet Protocol，TCP/IP）技術協議標準即出自於 IETF。IETF 體系結構分為三個層面，最高層面是網際網路架構委員會（Internet Architecture Board，IAB），其成員由 IETF 參與人員選出，主要是監管各個工作小組的工作狀況。第二個層面是網際網路工程指導團隊（Internet Engineering Steering Group，IESG），主要的職責是接收各個工作小組的報告，對他們的工作進行審查，然後從工作的方向上、品質上和程序上，提出標準、給予一定的指導性建議。第三個層面是在各領域裡面的工作小組，負責具體的標準制定工作；實際上 IETF 有上百個工作小組，這些小組是依據各種不同的研究課題來成立的，如依據網際網路路由、傳輸、應用領域等。IETF 主要產生兩種類型文件，第一種是網際網路草案（Internet Draft）；第二種是更為正式的意見徵詢書

（Request For Comments），是由 IETF 發布的一系列紀錄，通常被視為一種標準或是試驗性的歷史性文獻。

根據 IETF 主席 Alissa Cooper 在 2017 年時公開的資料表示，IETF 在 5G 上的標準化工作方向有二 [40]，第一個方向是發掘現有技術的新用途，第二是開發新技術與其文件。在發掘現有技術的新用途上，現行 5G SA3 小組所制定的加密與身分驗證標準中，所使用的可擴展身份驗證協議（EAP）是直接引用 IETF 現行標準的網路訪問身份驗證框架（RFC 3748），可直接適用基於 SIM 和 AKA 的身份驗證方法，故可能不需要 IETF 多做修改工作，但如果需要，IETF 可以發布新版本，例如，修訂版本的 EAP-AKA。既有的 HTTP/2 協定可作為 5G 核心網路應用層的通訊協定，IETF 於 2015 年發佈為 RFC 7540，透過該協議於 5G 和物聯網應用，可減少延遲並節省網路資源。

而在開發適用 5G 的新技術，IETF 目前正著手進行包含：第一、IP 層的新路由協議制定。第二、傳輸層的新協議制訂，即 QUIC（Quick User Datagram Protocol Internet Connections，快速用戶數據報協定網路連線）。第三、IP 層的確定性網路（Deterministic Networking）技術制訂，此乃搭配 5G 所需之高可靠性與低延遲通訊（URLLC）所需。第四、流量改善與管理工具開發，包含資料鏈結層與 IP 層之新型資料模型，以及軟體定義網路（SDN）的管理工具。

未來 IETF 持續和 3GPP 共同針對 5G 網路發展進行研究，包括以下幾項 [40]：

(一)現有 IETF 技術延伸至 5G 使用的的適用性，例如：EAP 身份驗證機制。

(二)對 5G 網路功能有明確需求的項目，但尚不清楚是否需要更改的技術，例如：5G 的網路切片技術，或是已經提出文件的確定性網路。

(三)對 5G 網路新特性所需新架構開發，例如：新的路由協定或是 CU、DU 分離下的協議。

第六節 下一代行動網路聯盟（NGMN）

下一代行動網路聯盟（Next Generation Mobile Networks，NGMN）[41]由全球主要電信業者（如德國 Deutsche Telekom AG、美國 AT&T、香港 PCCW、西班牙 Telefonica、英國 Vodafone、中國 China Mobile 等 28 家）於 2006 年成立，目標是推動下一世代的行動通訊網路技術，著重於電信業者本身發展需求，並積極主導 5G 標準之制定，力求在電信設備產業圈創造以市場需求為導向的生態圈。NGMN 是一個開放性的聯盟，歡迎更多電信業者、設備製造商、研究單位加入，共同在這個協會中推動下一代網路技術，並保證新技術的效能和實用性；同時也在推動全球標準化、測試設備的開發、進行實驗和評估等。

有關 5G 安全部份，NGMN 有成立專責單位如 P1 5G 架構小組（5G Architecture group）進行研究及發展，NGMN 認為未來 5G 網路安全上，應該建立更安全的用戶驗證方案，必須提供能保護各種數據、資訊的安全機制，且具備強韌性、可用性以及可靠性，以保障端對端安全。NGMN 針對 5G 網路安全提出一個名為《5G 網路能力開放之安全面向（Security Aspects of Network Capabilities Exposure in 5G）》[42]，以下簡述其內容：

(一)一般原則

在網路功能安全的要求之一般原則下，應制定相關規範清楚地說電信業者控制的內容以及可以向第三方機構公開的內容（例如，唯讀和讀寫）。

(二)安全要求

具有存取公開功能的第三方機構應由電信業者進行身份驗證和授權。在數據的傳輸和儲存中，應確保機密性、完整性和重送保護。

(三)安全能力

當用戶接取電信業者的 5G 網路時，UE 將會進行基於訂閱憑據的主要身份驗證，此 5G 網路身份驗證的結果可以公開並重新用於其他服務，這些結果除了包含用戶訂閱相關的模組外，還可能包括用戶的各種資訊與身份驗證方法等。

(四)身份驗證器

在 5G 網路系統中，可以公開與輔助身份驗證並啟動 EAP 身份驗證器。電信業者可以將部分身份驗證器給外部伺服器進行輔助接取身份驗證。驗證器可以從 UDM 獲取訂閱用戶的資料（例如，各種用戶識別碼），並檢查 UE 請求是否符合用戶訂閱和規範。

(五)切片身份驗證

對於 UE 接取切片，UE 應透過電信業者執行的主要身份驗證，電信業者再提供對 5G 網路的接取授權。

另外 NGMN 亦對 5G 網路安全提出相關建議：

(一)電信業者間的無線電介面密鑰傳遞

2G 到 4G 無線電介面金鑰會在核心網路中加密再透過像是 SS7 或 Diameter 等信令通道傳送到網路。要提供傳輸信令安全最直接做

法是提高 SS7/Diameter 安全性，例如加強 SS7 防火牆，同時，設計良好的 5G 密鑰管理協定也可以減少威脅，改善和減少金鑰暴露。（不去使用 SS7 / Diameter 或是類似的改善方法）。

(二)阻斷服務攻擊（DoS attacks）

在 5G 網路中，攻擊者將可能透過大量連接的設備啟動 DoS 和 DDoS 攻擊。DOS 攻擊會消耗目標的物理和邏輯資源，分為兩種類型：

1. 網路（基礎）設施的 DOS 攻擊：直接消耗 5G 用戶和設備的網路基礎設施資源，在上述情況下，攻擊目標在於電信業者的基礎設施，基礎設施攻擊也會間接影響所有被攻擊的網路基礎設備服務的裝置和用戶。

2. 用戶設備的 DOS 攻擊：直接消耗 5G 用戶設備的邏輯和物理資源的攻擊，在上述情況下，攻擊目標是用戶設備，對大量用戶裝置的攻擊可能會間接影響電信業者的基礎設備。

(三)大量受感染的 M2M（Machine to machine）或 IoT 設備

5G 系統將會帶起物聯網應用的蓬勃發展，屆時將會有大量 IoT 與 M2M 設備，這些設備中絕對存在著品質參差不齊的問題，會有許多低成本、低效能、低安全性的設備連上網路，這可能導致安全措施的落實與執行上產生弱點，造成設備容易被入侵、感染的風險，若是有大量受感染的 M2M 或 IoT 設備取得權限而接取網路時，將會迫使分配部分資源去支援這些設備，可能使信令平面超載，即為 DoS 和 DDoS 攻擊。此種攻擊概念是在某特定區域進行大量且同時的網路接取要求來消耗網路資源，如果沒有足夠的無線電資源來同時處理每臺設備的接取服務時，這種同時、連續和大量的無線電資

源攻擊（試圖連接到網路），將會導致系統超載。針對此一問題，應該使用如異常檢測之類的分析技術來分析此類攻擊，如檢測到可能是惡意設備執行的接取請求，將需要通過評估來識別傳輸模式，並選擇性地將那些惡意設備斷網，以防止進一步的破壞。

(四)故意觸發網路過載機制

行動網路可能具有檢測過載的機制，當過載機制觸發時，這些機制通常會暫時限制或阻止裝置對於網路資源的請求，直到過載狀況解除為止。通常受影響的區域中，所有網路資源都在一段時間內都會受到限制，也就是說，過載機制本身其實就是一種阻斷服務。如果攻擊者可以誘騙網路使其以為處於過載狀態下，並因此觸發過載防禦機制，那麼這將會是發動 DoS 攻擊的其中一種方法。降低這種風險的方式關鍵在於如何設計、評估、研究、開發網路過載機制（觸發器和相應的措施）。

第七節 結構化資訊標準促進組織（OASIS）

結構化資訊標準促進組織（Organization for the Advancement of Structured Information Standards，OASIS） [43]是一個推動電子商務標準的非營利國際化組織，組成來自 100 多個國家，成員包括如 McAfee、IBM、Microsoft 等 600 多家組織團體、研究機構和大型跨國企業，OASIS 在軟體開發領域影響力很大，其目標在於發展、整合以及統一世界各地電子商業的專用標準，制定眾多網頁服務標準的同時也提出了電子商務的標準；除提交著名的 XML 和 Web Services 標準，並制定出全球電子商業、網路服務、全球商業的流通，以及電子業出版的安全標準，其針對公眾領域和特定應用市場的標準化付出了很多貢獻。

OASIS 針對強化網路安全部分，在組織中的 IBM、McAfee 和其他 16 個網路安全相關業者共同宣布了開放網路安全聯盟計畫（Open Cybersecurity Alliance，OCA），對建立開放的網路安全生態系統感興趣的產品供應商、研究單位、相關團體組織，以及用戶組成，目標在於標準化所有設備商在軟、硬體開發上都可以使用共同協議商定的技術、數據標準和程序，透過共同開發的程式碼和工具，可以自由地交換資訊或數據、分析資料並得到預期的回應，這些成果將可應用在 5G 網路上，解決來自網路產品間缺乏互通相容能力所造成的問題，以達到產品間的最大效益，特別是能讓網路安全工具能發揮最佳效用，成功抵抗不斷增長的網路威脅。

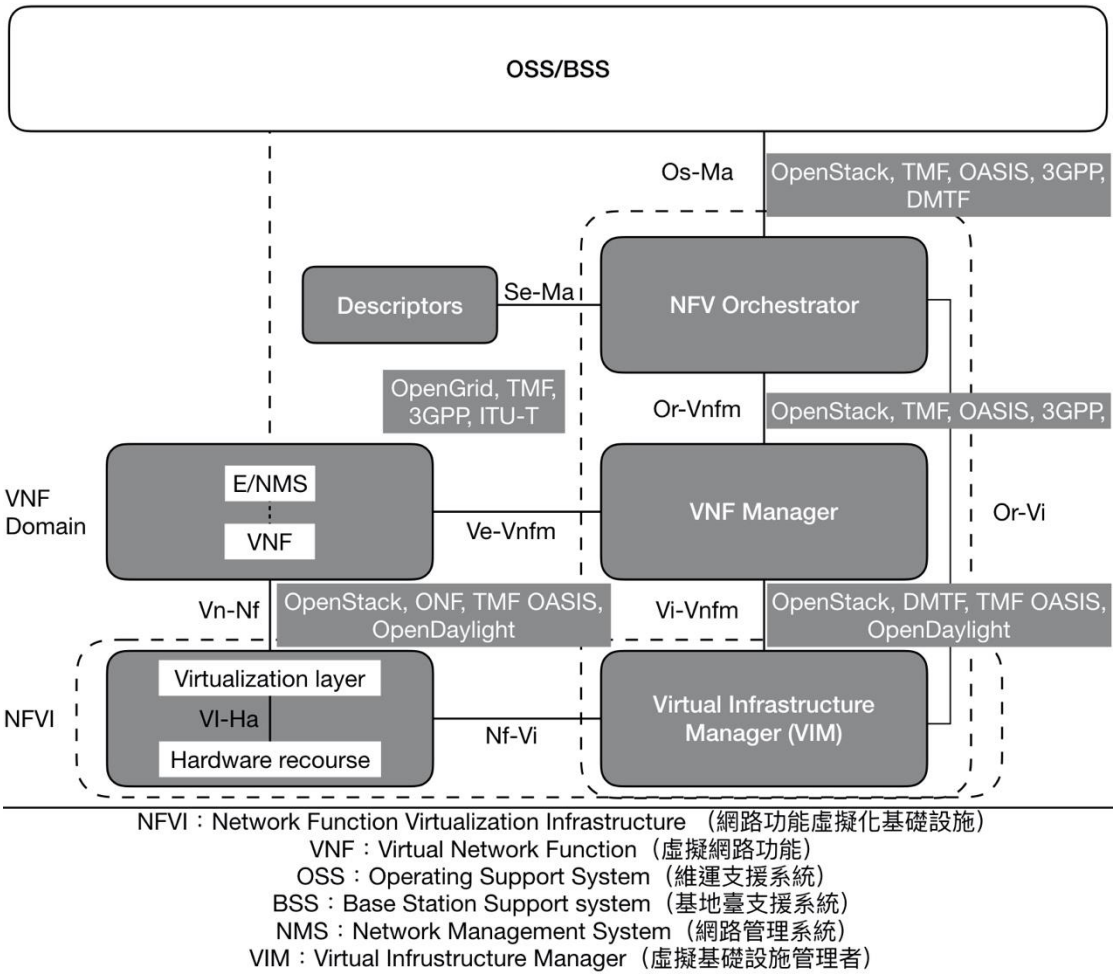


圖 2-20、網路功能虛擬化各介面與標準組織之關係

資料來源：Gray, K., & Nadeau, T. D. (2016). Network function virtualization. Morgan Kaufmann、本團隊整理

在 5G 的標準分工中，OASIS 所負責的部分是互連性（Interoperability）議題中的資訊交換語言的標準制定。具體的例子是 5G 的網路功能虛擬化（NFV）中，各個控制與管理介面的交換語言大部分是由 OASIS 的雲端應用的拓撲和業務流程規範（Topology and Orchestration Specification for Cloud Applications）所規範 [44]。OASIS 所制定的交換語言朝向在兩個面向，第一個是業務致能（service enablers）面向，第二是通訊協議與平臺（protocol/platforms）面向。所謂業務致能面向，乃存在於用戶與虛擬化網路功能之間，是指將複

雜的虛擬網路功能，包裝成一組通用的語言，使得用戶不需理解網路功能虛擬化備後實際的運作，即可完成用戶所需之功能與服務。而通訊協議與平臺就是指實際的虛擬機器基礎建設之間相互溝通的語言。例如上圖 2-20 中 [45]，位於圖右的三個介面 Os-Ma 介面、Or-Vnfm 介面以及 Vi-Vnfm 介面算是業務致能所需的介面，在這些介面中，電信業者的管理流程與作業人員都會有較大的操作、控制與監控權限，而 Nf-Vi 介面則大多是接收命令自動運行。

第八節 國際電信聯合會電信標準化部門（ITU-T）

國際電信聯合會電信標準化部門 [46]（International Telecommunication Union - Telecommunication Standardization Sector，ITU-T），該部門起源於 ITU [47]，ITU 是聯合國負責國際電信事務的特別機構，是世界上歷史悠久的國際機構之一，作為聯合國的機構，所有聯合國的成員都可以是 ITU 成員國，發佈的標準比大多數其他同一級別的技術規範制定組織擁有更高的國際認同度。1992 年時，在全球化日益發展以及世界電信市場逐步開放的背景下，ITU 於日內瓦召開的全權代表大會，並進行機構內部徹底重組及精簡，最終形成了三大部門，分別為電信標準化部門（ITU-T）、無線電通訊部門（ITU – Radiocommunication Sector，ITU-R，國際電信聯合會無線電通訊部門）和電信發展部門（ITU – Telecommunication Development Sector，ITU-D，國際電信聯合會電信發展部門）

ITU-T 部門成立於 1993 年 [48]，總部設在瑞士日內瓦，匯集世界各地的專家，主要負責制定國際標準〔被稱為 ITU-T 建議書（ITU-T Reccomendations）〕，這些國際標準在全球 ICT 基礎設施中扮演著極其重要的角色，無論進行語音、視訊或是數據交換，均可改善各國的 ICT 網路和設備使用相統一的標準化語言，對各國電信網路互連互通有至關重要的作用。

ITU-T 由各研究小組（Study Group，SG）進行，並交由 ITU-T 成員代表針對國際電信各個領域制定達成共識的建議書（ITU-T Reccomendations）。有關 5G 的相關標準化工作類似於 4G，基本上將 5G 發展劃分為 3 個階段，第一階段重點是完成 5G 宏觀描述，包括 5G 的目標，5G 的技術趨勢和 ITU 的相關決議；第二階段為技術準備階段，主要完成技術要求，技術評估方法和提交相關技術所需要的模

板等；第三階段是正式向全球匯集 5G 的初始技術，並進行技術評估、技術討論，並將達成一致之結果公告於全世界。另外，3GPP 是一個產業聯盟，其目標是根據 ITU 的相關需求，制定更詳細的技術規範與產業標準，並規範產業的相關作為。

至於網路安全的部分，是由 ITU-T SG17 負責制定相關安全標準。SG17 與數據安全相關的研究項目可分為以下幾類：通訊技術業務中涉及的個人資訊、生物特徵資訊的安全問題、雲計算的數據安全、大數據安全、電子商務與金融科技、生物識別、以及車聯網、區塊鏈等特殊應用產業等。SG17 持續研究安全和隱私管理標準，處理已識別的威脅和風險，提出可能的方法來制定技術建議書（ITU-T Reccomendations），並與 SG17 相關單位及利害關係人共同合作。

由於 5G 網路將會採取軟體定義網路（SDN）的架構，因此目前 ITU-T 對 5G 資安的相關研究主要以 SDN 安全面向進行研析，其中一份建議書 ITU-T Reccomendation X.1042 [49]中提到，SDN 安全方面可以分為集中式防火牆、集中式誘捕系統（Honey pot）、集中式 DDoS 攻擊減輕、集中式非法裝置管理以及接取控制管理，五個防護建議：

(一)集中式防火牆

集中式防火牆可以對 SDN 交換機進行管理，能夠在這些交換機上加入或取消政策，例如有發現新的威脅時，可以定義新的政策，並落實於交換機中。

(二)集中式誘捕系統

這個概念可以使得誘捕系統的位置受到動態管理，集中式誘捕系統可以誘使攻擊者掉入設下的陷阱中，即為誘捕系統，誘捕系統收集資訊後向集中式誘捕系統傳送、回報。

(三)集中式 DDoS 攻擊減輕

這項方法可以增加、刪除、修改 SDN 各個交換機的策略。

(四)集中式非法裝置管理

這項方法可以管理非法設備黑名單以防止設備流量，這些黑名單保存在資料庫中，且可以透過人工或是自動的方式進行更新。

(五)接取控制管理

接取控制管理（Access and Conrtol Management）功能利用 SDN 控制器可以分層管理接取權限，並達到防止惡意接取。

第九節 本章總結

面對 5G 網路的崛起，各國際組織均積極制定全球統一、通用的標準，包含通訊功能、安全規範等，以利各國家及地區在發展 5G 網路時有所依循，並且確保安全上的基準，後續再由各國根據這些標準各自發展出自己的策略。本計畫為推動國家 5G 通訊網路健全發展，研析各主要國際組織所發布之全球通用規範，包括 3GPP、ETSI、GSMA、NIST、IETF、NGMN、OASIS 與 ITU-T 八家國際組織，其中以 3GPP 與 GSMA 之 5G 相關規範為最大宗，例如 3GPP 主要發布 5G 網路架構的規範，發布了許多功能面、資安技術面的規範；GSMA 針對 5G 網路設備供應商提出一套標準。下表 2-6 綜整出上述八家國際組織之重要作為：

表 2-6、國際組織針對 5G NSA 網路資通安全要求總表

組織定位	國際組織	相關作為
架構制定組織（Architecture）	第三代合作夥伴協議（3GPP）	・ 發布許多全球通用的標準規範，其中以 TS 33.501 為最重要之安全指標，內容涵蓋網路系統中的各個面向之安全性，如隱私、身份驗證、密鑰管理、跨網路系統之介接、移動性等。 ・ 制定《設備安全保障方案（SeCurity Assurance Specification）》，作為網路設備供應商之審查評估及其設備測試評估之要求。 ・ 與 GSMA 共同制定了《網路設備安全保障方案（Network Equipment Security Assurance Scheme）》，主要用於設備供應商的管理要求。

組織定位	國際組織	相關作為
	全球行動通信系統協會（GSMA）	・ 與 3GPP 共同制定了《網路設備安全保障方案（Network Equipment Security Assurance Scheme）》，主要用於設備供應商的管理要求，內容包含設備商認證評估與設備測試評估兩大項。 ・ 發表《通用網路切片模板（Generic Network Slice Template）》指引，旨在提供一套標準化的網路切片屬性來作為網路切片服務應用應考量之面向及具體標準。
協定、平臺制定組織（Protocol/platform）	網際網路工程任務組（IETF）	・ 現行 3GPP 5G SA3 小組所制定的身份驗證協議（EAP）係直接引用 IETF 現行的網路接取身份驗證框架（RFC 3748）。 ・ 目前正著手研究：IP 層新路由協議制定、傳輸層的新協議制定、IP 層的確定性網路技術制定與流量改善與管理工具開發等四大研究課題。
服務啟動組織（Service enabler）	結構化資訊標準促進組織（OASIS）	・ 在 5G 網路中主要致力於互連性（Interoperability）議題中的資訊交換語言的標準制定。如 5G 在 NFV 中，各個控制與管理介面的交換語言大部分是由 OASIS 的雲端應用的拓撲和業務流程規範（Topology and Orchestration Specification for Cloud Applications）所規範。
流程與資訊模組制定組織（Process and information models）	國際電信聯合會電信標準化部門（ITU-T）	・ 主要投入於 SDN 應用的風險威脅，並提出相關建議書

組織定位	國際組織	相關作為
綜合性組織	歐洲電信標準協會（ETSI）	・ 主要制定歐盟市場地區性的統一規範。 ・ 與 3GPP 合作，採用許多 3GPP 的標準規範，並執行日常 3GPP 的維護工作。 ・ MEC 的開發。
	美國國家標準暨技術研究院（NIST）	・ 發表《強化關鍵基礎設施網路安全架構（Framework for Improving Critical Infrastructure Cybersecurity）》，除了作為美國公、私部門制定自身網路安全計畫之參考，全球亦有許多官方機關、私人組織參考此一架構。架構主要由核心、實現層級與組態三個要素所構成。
	下一代行動通信網路（NGMN）	・ 提出《5G 網路能力開放之安全面向（Security Aspects of Network Capabilities Exposure in 5G）》，內容講述 5G 網路安全風險，並提出建議。

資料來源：本團隊整理

本章節以資安角度為出發點，研析與彙整國際上重要組織之 5G 網路系統功能、架構、規範，其中最具影響力之一的組織即為 3GPP，它制定許多 5G 網路系統的通用標準，提供給世界各國政府與電信業者可依循標準規範來建置通訊系統，在 3GPP 的眾多文件報告中，以資安面來說最具代表的即是 TS 33.501 標準技術規範，其從資安面向切入並規範網路系統應該如何建置與操作，例如：移動性介接流程、密鑰推衍流程、跨網互通性之安全規範等，可作為電信業者在建置網

路系統以及施建資通安全控制措施時很重要的一份參考文件。然而，除技術面的議題外，國際上對於 5G 網路建設時，例如：如何識別、檢測、驗證及信任供應商設備是否可信賴，亦表達強烈關切，主要原因在於隨著 5G 網路逐漸普及，此類有資通安全疑慮之系統設備也將漸漸進入各國 5G 網路商用市場，各國主管機關若不積極督促與協助電信業者和系統設備商排除不安全之第三方系統設備商，將可能會有國家機密外洩之潛在風險等，而嚴重影響國家安全，為此，3GPP 和 GSMA 共同制定《網路設備安全方案》，發起國際性的設備認證，包含設備商製造流程以及產品的安全性評估，推動網路設備的安全性，以對應 5G 供應鏈相關之風險，對於業者之供應鏈風險評估或是資產盤點的部分均有很大的助益。最後值得一提的是美國 NIST 所提出的 CSF，此一文件提供非常完整的資通安全管理參考框架，總共涵蓋三個要素，框架核心、落實程度以及現況描述，其中框架核心點出資通安全管理中所應該遵循的流程，包含識別、保護、偵測、回應、及復原五大功能，指明出應該注意的威脅與風險，並且提出參考文件供使用者參酌以應對風險，後續再根據落實程度以及現況描述來讓使用者確認自身之資通安全管理狀況，以持續精進其資通安全管理政策。

第參章　全球各主要國家 5G 資通安全維護監理作為或法令以及電信業者相關作為

根據 GSA 截至 2019 年年底的統計 [50]，全球已有上百個國家正在規劃或已進行 5G 釋照作業與相關頻譜投資整備政策措施，如南韓於 2018 年 6 月完成了 3420-3700 MHz 與 26.5-28.9 GHz 的頻譜拍賣，澳洲於 2018 年 12 月釋出 3575-3700 MHz，美國在 2019 年 3 月完成 24 GHz 與 28 GHz 的頻譜拍賣，歐盟有 6 個國家；丹麥、芬蘭、法國、德國、義大利、瑞典，已完成 700 MHz 的頻譜拍賣，10 個國家；奧地利、捷克、芬蘭、德國、匈牙利、愛爾蘭、拉脫維亞、義大利、西班牙和英國，已完成 3.4-3.8 GHz 的頻譜拍賣；而義大利完成了 26 GHz 的頻譜拍賣，其他國家與其他頻譜在未來的近幾年都有 5G 頻譜拍賣計畫。在亞太地區 2019 至 2021 年間，香港、印度、紐西蘭、泰國、日本及我國也都有 5G 釋照計畫。在中東及非洲地，沙烏地阿拉伯、阿曼、卡達、坦桑尼亞、加納、巴林、南非及以色列在 2019 年也都有 5G 頻譜釋照計畫，顯見各國政府刻正大力推動 5G 頻譜整備與釋照及建設，希望藉由 5G 頻譜釋出與 5G 網路建置，推動創新服務應用發展與次世代行動通訊網路升級。各國 5G 已經商轉之電信業者整理如下表 3-1 所示：

表 3-1、各國已商轉 5G 電信業者一覽表

國家	業者
澳大利亞	Optus
	Telstra
紐西蘭	Spark

國家	業者
巴林	Batelco
	Viva
愛沙尼亞	Elisa
愛爾蘭	Vandafone
芬蘭	Elisa
	Telia
德國	Deutsche Telekom
	Vandafone
義大利	TIM
	Vodafone
科威特	Ooredoo
	Viva
	Zain
萊索托	Vodacom
馬爾地夫	Dhiraagu
摩納哥	Monaco Telecom
菲律賓	Globe
卡達	Ooredoo
	Vodafone
南韓	KT Corporation
	LG Uplus
	SK Telecom
羅馬尼亞	RCS & RDS （Digi Mobil）
	Vodafone
拉脫維亞	Tele2
沙烏地阿拉伯	STC

國家	業者
	Zain
南非	Rain
西班牙	Vodafone
瑞士	Sunrise Communications
	Swisscom
英國	EE
	Vodafone
	3UK
	O2
阿拉伯聯合大公國	Du
	Etisalat
烏拉圭	Antel
美國	AT&T
	Sprint
	T-Mobile
奧地利	Drei
中國	中國電信
	中國移動
	中國聯通

資料來源：GSA 2019/12

5G 新型態行動網路架構與通訊技術，將為未來社會帶來各式各樣垂直產業的新興服務，如 5G 智慧交通、5G 智慧工廠、5G 智慧醫療或開啟 5G 物聯網世代，卻也為網路資訊安全與用戶隱私保護帶來新的挑戰。

隨著 5G 釋照，另一個資通安全危機便是來自於不受信任之第三方系統設備商的加入。近期朝野立委針對我國政府機關採購不受信任第三方之系統設備表達強烈關切，主要原因在於 5G 網路未來將逐漸普及，然而此類有資通安全疑慮之設備商將其生產的系統設備若進入我國的 5G 網路商用市場，將會對我國的 5G 資安造成嚴重威脅，甚至危害到國家安全；5G 網路之安全議題，不僅止於資通安全之範疇，亦涉國家安全之考量，因此本章概述了美國、歐盟、日本等國所提出的 5G 安全相關建議。

第一節 全球主要國家針對 5G NSA 資通安全監理作為或法令

一、美國

美國聯邦通訊委員會（FCC）於 2018 年 9 月提出《美國 5G 科技加速計畫（Facilitate America's Superiority in 5G Technology，5G FAST Plan）》[51]，旨在奪回美國在 5G 的領導地位，領導力和國際影響力，刺激美國在 5G 基礎建設與創新投資，保持美國科技業的競爭力，並反對外國政府採取不正當手段和不正當手段在電信設備領域佔據主導地位，於 2018 年所提出的一系列作法，本計畫在此針對其供應鏈安全的作為與要求，整理各要點如下。

(一)透過 FCC 所掌管普及服務基金（USF），下達採購限制要求

多年來，美國政府之情報單位在各國電信設備供應鏈上扮演重要的角色，對於那些潛在造成國家安全的惡意設備表示擔心，這些惡意設備的滲透威脅所帶來的風險包括「惡意修改或竊取資料」和「進行更隱密的間諜活動」。FCC 所採取的策略是透過 FCC 所掌管近 90 億美金的普及服務基金（Universal Service Fund，USF），下達採購限制要求，引述其要求為「禁止繼續使用普及服務基金所支付購買或獲取對電信網路或電信供應鏈中會對國家安全構成威脅的任何公司所生產或提供的任何設備或服務」。

(二)向公眾徵詢意見，組成工作小組以列舉出清單

FCC 根據 USF 的使用管理權限，禁止對任何可能構成國家安全威脅的公司購買設備或服務，且對外徵求意見，包括：

1. 未來如何更好地實施禁令。

2. 應涵蓋哪些類型的設備和服務。

3. 如何持續辨識與增加所涵蓋之供應商清單。

4. 本案行政成本和效益分析，並評估所有可行的替代方法。

FCC 尋求公眾意見，如何更好地實施該提案，包括這樣做的成本和效益所擬議規則應涵蓋哪些類型的設備和服務，應如何確定涵蓋哪些供應商，以及 USF 預算執行者者如何審查那些供應商。FCC 相信，其蒐集的紀錄將能夠盡自己的一份力量來幫助保護美國的國家安全。

美國參議院於 2019 年 3 月提出《超越 5G 安全法案（Secure 5G and Beyond Act）》 [52]，除保護美國的基礎設施外，並推動美國盟友採取一致性安全防護行動，及協助外國盟友提高該國電信網路軟、硬體之安全性。

另外，美國國防部 2019 年 4 月提出《5G 網路科技之防護應用（Defense Applications of 5G Network Technology）》報告 [53]，建議制定供應鏈標準，並在 3GPP 工作小組內對其進行優先排序，推動未來的標準發布，以擬定電信安全計畫，驗證系統的可用性、機密性和完整性。

2019 年 5 月 15 日，美國總統川普（Donald Trump）簽署行政命令，依據《國際緊急經濟權力法（International Emergency Economic Powers Act，IEEPA）》 [54]，以國家安全為理由，簽置《保護資訊科技與服務供應鏈（Securing the Information and Communications Technology and Services Supply Chain）》行政命令 [55]，禁止美國企業採購對國安具備威脅之外國電信設備實施作法。

美國在網路安全標準的推動上主要由國家標準暨技術研究院（NIST）維護，其認為安全的供應鏈才能提升電信網路之可靠性，以下列出美國各個時期的行動通訊網路安全相關作為 [30]。

在 5G 初期的營運階段，都是仰賴 5G 系統與 4G 系統共存的架構，即 5G NSA，必然觸及 4G 安全議題。在 4G 的安全議題上，美國 NIST 於 2017 年發表技術文件《NIST SP 800-187：Guide to LTE Security（LTE 網路安全指南）》，該文中除說明 LTE 的網路營運基礎指南以及安全機制外，亦舉出對 LTE 網路構成的安全威脅與相關的緩解措施 [56]。

在此整理該文件三大要點，(1)LTE 安全架構、(2)LTE 網路威脅與(3)緩解措施，以下分點說明。

(一)LTE 安全架構

1. 加密概述：先說明 LTE 的安全架構，LTE 的加密功能主要發生在終端裝置與基地臺的空中介面，以及終端裝置的身份驗證功能，其後不論是後傳網路或者核心網路的資料傳遞都是 LTE 加密安全的關注重點，但 5G 會改善此一情況。

2. 通用積體電路卡（UICC）硬體安全：Universal Integrated Circuit Card（通用積體電路卡，UICC）是終端設備的身份驗證硬體晶片，優秀的 UICC 晶片具有防竄改與防止旁通道攻擊功能，也就是一般所知的 SIM 卡。UICC 在 LTE 的身份驗證中具有重要的角色，是身份密鑰的儲存體與衍生與基地臺通訊時的會話密鑰之產生器。

3. UE 認證協議：LTE 的 AKA 是由 3GPP TS 33.401 所規範 [57]。其中值得注意的是整個認證過程是由 MME 來進行身份確認，

無論是 UE 從 UICC 索取的密鑰以及 HSS 所提供之密鑰都是交由 MME 來進行比較確認，故若 LTE 之 MME 被攻陷或有軟體錯誤，則後續很難偵測與除錯，這點在 5G 也有改進。

4. 空中介面安全：此部份談論終端設備與基地臺之無線電連接層之安全性，同樣也是由 3GPP TS 33.401 所規範。其安全性主要是控制平面上的完整性保護且需不受重放攻擊的影響，當然機密性就不言而知，但在資料平面上則是僅有機密性，不具完整性保護。

5. E-UTRAN 安全：此部份主要解決終端裝置於基地臺間交遞時（Handover）的會話密鑰是否要需要 MME 介入重新交換的議題。

6. 後傳網路安全：此部份主要談及後傳網路的加密技術的議題，若情況允許，是建議開啟 IPsec，但開啟 IPsec 非強制規定。

7. 核心網路安全：在 LTE 中核心網路已是全面 IP 化，在 3GPP TS 33.210 中有規定不同網域的設備要互通時，其間之連線需啟用 IPsec，但在實務上業者僅會劃分一個網域，各網路元件的流量不需加密，使得本項規定淪為空談 [18]。

(二)LTE 網路威脅

1. 一般網路安全威脅：此部份如同一般的電腦網路，LTE 網路一樣面臨惡意程式之威脅，且電信網路愈開放，不論是智慧手機、x86（32 位元架構）基地臺以及雲端化的核心網路，所面臨的惡意程式將日益猖獗。另一個常被人忽略的是管理與營運網路（OAM） 網路的未經授權接取，由於維運上的需要，電信網路的功能元件都具有遠端管理的功能，設計不

良或者未強化安全設定抑或是疏於安全管理，會導致嚴重的事件。

2. 偽基地臺：攻擊者架設偽基地臺偽裝成合法業者，進行用戶與設備地理位置追蹤或阻斷其服務，如緊急通話。甚至透過降階攻擊，破壞空中介面的機密性與完整性保護，來竊聽或竄改用戶通話與數據。

3. 空中介面的監聽：如果業者沒有加密用戶平面的流量，則可能發生空中介面的竊聽。

4. 透過家用微型基地臺（Femtocell）發動攻擊：Femtocell 在網路的架構上是直接連結業者的核心網路，但不幸的是 Femtocell 的物理安全，恐不是業者可以預料的，攻擊者若可實際碰觸 Femtocell 系統或修改其電路，是有可能破壞業者的防禦機制或取得 IPsec 連線密鑰，進而對 CN 發動攻擊。

5. 無線電干擾攻擊：干擾攻擊是透過產生無線電的雜訊來中斷 LTE 網路的接取能力。干擾終端裝置抑或是基地臺皆可能發生。

6. 後傳網路與核心網路的竊聽：由於後傳網路與核心網路並不是強制啟用加密，故內部人士或者有心人士有機會竊聽後傳網路與核心網路的流量。

7. 對網路設備的物理攻擊：電信業務一樣是需要實體設備作為其基礎設施，但這些實體設施一樣會遭到天災與人禍，例如竊賊偷取銅纜，導致網路中斷。

8. 對身份密鑰的攻擊:LTE 的身份密鑰是 LTE 安全功能的基礎，存有密鑰的 UICC 以及位於業者核心網路的 HSS/AuC 乃攻擊者的高價值目標。

9. 服務竊取：攻擊者利用竊取、社交工程或者內部人合謀，取得或換發用戶的 UICC，進而牟利。

(三)緩解措施

1. 採用行業的最佳實行作法（Best Practice）。

2. 空中介面開啟加密。

3. 提示用戶目前是否處於加密保護。

4. 教導用戶關閉其手機中連接至 GSM 網路的選項。

5. 開啟 S1 介面的加密功能。

6. 開啟核心網路各元件之加密。

7. 啟用 SIM 卡之 PIN 碼。

8. 使用臨時身份識別碼機制，如 GUTI(Global Unique Temporary Identity，全球唯一臨時識別碼），取代 IMSI。

9. 聯合第三方提供端到端的保護，如應用層加密，而不僅僅是依賴電信業者所提供的安全機制。

10. 對遲遲未經認證的裝置，若已經判定其行為異常，允許業者可拒絕其接入網路。

美國為了強化聯邦機構間的合作與協調，2013 年 2 月歐巴馬總統發佈了「改善關鍵基礎設施網路安全（Improving Critical Infrastructure Cybersecurity）」行政命令 [31]，該行政命令指出，有鑑於關鍵基礎設施的網路威脅持續增長，成為嚴重的國家安全挑戰之一，為有效防止重要基礎設施網路入侵，需改進網路安全，維護關鍵基礎設施的可靠運作。行政命令同時要求公私部門必須進行網路安全資訊共享，並要求 NIST 制定網路安全框架，以減少關鍵基礎設施的網路風險。

NIST 於 2018 年 4 月發佈最新版《提升關鍵基礎設施資通訊安全之架構（Framework for Improving Critical Infrastructure Cybersecurity，CSF）》 [34]，供公私部門進行網路身分驗證與識別、資通安全風險自我評估、供應鏈管理及弱點察覺等資通安全防護參考，CSF 詳細內容整理請參照**第貳章 第四節 美國國家標準暨技術研究院（NIST）**。

美國總統川普（Donald Trump）就任後，發佈「加強聯邦網路和關鍵基礎設施網路安全的總統行政命令（Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure）」 [36]，其中，要求各聯邦機構應使用 NIST CSF 或任何後續文件，來管理該機構的網路安全風險 [58]。

二、歐盟

歐盟執委會於 2019 年 3 月 26 日公告《5G 網路之網路安全建議書（Commission Recommendation - Cybersecurity of 5G Networks，5G CR）》 [59]，5G CR 指出，歐盟各成員國應合作確保 5G 網路建設高度安全性，且各成員國應在 2019 年 6 月底之前完成對 5G 網路基礎設施的國家風險評估 [60]，ENISA 於 2019 年 11 月對外提供 5G 威脅報告《ENISA Threat Landscape for 5G Networks》 [61]。在此基礎上，成員國應更新對網路設備供應商的現有安全要求，尤其是在 5G 設備安全的許可方面。如果企業不遵守成員國的標準與相關法律規範，成員國有權基於國家安全原因將企業排除在市場之外，成員國應與歐盟執委會合作制定特定的設備資通安全規範，以適用於 5G 網路相關設備的公共採購，內容包括在公共採購中，應實施網路安全認證計畫的強制性要求，因為該計畫尚未對所有電信業者與設備供應商具有約束力，因此，成員國應制定適用於與 5G 相關的公共採購的具體安全要求，如網路安全認證計畫的強制性，一旦制定與 5G 網路相關的歐洲網路資通安全認證計畫，成員國應遵循聯盟法律，並通過國家法規，對網路資通安全認證計畫所涵蓋之 ICT 產品、服務或系統進行強制認證。

5G CR 建議書中指出，數位生態系統之基礎設施具有互聯性、跨國性，以及所涉及之威脅的跨境域性，這意味著若是有一個成員國發生與 5G 網路有關之任何重大漏洞或網路安全事件都將影響到整個聯盟，這也就是為何應該提供資通安全保護措施的主要原因。歐盟為提高整體安全級別的一致性，應開發網路資通安全認證計畫，此計畫的開發為當務之急，對於相關網路基礎設施安全保障至關重要，應針對 5G 網路相關之使用的資訊、ICT 產品、服務或流程等提供嚴密的保

護措施。各成員國和業者應積極參與此類認證計畫的開發，在尚未統一的歐盟法律情況下，各成員國可以遵循通過歐盟法律的國家技術法規，來考量開發歐洲網路安全認證計畫。

2019 年 6 月 27 日，公布《歐盟網路安全法案（EU Cybersecurity Act，CSA）》 [62]，加強網路安全結構、增強對數位技術的掌控、確保網路安全應當遵守的法律規範，並指定歐盟網路與資訊安全局（European Union Agency for Cybersecurity，ENISA）為永久性的歐盟網路安全職能機構，負責組織歐盟網路威脅演習，以測試面對威脅的恢復能力，並和歐盟各國的電腦安全緊急事件應變團隊（Computer Security Incident Response Team，CSIRT）一同應對網路安全事件，提供支持與分享資訊的平臺。

《歐盟網路安全法案（CSA）》提到，由於資訊服務流通可以跨越國境限制，歐盟基於單一市場的角度認為資通安全政策應能夠覆蓋整個歐盟。以下列出在近幾年資通安全方面，歐盟的主要政策，包含：

1. 2016 年生效的網路與資訊系統安全指令（Directive on security of network and information systems，簡稱 NIS 指令）。
2. 2016 年的隱私及電子通訊指令（Directive on Privacy and Electronic communications，簡稱 ePrivacy 指令）
3. 2018 年生效的一般資料保護規範（General Data Protection Regulation，簡稱 GDPR）。
4. 2019 年 6 月 27 日生效的歐盟網路安全法案（CSA）。

以上四部法規都與電信業者息息相關，電信業者為法案所規管或附帶義務的對象，以下分述之。

(一)NIS 指令

是歐盟有關網路安全的第一部法律，在 NIS 指令要求三項措施，以提升歐盟整體的資通安全水平，違反 NIS 指令者依各國法規不同，各有民事與刑事責任，如比利時民刑皆罰。NIS 三項措施如下。

1. 要求歐盟會員國提升該國 NIS 事務的主管機關權限，使其可以有權限行使 NIS 指令，做好適當資安資源的整備，例如建立電腦安全緊急事件應變團隊（CSIRT）。

2. 通過建立跨國合作工作小組，在所有會員國之間開展合作，以支持和促進會員國之間的戰略合作和資訊交流。還需要建立各 CSIRT 合作關係，以促進針對特定網路安全事件的快速有效的應變，並共享有關風險的資訊。

3. 各會員國需明確辨識該國哪些企業是屬於資通訊關建基礎建設的企業。這些被認定提供基本服務的業者，必須採取適當的安全措施，並將嚴重資安事件通知該國的主管機關。除了電信業者，服務提供商，如搜索引擎、雲端服務或電子商務等業者也將必須遵守 NIS 指令中的安全性和通報要求。

(二)ePrivacy 指令與 GDPR

皆為歐盟公民的數位隱私所設置的法規。ePrivacy 指令要求無論使用何種技術的業者，這些在公共網路上經營業務的企業須提供高水平的資料和隱私保護，如隱私始於設計（privacy by design）。電信業者和服務提供商都擁有大量的客戶數據，必須對其進行加密和採取適

當的保護，若發生資料竊取、外洩，或被違法存取，ePrivacy 指令要求業者通報給該國的隱私主管機關與受害者用戶。GDRP 則是規範隱私資料保護具體的要求與規範。

(三)歐盟網路安全法案

可被視為 NIS 指令的強化版本，除確立 ENISA 的角色與定位外，該法案設立了一個資訊安全的認證框架，該法案要求：

1. 為 ICT 產品、服務和流程建立歐盟網路安全認證框架。
2. 要求會員國至少指定一個該國國家級的網路安全認證機構。
3. 要求 ENISA 協助制定歐洲網路安全認證框架相關政策並協助各國實施。
4. 要求會員國在其本國法規中規範違反歐洲網路安全認證的後果與處罰。

(四)歐盟電子通訊法典（EECC，European Electronic Communications Code）

根據歐盟近期批准的電子通訊法典（EECC） [63]，會員國必須確保維護公眾電信網路的完整性和安全性，且各會員國需保證其電信業者所採取之技術和措施可以適當地管理、維運網路安全，此外，監理機關具有權限，發布具有約束力的指示並確保業者遵守這些指示的權力，各會員國可以附上額外有關保護公眾電信網路安全的其他要求，以防止未授權接取電信網路，保護通訊的機密性。根據以上要求，德國已經採取相關行動，如對 5G 設備發展的相關驗證機制，但未來 ENISA 若制定新的規範，且是獲得歐盟批准歐盟 5G 計畫，則必須以 ENISA 為主，因法案中也賦予 ENISA 制定標準的角色。

回到歐盟網路安全法案的規定，每個 ICT 產品、服務或流程都具有其獨立的認證計畫，認證計畫將是通用整歐盟範圍內，法案中規定認證計畫所需的多達 22 個要件，但總括來說，每個認證計畫均應具體說明：

1. 涵蓋的產品類別。
2. 具體網路安全要求，可參考相關標準或技術規範。
3. 評估執行的方法類型，可為自我評估或第三方評估。
4. 依照風險評估所預期的保證級別，分為基本、中級或高級。
5. 持續遵守資安規範的監督機制。
6. 取得認證後不遵守規範且被認定不合格的後果。
7. 與第三國相互認證的條件。
8. 製造商或供應商在提供補充資料時應遵循的格式和程序。
9. 認證計畫有效期間，至少每五年要審查一次。
10. 關於如何回報和處理新發現網路安全漏洞的機制。

歐盟網路安全認證目前還是採自願進行，但未來也不排除各國採納為強制的國家法規。歐盟也建議各會員國還可以通過政府採購來強化歐盟網路安全認證實施。

5G CR 與網路安全法案指導方針是建議採取一系列措施，以提升整個歐盟的 5G 網路安全，各成員國必須在 2019 年 6 月底前完成 5G 網路安全風險評估，並互相分享資訊，最晚在 2019 年 7 月 15 日之前將國家風險評估報告提交予歐盟執員會和 ENISA，並在執委會的支持下，ENISA 也在 2019 年 11 完成 5G 網路之歐盟層面的風險評估結

果，包括網路威脅風險類型、以及相關的緩解措施，以提升歐盟 5G 網路安全，遵循正確之 5G 網路安全推進方式與其預期之工作時程規劃，歐盟 5G 網路安全風險評估活動時序如下圖 3-1 所示。



圖 3-1、歐盟 5G 網路安全風險評估活動

資料來源：本團隊整理

國家層級的 5G 網路安全風險評估應包括以下概述 [64]：(1)影響 5G 網路的主要威脅和行動者、(2)5G 網路元件和功能以及其他資產的敏感程度、(3)各種類型的漏洞，包括技術漏洞和其他類型的漏洞；國家層級之風險評估與審查基準須與歐盟層級之評估標準一致，以維持風險評估一致性；風險評估與審查基準措施尤其應加強對供應商與電信業者之資訊提供義務，若設備商不符合國家標準或法律框架，在保護國家安全之前提下，會員國得排除該設備商參與網路建設。

2019 年 10 月 9 日，ENISA 發布《歐盟 5G 網路安全風險評估報告（EU coordinated risk assessment of the cybersecurity of 5G networks）》[65]，該報告提出主要的威脅、敏感的資產、主要的漏洞及其他戰略風險。在風險評估上，所使用的是 ISO/ISC:27005 風險評估方法，其所使用的參數包含有 5G 網路主要威脅類型、主要威脅的來源（者）、主要資產和脆弱性，主要漏洞、風險等情境，各參數說明如下：

(一)5G 網路主要威脅類型

5G 網路的各種威脅情境以機密性、完整性、可用性（CIA）三大類別為主，例如：網路中斷屬於可用性；而各種威脅或威脅的組合則會有其對應的嚴重性，例如：有多少用戶受到影響。

(二)主要威脅的來源（者）

例如：駭客、內部員工。

(三)主要資產

此處的資產並非針對單一設備，而是以能面區分，例如：3GPP 定義的 Core function（核心功能）、Access functions（接取功能），Transport and transmission functions（傳輸功能）、Internetwork exchanges（網路互工互通）、Management systems and supporting services（管理系統與支援服務）等。

(四)脆弱性

此處是說明有關 5G 的技術脆弱性，進而可能影響到的軟硬體，或是某些管理流程上的瑕疵，例如：與第三方服務供應商之前的相關管理制度。

(五)風險情境

由上述參數（1~4 項）之威脅情境與發生機率識別出風險與相關風險情境。

上述風險評估方法主要對應到風險的兩大要素：衝擊（Consequence）與發生機率（Likelihood），也就是威脅情境產生的衝擊與發生機率進而產生風險。

其在主要威脅部分，5G 網路的部署引發的網路安全風險主要增加供應鏈攻擊的風險，與 5G 網路安全相關的威脅場景必須考慮以下幾點：

1. 本地和全球 5G 網路的破壞（對可用性的威脅）。
2. 對 5G 網路基礎設施的流量和數據的監控(對機密性的威脅)。
3. 5G 網路基礎設施流量和數據的修改或選路由（Rerouting）（完整性和機密性的威脅）。
4. 對經過 5G 網路的其他數位基礎設施或訊息系統的破壞或修改（對完整性和機密性的破壞）。

與 5G 網路相關的特定威脅產生影響的嚴重程度是根據以下因素決定的：

1. 受影響的用戶數量和類型。
2. 事件發生後檢測或修復所花費的時間。
3. 受影響的服務類型，破壞和經濟損失的程度和範圍。
4. 訊息洩露的類型。

ENISA 於 2019 年 11 月對外提供 5G 威脅報告《ENISA threat landscape for 5G Networks》 [61]說明 5G 的威脅可從兩個面向來看，第一個從客觀的外部因素來分類各種威脅的類型，第二個是從 5G 系統各元件的脆弱性來分類 5G 的威脅種類。

客觀的外部威脅包含有：

1. 惡意活動、濫用（Nefarious activity, abuse）：此類威脅定義為針對特定 ICT 系統，基礎設施和網路所採取的惡意行為，旨在竊取，變更或破壞指定目標。

2. 竊聽、攔截、劫持（Eavesdropping, Interception, Hijacking）：此威脅定義為未經同意進行竊聽，干擾或控制第三方通信的行為。

3. 物理攻擊（Physical attack）此威脅定義為針對物理資產（例如基礎架構，硬件或互連）進行破壞，暴露，更改，禁用，竊取或未經授權訪問的行為”。

4. 損害（Damage）:此威脅定義為目的在造成財產或人員的破壞，傷害或傷害，並導致使用失敗或降低效率的有意行為。

5. 意外損壞（Unintentional Damage）：此威脅定義為導致財產或人員的破壞，傷害或傷害，並導致使用失敗或降低效率的意外行為。

6. 故障或失效（Failures or malfunctions）：此威脅定義為資產（硬體或軟體）的部分或全部功能不足。

7. 服務中斷（Outages）：此威脅定義為服務意外中斷或品質下降到要求水平以下。

8. 災難（Disaster）：此威脅定義為導致重大損害或生命損失的突然事故或自然災害。

9. 法律（Legal）：此威脅定義為第三方（基於合同的或其他方式）使用法律手段停止訴訟或賠償的損失。

從 5G 系統各元件的脆弱性來分類 5G 的威脅種類則包含如下：

1. 核心網路威脅：這些威脅與包括 SDN，NFV，NS 和 MANO（Management and Orchestration，管理與協調）在內的核心網路元素有關。大多數屬於「惡意活動、濫用」和「竊聽、攔截、劫持」類別。

2. 接入網路威脅：這些威脅與 5G 無線接取技術（RAT），無線接取網路（RAN）和非 3GPP 接取技術有關。其中包括與無線媒體和無線傳輸技術有關的威脅。大多數威脅屬於「竊聽、攔截、劫持」類別。

3. 多邊緣計算威脅：這些威脅與位於網路邊緣的組件有關。大多數屬於「惡意活動、濫用」和「竊聽、攔截、劫持」類別。

4. 虛擬化威脅：這些威脅與 IT 基礎架構，網路和功能的虛擬化有關。

5. 物理基礎架構威脅:這些威脅與支持網路的 IT 基礎架構有關。大多數屬於「物理攻擊」、「設備損壞或丟失」、「設備故障或失效」、「服務中斷」、「災難」類別。

6. 通用威脅：通常會影響任何 ICT 系統或網路的通用威脅很重要，因為有助於定義和構建 5G 專用威脅。例如：許多 5G 特定威脅可能導致網路服務關閉，通常將其定義為拒絕服務（DoS）攻擊的威脅。

7. SDN 威脅：與 SDN 功能相關的威脅，在整個 5G 基礎架構中無處不在。在此以 ENISA 所提及的 SDN 與 5G 威脅為範圍。

歐盟在 5G 安全的行動工作，截至目前已經完成幾項工作，第一，各會員國之國家層級的風險評估，提供問卷以一致性的方式取得各國的現況。第二，由 ENISA 彙整並提供歐盟層級的 5G 威脅態勢報告。

三、德國

德國政府於 2016 年 11 月 9 日發布了新版《德國網路安全戰略（Cybersecurity Strategy for Germany）》 [66]（如下圖 3-2）用以應對越來越多的針對政府機構、關鍵基礎設施、企業以及公民的網路威脅活動，該戰略的發展及實施的主要特點包括：(1)強化關鍵基礎設施防護、(2)重視國內資源有效整合、(3)注重國際網路安全協作。



圖 3-2、德國網路安全戰略

資料來源：BSI、本團隊整理

德國聯邦網路局（Bundesnetzagentur，Federal Network Agency，BNetzA）、德國聯邦資訊安全辦公室（Bundesamt für Sicherheit in der Informationstechnik，Federal Office for Information Security，BSI）於 2019 年 3 月發布《電信網路和服務的附加安全性要求的關鍵要素(Key elements of additional security requirements for telecommunications networks)》 [67]，該草案係德國聯邦網路局電信通訊法第 109 條第 6 項規定，與聯邦資訊安全辦公室（BSI）和德國聯邦資料保護與資訊

自由委員會（Bundesbeauftragter für den Datenschutz und die Informationsfreiheit，Federal Commissioner for Data Protection and Freedom of Information，BfDI）達成協議後制定，並由德國聯邦網路局發布之，適用於德國 5G 網路的發展，5G 網路技術係為未來核心關鍵基礎設施，為提升技術發展之安全性，電信網路公司必須滿足相關安全要求，鑑於 5G 對未來競爭力極具重要性 [68]，故用於構建 5G 之技術必須符合最高安全標準，且應盡可能排除安全問題，該標準同樣適用於所使用的硬體和軟體，附加的安全目錄要點基本內容如下：

(一)系統僅允許從嚴格遵守國家安全法規及電信保密和隱私法規，且值得信賴之供應商處獲得。

(二)必須定期且持續監控網路流量異常情況，如有疑問，應採取適當的保護措施。

(三)僅可使用經聯邦資訊安全辦公室對其 IT 安全性檢查核可且取得認證之安全相關的網路和系統元件（以下簡稱關鍵核心元件）。關鍵核心元件僅能從獲得信賴保證之供應商/製造商中取得。

(四)安全相關的關鍵核心元件應在交付期間進行適當之驗收測試後方能使用，且須定期和持續進行安全檢查。關鍵核心元件之定義將由德國聯邦網路局和聯邦資訊安全辦公室共同協議訂定。

(五)在安全相關領域，只能聘用經過培訓之專業人員。

(六)電信網路業者須證明所使用的產品中，實際使用經測試合格之安全相關元件硬體和供應鏈末端的原始碼。

(七)在規劃和建立網路時，應使用來自不同製造商的網路和系統元件，以避免類似「單一文化」（Monokulturen，Monoculture），

即避免技術生態圈無法均衡發展，以及易受市場波動影響之不良效應。

(八)外包與安全相關勞務時，僅可考慮有能力，可靠且值得信賴的承包商。

(九)對於關鍵且與安全相關的關鍵核心元件，必須提供足夠的備用元件（Redundanzen，Redundancy）。

此外，該草案亦指出電信商在採購 5G 相關設備時須向值得信賴、遵守國家安全規範及電信保密條款之供應商採購，且涉及網路安全之核心元件（如密碼模組）須經 BSI 認證之實驗室測試後始可安裝，通過定期測試後方能使用。另外，要求德國電信業者須分散設備的採購來源、避免過度依賴單一供應商，並僅允許經培訓的專業人員在安全相關領域工作且持續監控網路流量的異常情況，並採取適當的因應措施。電信商若想外包此類工作，則須選擇專業能力強、可靠且值得信賴的承包商。BNetzA 會根據當前安全形勢和技術發展定期修訂安全要求，這些要求將適用於所有網路，而不僅侷限於 5G 網路。

鑑於德國已於 3 月中旬拍賣 5G 頻譜，聯邦政府將大力推廣附加要求，並讓相關企業可以清楚瞭解進一步計畫。為確保立法層面之具體要求，聯邦政府計畫將對電信法第 109 條作重大修訂，明確規定操作人員必須證明符合安全規範，並由法律規範相關認證義務，針對關鍵基礎設施中使用的關鍵核心元件應來自可信賴之供應商/製造商，應適用於整體供應鏈。此外，德國聯邦政府擬針對聯邦資訊安全辦公室法進行修訂，包括關鍵基礎設施、其元件可信賴性之相關規範。依聯邦資訊安全辦公室法第 9 條規定，將在認證框架內提供可信賴性證明。

四、英國

2016 年 10 月成立英國國家網路安全中心(National Cyber Security Centre，NCSC)，與英國數位、文化、媒體暨體育部（Department for Digital, Culture, Media and Sport，DCMS）以及英國通訊管理局（Office of Communications，Ofcom）合作，提供英國網路安全能力及實用指南，其四大主要目標是：(1)降低英國的網路安全風險；(2)有效應對網路事件並減少損失；(3)瞭解網路安全環境、共享資訊並解決系統漏洞；(4)增強英國網路安全能力，並在重要國家網路安全問題上提供指導。NCSC 為 5G 網路在英國將會帶動機器人產業、製造業、智慧設施、交通運輸、自動車五大領域 [69]，上述五大應用領域的發展前提都必須建立在 5G 網路的安全性上，面對高度複雜的 5G 網路安全，不管是電信商內部或是政府外部規範，甚至是國際組織層級都必須要有更高的網路安全標準來規範 5G 網路，電信網路必須更具強韌性、可靠性、獨立性、機密性，呼籲電信業者須有能力掌控所提供的網路，確實瞭解網路系統裡的每一個部分，落實管理、營運、政策規範，例如第三方供應商之管理、發生資安事件時之處理、通報與應對措施等，且必須確實執行各個網路功能，如用戶驗證、控制策略與落實規範等、管理與加解密數據傳輸，各個網路功能均有其安全價值，缺一不可且必須全數落實才能提供一個安全、可靠的網路環境。

2017 年 3 月 1 日，英國政府發布《2017 英國數位戰略(UK Digital Strategy 2017)》 [70]，該戰略詳細闡述英國脫歐後將如何打造世界一流的數位經濟，並對未來如何推進數位轉型做出全面的部署，主要包括(1)連接戰略：打造世界一流的網路基礎設施、(2)數位技能與包容性戰略：使全民掌握所需的數位化技能、(3)數位經濟戰略：讓英國成為數位化業務發展的絕佳之地、(4)數位轉型戰略：幫助英國企業順利實

現數位化轉型、(5)網路空間戰略：提供全球最安全的網路空間環境、(6)數位政府戰略：提升英國電子政務的全球領先地位和(7)數據經濟戰略：釋放數據的經濟潛能等七大戰略。

其中提供全球最安全的網路空間環境，將繼續與國際夥伴保持合作，增強網路安全能力，共同維護一個自由、開放且安全的網際網路空間外，英國還將竭盡所能支持各組織和個人的網路安全，並確保兒童與青少年免受網路風險的影響。為此，英國將努力達成以下目標：

1. 防禦：具備相應的手段來抵禦不斷變化的網路威脅，具備應對網路惡意事件的工具。
2. 震懾：探測、調查並阻止針對國家和公民的敵對行動，對攻擊者進行起訴。
3. 發展：不斷發展和創新型網路安全產業，利用先進的分析能力和專業技術亦將使英國能夠應對並克服未來的威脅和挑戰。

2017 年 3 月，英國數位、文化、媒體暨體育部（Department for Digital, Culture, Media and Sport，DCMS）和財政部聯合發布《下一代行動裝置技術：英國 5G 戰略（Next Generation Mobile Technologies: A 5G Strategy for the UK）》 [71]，DCMS 主導通訊傳播服務提供者、消費者及企業對於通傳服務之需求的政策規劃。英國 5G 戰略旨在盡早利用 5G 技術的潛在優勢，塑造服務大眾的世界領先數位經濟，提升英國的領導地位。此戰略就七大關鍵(1)開發 5G 經濟案例（Building the economic case）、(2)實施適當的監管規則（Fit for purpose regulations）、(3)地區-治理及能力（Local areas - governance and capability）、(4)覆蓋範圍與能力 – 匯流與邁向 5G 網路（Coverage and capacity - convergence and the road to 5G）、(5)確保 5G 的安全部署

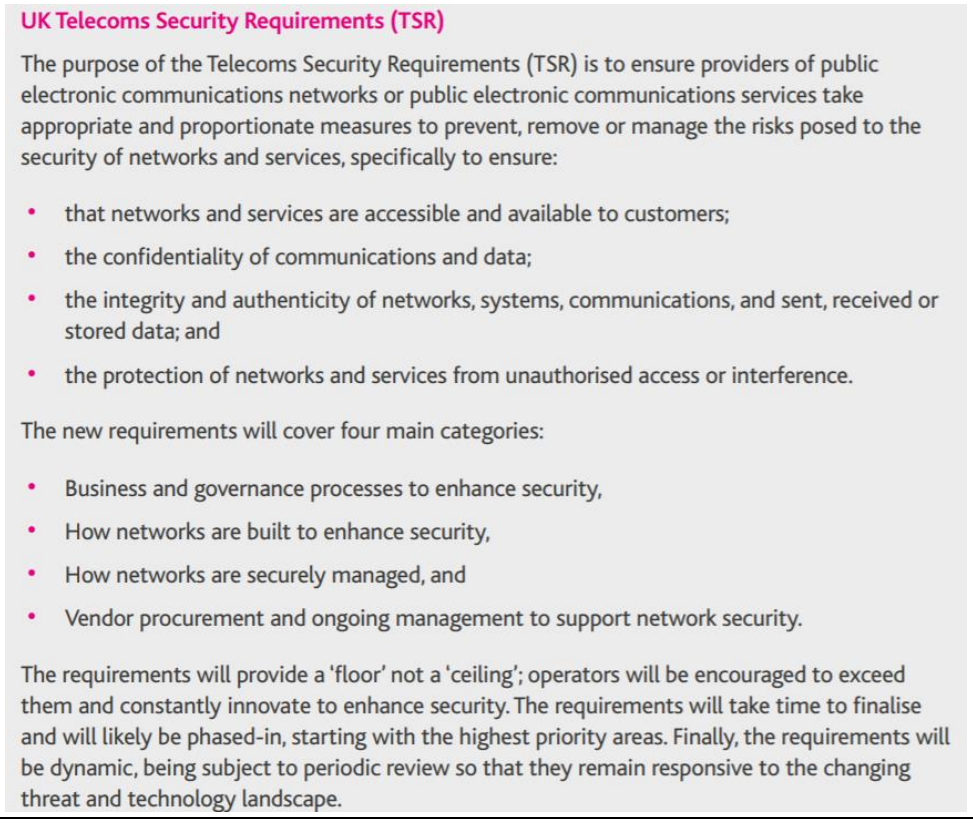
（Ensuring a safe and secure deployment of 5G）、(6)頻譜（Spectrum）、(7)科技與標準（Technology and standards），以上 7 點明述了英國對於 5G 發展應採取的相關作為。

其中確保 5G 的安全部署，係指與 NCSC 等機構聯合開發新的安全架構，以滿足 5G 應用與服務的預期需求；監理及支持 5G 安全技術的開發；協同其他政府機構探索新方式，提高公眾對 5G 機遇與潛力及所帶來的不同應用與服務的認識程度。

2018 年 10 月 DCMS 公布了《英國電信供應鏈評估報告（UK Telecoms Supply Chain Review）》 [72]，此評估報告係 DCMS 對電信供應鏈進行審查，對英國電信網路的供應布局進行全面評估，並於 2018 年 10 月提出第一版，2019 年 7 月提出最新版，在評估過程中，DCMS 與產業界、國際合作夥伴和 NCSC 密切合作，以確保評估結果有專家的技術建議支持，並能夠全面瞭解英國的市場狀況，評估的主要觀點為：(1)全光纖網路是促進英國繁榮的關鍵技術、(2)5G 和全光纖網路面臨安全挑戰、(3)整個行業缺乏將安全風險控制到適當水平的管理機制、(4)國家可依賴的供應商較少，因此 DCMS 認為在現有基礎上為 5G 和全光纖網路必須建立一個新的、更強大的安全框架，確保電信業者建構和營運安全的網路，並相應管理其供應鏈，如評估供應商對網路安全所構成的風險、採取管控措施來降低風險、定期審查新的安全框架，並在相關威脅、風險和技術發生變化時進行更新，最後評估報告提供了以下建議：(1)建立健全電信安全立法框架、(2)管控供應商帶來的安全風險、(3)制定新的電信安全要求（Telecoms Security Requirements，TSR）（如下圖 3-3），這項要求由英國通訊管理局（Office of Communications，Ofcom）與政府監管的電信業者共同實施網路設

計和管理工作，旨在確保網路業者採取適當的方法來避免、排除、管理網路服務安全風險。

(一)電信安全要求（Telecoms Security Requirements）



UK Telecoms Security Requirements (TSR)

The purpose of the Telecoms Security Requirements (TSR) is to ensure providers of public electronic communications networks or public electronic communications services take appropriate and proportionate measures to prevent, remove or manage the risks posed to the security of networks and services, specifically to ensure:

- that networks and services are accessible and available to customers;
- the confidentiality of communications and data;
- the integrity and authenticity of networks, systems, communications, and sent, received or stored data; and
- the protection of networks and services from unauthorised access or interference.

The new requirements will cover four main categories:

- Business and governance processes to enhance security,
- How networks are built to enhance security,
- How networks are securely managed, and
- Vendor procurement and ongoing management to support network security.

The requirements will provide a 'floor' not a 'ceiling'; operators will be encouraged to exceed them and constantly innovate to enhance security. The requirements will take time to finalise and will likely be phased-in, starting with the highest priority areas. Finally, the requirements will be dynamic, being subject to periodic review so that they remain responsive to the changing threat and technology landscape.

圖 3-3、UK 電信安全要求

資料來源：Telecoms Supply Chain Review

TSR（如上圖 3-3）將從業務和管理流程、網路構建、網路管理以及對供應商採購進行持續監管，以確保英國 FTTP（Fiber to the X）寬頻與 5G 網路免於威脅，並透過立法，賦予 Ofcom 更大的權力，以使 TSR 能夠得以有效執行，TSR 目標在於：

1. 提升網路和服務可供用戶接取和使用。
2. 提升通信和數據的機密性。

3. 提升網路、系統、通信以及發送、接收或存儲數據的完整性和真實性。

4. 提升網路和服務免受未經授權的接取或干擾。

TSR 將涵蓋以下四個面向(1)業務和治理流程以增強安全性、(2)如何建造一個高度安全的網路、(3)如何安全地管理網路、(4)如何在供應商採購與外部管理中取得網路安全。TSR 僅提供基準而非門檻，電信業者應盡可能地超越這份要求中所述之基準。

為防範供應商造成的資安風險，TSR 將：(1)要求電信業者藉由採購及合約管理對設備商進行嚴格監督、(2)在政府支援下，電信業者必須與設備商密切合作，確保設備、系統與軟體安全測試，並支援現行驗證協議、(3)針對現行造成英國資安疑慮之設備商實施額外管控，其中第二點「確保設備、系統與軟體安全測試，並支援現行驗證協議」，NCSC 特別指出電信商需要嚴格要求、監督、查驗設備供應商之設備驗證，因大部分設備商只會通過基本的通用規範（如 3GPP SCAS、GSMA NESAS、ISO 27001 等），而除了通過這些共通規範，電信商必須要特別考量到英國通訊網路系統之安全現況，以要求設備供應商提供更符合英國本土安全之設備。

英國政府於 2019 年 8 月日推出第三輪《網路技術即時作用基金（Cyber Skills Immediate Impact Fund，CSIIF）》 [73]，目的在增進英國國家網路安全產業之多元性發展，培訓業者可透過競標網路安全培訓計畫與企業雇主合作，從中培訓網路安全領域人才，並阻止技能落差持續擴大，以吸引更廣泛的人才從事網路安全工作。

五、 澳洲

2017 年 10 月發佈《5G – 啟動未來經濟（5G - Enabling the future economy）》 [74]，提出政府為支持 5G 發展而正在實施的 4 項即刻行動：(1)立即提供頻譜、(2)積極參與國際頻譜協調活動、(3)簡化相關程序，使行動網路電信業者能夠更快地部署基礎設施、(4)審查現有的監管方式，以確保其適用性。

2018 年 6 月 29 日澳洲通過《國家安全法修正案(National Security Legislation Amendment - Espionage And Foreign Interference)》 [75]，將可能損害澳洲國家安全關鍵基礎設施損害行為納入犯罪並強化資訊保密義務。

2018 年 8 月，發布《政府提供之 5G 安全指南予澳洲電信業者（Government provides 5G security guidance to Australian carriers）》 [76]，這項指南中特別針對 5G 網路設備供應商提出聲明，政府必須確認 5G 的完整性、機密性與可用性，並引出《電信部門安全改革法（Telecommunications Sectors Security Reforms，TSSR）》 [37]來規範所有電信業者與表明正與對於供應鏈風險的重視。這項指南中提到行動通訊網路可被分為「核心」網路和「邊緣」網路兩部分。核心網路負責一些敏感的功能，包括接取控制、身份驗證、語音與資料傳輸和計費功能等；邊緣網路主要由無線設備組成，用於將手機等終端設備連接到核心網路。過去的行動通訊網路系統中，核心與邊緣網路根據上述內容而分工明確，然而 5G 通過物理和邏輯功能分離化設計，使過去在核心網執行的敏感功能逐漸轉移到網路邊緣，如此一來，隨著網路發展和演進，核心與邊緣之間的功能劃分將逐漸消失，由於原本由核心網負責的「敏感功能」脫離了受到高度保護的核心環境，因此，這一網路構架的轉變為安全性帶來了新的挑戰，政府目前找出針對此

安全風險的一套減緩方案，然而在面對 5G 網路發展所伴隨的高度多樣性與複雜性安全風險，政府必須盡可能地保護行動網路的安全。澳洲政府期盼利用針對 5G 網路第三方供應商之 TSSR 來規範 5G 網路設備供應商與第三方服務之風險，澳洲政府考量到各國供應商或第三方服務之規範並不一致，因此極有可能會與澳洲法律相抵觸，進而造成澳洲電信網路被未經授權的接取或攔截等，TSSR 適用於所有在澳洲的電信業者，無論電信業者選擇哪一家供應商，他們仍應該做好管理機制，這項管理機制並不會取代現有的網路安全施行方針或是業務風險降低措施，政府已經做與業者合作共同打擊網路安全風險的準備。

2018 年 9 月 18 日生效之 TSSR [37]目的是加強管理澳洲電信網路的國家安全風險的框架，要求該國電信業者須採取相關合理、必要之行動，以保護電信網路避免遭受國家安全風險之威脅，以下敘述此法的關鍵四要素：

(一)履行安全性之義務

所有電信業者、服務提供商、系統業者等都必須盡力保護所提供的網路、設施以避免未授權的接取、攔截等，上述各營運相關業者必須善盡對於電信網路以及設施之「監督」責任以及有效「管理」。

(二)履行向政府報備之義務

電信業者與被指名的服務提供商如有預計改變其系統與服務之安全計畫，都必須遵守政府規範向政府報備。

(三)情資獲取之權力

內務事務部次長（Department of Home Affairs）具有從各電信業者、服務提供商、系統業者等取得相關情資與文件之權力，以有效監督、查核各營運業者是否有符合政府所規定之安全規範。

(四)指示之權力

內務事務部部長具有指示各電信業者、服務提供商、系統業者等該執行或不該執行任何特定之為保護涉及國安風險之網路與設施的安全相關事務。

六、日本

日本在分配 5G 頻譜給電信業者時，將評估電信業者的供應鏈風險，包括產品評估、供應鏈調查、關鍵零元件與所有硬體及軟體等，同時亦須考量對國家安全之影響。

日本國家資訊安全中心（内閣サイバーセキュリティセンター，National Information Security Center，NISC）制定政府規範之採購注意事項指引，如選擇個人電腦、伺服器和手機等通信設備的供應商判斷標準。在 2018 年 12 月 10 日召開制定《政府機構通信設備採購指引（Agreement on IT procurement policy and procedures for goods and services）》 [77]，確認新指引內容須確保《日本政府機構的網路安全 Common Standards for Information Security Measures for Government Agencies）》 [78]的要求，並在 2019 年內開始實施，日本政府表示，「不採購被植入竊取、破壞資訊和令資訊系統停止等惡意功能的設備是極其重要的」，因此，日本政府單位已表明將這類具有網路安全隱患的機器和在線服務排除出 5G 採購清單。

日本總務省在 5G 資安要求則是評估電信業者的供應鏈風險，包括產品評估、供應鏈調查、關鍵零元件與所有硬體及軟體等，同時亦須考量對國家安全之影響。

日本總務省 2019 年 10 日核准 NTT DoCoMo、KDDI、軟體銀行（SoftBank）和樂天（Rakuten）四家電信業者提出的 5G 營運申請案，將頻段分配給這 4 家公司，出於安全方面的考量，在審查條件第四項（如下圖 3-4）特別要求業者採取適當的網路安全措施，包括供應鏈的風險措施。



日本全國性5G頻譜釋照絕對審查基準

類別	編號	基準
區域擴展	1	核准後5年內，必須在全國及各地區配置5G高度特定基地臺，使5G基礎整備率達50%以上。
	2	核准後2年內，所有都道府縣必須啟用5G高度特定基地臺。
設備	3	具有確保基地臺設置場所、設備籌措以及確保設置工程體制之相關計畫。
	4	具有確保運用基地臺必要之電信設備安全、信賴措施之相關計畫。
財務	5	具有投資設備等必要資金籌措計畫以及核准有效期間（5年內）在期滿之前達成單年度盈利之計畫。
法遵	6	具有遵守法令、個人資料保護和使用者利益保護（包含廣告時的通訊速度以及服務地區表示等）相關措施以及實施措施的體制整備計畫。
服務	7	具有針對無行動電話執照者（如MVNO）提供電信服務或者電信設備接續方法以促進基地臺利用之計畫（本計畫的實績將作為將來指配的審查對象）。
	8	關於欲提供之服務，具有因應使用者通訊量需求、多樣資費設定之計畫。
干擾措施	9	採取防止對既有執照者所開設之無線電臺訊號干擾或其他妨害之具體措施。
其他	10	無同一集團的複數申請。
	11	接受指配的業者不讓渡給既有行動通訊業者。

圖 3-4、5G 申請審查基準概要

資料來源：總合通信基盤局、臺灣經濟研究院、本團隊整理

除此之外，日本總務省亦規範頻譜得標者在設置 5G 網路系統時所應該遵守之附加條件（如下圖 3-5），其中特別關注電信業者在建置 5G 系統時應盡可能地擴展其服務範圍，將 5G 的特性帶入無訊號的區域，使得全國用戶都可以享受 5G 所帶來的便利性，還有應考量到緊急災害所導致的停電情況下通訊系統不得運作之風險，應積極防止通訊設備因電力系統而不得運作，強化電力系統以提高通訊設備的強韌性。

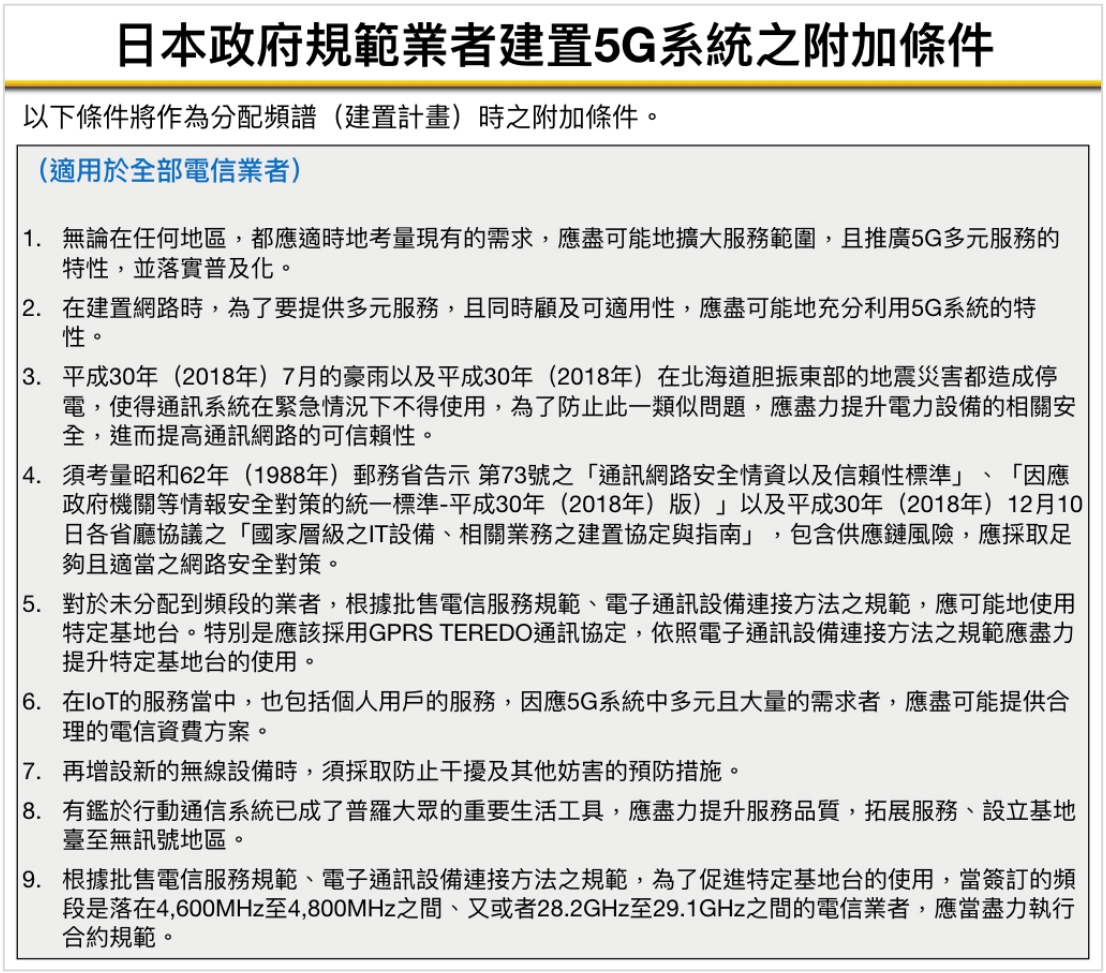


圖 3-5、5G 系統建置之附加條件

資料來源：總合通信基盤局、本團隊整理

七、 南韓

南韓已於 2018 年成立「5G 安全與技術諮詢委員會」，由電子通信研究院（한국전자통신연구원，Electronics and Telecommunications Research Institute，ETRI）、國家保安技術研究所（국가보안기술연구소，National Security Research Institute，NSRI）、南韓網路振興院（한국인터넷진흥원，Korea Internet and Security Agency，KISA）、科學技術資訊通信部（과학기술정보통신부，Ministry of Science and ICT，MSIT）等 20 名代表組成，提供南韓三大電信業者 5G 設備功能的安全檢查與稽核，及相關技術支援與諮詢，以提升 5G 網路安全；目前正在制訂 5G 基礎設施風險管理指南及資訊安全管理系統。

南韓 5G 網路於 2019 年 4 月 3 日正式商轉，南韓總統文在寅（문재인）於 2019 年 4 月 8 日之 5G 服務商轉儀式上宣布了《5G＋戰略》，計畫到 2026 年，培育 15 個以 5G 為基礎的戰略產業；《5G+戰略》包括 5 個核心服務和 10 個核心行業（如下表 3-2）。

表 3-2、南韓「5G +戰略」

5 個核心服務	10 個核心行業
1. 沉浸式內容	1. 次世代智慧型手機
2. 智慧工廠	2. 網路設備
3. 無人駕駛車	3. AR、VR 設備
4. 智慧城市	4. 穿戴式裝置
5. 數位醫療保健	5. 智慧型 CCTV
	6. 未來型無人機
	7. 連網機器人
	8. 5G V2X
	9. 資訊安全
	10. 邊緣運算

資料來源：國家實驗研究院科技產業資訊室

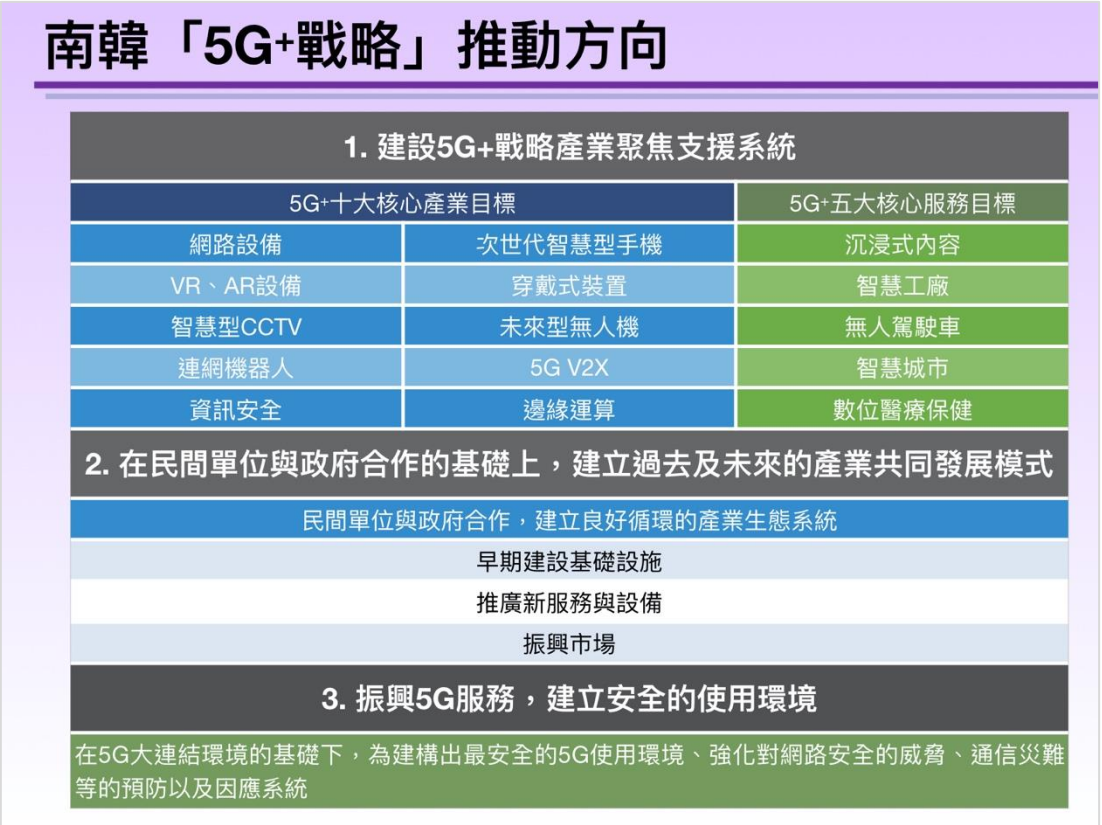


圖 3-6、南韓「5G+戰略」推動方向

資料來源：南韓中央行政機關，臺灣經濟研究院整理

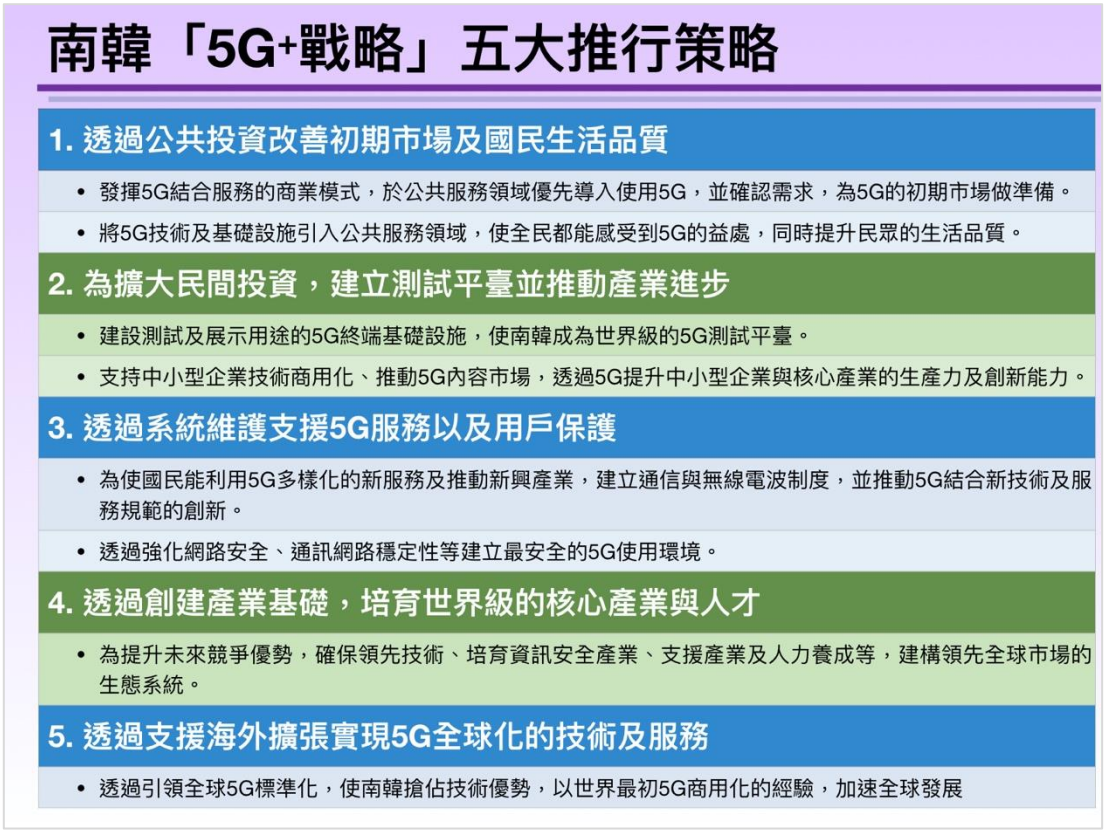


圖 3-7、南韓「5G+戰略」推行策略

資料來源：南韓中央行政機關、臺經院整理

為促進對 5G 服務和行業的投資，南韓政府計畫放寬對 5G 業務的監管，並修訂《位置資訊法（Location Information Act）》 [79]，以減少使用位置資訊進入 5G 融合服務的障礙；南韓政府也計畫修改法律，在法律基礎下，提升 5G 與物聯網的設備與服務之安全。

八、中國

2019 年 6 月 6 日，中國工業和信息化部（Ministry of Industry and Information Technology，MIIT，工信部）正式發布 5G 牌照 [80]，中國移動、中國電信、中國聯通及中國廣播電視網路有限公司均獲發牌照，正式進入 5G 通信時代，啟動了 6 GHz 以下的中頻段部署，中國移動獲得 2.6GHz 和 4.8GHz 頻段，而中國電信和中國聯通獲得 3.6 GHz 頻段。5G 牌照發放彰顯中國政府對於全力推進 5G 產業發展的決心，事實上，在 5G 牌照發放之前，中國三大電信業者自 2017 年已經廣泛開展了 5G 大規模試驗，中國積極聯合國內外眾多企業積極開展 5G 技術試驗，如中國電信已開通 SA 與 NSA 混合組網跨省跨域規模試驗網，並在北京、上海、廣州、深圳等 17 個城市開展 5G 創新示範試點，探索新的應用場景和新的商業模式。

中國目前並無專門針對 5G 發佈專有的監管規定，現在所知之消息都屬只聞其聲，不見其人，例如工信部表示後續應當加快 5G 安全領域關鍵核心技術研發，建立健全 5G 安全風險態勢感知和預警處置機制，統籌做好 5G 網路設施安全、應用系統安全、數據安全等工作，才能全面提升 5G 安全保障水準，提升 5G 在各行業領域應用安全。為此，工信部將從四個方面體系化推進網路安全各項工作：

(一)完善政策法規

全面落實《網絡安全法》，強化網路基礎設施保護和數據安全管理，制定出臺《加強工業網際網絡安全工作的指導意見》。

(二)健全安全監管機制

統籌營運安全評估，風險通報等監管手段，加大網路安全防護檢查和威脅治理力度，構建起涵蓋事前、事中、事後的閉環監管體

系，注重協同聯動和資訊共享。與中央網信辦、公安部等聯合開展《關於縱深推進防範打擊通訊信息詐騙工作》，營造晴朗的網路空間。

(三)強化網路安全技術保障

加快推進網路安全態勢感知、威脅資訊共享、應急管理等技術手段的建設，提升行業的網路安全手段建設水平和保障能力。

(四)推進網路安全產業的發展

支持國家網路安全產業園區的建設，推動建立北京國家網路安全產業園區，同步推進國家園區的整體佈局，促進網路安全產業發展，深化網路安全。深入實施工業網際網路創新發展工程，支持產業鏈互相競爭提高多樣性影應對高複雜度的網路安全。

雖然中國並無針對 5G 制定專用資安監管規定，但是本計畫認為這並不是中國忽視資安的重要性，而是中國早以資安為由，在各方面已經制定專門的法規，緊緊地抓住與監控網際網路空間，監管和法制力度可能是世界之最。

具體的表現在於 2017 年的《中華人民共和國網絡安全法》，引述其條文如下：

(一)「第二十四條 網路運營者為用戶辦理網路接入、域名註冊服務，辦理固定電話、移動電話等入網手續，或者為用戶提供信息發布、即時通訊等服務，在與用戶簽訂協議或者確認提供服務時，應當要求用戶提供真實身份信息。用戶不提供真實身份信息的，網路運營者不得為其提供相關服務」：該法確立了網路實名化的原則。

(二)「第二十八條 網路運營者應當為公安機關、國家安全機關依法維護國家安全和偵查犯罪的活動提供技術支持和協助」：該法為加強網路管制的國安治安單位提供了強有力的工具。

(三)「第三十五條 關鍵信息基礎設施的運營者採購網路產品和服務，可能影響國家安全的，應當通過國家網信部門會同國務院有關部門組織的國家安全審查。」：該法亦有以國安角度對產品進行安全審查之規範。

再來談論對於電信業的監管作為，由於中國在加入世界貿易組織時，並不承諾開放電信服務業，是以目前中國的電信事業的經營，不論是第一類還是第二類業者皆需申請執照，在這個部份中國設立了非常明確的市場進入原則，以嚴格限制潛在設備商的進入，例如外資不許投資或限制在 49%內，同時在電信業務的經營上也賦與相當大的義務，若不配合政府執行，會不許其繼續經營業務。這類義務類別相當龐雜，例如經營者需通過四項技術評測要求，包括：機房運行安全測評、接入資源系統測評、網站備案系統測評和資訊安全管理系統測評。

在此節錄依其《電信業務經營許可管理辦法》下的一份行政命令《關於進一步規範因特網數據中心（Internet Data Center，IDC，網際網路數據中心）業務和因特網接入服務（Internet Service Provider，ISP，網際網路服務供應商）業務市場准入工作的實施方案》，其要求與規範十分細緻：

(一)有與開展經營活動相適應的資金和專業人員，申請 IDC 和 ISP 業務的企業，註冊資本應符合有關規定

申請 IDC 和 ISP 業務的企業，需建立網路和資訊安全專人專崗制度，配備與本企業接入網站數量相匹配的網路和資訊安全管理人

員。企業要明確 2 名應急聯繫人，負責 7 天 24 小時全年無休應急聯繫處置工作，每接入 1 萬個網站至少配備 2 名專職網路和資訊安全工作人員，並根據需要配備必要的技術、管理、客戶服務等工作人員。建立相應的客戶服務部門，配備專職投訴處理人員，設置用戶投訴處理公開服務熱線。

(二)有必要的場地、設施及技術方案

1. 申請經營 IDC 業務的企業，應利用自有或租用的機房和場地，以外包出租的方式為用戶的伺服器等網際網路相關設備提供放置、代理維護、系統配置及管理服務，以及提供數據庫系統或伺服器等設備的出租以及存儲空間的出租、通信線路和出口頻寬的代理租用和其他應用服務。機房要滿足《通信機樓消防安全監督管理辦法》（工信部電管〔2010〕543 號）和《通信網路供電系統運行安全監督管理辦法》（工信部電管〔2010〕563 號）的相關規定；所使用的交換和路由設備應取得電信設備進網許可證。其中 IDC 機房包括 UPS、發電設備、冷卻系統、機櫃等設備。IDC 機房和場地的證明材料包括：房產證或者租用合同、機房設計文檔、監理報告、機房施工文檔等。

2. 申請 IDC 和 ISP 業務的企業，應建設獨立並具有以下功能的 IDC 和 ISP 企業資源和業務管理系統。

   A. 建設企業端網際網路網站備案管理系統，記錄並及時變更所接入網站的主體資訊、聯繫方式和接入資訊等，並實現與部、省網站備案管理系統的連接。

B. 建設企業接入資源管理平臺，記錄接入資源的分配、使用、出租、轉讓等資訊，對接入資源異常使用實行日常發現、分析和處置，並實現與部電信業務市場綜合管理系統的連接。

C. 提供虛擬主機（存儲空間出租等）的 IDC 企業要建立相應的製度，對在本企業進行主機託管並提供虛擬主機服務的客戶資訊進行審核和登記，並報電信主管部門。

3. 提供域名註冊服務的 IDC 和 ISP 企業，應按照《中國互聯網域名管理辦法》（信息產業部令第 30 號）的規定，向電信主管部門申請獲得網際網路域名註冊服務機構資質，並嚴格落實域名實名註冊要求，規範域名註冊服務行為。

4. 申請經營 IDC 和 ISP 的企業，應滿足以下安全管理要求，並建設相應的網路和資訊安全管理系統。

A. 網路安全管理要求:按照《通信網路安全防護管理辦法》（工業和信息化部令第 11 號）、《互聯網網路安全信息通報實施辦法》（工信部保[2009]156 號）、《木馬和殭屍網路監測與處置機制》（工信部保[2009]157 號）、《移動互聯網惡意程序監測與處置機制》（工信部保[2011]545 號)的要求,落實通信網路安全防護系列標準,制訂並完善網路安全應急預案，開展應急演練，接受主管部門對各項網路安全工作落實情況的監督檢查。

B. 資訊安全管理要求：按照《中華人民共和國電信條例》和《互聯網信息服務管理辦法》的要求，建立違法網站和違法資訊的巡查與處置、用戶資訊安全管理、資訊安

全評估等管理制度。按照《互聯網數據中心和互聯網接入服務信息安全管理系統技術要求》和《互聯網數據中心和互聯網接入服務信息安全管理系統接口規範》等標準要求，建設 IDC 和 ISP 資訊安全技術管理手段，具備基礎數據管理、接取日誌管理、違法違規網站及違法資訊發現處置等技術能力。

九、 國際布拉格會議之布拉格 5G 資通安全提案

布拉格 5G 安全大會於 2019 年 5 月 2 日於捷克首都布拉格召開為期 2 天的會議，來自全球 32 個國家（包含澳洲、美國、荷蘭、日本、南韓等）的產、官、學、研代表，參與全球 5G 網路部署涉及國家安全、經濟安全、全球利益及穩定發展之關鍵問題的討論。在探討降低 5G 網路通訊基礎設施之發展、部署、營運、維護之網路安全風險中，會議主席提出了以下觀點 [81]：

(一)維持網路安全不僅僅是技術議題

網路安全不能被視為一個純粹技術性的問題，需有合適的國家策略、健全的政策、完善的法律框架以及經過適當教育訓練的從業人員才能建立出一個安全、可靠的網路基礎，公民自由與隱私的背後是需要有良好的網路安全來支持。

(二)起源於技術與非技術面之網路威脅

在處理網路安全威脅時，不僅需要考量到技術層面，還要包括特定的政治、經濟意圖或是試圖利用社會對於通訊技術依賴性的惡意行為。

(三)5G 網路的中斷可能造成嚴重的影響

5G 網路的革新特性將帶來極為廣泛的應用；如智慧交通、智慧工廠、智慧醫療等，如果有未經授權的接取，將會使得大量資訊暴露其中，甚至會破壞整體社會的秩序。

(四)廣及國家層級的應對措施

確保高度網路安全的措施與實行不只是主要企業（如電信業者、技術服務供應商等）的目標與義務，還涵蓋其他領域（如教育、外交、研究發展單位等）的所有利益相關方，這些利益相關方也可能會對於 5G 網路安全有著重大的影響，因此維持通訊基礎設施的網路安全不單單只是經濟與商業議題。

(五)必須要有適當的風險評估

擁有系統性且徹底的風險評估是創造與維護一個真正可靠網路通訊系統的必須要素（包含技術與非技術面的網路安全風險評估）。應制定和部署一套基於風險的安全框架，同時考慮到現有技術政策與減輕安全風險的方法。

(六)安全措施的廣泛性

網路安全措施需具有足夠的廣度來包含整體網路安全風險，例如：人員、過程、實體基礎設施以及營運與策略層面的方法、工具等。

(七)沒有一套通用的解決方案存在

在制定適合的網路安全升級措施當中，各國對於最佳策略的選擇反映出各自不同的考量面向，如社會面、法規面、經濟面、隱私面、技術面以及其他相關的因素等，因此沒有一套通用的解決方案。

(八)在創新、發展的同時應確保安全

革新進步是現代社會發展與經濟成長的主要推手，它也帶來了嶄新的安全解決方案。政策、法律、規範應該允許安全措施具有一定的機動性來管理安全與特定國情之間的互動，透過這種機動性，創新與發展才能被推動。

(九)安全的建置需要成本

達成一個適當且足夠的安全標準往往需要付出更高的代價，然而為了安全考量，這些付出都是值得且必要。

(十)供應鏈安全

維持供應鏈安全是所有利益相關方的責任，網路通訊系統的業者往往會依賴其他供應商的技術，主要的安全風險是來自於 ICT 設備供應商的日益全球化，這增加了跨域的複雜性。應根據相關資訊將供應鏈納入風險考量，並設法防止惡意設備的滲透。

與會中世界各國代表共同提出一項非約束性的政策「布拉格提案」，此提案從政策、技術、經濟、安全、隱私和強韌性之觀點，對 5G 網路資通安全維護提議之結論相關資訊詳述如下。

(一)政策

1. 通訊系統與網路服務必須建立在強韌性與安全性之上，且應以國際開放、基於共識的標準以及網路安全最佳實行做法來設置、維護與營運，此外，各國應共同規範明確的全球可互通性網路安全指南，來維持網路安全的產品與服務，同時提升所有利益相關方之安全能力。

2. 根據國際法，每個國家都有自由制定自己的國家安全規範與執法原則，但前提是必須尊重隱私，並遵守防止資訊不當收集和濫用的相關保護法律。

3. 規範網路和連線服務的法律和政策應遵循透明且公平之原則，同時考慮到全球經濟和可互通性的規則，且各國應尊重法治以充分監督、確實執行。

4. 應考慮到第三國的整體供應商風險之影響，特別是其治理模式；是否缺乏安全合作協議或類似約定（如數據保護）；或者該國是否是網路安全、打擊網路犯罪或資料保護的國際多方、或雙方協議的締約國。

(二)技術

1. 利益相關方應在系統正式運行期間以及產品發布之前，定期在所有元件和網路系統中進行風險減輕與漏洞評估，並且建立搜尋、修復、修補的流程來降低已識別出的漏洞且儘快修復或修補。

2. 供應商的風險評估應考慮所有相關因素，包括適用的法律環境和供應商生態等種種面向，因為這些因素可能會關係到利益相關方為維持最高網路安全標準所付出的努力。

3. 在鞏固網路的強韌性和安全性時，應該注意到惡意的網路活動並不是總是發生在技術漏洞上，例如：內部人員的攻擊。

4. 為了提升全球通訊產業各方的利益，各國應採取相關政策以實現高效率和安全的網路環境。

5. 利益相關方應考慮到 5G 網路推出所伴隨的技術變革，例如：MEC、SDN、NFV 的使用，以及其對通訊傳輸通道整體安全性之影響。

6. 根據現有技術和相關的商業與專業的執行方法；包括產品和服務的維護、更新和修正；無論是用戶、政府、電信業者或是製造商，都必須瞭解那些會影響產品或服務安全的元件和軟體的來源與途徑。

(三)經濟

1. 多樣化且充滿活力的通訊設備市場與供應鏈對於安全和經濟的復甦至關重要。

2. 研發上穩定的投資除了有利於全球經濟和技術的進步，同時也會增加技術解決方案的多樣性，整體對通訊網路的安全有著正面的影響。

3. 應使用採購、投資和承包方面的標準施行原則，來公開透明地為通訊網路和網路服務提供資金。

4. 國家對於 5G 通訊網路和服務提供商的扶持、補貼或融資應該基於公開市場競爭原則，考慮到貿易規範，尊重公平原則，商業上合理，公開透明地進行。

5. 有效監督影響電信網路發展的主要金融和投資手段極其重要。

6. 通訊網路和網路服務提供商應具有透明的所有權、合作夥伴關係和公司治理結構。

(四)安全、隱私和強韌性

1. 包括業界在內的所有利益相關方應共同努力，以促進國家關鍵基礎設施網路、系統和連接設備的安全性和強韌性。

2. 應推動經驗分享以及最佳實行做法；包含從網路攻擊、破解、中斷中來適時地提供減輕、調查、回應、恢復的協助。

3. 供應商和網路技術的安全和風險評估應考慮到法治、安全環境、供應商瀆職行為以及對開放、可互通性、安全標準和業界

最佳實行做法的遵從性，以促進充滿活力和強大的網路安全產品和服務供應進而應對不斷上升的挑戰。

4. 風險管理框架應遵循資料保護原則，以確保使用網路設備和服務的公民的隱私。

第二節 全球主要電信業者針對 5G NSA 網路資通安全相關作為

相較於目前 4G 網路，5G 核心網路根據於軟體定義網路（SDN）與網路功能虛擬化（NFV）等新技術，在架構和功能上提供更開放的接取支援、更靈活的控制和轉傳機制，以及更人性化的能力開放方式，打破了傳統行動網路的封閉性，同時能與雲端化基礎設施結合，為用戶、應用服務商和垂直產業提供網路切片（NS）、多重接取邊緣運算（MEC）等新興之業務能力。5G 網路新技術與新應用服務所帶來便利性之同時，全球也面臨新形式之資通安全防護議題，亟需克服。

5G 網路所面臨的資通安全防護議題概括：實體網路元件轉換為虛擬化軟體元件，物理資源共享，定義模糊之設備安全邊界，開放性接取端變成數據資料洩露之弱點，各式各樣終端之安全防護能力差異極大，因此非常容易成為新的攻擊目標與垂直應用服務場景下安全責任釐清與所屬等問題。

2019 年 5 月由 Business Performance and Innovation （商業表現及發展革新組織，BPI）及應用網路技術領導設備商 A10 Networks 主要以北美及歐洲電信業者為主所作的調查報告《維護未來智慧世界的安全 - 在串連 5G 經濟世界之機會與挑戰（Securing the Future of a Smart World - Opportunities & challenges in a 5G connected economy）》[82]，其中根據一項電信業者預計部署 5G 網路的時程（如下圖 3-8），67%的電信業者將在 18 個月內部署其首個商用 5G 網路，另有 20%的電信業者也將在兩年內完成部署；94%的電信業者預期網路流量、連網設備和任務關鍵型物聯網使用案例的增長，將顯著增加 5G 網路的安全性和可靠性問題；79%的電信業者表示 5G 是當前安全投資決策的一項考慮因素。

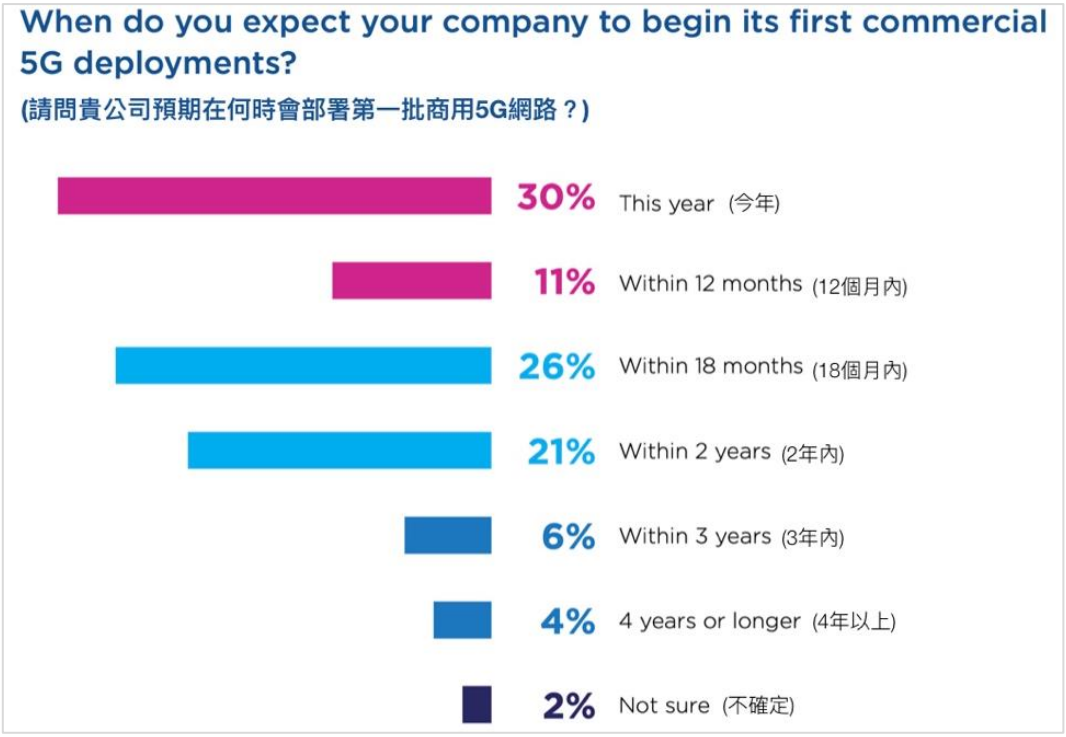


圖 3-8、電信業者預計部署首批 5G 商用網路時程

資料來源：Securing the Future of a Smart World

「貴公司是否將 5G 納入目前安全投資規劃的考慮因素？」（如下圖 3-9）統計為：全球有 79%的受訪者表示已將 5G 納入當前安全投資的考慮因素。

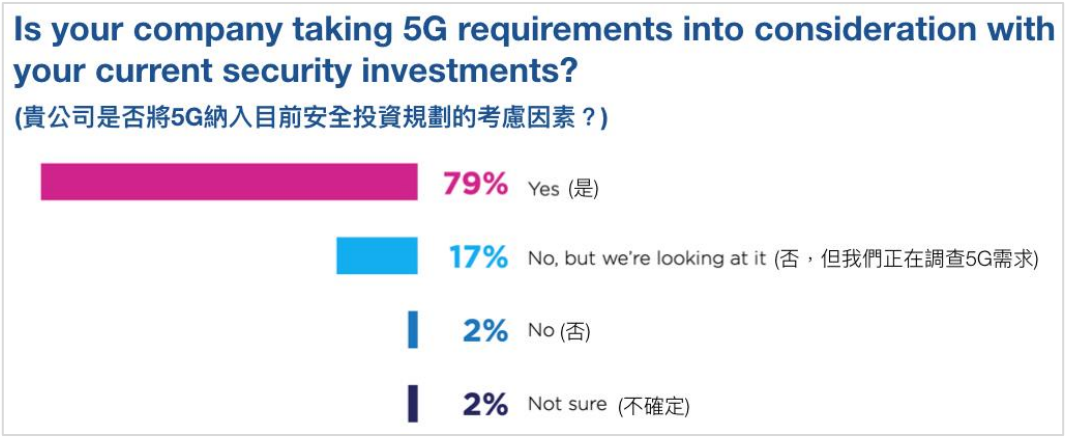
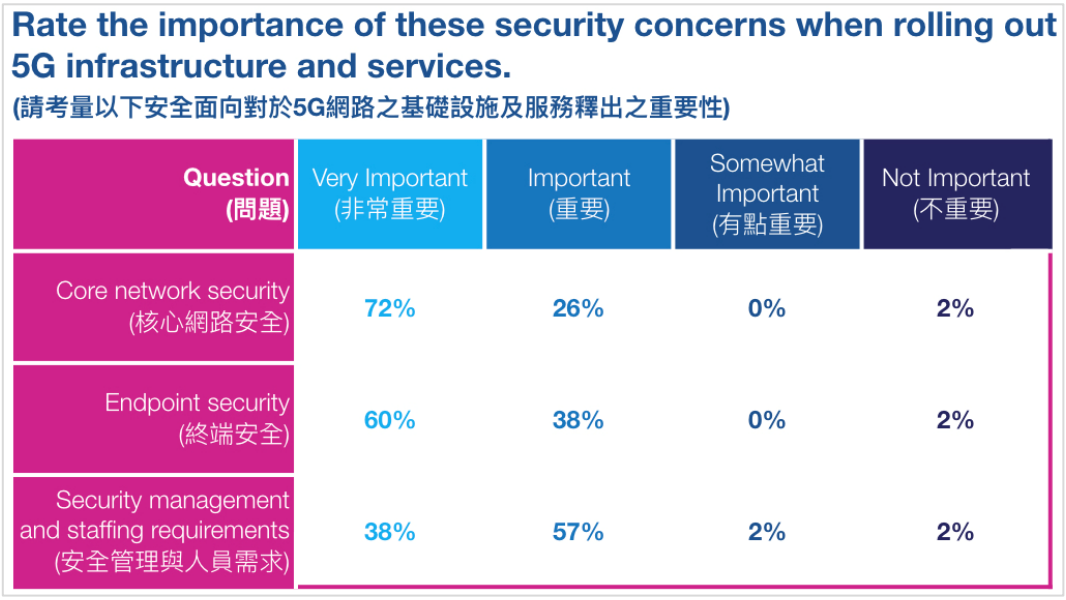


圖 3-9、電信業者 5G 網路安全投資需求

資料來源：Securing the Future of a Smart World

而在 5G 網路基礎設施與服務釋出的重要性評估中（如下圖 3-10），有 98% 的受訪者表示「核心網路安全」在 5G 網路為重要， 其中 72% 非常重要，26%為重要，勝於網路終端安全及安全管理等。



Rate the importance of these security concerns when rolling out 5G infrastructure and services.
(請考量以下安全面向對於5G網路之基礎設施及服務釋出之重要性)

Question (問題)	Very Important (非常重要)	Important (重要)	Somewhat Important (有點重要)	Not Important (不重要)
Core network security (核心網路安全)	72%	26%	0%	2%
Endpoint security (終端安全)	60%	38%	0%	2%
Security management and staffing requirements (安全管理與人員需求)	38%	57%	2%	2%

圖 3-10、電信業者 5G 網路元件之重要性

資料來源：Securing the Future of a Smart World

基於網路訊務量提升和 5G 網路可靠度要求，電信業者對於改善防火牆的態度（如下圖 3-11）約有 79%受訪者打算更新，但實際上在 2019 年 5 月前，僅有 11%完成升級。因此預估電信業者在 2019 年下半年對於防火牆的更新需求將大幅增加，以提供更安全的網路服務；在迎接 5G 到來的路上，仍有大量的工作須完成以鞏固網路。

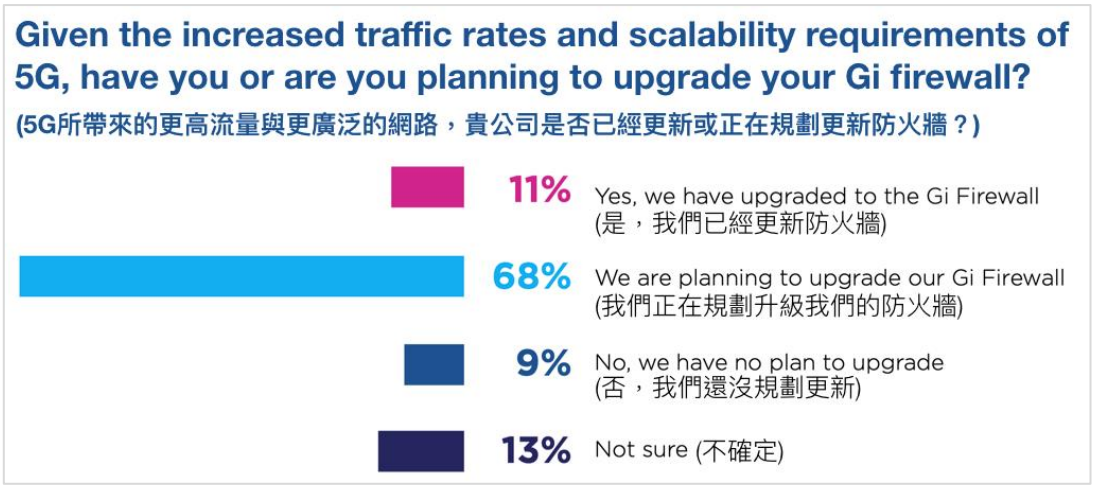


圖 3-11、電信業者對於防火牆的更新需求

資料來源：Securing the Future of a Smart World

調查報告中，亦請電信業者就未來 5G 網路安全部署主要考量面相提供意見（如下圖 3-12），安全問題中最關鍵的便是核心網路安全和 DDoS（Distributed Denial-of-service，分散式阻斷服務）防護，63%的受訪者認為在 5G 網路中，進階 DDoS 防護是最重要且必要的安全功能；其次則為 4G 與 5G 網路的相容性要求。

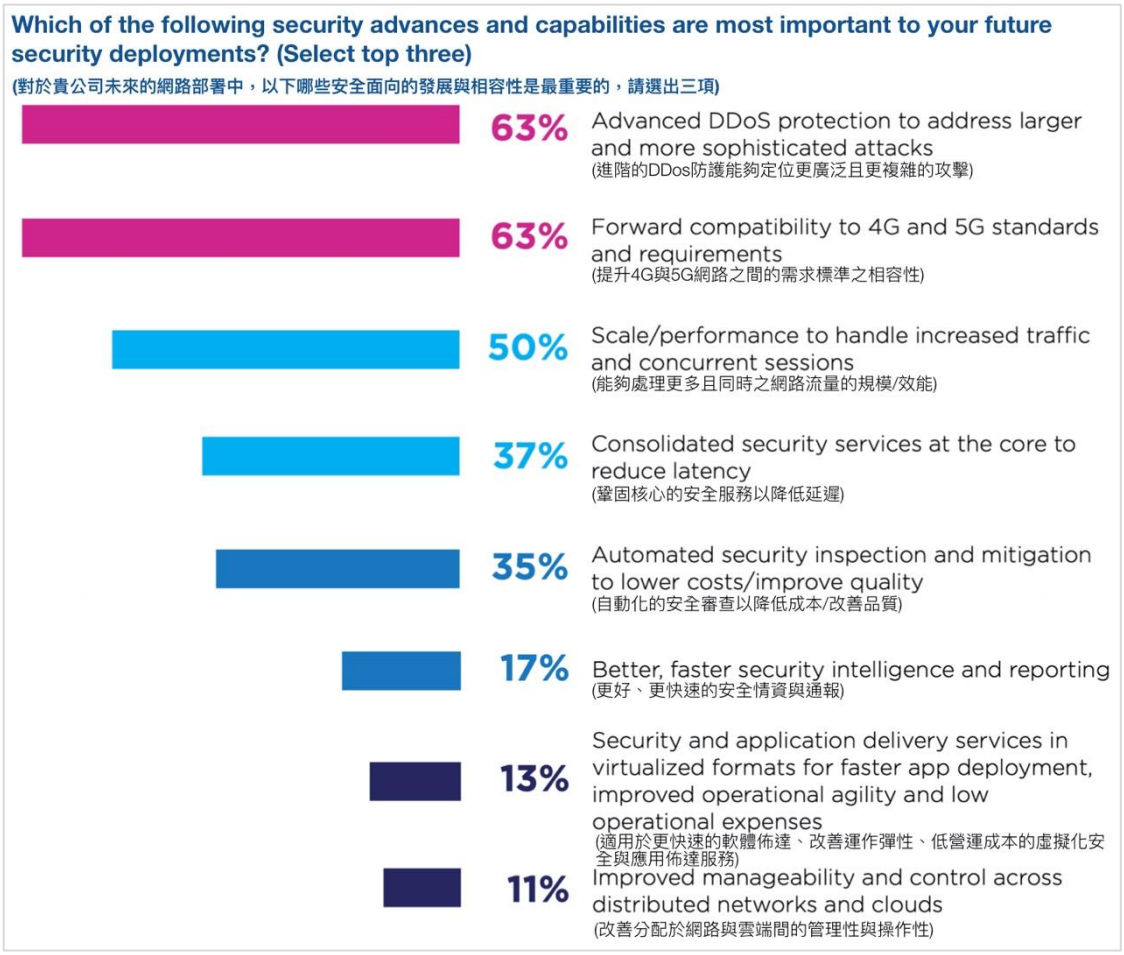


圖 3-12、電信業者對於未來 5G 網路安全部署需求

資料來源：Securing the Future of a Smart World

從調查報告中，得知多數電信業者皆認為 5G 網路的資安很重要，但實際真正有投入人力及資金的業者比例卻不高，但業者普遍相信要完全實現 5G 網路的潛力，必須大幅提高安全性。

本章節針對已商轉或即將商轉之全國各主要國家之電信業者 5G NSA 資安作為或看法進行研析與蒐集，以作為我國後續法規修訂與調整之借鏡，但由於電信業者的資安相關作為涉及商業機密，亦為其資安維護範圍之一部分，故這部分公開的資料較缺乏，本團隊研析與蒐集包含美國、德國、澳洲、日本、南韓五大國家之電信業者相關資料，並進行整理統合。

一、美國

(一) AT&T

美國 AT&T 之資安防護計畫係參考 NIST 所發佈之網路安全參考框架（CSF），AT&T 認為這是一個改善關鍵基礎設施和實體網路安全很好的參考資訊 [83]。AT&T 基於國際安全標準（例如 ISO 27001、SAS No. 70 和 NIST 800-53）已擬定一套內部安全策略 [84] [85]，名為《AT&T 安全政策與要求（AT&T Security Policy and Requirements）》，透過這套策略進行內部網路安全管理及個人數據的保護，此外，AT&T 還擬定了《AT&T 資訊與網路安全客戶參考指南（AT&T Information & Network Security Customer Reference Guide）》[86]，內容闡述 AT&T 對於網路安全的實踐（如下表 3-3）23 項要點，其內容將同樣適用於 5G 網路：

表 3-3、AT&T 資訊與網路安全客戶參考指南

1. 隱私（Privacy）
2. 接取控制（Access Controls）
3. 網路周邊防護（Network Perimeter Protection）
4. 公眾網站保護（Public-facing Website Protection）
5. 入侵檢測（Intrusion Detection）
6. 工作站安全管理（Workstation Security Management）
7. 安全組態檢查及漏洞測試（Security Status Checking and Vulnerability Testing）
8. 風險管理（Risk Management）
9. 安全顧問計畫（Security Advisory Program）
10. 安全事件報告與管理（Security Incident Reporting and Management）
11. 安全合規性審查（Security Compliance Reviews）

12. 內部及外部審查（Internal and External Reviews and Audits）
13. 符合標準及法規（Compliance with Standards and Regulations）
14. 變更管理（Change Management）
15. 業務持續管理（Business Continuity Management）
16. 網路災害復原（Network Disaster Recovery）
17. 管理階層的資安參與度（AT&T Corporate Management Engagement）
18. 持續改進的策略（Strategy of Continuous Improvement）
19. 人員安全（Personnel Security）
20. 安全意識和教育訓練（Security Awareness and Education）
21. 舉辦網路安全會議（AT&T Cyber Security Conference）
22. 舉辦安全執行討論會議（Security Executive Briefings and Roundtables）
23. 安全訓練和認證（Security Training and Certifications）

資料來源：AT&T、本團隊整理

第五代行動通信系統資通安全維護計畫載明 17 項資通安全維護義務之要求(請參考第伍章)，敘明業者所設置之 5G 系統之資通安全防護政策、目標、範圍、措施等之時程、人力與資源配置、流程管理、風險評估及設置等事項，確保得標者所設置的 5G 系統是安全、可信賴的，以保障我國關鍵基礎設施之資通安全及消費者權益，故上述 AT&T 對於網路安全之 23 項說明以及 NIST 所提之網路安全參考框架，可作為國內得標者在撰寫資通安全維護計畫之參考。此外，其中 17 項應載明事項與 AT&T 資訊與網路安全客戶參考指南、網路安全參考框架之對應關係可參考下表 3-4。

表 3-4、資通安全維護計畫應載明事項與 AT&T 資訊與網路安全客戶參考指南、網路安全參考框架之對應

資通安全維護計畫應載明事項	AT&T 資訊與網路安全客戶參考指南	NIST 網路安全參考框架
1. 資通安全政策及目標		• Asset Management (ID.AM) • Business Environment (ID.BE) • Governance (ID.GV)
2. 核心業務及其重要性	15. 業務持續管理	• Asset Management (ID.AM) • Business Environment (ID.BE)
3. 行動寬頻系統資通安全維護範圍	15. 業務持續管理 8.風險管理	• Asset Management (ID.AM)
4. 資通安全組織	17. 管理階層的資安參與度 23. 安全訓練和認證	• Asset Management (ID.AM) • Governance (ID.GV) • Information Protection Processes and Procedures (PR.IP) • Communications (RS.CO)
5. 專責人力及經費之配置	17. 管理階層的資安參與度 23. 安全訓練和認證	• Asset Management (ID.AM) • Governance (ID.GV) • Awareness and Training (PR.AT) • Information Protection Processes and Procedures (PR.IP) • Communications (RS.CO)
6. 資通安全長之配置	17. 管理階層的資安參與度 23. 安全訓練和認證	• Asset Management (ID.AM) • Governance (ID.GV)

資通安全維護計畫應載明事項	AT&T 資訊與網路安全客戶參考指南	NIST 網路安全參考框架
		・ Awareness and Training (PR.AT) ・ Information Protection Processes and Procedures (PR.IP) ・ Communications (RS.CO)
7. 訊及資通系統之盤點規劃(含系統設備符合ITU或3GPP發布之資通安全規定)	8.風險管理	・ Asset Management (ID.AM) ・ Supply Chain Risk Management (ID.SC)
8. 資通安全風險評估	8.風險管理	・ Risk Assessment (ID.RA) ・ Risk Management Strategy (ID.RM) ・ Supply Chain Risk Management (ID.SC)
9. 資通安全防護及控制措施	2.接取控制 3.網路周邊防護 5.入侵檢測 6.工作站安全管理 7.安全組態檢查及漏洞測試 14. 變更管理	・ Risk Assessment (ID.RA) Risk Management Strategy (ID.RM) ・ Identity Management, Authentication and Access Control (PR.AC) ・ Data Security (PR.DS) ・ Information Protection Processes and Procedures (PR.IP) ・ Maintenance (PR.MA) ・ Protective Technology (PR.PT) ・ Security Continuous Monitoring (DE.CM)

資通安全維護計畫應載明事項	AT&T 資訊與網路安全客戶參考指南	NIST 網路安全參考框架
		• Detection Processes (DE.DP)
10. 資通安全事件通報、應變及演練相關機制	10. 安全事件報告與管理 15. 業務持續管理 16. 網路災害復原	• Information Protection Processes and Procedures (PR.IP) • Anomalies and Events (DE.AE) • Security Continuous Monitoring (DE.CM) • Detection Processes (DE.DP) • Response Planning (RS.RP) • Analysis (RS.AN) • Mitigation (RS.MI) • Improvements (RS.IM) • Recovery Planning (RC.RP) • Improvements (RC.IM) • Communications (RC.CO)
11. 資通安全情資之評估及因應機制	9.安全顧問計畫 21. 舉辦網路安全會議 22. 參加安全會議	• Risk Assessment (ID.RA) • Information Protection Processes and Procedures (PR.IP) • Communications (RS.CO)
12. 資通系統或服務委外辦理之管理措施		• Supply Chain Risk Management (ID.SC)
13. 所屬人員辦理業務涉及資通安全事項之考核機制	19. 人員安全 20. 安全意識和教育訓練	• Awareness and Training (PR.AT) • Information Protection Processes and Procedures (PR.IP)

資通安全維護計畫應載明事項	AT&T 資訊與網路安全客戶參考指南	NIST 網路安全參考框架
14. 資通安全維護計畫與實施情形之持續精進及績效管理機制	11. 安全合規性審查 12. 內部及外部審查 13. 符合標準及法規 18. 持續改進的策略	・ Information Protection Processes and Procedures (PR.IP) ・ Improvements (RS.IM) Improvements (RC.IM)
15. 資通安全偵測與防護之建置及執行方案(含資通安全防護架構、防禦縱深及其建置時程)		・ Risk Assessment (ID.RA) Risk Management Strategy (ID.RM) ・ Identity Management, Authentication and Access Control (PR.AC) ・ Data Security (PR.DS) ・ Information Protection Processes and Procedures (PR.IP) ・ Maintenance (PR.MA) ・ Protective Technology (PR.PT) ・ Security Continuous Monitoring (DE.CM) ・ Detection Processes (DE.DP)
16. 執行前述執行方案所蒐集、儲存、處理及利用用戶資料之安全保護措施	1.隱私 4.公眾網站保護	・ Data Security (PR.DS)
17. 通過資通安全管理驗證之執行方案	11. 安全合規性審查 12. 內部及外部審查 13. 符合標準及法規 18. 持續改進的策略	

資料來源：本團隊整理

(二)Verizon

Verizon 於 2019 年 4 月宣布 5G 行動服務上市 [87]，成為美國第一家商用 5G 行動服務的電信業者。其認為在 5G 網路開發的過程中需要注意到很多面向，像是商業利益、可靠性、效能、安全性等，在這所有的面向中 Verizon 總是以「安全性」為第一考量。在設備商的選擇中，Verizon 只跟可信賴且長期經營的設備商購買相關元件 [88]，且更會要求設備商為每一個的元件提供品質與安全性的保證，再由 Verizon 實際連上網路測試這些產品，且對於世界各國的設備商都秉持此一標準，另外，針對中國設備商之疑慮，美國政府發布法令規定在美國國內 5G 網路的公共關鍵基礎設施上禁止使用任何中國產品，Verizon 會完全遵守這項禁令並且已經擬出相關的應對措施，同時在此更近一步聲明 Verizon 之核心線纜（Core wireline）以及行動網路（包含新的 5G 網路）中沒有使用任何華為或是中興通訊旗下的任何設備 [88]。

Verizon 作為一個全球的網路服務的營運者，必定會連接到跨國網路營運者所提供的網路，然而各地區有著不同的法規以及各電信商對於供應鏈、網路資訊安全管理做出了不同的評估與應對措施，例如連接那些不受中國設備禁令約束的網路提供商所提供的網路或是本身在不受禁令約束的地區下營運網路時可能會增加潛在的資安風險，對此一風險，Verizon 特別組織了自己的網路且已做好萬全的準備來維持用戶的安全。Verizon 也意識到，並不能一直控制消費者對於裝置（如手機、路由器）的選擇，而消費者所選擇的裝置可能會連上 Verizon 的網路邊境而帶來資安風險，因此 Verizon 利用了網路的性質來處理任何在網路邊境的惡意活動，例如研發出一項

新的 5G 安全技術可以讓用戶裝置在完全取得的信賴之前，先隔離此裝置 [88]。

Verizon 未來在邁向 5G 網路的發展會著重建置更加安全的網路，例如：提供更強大的加密機制、更多的網路邊境防護系統以及提升創造更多安全的網域或是網路切片（Slices）的能力。 [88]。

二、德國

(一)Deutsche Telekom

德國電信（Deutsche Telekom） [89]2019 年 7 月 3 日宣布，即日起將於首都柏林和總部所在地波恩（Bonn）開放 5G 測試網路，成為德國率先推出 5G 服務的電信商。

德國電信認為營運 5G 網路的首要考量即為「網路安全」，5G 所帶來的數位革命時代皆需建立在網路安全之上，而身為德國率先推出 5G 網路的電信業者，更應該完善 5G 之資通安全、服務品質。在面對 5G 即將帶來的全面物聯網數位時代，屆時會有大量的裝置連上網路，德國電信在 5G 的裝置身份驗證上（Authenitcation）除第一道的 SIM（Subscriber Identity Module，用戶身份模組）卡驗證以外 [90] [91]，內部網路會再進行第二道擴展認證協議（EAP）的驗證，以防止惡意裝置連線，且為了防止 IMSI-catcher 成功取得用戶資訊、竊聽，德國電信亦保護 SUCI，透過加密機制儘可能地藏匿免於駭客得知。另外，德國電信也特別關注網路設備供應商的風險（如下圖 3-13），根據 NESAS，德國電信對於網路設備供應商上分為兩個層面的審查，一個為網路設備之安全評估，另一個為設備供應商之產品開發生命週期的審查，在流程上，由設備供應商定義其安全開發的生命週期流程，再由審查驗證者進行驗證，另一方面，設備商所製造出的產品也必須經由測試實驗室來進行安全評估，要經過產品開發生面週期的驗證以及產品安全評估後，德國電信才會考慮使用該網路設備。此外，德國電信尤其指出在網路設備商的選擇上，不能只仰賴單一設備商，應分散風險，且將認真對待中國網路設備供應商的安全問題。

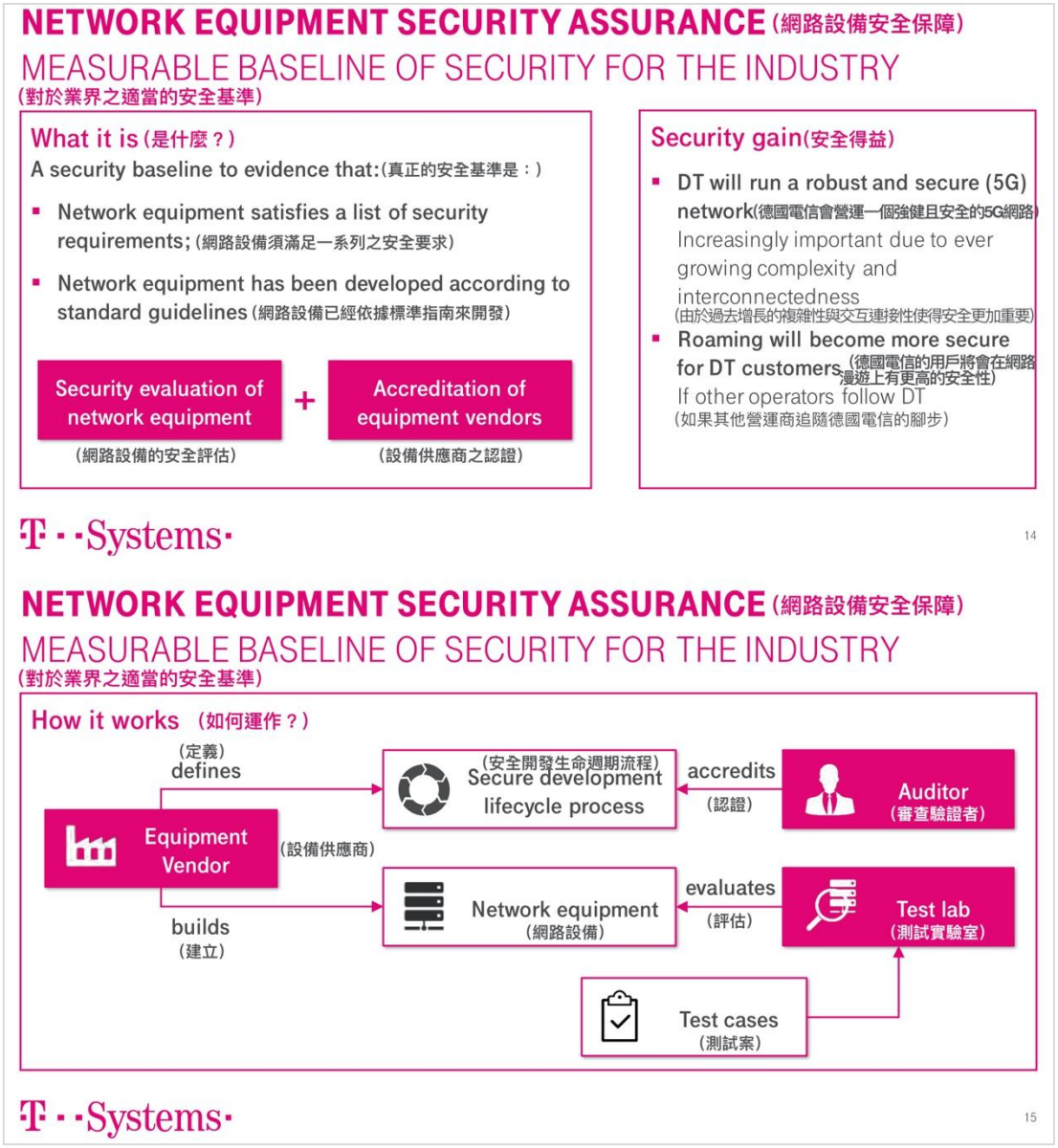


圖 3-13、德國電信所採取之網路設備安全保障概述

資料來源： Deustche Telekom

除此之外，聲明中提出 3 大保護措施：

1. 國家認證：所有關鍵基礎設施在部署前都應由國家監督下的獨立實驗室進行獨立安全認證；所有 5G 網路的基礎設備實驗室，都應該接受政府監控。

2. 信任的第三方擁有原始碼（Source Code）：5G 設備商應提供原始碼給政府信任的第三方機構，使這些信任機構有權接取原始碼，以防範、解決安全漏洞；而在特定情況下，電信業者有權獲取原始碼以應對安全漏洞問題。

3. 擴大法律規範範圍：應擴大法律規範，除了規定 5G 設置的法律義務和責任外，也應該規範網路設備供應商。

三、澳洲

澳洲是繼南韓及美國之後，第三個提供 5G 服務的國家；2019 年 5 月 28 日 Telstra 發表 5G 行動電話服務 [92]。

Telstra 在 2019 年提出了《2019 年 Telstra 安全報告(2019 Telstra Security Report)》 [93]，報告中指出「安全」將成為澳洲企業的首要戰略重點，安全投資的增加反映出對於安全性的高度關注，因此 Telstra 視「網路安全」為 5G 網路營運的第一考量，表示將遵守《政府提供之 5G 安全指南予澳洲電信業者（Government provides 5G security guidance to Australian carriers)》 [76]辦理 5G 相關業務。Telstra 認為面對網路安全威脅，大多數的應對措施都著重在技術面，然而用戶資安意識的薄弱，往往是網路安全的突破口，因此提出了「五個需知」(如下圖 3-14） [94]來建議從用戶到技術人員再到管理階層的每個人，在面對網路安全的風險管理時，都必須注意下述五個重點：(1)知道數據的價值、(2)知道誰有權限接取你的數據、(3)知道你的數據儲存在哪、(4)知道誰在保護你的數據、(5)知道你的數據如何受到保護，才能有效管理網路安全風險。

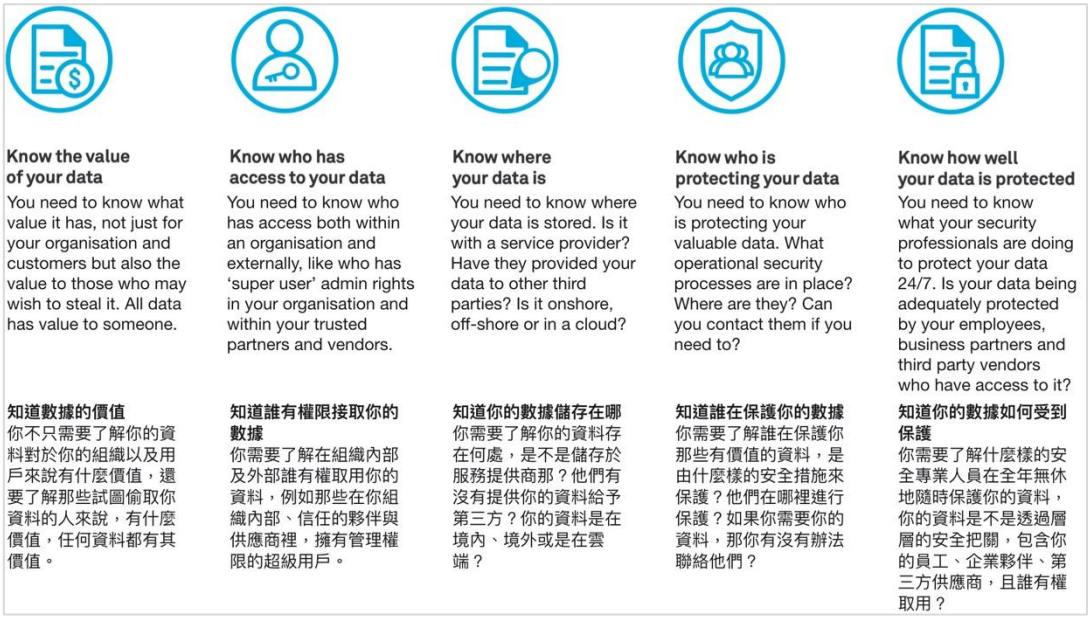


圖 3-14、網路安全五個需知

資料來源：Telstra

Telstra 認為在管理網路安全時，還需要考慮更廣泛的安全領域，未來 5G 將帶動物聯網時代的革命，連接設備越多，安全範圍就越廣，這為新技術帶來了改善端到端可見性和更好地安全風險管理的機會，隨著安全威脅變得越來越複雜，Teltra 事業部部長 Michael Ebeid 也表示企業必須尋找方法來準備複雜的新興威脅，並將其作為安全策略的一部分，公司必須保持警惕，充分掌握日益連接的網路世界，以保護自己和客戶。

另外在 Telstra 安全年報中，針對 5G 網路的隱私和安全部分有特別聲明敘述如下 [93] [95]：維護用戶數據的隱私和安全至關重要，是 Telstra 做任何事情的首要任務。全球網路威脅不斷成長，包括針對澳洲個人和公司的國內外駭客集團，日趨復雜的網路釣魚詐騙，以及針對關鍵電信基礎架構的網路攻擊，再加上未來 5G 網路的高度安全需求；因此 Telstra 的用戶隱私和安全，以及重要的商業資料將可能受到多種方式破壞，包括違反 5G IT 系統和供應商系統的不

正常作業、未經授權或無意地訊息發佈、或是人為錯誤，如果其系統受到破壞，將會影響網路的營運，損害客戶的信任度，並可能嚴重威脅到品牌聲譽，進而影響 5G 網路的發展。

Telstra 有多種策略來應對上述的網路威脅：例如測試員工執行相關業務時之合規性以及企業級網路事件攻防演練、對 5G 網路設備與服務之第三方安全性進行審查以確認其符合其制定的標準與政策和程序。Telstra 會定期更新隱私聲明和隱私程序，同時並考慮社會期望和技術變化對蒐集、儲存和利用用戶資訊的影響。

四、日本

(一)NTT DoCoMo

NTT Docomo [96]與資安公司趨勢科技 [97]合作開發一套針對 5G 網路時代需求的最新網路安全解決方案，此方案是趨勢科技在 NTT DoCoMo 的「DoCoMo 5G open cloud(DoCoMo 5G 開放雲端)」上推出以 Virtual Network Function Suite（虛擬網路功能套組）為基礎的一項方案，進行包含 5G NFV 與雲端功能的技術驗證。「DoCoMo 5G Open Cloud」是一套專為商業合作夥伴所提供的 5G 技術驗證平臺，方便合作夥伴開發針對 5G 時代的新式解決方案。另外，趨勢科技虛擬網路功能套組是在虛擬化環境（如 NFV 和雲端）上實施網路資安功能的網路防護解決方案，同時還能針對個別物聯網裝置套用必要的防護，這可使得那些無法安裝額外防護的物聯網裝置得到保護，趨勢科技將 VNFS 技術運行在 DoCoMo 5G Open Cloud 上，然後將雲端上各服務的網路流所暗藏的威脅加以可視化，以達到偵測、攔截、排除、解決，進而為用戶提供安全的 5G 環境。

以下為 NTT DoCoMo 之 5G 系統申請時之 5G 資安防護計畫[130]

1. 建立電信設備安全標準及 DoCoMo CSIRT 電腦安全緊急事件應變團隊（如下圖 3-15）。



圖 3-15、Docomo CSIRT 組成

資料來源：NTT 安全可靠通信部

2. 建立內部人員安全認證體系，所有員工都需進行資通安全教育訓練。

3. 設備採購時必須符合電信設備安全標準規定，未符合時則進行風險評估，與內部相關組織就配合政策達成協議，並組成安全審查小組進行審驗。

4. 設備將嚴格進行資安管控機制，包含風險評估、弱點評估、權限識別、服務監控等作為。

5. 針對通信網路異常行為引入機器學習檢測機制。

6. 全天候進行網路資安事件的偵測與掌握，成立資訊安全監控中心（Security Operation Center，SOC）（如下圖 3-16）並配置多名具有資安相關證照的人員。

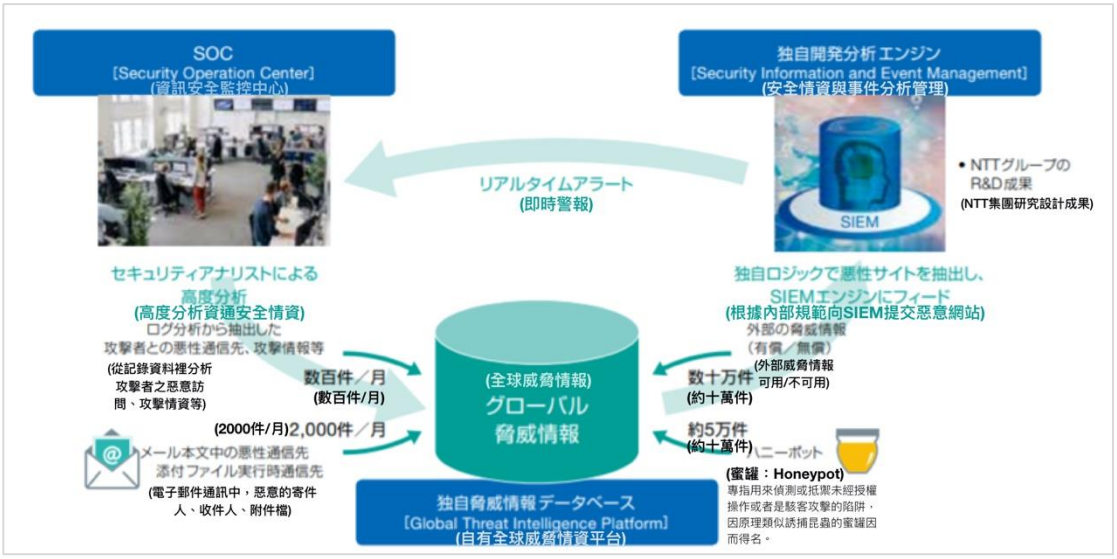


圖 3-16、NTT SOC 中心

資料來源：NTT 安全可靠通信部

7. 當事件發生時，啟動緊急應變機制，針對網路攻擊事件進行應對、解決及回報。

(二)KDDI

以下為 KDDI 之 5G 系統申請時之 5G 資安防護計畫 [98][130]

1. 制定風險管理規則、基本資訊安全規則、資訊安全措施標準等。
2. 成立 KDDI-CSIRT 電腦安全緊急事件應變團隊，進行資安事件應對及演練，強化應變能力。
3. 舉辦ICT-ISAC活動，進行漏洞訊息通報，資產版本漏洞管理、修正，培育資安人才。
4. 根據 KDDI 採購政策和 KDDI 供應鏈促進指南，要求設備商之品質保證及管理。
5. 每兩個月舉行一次營運資訊安全委員會。

6. 根據公司範圍的系統安全管理指南和網路應用程序管理指南，執行安全審核和網路漏洞診斷。

7. 針對物聯網設備進行安全措施檢查。

8. 全年無休地隨時監控未經授權的入侵、偽造和 DDoS 攻擊等網路安全事件。

9. 擬定網路攻擊發生時的應變流程,並將其發佈在公司網站上。

10. 實施網路安全標準化和研發工作。

(三)SoftBank

以下為 Softbank 之 5G 系統申請時之 5G 資安防護計畫 [99][130]

1. 建立基本資訊安全規則，資訊管理規則等。

2. 建立 SoftBank CSIRT 電腦安全緊急事件應變團隊，以應對網路攻擊，並進行事前準備及事中應處機制。

3. 進行員工資通安全培訓和資安事件應對演練。

4. 針對系統開發和採購，制定安全要求（適用於商業網路和開發環境，並要求外包合作夥伴遵守）。

5. 進行風險評估，安全驗收測試等，以提升安全。

6. 將監控系統設置在安全等級較高的機房，並進行嚴格的機房出入境管理,及設備帳戶管理、日誌獲取,並定期執行漏洞診斷等。

7. 在未與外部連接的獨立網路上,全年無休地隨時監控其設備、流量和服務。

8. 編撰並落實網路安全事件發生時所要進行的通報、應變作業及程序。

(四)樂天

以下為樂天之 5G 系統申請時之 5G 資安防護計畫 [100][130]

1. 建立資訊安全和資訊系統管理規則。
2. 成立樂天行動網路危機應變小組（RMN-ERT），專門應對網路安全事件。
3. 制定公司內部之資通安全政策，並為所有員工提供資通安全培訓。
4. 針對設備執行安全檢測，如基準測試、標準一致性測試、弱點掃描，以及所有電信設施安裝和部署期間的 DDoS 對策。
5. 進行滲透測試和漏洞評估以確保資通安全到達一定的層級。
6. 通過數據中心的視訊監控系統提升物理安全
7. 嚴格執行身份管理，並決定授予接取權限。
8. 成立 SOC，並全年無休地隨時監控網路上的攻擊和流量；並透過 SOC，收集和檢查日誌，以檢測和防止未經授權的活動。
9. 套用修正檔或更新時，採取一貫的步驟確認安全性，以及制訂業務持續營運改善計畫等。

上述四家電信業者除了應日本總合通信基盤局要求針對 5G 網路安全提出整體的因應對策之外，總合通信基盤局亦要求各電信業者必須對於 5G NSA 初步架構之 gNB 基地臺的設置安全性提出相應對策計畫[130]，並且對其進行計畫評分，評分方式採競爭性評比，基準值為 0 分，如果有表現較優異者再加分，評比結果各電信業者表現均評為相同等級，故沒有優劣均為 0 分，下表 3-5 綜整其內容：

表 3-5、日本各電信業者針對 5G 基地臺安全性之相應對策計畫

研提 5G 基地臺之安全對策，以保障通訊設備的安全性與可靠性，請各家業者依據下述面向提研對策計畫： 1. 在通訊設備的設計、施工、維運上，應採取可以降低人為疏失導致之數據傳輸錯誤或組態設置錯誤的相應對策。 2. 考量到連接數的增加，採取提升巨量連接之對策。 3. 採取相關對策以預防軟體設計上的缺陷而造成網路運作異常。			
NTT DoCoMo	**KDDI**	**SoftBank**	**Rakuten**
預防人為疏失的對策			
・ 運用透過過去通訊異常事件整理成的「無人為故障之對策措施」，並共享過去的異常案例（故障案例等），並引 SON（Self-organizing Network，自組織網路）技術，減少發生人為疏失的	・ 強化人員聘用標準及流程，制訂作業步驟和規範並加強宣導遵守。。 ・ 利用服務功能安全檢查表掌握風險，並記錄。 ・ 將過去的異常事件製作成資料備查。 ・ 培育安全推動人員（公司	・ 製作標準作業程序書，並由管理階級人員認可之，以防施工中的疏忽。 ・ 禁止使用程序書以外的步驟施工，施工作業要由員工親自進行，或在員工的監督下由供應商進行。	・ 商用設備在施工時，必須依據過去經驗與遵循通過主管認可的程序書進行施工，並將作業內容、時間日期進行登錄、管理與共享。 ・ 預測風險或運用公司的 SNS（Social Networking Service 社群

機會來降低風險。 ・ 發生事故時依情況向上呈報，且從首次通報到復原為止，應即時且適當地維護用戶服務，事故結束後招開檢討會議釐清事由、研擬預防對策，在未來以此預防對策為基礎來執行服務，以預防相關事故發生。	內部資格：認證約200人)。 ・ 推動業務自動化與 AI 化，以減少人為疏失。 ・ 在開發階段讓營運部門參與驗證實驗(早期學會技術）。 ・ 實施 15 分鐘內服務復原的機制，縮短事故發生時的復原時間。	・ 針對疏失，釐清原因與研擬應對策略等，並製作成資料備查，近一步再與相關人員共享（與相關部門合作進行訓練，落實策略以防事故再次發生）。 ・ 運用 ICT 以減少人為疏失，同時提高精準性(同步執行報告的製作與擬定事故通報制度，要求回報施工進度及指派施工中的聯絡窗口，同時強化資訊安全）。 ・ 運用VR技術製作影片，並引進安全課程中。	網路服務）工具等，建立多元化共享資訊的管道。 ・ 實施作業時，採用具有雙重確認的兩人執行體制，並為實際作業徹底進行紀錄。 ・ 作業結束後，定期對作業員進行教育訓練，並相互分享、討論。 ・ 積極進行系統化的教育訓練和事故相關訓練。
提升巨量連接與極大流量的對策			
・ 針對基地臺的用戶平面和控制平面需求，設計、規劃相關設備。	・ 依需求適度強化設備的連接能力，每年最少兩次依照事業計畫書與近期	・ 依據過去的流量趨勢及裝置連接數，預測出未來需求並提升	・ 每月計算、統計每一名用戶的使用流量，監控通訊設備的效能

• 為提升 5G NR 的數據穩定傳輸，以小型基地臺作為建置基礎、波束成形（Beamforming）技術來抑制訊號扇區間的干涉、MEC 的負載分散等。 • 在大型活動的超巨量連網及超大流量需求對策中，除了使用傳統的行動基地臺車外，還計畫引進手提式行動基地臺，並運用 AI 來分析基地臺紀錄檔的大數據、利用群眾委外（Crowdsourcing）的策略來提升網路的品質。	的流量狀況，實施需求預測與實際流量的差異分析。 • 巨量連接時，考量到設備發生故障時的因素，並將其反應到設計上，以提升裝置的連接能力。 • 使用大數據及 AI 預測流量並採取對策。 • 實施 5G 設備的網路功能虛擬化措施或利用網路切片來隔離設備資源。	足夠的裝置連接容量。 • 於事前的評估檢驗中，依據最新的流量模式實施負載測試或過負載測試。 • 針對特定區域的巨量連網及超大流量需求，透過部署大量設備進行分散和同時處理讓連網能力更加寬裕以維持服務品質。 • 定期進行容量管理，如需求量超過基準值時，會研討是否需要強化設備。	表現及系統紀錄檔等。 • 依據上述內容，每三個月實施一次流量需求預測及改善設備計畫。 • 一年實施兩次以上的中長期需求預測（依據技術動向、市場動向和本公司的流量變化等），擬定設備擴充計畫。
預防軟體設計錯誤而造成網路異常的對策觀點			
• 由開發部門確認軟體功能，確保製造商交付的檔	• 用自家公司的驗證設備，由專門驗證的開發部門	• 針對供應商交付的軟體，由本公司和供應商雙方	• 供應商除了進行各個模組的驗證外，還會在供應

案（韌體）是否滿足要求的規格。 ・ 營運部門應事先在未來商用網路中抽選幾個基地臺進行實際測試，確認能在一定期間維持穩定運行後，再擴大規模，並階段性部署到全國。 ・ 開發部門與設備運用部門採取密切的合作體制，在引進設備時進行運用實驗防止軟體錯誤。 ・ 發生異常時應切換回舊版本。	針對交付的軟體進行測試和評估。 ・ 完成測試和評估的軟體，會先安裝在一臺商用網路的設備上，確認穩定運作後，再逐漸擴大規模部署到全國的設備。 ・ 建立可用End-to-End驗證的通訊設備商用環境，並模組化與自動化軟體測試，然後在發生錯誤時分析緣由，同時持續落實預防措施。 ・ 建立軟體切換機制，當發生問題時可將軟體切換回舊版本。	各自進行驗證、測試確認有無問題。 ・ 測試後的軟體，先在小型商用設備上執行，並確認正常運作後，再大規模部署於商用服務中。 ・ 在重大事故後，重新檢視執行流程和強化測試項目等，防止問題再次發生。 ・ 確認軟體有問題後，落實軟體切換機制，回歸舊軟體以維持、回復服務正常運作。	商的實驗室中實施單一節點驗證測試，同樣在本公司實驗室也應實施測試。 ・ 在相關部門的設備評估會議上決議認可的軟體，並應先行部署在小型的設備上，之後再擴大規模到商用設備上。 ・ 尋找符合本公司要求的供應商，在開發階段與其達成協議，並透過召開例會等方式確認進度。 ・ 收集商用設備發生的警告或異常相關資訊，並進行風險分析及採取必要的應對措施。
1. 「預防人為疏失的對策觀點」中，針對作業步驟與認可程序等皆有完善的公司內部規定，且會於公司內部共享發生的事故案例，同時依內容進行訓練並採取相關對策以防止人為疏失，所以無法判斷哪一方較為優異，故認定為相同等級。			

2. 「提升巨量連接與極大流量的對策觀點」中，皆有採取相應策略以提升網路流量與連接量之服務品質，例如依照流量需求等設定等，因此無法判斷哪一方較為優異，故認定為相同等級。 3. 「預防軟體設計錯誤而造成網路異常的對策觀點」中，皆會確認交付的軟體是否符合要求的規格，同時侷限商用設備的範圍先實施小規模的實際測試後，再依序擴大範圍以防止軟體錯誤的問題發生，因此無法判斷哪一方較為優異，故認定為相同等級。 上述各觀點中，各家業者表現評估為同等，無優劣之分。			
0 分	0 分	0 分	0 分

資料來源：日本總合通信基盤局、本團隊整理

五、 南韓

(一)SK Telecom

南韓 SK Telecom 於 2019 年 3 月表示，將與瑞士日內瓦 ID Quantique 量子技術公司合作 [101] [102]，引進量子安全等級之網路加密方案（Quantum-safe network encryption solutions）應用於 5G 網路安全上，以提升 5G 網路的安全。這項方案是 ID Quantique 以自行研發之量子隨機數產生器（Quantum random number generator，QRNG）在結合量子密鑰分配（Quantum key distribution，QKD）協議所發展出的方案 [103]，其密鑰可達到 AES-256 之標準（Advanced Encryption Standard，進階加密標準） [104]，其中因量子的不可確定性（Quantum indeterminacy）與不可複製理論（Quantum no-cloning theorem），使得 QKD 協議能有效防止駭客竊取正確的密鑰來解密所傳輸的數據，避免數據遭到攔截或竊聽，提供極安全的資料傳輸。SK Telecom 將這項安全方案應用於 5G 網路的用戶驗證伺服器中以提升其用戶的個人資訊安全，該公司近期還計畫了將會使這項方案向下拓展應用至現有的 4G LTE 網路，以鞏固 SK Telecom 全盤網路的安全性。

(二)KT Corporation

南韓 KT Corporation [105]意識到 5G 網路的特性將帶來物聯網設備數量的明顯提升，會開啟大規模物聯網的數位新時代，在這個有大量設備連接的網路中，將會大幅提高網路安全的風險，因此 KT Corporation 於 2019 年推出了基於區塊鏈技術的 5G 網路品牌「GiGA Chain」及相關的區塊鏈服務 [106]，區塊鏈層可以提供現有集中式基礎設施無法比擬的安全級別，能有效提高物聯網設備的安全性，

保護他們免受網路攻擊。KT Corporation 透過區塊鏈的技術開發了「GiGA Stealth」，其利用非對稱式加密（Asymmetric encryption）和安全散列算法（Secure Hash Algorithm）使得連網設備將根據其本身相應的區塊鏈地址進行註冊，能夠隱藏連網設備的 IP 位址以保障其身份來防止駭客攻擊。

(三)LG Uplus

南韓電信業者 LG Uplus 同樣地也已經為 5G 所帶來的新興安全威脅作出相關應對，LG Uplus 與 Juniper Networks（瞻博網路）合作 [107]，計畫可以提高 5G 網路系統的安全，例如引入自動化識別異常等，除了與業界合作之外，LG Uplus 亦與學界合作，如與高麗大學（고려대학교，Korea University）合作，進行 5G 安全評估、安全漏洞診斷並擬訂出相應對策 [108]，也與首爾國立大學（서울대학교，Seoul National University）工程數學中心與 Cypolab 共同致力於有關量子密碼技術的研究 [109]，期盼可以為未來的通訊網路以及物聯網時代提供更安全的保障。

除與各產學界合作以外，在吵得沸沸揚揚的供應鏈議題上，LG Uplus 是唯一南韓三大電信商中唯一使用中資設備的電信業者 [110]，LG Uplus 在使用中資設備時，會先將設備的原始碼與各軟硬體元件與材料等送至國際測試實驗室認證並通國際通用標準，通過後內部會再進行安全性測試，設備中的每一個元件，包含軟硬體、運作狀態等均確認安全無虞後才使得建置。

第三節本章總結

5G 通訊網路的新技術將會帶來數位革命的時代，同時也是一個會帶動國家整體經濟、利益、社會福祉的重要基礎工程，因此各國家無論是政府單位或是私人機構均大力推動通訊產業，積極發展 5G 網路，以保障通訊產業在未來能穩定正向發展，然而通訊網路的發展必須建立在安全性之上，因此各國家在發展 5G 之際，政府也頒布具有公權力的規範、法令來保障 5G 網路的安全性，電信業者也相繼遵循政府所頒布的措施，並且以實際經驗、技術發展、成本考量上擬定與執行相關應對策略，本章探討各主要國家政府針對 5G 網路安全的相關監理作為以及共識，且也蒐集部分國家電信業者的相關資通安全作為，以上內容綜整如下表 3-6 及 3-7 所示：

表 3-6、全球各主要國家 5G 資通安全維護監理作為或法令統整

國家、聯合會議	官方相關作為與共識
美國	・ 因 5G 網路系統設置初期採 5G NSA 架構，建立在 4G LTE 網路系統架構之上，故仍須遵守《NIST SP 800-187：Guide to LTE Secirity》，此文件列出三大重點(1)LTE 安全架構、(2) LTE 網路威脅與(3)緩解措施。 ・ 根據 NIST 所發布之《提升關鍵基礎設施資通訊安全之架構(Framework for Improving Critical Infrastructure Cybersecurity)》供給公、私部門機關針對 5G 網路安全策略參考。 ・ 發布《美國 5G 科技加速計畫，5G Fast Plan》，旨在促進美國 5G 產業的競爭力，確保全球市場正當、公平發展與競爭。 ・ 發布《超越 5G 安全法案(Secure 5G and Beyond Act)》，主要用於美國關鍵基礎設施之保護，呼籲美國盟友採取一致性的策略，並提供安全性上的協助。

國家、聯合會議	官方相關作為與共識
	・ 發布《5G 網路科技之防護應用（Defense Applications of 5G Network Technology）》，建議制定供應鏈標準，以提升上、下游供應鏈之設備安全。 ・ 簽署《保護資訊科技與服務供應鏈（Securing the Information and Communications Technology and Services Supply Chain）》行政命令，禁止美國企業採購對國安具備威脅之外國電信設備。
歐盟	・ 公告《5G 網路之網路安全建議書（Commission Recommendation - Cybersecurity of 5G Networks》，指出歐盟各成員國應合作提升 5G 網路建設高度安全性，且各成員國應完成 5G 網路基礎設施的國家風險評估報告。 ・ 通過《歐盟網路安全法案（EU Cybersecurity Act）》，加強網路安全結構、增強對數位技術的掌控、確保網路安全應當遵守的法律規範。 ・ 發布《歐盟 5G 網路安全風險評估報告（EU coordinated risk assessment of the cybersecurity of 5G networks）》，該報告提出主要的威脅、敏感的資產、主要的漏洞及其他戰略風險。
德國	・ 遵守歐盟層級所發布的命令、規範、政策。 ・ 發布《德國網路安全戰略（Cybersecurity Strategy for Germany）》，用以應對針對政府機構、關鍵基礎設施、企業以及公民的網路威脅活動，該戰略的發展及實施的主要特點包括：(1)強化關鍵基礎設施防護、(2)重視國內資源有效整合、(3)注重國際網路安全協作。 ・ 發布《電信網路和服務的附加安全性要求的關鍵要素（Key elements of additional security requirements for telecommunications networks）》，提升技術發展之安全性，電信網路公司必須滿足相關安全要求，於構建 5G 之技術必須符合最高安全標準，且應盡可能排除安全問題。
英國	・ 遵守歐盟層級所發布的命令、規範、政策。 ・ 針對英國 5G 網路之四大發展目標：(1)降低英國的網路安全風險、(2)有效應對網路事件並減少損失、(3)瞭

國家、聯合會議	官方相關作為與共識
	解網路安全環境、共享資訊並解決系統漏洞、(4)增強英國網路安全能力。 ・ 發布《2017 英國數位戰略（UK Digital Strategy 2017）》，該戰略詳細闡述了英國脫歐後將如何打造世界一流的數位經濟，並對未來如何推進數位轉型做出了全面的部署，主要包括(1)連接戰略、(2)數位技能與包容性戰略、(3)數位經濟戰略、(4)數位轉型戰略、(5)網路空間戰略、(6)數位政府戰略、(7)數據經濟戰略七大戰略。 ・ 發布《下一代行動裝置技術：英國 5G 戰略（Next Generation Mobile Technologies: A 5G Strategy for the UK）》，旨在盡早佈局 5G 技術的優勢，並於世界領先數位經濟，此戰略就七大關鍵(1)開發 5G 經濟案例、(2)實施適當的監管規則、(3)地區-治理及能力、(4)覆蓋範圍與能力 – 匯流與邁向 5G 網路、(5)提升 5G 的安全部署、(6)頻譜、(7)科技與標準，明述英國對於 5G 發展應採取的相關作為。 ・ 公布《英國電信供應鏈評估報告（Telecoms Supply Chain Review）》，此評估報告係對電信供應鏈進行審查，進行全面評估，評估的主要觀點為：(1)全光纖網路是促進英國繁榮的關鍵技術、(2)5G 和全光纖網路面臨安全挑戰、(3)整個行業缺乏將安全風險控制到適當水平的管理機制、(4)國家可依賴的供應商；並提出下列建議：(1)建立健全電信安全立法框架、(2)管控供應商帶來的安全風險、(3)制定新的電信安全要求。 ・ 推出第三輪《網路技術即時作用基金（Cyber Skills Immediate Impact Fund》，目的在增進英國國家網路安全產業之多元性發展，培訓業者可透過競標網路安全培訓計畫與企業雇主合作，從中培訓網路安全領域人才，並阻止技能落差持續擴大，以吸引更廣泛的人才從事網路安全工作。
澳洲	・ 發佈《5G – 啟動未來經濟（5G - Enabling the future economy）》，提出政府為支持 5G 發展而實施的 4 項

國家、聯合會議	官方相關作為與共識
	行動：(1)立即提供頻譜、(2)積極參與國際頻譜協調活動、(3)簡化相關程序、(4)審查現有的監管方式。 ・ 發布《政府提供之 5G 安全指南予澳洲電信業者（Government provides 5G security guidance to Australian carriers）》，這項指南中特別針對 5G 網路設備供應商提出聲明，政府必須確認 5G 的完整性、機密性與可用性。 ・ 發布《電信部門安全改革法（Telecommunications Sectors Security Reforms）》，目的是加強管理澳洲電信網路的國家安全風險，要求電信業者須採取相關合理、必要之行動。
日本	・ 分配 5G 頻譜給電信業者時，將評估電信業者的供應鏈風險，包括產品評估、供應鏈調查、關鍵零元件與所有硬體及軟體等，同時亦須考量對國家安全之影響。 ・ 制定《政府機構通信設備採購指引（Agreement on IT procurement policy and procedures for goods and services）》，確認新指引內容須確保《日本政府機構的網路安全 Common Standards for Information Security Measures for Government Agencies）》的要求。 ・ 提出 5G 頻譜釋照絕對審查基準，包含下列面向：(1)區域擴展、(2)設備、(3)財務、(4)法遵、(5)服務、(6)干擾措施等。 ・ 提出建置 5G 網路時之附加條件。
南韓	・ 成立「5G 安全與技術諮詢委員會」，提供南韓三大電信業者 5G 設備功能的安全檢查與稽核，及相關技術支援與諮詢，以提升 5G 網路安全。 ・ 提出《5G +戰略》，包括五個核心服務：(1)沉浸式內容、(2)智慧工廠、(3)無人駕駛車、(4)智慧城市、(5)數位醫療保健，與十大核心產業目標：(1)網路設備、(2)次世代智慧型手機、(3)AR, VR 設備、(4)穿戴式裝置、(5)智慧型 CCTV、(6)未來型無人機、(7)連網機器人、(8)5G V2X、(9)資訊安全、(10)邊緣運算。

國家、聯合會議	官方相關作為與共識
	・ 修訂《位置資訊法（Location Information Act）》，以減少使用位置資訊進入 5G 融合服務的障礙。
中國	・ 全面落實《網絡安全法》，強化網路基礎設施保護和數據安全管理。 ・ 統籌營運安全評估，風險通報等監管手段。 ・ 加快推進網路安全態勢感知、威脅資訊共享、應急管理等技術手段的建設。 ・ 支持國家網路安全產業園區的建設，推動建立北京國家網路安全產業園區，同步推進國家園區的整體佈局。 ・ 確保落實《中華人民共和國網絡安全法》。 ・ 電信業者必須通過四大要求：(1)機房運行安全測評、(2)接入資源系統測評、(3)網站備案系統測評和(4)資訊安全管理系統測評。
國際布拉格 5G 資通安全會議	・ 提出下列觀點：(1)維持網路安全不僅僅是技術議題、(2)網路威脅起源於技術與非技術面上、(3)5G 網路的中斷可能造成嚴重的影響、(4)廣及國家層級的應對措施、(5)必須要有適當的風險評估、(6)安全措施的廣泛性、(7)沒有一套通用的解決方案存在、(8)在創新、發展的同時應提升安全、(9)安全需要成本、(10)供應鏈安全。 ・ 會議上從政策面、技術面、經濟面以及安全隱私和強韌性上討論，並提出相關建議、提案。

資料來源：本團隊整理

表 3-7、各主要國家電信業者針對 5G NSA 網路資通安全維護比較

國家	電信業者	5G NSA 網路資通安全維護關注重點
美國	AT&T	・ 制定《AT&T 安全政策與要求》，進行內部網路安全管理及個人數據的保護。

國家	電信業者	5G NSA 網路資通安全維護關注重點
		・ 制定《AT&T 資訊與網路安全客戶參考指南》，內容闡述 AT&T 對於網路安全的實踐。
	Verizon	・ 特別關注供應鏈風險，只與可信賴且長就經營的設備商購買設備，且必須提供安全保證。 ・ 建立自己的獨立網路架構，為防止與其他電信網路連接而產生之風險。 ・ 開發出一套技術，來處理在網路邊境發生的惡意活動。
德國	Deustche Telekom	・ Sim 卡驗證機制加上第二道 EAP 驗證，以防止惡意連線。 ・ 保護 SUCI 免於駭客得知相關資訊，以防止用物數據之取得、竊聽。 ・ 設備供應商產品生命週期流程之審查、由國家認證之安全測試實驗室測試網路設備安全性、且不仰賴單一設備供應商。 ・ 設備供應商應提供原始碼給予政府信任之第三方機構，以防範、解決安全漏洞。 ・ 擴大法律適用範圍於設備供應商。
澳洲	Telstra	・ 應注意用戶之資安意識，故提出「五個知道」，來建議每個人所應該瞭解之網路安全議題。 ・ 應注意物聯網的大規模連接將擴大網路安全範圍。 ・ 著重在用戶數據資料之隱私及安全性。
日本	NTT DoCoMo	・ 與趨勢科技合作開發出一套資安解決方案。 ・ 建立安全標準與 CSIRT。 ・ 建立內部人員安全體系。 ・ 採購的設備須符合電信設備安全標準規定，且嚴格控管。 ・ 將機器學習引入通信網路異常處理。 ・ 成立 SOC。
	KDDI Corporation	・ 制定資安管理規則。

國家	電信業者	5G NSA 網路資通安全維護關注重點
		・ 建立安全標準與 CSIRT。 ・ 建立內部人員安全體系。 ・ 舉辦資安議題相關活動。 ・ 設備供應商必須保證其品質與管理。 ・ 採購的設備須符合電信設備安全標準規定，且嚴格控管。 ・ 隨時監控網路活動。 ・ 制定資安事件應變流程。
	SoftBank	・ 建立資訊安全與管理規則。 ・ 成立 CSIRT。 ・ 員工資安培訓、資安事件演練。 ・ 制定設備採購規範。 ・ 機房出入嚴格管理。 ・ 隨時監控網路活動。 ・ 制定資安事件應變流程。
	Rakuten	・ 建立資訊安全與管理規則。 ・ 成立 RMN-ERT。 ・ 制定資通安全政策、進行員工資安培訓、資安事件演練。 ・ 設備安全性檢測。 ・ 進行滲透測試與漏洞評估以提升網路安全。 ・ 隨時監控網路活動。 ・ 成立 SOC。
南韓	SK telecom	・ 與 ID Quantique 合作，將量子技術引進 5G 通訊加密中，降低數據遭攔截、竊聽之風險，有效提升用戶資訊安全。
	KT telecom	・ 應注意物聯網的大規模連接將擴大網路安全範圍。

國家	電信業者	5G NSA 網路資通安全維護關注重點
		・ 利用區塊鏈技術開「GiGA Stealth」技術，能夠隱藏設備的 IP 位址以保障其身份免受駭客攻擊。
	LG Uplus	・ 與 Juniper Networks 合作，引入 AI 自動識別異常技術。 ・ 與高麗大學合作，進行 5G 安全評估、安全漏洞診斷並擬訂出相應對策。 ・ 與首爾國立大學合作，共同致力於有關量子密碼技術的研究 ・ 使用中資設備，先將設備的原始碼與各軟硬體元件與材料等送至國際測試實驗室認證並通國際通用標準，通過後內部會再進行安全性測試，設備中的每一個元件，包含軟硬體、運作狀態等均確認安全無虞後才使得建置。

資料來源：本團隊整理

各國政府非常重視 5G 網路系統的發展，例如：美國提出的《5G 科技加速計畫》，目的在強化美國於 5G 網路產業的競爭力；英國提出的《下一代行動裝置技術：英國 5G 戰略》，旨在提升英國於 5G 網路的領先地位；澳洲提出的《5G – 啟動未來經濟》，即刻研議 5G 頻譜可用性與適法性，並且審視現有的監管方式等。各國政府在政策上提出許多具體聲明，可以體會各國對於 5G 發展付出極大的努力，然而在 5G 的美麗願景當中，聚光燈是矚目在安全性之上，5G 的軟體化與虛擬化新型的技術可以發展出許多的創新應用，但同時也為 5G 的安全性帶來許多挑戰，如同在國際布拉格會議中的共識，5G 網路的風險評估與安全控制措施非常廣泛，是涉及技術與非技術面的議題，是

一個仰賴全球政府與相關業者共同努力的目標，所以各國政府也陸陸續續發表許多安全性聲明與研究，也頒布相關法規與命令來確保整體國家的網路安全，部分官方單位特別針對其國家識別出網路安全風險，例如：歐盟的《歐盟 5G 網路安全風險評估報告》，提出 5G 網路主要威脅類型、主要威脅的來源（者）、主要資產和脆弱性、主要漏洞與風險等情境；英國的《電信供應鏈評估報告》，講述國家應掌握電信業者之資通安全管理並制定相關規範，且應包含整個供應鏈生態系。除此之外，歐盟後續將交由 ENISA 根據所提出的風險評估報告擬定相關之應對措施。在研究過程中，因為 5G 的多元服務與開放式架構的緣故，大部分的監理單位將焦點放在網路設備供應鏈安全性與第三方服務提供者的風險上，規範其電信業者應該遵循標準流程採購設備，以確保國家安全，再者，有部分研究報告指出 5G NSA 跨系統整合之安全性與互通性，初期的 5G 與 4G 系統的介接以及跨網路互通的安全性，5G 網路各個設備元件之 IT、CT 與 OT 之風險與威脅也是一個值得注意的課題。另外在各國電信業者上因涉及商業機密與資通安全上的考量，此一部分資料較缺乏，但也可以看出電信業者對於 5G 網路安全性所付出的努力，例如美國 AT&T 制定了安全政策以確保資通安全管理，南韓 SK Telecom 應用量子密鑰技術在 5G 網路加密上，日本 NTT DoCoMo 亦與趨勢科技合作共同開發出一套資安解決方案。

第肆章　5G NSA 網路元件、威脅說明及資安相關因應方向

2018 年 6 月，3GPP 完成了 5G 標準第一個版本 Release 15 [1]，並定義 5G 新無線電（5G New Radio，5G NR）技術與 5G 核心網路架構。5G 系統的架構可分為非獨立組網（Non-Standalone，NSA）與獨立組網（Standalone，SA）兩種，5G SA 的網路架構是全面使用 5G 網路設備，另一方面 5G NSA，其核心網路設計是利用現有 4G 核心網路（Evolved Packet Core，EPC）透過軟體更新的方式升級至 5G EPC 來完成，並採用軟體定義網路（Software-defined Network，SDN）與控制/用戶平面分離（Control/User Plan Separation，CUPS）等新技術，實現 5G 網路之三大應用場景，增強型行動寬頻（Enhanced Mobile Broadband，eMBB）、超可靠低延遲通訊（Ultra-reliable low latency communication，uRLLC）與巨量多機器型通訊（Massive Machine Type Communications，mMTC）。在三大垂直應用服務場景上，5G 的架構允許第三方服務提供者在面臨高速運算需求下，如 eMBB 與 uRLLC，均可透過電信業者的 MEC 提供用戶即時服務。以上以用戶觀點所發展之創新式行動技術，使得 5G 網路大量使用資訊科技的軟體化系統與開放軟體介面，致使 5G 網路所面臨之資通安全威脅相較封閉的 4G 網路更為多樣且嚴峻。

5G 網路之資通安全風險大致可分為三個態樣：(1)已由 3GPP 等組織提出的弱點、威脅及可能防護建議者；(2)已知資通安全威脅但未有風險管理與相關防護建議者；(3)尚未發現之資通安全風險者。是以我國電信監理機關－通傳會須針對 5G 網路資通安全之範疇充分掌握與瞭解，而其可能存在的弱點、威脅以及風險亦須要經過詳細的評估，以確保消費者權益、國家安全，及滿足民眾對電信業者的期待。

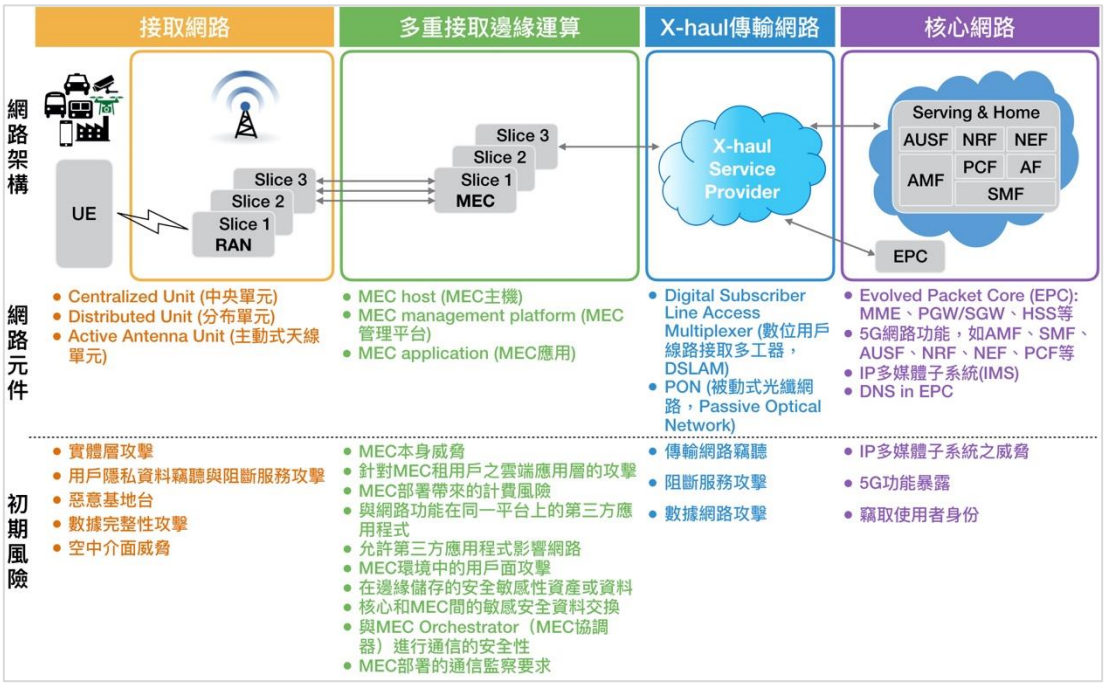


圖 4-1、5G 網路四大區塊與對應之資通安全威脅

資料來源：本團隊整理

本計畫在研析各國際組織、監理單位以及電信業者相關資通安全報告與作為之後，整理 5G NSA 網路系統可分別由以下四個部分對網路釋照初期可能面臨之資通安全風險進行論述（如上圖 4-1）：(1)無線電接取網路（Radio Access Network，RAN）、(2)多重接取邊緣運算（Multi-access Edge Computing，MEC）、(3)傳輸網路（X-haul Transport Network，TN）以及(4)核心網路（Core Network，CN）。

第一節 無線電接取網路（RAN）

一、無線電接取網路（RAN）元件介紹

5G NSA 網路概念是基於 4G 網路升級至 5G 網路的一種部署方式，在既有 4G 網路上新增 5G 新無線電技術 [1]，5G 基地臺（Next generation Node B，gNB）透過 4G 基地臺（Evolved Node B，eNB）的協助與升版的 4G 核心網路（即為 5G EPC）完成連線，稱為 4G-5G 雙連線（E-UTRA-NR Dual Connectivity，EN-DC）架構。目前電信業者最可能採用 5G NSA 佈建方式為 Option 3（Option 3 family）架構 [1] [111]，此種架構下，電信業者以 4G eNB 做為主控（Master）基地臺，5G gNB 則為第二（Secondary）基地臺，此為 4G 網路升級 5G 網路所採用的 5G NSA 模式，其網路架構如下圖 4-2 所示；另外，就 5G SA 而言，其網路架構是完全 5G 獨立的網路系統，具有獨立 5G 核心網路，而非如 5G NSA 所利用之升級 4G EPC，同時 5G SA RAN 與 4G RAN 為互相獨立的系統，因此用戶連接網路時不需仰賴 5G NSA 中所使用的 4G-5G 雙連線（EN-DC），可以直接透過 5G NR（5G 新無線電）接取 5G 核心網路，故在介接上 5G SA 較 NSA 簡易。

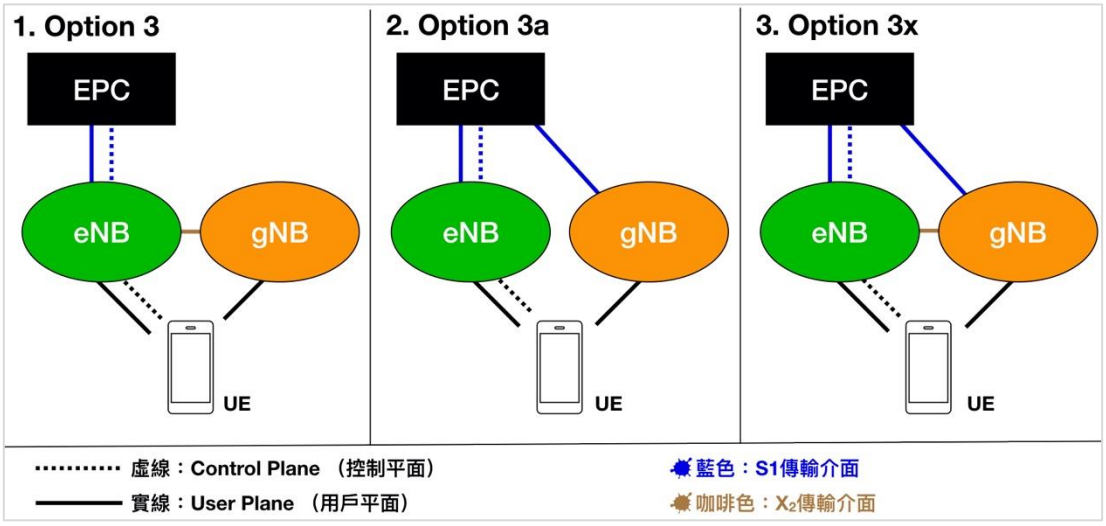


圖 4-2、5G NSA Option 3 之網路架構

資料來源：Global TD-LTE Initiative、3GPP、本團隊整理

1. Option 3: 控制平面（Control Plane）由 EPC 至 eNB 至用戶設備（User Equipment，UE），數據資料透過用戶平面（User Plane）由 EPC 傳至 eNB 至 gNB 至 UE。
2. Option 3a: 控制平面（Control Plane）由 EPC 至 eNB 至 UE，數據資料透過用戶平面（User Plane）由 EPC 傳至 gNB 至 UE 。
3. Option 3x: Option 3 與 Option 3a 之結合。

5G NSA 網路中的 eNB 及 gNB 除了能力協調（Capability Negotiation）外，其資安要求基本上是依據既有 4G-5G 雙連線（EN-DC）的技術規範，進行雙連線時，主基地臺（eNB）會檢查用戶端是否具備 5G NR 的能力與權限以連接第二基地臺（gNB），主基地臺會導出與傳送密鑰給第二基地臺以建立 5G NR 的安全連線，用戶端也會導出相同密鑰，不同於既有 4G LTE 雙連線架構，僅由主基地臺與用戶建立無線電資源控制（Radio Resource Control，RRC）連線，EN-DC 在用戶跟 5G 基地臺間也可以建立 RRC 連線，因此，可以透過 RRC 連線導出 RRC 訊息完整性（Integrity）、機密性（Confidentiality）及用戶平面（User Plane）的密鑰。

5G SA 網路中採用第二道驗證（Secondary Authentication）機制 [1] [7]，為一種擴展驗證協議框架（Extensible Authentication Protocol，EAP），在 5G SA 連線安全的驗證流程中僅會牽涉到 5G 核心網路的會話管理功能（Session Management Function，SMF）元件，以及 5G 無線電接取網路的用戶平面功能元件（User Plane Function，UPF），5G SA 網路用戶終端裝置要加入某一特定網路切片服務時，需先完成驗證程序來接入 5G 核心網路，接下來在第二道驗證階段，由 SMF 作

為 EAP 者之的角色，將驗證資訊轉送至外部第三方 DN-AAA（數據網路-驗證、授權與計費 Data Network – Authentication, Authorization and Accounting）伺服器來驗證和授權，完成 5G SA 網路用戶終端裝置與第三方服務的驗證和授權工作，最後由 SMF 向 UPF 配置適當的轉發路由，完成整個切片的協議數據單元（Protocol Data Unit，PDU）會話連接。

在 4G RAN 技術上，傳統基地臺由基頻單元（Base Band Unit，BBU）、遠端無線電單元（Remote Radio Unit，RRU）以及被動式天線單元（Passive Antenna Unit）所組成。而到 5G NSA RAN 技術上（如下圖 4-3），將採取分離傳統基地臺運作模式，其中 BBU 分為中央單元（Centralized Unit，CU）與分布單元（Distributed Unit，DU）兩個層級，RRU 與大型天線組成主動式天線單元（Active Antenna Unit，AAU），而且 BBU 部分實體層（Phyical layer）功能會被移入到 AAU 中，5G RAN 利用 CU 和 DU 功能的切分方法，並且以資訊內容處理的即時性，分離 5G 基地臺結構與運作層級，此種前瞻性無線電接取網路技術將與傳統基地臺無線電接取網路之運作有著非常大之差異。

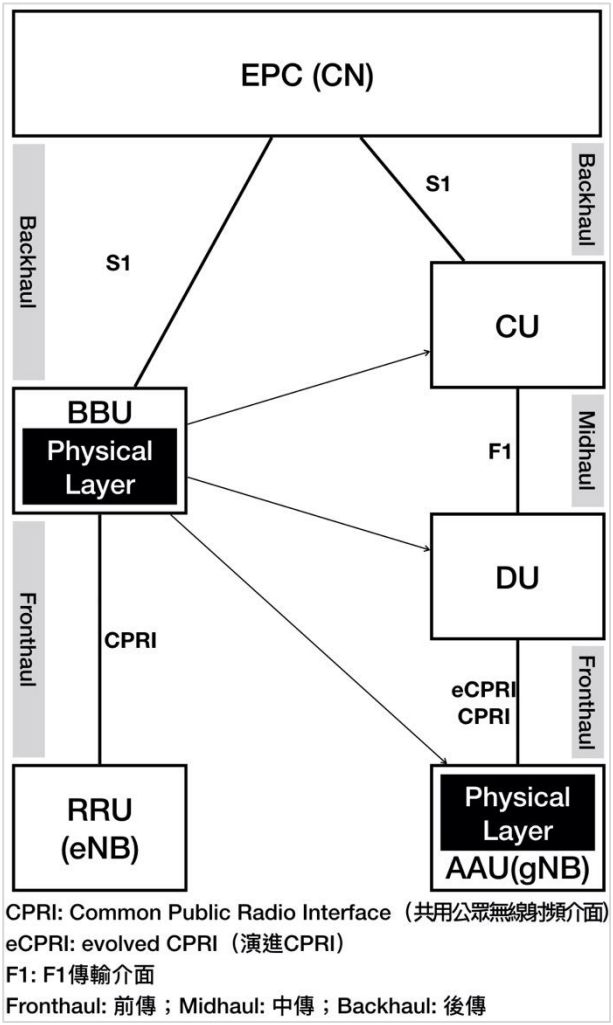


圖 4-3、5G NSA 之無線電接取網路實體元件架構

資料來源：本團隊整理

為提升用戶即時體驗，透過導入 CU 處理技術，電信業者可以使用集中式技術統一管理無線資源與用戶移動狀況，進而提升整體網路效能。在基地臺架構層級上，CU 可以彈性且靈活的將資源集中到電信業者之雲端平臺系統，亦可在既定硬體上運用雲端運作概念來設計系統，達成資源集中化與部署自動化，以減少電信業者之營業費用與成本支出。

目前 3GPP 已確定將封包數據匯聚通訊協定（Packet Data Convergence Protocol，PDCP）/無線電連結控制（Radio Link Control，

RLC）間切分作為 CU 與 DU 之分離方案 [1]，並圍繞該方案討論需要標準化的內容，但仍存在以下問題有待加強關注並推動更深入的標準化，真正實現 F1 介面的開放。

(一)中央單元（CU）與分布單元（DU）切分後功能/性能保障

由於 PDCP/RLC 間切分將控制平面的無線電資源控制（Radio Resource Control，RRC）功能放入 CU，無線電資源管理（Radio Resource Management，RRM）功能放入 DU，使得不同的控制平面功能分屬不同的處理單元，帶來控制平面的延遲，可能影響整體系統的性能，進而導致服務品質（QoS）下降，例如對於終端隨機性接入、切換等流程，由於 RRC/RRM 協定模組從傳統的較強的聚合轉到低耦合，接入過程跨越 CU 和 DU 設備，增加管理控制流程，對業務和用戶體驗將造成負面的影響。

(二)操作維護功能標準化

在標準化 CU 與 DU 間 F1 介面協定時，不僅要關注各自功能的交操作運行性，而且還要顧及到操作維護層面，例如，如何分別配置 CU 和 DU 設備，如何保持 CU 與 DU 間配置參數一致性等。

(三)F1 介面安全性

CU 與 DU 在 PDCP/RLC 切分，原來的設備內部介面變為設備間介面，兩個設備間會利用 F1 介面來當作中間的傳輸網路（TN），將可能導致傳輸網路被竊聽的風險，故需要一套低成本的傳輸網路加密機制，如網際網路安全協定（IPsec）機制，有效保證 F1 介面數據傳輸的安全性，同時也要考慮傳輸時延、傳輸頻寬、實現/介面複雜度。

二、 無線電接取網路（RAN）可能的威脅

5G NSA RAN 端採取分離傳統基地臺 BBU 為 CU 與 DU 功能之技術 [1]，實現網路切片（Network Slicing，NS）與高彈性及可規模化之網路架構，以提供高速率與低延遲之應用服務。5G NSA RAN 為彈性支援各種潛在可能、複雜的應用服務及建置型態，因此開放式 RAN 型態之資通安全風險與威脅將與時俱增。以下探討 5G NSA 網路重要元件及釋照初期可能面臨之資通安全議題。

(一)實體層（Physical Layer）攻擊

由於 5G 高頻寬特性及人口稠密地區對頻寬和占地面積的要求，將導致小型基地臺大量部署，5G 將大量引入並安裝更便宜的小型基地臺。這些安裝在公共場所的基地臺較容易遭受物理破壞，並允許攻擊者實體接觸基地臺的網路介面，獲得非法授權，達到破壞目的。

(二)用戶隱私資料竊聽與阻斷服務（DoS）攻擊

國際行動用戶識別碼擷取器（International Mobile Subscriber Identity-catcher，IMSI-catcher）的出現，導致用戶隱私被攔截、竊聽的威脅，如國際行動用戶識別碼（IMSI）、所在之地理位置、活動紀錄等，有曝光的風險。此外，攻擊者利用 UE 在開始接入基地臺過程中，進行用戶身份轉移，使得攻擊者通過中間人攻擊來偽裝用戶，竊取客戶流量或發起阻斷服務（Denial-of-service，DoS）攻擊，而拖垮整個網路傳輸。因此在 5G 中，電信業者需要施作用戶隱藏識別碼（Subscription Concealed Identifier，SUCI）的來保障客戶隱私。

(三)惡意基地臺

惡意基地臺（False base station，又稱偽基地臺），由於軟體定義無線電的流行，使用惡意基地臺的成本門檻大幅降低，攻擊者可以借以干擾終端裝置的通訊品質，或者試圖偽冒合法業者的基地臺空中訊號，攔截來自 UE 的語音和數據傳輸等，IMSI-catcher 是偽基地臺最常見的攻擊方式，用來嗅探（Sniffing）附近的用戶 IMSI，或者辨識與追蹤特定用戶 IMSI，例如，2018 年美國國土安全部證實在美國國會大廈周邊遭不明人士安裝 IMSI Catcher。5G 系統在設計之初，於 3GPP TS 33.501 與 TR33.804 技術文件相關的安全改進，包括在空中介面不使用與顯示 SUPI、GUTI 的保證更新、受保護的本籍網路重定向以及提出檢測偽基地臺的解決方案等。

根據 3GPP TR 33.804 指出，偽基地臺的威脅有以下四種議題，同時需要額外注意偽基地臺攻擊透過濫用災防告警細胞廣播訊息系統（Public Warning System）功能的安全議題，例如繞過身分認證等。

1. 對終端裝置發動 DoS 攻擊：試圖阻止 UE 接取網路。
2. 對行動網路發動 DoS 攻擊：試圖阻止業者向用戶提供服務。
3. 惡意服務：嘗試向 UE 提供未經授權或未經請求的服務（例如廣告簡訊和來電呼叫）。
4. 對用戶隱私的攻擊：嘗試識別用戶識別符或追蹤 UE，掌握用戶的生活作息或目前所在位置。

(四)數據完整性攻擊

在 4G 網路中對用戶平面（User plane）之數據傳輸，並沒有完整性保護機制。在 2018 年即有研究人員提出演示案例，可利用上述風險達到竄改用戶網域名稱系統（Domain Name System，DNS）之請求，以進行後續的釣魚欺騙。另一方面在控制平面（Control plane）的數據上，也缺乏完整性與不可否認性的安全保護，過往電信業者們總是默認相互信任，例如在跨國漫遊的 SS7（Signaling System Number 7，第七號信號系統）、Diameter 協議信令，這些控制信令是不需要進行驗證，但是，隨著加入漫遊的電信業者越來越多，虛擬電信業者的興起等，這樣的信任關係已經不再存在，2018 年（美國國際駭客年會）上 NOKIA 的研究人員即指出透過 SS7/Diameter 的跨國攻擊是非常難以追查 [112]，故在 5G 中，電信業者除了需要保障其客戶之用戶數據平面的完整性外，同時電信業者也需建置在跨電信業者的網路邊界上的驗證與保護機制。

(五)空中介面（Air Interface）威脅

空中介面之安全性仰賴於位元層級之串流加密法（Bit-level Cryptographic），倘若密鑰長度及加密演算法強度不足將導致竊聽、中間人攻擊等可能性。另外，空中介面威脅也包含攻擊者可能利用偽基地臺假冒電信業者訊號，迫使用戶離開正常網路，或透過同頻干擾方式致使用戶無法接取服務（即 DoS 攻擊）。根據 2018 年學者 Hussain 等人所發表的有關長期演進（Long Term Evolution，LTE）之安全性技術論文 [113]即載明該年美國四大電信業者其中之一，在其空中介面從未啟用過加密功能，進而呼籲電信業者中止這種不安全的做法。故本計畫認為與其放任各電信業者自行決定這些實務操作，倒不如集結各方利害關係人，共同建立最佳實行做法（Best

Practice），同時使規範能被持續的保持及更新，促使電信業者能夠一致採用並與時俱進。

第二節多重接取邊緣運算（MEC）

一、多重接取邊緣運算（MEC）元件介紹

多重接取邊緣運算（Multi-access Edge Computing，MEC）是一種網路架構，由 ETSI 在 2014 年提出 [114]，利用前端無線電接取網路（RAN）結合雲端運算資源提供資訊科技（Information technology，IT）服務的一種技術。透過在行動網路邊緣（基地臺後端）提供雲端運算的能力，用戶端可不經核心網路直接取得遠端伺服器數據，因此可以減少延遲，獲得更佳的服務體驗；因此透過 MEC 架構將可大幅推動需要極低延遲的服務發展；比如 4K/8K 現場直播或 OTT 服務（Over-the-top Service，意指透過網際網路直接向用戶提供的應用服務）、虛擬實境（Virtual Reality，VR）與擴增實境（Augmented Reality，AR）、自動化工廠、車聯網（Vehicle-to-everything，V2X）自駕車或無人機操控等應用場景。

事實上，為因應不同種類的應用服務範圍與延遲需求的差異，MEC 平臺可被建置於整套行動通訊網路中不同位置 [115] [116]，MEC 的部署可以區分為四種場景，基地臺端（無線電接取網路端，RAN）、傳輸節點（Transmission node）、網路匯集點（Network aggregation point）或核心網路（CN）內，其中部署於基地臺後端是現階段比較常見的情況，以下為 ETSI MEC ISG 規劃演進至 5G 的四種 MEC 可能的部署場景（如下圖 4-4）：

1. MEC 與基地臺共站。
2. MEC 與傳輸節點共站（Transmission node），也可能與用戶平面功能設備（User Plane Function，UPF）共站。

3. MEC 和用戶平面功能（UPF）與網路匯集節點（Network aggregation point）共站。

4. MEC 與在核心網路（CN）系統共站。

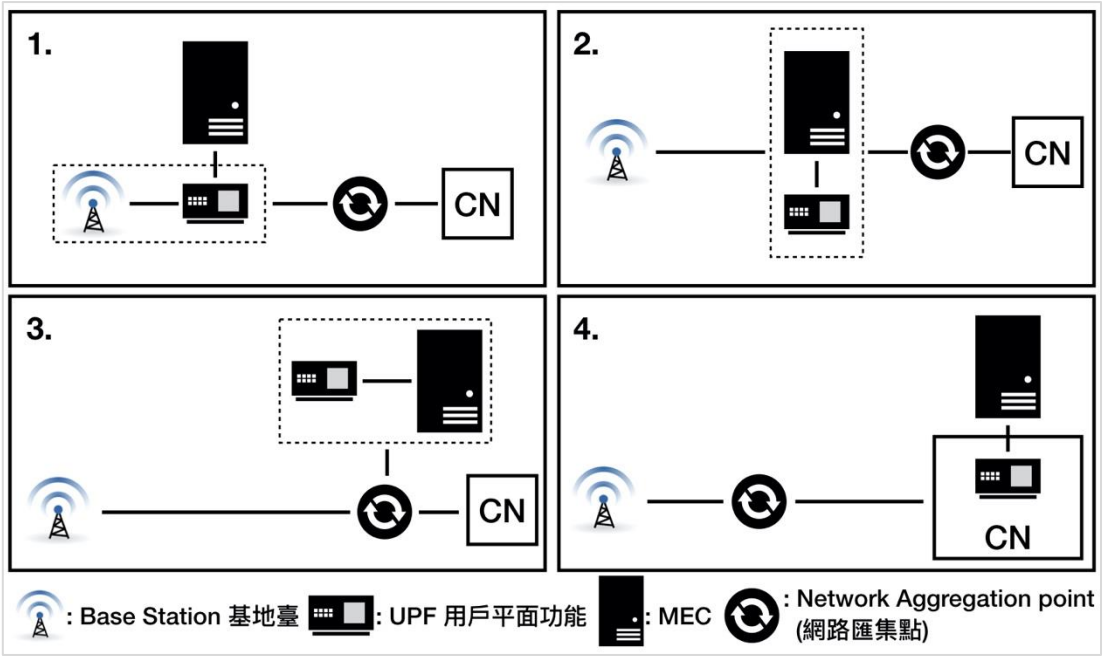


圖 4-4、MEC 之四種可能的部署場景

資料來源：ETSI MEC in 5G networks、本團隊整理

ETSI MEC ISG 致力於 MEC 的研究 [117]，公佈了關於 MEC 的基本技術需求和參考架構的相關規範，以下為 MEC 的網路框架和參考架構標準定義：

如下圖 4-5 所示，針對 MEC 的架構劃分了三個實體功能層級，包括網路層級、主機層級和系統層級。其中 MEC 主機層級包含 MEC 主機（Host）和對應的 MEC 主機管理（MEC Host-Level Management）兩者，MEC 主機內部又可以進一步劃分為 MEC 平臺（MEC Platform）、MEC 應用（MEC Application）和虛擬化基礎設施（Virtualization Infrastructure）等三個結構；網路層級主要包含 3GPP 所規範之行動通訊網路系統、本地區域網路和外部網路等相關連外實體，主要表示這

些實體的連接情況；最上層級是 MEC 系統的管理實體，負責對 MEC 系統進行整體的監控與操作。

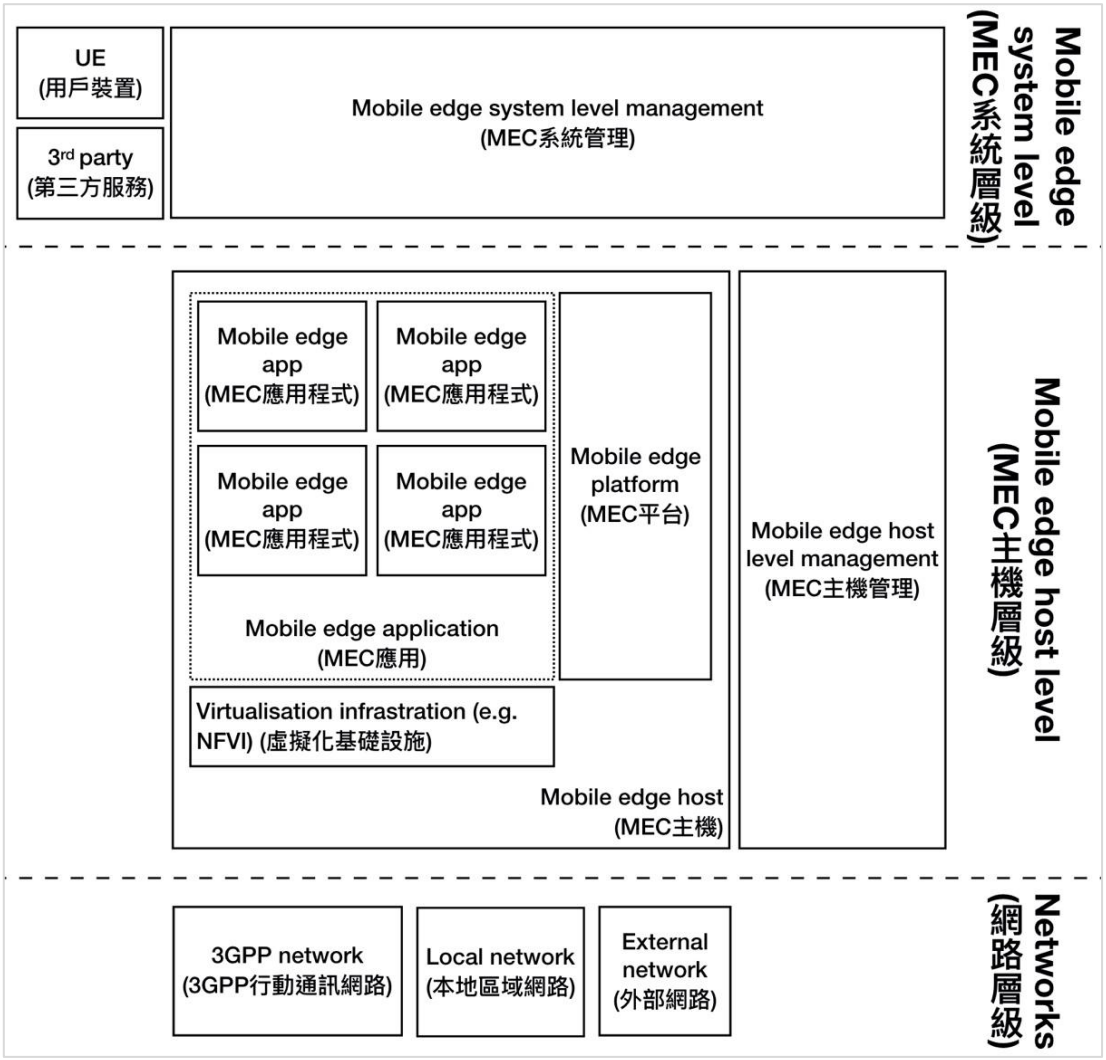


圖 4-5、5G NSA 之多重接取邊緣運算實體元件架構

資料來源：ETSI MEC ISG、本團隊整理

二、多重接取邊緣運算（MEC）可能的威脅

MEC 伺服器是行動通信網路中一種全新類型的實體。除連接到其他行動網路節點實體〔包括營運、管理與維護（Operations, administration and maintenance，OAM）系統、UPF、LI （Lawful Interception）-通訊監察等〕以及容納第三方應用服務程式外，另外還

可能連接到外部第三方雲端應用服務網路，雖然目前已有安全技術〔如 IPsec、傳輸層安全性協定（Transport Layer Security，TLS）、防火牆〕可保護這些連接，以阻止 MEC 服務網路、前端行動通信系統和第三方應用服務網路的攻擊，但是這些方案不足以解決由 MEC 引入的新安全問題，例如：運行在 MEC 系統中的惡意應用程式可能意圖與佔用服務網路中的資源，導致使用同一服務系統中的其他應用無法正常運行；而且應用程式還可能透過應用程式介面（Application Programming Interface，API）自由更改前端無線電接取網路的參數配置，這將大幅損害、影響整個網路的性能，儘管有資源隔離機制、配置參數範圍限制和其他解決方案可以緩解攻擊的影響，但它們無法完全排除此威脅。此外由於 MEC 具備 NFV、NS 等網路結構以及透過 API 可提供外部第三方應用服務網路連結等特性，因此也具備從設備本身軟硬體、資料傳輸到傳輸網路、到上層雲端服務應用各層面皆可能面臨多種資安威脅到上層 IT 服務應用等各種弱點及潛在性威脅；包括：不安全的通訊協定、拒絕服務攻擊、中間人攻擊、資訊偽造、隱私洩漏、數據丟失及防護機制不足等在現今一般資通訊設備及網際網路上常見的攻擊或危險都會存在；任何從端到端、系統/網路間所傳輸的資料安全和保護不足都將導致機密性數據被攔截和竊取，輕則影響網路服務能力，重則使用戶權益遭到侵害。

在 5G 網路時代，使通信傳輸設備透過虛擬化（NFV）與軟體化（SDN），達成資源共享，已經成為電信業者們降低建設與營運成本的重要策略，使得如何要求電信業者在採用 NFV 與 SDN 所帶來的優勢的同時，降低伴隨而來的資通安全漏洞與威脅，甚至要求適切的事件應變與處理機制，協同一致的國家網路安全政策，將是 5G 資通安全防禦的一大挑戰。

MEC 結合 5G 基礎建設大量採用雲端虛擬化技術達成網路切片（NS）功能，然而此時系統與軟體運行、軟體版本更新等帶來維運工作將較 4G 更為繁複，3GPP 在 TR 38.811 [118]以及 TR 33.813 [119]針對 NS 的安全有更多的討論與要求，以避免 5G 之 eMBB、URLLC、mMTC 的資通安全風險在雲端虛擬化後更進一步地引發或擴大。美國聯邦通訊委員會（Federal Communications Commission，FCC）在 2016 年的報告《軟體定義網路/網路功能虛擬化之最佳安全通用實行做法建議（Security BCP Recommendations for SDN/NFV）》 [120]中，針對以下 5 類高優先級的領域提出電信業者使用 SDN 的潛在安全威脅，包含：通信資料與訊息被竄改的威脅、基礎設施之軟體或韌體漏洞，使得安全機制與分層隔離失效、DoS 的威脅、不安全的 API、以及未妥善管理授權之威脅，另外，根據 ETSI 文件指出 NFV 所引入的安全威脅 [121]，包含：資料操作（Data manipulation）、權限濫用（Privilege misuse）、封包修改（Package modification）、惡意的虛擬網路功能（Rogue Virtual Network Function）、惡意的程式碼或用戶（Malicious code or tenant）、組態設定修改（Configuration modification）、資源配置議題（Resource allocation issues）、圖像竄改（Image tampering）、目錄資訊之利用（Catalogue information exploit）、上傳惡意圖像（Uploading malicious images），此外 5G 網路可以支援多種接取（Access）技術，如 WiFi（無線區域網路）、專用網路、固網、衛星等，因此 5G 網路相較於 4G，第一進入點（Point of entry）多且種類繁複，且從架構上來看，進入點後即是這些 MEC 服務，因此預料 5G MEC 未來將受到更多攻擊類似於目前網際網路類型的攻擊。

綜合以上所述，本計畫歸納以下多項關鍵議題，深入探討而整理出 MEC 可能引入的安全威脅：

(一)MEC 本身威脅

與傳統行動電信業者網路相比，MEC 在系統架構，服務提供方式和營運模式方面都有很大的變化，對安全性的要求更是產生新的挑戰。在系統結構方面，MEC 節點更貼近用戶，更容易受到物理層面的影響或攻擊，在服務提供方面，受託管多個第三方邊緣計算應用程序需要在不同應用程序彼此間，以及應用程序和網路元件間進行良好隔離，在營運模式方面，需要長期累積行動邊緣計算平臺和第三方應用的協同管理和營運經驗，才能建立完整有效的防禦機制，此外，向第三方合作單位公開網路功能將涉及基本安全問題，如網路安全、服務和用戶數據安全、用戶隱私管理和控制。

(二)針對 MEC 租用戶之雲端應用層的攻擊

由於 MEC 系統設備同時連接行動通訊網路內部元件及外部服務環境，提供 IT 服務環境和雲計算功能，能有效處理行動網路邊緣的服務應用程式。因此部分 MEC 服務應用程式可能需要連結外部雲端網路維持正常功能運行，該第三方應用程式不直接由電信業者控制，存在耗盡網路資源，影響網路正常功能的風險；更可能因導入有設計缺陷的應用程序，容易遭受攻擊或被駭客入侵，甚至埋入惡意應用程式。

(三)MEC 部署帶來的計費風險

在傳統行動通信網路中，計費業務由核心網路（CN）負責〔例如：GPRS 服務支援節點（Serving GPRS support node，SGSN）、PDN Gateway〕，在漫遊時也通常由漫遊網路核心路由回原本籍網路之計費核心元件。此機制可使兩個行動網路都可以持續追蹤記錄用戶使用了多少數據以及使用哪些計費服務，從而助於防止計費錯誤或者故意欺詐，但是在 MEC 中，預計大量數據將直接在 UE 和網路邊緣流動，無需透過核心網路（在漫遊情況下完全不接觸本籍網路），

因此漫遊所在之網路必須依靠 MEC 元件來提供它向本籍網路發送哪些計費記錄,而本籍網路也必須完全依賴這些元件自身的設置/保護機制，由於網路邊緣遠比核心更容易受到攻擊，因此將會產生很大的風險，既有帳單錯誤、帳單欺詐、計費不足固然是一個明顯的風險，但計費過高的情況也可能發生而無法驗證，另外電信業者間的漫遊欺詐也是一個可能問題。

(四)與網路功能在同一平臺上的第三方應用程式

隨 5G 網路功能虛擬化（NFV）的引入，MEC 的一個可能部署模型是邊緣計算應用程式將與某些網路功能使用相同的物理平臺，這些不直接受營運業者操控的第三方應用程式存在獨佔網路資源的風險，還可能因應用程式設計不當、允許駭客滲透到平臺，因此影響平臺網路功能，甚至可能被惡意應用程式滲透操控。

(五)允許第三方應用程式影響網路

在 ETSI 所發布的《行動邊緣計算：邁向 5G 的關鍵技術技術（Mobile Edge Computing: A key technology towards 5G）》 [117]白皮書中，提到可以大幅提升應用程式的效能，可即時提高網路效率和客戶體驗；在某種程度上，這意味著應用程式的收發資料流可能會影響該區 RAN 的配置方式，如果效能提升過高，可能會導致其他用戶的體驗嚴重降低或遭受拒絕服務，無論是偶然還是惡意的，一些不良的應用程式可能會與競爭對手應用程式（及其客戶）搶奪無線資源。

(六)多重接取邊緣計算環境中的用戶平面攻擊

在 5G 系統中導入 MEC 產生的新型網路邊緣架構會將 IP 連接層移近用戶，在這種新架構中，上層服務的運算、儲存和內容傳送

將由位於網路邊緣的應用服務伺服器處理，而且 DNS 解析與持續遞送（Continuous Delivery，CD）功能也將更靠近網路邊緣，在這種新架構中，UE 的 IP 連接一般都將在電信業者網路的邊緣（RAN 中）的伺服器結束，這將緩解許多高畫質視訊服務之端到端（UE 到視訊服務伺服器）的改善延遲挑戰；因為服務內容現在可從儲存於電信業者邊緣網路的應用服務伺服器中的副本傳遞，但這也帶來了新的資安挑戰；如：網路邊緣服務伺服器使用 HTTP/HTTPS〔超文本傳輸（安全）協定，Hypertext transfer protocol (Security)〕的安全威脅、除了針對伺服器和暫存的傳統攻擊外，針對內容暫存的新型攻擊（暫存中毒攻擊）將可能發生，例如，在網路邊緣部署的伺服器其大量暫存容量可能會比傳統部署的容量小得多〔電信業者/CDN（內容遞送網路，Content Delivery Network），暫存通常傾向部署離網際網路出口/入口最近的位置，以服務更多的用戶〕，此類攻擊可能會破壞電信業者承諾的服務水準（service-level）。

(七)在邊緣儲存的敏感性資產或資料

如果儲存在邊緣計算的虛擬化主機的敏感性資產或資料受到偷竊或損害，則攻擊者可能會惡意使用它們以進行欺騙、竊聽或數據操縱等攻擊。

(八)核心和多重接取邊緣運算平臺間的敏感性資料交換

如果在核心網路和多重接取邊緣計算網路間交換敏感性資料時遭受到入侵或攻擊，則攻擊者可能惡意使用那些資料流以連接核心網路進行欺騙，竊聽或數據操縱等攻擊。

(九)與 MEC 協調器（MEC Orchestrator）進行通信的安全性

由於從核心網路到多重接取邊緣計算網路的物理連接常發生在行動網路電信業者的良好防護機房範圍之外，因此實體或邏輯鏈路很容易受到侵入或破壞等威脅，而位在 MEC 內部的 MEC 協調控制器也非常可能遭到破壞，欺騙或修改。

(十)MEC 部署的通信監察要求

通常電信業者必須滿足當地政府組織執法要求，包括 LI 通訊監察和保留數據等需要承載大網路流量能力；此功能通常是由核心網路內的專用單元負責，但是目前從 UE 到網路邊緣的服務應用的流量被設計為避開核心，因此將避過通常的攔截點而無法進行監聽追蹤，如將在 MEC 所在的網路邊緣周圍放置多個 LI 節點，將帶來更多的安全風險，更容易受到攻擊而失效。

第三節傳輸網路（TN）

一、傳輸網路（TN）元件介紹

如下圖 4-6 所描述，隨著 5G NSA 基地臺之擴建，龐大的寬頻資料流量將自基地臺傳輸到核心網路，因此傳輸網路（Fronthaul、Midhaul、Backhaul Transport Network，TN）建設成為 5G NSA 網路建設的關鍵重點之一。當 5G gNB 大量部署時，必須採用有線寬頻網路執行傳輸，5G NSA 無線與有線寬頻網路結合的固定行動網路匯流，成為 5G 商用網路建設主流。

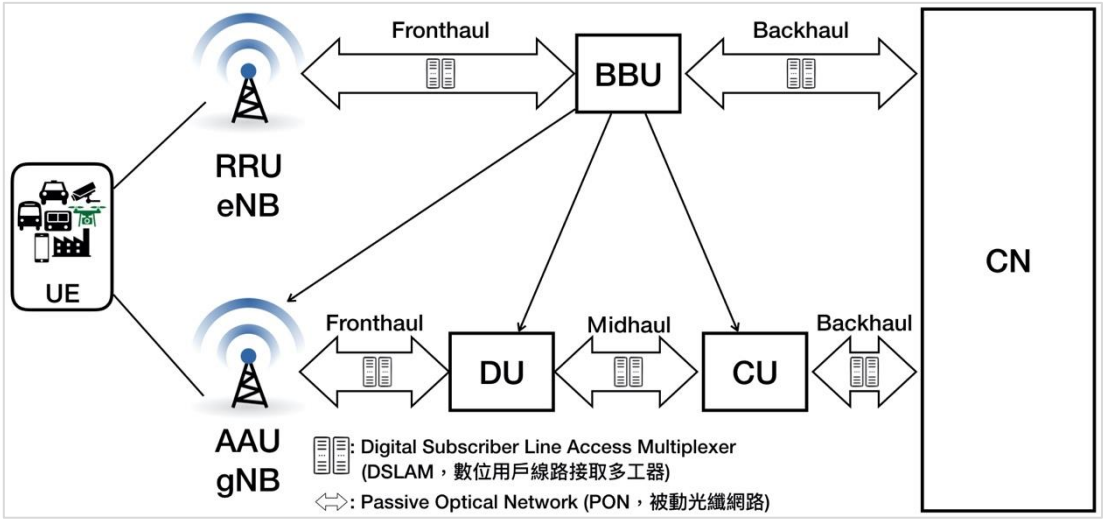


圖 4-6、5G NSA 之傳輸網路實體元件架構

資料來源：本團隊整理

另外由於 5G NSA RAN 隨著基地臺 BBU 功能切分技術的引入，傳統 4G RAN 中的 TN 環境也演變為兩種傳輸模式；其中分離的 DU 和 CU 分別被放置在 5G NSA RAN 中 AAU 的後端以及 EPC 的前端，以提供未來用戶即時性與非即時性垂直應用服務功能，在此架構中，前傳（Fronthaul）網路描述 AAU 和 DU 之間的連接，而新功能中傳（Midhaul）網路用於描述 DU 和 CU 之間的連接，從傳輸技術的角度來說，共用公眾無線電介面（Common Public Radio Interface，CPRI）

將採用波長多工（Wavelength Division Multiplex，WDM）傳輸技術，並部署在 4G RAN 與 5G RAN 前傳（Fronthaul）網路模式中。DU 和 CU 之間的傳輸利用新型之低延遲規範乙太網路。4G RAN 的 BBU 與 5G NSA RAN 的 CU 及 EPC 之間的後傳網路（Backhaul）連接，儘管 5G 網路中用戶平面（UP）與控制平面（CP）的即時資料大量的注入傳輸網路中，亦將利用類似的快速傳輸技術規範來解決時間延遲問題；整體 5G NSA RAN 傳輸網路完整架構如下圖 4-7 描述。

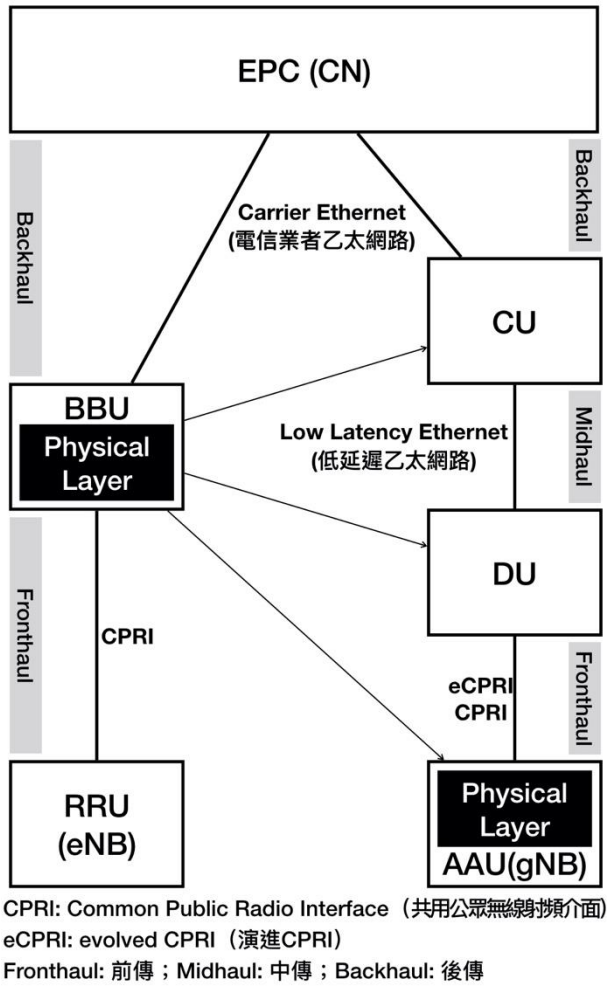


圖 4-7、5G NSA 之傳輸網路示意圖

資料來源：本團隊整理

光纖是目前傳輸網路（TN）建置最普及的傳輸設備，相較於過往的銅纜設備，更具有高頻寬、穩定傳輸、不受電波干擾之優點，使光

纖成為 5G NSA 基地臺於資料聚合與核心網路傳輸之最佳傳輸媒介設備，其特點為光纖可以提供超過 1 Gbps 的傳輸頻寬使用。以 5G NSA 網路為例，當個 5 個基地臺共用一傳輸網路之頻寬為 5 Gbps 時，光纖技術是目前唯一可採用聚合之技術來達到超過 5 Gbps 頻寬需求的傳輸媒介。光纖業者不斷在低成本線路實體與技術進步開發下，光纖通信是可能為部署 5G NSA 傳輸網路的主要角色，亦是傳輸聚合與核心網路（CN）之主要傳輸技術。

二、傳輸網路（TN）可能的威脅

目前 5G NSA 網路的傳輸技術還是是基於 4G 傳輸網路技術發展而來，然而 4G 傳輸網路所面臨之資通安全議題不會因為系統升級至 5G NSA 而全然解決；在無線接取網路與核心網路之間，以及基地臺與基地臺間的相互連接依然繼承 4G 傳輸既存之安全問題，以下將描述 5G NSA 傳輸網路可能面臨之資通安全議題。

(一)傳輸網路竊聽

5G 基地臺採用 CU 與 DU 邏輯分離之雲端化無線電接取網路（Cloud Radio Access Network，C-RAN）部署方式，亦是切分即時性與非即時性資料處理之關鍵技術，但在目前 4G LTE 基地臺架構中，從空中介面解密後，到核心網路（CN）行動管理實體（Mobility Management Entity，MME）端之前，這一段鏈路傳輸並無採取任何加密保護措施，也就是說，電信業者未來的任務為防止惡意者進行 5G 傳輸網路之竊聽攻擊，並且也要確保部署在網路邊緣的 DU 無法接取任何用戶數據。

(二)阻斷服務攻擊

目前分散阻斷服務（DDoS）攻擊的頻率與強度日益升高，由於預期 5G 時代各種 IoT 設備將呈現爆發式的指數型成長，而且較一般終端設備更容易被植入惡意程式或遭駭客入侵；數以百萬計的僵屍設備將用來發動阻斷服務的巨大流量攻擊，如果發生在特定集中或高密度區域，便容易造成傳輸網路頻寬飽和，讓網路效能與可用性大幅下降，甚至造成服務無法運作；此外，攻擊者也可能利用終端在開始接入基地基地臺過程進行用戶身份轉移，通過中間人方式來偽裝其他用戶發起阻斷服務攻擊。

(三)數據完整性攻擊

由於標準未強制規定，現行 LTE 傳輸網路從空中介面解密後到核心網路間並無任何加密保護機制要求，而且用戶平面之數據資料也沒有完整性保護機制，此外在控制平面的數據上，也缺乏完整性與不可否認性的安全保護；另外 5G NSA 必須考慮與現有 LTE 系統網路的相容性，仍使用既有的傳輸標準，容易遭受惡意人士竄改攻擊，竊取其個人資料與權限，故在 5G 中，電信業者除了需要保障其客戶之用戶平面的完整性外，同時也要強化跨電信業者間之國際漫遊傳輸網路邊界上的驗證保護機制。

電信業者在建置 5G 基地臺所採用的傳輸網路時，若以專線連接之封閉性網路，將不會啟動網際網路安全協定（IPsec）保護功能。然而針對 5G 基地臺之傳輸網路加密技術，可分為開放式與非開放式網路兩種形式建置，其中開放式網路將會開啟 IPsec 功能進行防護，並新增了 DTLS over SCTP（Datagram Transport Layer Security protocol over the Stream Control Transmission Protocol，保護控制信令傳輸），為提升用戶隱私性保護強度，在 5G NSA RAN 建置架構上，不論 CU 端、DU 端、MME 端之前皆可以設置安全閘道器（Security Gateway）來進行整體傳輸網路安全性管理及防護措施，對於啟動 IPsec 功能而影響到整體網路承載量問題，電信業者可以透過增加傳輸網路頻寬方式來克服此問題。

第四節 核心網路 （CN）

核心網路（Core Network，CN）建設成本對業者也是一筆不可小覷的支出，故在 5G 建設初期延用 4G 時代的核網，轉為全力建設 5G 基地臺，同時提升傳輸網路的容量是相當合理的策略。在**第肆章 第一節-5G NSA RAN** 網路元件介紹中，本案報告已經說明 5G NSA 架構的核心網路是 4G 的 EPC 核心網路搭配 4G 基地臺作控制平面的傳輸，5G 基地臺僅作為高頻寬的輔助通道。

一、核心網路 （CN）元件介紹

3GPP TS 33.501 在討論核心網路架構時 [7]，忽略不談外部數據網路（Data Network，DN）這個部分，但是本計畫認為有必要在核心網路章節添加上去，因為第三方設備商所提供之外部服務應用或加值服務系統（如 IMS - IP 多媒體子系統、來電答鈴、多媒體影音等）等也是業者在核心網路的重要子系統。雖然 3GPP TS 23.501 [9]與 TS 33.501 [7]只專注提供網路層的接取服務，5G 核心網路只要使得 UE 能夠連接上目的伺服器即完成工作，並不處理上面乘載的業務，對 5G NSA 核心網路（或者更精確的說是 EPC 核網而言），無論是 VoLTE（透過長期演進技術傳輸之語音，又稱為高品質語音通話)語音業務、數據業務或者簡訊業務等都不是 EPC 核網處理的範圍，這些業務現在大多移到 IMS 子系統處理。而在 5G 時代，這些業務會更加多元化，例如網頁快取、車聯網等特定應用。

EPC 的網路架構及重要網路元件介紹如下圖 4-8 所示：

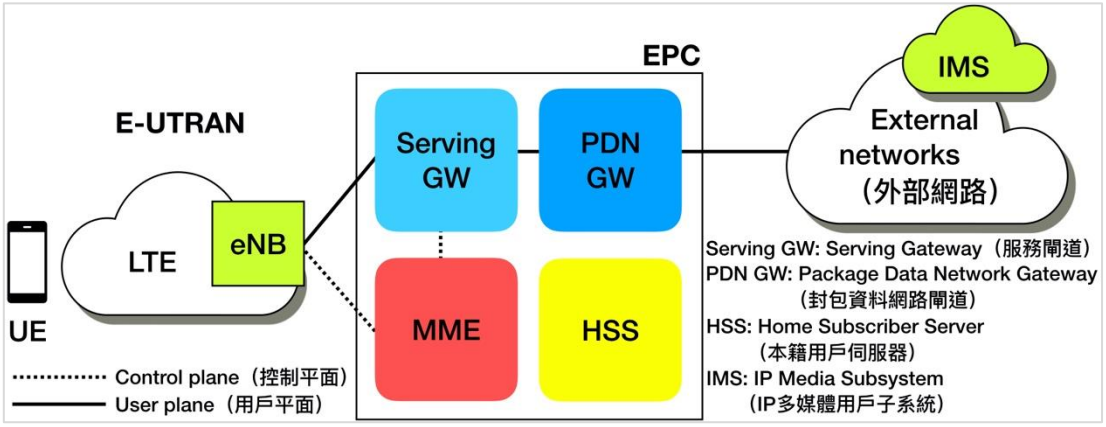


圖 4-8、5G NSA 之核心網路實體元件架構

資料來源：3GPP、本團隊整理

(一)行動管理實體（Mobility Management Entity，MME）：

為核心網路實際管理用戶終端的元件，負責移動性管理、入網程序、用戶身份驗證、呼叫和會話建立、以及功能授權與安全性等控制訊號（Control Signaling）管理。

(二)服務閘道器（Serving Gateway）：

做為無線電接取網路和核心網路的主要互連點，主要功能是傳遞用戶資料，通過路由機制傳送用戶數據封包，與 PDN（Package Data Network，PDN）GW 共同負責處理用戶平面，在用戶設備（UE）和外部網路之間傳輸數據流量，也提供與其他系統間（如 2G、3G）相容切換之接入錨點。

(三)封包數據網路閘道器（Packet Data Network Gateway，PDN Gateway）：

主要負責用戶 IP 位址分發，路由用戶封包數據至網際網路或其他專屬網路，並提供策略與控制決策（Policy and Rules）、監控流

量、品質控管（Quality of Service，QoS）及計費機制（Charging），同時相容非 3GPP 系統〔如 WiFi、WiMAX(Worldwide Interoperablity for Microwave Acess，全球互通微波接取)〕切換。

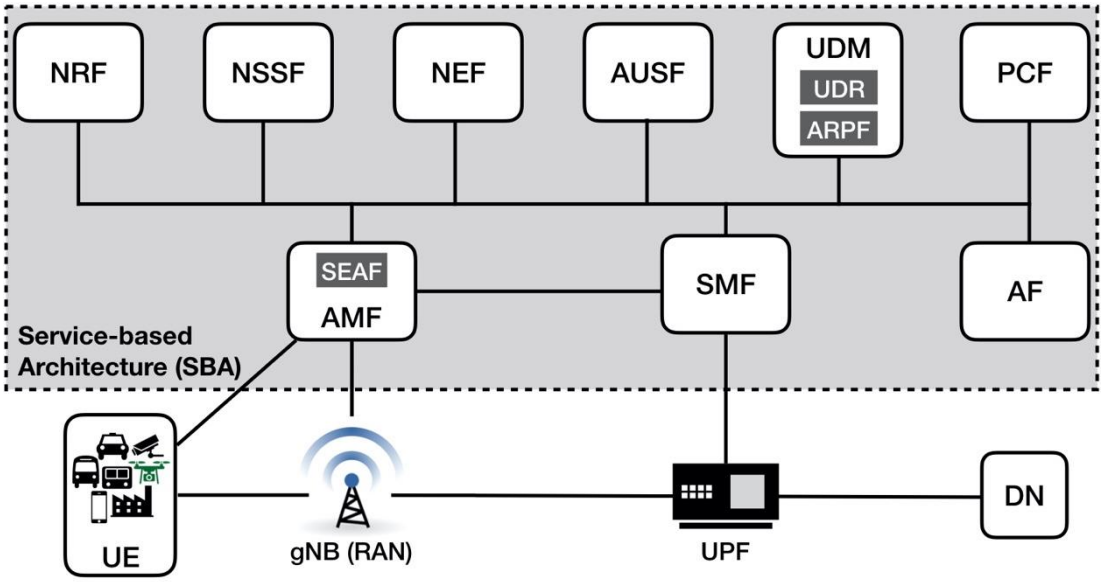
(四)本籍用戶伺服器（Home Subscriber Server，HSS）：

為一個包含用戶相關資訊的中央資料庫，主要功能涵蓋行動位置紀錄、通話與會話建立、用戶入網時的驗證、加解密機制與接取授權。

(五)IP 多媒體子系統（IP Multimedia Subsystem，IMS）：

一個基於 IP 網路協定提供 VoLTE 語音及多媒體業務的子系統架構，作為取代 2G/3G 傳統電路交換語音服務。IMS 基於會話初始化協定（Session Initiation Protocol，SIP），支援行動通訊網路與固網，提供語音、視訊、數據整合平臺，IMS 能協助電信系統業者，提供更多創新的多媒體服務給用戶。

根據 3GPP TS 23.501 [9]所述之內容，新的 5G 核心網路使用類似雲端技術之服務導向架構（Service-based Architecture，SBA），該架構支援控制平面（CP）功能的交互性、可重用性、靈活性之連接與服務，5G 核心網路與 4G 核心網路中對應之功能有類似之處，例如：與用戶進行通訊、存儲、訂閱以及驗證等，並且允許接取外部網路與服務，提供安全性、網路管理、接取以及移動性。5G 核心網路利用了許多新的網路功能（Network Function，NF） [8] [7] [11]，這些新的網路功能主要包括下列各項與圖 4-9 所示：



SBA：Service-based Architecture，服務導向架構
AMF：Access and Mobility Management Function，存取及移動性管理功能
SEAF：SEcurity Anchor Function，安全固定功能
SMF：Session Management，會話管理功能
UPF：User Plane Function，用戶平面功能
PCF：Policy Control Function，策略控制功能
AUSF：Authentication Server Function，身份驗證伺服器功能
DN：Data Network，數據網路
UDM：Unified Data Management，統一數據管理
UDR：Unified Data Repository，統一數據貯存
ARPF：Authentication credential Repository and Processing Function，身份驗證憑證貯存與處理功能
AF：Application Function，應用功能
NEF：Network Exposure Function，網路開放功能
NRF：Network function Repository Function，網路功能貯藏功能
NSSF：Network Slice Selection Function，網路切片選擇功能

圖 4-9、服務導向之 5G 核心網路功能架構

資料來源：3GPP、本團隊整理

(一)接取和移動性管理功能（Access and Mobility Management Function，AMF）

NAS（Non-access Stratum，非接取層）信號的終止點，NAS 信令機密性和完整性保護，註冊管理，連接管理，移動性管理，接取身份驗證和授權，安全上下文（Security Contexts）管理。

(二)安全固定功能（Security Anchor Function，SEAF）

位於 AMF 中，是保管、儲存最高權限密鑰（Root key，也稱為 Anchor key）的地方。

(三)會話管理功能（Session Management Function，SMF）

會話管理（會話建立、修改、發布），用戶 IP 地址分配和管理，DHCP（Dynamic Host Configuration Protocol，動態主機配置協定）功能，與會話管理有關的 NAS 信號終止，下傳（Downlink）數據通知，UPF 的流量控製配置正確流量路由。

(四)用戶平面功能（UPF）

分組路由和轉發以及分組檢查，QoS 處理，充當與數據網路（DN）互連的外部 PDU 會話點，並且是無線電接取技術（Radio Access Technology，RAT）內部和 RAT 間移動性的錨點。

(五)策略控制功能（Policy Control Function，PCF）

統一的策略框架，為控制平面（CP）功能提供策略規則，控制用戶進行策略決策。

(六)身份驗證伺服器功能（Authentication Server Function，AUSF）

作為身份驗證伺服器。

(七)統一數據管理（Unified Data Management，UDM）

利用儲存於 UDR 內的用戶資訊來支援身份驗證和密鑰協議（Authentication and Key Agreement，AKA）、憑證的生成、用戶標識處理、接取授權、用戶訂閱管理

(八)統一數據儲存（Unified Dada Repository，UDR）

位於 UDM 中，用於儲存用戶資訊。

(九)身份驗證憑證儲存與處理功能（Authentication credential Respository and Processing Function，ARPF）

位於 UDM 中，可提供儲存驗證憑證功能。

(十)應用功能（Application Function，AF）

處理服務應用對流量路由的影響、接取 NEF（Network Exposure Function，網路開放功能），並根據策略框架協助執行策略控制。

(十一)網路開放功能（NEF）

支援能力和事件顯露，從外部應用程序到 3GPP 網路的安全資訊提供，內部/外部資訊的轉換。

(十二)網路功能貯藏功能（Network function Repository Function，NRF）

負責 NF 應用探索，維護 NF 運行準則和可用的 NF 案例。

(十三)網路切片選擇功能（Network Slice Selection Function，NSSF）

選擇適合用戶服務的網路切片，確保的網路切片選擇輔助資訊（Network Slice Selection Assistance Information）的正確性，決定要用於用戶服務 AMF。

為了促進實現不同的網路服務和需求，NF 必須進一步簡化，其中大多數是基於軟體特性，因此可以根據需要進行調整。現有網路中閘道器集成了用戶平面（UP）以及控制平面（CP）的部分功能，在 5G 時代，對於低延遲的要求以及支援眾多裝置的龐大運行業務中，閘道器需要下移到機房中心，造成閘道器數量增加多達 20 至 30 倍，若保持現有的閘道器架構，則必然會增加閘道器業務配置的複雜性，大幅提升電信業者網路的成本支出（Capital Expenditure，CAPEX）和（Operating Expense，OPEX）。同時，如果 CP 記錄了用戶的位置資訊，且 RAT 回報了時間的資訊，將會產生大量資料需於基地臺處理，且數量眾多的閘道器、統一集中化的 CP 帶來顯著的傳輸介面互連和

切換/更新信令的負荷，將進而加重閘道器的負擔，因此需要對閘道器的 CP 及 UP 進行分離（CUPS），CUPS 不僅可以有效降低分布式部署帶來的成本壓力，同時也可以減緩閘道器傳輸介面的負擔，此外，CUPS 是支援用戶平面和控制平面的獨立彈性，進一步提升了網路架構的靈活性，且容易運用網路切片以及多樣化服務之應用。

CUPS 首先要做到功能輕量化，分離複雜的控制邏輯功能並集中到 CP 中；其次要對核心的基本用戶平面功能進行模型建置，定義出具通用的用戶平面模組，以實現可程式編譯的轉傳邏輯，支援良好的擴展性。CP/UP 分離後，兩者之間的傳輸介面可以採用 GTP〔General Package Radio Service （GPRS） Tunneling Protocol，通用封包無線電服務洞道協議〕之增強協議，CP 基於用戶接取類型等，來決策出針對用戶服務的業務安排，再經由 GTP 傳輸介面發送給用戶平面，用戶平面基於業務特性向 CP 發送相關資訊。

在面對業務特性之 5G 網路架構中，可以將邏輯控制功能抽象解讀成獨立的網路功能，這些獨立的網路功能可以根據業務需求靈活的組合。網路功能元件及其他元件在邏輯功能上環環相扣，且網路功能支援中立化的傳輸介面，可以透過相同的傳輸介面向其它網路功能調用元件以提供服務，將多個相扣的傳輸介面轉變為單一傳輸介面從而減少了傳輸介面數量。

網路功能管理框架提供網路功能的註冊、監控等管理功能，其特性使得在新增或升級 5G 網路功能的過程中，能確保現有的網路服務不受影響，相較於現有之緊密耦合網路控制功能，元件化的 CP 架構透過網路功能的靈活安排及即插即用大大簡化 5G 新業務的拓展及上線時程，為 5G 網路端到端切片的功能奠定了基礎架構。

5G 核心網路有著服務管理框架的規範下，CUPS 使得網路狀態資訊可以集中儲存在統一數據庫中，任何網路功能都可以通過標準傳輸介面與數據模型進行接取，並將相關的動態用戶數據資訊保存至本地網路，如此一來能夠減緩過去在分布式數據庫時的同步成本，而網路狀態資訊也能夠實現跨數據中心的即時備份。

二、核心網路 （CN）可能的威脅

首先是 5G 核心網路與營運作業（OAM）管理威脅，這是因為 5G NSA 核心網路延續自 4G 核心網路，為一扁平且 IP 化的網路結構，倘若管理不善，會影響後續各項業務，如用戶驗證、接取授權、IP 位址分配、移動性相關信令、QoS 和安全性相關信令處理和計費等。

另一方面，談到外部資料網路（DN），外部服務指電信業者對外連接的各種外部服務部分，包含了行動網路的 IMS 服務子網路、漫遊至其他電信業者的行動網路、以及連接網際網路等部分，其主要威脅如下：

(一)IP 多媒體子系統（IMS）威脅

根據 3GPP 定義，IMS 是一種提供多媒體（語音，視訊，數據等）的服務子系統，而不管行動通訊網路中使用的接入類型、服務提供商或用戶設備，IMS 中的安全管理尤為重要，因為它對 QoS、計費及應用程序的啟用都有影響，其主要安全威脅包括未經授權的接取、服務濫用、盜竊服務、及網路竊聽與會話脅持等。

1. 未經授權的接取：IMS 的開放和分布式架構產生了眾多必須保護的節點，各服務供應商會提供不同的服務或是具有不同的安全標準，其對於 IP 的授權連接管理通常位於不具高度安全性的區域，這可能使 IMS 核心易受攻擊。大量的多媒體流

資料量需要可靠的保護機制，以免受經網際網路跨接多個技術子系統的攻擊。

2. 服務濫用與盜竊服務：這意指用戶服務權益受損以及行動業者的收入損失。服務濫用是通過訂戶獲得比分配給用戶的服務更多的服務來實現的。 攻擊者可以通過受感染的 UE 接取 IMS，並不在 UE 和 IMS 核心之間釋放建立的媒體流，導致攻擊者繼續保持與媒體流的連接時系統不會計費。

3. 網路竊聽與會話脅持：攻擊者攔截 SIP 會話中兩個用戶之間的數據傳輸，如果沒有網路保護，攻擊者可以使用 Wireshark 等工具捕獲 SIP 信令，會話劫持涉及攻擊者插入惡意數據包，替換流量和破壞完整性，影響 QoS。由 SS7 或 Diameter 所引起一系列安全問題已經獲得監理機關與各大電信業者的關注，例如 SS7 中的簡訊服務（Short message service，SMS）竊取或通話竊聽攻擊等。有鑑於 5G 系統也需要與其他通信系統保持互通，故依然會引入上述安全議題。

(二)5G 功能暴露

5G 可將其核心網路驗證功能與無線電接取網路之連線功能向外暴露給垂直應用業者，以提供更全面的服務整合，如密鑰生成、驗證，接取控制等，這些暴露之功能可能帶給攻擊者更多能力與機會，利用旁通道攻擊，攻擊存在同一實體資源的用戶。

(三)竊取用戶身份

5G 中提供輔助身份驗證功能，用於對電信業者外的第三方服務商（如影音服務或銀行服務）進行身份驗證，甚至金流付費功能。

故攻擊此身分驗證機制，除了可以大量取得用戶行動數據外，還可竊取其個人存放在其他服務商的資料與權限，甚至金錢。

第五節 本章總結

本章節將 5G 網路系統分為四大區塊來敘述，分別為無線電接取網路（RAN）、多重接取邊緣運算（MEC）、傳輸網路（TN）與核心網路（CN），主要介紹各個區塊的元件、功能及威脅等，下表 4-1 綜整了上述內容：

表 4-1、四大區塊威脅風險總表

類別	威脅種類	內容簡述
無線電接取網路（Radio Access Network，RAN）	實體層（Physical Layer）攻擊	• 5G 將大量引入並安裝更便宜的小型基地臺。這些安裝在公共場所的基地臺較容易遭受物理破壞，並允許攻擊者實體接觸基地臺的網路介面。
	用戶隱私資料竊聽與阻斷服務（DoS）攻擊	• 國際行動用戶識別碼擷取器（IMSI-Catcher）的出現，導致用戶隱私被攔截、竊聽的威脅。 • 攻擊者可能利用 UE 在開始接入基地臺過程中，通過中間人攻擊來偽裝用戶，竊取客戶流量或發起阻斷服務（Denial-of-service，DoS）攻擊。
	惡意基地臺	• 攻擊者可以試圖將惡意基地臺引入網路，模擬電信業者的節點，並攔截來自 UE 的語音和數據傳輸，達到竊聽或重新導向用戶到不同的網路。
	數據完整性攻擊	• 在 4G 網路中，用戶平面（User plane）之數據傳輸，並沒有完整性保護機制。 • 控制平面（Control plane）的數據也缺乏完整性與不可否認性的安全保護。
	空中介面（Air Interface）威脅	• 空中介面之安全性仰賴於位元層級之串流加密法（Bit-level Cryptographic），倘若密鑰長度及加密演算法強度不足將導致竊聽、中間人攻擊等可能性。
多重接取邊緣運算	MEC 本身威脅	• 系統結構方面，MEC 節點更貼近用戶，更容易受到物理層面攻擊。

類別	威脅種類	內容簡述
（Mobile Edge Computing，MEC）		• 服務提供方面，受託管多個第三方邊緣計算應用程序需要在不同程序間、以及網路元件間進行良好隔離。 • 營運模式方面，需要長期累積 MEC 平臺和第三方應用管理和營運經驗，才能建立完整有效的防禦機制。
	針對 MEC 租用戶之雲端應用層的攻擊	• MEC 可能需要連結外部雲端網路，不直接由電信業者控制，存在耗盡網路資源的風險。 • 可能因應用程序缺陷導致遭受攻擊或被駭客入侵，甚至埋入惡意應用程式。
	MEC 部署帶來的計費風險	• MEC 中大量數據直接在 UE 和網路邊緣流動，遠比核心更容易受到攻擊，可能產生帳單錯誤、帳單欺詐、計費不足等風險。
	與網路功能在同一平臺上的第三方應用程式	• 隨 5G NFV 引入，MEC 可能將邊緣計算應用程式與網路元件結合於相同平臺，存在獨佔網路資源的風險外，還可能因應用程式設計不當、被惡意程式滲透操控。
	允許第三方應用程式影響網路	• 一些不良應用程式可能會搶奪無線資源，導致其他用戶的體驗嚴重降低或遭受拒絕服務。
	多重接取邊緣計算環境中的用戶平面攻擊	• 網路邊緣服務伺服器使用 HTTP/HTTP 協定，存在既有弱點，除伺服器和暫存的傳統攻擊外，針對內容暫存的新型攻擊（暫存中毒攻擊）也將可能發生，
	在邊緣儲存的敏感性資產或資料	• 儲存在邊緣計算的虛擬化主機的敏感性資產或資料較容易遭到偷竊或損害。
	核心和多重接取邊緣運算平臺間的敏感性資料交換	• 如果在交換敏感性資料時遭受到入侵或攻擊，則攻擊者可能連接核心網路進行欺騙，竊聽或數據操縱等攻擊。

類別	威脅種類	內容簡述
	與 MEC 協調器進行通信的安全性	• 邊緣計算網路的物理連接常發生在良好防護機房之外，因此實體或邏輯鏈路很容易受到侵入或破壞。
	MEC 部署的通信監察要求	• 在 MEC 的網路邊緣周圍放置多個 LI 節點，將帶來更多的安全風險，更容易受到攻擊而失效。
傳輸網路（X-haul Transport Network，TN）	傳輸網路竊聽	• 目前 LTE 基地臺架構中，從空中介面解密後，到核心網路（CN）之前的鏈路傳輸並無採取任何加密保護措施。 • 針對 5G 基地臺開放式網路將會開啟 IPsec 功能進行防護，並新增 DTLS 以提升用戶隱私性保護強度。
	阻斷服務攻擊	• 由於 5G 時代物聯網設備將呈現指數型成長，而且較一般終端設備更容易被植入惡意程式或遭駭客入侵；數以百萬計的僵屍設備將用來發動阻斷式巨大流量攻擊，讓網路效能與可用性大幅下降，甚至造成服務無法運作。
	數據完整性攻擊	• 現行 LTE 傳輸網路從空中介面解密後到核心網路間並無任何加密保護機制要求，並使用既有老舊的互聯傳輸標準，容易遭受惡意人士竄改攻擊，竊取其個人資料與權限。
核心網路（Core Network，CN）	IP 多媒體子系統（IMS）威脅	• 未經授權的接取：IMS 的開放和分布式架構產生了眾多必須保護的節點，通常位於半可信區域，這可能使 IMS 核心易受攻擊。 • 服務濫用與盜竊服務：攻擊者可通過受感染的 UE 接取 IMS，導致攻擊者繼續保持與媒體流的連接時系統不會計費。 • 網路竊聽與會話脅持：攻擊者攔截 SIP 會話中兩個用戶之間的數據傳輸，劫持並插入惡意數據包，替換流量和破壞完整性，影響 QoS。
	5G 功能暴露	• 5G 將其核心網路驗證功能與無線電接取網路之連線功能向外暴露給垂直應用業者，攻

類別	威脅種類	內容簡述
		擊者可利用旁通道攻擊，攻擊存在同一實體資源的用戶。
	竊取用戶身份	· 5G 中提供輔助身份驗證功能，當此身分驗證機制遭受攻擊，除可取得用戶行動數據外，還可竊取其個人的資料與權限，甚至金錢。 · 由 SS7 或 Diameter 所引起一系列安全問題已經獲得監理機關與各大電信業者的關注。鑑於 5G 系統也需與舊系統保持互通，故依然會引入上述安全議題。

資料來源：本團隊整理

本計畫將 5G 網路安全風險威脅分成四大區塊來探討，分別為 RAN、MEC、TN 與 CN，並於本章節評估出四大區塊可能面臨的風險，其中技術性風險為主，以非技術面為輔，可作為業者未來在擬定資產盤點、風險評估及資通安全防護控制措施時的參考依據，亦是本計畫擬定「行動寬頻系統審驗技術規範」資安查驗項目的參考依據。除技術議題以外，管理面議題風險威脅如資產、供應鏈、存取控制、異常偵測、回復計畫等，也是重點之一。上述之技術面與非技術面的風險與威脅均可以在資通安全維護計畫參考框架應載明事項 17 項（詳如附第伍章）中找到相對應之風險管理因應方向；以供應鏈風險評估流程為例，該流程必須對各元件之第三方軟硬體包含 5G 系統營運之軟硬體資源之上下游供應鏈管理，包含資安政策與管理措施之布達規劃，如有供應鏈如涉及國防安全或敏感國家等，應依據通傳會要求說明供應鏈資格審核並強化資安管控措施。

ISO 27001 為常見用於 IT 系統之資通安全管理系統的標準，為一通用性的標準，而資通安全維護計畫考框架則是考量 5G 網路之特性，

包含網路功能軟體化，以達到網路功能的快速擴充與彈性，並從運算、存儲及軟體運作的角度，考量 5G 網路將納入更多元與廣泛的資訊技術與通訊技術，載明 17 項資通安全維護義務之要求，故 ISO 27001 無法完全適用於 5G 網路之資訊安全管理，但資通安全維護計畫應載明事項中，ISO 27001 部分內容可對應到應載明事項，而未直接對應部分係為附錄 A 之控制項，而控制項可供各家業者在規劃資通安全防護措施時，參考並選用適合之之控制項作為防護措施，故未直接對應之部分係由業者依規劃選擇適用之控制項。

表 4-2、資通安全維護計畫應載明事項與 ISO 27001 之對應

資通安全維護計畫應載明事項	ISO 27001:2013
1. 資通安全政策及目標	4.1 瞭解組織及其全景 4.2 瞭解關注方之需要及期望 5.2 政策 6.2 資訊安全目標及其達成之規劃 A.5 資訊安全政策
2. 核心業務及其重要性	A.17 營運持續管理之資訊安全層面
3. 行動寬頻系統資通安全維護範圍	4.3 決定資訊安全管理系統範圍
4. 資通安全組織	5.3 組織角色、責任及權限 7.2 能力 7.3 認知 7.4 溝通或傳達
5. 專責人力及經費之配置	7.1 資源 A.7 人力資源安全
6. 資通安全長之配置	5.1 領導及承諾 7.4 溝通或傳達
7. 資訊及資通系統之盤點規劃（含系統設備符合 ITU 或 3GPP 發布之資通安全規定）	A.8 資產管理

8. 資通安全風險評估	6.1 因應風險及機會之行動 8.2 資訊安全風險評鑑 8.3 資訊安全風險處理
9. 資通安全防護及控制措施	6.1 因應風險及機會之行動 6.2 資訊安全目標及其達成之規劃 8 運作 A.5 ~ A.18 適用之控制項
10. 資通安全事件通報、應變及演練相關機制	A.16 資訊安全事故管理 A.17 營運持續管理之資訊安全層面
11. 資通安全情資之評估及因應機制	A.6 資訊安全之組織
12. 資通系統或服務委外辦理之管理措施	A.15 供應者關係
13. 所屬人員辦理業務涉及資通安全事項之考核機制	A.7 人力資源安全
14. 資通安全維護計畫與實施情形之持續精進及績效管理機制	9 績效評估 10 改善
15. 資通安全偵測與防護之建置及執行方案（含資通安全防護架構、防禦縱深及其建置時程）	A.5 ~ A.18 適用之控制項
16. 執行前述執行方案所蒐集、儲存、處理及利用用戶資料之安全保護措施	A.18 遵循性
17. 通過資通安全管理驗證之執行方案	4.4 資訊安全管理系統 7.5 文件化資訊

資料來源：本團隊整理

第伍章　「行動寬頻業務管理規則」修正草案

5G 網路為我國未來最重要之資通訊基礎建設，為加速與完備 5G 網路資通安全發展，敦促電信業者依據我國電信法規及行動寬頻業務監理要求，評估資通安全威脅和風險，建立 5G 網路及資通安全政策，以確保自建和（或）租用網路之機密性、完整性、可用性、適法性及可靠性。通傳會爰依據電信法第 14 條第 6 項及「行動寬頻業務管理規則」第 40 條第 5 項規定，並參酌資通安全管理法第 10 條及施行細則第 6 條意旨，行動寬頻業者於業務籌設或事業計畫書變更時，應向通傳會提出「資通安全維護計畫」，敘明建構網路及資安防護機制之時程、人力、資源配置、風險評估及維護規劃等事項，另外，通傳會為因應 5G 網路發展之需，擬修訂「行動寬頻業務管理規則」，需增訂 5G 網路建設之開臺門檻及建設義務等相關規定，俾使通傳會充分掌握與瞭解電信事業 5G 網路資通安全防護規劃，確保業者設置 5G 網路之信任、可靠及安全性，保障消費者權益，維護新興垂直應用場域與創新服務穩定發展。

有鑑於 5G 網路面臨之資通安全與國家安全威脅較 4G 網路更嚴峻且多元，為完備我國 5G 系統建設與相關產業發展，第一波 5G 頻譜得標者需負擔公共義務，於申請籌設許可時，提報 5G 系統設置之「第五代行動通信系統資通安全維護計畫」。

該資通安全維護計畫要求得標者應載明通傳會於 108 年 9 月 3 日修正公告之「行動寬頻業務管理規則」第 40 條規定之 17 項資安維護義務，並自述「資通安全維護計畫」具體可行措施，為引導業者正確研擬該計畫，本團隊研析相關資料並與通傳會討論，研提「資通安全維護計畫參考框架」供業者參酌，據以要求 5G 頻譜得標者之「資通

安全維護計畫」應包含「行動寬頻業務管理規則」第 40 條規定要求之 17 項應載明事項。

第一節 第五代行動通信系統資通安全維護計畫參考框架

一、前言

(一)依據

行動寬頻演進至第五代行動通信系統(以下簡稱 5G 系統),其創新的架構與技術,不僅進一步提升超寬頻傳輸速度,更是要提供大規模的傳輸容量與超低延遲的傳輸品質。這些能力將成為推動與支援數位時代下各種新興服務與創新應用,如物聯網、智慧交通、智慧工廠與智慧醫療等的關鍵基礎建設。因此,世界各國在要達到數位國家、數位經濟與第四代工業革命的願景上,於促進產業轉型與發展的政策都是以 5G 系統為發展基磐,以打造數位國家創新生態的目標。

為此,5G 系統在架構設計上就是以具備強大功能擴充彈性為理念,以因應未來各種潛在應用服務為目標,包含導入無線電接取網路之 CUPS、以服務為根基的核心網路架構、網路切片(Network Slicing, NS),以及邊緣運算的設置型態。因此,不同於 4G 系統架構,5G 系統高程度地將過往硬體為主的網路系統設置模式做大幅的分解,將網路功能軟體化(Network Function Softwarization),以達到網路功能的快速擴充與彈性。從運算、存儲及軟體運作的角度,5G 系統將納入更多元與廣泛的資訊技術(Information Technology,IT)與通訊技術(Communications Technology,CT)以及平臺與產品在整體網路營運及服務提供上面。對電信業者而言,這些新穎的架構與開放除將帶來成本和部署的敏捷性外,同時亦將使得 5G 系統面臨更為複雜與多元之資通安全風險與威脅。5G 網路時代,各種網路設備將會與新穎開放之電信網路連結,亦為資訊科技會與維運科技(Operation Technology,OT)結合,電信業者也必須更關注 OT 設備的安全性;

此外，5G 將是未來國家發展重要的關鍵基礎設施，確保 5G 網路端對端的資料傳輸安全，也同樣不可忽略。

5G 資通安全可以從制度面和管理面以及技術面三個層次闡述，但最重要的內涵就是要做到 Security By Design（預設安全），也就是說，要求所有電信業者在進行 5G 網路建設之初，就必須納入資通安全防護機制，未來在營運時，也具備足夠的資通安全防護能量，真正做到確保 5G 網路的安全性，也可以進一步做到促進各種垂直應用場域及創新應用服務的發展。通訊網路是我國八大關鍵基礎設施之一，為完備 5G 系統建設與相關產業的發展，第一波釋照得標者需負擔公共義務。**通傳會爰依據電信法及行動寬頻業務管理規則第 40 條第 5 項載明得標者應行之資通安全事項**，於得標後申請籌設許可時，應向通傳會提報 5G 系統設置「事業計畫書」與「第五代行動通信系統資通安全維護計畫」。其中後者載明 17 項資通安全維護義務之要求，敘明業者所設置之 5G 系統之資通安全防護政策、目標、範圍、措施等之時程、人力與資源配置、流程管理、風險評估及設置等事項，確保得標者所設置的 5G 系統是安全、可信賴的，以保障我國關鍵基礎設施之資通安全及消費者權益，鼓勵創新服務與健全電信產業發展。

5G 主要來自於資訊科技與維運科技的結合，因此「第五代行動通信系統資通安全維護計畫」在技術面的部分，參考了國際標準組織 3GPP 與美國 NIST：Cybersecurity Framework 的規範；在管理與制度面，則參考了 2019 年 5 月歐盟與北約組織舉辦 5G 安全會議結論的「布拉格提案」（Prague Proposals）以及在 10 月公布的「歐盟 5G 網路安全風險評估報告」（Report on the EU Coordinated Risk Assessment on Cybersecurity in Fifth Generation Networks），透過上述的各種參考指引，協助臺灣的電信業者聚焦 5G 資通安全風險議題，並要求得標電信業者需提出相對應的解決方案。5G 是發展中的新興技術，通傳

會亦首度要求 5G 得標業者，須自述對於 5G 資通安全的管理政策，以及提供 5G 行動網路服務想要達到的營運目的，希望透過由業者自行撰寫相關的 5G 資通安全維護計畫，讓業者真正瞭解並降低 5G 資通安全的風險管理困難度。此外，在 5G 正式營運後，通傳會將扮演稽核監理的角色，並且透過適當的監理以確保 5G 網路的安全可靠。

(二)5G 系統設置之風險、威脅及挑戰

根據 3GPP 標準文件，本參考框架可將 5G 系統設置概分為無線電接取網路（Radio Access Network, RAN）、多重接取邊緣運算（Multi-access Edge Computing, MEC）、X-Haul 傳輸網路（X-Haul Transport Networks (X-Haul, TN), 包含 Fronthaul, Midhaul, and Backhaul transport networks）以及核心網路（Core Network, CN）四大區塊，如下圖所示。

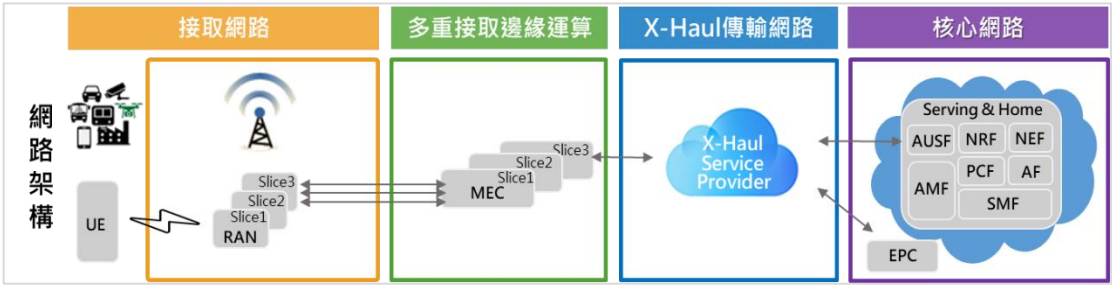


圖 5-1、5G 系統架構圖

資料來源：本團隊整理

5G 系統架構因為採取網路功能軟體化的做法，我們預期未來 5G 系統將會有大量的軟體功能模組，如軟體定義網路（Software-Defined Network, SDN）、網路功能虛擬化（Network Functions Virtualization, NFV）、網路切片、基地臺基頻單元（Base Band Unit, BBU）邏輯分離等，亦即在配合包括網路控制功能軟體化、網路化等設計下，將大幅度地導入資訊技術與通訊技術之軟硬體及平臺，此舉將使網路功能元件與元件間之實作及連接介面更開放與具備互通、整合與擴增的彈性。然而 5G 系統建置並非一蹴可幾，得標者多半將分階段進行，例如建

置初期預期會以非獨立（Non-Standalone, NSA）形式為主，亦即先行佈建 5G 系統之無線電接取網路，並與現行 4G 系統整合以提供 5G 服務，再於下一階段逐步導入 5G 系統之核心網路功能，提供獨立（Standalone, SA）形式之 5G 服務。

以 5G 系統為發展基磐，5G 系統將扮演促進創新服務與市場及推動我國含括國家、社會、經濟、產業、企業及國民在增進數位競爭力與優勢的重要角色。因此，5G 系統架構的設計理念就是以能夠彈性並快速支援未來各種可能的新興應用服務及其設置型態為核心，其中無線電接取網路採取分離傳統基地臺基頻單元為中央單元（Centralized Unit, CU）與分布單元（Distributed Unit, DU）；多重接取邊緣運算利用前端無線電接取網路結合雲端運算資源，在網路邊緣提供資訊技術與通訊技術融合的快速與敏捷性的服務提供；核心網路的設計更是以服務導向架構(Service-based Architecture, SBA)為根基，讓得標者可根據新興服務的需求彈性、快速地進行服務提供所需的功能建置或擴展，以及達到自主軟體運作、區隔及獨立維運；在達到端對端（End-to-end）大寬頻、低延遲、全面 5G 系統服務覆蓋的網路建置，支援無線電接取網路與核心網路之間高頻寬傳輸需求之 X-Haul 傳輸網路，將扮演極為重要的角色。因為 5G 系統架構將網路功能軟體化列為主要實踐目標之一，我們預期 5G 系統的建置將大量使用資通訊科技在網路系統的實作並開放網路功能和系統的介面，形成 5G 系統設置的開放性、彈性與整合性。

此亦致使 5G 系統設置面臨比傳統 3G、4G 系統設置更為多元與嚴峻的資通安全風險、威脅與挑戰：(1)資通安全控制措施不足之風險情境，例如組態配置錯誤、缺乏適當的驗證與授權機制；(2)5G 供應鏈相關之風險情境，例如對於 5G 資訊技術與通訊技術及產品品質保證之缺乏、單一供應商之依賴性、供應鏈上下游之依賴性；(3)脅來源

的發動攻擊的風險，例如第三方對於供應鏈之干預、攻擊 5G 系統的部分功能以阻斷服務或竊取用戶隱私資料；(4)5G 系統與關鍵基礎設施相依性之風險情境，例如透過 5G 系統進而攻擊其他關鍵基礎設施、因電力系統中斷導致 5G 系統無法運作；(5)與用戶設備有關之風險情境，例如利用物聯網設備攻擊 5G 系統。此外，在建置初期，5G 系統因採用非獨立形式建置並與 3G、4G 系統整合，會面臨既有 3G、4G 系統之風險，而 5G 無線電接取網路之中央單元與分布單元邏輯分離核心模式，可能面臨潛在性技術風險包含實體層攻擊（Physical Attack）、用戶隱私資料竊聽（User Data Eavesdropping Attack）與阻斷服務攻擊（Denial-of-Service Attack）、偽基地臺（Rogue Base Station）、資料完整性攻擊（Data Integrity Attack）、空中介面攻擊（Air Interface Attack）等威脅；中央單元隨著軟體化而產生新的風險，亦對管理制度帶來挑戰，例如，中央單元相關的軟體更新制度與流程，組態變更之控制管理，皆產生不同面向之風險。

多重接取邊緣運算架構的理念是可讓 5G 系統服務提供者在為達到特別是低延遲服務效能的目標下可以直接使用 5G 系統之網路邊緣所部署的運算、儲存資源或數據，大幅減少連結遠端雲端運作所需的傳輸延遲，以提供用戶端更佳的服務品質與體驗。因此，得標者未來可能提供第三方服務提供者多重接取邊緣運算服務或是開放允許他們設置相關系統於 5G 系統的網路邊緣，此舉對比於前二代相對封閉式的網路與系統設置，在資通安全維護上將產生新的風險、威脅及挑戰。例如，得標者提供包含運算、儲存等基礎設施與運作平臺，允許第三方服務提供者將其服務系統運作其上，此一政策得標者則必須審慎採取必要措施確保各系統間的運行、效能與安全之隔離與管理，避免可能的資源濫用、翻牆、滲透與入侵，建立妥適的資通安全管理制度、流程與機制；倘若第三方服務提供者之服務系統有連結外部系統

或是網路的需求，此舉可能有因其程式或系統缺陷而導致遭受攻擊或被駭客入侵，埋入惡意應用程式，蔓延擴散而影響整體 5G 系統正常運作的高度風險，必須慎重應對。或是，得標者對於多重接取邊緣運算之部署政策是允許第三方服務提供者放置其設備於得標者機房，相關機房管理政策與制度應包含實體層面、維運及人員管理之風險及威脅納入考量。如何建立完整有效的整體多重接取邊緣運算資安維護之政策、管理制度與防禦機制是一項新的挑戰。

5G 系統 X-Haul 傳輸網路之設置架構在 4G 系統常見採用光纖傳輸，其資安威脅包含可能的傳輸竊聽（Eavesdropping Attack）等攻擊。倘若得標者非自建而採取租用或共用他方之傳輸線路，在資通安全維護之政策與管理制度應考量所有可能的風險及威脅，包含線路提供者所可能帶來的風險，或是與線路共用者間之資通安全管理責任與防護作為，應有明確區分與相關管控措施。

以服務為基礎的核心網路裡，網路切片可能遭受惡意攻擊的威脅，為防止威脅擴散，應強化其隔離之安全性。此外，網路切片透過軟體化技術，協同多個網路功能模組提供服務，各功能模組面臨之威脅，例如前述之軟體更新與組態管理等風險，亦增加資通安全管理之挑戰。

(三)目的

本參考框架之目的是提供 5G 執照得標者在 5G 系統資通安全維護計畫內容擬定與撰寫的參考。具體而言，是對 5G 系統設置之資通安全維護計畫的各項目主題敘明其內容目標與重點議題，涵蓋以下五大面向：

1. 達到安全、可信賴之 5G 系統設置與管理：建立安全可靠之 5G 服務環境為得標者之關鍵任務，得標者訂定第五代行動

通信系統資通安全維護計畫時，應以 5G 系統架構全景及其網路系統特性為基礎，評估 5G 整體相關業務之資通安全需求與可能風險，訂定與落實第五代行動通信系統資通安全維護計畫。

2. 安全的軟體更新與部署管理（Secure Software Update and Distribution Management）：得標者在面對軟體更新與部署、組態變更之控制管理等安全防護時，管理制度上必須考量如檔案更新流程、版本制度、相關伺服器主機維運管理、密鑰安全防護、軟體開發流程、軟體發布與部署環節、安全軟體發展生命週期、軟體供應鏈及整體 5G 系統流程管理等資通安全防護及控制措施，並全面掌握可能發生之威脅、風險及盤點防護面向。

3. 安全的上下游供應鏈管理（Secure Supply Chain Security Management）：得標者可於 5G 產業生態鏈中，包含得標者、電信設備供應商、應用服務提供商及終端用戶此一脈絡展開，瞭解其可能影響到 5G 系統、服務及營運之資通安全議題與風險，尤其隨著 5G 系統服務逐步走向開放式架構，5G 系統資通訊系統將結合更多委外或第三方供應商之服務，得標者對於供應鏈與相關人員、軟體開發之之管理，應更加掌握及透明（Transparency），以降低潛在資安風險。

4. 建立資安事件通報與應變機制：在面對瞬息萬變的 5G 產業需求與環境變化，得標者應與主管機關配合，制訂相關通報因應機制，以強化自身之強韌性（Resilience），並透過事前演練，瞭解與熟悉相關應變機制。

5. 5G 資通安全維護措施的持續精進：得標者在規劃與設置資通安全偵測與防護之執行方案時，除前述資通安全議題外，應在確保用戶資料安全與保護用戶隱私之前提下，從設置網路、提供應用服務及營運管理等持續精進相關管理機制與保護措施，完善 5G 系統之整體資通訊安全。

二、適用範圍

本 5G 系統設置說明適用於參與中華民國一百零八年開放特許執照之競價程序，並依行動寬頻業務管理規則第 36 條規定，向主管機關一次繳清得標金，或繳納得標金頭期款及得標金餘額及其利息之支付擔保後之得標者。

前述得標者，依行動寬頻業務管理規則第 40 條，檢具第五代行動通信系統資通安全維護計畫向通傳會申請核發籌設同意書，或已為得標者之得標者，向通傳會申請第五代行動通信系統資通安全維護計畫之變更，內容均應符合 5G 系統設置資通安全維護計畫參考框架之說明。

三、撰寫說明

依行動寬頻業務管理規則第 40 條第 5 項規定,「第五代行動通信系統資通安全維護計畫」應載明十七個項目，以下就每一項目敘明應載明事項：

(一)資通安全政策及目標（Policy & Goals）

背景說明

有鑒於 5G 系統將是我國通訊傳播網路基礎設施很重要的一部份，且是促進我國創新服務及推動數位國家、數位經濟的重要基磐。

自述重點

請得標者對所設置之 5G 系統在資通安全維護提出政策方案與目標。

得標者之資通安全維護政策應包含以下面向：

- 於網路建置、運作與營運管理
- 於服務提供與管理
- 於與其他關鍵服務之相依性（Dependency），包含現行行動寬頻網路
- 於遭遇災害時之強韌性
- 利害關係人及其需求，例如中央主管機關及用戶
- 相關法規遵循
- 於網路資料傳輸與儲存之隱私保護

得標者應對自述之政策提出具體且明確欲達成的目標。本項目所述之政策與目標，應鏈結並扣合本維護計畫第二至十七項之內容。

(二)核心業務及其重要性（Core Business & Significance）

背景說明

得標者為經營 5G 業務需執行一系列活動。得標者應檢視並評量其業務之主要領域及活動，視為核心業務。在認定業務或活動之重要性上，可透過分析業務遭受衝擊時可能造成的影響，盤點並釐清 5G 業務在功能面、管理面及法遵面於得標者營運時的重要性及相依性，以建立 5G 核心業務之全景，並瞭解核心業務在運作及服務提供上於機密性、完整性、可用性、可靠性及適法性等的要求是關鍵且必要。同時，當各業務失效（Business Failure）包含遭受威脅攻擊與天然災害時，可能產生網路或服務無法完整運作與提供，應考量強韌性需求，包含隔離影響區域或業務、緊急應處、災難復原、恢復正常作業，以維持業務不中斷。

業務相依性之內容，除 5G 與其他外部關鍵服務之相依性需敘明外，支持 5G 業務之內部服務其相依性也應納入考量。

自述重點

請得標者對於所欲建設及經營之 5G 系統，請先說明所使用之評量基準，再列出判定為核心業務的項目及說明其重要性。

得標者之核心業務及其重要性與相依性應考量以下面向：

- 於整體網路運作、服務提供及營運目標之重要性
- 於整體網路運作、服務提供及營運之可靠性、機密性、完整性、可用性及適法性
- 於所負擔之指定義務，如災害防救、動員準備或通訊監察等業務的相依性於業務失效時可能產生之影響

- 於維持網路服務持續運作之強韌性

此一項目之內容，得標者應扣合第一項「資通安全政策及目標」所提出之政策與目標，力求一致，並參酌上述說明。

(三)行動寬頻系統資通安全維護範圍（Scope of Protection）

背景說明

得標者應說明，為落實第一項「資通安全政策及目標」所提出之政策與目標，以及第二項「核心業務及其重要性」之內容，盤點出要納入本計畫之資通安全維護範圍，例如業務項目、電信設備、營運系統、營運機房、營運人員等。

自述重點

得標者擬定資通安全維護範圍時，應考量以下面向：

- 於與得標者既有異質行動通信網路及固定通信網路之整合介接
- 於與外部其他電信網路之介接
- 於用於 5G 系統營運之軟硬體資源之上下游供應鏈管理
- 於如有允許第三方服務提供商之設備且/或系統建置於得標者之 5G 系統內之相關資通安全政策與管理措施，以及是否納入本計畫之資通安全維護範圍

(四)資通安全組織（Cybersecurity Executive Organization）

背景說明

為落實資通安全政策與達成資通安全目標，得標者應成立專責且獲充分授權之資通安全組織，訂定各項資通安全之政策與制度、規劃與協調跨部門資通安全維護之權責與分工，包括涵蓋第三項「行動寬頻系統資通安全維護範圍」之業務單位；週期性持續之資通安全措施規劃、防護、績效評估及改善等相關作業；核定各項資通安全維護範圍內之業務之資通安全負責人員以督導相關工作事項，落實到各業務單位。資通安全組織成員應具資通安全相關經驗或相關能力證明，成員名單、職掌及權責應予以造冊並適時更新。得標者應依據本資通安全維護計畫內容，提供建立、執行及持續改善等作業所需之資源。

自述重點

得標者於成立資通安全組織時，應考量參酌上述背景說明，扣合本文件第一項、第二項及第三項之自述內容，訂出資通安全組織相關辦法。

得標者之資通安全組織應考量以下面向：

- 專責且於組織架構中具相當位階
- 訂定資通安全政策與相關制度
- 規劃資通安全組織之組成、分工、職掌、權責等內容
- 跨部門協調資通安全維護之權責與分工包含明訂必須涵蓋之第三項「行動寬頻系統資通安全維護範圍」之業務單位
- 週期性持續之資通安全措施規劃、防護、績效評估及改善等相關作業原則與管理辦法

- 資通安全組織成員之資格與能力，例如應具備之資通安全相關經驗與能力
- 於規劃執行資通安全維護計畫內容時所需人力、預算及資源

(五)專責人力及經費之配置（Dedicated Personnel and Budget Allocation）

背景說明

為落實資通安全政策與達成資通安全目標，得標者應考量第四項所述之「資通安全組織」之工作與執掌內容，配置專責人力、經費與資源，並明訂制度做定期之檢視、檢討與改進。資通安全預算配置應於得標者整體預算中佔合理之比例且符合整體 5G 系統資通安全維護之政策、目標與需求。此項目應納入資通安全維護計畫持續改善與績效管理評量項目之一。

自述重點

得標者應考量參酌上述背景說明，扣合第四項「資通安全組織」自述之內容，配置 5G 系統所需之專責人力、經費與資源。

得標者之資通安全專責人力、經費與資源之配置應考量以下面向：

- 符合第四項「資通安全組織」所述之工作及執掌內容敘明應配置之人員人數、資格及資源
- 符合整體 5G 系統資通安全維護之政策及目標之資通安全預算於得標者整體預算中佔之比例
- 5G 系統之資通安全維護作業應涵蓋第三項「行動寬頻系統資通安全維護範圍」之業務單位
    - 應週期性且持續審視資通安全組織之人員與經費等資源配置

(六)資通安全長之配置（Chief Security Officer）

背景說明

得標者應設置專責人員擔任 5G 系統資通安全執行長，負責本計畫所訂定之業務之執行，包括領導 5G 系統資通安全組織，推動相關政策，及協調跨部門 5G 系統資通安全維護之權責與分工。資通安全執行長應熟習公司組織結構及業務，避免職務重疊或利益衝突，並具備充分之資通安全管理之專業知識及實務資歷與經驗。

自述重點

得標者應參酌上述背景說明，扣合第四項「資通安全組織」之內容，敘明資通安全執行長之職掌與權責、資格、派任等。

得標者之資通安全執行長配置應考量以下面向：

- 依據第四項「資通安全組織」所述之內容，明訂執行長之職掌與權責
- 於組織管理架構中之位階
- 人選資格
- 派任方式

(七)資訊及資通系統之盤點規劃（含系統設備符合 ITU 或 3GPP 發布之資通安全規定）（Identification of Information and Communications Systems (including Equipment in Compliance with ITU or 3GPP Regulations）

背景說明

得標者應就第三項「行動寬頻系統資通安全維護範圍」所述之內容，對所有納入本計畫之資通安全維護範圍的業務項目、電信設備、營運支援系統（Operations Support Systems）、營運機房等，就其於業務執行、功能運作與維護時所採用之資訊技術與通訊技術及產品包含硬體、軟體、網路功能、系統等進行盤點。前述盤點出之 5G 系統相關設備，應進一步確認其是否符合 ITU 或 3GPP 發布之資通安全規定。此外，5G 系統初階段之建置，如有與現行 3G、4G 系統共存並整合，亦應同時盤點這些網路之系統與整體 5G 業務執行、功能運作與維護之相關介面、模組等。

自述重點

得標者應考量參酌上述背景說明，扣合第三項「行動寬頻系統資通安全維護範圍」自述之 5G 系統資通安全維護範圍，就其業務執行、功能運作與維護時所採用之資訊技術與通訊技術及產品包含硬體、軟體、網路功能、系統等進行盤點。特別注意的是 5G 系統初階段之建置，如有與現行 3G、4G 系統共存並整合，亦應同時盤點這些網路之系統與整體 5G 業務執行、功能運作與維護之相關介面、模組等。

得標者進行盤點時應考量以下面向：

- 5G 系統涵蓋四大區塊，於各區塊下用以支援其業務執行、功能運作與維護所採用之資訊技術與通訊技術及產品包含硬體、軟體、網路功能、系統
- 於 5G 系統初階段之建置，如有與現行 3G、4G 系統共存並整合，應同時盤點這些網路之系統與整體 5G 業務執行、功能運作與維護之相關介面、模組等
- 於盤點出之模組、技術及產品，確認是否符合 ITU 或 3GPP 發布之資通安全規定

(八)資通安全風險評估（Cybersecurity Risk Assessment）

背景說明

為建立安全、可靠及具強韌性之 5G 系統與服務環境，得標者應考量 5G 系統下各區塊之功能架構與運作特性，就其業務執行、功能運作與維護，及其營運支援系統採用資訊技術、通訊技術與產品可能之威脅種類與威脅者（Threat Actors），以及扣合第二項「核心業務及其重要性」、第三項「行動寬頻系統資通安全維護範圍」及第七項「資訊及資通系統之盤點規劃」自述之內容，就納入本行動寬頻系統資通安全維護範圍之資產各自的重要性，及用以支援其業務執行、功能運作與維護所採用之資訊技術與通訊技術及產品等硬體、軟體、網路功能及系統等潛在之不同程度的弱點（Vulnerability），評估可能的主要風險與情境。此外，檢視威脅種類與威脅者應包含得標者之組織運營、制度、程序及人員作業等各層面可能產生的風險。

自述重點

得標者應參酌上述背景說明，評估可能的主要資通安全風險與情境。

得標者之資通安全風險評估應考量以下面向：

- 於達到建立安全、可靠及具強韌性之 5G 系統與服務環境，並考量 5G 系統下各區塊之功能架構與運作特性，請就納入本行動寬頻系統資通安全維護範圍之資產的重要性，及用以支援其業務執行、功能運作與維護所採用之資訊技術與通訊技術及產品等硬體、軟體、網路功能及系統等，評估：1) 可能之威脅種類與威脅者；2) 潛在之不同程度的弱點（Vulnerability）；及 3）可能的主要風險與情境類別包含營

運策略、資源管理、供應鏈管理、災害應變、作業管理、實體安全、技術管理，軟硬體與其上下游供應鏈管理、第三方服務供應商等

- 檢視威脅種類與威脅者應包含得標者之組織運營、制度、程序及人員作業等各層面可能產生的風險。

(九)資通安全防護及控制措施（Cybersecurity Protection and Control Measures）

背景說明

得標者應扣合於第八項「資通安全風險評估」所提出的評估資料，提出妥適的資通安全防護及控制之架構與措施，措施應包含系統的基準配置（Baseline Configuration of Systems）、系統開發生命週期、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理。並應就所提之架構與措施，評估其防護之效益，以及一旦失效時可能帶來的衝擊。

自述重點

得標者應考量參酌上述背景說明，在擬定資通安全防護及控制之架構與措施應涵蓋選擇合適的資通安全防護技術，或使用安全設計原則以設計運作管理流程與實體設施安全管控機制。

得標者之資通安全防護措施應考量以下面向：

- 於第八項已識別之風險與情境，提出妥適的資通安全防護及控制之架構與措施，措施應包含系統的基準配置、系統開發生命週期、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序與流程管理、技術、人員管理
- 於所提之架構與措施，評估其防護之效益，以及一旦失效時可能帶來的衝擊
- 於落實第一項所自述之資通安全政策與目標
- 於資通安全防護與控制措施之執行單位與執行方式

(十)資通安全事件通報、應變及演練相關機制(Notification, Response, and Exercise of Cybersecurity Event)

背景說明

因為得標者設置之 5G 系統，將會成為我國通訊關鍵基礎設施的一部份，因此，對於發生的資安事件，應遵循資通安全管理法訂定資通安全事件通報及應變處理之程序、流程與作業辦法，以確保能夠及時、快速地反應並處理所發生的資安事件，最大程度地減少損失，減輕被利用的漏洞，恢復服務和流程並降低未來事件帶來的風險。

自述重點

得標者應根據資通安全管理子法(資通安全責任等級分級辦法、資通安全事件通報及應變辦法)、行動寬頻業務管理規則第五十五條之一，並參酌上述背景說明，扣合第二項「核心業務及其重要性」、第三項「行動寬頻系統資通安全維護範圍」、第七項「資訊及資通系統之盤點規劃」、第九項「資通安全防護及控制措施」等自述之內容，敘明資通安全事件通報、應變及演練相關機制。

得標者自述之資通安全事件通報、應變及演練相關機制應考量以下面向：

- 擬定資通安全事件應變小組成員與執掌，成員應至少包括資安長、資安技術人員和資訊技術人員、所涉及的部門的資安人員，及其他核心業務的代表人員
- 擬定資通安全事件應變計畫，其內容應包含事件發生時與發生後的處置含應處程序，流程與作業；事件發生時相關單位之協調溝通;事件發生時損害控制措施;事件發生後之復原、鑑識、調查及改善機制

- 擬定建立資通安全事件發生時之通報作業辦法，其內容應包含於資通安全事件發生時，依照主管機關訂定之資通安全事件通報作業規範，訂定通報處理程序、流程與作業例如通報時限與方式及通報項目。同時，應就資通安全事件相關單位之協調溝通包含組織內與組織外的單位例如政府執法單位、應變處理涉入之人員指派與應變處理的溝通協調所應遵循的程序與流程
- 擬定資通安全事件應處與通報計畫之定期演練計畫，以驗證防護措施有效性，並做為持續改善資通安全成熟度之參考

(十一)資通安全情資之評估及因應機制（Cybersecurity Threat Intelligence Evaluation and Response）

背景說明

5G 系統架構因採網路功能軟體化與虛擬化，建置時將大量使用資通訊科技於網路系統之實作，並開放網路功能和系統的介面，形成5G 系統設置的開放性、彈性與整合性。同時也增加 5G 系統之資通安全威脅，且威脅之面向更為多元，資通安全情資需考量 5G 系統本身的威脅，以及所使用之各種資訊技術與通訊技術所可能帶來的威脅，據此建立資通安全威脅情資之評估及因應的機制。

得標者應擬定資通安全威脅情資程序（Cyber Threat Intelligence Cycle），其包含訂定所欲蒐集之情資、情資來源、情資分析，及情資結果分享與評估。情資來源應涵蓋多個來源，例如透過建立共享機制、同業間的聯繫、供應商發布之安全通告等，即時掌握情資；針對所蒐集情資，進行情資分析應有一套嚴謹思維與方法，採用可靠的分析技術以確保能夠有效識別和管理所蒐集情資資訊裡可能的偏差與不確定內容，且情資評估分析的結果，需依照情資因應機制決定其處理方式。

自述重點

得標者應參酌上述背景說明，扣合第二項「核心業務及其重要性」、第三項「資通安全維護範圍」及第八項「資通安全風險評估」以訂定資通安全情資之評估及因應機制。

得標者之資通安全情資之評估及因應機制應考量以下面向：

- 擬定資通安全威脅情資程序，訂定情資蒐集種類、情資來源、情資分析、情資分享、因應機制等

- 於評估情資，應參酌第二項、第三項之自述內容，掌握情資是否涉及核心業務與其影響範圍

(十二)資通系統或服務委外辦理之管理措施（The Management of Outsourcing）

背景說明

5G 系統架構的設計理念是以能夠彈性並快速支援未來各種可能的新興應用服務及其設置型態為核心，尤其隨著 5G 系統服務逐步走向開放式架構，得標者所建置之 5G 系統例如軟體或是服務可能委外辦理或由第三方供應商提供，對於其開發與管理之供應鏈及相關人員，必須要有相當之掌握包含瞭解影響產品或服務安全級別的元件或軟體之來源（Origin）及產品開發或供應之上下鏈結的生態系，以及產品和服務之維護、更新與修復的透明度，以降低並能管控可能潛在的資通安全風險。得標者應就 5G 系統如有資訊技術或通訊技術及產品包含硬體、軟體、網路功能、系統等訂定委外辦理的管理辦法與機制。

自述重點

得標者應參酌上述背景說明，並扣合第二項「核心業務及其重要性」、第三項「行動寬頻系統資通安全維護範圍」及第八項「資通安全風險評估」，評估委外辦理可能涉及之核心業務與風險，訂定委外辦理管理措施。

得標者之資通系統或服務委外辦理之管理措施應考量以下面向：

- 訂定委外辦理管理辦法與機制，包含委外需求評估需考量可能涉及之核心業務與風險；委外服務提供商之選擇應掌握其資通安全管理能力；對於涉及系統開發與管理之供應鏈與相關人員，必須要有相當之掌握包含瞭解影響產品或服務安全級別的元件和軟體的來源與開發供應者之上下鏈結的生態系，以及產品和服務之維護、更新和修復的透明度

(十三)所屬人員辦理業務涉及資通安全事項之考核機制（Performance Evaluation of Personnel with Job Assignment Involved 5G Security）

背景說明

得標者應針對 5G 系統資通安全維護計畫施行範圍內之相關人員，包含 5G 業務之所屬人員及服務委外機構如有涉及 5G 系統資通安全維護事項，應訂定契合資通安全維護政策與目標之考核機制，例如資通安全維護措施之執行績效、資通安全事件通報與應變績效，以完善 5G 系統資通安全維護與持續精進。

自述重點

得標者應參酌上述背景說明，並扣合第一項「資通安全政策及目標」、第二項「核心業務及其重要性」及第三項「行動寬頻系統資通安全維護範圍」，訂定所屬人員辦理業務涉及資通安全事項之考核機制。

得標者之所屬人員資通安全考核機制應考量以下面向：

- 於參酌資通安全政策及目標，訂定資通安全績效指標，激勵所屬人員達成資通安全之目標
- 於所屬人員考核績效之回饋，如遇未達資通安全目標者，應依分析其原因並作為持續改善之參考依據，且應將該項未達標之風險納入評估以調整防護措施

(十四)資通安全維護計畫與實施情形之持續精進及績效管理機制（Continual Improvement and Review of 5G Network Protection Plan）

背景說明

得標者為確保所訂定之 5G 系統資通安全防護計畫之內容能有效保障 5G 系統、服務及營運之資通安全，確保用戶資料安全與保護用戶隱私，得標者應針對資通安全維護計畫實施情形，建立持續精進程序與績效管理機制，藉以提升資通安全治理成熟度，且得標者所設置之 5G 系統在面對層出不窮、與日俱增之各種潛在威脅、風險及攻擊時能夠持續不斷檢視與改善弱點、降低風險並維持資通安全管理及防護措施有效運作。

自述重點

得標者應針對資通安全維護計畫各項防護措施及實施情形，自述持續精進程序與績效管理制度，包括資通安全維護計畫與實施結果之績效管理審查以及稽核機制。

得標者之持續精進及管理機制應考量以下面向：

- 資通安全維護計畫實施情形的績效管理，應包含定期稽核與擬定可行有效的稽核方案，以及召開資通安全管理績效審查會議，定期檢討資通安全維護計畫所訂定之措施及其實施情形，是否符合計畫目標及內容
- 如有資通安全績效未達目標或有待改善項目者，應提出改善措施並追蹤後續改善績效，以確保 5G 系統資通安全維護計畫之有效實施及所採用之防護措施的有效性

- 資通安全維護計畫實施情形的績效管理應持續進行，以精進防護措施並確保整個計畫執行之適切性與有效性

(十五)資通安全偵測與防護之建置及執行方案（含資通安全防護架構、防禦縱深及其建置時程）（Implementation Plan for Detection and Protection（Including Architecture, Defense In-Depth Measures, and the Timetable））

背景說明

得標者依據第一項至第十四項之自述內容，提出具體、周全、可行的建置與執行方案，也就是提出實施計畫（Implementation Plan）確保在事業計畫書所規劃建置之 5G 系統會是安全、可靠且具強韌性。實施計畫之內容，第一、應提出整體 5G 系統資通安全防護架構與建置方案，其中需針對 5G 系統四大區塊各自之資通安全防護架構及其防護之實施提出規劃與具體解決方案，以及整體網路之整合防護計畫。第二、對於在各區塊用來實作資通安全偵測與防禦所建置之各種資通訊設備與安全防護系統，亦須說明防護其安全之措施，以確保這些建置與設施亦是安全、可靠的。第三、對於執行 5G 系統資通安全防護計畫之建置與實施計畫，應說明整體資通安全管理制度、流程、專責之資通安全組織、其轄下之資通安全執行長及所有專職人員的配置、執掌與分工，及建置時程等，以確保達成本計畫所設定之政策與目標。

自述重點

得標者應參酌上述背景說明，並依據第一項至第十四項之自述內容，敘明 5G 系統整體與四大區塊各自需建置之資通安全偵測與防禦之執行方案。

得標者之實施計畫應考量以下面向：

- 整體 5G 系統資通安全防護架構

- 5G 系統所含之四大區塊各自的資通安全防護架構及其建置與執行方案
- 整體網路之整合防護方案
- 對於在各區塊用來實作資通安全偵測與防禦所建置之各種資通訊設備與安全防護系統，說明防護其安全之措施，以確保這些建置與設施亦是安全、可靠的
- 對於所提出之建置與實施計畫，應說明整體資通安全管理制度、流程、專責之資通安全組織，以及其轄下之資通安全執行長及所有專職人員的配置、執掌與分工
- 建置時程
- 提出可驗證所提之建置與執行方案執行成效之方法與機制

(十六)執行前述執行方案所蒐集、儲存、處理及利用用戶資料之安全保護措施(Security Measures for Subscriber Data Protection in terms of Collection, Storage, Process and Use)

背景說明

5G 系統架構以能夠彈性並快速支援未來各種可能的新興應用服務為核心，得標者在建立安全可靠具強韌性之 5G 服務環境時，除前述資通安全議題外，應確保用戶隱私及資料之安全保護。因此，包含網路管理、服務提供、營運管理及資通安全防護目的，得標者於用戶相關資料之蒐集、儲存、處理及利用應提出用戶隱私及資料保護政策與措施並定期檢視執行績效與妥適性。

自述重點

得標者應參酌上述背景說明，及我國個人資料保護法、個人資料保護法施行細則等相關法規，於網路管理、服務提供、營運管理及資通安全防護等目的作業下，如有用戶網路與服務使用相關資料之蒐集、儲存、處理及利用，應提出用戶隱私及資料保護政策與措施，以及定期檢視執行績效與妥適性。

得標者之於各種營運目的對用戶隱私及資料保護應考量以下面向：

- 於網路管理、服務提供、營運管理及資通安全防護等目的作業下，對用戶網路與服務使用進行資料之蒐集、儲存、處理及利用之用戶隱私及資料保護政策與措施

- 於合作之第三方服務提供商如有網路與服務使用進行資料收集及資料分享，應提出用戶隱私及資料保護政策與措施，並確保執行方案的透明
- 定期檢視執行績效與妥適性方案

(十七)通過資通安全管理驗證之執行方案（Formal Certification of Cybersecurity Management）

背景說明

建立安全可靠之 5G 系統與服務環境為得標者之關鍵任務，為落實其資通安全維護計畫之自述內容，應提出資通安全防護措施之管理驗證執行方案，以確保於制度面與管理面等程序落實資通安全政策與達成資通安全目標，例如通報與應變機制、5G 系統之軟體更新與部署等，以及 5G 資通安全防護措施之持續精進。

自述重點

得標者應參酌上述背景說明，擬定 5G 系統資通安全管理驗證之執行方案，內容應具體、可驗證並扣合第一項至第十六項之自述內容，且應定期由第三方公正單位稽核得標者之執行成效，以確保於制度面與管理面等程序落實資通安全政策與達成資通安全目標。

得標者在擬定通過資通安全管理驗證之執行方案時，應考量以下面向：

- 於第一項至第十六項自述內容框列驗證項目與範圍
- 擬定驗證執行方案，包含時程、內部驗證機制與第三方驗證機制
- 擬定定缺失改善管理辦法

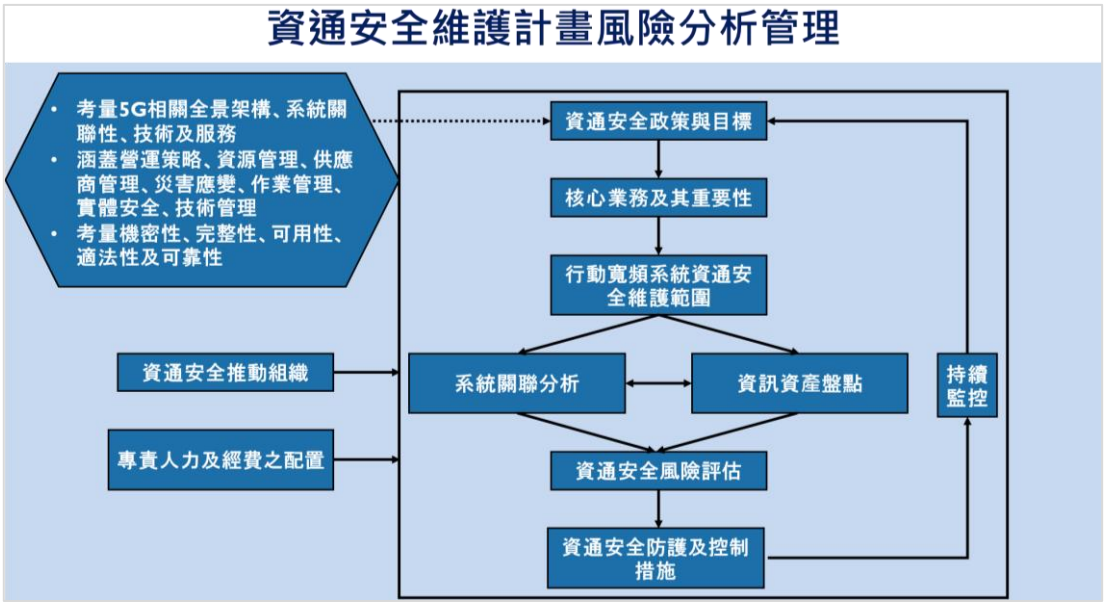


圖 5-2、資通安全維護計畫風險分析管理

資料來源：本團隊整理

第二節 意見徵詢會議與業界說明會辦理

本團隊於計畫執行期間舉辦「資通安全維護計畫應載明事項參考框架之意見徵詢會」，以及「資通安全維護計畫應載明事項參考框架之業界說明會」(如下表 5-1 所示)，邀集產官學研等專家學者，共同探討適用於我國 5G 網路資通安全維護計畫之適用性及可行性，透過本次意見徵詢會議及說明會，共同提升整體資通安全防護及法規調適措施，建立國家 5G 資訊安全防護能量，確保 5G 網路資安防護功能與國際接軌，進而促進相關垂直應用場域及創新應用服務之發展。

表 5-1、意見徵詢會議與業界說明會列表

項次	主辦單位	活動日期	會議名稱
1	財團法人電信技術中心	108 年 10 月 31 日	資通安全維護計畫應載明事項參考框架之意見徵詢會
2	財團法人電信技術中心	108 年 12 月 17 日	資通安全維護計畫應載明事項參考框架之業界說明會 – 臺北場
3	財團法人電信技術中心	108 年 12 月 18 日	資通安全維護計畫應載明事項參考框架之業界說明會 – 高雄場

資料來源：本團隊整理

本計畫已針對以下會議中業者較關注議題作為擬定此參考框架之考量（詳細紀錄如附件一）：

(一)資通安全查驗項目與範圍之可執行性評估

參考資通安全維護計畫參考框架中第十項「資通安全事件通報、應變及演練相關機制」，並扣合第二項「核心業務及其重要性」、第三項「行動寬頻系統資通安全維護範圍」、第七項「資訊及資通系統之盤點規劃」、第九項「資通安全防護及控制措施」等之強韌性要求，業者可考量自身 5G 網路架構、風險管控及團隊工

作能力等，擇訂若干防護範圍。本案計畫於擬定框架與後續稽核事宜時，會考量適當之技術脆弱性評估方法，例如弱點掃描或滲透測試等，驗證防護措施之有效性，並說明辦理情形。又例如針對強化強韌性之要求，本計畫亦考量相關可行之基本做法作為後續審查基準，例如建議業者可提供最近一場次執行資通安全事件通報及應變演練紀錄，以佐證確保當系統設備障礙發生時，能維持網路服務持續運作之強韌性。

(二)監理單位是否需規劃並且公告合格資通安全查驗第三公正單位，及符合 ITU 或 3GPP 發佈之資通安全規範電信系統設備供應商清單，俾便業者遵循

有關第三方公正單位可參酌資通安全管理法第七條第一項規定，資通安全責任等級分級辦法「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構。另業者可主動請設備供應商，提供 5G 系統設備符合 ITU 或 3GPP 發布之資通安全規定之佐證資料，此項亦為業者於供應商管理之責任，例如 gNb 設備應請供應上提供符合 3GPP TS 33.511 [122]之要求。

(三)系統功能性審驗作業是否需與資通安全防護查驗作業脫勾

二者監理目的與屬性不太相同，前者審驗作業著重系統能否正常提供服務；後者則為資通安全之管理維護，但系統功能性審驗作業之資安功能審驗與資通安全防護查驗作業有部分雷同之處。本計畫為落實 Security by Design 之精神，規劃開臺前系統審驗項目已考量資通安全維護計畫 17 項應載明事項，並且顧及業者執行上的可行性，已盡可能降低因審驗導致潛在業務失效之風險，大多以一般性審驗為主，少部分功能性審驗為輔，以確保業者之資通安全維護計畫執行狀況，以保障功能面與資安面之基

本要求，後續較嚴謹之資安查驗將依開臺後資通安全維護計畫定期查驗稽核。

(四)部分業者現有 NSA 系統架構已上線支援 5G 功能，並符合現行資通安全防護相關規定。已上線之系統基於資安防護需求，是否需再接受其他具有潛在風險之入侵測試，或再下線進行未來新增之資安防護查驗

本計畫已考量業者已上線之系統進行資安項目查驗之風險，擬定開臺前之系統資安審驗標準，並於開臺前，在不影響服務水準之情況下，進行相關資通安全檢測，以確保資通安全防護措施之有效性。另建議業者於建置 5G NSA 系統時，可自行進行資通安全檢測並保留紀錄以確認系統是否符合資安防護規定，確保資通安全控制措施為可用且有效。

第陸章　「行動寬頻系統審驗技術規範」修正草案及其相關審驗作業程序

通訊網路是我國八大關鍵基礎設施之一，為完備 5G 系統建設與相關產業的發展，確保得標者所設置的 5G 系統是安全可信賴，以保障我國關鍵基礎設施之資通安全及消費者權益，鼓勵創新服務與健全電信產業發展。通傳會爰依據電信法第 39 條及行動寬頻業務管理規則第 47 條載明得標者於完成 5G 基地臺設置數量達二百五十臺以上時，始得向主管機關申請系統技術審驗，經審驗合格後並由主管機關發給系統技術審驗合格證明，始得正式開基地臺使用。

本技術規範增訂 5G 資通安全相關之一般性與功能性對應審驗規定，以確認上述開臺門檻及建設義務之履行以確保能對應 5G 新系統、新設備、新型態與複雜之 5G 網路資通安全風險，俾使通傳會充分掌握與瞭解電信事業 5G 網路資通安全防護規劃，確保業者設置 5G 網路之信任、可靠及安全性，保障消費者權益，維護新興垂直應用場域與創新服務穩定發展。

第一節 行動寬頻系統審驗技術規範部分規定修正草案及審驗作業程序

一、總說明

因應第五代行動通信技術（5G）發展之需，通傳會擬修訂行動寬頻業務管理規則，增訂 5G 網路建設之開臺門檻及建設義務等相關規定。本技術規範除增訂 5G 相關用詞定義外，亦對應調整相關審驗規定，俾確認上述開臺門檻及建設義務之履行。

本次修正亦加入資通安全維護之查核措施，依據電信法第 39 條及行動寬頻業務管理規則第 47 條載明得標者應行之系統資通安全事項，得標者於其 5G 公眾電信網路設置完成後或其後電信基礎設施有異動時，應檢具自評報告向主管機關申請審驗，並經主管機關審驗合格，發給審驗合格證明文件後，始得使用（基地臺開臺）。其中一般性審驗要求得標者提供其所設置 5G 系統之資通安全防護及控制措施執行情形之佐證資料；功能性審驗則要求得標者所設置之 5G 系統需提供全數審驗之資通安全防護佐證資料，亦需通過實地抽樣驗證測試，確保得標者所設置的 5G 系統是安全、強韌與可信賴，以保障我國關鍵基礎設施之資通安全及消費者權益，鼓勵創新服務與健全電信產業發展。為掌握業者確實依照自述之資通安全維護計畫執行，以確保 5G 系統之安全性、強韌性及可信賴性，爰針對其系統、設備或應用服務軟體等營運前應完成之措施，明定相關要求與審驗技術程序。

二、部分規定修正草案及審查作業程序條文對照

5G 系統為因應未來各種潛在應用服務，在設計上係以彈性擴充功能為理念，除採取以服務為基礎的核心網路架構外，並導入大量的軟體功能模組，如 SDN、NFV 及網路切片等。有別於傳統通訊協定及硬體可能產生之風險，系統與軟體運作、軟體版本更新、第三方軟體功能模組等面向，所帶來的資安漏洞與風險都是 5G 系統維運的挑戰。

為確保我國 5G 系統之資通安全，通傳會除已修正行動寬頻業務管理規則，要求 5G 得標者據以提報並執行資通安全維護計畫，建設之資通訊設備（系統設備）應符合國際組織資通安全規定外，並透過開臺前的系統審驗與後續定期稽核，檢查業者實施資通安全維護計畫之情形，以確保業者所設置之 5G 系統安全、強韌與可信賴。

按 5G 得標者提報之資通安全維護計畫已就其資通安全政策及目標、核心業務及其重要性、資通安全維護範圍、資通安全推動組織、專責人力及經費配置、資訊及資通系統盤點結果、資通安全風險評估等項目，提出資通安全防護及控制措施等作為。鑒於業者資通安全防護及控制措施之落實與否，攸關 5G 系統資通安全之良窳、用戶個人資料與隱私的安全、及服務品質與消費者權益保障，爰 5G 系統營運前之審驗重點將側重於以一般性或功能性審驗進行查核，以確認業者建置之資通安全措施，有涵蓋「基地臺安全」、「傳輸網路安全」、「核心網路安全」、「系統設備安全」、「整體網路安全」及「OT 安全」，確保 5G 系統確實為安全且可信賴的環境。

表 6-1、行動寬頻系統審驗技術規範部分規定修正草案條文與說明

資安要求審驗規定	說明	審驗作業程序
3.2.2.2 相關資料 (2)系統維運測試紀錄 申請人須先完成報驗系統之測試，並檢附經高級電信工程人員簽署之測試紀錄，其格式及測試項目由申請人自訂。<u>但涉資通安全防護及（或）控制項目之測試紀錄，需經資安長或資安執行長簽署。</u>		修正 3.2.2.2(2) 系統維運測試紀錄，明定報驗系統之測試涉及資通安全防護及（或）控制項目者，其測試紀錄，需經資安長或資安執行長簽署。
一般性審驗 **4.7 資通安全防護及控制** 4.7.1 系統設備符合 ITU、3GPP 或 NIST 等組織資通安全規定之證明文件或佐證資料。 4.7.2 資通安全防護設備之廠牌、型號、數量、功能及容量，與整體防護架構，應符合或優於系統建設計畫。 4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管	**一般性審驗** **4.7 資通安全防護及控制** 4.7.1 【設備安全】為因應 5G 面臨之資通安全風險及威脅，ITU、3GPP 或 NIST 等組織已發布相關資通安全防護建議。為確保業者採購之系統設備符合國際要求，行動寬頻業務管理規則第 40 條第 5 項第 7 款已明定相關要求，復於審驗階段確認其落實情形。 4.7.2 【整體網路安全】為因應 5G 面臨之資通安全風險及威脅，業者已於系統建設計畫提出各項防護設備放置於 5G 系統中，以構成整體防護架構。為保護 5G 系統核	**一般性審驗作業程序** 依據 4.7 項資通安全維護所制定，依資通安全維護計畫提報有關系統設備之資通安全維護執行情形之佐證資料，執行一般性審驗作業。

資安要求審驗規定	說明	審驗作業程序
理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。	心網路安全，爰要求建置之資通安全防護設備應符合或優於其系統建設計畫。 4.7.3 【OT 安全】因面臨資通安全防護及控制措施不足之風險，例如組態配置錯誤、缺乏適當的驗證與授權機制，本項透過 5G 業者提出 17 項所列之各項安全操作流程，達到 OT 安全，並配合第一項所述之說明，達成安全的設備與其安全之操作流程。	
功能性審驗 **5.1 抽樣審驗項目** 5.1.9 空中介面加密功能（終端設備與基地臺間、終端設備與核心網路間） (1) 抽樣方法： 依申請人檢送附表二中報驗之基地臺數量，按附錄一「系統審驗基地臺抽樣基準」決定抽驗數量，每一抽驗基地臺於其電波涵蓋範圍內任選一定點進行測試。 (2) 合格條件 基地臺至用戶終端設備之空中介面開啟加密功	**功能性審驗** **5.1 抽樣審驗項目** 5.1.9 【加密功能查驗】為避免信令與使用者資料遭攔截竄改之風險，爰將其納入，審驗其 5G 系統加密與完整性功能。	**功能性審驗作業程序** **5.1 抽樣審驗項目** 5.1.9 空中介面加密功能審驗作業程序: (1)由電信業者提供受測系統已開啟 NAS 與 AS 層加密機制 (128-bit Ciphering & Integrity Algorithms)之佐證資料。 (2)於抽驗基地臺電波涵蓋範圍內以可顯示 NAS/AS 相關訊息之工程手機，依照數據功能審驗方式進行測試並錄製 Log 存檔。

資安要求審驗規定	說明	審驗作業程序
能，並符合 3GPP 之資料加密機制。 (3) 測試方法 (3.1) AS 層加密功能 依 5.1.1 數據功能及 5.1.2 語音功能之測試方法。 (3.2) NAS 層加密功能 依 5.1.1 數據功能及 5.1.2 語音功能之測試方法。 (4) 測試結果 測試結果應記錄於附表三之九「數據空中介面加密功能測試紀錄表」及附表三之十「語音空中介面加密功能測試紀錄表」。		(3)於抽驗基地臺電波涵蓋範圍內以可顯示 NAS/AS 相關訊息之工程手機，依照語音功能審驗方式進行測試並錄製 Log 存檔。 (4)分析 Step1~3 Log 存檔，分別確認受測系統空中介面 NAS 與 AS 層加密機制是否已經開啟，並將結果紀錄於測試紀錄表單中。 審驗測試紀錄表單 3.2.3.9 與 3.2.3.10 空中介面加密功能測試紀錄表（附表三之九、三之十）。
5.2 全數審驗項目 5.2.1 基地臺管理 基地臺發射機最大射頻輸出功率大於一點二六瓦特者，系統應具備告警、組態及帳號權限等功能，並檢附網路管理系統及網路安全之相關佐證資料 5.2.2 增波器管理 增波器發射機最大射頻輸出功率大於一點二六瓦特者，系統應具備告	**5.2 全數審驗項目** 5.2.1 【基地臺安全】 為因應基地臺面臨之資通安全風險與威脅，包含頻譜資源遭到合法使用者濫用或非法使用者干擾之風險、基地臺遠端接取介面之非法存取或濫用、人為故意破壞/竊取 5G 系統的實體設施與功能元件，造成頻譜利用效益不符預期等，爰要求基地臺管理系統	**5.2 全數審驗項目審驗作業程序** 依據 5.2 項全數審驗項目所制定，依事業計畫書與資通安全維護計畫提報有關系統設備之功能正常運作與資通安全維護執行情形之佐證資料，執行功能性審驗作業。

資安要求審驗規定	說明	審驗作業程序
警及帳號權限等功能，並檢附網路管理系統及網路安全之相關佐證資料。 5.2.3 網路狀態監控 5.2.3.2 所報系統屬 4G 或 5G 者： 5.2.3.2.1 網管系統應具備監控非核心網路功能元件（eNB、gNB、UPF，及其他具網管功能之接取網路設備）之功能與性能，包括元件正常登錄顯示與異常登錄告警、組態更動告警、及設備元件間介面（S1-MME、S1-U、X2、Xn）之連線正常顯示與異常告警功能。 5.2.3.2.2 網管系統應具備監控核心網路功能元件（MME、PGW、HSS、UDM、AUSF、AMF、SMF、UPF、NEF、NRF、SEPP、NSSF）之功能與性能，包括元件正常登錄顯示與異常登錄告警、組態更動告警、及元件間介面（S5、S10、S11、S6a、N1、N2、N3、N4、N6、N7、N8、N9、N10、N11、N12、N13、	應具備告警、組態及帳號權限等功能。 5.2.2 同上（增波器僅有部分基地臺的功能）。 5.2.3.2.1 【非核心網路功能元件異常偵測能力】為降低惡意攻擊或意外操作，導致非核心網路功能元件產生不符合預期功能及性能的資安風險，爰明定網管系統應確實掌握非核心網路功能元件的功能及性能。 5.2.3.2.2 【核心網路功能元件異常偵測能力】為降低惡意攻擊或意外操作，導致核心網路功能元件產生不符合預期功能及性能的資安風險，爰明定網管系統應確實掌握核心網路功能元件的功能及性能。 5.2.4.2 【傳輸網路強韌性】為降低天然災害發生對 5G 系統的傳輸功能與性能產生之風險，特別是傳輸網路的重要節點部分，爰明定核心網路及基地臺匯集點（Hub	

資安要求審驗規定	說明	審驗作業程序
N14、N15、N16）之連線正常顯示與異常告警功能。 5.2.4 核心網路交換設備及基地臺控制器間傳輸網路備援 5.2.4.2 核心網路及基地臺匯集點（Hub Site）間之傳輸網路應具有備援電路。 5.2.7 核心網路強韌性 核心網路功能元件（MME、PGW、HSS、UDM、AUSF、AMF、SMF、UPF、NEF、NRF、SEPP、NSSF）應具備強韌性，如提供容錯系統及備援機制。 5.2.8 資通安全防護 非核心網路、核心網路及網管系統應具備資通安全防護及控制措施。	Site）間之傳輸網路應具有備援電路。 5.2.7 【核心網路功能元件之強韌性】為降低核心網路之網路功能元件遭到資源消耗攻擊之風險，避免造成網路功能元件之功能及性能不符合預期，爰明定核心網路應具備容錯系統及備援機制，特別是身分認驗證功能異常時，必須能及時回歸正常效能。 5.2.8 【網管系統及核心網路安全性】考量 5G 系統與既有行動通信系統共存、整合之事實，為降低非核心網路、核心網路及網管系統面臨之網路架構設計與規劃之防護措施不足的風險，例如組態配置錯誤、缺乏適當的認驗證與授權機制，爰明定非核心網路、核心網路及網管系統應具備資通安全防護及控制措施，以確保行動寬頻系統非核心網路、核心網路及網管系統之資通安全。	

資料來源：本團隊整理

表 6-2、資通安全維護計畫應載明事項與行動寬頻系統審驗技術規範部分規定修正草案對照表

資通安全維護計畫應載明事項	是否納入審驗	建議審驗規定
1. 資通安全政策及目標	不適用於系統技術審驗範圍	
2. 核心業務及其重要性	不適用於系統技術審驗範圍	
3. 行動寬頻系統資通安全維護範圍	是	4.7.1 系統設備符合 ITU、3GPP 或 NIST 等組織資通安全規定之證明文件或佐證資料。
4. 資通安全組織	是	4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。
5. 專責人力及經費之配置	是	4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、

資通安全維護計畫應載明事項	是否納入審驗	建議審驗規定
		容量管理及資通安全事件通報應變與情資分析。
6. 資通安全長之配置	是	4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。
7. 資訊及資通系統之盤點規劃（含系統設備符合 ITU 或 3GPP 發布之資通安全規定）	是	4.7.1 系統設備符合 ITU、3GPP 或 NIST 等組織資通安全規定之證明文件或佐證資料。 4.7.2 資通安全防護設備之廠牌、型號、數量、功能及容量，與整體防護架構，應符合或優於系統建設計畫。 4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。 5.1.9 空中介面加密功能 5.2.1 基地臺管理 5.2.2 增波器管理 5.2.3 網路狀態監控

資通安全維護計畫應載明事項	是否納入審驗	建議審驗規定
		5.2.4 核心網路交換設備及基地臺控制器間傳輸網路備援 5.2.7 核心網路強韌性
8. 資通安全風險評估	是	4.7.2 資通安全防護設備之廠牌、型號、數量、功能及容量，與整體防護架構，應符合或優於系統建設計畫。 4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。 5.1.9 空中介面加密功能 5.2.1 基地臺管理 5.2.2 增波器管理 5.2.3 網路狀態監控 5.2.4 核心網路交換設備及基地臺控制器間傳輸網路備援 5.2.7 核心網路強韌性
9. 資通安全防護及控制措施	是	4.7.2 資通安全防護設備之廠牌、型號、數量、功能及容量，與整體防護架構，應符合或優於系統建設計畫。 4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資

資通安全維護計畫應載明事項	是否納入審驗	建議審驗規定
		產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。 5.1.9 空中介面加密功能 5.2.1 基地臺管理 5.2.2 增波器管理 5.2.3 網路狀態監控 5.2.4 核心網路交換設備及基地臺控制器間傳輸網路備援 5.2.7 核心網路強韌性 5.2.8 資通安全防護
10. 資通安全事件通報、應變及演練相關機制	是	4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。
11. 資通安全情資之評估及因應機制	是	4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。

資通安全維護計畫應載明事項	是否納入審驗	建議審驗規定
12. 資通系統或服務委外辦理之管理措施	是	4.7.1 系統設備符合 ITU、3GPP 或 NIST 等組織資通安全規定之證明文件或佐證資料。 4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。
13. 所屬人員辦理業務涉及資通安全事項之考核機制	是	4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。
14. 資通安全維護計畫與實施情形之持續精進及績效管理機制	是	4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。

資通安全維護計畫應載明事項	是否納入審驗	建議審驗規定
15. 資通安全偵測與防護之建置及執行方案（含資通安全防護架構、防禦縱深及其建置時程）	是	4.7.2 資通安全防護設備之廠牌、型號、數量、功能及容量，與整體防護架構，應符合或優於系統建設計畫。 4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。 5.1.9 空中介面加密功能 5.2.1 基地臺管理 5.2.2 增波器管理 5.2.3 網路狀態監控 5.2.4 核心網路交換設備及基地臺控制器間傳輸網路備援 5.2.7 核心網路強韌性 5.2.8 資通安全防護
16. 執行前述執行方案所蒐集、儲存、處理及利用用戶資料之安全保護措施	是	4.7.3 資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資通安全事件通報應變與情資分析。
17. 通過資通安全管理驗證之執行方案	不適用於系統	

資通安全維護計畫應載明事項	是否納入審驗	建議審驗規定
	技術審驗範圍	

資料來源：本團隊整理

修正附表三

行動寬頻系統審驗項目測試紀錄表（1/12）

申請人（公司）		申請日期	年　月　日

1. 一般性審驗

項別	審驗內容	自評	審驗結果	備註
7.資通安全防護及控制	（1）系統設備符合 ITU、3GPP 或 NIST 等組織資通安全規定之證明文件或佐證資料。 （2）資通安全防護設備之廠牌、型號、數量、功能及容量，與整體防護架構，應符合或優於資通安全維護計畫及系統建設計畫。 （3）資通安全防護及控制措施之佐證資料，包括系統基準配置（Baseline Configuration）、系統開發生命週期、委外管理、變更控制程序、備份計畫、資料與隱私管理、系統暨軟體漏洞管理、作業程序（Procedure）與流程（Process）管理、技術及人員管理、資產盤點與管理、存取控制、機房管理、容量管理及資安事件通報應變與情資分析。	□符合 □不符合	□符合 □不符合 □待澄清	檢附佐證資料。

公司章及負責人員：　　審驗單位：　　審驗人：

行動寬頻系統審驗項目測試紀錄表（9/12）

2. 功能性審驗

項別	審驗內容	自評	審驗結果	備註
10.基地臺管理	基地臺發射機最大射頻輸出功率大於一點二六瓦特者，系統應具備告警、組態及帳號權限等功能，並檢附網路管理系統及網路安全之相關佐證資料。	□符合 □不符合	□符合 □不符合 □待澄清	檢附資料
11.增波器管理	增波器發射機最大射頻輸出功率大於一點二六瓦特者，系統應具備告警及帳號權限等功能，並檢附網路管理系統及網路安全之相關佐證資料。	□符合 □不符合	□符合 □不符合 □待澄清	檢附資料
12.網路狀態監控	（1）所報系統屬 2G 或 3G 者： （1.1）網管系統應顯示基地臺與基地臺控制器間、基地臺控制器與核心網路交換設備間、核心網路交換設備與核心網路交換設備間之連線狀態。 （1.2）網管系統對 BTS 與 BSC、BSC 與 BSC、BSC 與 MSC、MSC 與 MSC、NodeB 與 RNC、RNC 與 RNC、RNC 與 SGSN、RNC 與 MSC、MSC 與 MSC、MSC 與 SGSN 等設備間連線，應具備顯示、登錄及告警等功能。 （2）所報系統屬 4G 或 5G 者： （2.1）網管系統應具備監控非核心網路功能元件（eNB、gNB、UPF，及其他具網管功能之接取網路設備）之功能與性能，包括元件正常登錄顯示與異常登錄告警、組態更動告警、及元件間介面（S1-MME、S1-U、X2、Xn）之連線正常顯示與異常告警功能。 （2.2）網管系統應具備監控核心網路功能元件（MME、PGW、HSS、UDM、AUSF、AMF、SMF、UPF、NEF、NRF、SEPP、NSSF）之功能與性能，包括元件正常登錄顯示與異常登錄告警、組態更動告警、及元件間介面（S5、S10、S11、S6a、N1、N2、N3、N4、N6、N7、N8、N9、N10、N11、N12、N13、N14、N15、N16）之連線正常顯示與異常告警功能。	□符合 □不符合	□符合 □不符合 □待澄清	檢附資料

公司章及負責人員：　　審驗單位：　　審驗人：

行動寬頻系統審驗項目測試紀錄表（10/12）

2. 功能性審驗

項別	審驗內容	自評	審驗結果	備註
13.核心網路交換設備及基地臺控制器間傳輸網路備援	（1）對 BSC 與 MSC、RNC 與 MSC、RNC 與 SGSN、MSC 與 MSC、SGSN 與 SGSN、MME 與 MME、SGW 與 SGW 等設備間之傳輸網路應具有備援電路，並檢附網路管理系統之相關佐證資料。 （2）核心網路及基地臺匯集點（Hub Site）間之傳輸網路應具有備援電路。	□符合 □不符合	□符合 □不符合 □待澄清	檢附資料
16.核心網路強韌性	核心網路功能元件（MME、PGW、HSS、UDM、AUSF、AMF、SMF、UPF、NEF、NRF、SEPP、NSSF）應具備強韌性，如提供容錯系統及備援機制。	□符合 □不符合	□符合 □不符合 □待澄清	檢附資料
17 資通安全防護	非核心網路、核心網路及網管系統應具備資通安全防護及控制措施	□符合 □不符合	□符合 □不符合 □待澄清	檢附資料

公司章及負責人員：　　審驗單位：　　審驗人：

附表三之九

數據空中介面加密功能測試紀錄表

測試日期：　年　月　日

測試時間	測試地址	系統別	發受信端	測試方法	測試結果	自評	審驗結果	備註
	發信端： 受信端：	□5G □4G □3G □5G⇔4G □5G⇔3G □4G⇔3G □其他 _____	發信端行動臺識別碼或 IP： _____ 受信端行動臺識別碼或 IP： _____	□一、本網互通 □同一核心網路交換設備（　　） □同一基地臺控制器（　　） □不同基地臺控制器（　　） □不同核心網路交換設備（　　） □二、異質網路跨網互通 □5G⇔4G □5G⇔3G □4G⇔3G 註： 1. 核心網路交換設備係指 MSC、MME/SGW 等。 2. 基地臺控制器係指 RNC、eNodeB 及 gNodeB 等。 3. 括弧內請填入測試之核心網路交換設備或基地臺控制器名稱。	檢查數據功能測試紀錄檔， NAS 是否有開啟加密： □是，使用何種加密機制： _____ □否，原因： _____ AS 是否有開啟加密： □是，使用何種加密機制： _____ □否，原因： _____	□符合 □不符合	□符合 □不符合 □待澄清	

經營者代表：　　審驗單位：　　審驗人員：

附表三之十

語音空中介面加密功能測試紀錄表

測試日期：　年　月　日

測試時間	測試地址	系統別	發話端	受話端	測試方法	測試結果	自評	審驗結果	備註
	發話端： 受話端：	□5G(VoNR) □4G(VoLTE) □3G □2G □VoNR⇔VoLTE □VoNR⇔3G □VoNR⇔2G □VoLTE⇔3G □VoLTE⇔2G □3G⇔2G □其他 _____	□行動臺 □本網 □他網 □市內電話 □公用電話 電話號碼： _____	□行動臺 □本網 □他網 □市內電話 □國際通信選接 □撥號選接 □指定選接 電話號碼： _____ □110 □112 □119	□一、本網互通 □同一核心網路交換設備（　　） □同一基地臺控制器（　　） □不同基地臺控制器（　　） □不同一核心網路交換設備（　　） □二、異質網路語音互通 □VoNR⇔VoLTE □VoNR⇔3G □VoNR⇔2G □VoLTE⇔3G □VoLTE⇔2G □3G⇔2G 註： 1. 核心網路交換設備係指 MSC、MME/SGW 等。 2. 基地臺控制器係指 RNC、eNodeB 及 gNodeB 等。 3. 括弧內請填入測試之核心網路交換設備或基地臺控制器名稱。	檢查語音功能測試紀錄檔， NAS 是否有開啟加密： □是，使用何種加密機制： _____ □否，原因： _____ AS 是否有開啟加密： □是，使用何種加密機制： _____ □否，原因： _____	□符合 □不符合	□符合 □不符合 □待澄清	

經營者代表：　　審驗單位：　　審驗人員：

第二節 意見徵詢會議辦理

為確保我國 5G 系統之資通安全，政府除要求 5G 得標者依據新版行動寬頻業務管理規則提報並執行資通安全維護計畫，並透過開臺前的系統審驗與後續定期稽核，從營運開始就確保業者所設置之 5G 網路系統具備足夠的安全、強韌、及可信賴性。

鑒於 5G 得標者於建置網路前已提報之資通安全維護計畫並提出資通安全防護及控制措施等作為，唯業者建置網路時所實施之資通安全防護及控制措施是否完整有效，將攸關 5G 網路系統的安全可靠、用戶個人資料隱私、以及服務品質與消費者權益，因此業者在正式開臺營運前需配合監理機關之系統審驗作業再次進行查驗，此階段之審驗重點將側重於以一般性或功能性審驗進行查核，用以確認業者實施之資通安全作為，能夠確保 5G 系統為安全且可信賴的環境。為事先確保法規調整方向與內容能配合實際需要並與外界充分溝通，故本團隊在計畫執行期間於 108 年 10 月 31 日舉辦「行動寬頻系統審驗技術規範修正草案」之業界意見徵詢會議並支援通傳會進行後續溝通活動，宣導 5G 通訊架構應具備之資訊安全作為，並且與產、官、學、研及相關利害關係人交流，以利後續法規調適之參考。

為完善行動寬頻系統審驗技術規範草案修正，於上述會議中與眾多與會人員進行討論，因會議時間有限，亦有與會者於會後與研究團隊進行交流，本計畫考量下列會議關注議題作為擬定行動寬頻系統審驗技術規範修正草案之參考（詳細紀錄如附件一）：

(一)關於「4.7.1 系統設備符合 ITU、3GPP 或 NIST 等組織資通安全規定之證明文件或佐證資料」目前業者之行動寬頻系統主要網路設備採購皆遵循法規，除大陸廠牌設備以外，若有其它國家安全考量事項，是否可給予業者實際指引？

根據業者提報之資通安全維護計畫第七項「資訊及資通系統之盤點規劃」，業者已確實遵守規範，未採購不受信任之第三方國家設備聲明。另有關國家安全考量事項，建議業者可參酌「各機關對危害國家資通安全產品限制使用原則」之相關規定，除盤點已經採購、來自危險地區的產品清單外，亦可持續關注禁用產品清單之發布狀態。

(二)關於「4.7.1 系統設備符合 ITU、3GPP 或 NIST 等組織資通安全規定之證明文件或佐證資料」，其佐證資料是否需由原廠出示切結？

根據業者提報之資通安全維護計畫第七項「資訊及資通系統之盤點規劃」，可得知業者之系統設備符合國際相關規範。後續於系統審驗階段時，本計畫建議業者可主動請原廠設備供應商，提供 5G 系統設備符合上述國際組織所發布之資通安全規定佐證資料，此議題亦為業者於供應商管理之責任，業者亦宜考量培養自身資通安全能力，以近一步驗證設備供應商所提出之佐證資料是否正確無誤。

(三)5.1.9 空中加密測項中，AS 與 NAS 加密是否皆能提供佐證資料

根據業者提報之資通安全維護計畫第九項「資通安全防護及控制措施」，並扣合第八項「資通安全風險評估」之安全、可靠及具強韌性要求，系統應具備安全、可靠及具強韌性。空中介面 NAS 與 AS 層的加密機制為 3GPP 規範訂定，所有系統（包含 GSM、LTE、5G）應遵照語音及數據測試進行，經本計畫與相關業者諮詢後，AS 與 NAS 皆能提供佐證資料，除非系統經設備商提供無法開啟該項功能之切結，否則應與其他功能性審驗項目

相同，接受抽樣檢測證明系統已開啟加密機制（或可考慮以工程手機或截取系統 Log 呈現）。

第柒章　結論與未來展望

第一節 結論

本計畫執行宗旨為確保我國 5G 網路，於建置初期即將 5G 安全納入考量（Security by design）並建立資安防護的制度、程序、措施與能力，保障我國 5G 網路安全及可信賴，促進垂直場域應用與創新應用服務之發展。

我國於 108 年的行動寬頻業務管理規則明訂電信業者得標後應行之資通安全事項，於得標後申請籌設許可時，應向通傳會提報「第五代行動通信系統資通安全維護計畫」並載明 17 項資通安全維護義務之要求。主管機關通傳會為協助業者規劃 5G 網路安全政策與措施，以撰寫 5G 網路資通安全計畫，特別研析 5G 相關國際組織在此議題的看法與措施，以及世界各主要國家相關的政策與其電信業者的措施，據以產生 5G 網路資通安全計畫參考框架，提供業者在審視 5G 資通安全與擬定資通維護計畫時參考，並提醒業者在 5G 資安的重要議題需納入考量。

本計畫主要有三項重要成果：

一、研析國際組織、國內外政府以及業者對 5G 的相關作為

為使我國 5G 網路於建置時就考量安全性並與國際接軌，本計畫研析國際組織、國內外政府以及業者對 5G 的相關作為，以確保我國 5G 網路安全之正向發展。

截至 2019 年底，約有 71 個國家和地區已規劃 5G 使用之頻譜，其中 36 個國家和地區完成 5G 頻譜釋照程序。我國則於 2020 年 2 月

21 日完成 5G 頻譜拍賣競價，為世界第 37 位。5G 網路被世界各國視為是實踐數位國家、數位經濟、促進產業轉型與升級，及邁向智慧社會之重要基磐。因此，5G 網路資安已經提升到國家安全與競爭力的層級，其中最受關注的議題之一是 5G 設備供應商的信賴。各主要國家政府陸續提出具體聲明，例如美國的《5G 科技加速計畫》、英國的《下一代行動裝置技術：英國 5G 戰略》等；或頒布法規、建議與規範，例如歐盟於 2019 年 6 月提出《歐盟網路安全法案》，進而要求其會員國於同年 6 月提出各國的《5G 網路安全風險評估》，彙整後於同年 10 月發佈《歐盟 5G 網路安全風險評估報告》，後續交由 ENISA 進行 5G 網路風險之相關防護措施的研析，大多措施聚焦在設備供應鏈安全性、第三方服務提供者的風險，以及 5G NSA 跨系統整合之安全性。

同時，各國電信業者對於 5G 網路安全性也是非常重視，例如美國 AT&T 制定安全政策以確保資通安全，南韓 SK Telecom 應用量子密鑰技術於 5G 網路加密上，日本 NTT DoCoMo 與趨勢科技合作共同開發一套資安解決方案。

目前就 3GPP 截至 R16 版本所提出之 5G 網路安全規範，其首先承接 LTE 網路系統之安全規範，再加上考量 5G 系統帶來的新風險。聚焦在 5G 資料平面、控制平面與管理平面傳遞之訊息的安全性，透過 5G 標準規範的驗證與加密機制，強化 5G 系統在網路層與傳輸層的安全性。在業者如何維運一個安全可信賴 5G 系統的營運技術、相關安全控制措施如軟體更新、情資蒐集分析等鮮少著墨，有賴業者參考其他國際組織相關指引與各國監理機關訂定相關管理制度與措施，建構整體 5G 網路的安全。

綜整以上，不同於過往 3G、4G 網路，本計畫總結出 7 個在 5G 網路資安領域中的重要議題。

(一)5G 系統之新型架構：

5G 為因應未來在不同產業創新應用與服務場景所需的多元需求，不同於傳統 3G 及 4G 等之封閉架構，改採以服務為本之開放式架構，期能快速、彈性擴充網路功能，以因應各種創新應用的推出，而這個能力仰賴軟體實作與部署。

5G 系統軟體化與開放式的架構會引入前所未有的風險與威脅，因此初期建設 5G 系統時一定要將網路安全議題納入設計藍圖中，倘若事後才進行安全功能的增補將會耗費更多的成本，導致大幅增加資通安全事件發生之機率以及降低安全措施之完備性。

不同於封閉式的 4G 系統，5G 系統軟體的發布或更新過程中，如有任何環節的安全政策未落實，就有機會被駭入。5G 應用滲透各個領域，5G 的風險議題既深且廣，5G 場景就是整合 IT 與 OT 的應用，成為國家與社會數位轉型之重要支柱，世界各國都關注 5G 軟體的安全。

(二)網路系統之強韌性與可靠性：

5G 所面臨之安全議題是非常嚴峻且影響深遠，提升 5G 網路與整體通訊系統的強韌性與可靠性對國家的基礎建設施環境至關重要。通訊關鍵基礎設施必須具備強韌性，可以承受一定的網路攻擊或天然災害時維持服務不中斷，例如發生網路事件時隔離影響區域防止擴大、緊急應變機制、災難復原等，如何維持服務供應不中斷與使影響規模最小。

(三)供應鏈管理：

上下游供應鏈之依賴性，包含軟硬體開發、第三方服務提供商、掌握供應鏈生態系等的掌握並瞭解相關威脅，落實禁止使用有資通安全風險疑慮供應商之設備，以確保國內 5G 網路安全。

除參照國際標準來確保網路設備安全性之外，各個國家法規環境不同，為達到供應鏈風險最小化，我國於 5G 中禁止使用中國設備，日本政府則制定一套供應鏈規範。此外，業者亦可成立設備測試實驗室依據個別需求與環境自行檢測產品的安全可信度。

再者，風險分散也是必須要考量的議題，應使用多家受信任第三方之供應商，防止單一供應鏈風險。

(四)網路之互通性：

網路的連結沒有國界，跨網路之互通必定會牽涉到跨境資料傳輸，因此，網路互通的安全防護是一個全世界必須要一起重視的議題，這包含技術與非技術面向例如安全的網路互通、合作雙方的協議、資通安全的能力、服務運作的透明度等。

(五)開放的網路架構與多元的服務提供：

5G 網路採取的是一個開放的架構，將納入更廣泛的資通訊技術（ICT）與設施於網路的佈建與多元服務的提供，以發展出許多的創新應用，但同時也為 5G 網路的安全性帶來更多元及複雜的挑戰。因此，這些 ICT 設施的安全也會是整體 5G 網路安全的重要一部份，其「安全可信賴」的 ICT 生態鏈亦是一項重要的關鍵。

(六)情資分享與管理：

網路是跨國界互相連結，因此國與國間，業者與業者間在資安情資的收集與分享對於整體通訊網路以及 5G 網路的資通安全維護是至關重要，包含增加情資來源之多元化與可信度、情資分析、情資評估、情資共享、應變措施等，如果掌握妥當，可以大幅降低網路安全風險。例如日本政府成立官方情資中心，蒐集國內外包含電信業者、產品與服務供應商等資通安全事件，再分享相關業者，以大幅降低業者建置情資中心的成本，提升情資流通的透明度。我國 NCC 於 2019 年成立 NCCSC，亦是建置並進行相似的措施。

(七)物聯網時代的崛起：

5G 服務的目標之一是萬物聯網，現今很多的物聯網設備預設安全性不足，我們不希望終端的物聯網成為威脅者的工具作為攻擊阻斷 5G 網路的正常服務提供，亦是一個重要課題。

二、提出「第五代行動通信系統資通安全維護計畫參考框架」

為完備我國 5G 網路資安防護作為，通傳會於 2019 年修正行動寬頻業務管理規則，載明 5G 得標者於申請籌設許可時，必須向通傳會提報「事業計畫書」與「第五代行動通信系統資通安全維護計畫」。該資通安全維護計畫應載明「行動寬頻業務管理規則」第 40 條規定之 17 項資安維護義務。由於我國政府是首次在行動寬頻網路建置時，要求業者本著 Security by design 的精神，在網路建置時，就將網路安

全一併考量與建置。因此，為減輕業者負擔，業者將採用自述的方式就 17 項資安防護提出具體可行政策、目標、範圍與措施。

本計畫為引導業者正確撰擬資通安全維護計畫，提點擬定方向與重點，經研析國內、外相關資料整理出 7 大資安議題，並與通傳會共同研提「第五代行動通信系統資通安全維護計畫參考框架」，就 17 項資安防護義務敘明各項的背景及重點要件與議題，供業者撰擬資通安全維護計畫之參考。該參考框架涵蓋五大面向：

(一)達到安全、可信賴之 5G 系統設置與管理：建立安全、可靠、具強韌性之 5G 服務環境為得標者之關鍵任務，業者訂定第五代行動通信系統資通安全維護計畫時，應以 5G 系統架構全景及其網路系統特性為基礎，評估 5G 整體相關業務之資通安全需求與可能風險，訂定與落實第五代行動通信系統資通安全維護計畫。

(二)安全的軟體更新與部署管理：業者在面對軟體更新與部署、組態變更之控制管理等安全防護時，管理制度上必須考量檔案更新流程、版本控管制度、相關伺服器主機維運管理、密鑰安全防護、軟體開發流程、軟體發布與部署環節、軟體生命週期、軟體供應鏈及整體 5G 系統管理流程等資通安全防護及控制措施，以全面掌握可能發生之威脅、風險及盤點防護面向。

(三)安全的上下游供應鏈管理：5G 產業鏈包含 5G 頻譜得標者、設備供應商、應用服務提供商及終端用戶此一脈絡展開，瞭解其可能影響到 5G 系統、服務及營運之資通安全議題與風險，尤其隨著 5G 系統服務逐步走向開放式架構，5G 系統將結合更多委外或第三方供應商之服務，得標者對於供應鏈與相關人員、軟體開發之管理，應加強掌握及公開透明，以降低潛在資安風險。

(四)建立資安事件通報與應變機制：在面對瞬息萬變的 5G 產業需求與環境變化，業者應與主管機關配合，制定相關通報因應機制，以強化自身之強韌性（Resilience），並透過事前演練，瞭解與熟悉相關應變機制。

(五)5G 資通安全維護措施的持續精進：業者在規劃與設置資通安全偵測與防護之執行方案時，除前述資通安全議題外，應在確保用戶資料安全與保護用戶隱私之前提下，從設置網路、提供應用服務及營運管理等持續精進相關管理機制與保護措施，完善 5G 系統之整體資通安全。

三、增修「行動寬頻系統審驗技術規範」之資安要求

為貫策安全始於設計（Security by Design）之精神，業者除提交資通安全維護計畫外，本計畫於「行動寬頻系統審驗技術規範」中新增資安審驗項目，以確保業者之 5G 系統於開臺前系統審驗階段即具備基本之資安防護能力。

業者提交事業計畫書與資通安全維護計畫經主管機關核定後，即得申請系統建設。建設完成經主管機關審驗合格，發給審驗合格證明文件並換發事業執照後，始得開臺營運。為查驗業者確實依照自述之「資通安全維護計畫」執行，爰透過資料研析及與 5G 系統相關業者、研究者交流與討論，提出「行動寬頻系統審驗技術規範」之資安要求與技術審驗程序草擬條文。

主管機關除要求得標者提供其所設置 5G 系統之資通安全防護及控制措施執行情形之佐證資料（一般性審驗）及對非核心網路、核心網路及網管系統資通安全防護及控制措施佐證資料之書審外，亦將透

過實地抽樣審驗，以確認 5G 系統、設備或應用服務軟體等營運前應完成之資安防護措施，確認得標者設置的 5G 系統具備安全性、強韌性與可信賴性，以保障我國 5G 關鍵基礎設施資通安全及消費者權益，帶動創新服務與電信產業發展。

第二節 未來展望

5G 系統不同於過往以特殊硬體提供各種功能的行動通訊系統，它引進 SDN 與 NFV 等架構，透過彈性的軟體控制平面讓 5G 系統達到全面軟體化與虛擬化，此外，透過開源軟體等技術可降低 5G 系統的開發與建置成本、大幅提升應用彈性與可擴充性，以因應各種垂直應用的需求，但這些好處的背後也同時帶來更多的潛在漏洞威脅與被攻擊的機率，加劇整體網路的脆弱性、提升服務全面癱瘓的可能性。因此如何確保軟體安全已經成為 5G 時代最重要的安全挑戰之一。

5G 系統大量軟體化與虛擬化的另一重大安全挑戰就是供應鏈安全，因為直接在 5G 供應商提供的解決方案內，嵌入威脅來源是滲透 5G 系統最有效的方式之一。妥善的供應鏈安全管理將會是降低 5G 系統大規模安全事件最為重要的一個環節。

網路安全措施是否完備是一個很難量化的議題，且監理單位與業者針對 5G 網路安全的觀點不同，監理單位可能較難顧及到技術面的具體防護議題，反觀業者可能會因為執行上的困難而導致網路安全不易落實。通盤考量各個因素而擬定出一個最佳施行作法將會是未來的發展目標。

為因應 5G 網路正式商轉，本案下期計畫目前與主管機關依據「第五代行動通訊系統資通安全維護計畫應載明事項之參考框架」，研擬並已提出「第五代行動通信系統資通安全維護計畫」審查基準，正在執行資通安全維護計畫之審查作業，未來預計產出後續稽核計畫及標準作業程序，同時參考國際組織及監理機關之資安防護驗證措施，持續蒐集國際 5G 標準組織資通安全技術發展、主要國家 5G 資通安全法制與政策趨勢，並規劃及建置 5G 網路資安檢測及驗證實驗室，驗

證 5G 業者資通安全維護計畫的可行性與妥適性等建議內容，並參與國外資安會議汲取經驗。

綜合上述，本案下期計畫將下列定為研究方向，並期望能產出相關研究成果：

(一)依參考框架項目研析國際組織及監理機關之資通安全防護驗證措施：本案下期計畫目前依據「第五代行動通訊系統資通安全維護計畫應載明事項之參考框架」，從制度面、管理面及技術面，正在蒐集國際組織針對 5G 網路資通安全風險評估及對應之防護驗證措施，並且蒐集主要國家 5G 資通安全維護監理作為及防護驗證措施，期望未來可提出相關研析報告。

(二)產出 5G 網路資通安全稽核計畫及標準作業程序：本案下期計畫目前依據參考框架項目以及國際組織及監理機關之資通安全防護驗證措施，正在研擬並期望未來可提出「第五代行動通訊系統資通安全維護計畫」之稽核計畫及標準作業程序。

(三)規劃及建置 5G 網路資通安全檢測及驗證實驗室：本案下期計畫將依據稽核計畫及標準作業程序之內容，研擬並期望未來可提出 5G 網路資通安全檢測及驗證實驗室建置規劃書，並且進行 5G NSA 核心網路、接取網路及終端設備等資通安全功能檢測及驗證實驗室建置。

(四)規劃及建置 5G SA 網路及 MEC 應用資通安全驗證測試場域：本案下期計畫正在研擬並期望未來可提出 5G SA 網路及 MEC 應用資通安全檢測及驗證實驗室建置規劃書，並建置 5G SA 核心網路、接取網路及終端設備及 MEC 應用等資通安全功能檢測及驗證實驗室。

(五)持續完備 5G 網路相關資通安全法規，聚焦網路營運之資通安全防護：持續盤點及研析國際組織及主要國家監理機關之 5G SA 網路資通安全技術及測試標準資通安全防護驗證措施，滾動修正「行動寬頻系統審驗技術規範」、「國家通訊傳播委員會所管特定非公務機關資通安全管理作業辦法」及「資通安全維護計畫」適用於 5G SA 網路之資通安全條文。

(六)掌握軟硬體各元件安全確保技術：掌握各元件安全的確保技術，包含上線前或更新前安全測試、原始碼溯源、第三方之變更管理、錯誤復原與緊急更新等。透過熟悉與持續發展 5G 系統實務上之關鍵技術與解決方案，研析網路作業系統到功能元件等各層次的軟體安全實施作業現況，進而研提 5G 安全確保之做法，以協助 5G 業者提升其軟體安全。

(七)監理技術能力的精進：未來監理單位可強化其監管 5G 業者商轉網路安全組態（Security Configuration）實務操作之能力，並瞭解業者與供應商未來網路安全規劃之技術發展方向，與 5G 設備供應商合作，進而落實國家 5G 資通安全監理政策，避免造成制度與實務有所歧異。

(八)建立 5G 系統供應鏈安全管理制度：透過研析 5G 系統供應鏈之分工架構及對應之安全威脅，進而研提 5G 系統供應鏈安全管理之建議，協助 5G 網路運營商建立供應鏈安全管理，帶動 5G 產業供應鏈著重資通安全防護力，保障國家 5G 網路安全。

(九)建立 5G 供應鏈對話管道：可透過與 5G 供應鏈之對話與溝通，建立政府與業界之合作夥伴關係，讓政府發布之政策能夠符合產業需求，並得到實際之支持與落實。

(十)從營運角度看待 5G 安全性：為降低 5G 系統中因業務質與量之變革所帶來的資通安全風險，在國際通信網路中成為可靠之一員，可透過與廠商溝通與合作，確實掌握國內 5G 業者與設備商之現狀與發展規劃並適時給予指導與幫助。

第捌章　計畫查核說明

第一節 Milestone & 計畫整體 End-point 達成情形

本計畫執行已完成之 Milestone & 計畫整體 End-point 達成情形說明如下表 8-1 所示：

表 8-1、本計畫查核點說明

工作項目		查核時間		
		9/30	10/31	12/31
5G 網路資通安全防護及相關法規整備				
1. 5G NSA 網路資通安全風險評估及資通安全防護要求研究				
	1.1 國際組織針對 5G NSA 網路資通安全要求	●		
	1.2 全球各主要國家 5G 資通安全維護監理作為或法令	●		
	1.3 全球各主要國家電信業者就 5G NSA 網路資通安全之相關作為	●		
	1.4 配合國際趨勢進行報告更新			●
2. 「行動寬頻業務管理規則」修正草案及所定文件填寫範例研擬				
	2.1 草案第 40 條「資通安全維護計畫」應載明事項之參考框架		●	
	2.2 召開意見徵詢會議，研議參考框架之適用性及可行性		●	
	2.3 舉辦 2 場資通安全維護計畫參考架構業界說明會			●

工作項目		查核時間		
		9/30	10/31	12/31
3. 「行動寬頻系統審驗技術規範」修正草案及其相關審驗作業程序研擬				
	3.1 研訂資通安全之一般審驗規定及其作業程序		●	
	3.2 召開意見徵詢會議，研議草案及審驗作業程序之適用性及可行性		●	
	3.3 預告草案之外界意見研析及回覆			●
4. 5G 資通安全相關國際交流合作				
	4.1 參與國際 5G 資通安全相關活動			●
	4.2 舉辦 5G 資通安全相關國際論壇			●

第二節 本計畫成果報告說明

本計畫執行成果扣合預期效益，達到**掌握趨勢**，掌握國際主要國家 5G 網路建設資通安全防護政策與實際作為；**法規調適**，整備 5G 第一階段釋照得標業者 5G 網路建設之資通安全防護的完備性與妥適性；**確保安全**，貫策 Security by Design 之精神，確保國家通訊網路安全，完備 5G 資通安全防護以促進 5G 網路創新應用服務發展，此外，為了確保業者於建置 5G 網路時，確實按照資通安全維護計畫推動與執行，本案下期計畫（109 年度）將產出相關稽核項目與方法，以驗證業者之 5G 網路為安全可信賴，具體完成事項總結如下：

(一)完成 5G NSA 網路資通安全風險評估及資通安全防護要求研究報告

本團隊已彙整並研析第三代合作夥伴計畫（3GPP）、全球行動通信系統協會（GSMA）、美國國家標準暨技術研究院（NIST）等國際組織提出之 5G NSA 網路資通安全風險、資通安全防護要求及相關文獻，及美、韓、歐盟等已（即將）商轉 5G 網路國家之監理單位及電信業者就 5G NSA 網路之資通安全防護要求或相關作為，並產出相關研究報告。作為修訂我國相關法規 5G 資安要求之參考，以確保我國 5G 網路之資安防護能力接軌國際要求。

(二)完備我國相關法規之 5G 資安要求

為落實 Security by Design 之精神，配合我國首波 5G 釋照時程及完備我國相關法規之 5G 資安要求，依原定規劃及前述 5G NSA 網路資通安全風險評估及資通安全防護要求研究報告，研提前揭管理規則第 40 條所定「資通安全維護計畫」應載明事項參考框架。據以引導 5G 業者瞭解 5G 面臨之資安風險，及撰擬「資通安全維

護計畫」時，應注意及敘明之資安防護面向。同時本團隊刻正研提「行動寬頻系統審驗技術規範」資通安全之一般審驗規定及其作業程序草案。藉由相關法規明定 5G 業者在其系統營運前的各個重要階段，應盡之網路資安防護義務；營運後，更將輔以「資通安全維護計畫」稽核機制，以確保我國 5G 網路安全可信賴。復為確保相關資安要求之妥適性及可行性，本團隊已於 108 年 10 月 31 日召開意見徵詢會議，蒐集相關利害關係人之意見作為持續調適相關法規之參考。

(三)完成國內 5G 資通安全國際論壇

本團隊於 12 月 10 日假臺大醫院國際會議中心舉辦「5G 垂直應用實證與資安策略國際論壇」,除邀請國內外專家學者分享 5G 時代應注意之資通安全管理面與制度面議題外，更藉由產、官、學、研專家就 5G 資通安全議題之交流，提升各界對於 5G 資通安全防護意識。

(四)參與 5G 資通安全相關國際交流

本團隊參與國際組織舉辦之「2019 洛杉磯－全球行動通信系統協會世界行動通訊大會（MWCLA）」、「2019 歐盟網路安全法國際會議（EUCA）」與「2019 沖繩開放國際會議（OOD）」5G 資安重要活動，掌握國際 5G 最新資通安全趨勢及主要國家針對 5G 資通安全之相關政策及作為，作為本團隊未來持續完備相關法規資安要求之參考。

本計畫執行計畫成果報告說明簡述如下表 8-2 所示：

表 8-2、本計畫成果報告說明

日期	里程碑說明	成果說明
5G 釋照之先期資通安全法規整備計畫		
9/30	5G NSA 網路資通安全風險評估及資通安全防護要求研究	・ 本計畫已彙整並研析第三代合作夥伴計畫（3GPP）、全球行動通信系統協會（GSMA）、美國國家標準暨技術研究院(NIST)等國際組織提出之 5G NSA 網路資通安全要求及相關文獻，並蒐集美、韓、歐盟等已（即將）商轉 5G 網路國家之監理單位及電信業者就 5G NSA 網路之資通安全防護要求或相關作為，作為修訂我國相關法規 5G 資安要求之參考，以確保我國 5G 網路之資安防護能力接軌國際要求。
10/31	「行動寬頻業務管理規則」修正草案及所定文件填寫範例研擬 「行動寬頻系統審驗技術規範」修正草案及其相關審驗作業程序研擬	・ 為配合我國首波 5G 釋照時程，本計畫提出「行動寬頻業務管理規則」要求第 40 條要求之「資通安全維護計畫」應載明事項參考框架供 5G 業者參酌以及所定文件填寫範例研擬，同時已研提「行動寬頻系統審驗技術規範」修正草案，規劃增訂資通安全之一般審驗規定及其作業程序。藉由相關法規明定 5G 業者在其系統營運前的各個重要階段，應盡之網路資安防護義務，以確保我國 5G 網路安全可信賴。復為確保相關資安要求之妥適性及可行性，本計畫已於 108 年 10 月 31 日召開意見徵詢會議，蒐集相關利害關係人之意見作為持續調適相關法規之參考。

日期	里程碑說明	成果說明
12/31	5G 資通安全相關國際交流合作	・ 本團隊已藉由參與國際組織舉辦之「2019 洛杉磯－全球行動通信系統協會世界行動通訊大會（2019 GSMA Mobile World Congress Los Angeles）」、「2019 歐盟網路安全法國際會議（2019 International Conference on the EU Cybersecurity Act）」、「2019 沖繩開放國際會議（2019 Okinawa Open Days Conference）」等 5G 資安重要活動以及與日本國立研究開發法人情報通信研究機構（NICT）、日本電信網路商（NTT Communications）、日本電氣商（NEC）、日本富士通（Fujitsu）公司等進行訪談與交流，持續掌握國際 5G 最新資通安全趨勢及主要國家針對 5G 資通安全之相關政策及作為，作為通傳會未來持續完備相關法規資安要求之參考。 ・ 本團隊於 12 月 10 日假臺大醫院國際會議中心舉辦「5G 垂直應用實證與資安策略國際論壇」，邀請國內外專家學者分享 5G 時代應注意之資通安全管理面與制度面議題，並藉由產、官、學、研專家就 5G 資通安全之準備與看法交流，俾以喚醒各界對於 5G 資通安全之重視。

資料來源：本團隊整理

第玖章　參考文獻

[1] “TR #21.915 Release 15 Description_v15.0.0,” The 3rd Generation Partnership Project (3GPP), 2019-09.

[2] "Evolution of LTE to 5G," [Online]. Available: https://gsacom.com/paper/evolution-of-lte-to-5g-august-2019-update/.

[3] "3GPP on Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/3GPP.

[4] "3GPP Partners," [Online]. Available: https://www.3gpp.org/about-3gpp/partners.

[5] S.Schröder, "Security in 5G Inter-network Signalling," 2018. [Online]. Available: https://docbox.etsi.org/Workshop/2018/201806_ETSISECURITYWEEK/5G/S02_SECURITY_5G_INTER-NWK_SIGNALLING_/SBA_INTRO_SA3_STATUS_T-SYSTEMS_SCHROEDER.pdf.

[6] A. R. Prasad, "4G to 5G Evolution: In-Depth Security Perspective," in *RSA Conference*, 2019.

[7] “TS #33.501 Security Architecture and Procedures for 5G System_v16.0.0,” The 3rd Generation Partnership Project (3GPP), 2019-09.

[8] A. R. Prasad, S. Arumugam, S. Baskaran and A. Zugenmaier, "3GPP 5G Security," *Journal of ICT Standardization*, vol. 6.1, 2018.

[9] “TS #23.501 System architecture for the 5G System (5GS)_v16.2.0,” The 3rd Generation Partnership Project (3GPP), 2019-09.

[10] R. P. Jover and V. M. Marojevic, "Security and Protocol Exploit Analysis of the 5G Specifications," *IEEE Access*, vol. 7, 2019.

[11] X. Zhang, A. Kunz and S. Schröder, "Overview of 5G Security in 3GPP," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, 2017.

[12] “TS #23.003 Numbering, addressing and identification_v15.6.0,” The 3rd Generation Partnership Project (3GPP), 2018-12.

[13] “TR #33.899 Study on the security aspects of the next generation system_v1.3.0,” The 3rd Generation Partnership Project (3GPP), 2017-08.

[14] “TS #38.323 NR; Packet Data Convergence Protocol (PDCP) specification_v15.6.0,” The 3rd Generation Partnership Project (3GPP), 2019-06.

[15] “TS #23.502 Procedures for the 5G System (5GS)_v16.2.0,” The 3rd Generation Partnership Project (3GPP), 2019-09.

[16] “TS #38.470 NG-RAN; F1 general aspects and principles_v15.6.0,” The 3rd Generation Partnership Project (3GPP), 2019-07.

[17] “TS #38.472 NG-RAN; F1 signalling transport_v15.5.0,” The 3rd Generation Partnership Project (3GPP), 2019-10.

[18] “TS #33.210 3G security; Network Domain Security (NDS); IP network layer security_v15.2.2,” The 3rd Generation Partnership Project (3GPP), 2019-09.

[19] “TS #33.310 Network Domain Security (NDS); Authentication Framework (AF)_v15.2.0,” The 3rd Generation Partnership Project (3GPP), 2018-12.

[20] “TS #36.300 Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2_v15.7.0,” The 3rd Generation Partnership Project (3GPP), 2019-08.

[21] “Network Equipment Security Assurance Scheme Overview Version 0.3,” Global System for Mobile Communications Association (GSMA), 2016-05.

[22] “TR #33.805 Study on security assurance methodology for 3GPP network products_v12.0.0,” The 3rd Generation Partnership Project (3GPP), 2013-12.

[23] “TR #33.916 Security Assurance Methodology (SCAS) for 3GPP network products_v15.0.0,” The 3rd Generation Partnership Project (3GPP), 2018-06.

[24] “TR #33.926 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes_v16.2.0,” The 3rd Generation Partnership Project (3GPP), 2019-12.

[25] "ETSI on Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/ETSI.

[26] "Global System for Mobile Communications Association (GSMA) official website," [Online]. Available: https://www.gsma.com/futurenetworks/.

[27] "GSMA on Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/GSMA.

[28] “From Vertical Industry Requirements to Network Slice Characteristics,” Global System for Mobile Communications Association (GSMA), 2018-08.

[29] “Generic Network Slice Template Version 2.0,” Global System for Mobile Communications Association (GSMA), 2019-10.

[30] "NIST on Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology.

[31] "Improving Critical Infrastructure Cybersecurity," US Executive Office of the President, 2013-02. [Online]. Available:

https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

[32] “NIST SP 800-39: Managing Information Security Risk - Organization, Mission, and Information System View,” National Institute of Standards and Technology (NIST), 2011-03.

[33] “NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations,” National Institute of Standards and Technology (NIST), 2018-12.

[34] “Framework for Improving Critical Infrastructure Cybersecurity v_1.1,” National Institute of Standards and Technology (NIST), 2018-04.

[35] "Path Forward to Support Adaption and Adoption of Cybersecurity Framework," National Institute of Standards and Technology (NIST), 2018-02. [Online]. Available: https://www.nist.gov/system/files/documents/2018/02/06/session_iii_-_barrett_csf.pdf.

[36] "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," The White House, 2017-05. [Online]. Available: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[37] “Telecommunications Sector Security Reforms,” Department of Home Affairs, 2019-06.

[38] "NIST Special Publication 800-53," National Institute of Standard and Technology, 2012-09. [Online]. Available: https://nvd.nist.gov/800-53.

[39] "IETF on Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force.

[40] "Working Together with 3GPP on 5G," 2017-06. [Online]. Available: https://ietf.org/blog/working-together-3gpp-5g/.

[41] "NGMN on Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Next_Generation_Mobile_Networks.

[42] "Security Aspects of Network Capabilities Exposure in 5G," Next Generation Mobile Networks (NGMN), 2018-09.

[43] "OASIS on Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/OASIS_(organization).

[44] "OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) TC," Organization for the Advancement of Structured Information Standards (OASIS), [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca.

[45] K. Gary and T. D. Nadeau, Network function virtualization, Morgan Kaufmann, 2016.

[46] "ITU-T on Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/ITU-T.

[47] "ITU on Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/International_Telecommunication_Union.

[48] "ITU-T official website," [Online]. Available: https://www.itu.int/en/ITU-T/Pages/default.aspx.

[49] “ITU-T X1042, Security services using software-defined networking,” International Telecommunication Union - Telecommunication Standardization Sector (ITU-T), 2019.

[50] "5G Market Status: Snapshot January 2020," Global Mobile Suppliers Association (GSA), 2020-01. [Online]. Available: https://gsacom.com/paper/5g-market-status-snapshot-january-2020/.

[51] “5G FAST Plan,” Federal Communications Commission (FCC), 2018-09.

[52] “Secure 5G and Beyond Act of 2020,” US Government , 2019-03.

[53] “Defense Applications of 5G Network Technology,” United States. Defense Science Board, 2019-04.

[54] "International Emergency Economic Powers Act," US Government, 1977-10. [Online]. Available: https://www.govtrack.us/congress/bills/95/hr7738.

[55] “Securing the Information and Communications Technology and Services Supply Chain,” U.S. Department of Commerce., 2019-12.

[56] “NIST SP 800-187: Guide to LTE Security,” National Institute of Standards and Technology (NIST), 2017-12.

[57] “TS #33.401 3GPP System Architecture Evolution (SAE); Security architecture_v16.1.0,” The 3rd Generation Partnership Project (3GPP), 2019-12.

[58] "Overview of Risks Introduced by 5G Adoption in the United States," United States Department of Homeland Security (DHS), 2019-07.

[59] "Commission Recommendation - Cybersecurity of 5G Networks," European Commission, 2019-03. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks.

[60] “Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings,” European Commission, 2019-03.

[61] “ENISA Threat Landscape for 5G Networks,” European Union Agency for Cybersecurity (ENISA), 2019-11.

[62] “EU Cybersecurity Act,” European Commission, 2019-06.

[63] “European Electronic Communications Code,” Official Journal of the European Union, 2018.

[64] “Technical Guideline on Security Measures_v2,” European Union Agency for Cybersecurity (ENISA), 2014-10.

[65] “EU coordinated risk assessment of the cybersecurity of 5G networks,” European Union Agency for Cybersecurity (ENISA), 2019-10.

[66] “Cyber-Sicherheitsstrategie für Deutschland (Cybersecurity strategy for Germany),” Federal Ministry of the Interior (BMI), 2016-11.

[67] “Key elements of additional security requirements for telecommunications networks,” Federal Ministry of the Interior (BMI), 2019-03.

[68] “5G Strategy for Germany,” Federal Ministry of Transport and Digital Infrastructure, 2017-07.

[69] "5G Security: A government view," National Cyber Security Centre (NCSC), 2017. [Online]. Available: https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/06_5GSECURITY/S02/NCSC_HAIGH.pdf.

[70] “UK Digital Strategy 2017,” Department for Digital, Culture, Media and Sport (DCMS), 2017-03.

[71] “Next Generation Mobile Technologies: A 5G Strategy for the UK,” Department for Digital, Culture, Media and Sport (DCMS), 2017-03.

[72] “UK Telecoms Supply Chain Review Report,” Department for Digital, Culture, Media and Sport (DCMS), 2019-07.

[73] "Cyber Skills Immediate Impact Fund," Department for Digital, Culture, Media and Sport (DCMS), 2019-08. [Online]. Available: https://www.gov.uk/government/publications/cyber-security-skills-immediate-impact-fund.

[74] "5G - Enabling the future economy," Department of Commission and the Arts, 2017-10.

[75] "National Security Legislation Amendment - Espionage And Foreign Interference," Australia Government, 2018-06. [Online]. Available: https://www.legislation.gov.au/Details/C2018A00067/Controls/.

[76] “Government Provides 5G Security Guidance to Australian Carriers,” Department of Commission and the Arts, 2017-10.

[77] "Agreement on IT procurement policy and procedures for goods and services," 2018-12. [Online]. Available: https://zh.cn.nikkei.com/politicsaeconomy/politicsasociety/33405-2018-12-07-11-33-55.html.

[78] "Common Standards for Information Security Measures for Government Agencies, 2016-08," Cybersecurity Strategic Headquarters, 2016-08. [Online]. Available: https://www.nisc.go.jp/eng/pdf/Common%20Standards(FY2016).pdf.

[79] "Location Information Act," 2016-05. [Online]. Available: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=43349&lang=ENG.

[80] "MIIT official website," [Online]. Available: http://www.miit.gov.cn.

[81] "Prague 5G Security Conference," 2019-01. [Online]. Available: https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-173333/.

[82] “Securing the Future of a Smart World - Opportunities & challenges in a 5G connected economy,” Business Performance and Innovation & A10 Networks, 2019-05.

[83] "The NIST cybersecurity framework (CSF) and what it can do for you," [Online]. Available: https://cybersecurity.att.com/blogs/security-essentials/the-nist-cybersecurity-framework-csf-and-what-it-can-do-for-you.

[84] "AT&T official website," [Online]. Available: https://www.att.com.

[85] “AT&T Developer Program: Security Requirements for Authorized Wireless AT&T Devices,” AT&T, 2007-05.

[86] “AT&T Information & Network Security Customer Reference Guide_v5.1,” AT&T, 2013-02.

[87] "Verizon Official website," [Online]. Available: https://www.verizonwireless.com.

[88] C. Silliman, "Verizon’s approach to 5G security," 2019-04. [Online]. Available: https://www.verizon.com/about/news/verizons-approach-5g-security.

[89] "Deustche Telekom official website," [Online]. Available: https://www.telekom.com/en.

[90] S. Schröder and S. Lachmund, "5G Security Driven By Deutsche Telekom," in *Cyber Security Tech Summit Europe*, 2019-03.

[91] "Cyber Security Tech Summit Europe," [Online]. Available: https://cyber-security-tech-summit.eu/en/2019.html.

[92] "Telstra official website," [Online]. Available: https://www.telstra.com.au.

[93] “Telstra Security Report 2019,” Telstra, 2019.

[94] "The five knows of Cybersecurity," Telstra, 2015-08.

[95] “Telstra Security Report 2018,” Telstra, 2018.

[96] "NTT DoCoMo official website," [Online]. Available: https://www.nttdocomo.co.jp/english/.

[97] "Trend Micro and NTT DOCOMO Collaborate to Provide New Solution for 5G Era," [Online]. Available: https://www.trendmicro.com/en_hk/about/newsroom/press-releases/2018/2018-11-02.html.

[98] "KDDI Corporation official website," [Online]. Available: https://www.kddi.com/english/.

[99] "SoftBank Mobile official website," [Online]. Available: https://www.softbank.jp/en/mobile/.

[100] "Rakuten officital website," [Online]. Available: https://mobile.rakuten.co.jp/corporate/english/.

[101] "SK Telecom official website," [Online]. Available: https://www.sktelecom.com/index_en.html.

[102] "SK Telecom Continues to Protect its 5G Network with Quantum Cryptography Technologies," SK Telecom & ID Quantique, 2019-03. [Online]. Available: https://www.idquantique.com/sk-telecom-continues-to-protect-its-5g-network-with-quantum-cryptography-technologies/.

[103] "ID Quantique official website," [Online]. Available: https://www.idquantique.com.

[104] "Quantum-Safe Security Relevance for Central Banks," ID Quantique, 2018-06. [Online]. Available: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180718/Documents/O_Pfeiffer.pdf.

[105] "KT Corporation official website," [Online]. Available: https://corp.kt.com/eng/.

[106] "KT embraces 5G with high level security technologies," [Online]. Available: https://www.telecomreview.com/index.php/articles/exclusive-interviews/3003-kt-embraces-5g-with-high-level-security-technologies.

[107] "New Measures on 5G by South Korean Telecompanies," [Online]. Available: https://kknews.cc/tech/bxnx64n.html.

[108] "The collaboration between LG U+ and Korean University on 5G Cybersecurity," [Online]. Available: http://www.zdnet.co.kr/view/?no=20191106173300.

[109] "The Collaboration among LG U+, Seoul National University and CryptoLab on the Development of Solutions towards Cybersecurity," [Online]. Available: http://www.newsis.com/view/?id=NISX20191219_0000865199&cID=13001&pID=13000.

[110] M. Herh, "LG U+ Says Final Reports on Huawei Security Verification to Come in August or September," [Online]. Available: http://www.businesskorea.co.kr/news/articleView.html?idxno=29009.

[111] “GTI 5G Network Architecture White Paper,” GTI group organization, 2018-02.

[112] S. Holtmanns 且 I. Singh, “4G - Who is paying your cellular phone bill?,” 於 *DEF CON 2018*, 2018.

[113] S. Hussain, O. Chowdhury, S. Mehnaz and E. Bertino, "LTEInspector: A systematic approach for adversarial testing of 4G LTE," in *Network and Distributed Systems Security (NDSS) Symposium*, 2018-02.

[114] “Mobile Edge Computing - Introductory Technical White Paper,” European Telecommunications Standards Institute (ETSI), 2014-09.

[115] “MEC Deployments in 4G and Evolution Towards 5G,” European Telecommunications Standards Institute (ETSI), 2018-02.

[116] “MEC in 5G networks,” European Telecommunications Standards Institute (ETSI), 2018-06.

[117] “Mobile Edge Computing: A key technology towards 5G,” European Telecommunications Standards Institute (ETSI), 2015-09.

[118] “TR #33.811 Study on security aspects of 5G network slicing management_v15.0.0,” The 3rd Generation Partnership Project (3GPP), 2018-06.

[119] “TR #33.813 Study on security aspects of network slicing enhancement_v0.5.0,” The 3rd Generation Partnership Project (3GPP), 2019-07.

[120] “Security BCP Recommendations for SDN/NFV,” Federal Communications Commission (FCC), 2016-12.

[121] “Network Functions Virtualisation (NFV) Release 3; Security - Security Management and Monitoring specification_v3.1.1,” European Telecommunications Standards Institute (ETSI), 2017-02.

[122] “TS #33.511 Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class_v16.2.0,” The 3rd Generation Partnership Project (3GPP), 2019-12.

[123] “資通安全管理法,” 行政院, 2018-06.

[124] “資通安全管理法施行細則,” 行政院, 2018-11.

[125] “臺灣 5G 行動計畫,” 行政院科技會報辦公室, 2019-06.

[126] “資通安全專業證照列表,” 行政院國家資通安全會報, 2019-03.

[127] “國家傳播通訊委員會-雙語詞彙,” [線上]. Available: https://www.ncc.gov.tw/chinese/bilingual.aspx.

[128] “行動寬頻業務管理規則,” 國家通訊傳播委員會, 2019-06.

[129] “國家教育研究院-雙語詞彙、學術名詞暨詞書資訊網,” [線上]. Available: http://terms.naer.edu.tw.

[130] “5G 基地臺開設計畫審查結果,” 總合通信機盤局, 2019-04.

[131] "電信法," 交通部, 2013-12.

[132] "電信管理法," 國家通訊傳播委員會, 尚未生效.

[133] “國家資通安全戰略報告-資安即國安,” 中華民國總統府, 2017-09. [線上]. Available: https://www.president.gov.tw/Page/317/969/國家資通安全戰略報告-資安即國安-.

附件一　「資通安全維護計畫參考框架」與「行動寬頻系統審驗技術規範修正草案」意見徵詢會與業界說明會徵詢意見與問題彙整紀錄

壹、 辦理「資通安全維護計畫應載明事項參考框架」之意見徵詢會議與業界說明會

本團隊於計畫執行期間舉辦「資通安全維護計畫應載明事項參考框架之意見徵詢會」，以及「資通安全維護計畫應載明事項參考框架之業界說明會」(如下表 1 所示)，邀集產官學研等專家學者，共同探討適用於我國 5G 網路資通安全風險評估項目及審驗作業程序之適用性及可行性，透過本次意見徵詢會議及說明會，共同提升整體資通安全防護及法規調適措施，建立國家 5G 資訊安全防護能量，確保 5G 網路資安防護功能與國際接軌，進而促進相關垂直應用場域及創新應用服務之發展。

表 1、意見徵詢會議與業界說明會列表

項次	主辦單位	活動日期	會議名稱
1	財團法人電信技術中心	108 年 10 月 31 日	資通安全維護計畫應載明事項參考框架之意見徵詢會
2	財團法人電信技術中心	108 年 12 月 17 日	資通安全維護計畫應載明事項參考框架之業界說明會 – 臺北場
3	財團法人電信技術中心	2018 年 12 月 18 日	資通安全維護計畫應載明事項參考框架之業界說明會 – 高雄場

資料來源：本團隊整理

註：項次 1「【行動寬頻業務管理規則】意見徵詢會議」會中邀請到通傳會孫委員雅麗講述資通安全維護計畫參考框架之核心價值與內涵，並獲得熱烈迴響，亦蒐集到多項寶貴意見，作為後續編修之參考。項次 2、3 辦理兩場次之業界說明會亦與與會業者有充分溝通，對於後續撰寫第五代行動通信系統資通安全維護計畫方向也更聚焦。

為完善資通安全維護計畫參考框架後續編修，除了於上述會議蒐集與會人員之意見，因會議時間有限，亦有與會者於會後提供相關意見並與研究團隊就參考框架內容與行動寬頻系統審驗技術規範修正方向交換意見，彙整如下表 2。

表 2、資通安全維護計畫參考框架意見彙整表

資通安全維護計畫參考框架		
項次	意見/ 團隊回覆	內容說明
1.	意見	NCC 應先提供系統審驗辦法中有關資安查驗項目與範圍之草案內容予業者討論，以評估可執行性，例如：若要求業者進行系統設備弱點掃描之資安測試，業者僅能提供 1 家『無高級以上資通安全風險』之證明文件；請業者提供系統上線前之核心網路系統切換、備援測試之文件，以說明當系統設備障礙發生時維持網路服務持續運作之強韌性。
	團隊回覆	現階段業者意見部分採納，亦可作為往後修訂的參考。電信技術中心已於 10/31 召開「行動寬頻系統審驗技術規範修正草案」意見徵詢會議並於會議與業者討論有關資安查驗項目與範圍之草案，內容。此外，於現行提供框架 17 項應載明事項，業者應考量自身風險與團隊工作能力，擇訂防護範圍。再以弱點掃描與滲透測試等方法，驗證防護措施之有效性。目前於修正草案中，僅要求業者應執行系統滲透測試、弱點掃描及相關修補作業，並說明辦理情形與提交佐證資料。另外針對強韌性之要求，業者應提供最近一場次執行資通安全事件通報及應變演練紀錄，以確保當系統設備障礙發生時，能維持網路服務持續運作之強韌性。
2.	意見	NCC 應規劃並公告合格資安查驗第三公正單位，及符合 ITU 或 3GPP 發佈之資通安全規範電信系統設備供應商清單，俾便業者遵循。
	團隊回覆	現階段業者意見部分採納，亦可作為往後修訂的參考。有關資安查驗第三方公正單位之議題，目前各業者之資

資通安全維護計畫參考框架		
		訊安全管理系統皆有通過第三方驗證，可考量於原本驗證範圍，延伸納入資通安全維護計畫應載明十七項自述內容。另第三方公正單位可參酌資通安全管理法（以下簡稱本法）第七條第一項規定，資通安全責任等級分級辦法「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構。另業者應主動請設備供應商，提供 5G 系統設備符合 ITU 或 3GPP 發布之資通安全規定之佐證資料，此項亦為業者於供應商管理之責任，尤以現今科技發展快速，倘若由通傳會公布符合 ITU 或 3GPP 發佈之資通安全規範電信系統設備供應商清單，恐有耽誤業者佈建或開基地臺之虞。例如 gNb 設備應請供應上提供符合 3GPP TS 33.511 之要求。主管機關將持續關注世界國際標準組織 3GPP、ITU 等 5G 資通安全標準發展狀況，但業者需就部署之相關設備自行與供應商確認並提供相關佐證資料。
3.	意見	NCC 應將系統功能性審驗作業與資安防護查驗作業脫勾，因二者監理目的與屬性均不相同，前者審驗作業著重系統能否正常提供服務；後者則為資通安全之管理維護。
	團隊回覆	現階段業者意見不宜採納，但可作為往後修訂的參考。依照 Security by Design, Security by Default 原則，資通安全應是 5G 系統原生功能，系統功能性審驗作業之資安功能審驗與資通安全防護查驗作業有部分雷同之處，現階段規劃之開臺前系統審驗項目已考量資通安全維護計畫 17 項應載明事項，大多以一般性審驗為主，少部分以功能性審驗以確保業者之資通安全維護計畫執行狀況，同時保障功能面與資安面之基本要求，開臺後將依資通安全維護計畫定期查驗稽核。
4.	意見	業者現有 NSA 系統架構均已上線支援 5G 功能，並符合現行資安防護相關規定，已上線之系統基於資安防護需求，無法接受任何潛在風險之入侵測試，亦無法再下線進行未來新增之資安防護查驗，應列在未來查驗之排除項目。
	團隊回覆	現階段業者意見不宜採納，但可作為往後修訂的參考。業者現有 5G NSA 系統尚未正式開基地臺，於商轉前進

資通安全維護計畫參考框架		
		行資安檢測以確認其是否符合資安防護規定應不致影響既有系統之運作，且資通安全檢測並非測試 5G 系統極限，而是確認資通安全控制措施為可用且有效，再者檢測並非長期性作業，只要慎選測試項目、時間及地點，可控制影響範圍與時段，業者亦可透過檢測掌握自身系統不足之處，以面對日益嚴峻之資通安全挑戰。業者在 5G 系統正式開臺前，宜考量於不影響服務水準之情況下，進行相關資通安全檢測，以確保資通安全防護措施之有效性。
5.	意見	建議未來僅就 5G 尚未上線之雲化系統（SA 5GC）進行較多之資安查驗，因 5G NFV 實體仍在各業者高度管制之機房內且使用非 OPEN SOURCE 之設備供應商軟體，應可簡化資安查驗項目。
	團隊回覆	現階段業者意見不宜採納，但可作為往後修訂的參考。現有已上線系統（如 5G NFV 實體）不論目前商轉與否或是位於高度管制之機房內，亦有可能因未來加入之新系統或規劃產生資通安全風險，因此進行資安查驗時應通盤考量各種可能威脅與風險，評估必要之資安查驗項目。為保障我國通訊網路關鍵基礎設施與消費者權益之基磐，業者應設置可信賴之 5G 系統，確保用戶隱私、資料與傳輸安全，以及 5G 系統之強韌性，主管機關亦宜敦促業者善盡社會責任。目前各業者之資訊安全管理系統驗證範圍與所提之資通安全維護計畫應載明十七項自述內容不盡相同。業者除應確實依資通安全維護計畫執行，亦須依照行動寬頻系統審驗技術規範，就行動寬頻系統暨設備資安防護之項目，提報執行情形佐證資料。
6.	意見	有關「十、資通安全事件通報、應變及演練相關機制」之資通安全事件應變小組成員是否須包含資通安全長？
	團隊回覆	業者宜考量針對資通安全事件或事故訂定處理程序，並依照事件或事故等級通報處理，倘若發生事件或事故時，如需啟動緊急應變計畫，宜由適當之資通安全權責人員確認啟動。
7.	意見	第二項核心業務及其重要性中，支持 5G 業務的內部服務的相依性也需考量，「內部服務」是指什麼？

資通安全維護計畫參考框架		
	團隊回覆	在行動通信系統中，尚有許多相關業務支援部門，未來與 5G 系統介接或是維運部門，例如資訊技術部門、網路技術部門等，亦須納入考量。
8.	意見	在十七、通過資通安全管理驗證之執行方案中，所謂第三方驗證機制之第三方驗證組織為何？
	團隊回覆	根據目前資安管理法下資通安全等級分級辦法，有關資訊安全管理系統第三方驗證的規定，如臺灣認證機構（Taiwan Accreditation Foundation，TAF），或國際認證機構認可的驗證機構皆可進行驗證。
9.	意見	有關十三、所屬人員辦理業務涉及資通安全事項之考核機制是否須針對 5G 系統獨立列出審查評估機制？
	團隊回覆	業者可重新審視現有人員資通安全績效考核機制，惟考核方式與內容宜進一步確認是否足以涵蓋 5G 系統與其相關風險等。
10.	意見	通傳會可否提供資通安全維護計畫之範本，作為撰寫之參考？
	團隊回覆	現階段業者意見不宜採納，但可作為往後修訂的參考。考量各家業者電信系統設計架構不一，使用之資通訊技術或設備亦不相同，業者應依據自身規劃與架構，撰寫資通安全維護計畫。

資料來源：本團隊整理

貳、 辦理「行動寬頻系統審驗技術規範」之意見徵詢會議

為確保我國 5G 系統之資通安全，政府除要求 5G 得標者依據新版行動寬頻業務管理規則提報並執行資通安全維護計畫，並透過開臺前的系統審驗與後續定期稽核，從營運開始就確保業者所設置之 5G 網路系統具備足夠的安全、強韌、及可信賴性。

鑒於 5G 得標者於建置網路前已提報之資通安全維護計畫並提出資通安全防護及控制措施等作為，唯業者建置網路時所實施之資通安全防護及控制措施是否完整有效，將攸關 5G 網路系統的安全可靠、用戶個人資料隱私、以及服務品質與消費者權益，因此業者在正式開臺營運前需配合監理機關之系統審驗作業再次進行查驗，此階段之審驗重點將側重於以一般性或功能性審驗進行查核，用以確認業者實施之資通安全作為，能夠確保 5G 系統為安全且可信賴的環境。為事先確保法規調整方向與內容能配合實際需要並與外界充分溝通，故本團隊於計畫執行期間舉辦「行動寬頻系統審驗技術規範修正草案」之業界意見徵詢會議並支援通傳會進行後續溝通活動，宣導 5G 通訊架構應具備之資訊安全作為，並且了解產、官、學、研及相關利害關係人之意見回饋及建議，以利後續法規調適之參考。

註：「【行動寬頻系統審驗技術規範修正草案】意見徵詢會議」亦透過與電信業者討論，逐漸收斂業者對行動寬頻系統審驗技術規範修正草案之看法。

本團隊在計畫執行期間於 108 年 10 月 31 日舉辦「行動寬頻系統審驗技術規範修正草案」意見徵詢會議，邀集產官學研等專家學者，共同探討適用於我國 5G 網路資通安全風險評估項目及審驗作業程序之適用性及可行性，透過本次意見徵詢會議及後續意見收集整理說明會，共同提升整體資通安全防護及法規調適措施，建立國家 5G 資訊安全防護能量，確保 5G 網路資安防護功能與國際接軌，進而促進相關垂直應用場域及創新應用服務之發展。

為完善行動寬頻系統審驗技術規範草案修正，除了於上述會議蒐集與會人員之意見，因會議時間有限，亦有與會者於會後提供相關意見並與研究團隊就參考框架內容與行動寬頻系統審驗技術規範修正方向交換意見，彙整如下表 3。

表 1、行動寬頻系統審驗技術規範修正方向意見彙整表

行動寬頻系統審驗技術規範修正方向		
1.	意見	有關 5G 行動寬頻系統審驗技術規範草案 4.7 項：資通安全防護及控制 4.7.1 系統設備符合 ITU、3GPP 或 NIST 等組織資通安全規定之證明文件或佐證資料。 臺灣大哥大電信提問：目前行動寬頻系統主要網路設備皆已遵循法規，未採購大陸廠牌設備，若有其它國家安全考量事項，請給予業者實際指引。
	團隊回覆	現階段業者意見不宜採納，但可作為往後修訂的參考。有關國家安全考量事項，業者可參酌「各機關對危害國家資通安全產品限制使用原則」之相關規定，除盤點已經採購、來自危險地區的產品清單外，亦可持續關注禁用產品清單之發布狀態。
2.	意見	有關 5G 行動寬頻系統審驗技術規範草案 4.7 項：資通安全防護 4.7.1 系統設備符合 ITU、3GPP 或 NIST 等組織資通安全規定之證明文件或佐證資料。

行動寬頻系統審驗技術規範修正方向		
		五大電信提問：是否由原廠出示切結即可？
	團隊回覆	現階段業者意見不宜採納，但可作為往後修訂的參考。業者應主動請設備供應商，提供 5G 系統設備符合 ITU、3GPP 或 NIST 發布之資通安全規定之佐證資料，此項亦為業者於供應商管理之責任。此外，除要求設備供應商提出佐證資料外，業者宜培養自身資通安全能力，以近一步驗證設備供應商所提出之佐證資料是否正確無誤。
3.	意見	有關 5G 行動寬頻系統審驗技術規範草案 5.1.9 項：空中介面加密功能 遠傳提問： 1 詢問原廠，AS 無法提供，僅能提供 NAS 手機截圖。至於執行語音及數據 NAS 及 AS 審驗，是否也能考量採用設備商切結模式？ 2. 建議使用切結書方式滿足系統審驗需求 註：其餘業者回覆：實務面如何確認，如何提供佐證資料，已請承商了解中，尚未回覆（亞太電信另增加「排除 GSM 系統外」）。
	團隊回應	現階段業者意見不宜採納，但可作為往後修訂的參考。空中介面 NAS 與 AS 層的加密機制為 3GPP 規範訂定，所有系統（包含 GSM、LTE、5G）應遵照語音及數據測試進行，除非系統經設備商提供無法開啟該項功能之切結，否則應與其他功能性審驗項目相同，接受抽樣檢測證明系統已開啟加密機制（或可考慮以工程手機或截取系統 Log 呈現）。

資料來源：本團隊整理

附件二 「2019 洛杉磯－全球行動通信系統協會世界行動通訊大會（GSMA Mobile World Congress Los Angeles，MWCLA）」參訪報告

財團法人電信技術中心出國報告

出席 2019 洛杉磯－全球行動通信系統協會行動通訊大會（GSMA Mobile World Congress 2019 Los Angeles）

單位名稱：檢測暨網通技術組、資通安全組

姓名職稱：吳東興高級工程師、李兆文工程師、李贛麟工程師

派赴國家：美國

出國期間：2019/10/20-2019/10/27

報告日期：2020/01

摘要

2019 年 10 月 22 日至 24 日於美國洛杉磯舉辦之「2019 洛杉磯－全球行動通信協會世界行動通訊大會（MWCLA）」，本次大會主題為「智能連結（Intelligent Connectivity）」，本團隊參加 MWCLA 展覽會議，藉由會中電信業者、設備製造商、服務應用提供者、政府機關等組織單位分享經驗，汲取美國在 5G、IoT 物聯網、以及電信安全發展之最新技術及趨勢，並將此次參訪所獲得之最新資訊與成果紀錄於參訪報告中。

今年 MWCLA 展場最令人驚艷的為許多 5G 的具體實現，展覽會場上展出許多 5G 的設備從晶片、手機、基地臺、到核心網路及網路技術解決方案，並透過眾多 5G 場域的垂直應用體現，以及物聯網應用結合人工智慧(AI)，除展現今年大會智慧聯接(Intelligent Connectivity)的主題，讓各界參加者可藉由各種展出思考未來可能的商業模式與發展。在此引述 GSMA 執行長洪曜莊(John Hoffman)的談話，他表示「行動產業觸及全球數十億人的生活，隨著 5G 到來，它將再次改變全球消費行為和商業模式。2019 MWCLA 將展示橫跨整個產業的龐大生態系統和鄰近產業的一系列最新行動科技的變革用例，探索當今的新可能性。」

參、 目的

本次前往美國洛杉磯參與參加 MWCLA 論壇會議，主要是邀關注美國在 5G 上的發展趨勢，並鎖定相關技術發展之資安議題，調查美國最新政策作為或防護指引。本次 MWCLA 的參與者主要來自歐美地區，亞洲廠商偏少，且中國品牌的 5G 設備供應商並無出席。近兩萬名與會者共同探討 5G 行動行業和更廣泛的生態系統的主要趨勢。本次出國行程主要目的包含：

參加 MWCLA 論壇會議，了解全球各國際組織、官方單位、國際電信設備製造商、大型跨國電信業者等專題演講、就 5G 技術、垂直應用專網、物聯網應用服務、以及資安議題，包含邊緣運算 MEC、網路虛擬化、網路切片、開源端對端設備、智慧城市應用、領域知識及商業模式進行資料收集與了解。

參觀 MWCLA 各電信設備廠商或垂直應用服務業者之展示攤位，蒐集全球最新主流之通訊技術、應用服務及商業模式等相關資訊。

肆、 行程

一、 出國時間：108 年 10 月 21 日至 10 月 27 日

二、 地點：美國洛杉磯

三、 本中心出席人員：吳東興高級工程師、李兆文工程師、李贛麟工程師

四、 時間安排：

日期	行程
10 月 20 日(日)	差旅時間：臺北－洛杉磯 桃園機場 10 月 20 日 19:20 出發 洛杉磯國際機場 10 月 20 日 16:20 抵達 （臺灣時間 10 月 21 日上午 7：20）
10 月 21 日(一)	調整時差、會議準備
10 月 22 日(二)	2019 洛杉磯世界行動通訊大會 MWCLA 三日議程
10 月 23 日(三)	
10 月 24 日(四)	
10 月 25 日(五)	整理會議資料
10 月 26-27 日 (六-日)	差旅時間：洛杉磯－臺北 洛杉磯國際機場 10 月 26 日 00:50 出發 （臺灣時間 10 月 26 日下午 15：50） 桃園機場 10 月 27 日 05:45 抵達

五、 會議資訊

(一)會議名稱：2019 洛杉磯世界行動通訊大會（MWCLA）

(二)2019 MWC Los Angeles 展覽會場資訊：

https://www.mwclosangeles.com/conference-programs/agenda/#day=1799

(三)會議時間：108 年 10 月 22 日至 10 月 24 日

(四)會議地點：洛杉磯會議中心（Los Angeles Convention Center）

(五)會議議程：

除了主題演講活動之外，MWCLA 洛杉磯大會還推出 27 場數位轉型相關的專題活動，以 5G、物聯網(IoT)、人工智慧(AI)和沉浸式內容為四大主題。主題具體內容包括：



圖表 1：2019 洛杉磯世界行動通訊大會四大主題

- 5G：經濟學、邊緣運算、工業物聯網、頻譜和網路切片。
- 物聯網：運輸、協作智慧和安全。
- 人工智慧：倫理觀、區塊鏈、顛覆性創新和資料分析。
- 沉浸式內容：擴增實境/虛擬實境(AR/VR)、現場表演、內容創作、發行、遊戲、運動和娛樂等主題領域。

「主題演講 Keynote」議程 (Keynote Auditorium)		
10/22	09:30~ 11:30	開幕專題演講 Keynote 1: Opening Keynote
10/23	09:00~ 10:30	專題演講 Keynote 2
	10:45~ 11:45	技術長們對 5G 之看法 CTOs Talk 5G

「主題演講 Keynote」議程 (Keynote Auditorium)		
	11:45~ 12:00	加速美國創新–國防部 5G 契機 Accelerating American Innovation – DoD 5G opportunities
10/24	09:30~ 11:00	專題演講 Keynote 3

「政策演講 Everything Policy」議程 (Theater 411)		
10/22	13:00~ 13:45	立法政策倡議：國會議程 Legislative Policy Initiatives: Congressional Agenda
	13:45~ 14:05	FCC 委員 Brendan Carr 主題演講 Keynote Remarks Featuring FCC Commissioner Brendan Carr
	14:05~ 14:50	5G 年：頻譜政策更新 The Year of 5G: A Spectrum Policy Update
	14:55~ 15:10	CISA 總監 Christopher Krebs 主題演講 Keynote Remarks Featuring CISA Director Christopher Krebs
	15:10~ 15:55	保護新興的 5G 網路 Securing the Emerging 5G Networks
	16:00~ 16:15	FCC 委員 Jessica Rosenworcel 主題演講 Keynote Remarks Featuring FCC Commissioner Jessica Rosenworcel
	16:15~ 17:00	5G 20/20：美國的市場驅動力 5G 20/20: Market Drivers across the U.S.
10/23	13:00~ 13:15	FCC 委員 Mike O'Rielly 主題演講 Keynote Remarks Featuring FCC Commissioner Mike O'Rielly
	13:15~ 14:00	無人空中服務 Up, Up and Away: Unmanned Aerial Services
	14:05~ 14:50	WRC-19 的國際頻譜優先事項 International Spectrum Priorities Heading into WRC-19

「政策演講 Everything Policy」議程 (Theater 411)		
	14:55~ 15:10	NTIA 助理部長 Diane Rinaldo 主題演講 Keynote Remarks Featuring Diane Rinaldo
	15:10~ 15:55	通過聯邦隱私立法保護消費者 Protecting Consumers with Federal Privacy Legislation
	16:00~ 16:15	FCC 委員 Geoffrey Starks 主題演講 Keynote Remarks Featuring FCC Commissioner Geoffrey Starks
	16:15~ 17:00	內部的無線政策：FCC 顧問的觀點 Wireless Policy from the Inside: FCC Advisors' Views

「5G 演講」議程 (Concourse 152)		
10/22	13:00~ 14:00	5G 營銷：從速或從優進入市場？ Marketing 5G: First or Best to Market?
	14:15~ 15:15	偏鄉地區之連接：商業模式是否存在？ Rural Connectivity: Is the Business Model There?
	15:45~ 17:00	5G：力量、全球、利潤 5G: Power, Planet, Profit
10/23	13:00~ 14:00	5G 網路：深入討論 5G Networks: Hard Talk
	14:15~ 15:15	專用網路 vs 5G 網路切片 Private Networks vs 5G Network Slicing
	15:45~ 17:00	5G 之網路邊緣 5G On The Edge
10/24	11:00~ 12:00	保障 5G 策略不過時 Future Proofing your 5G Strategy
	12:15~ 13:15	5G 對您的未來安全嗎？ Is your Future Safe with 5G?
	14:00~	這是我們所熟知的行動終端嗎？

	15:00	Is this the End of Mobile as we Know it?

「IoT 演講」議程 (Concourse 151)		
10/22	13:00~ 14:00	擴展智能物聯網 Scaling the Internet of Intelligent Things
	14:15~ 15:15	邊緣計算：創造新的物聯網應用 Edge Computing: Creating New IoT Applications
	15:45~ 17:00	物聯網連接的承諾 The Promise of IoT Connectivity
10/23	13:00~ 14:00	零售物聯網：逛街及購物體驗 IoT in Retail: The Shopping and Purchase Experience
	14:15~ 15:15	醫療照護物聯網：改變治療及改變生命 IoT in Healthcare: Changing Treatments and Changing Lives
	15:45~ 17:00	製造業物聯網：自動化、改善與機器人 IoT in Manufacturing: Automation, Optimization and Robots
10/24	11:00~ 12:00	智慧城市及智慧世界 Smarter Cities, Smarter World
	12:15~ 13:15	物聯網裝置：始終傾聽、觀察及學習 IoT Devices: Always Listening, Watching and Learning
	14:00~ 15:00	安全的物聯網 The Internet of Safe Things

「IoT 演講」議程 (NexTech Stage - West Hall)		
10/23	10:30~ 11:15	網路防護 Safeguarding the Network
	11:30~ 12:30	5G 案例及新興資安需求 5G Use Cases and New Security Needs
	14:00~ 14:45	物聯網安全 IoT Security
	15:00~ 15:45	如何在 5G 時代持續受到保護 How to Stay Protected in the 5G Era

伍、 會議過程及內容

以下就主要展場參觀及交流、參與場次分別重點介紹：

一、 主題演講（Keynote）

(一)技術長們對 5G 之看法

ACG Research 行動與無線網路首席分析師 Chris Nicoll 提出到 2020 年為止，全球將會超過 1/5 的市場推出 5G 服務，並且在 5G 網路基礎設施建置上的總共花費將達到 2440 億美元。5G 時代的來臨是必經的行動網路演進過程，未來行動網路服務與數位生態系統服務之融合成為必然趨勢。相關電信運營商在推動 5G 服務下，如何因應快速變化的環境採取相對應之經營策略，並在競爭激烈的市場上取得適當的角色定位。電信業者除了探討傳統電信網路營運成本外，未來還必需考慮到 5G 網路商業化之經營條件與要素，本次受邀出席的技術長們（Chief Technology Officer, CTO），將暢談自家公司 5G 網路推出之準備情形，以及未來的發展藍圖。AT&T 技術長 Andre Fuetsch 宣示，公司將全力以赴為企業組織提供 5G 服務。Fuetsch 表示，我們認為 5G 最大宗之用戶將會是公司企業，而且我們正在進行數十項測試來證明這一點。Fuetsch 敘述，5G 多接取邊緣運算（Multi-access Edge Computing, MEC）技術在智慧工廠上扮演重要角色,例如能完成生產線上所有產品之數據即時收集、分析、傳輸，這主要依賴於 5G 增強型行動寬頻通訊（Enhanced Mobile Broadband, eMBB）之實現。確切來說，智慧工廠可以透過 5G 網路將傳送過來之大量之產品數據進行分析，瞭解使用者之實際操作情形，透過 5G eMBB 之優勢，縮短工廠和使用者間的認知差異。未來 5G 在智慧辦公室應用中也將扮演重要角色，5G MEC 平臺可以創造更多的垂直應用服務功能，包括位置感知、安全性、地理圍

欄（Geofencing）技術之驗證、自動化作業等。Fuetsch 說，有了 5G，用戶實際上可以將位置精準度由幾公尺降低到幾公釐。企業能利用 5G 網路優越特性，在地理圍欄範圍內控制特定物理位置之資料生成或數據傳輸。AT&T 認為這些就是令人振奮之 5G 垂直應用服務場景實現，這些位置應用服務亦可以實現在辦公室空間範圍內，位置感知只是許多不同應用服務場景中的一種。Fuetsch 舉例製造商能透過改變智慧手機的外形尺寸來獲得利益，這就是 5G 自由度的表現，而且 5G 確實為不同設備之間的互通性打開了大門。另外，自駕車和虛擬實境（Virtual Reality, VR）之應用服務確實給消費者留下深刻的印象，但是 Fuetsch 認為未來 5G 將會改變消費者的生活，包括人們生活中的大小事務。Fuetsch 提供了一個令人驚訝的例子，具物聯網（Internet of Things, IoT）功能的叉子和牙刷可以分析消費者熱量的攝取或牙菌斑的形成。當看似普通的日常事物可以用數據進行分析並幫助消費者有益之處，而且可以即時了解自己的健康狀況，因此 5G 可以驅使人們養成更健康的習慣。5G 真的是令人振奮，因為 5G 是一個完全不同的網路架構，Fuetsch 認為這些改變將成為改變世界的真正關鍵因素。Sprint 技術長 John Saw 闡述，Sprint 是美國唯一一家提供 2.5GHz 頻段服務的電信運營商，並指出其客戶使用的數據量是其 4G 網路的 3~5 倍，而且其 5G 手機的平均下載速率可以達到 200Mb/s，而 4G 手機的平均下載速率達到 37.5 Mb/s。目前 Sprint 的 5G 網路的覆蓋率已經包括了 9 個都會區約 1600 萬人。另外，Saw 針對他們的競爭對手 AT＆T 和 Verizon 電信業者以悠然自得的態度評論，AT＆T 以及 Verizon 都在毫米波（mmWave）上推出了 5G 的服務，但是他們忽略了覆蓋率這個關鍵問題。然而，Sprint 的優勢在於我們擁有全國最大的 5G 覆蓋範圍，我們的行動客戶在城市中任何地方都可以體驗 5G 網路的快速

服務。甚至 AT&T 以及 Verizon 的毫米波系統操作人員，其手上可能並沒有相對應之 5G 基地臺部署之精準對應地圖。Sprint 可以讓我們行動用戶體驗到 5G 網路的使用快感，因為我們才是真正實踐 5G 行動網路室內、外覆蓋率的重要推手。Sprint 亦看到了 2.5 GHz，這個中頻帶的真正潛力，其頻譜使用效率令人印象深刻，Sprint 相信中頻頻譜的利用，有實力成為企業與消費者的最佳使用頻段。T-Mobile USA 技術長 Neville Ray 強調 T-Mobile 計畫將在今年年底之前為 2 億人提供 600 MHz 頻段之使用覆蓋率，而且會找尋可以使用於該頻段並具相容性之行動網路設備，預計在 5G 網路開臺之前就會公布所使用之 600MHz 行動網路設備。行動網路設備運營商在今年初已經在 28 GHz 和 39 GHz 毫米波頻段中提供一些相關的 5G 應用服務。Ray 亦在該議程上說明，我們的行動網路設備商將計畫與 Sprint 進行大規模的商業合併，進而可以提供低、中、高頻段的 5G 網路服務。我們的頻譜與 Sprint 的頻譜能夠合併使用，對公司來說是非常振奮人心的事。目前，T-Mobile 已經推出了 5G 網路毫米波的應用服務，我們將會在今年底之前在美國境內推出 600 MHz 的 5G 網路服務，其中 Sprint 所提供的 2.5 GHz 頻帶可以與我們的 5G 網路中頻帶一起融合使用，這也是讓美國的電信商用市場夠能真正實現 5G 應用服務體驗的一種方式。我們亦可以在美國境內的沿海、農村、城市地區進行頻譜、公司設備資產的合併使用。如果 Sprint 所提的合併案能獲准，Ray 預計美國將成為未來幾年中第一個，也是唯一一個能夠支援 5G 網路低、中、高頻段之全頻段使用之國家。T-Mobile 除了預計在 5G 推出之前推出 600MHz 的使用，亦將會推出一款 5G 智慧型手機，並且能夠支援即將推出的 5G 網路 600 MHz 頻段。另外，美國運營商 OnePlus 將獨家提供 OnePlus 7T Pro 5G McLaren 智慧型手機以供消費者使用。Verizon 資深副總

裁兼首席網路官 Nicki Palmer 談論到，Verizon 的 5G 服務即將來臨，將會在 2020 年正式提出商用 5G 獨立（Standalone, SA）網路解決方案。5G SA 關鍵基礎設施架設就是 Verizon 未來發展方向，我們會儘快實現。Verizon 對 5G SA 的商用化非常重視，因為 5G SA 網路能夠實現才能真正展現 5G 網路服務的快速特性。Verizon 現在正在與 Ericsson、Nokia、Samsung 協作建設 5G 網路關鍵基礎設施，2020 年也將大規模實施動態頻譜共享（Dynamic Spectrum Sharing, DSS）技術。Palmer 強調，5G SA 架構具有獨立的 5G 核心網路（Core Network）與 5G 無線電接取網路（Radio Access Network, RAN）新無線電（New Radio, NR）技術，並能夠執行網路切片（Network Slicing）功能，把特定數量的網路切片和頻譜資源彈性化按照用戶需求分配給指定客戶使用。網路切片功能對 5G 核心服務業務具有很大的商業經營效益。Palmer 亦提到目前最新的無線電接取技術_開放式無線電接取網路（Open Radio Access Network, Open RAN）概念。很明顯的，開放式無線電接取網路前景很好，但是要能真正實現，系統和功能必需具備整合性與互通性兩個關鍵因素，因此 Verizon 一直朝著這個目標持續努力。Verizon 希望掌握 5G 服務在商業界與企業界之消費者需求，並能超越同業競爭對手，所以近期公司內部單位進行了一些人事組織改組。雖然目前 5G 非獨立（5G New Radio Non-Standalone, NSA）網路即將商用，但是 Verizon 還是會繼續投資在 4G LTE 網路之關鍵基礎設施建置以及相關垂直應用服務開發。

(二)加速美國創新–國防部 5G 契機

美國國防部（United States Department of Defense, DoD）透露了目前正在評估 5G 實驗並尋求建議，同時計畫在許多軍事基地啟動 5G 測試平臺的計畫，DoD 將與民營公司夥伴合作進行大規模實驗。國防部副部長 Dr. Lisa Porter 在發表演講時說；「國防部認為，掌握

無處不在的網路連結將使軍隊維持與對手的競爭優勢。」但她也補充說明選擇 5G 並非是最終的決定，而是保持「我們將永不辜負我們與持續創新的承諾」，與民營企業和整個政府的合作夥伴進行合作。

此外 Lisa 還強調了 5G 的安全性試驗：「我認為最大的挑戰是我們想確保我們真正了解 5G 的潛在弱點（Vulnerability），例如使用 5G 可能暴露用戶的位置，將用戶的服務降級到舊的行動數據網路，大量增加用戶的無線網路賬單，甚至追踪用戶打電話、發短訊、瀏覽網頁之記錄。國防部真的想與業界合作，以確保我們儘早了解 5G 技術及安全性的發展，並開始推動大眾對行動數位化時代的安全性重視。」國防部預計將在今年 2019 年末時候開始宣布測試地點和用例，並根據當年度可用預算，進行各季預算調配，與民間企業進行合作，確保 5G 對國防之可用性及安全性。

第一部分將涵蓋四個軍事基地，主要包含：動態頻譜共享模型，以展示 5G 如何在軍事雷達流量擁擠的環境中運行（類似於 3.5GHz 中已經完成的工作）；整合 AR 和 VR 進行任務計畫和培訓；和智慧倉庫技術來改善物流。

(三)10/24 專題演講

關於全球關注的 5G 對氣候衝擊議題方面:多位演講者提到 5G 支持的應用將為環保計畫做出重大貢獻，而這將超過新技術帶來的能源使用增加。

惠普企業首席可持續發展官克里斯托弗 Wellise 說，儘管他預期 5G 將導致功耗的增加，但是給社會帶來的好處將遠遠超過所產生的功耗:「到 2025 年，我們預計所有數據的三分之二將在邊緣生成，不再需要在集中的運算中心發生。它發生在農業領域，智能城市，智能工廠車間。」Wellise 說。「我們需要將計算移動到數據所在的位置，而不是將數據移動到計算所在的位置。移動數據要比處理數據多耗費一個數量級。」。

Verizon 首席可持續發展官兼 ICT 可持續發展組織 GeSI 主席 James Gowen 同意，儘管 5G 可能「潛在地」導致更多的能源使用，但 5G 帶來的應用影響將產生重大影響。他說:「5G 絕對會對氣候產生巨大影響。」,「當我們將 Verizon 的工作與全球各地的公司結合在一起時，我們正在尋找可以合作的方法，因為最終，可持續性是我們必須要做的事情。」。

美國國家可再生能源實驗室副實驗室副主任道格•阿倫特（Doug Arent）補充說:「我們認為，減碳是智能解決方案未來的核心要素。它是智能電網，交互式建築，是智能移動平臺，結合了邊緣計算,人工智能,機器學習和預測算法,可為人類提供預測能力。」。

另外有關 5G 提供娛樂潛力方面，華納兄弟娛樂公司首席數位官 Thomas Gewecke 則指出了行動通訊設備已成為日益增長的消費媒體內容平臺，因此華納兄弟娛樂公司現在正在將 5G 視為一種利用移動優勢，並為消費者提供新內容體驗的管道。他表示：移動設

備正成為影視消費不可思議的重要平臺,「它不僅適用於短片內容,而且適用於長片電視劇和電影。」,同時並強調手機也是「最大,增長最快的手機遊戲類別之一」。

二、 政策演講（Everything Policy）

由 CTIA 主導的「政府與公共政策（Government and Public Policy）」專題活動將由知名政策制定者和業界專家參加，探討頻譜、基礎設施及監管政策的決策如何影響投資和創新。

(一)CISA 總監 Christopher Krebs 主題演講

主講人做為美國國土安全部新成立的部門主管，他認為美國在 2016 年的大選中所遭到的網路安全事件,使得美國民眾開始把網路安全視為重要的事情，美國人民意識到網路安全的風險與攻擊，不僅僅是破壞銀行或商業公司，亦有可能動搖了美國人的生活方式並且造成政府動盪。所以主講人的單位開始與國會以及其他的聯邦機構合作與對談來應付目前的情況。除了政府機關煎的合作，也需要民間更廣泛的參與，達成風險識別和解決方案的整合，也就是說 CISA 將進行合作式風險管理和風險分析，共享資訊，並以公私協力聯繫以幫助管理風險。主講人認為若要達成上述願景，需要有四個支柱，第一個支柱是確保和提高美國關鍵基礎設施的強韌性。第二個支柱是與聯邦機構合作，以增強防禦態勢。第三個支柱是創建可互通的緊急通信，而第四個是長期風險管理。最後主講人提到他們今年已經與其他聯邦機構展開工作，並對聯邦政府的 ICT 供應鏈安全作出指導建議。

網路安全和基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）總監 Christopher Krebs 闡述，CISA 負責保護國家之關鍵基礎架構免受物理和網路的威脅，此項任務需要政府

部門和民營組織之間的合作與協調。在執行網路全面保護上，CISA 提供網路安全工具，分析事件響應和網路防禦功能，並向聯邦政府提供全天候之網路狀態感測，以保護與支援聯邦民政部門和機構之基本運營網路。CISA 採取公共部門與民營部門之間合作方式來協調安全性和彈性之工作，並為聯邦政府有關業者、基礎設施業者及運營商提供培訓、技術支援以及評估。CISA 透過國家風險管理中心（National Risk Management Center）為美國關鍵基礎設施提供安全與威脅評估以及整合，並進行規劃、分析、合作、協調等關鍵性資通安全工作，以識別和應對美國國土內之關鍵基礎設施之相關重大風險。CISA 加強了各級政府間公共安全訊息傳遞，提供培訓、協調、工具及指南，以幫助合作夥伴發展其緊急通信能力，包括宣傳活動、支援及增強緊急應變當發生自然災害或恐怖主義行為、災難發生時之傳遞能力。CISA 總監 Christopher Krebs 強調，做為美國國土安全部新成立的部門主管，他認為美國在 2016 年的大選中所遭到的網路安全事件，使得美國民眾開始把網路安全視為重要的事情，美國人民意識到網路安全的風險與攻擊，不僅僅是破壞銀行或商業公司，亦有可能動搖了美國人的生活方式並且造成政府動盪。所以主講人的單位開始與國會以及其他的聯邦機構合作與對談來應付目前的情況。

除了政府機關間的合作，也需要民間更廣泛的參與，達成風險識別和解決方案的整合，也就是說 CISA 將進行合作式風險管理和風險分析，共享資訊，並以公私協力聯繫以幫助管理風險。主講人認為若要達成上述願景，需要有四個支柱，第一個支柱是確保和提高美國關鍵基礎設施的強韌性。第二個支柱是與聯邦機構合作，以增強防禦態勢。第三個支柱是創建可互通的緊急通信，而第四個是

長期風險管理。最後主講人提到他們今年已經與其他聯邦機構展開工作，並對聯邦政府的 ICT 供應鏈安全作出指導建議。

(二)保護新興的 5G 網路

主持人首先詢問關於聯邦政府的供應鏈管理的議題，提到關於近期美國聯邦政府所組織的 ICT 供應鏈風險工作小組(Information and Communications Technology Supply Chain Risk Management Task Force)的完成工作與目前情況。由來自美國國土安全部(DHS)的 Robert Kolasky 回答，Kolasky 表示這是一個跨機關的工作小組，這個工作小組本身沒有特定的法定職權去決定任何事情，但 DHS 有建立公私合作的職權，它所做的事情是把利害關係人都聚集在一起，包含政府機關與私人公司，這個工作小組會指導各聯邦政府機關如何降低供應鍊風險，他認為這樣展開對公共政策的對話做法是相當合適與聰明的。該工作小組第一年的成果是已經建立一些模組，這些模組有些可以展示供應鏈目前有哪些威脅與風險，也有的模組是進行情資分享，特別是從情報部門來的情資，另外有些模組是針對如何進行軟硬體設備的採購。透過這樣的模組框架，聯邦政府除了可以對各模組進行整合外，聯邦政府可以大量採用這些模組，這也有助於情資分享。小組的另一個工作成果是該工作小組列出好幾種關於供應鏈的風險情境，把威脅進行分類，也針對業務需要進行分類，同時也列出資安防護的最佳實務。

主持人接著詢問來自 NTIA 的 Evelyn Remaley，問道：該工作小組的構成是否符合期待。Remaley 回答這是由政府與產業界組成的工作小組，成員們具有很強的領導力。她認為該工作小組最大的特色是連續性，也就是從國會的政策指導與法案、各級聯邦政府的採購執行以及產業界的解決方案，這些都需要廣泛的與各界溝通與

聯繫，使得供應鏈安全可以連續而不出現缺口。DHS 的 Kolasky 也附和這樣的談話，他認為需要有這樣的機制，使得多達二十多個聯邦機構有對話的機會。他認為如果美國的最終目標是擁有可持續且安全的供應鏈，最好就是把政府機構與產業界都找來，商討建立最佳實務與示範案例。他繼續提到工作小組的下一個目標是情資分享的機制，DHS 已經有一些成果，但這事永遠有進步空間。

主持人詢問 Evelyn Remaley 關於總統網路安全命令(Cybersecurity Executive Order，EO)最近的進度。Remaley 回答這也是跨機關的工作，有 DHS 也有情報部門參與。當把供應鏈安全作為整體安全考量的一環時，總統網路安全命令是一項可以使用的工具。但不僅僅是供應鏈，從美國經濟利益考量與維持美國長久的經濟的競爭力，目前新興的科技如 5G、AI 與 IoT 等，美國需要採取措施來保證這些科技的生態圈是可以信任的，特別是這些科技在基礎設施的使用，如 5G，所以 NITA 目前致力於軟體元件透明度。另外去年 EO 也使得 IoT 設備的資安基準有所提升，在殭屍網路的防治上有一定的成果。

主持人詢問來自產業界的與談人，各公司在邁向 5G 時如何處理供應鏈安全問題。

Ericsson 的 Jason Boswell 認為與政府合作是個好的起點，要使得供應鏈更加透明，且要關注端到端的安全，在設計軟體與硬體時就需要將安全與可靠性考量進去。Ericsson 在美國 5G 市場會帶入許多第三方供應商，Ericsson 也會提升這些第三方產品與服務透明度。

Nokia 的 Mohammad Khaled 則說 Nokia 會先對風險進行評估，如核心網路就比接取網路重要。Nokia 在設計階段也如 Ericsson 一

樣納入安全考量也有保證流程，如弱點分析、安全軟體設計，軟體發佈後也有更新機制。他認為虛擬化的安全也是相當重要，如何知道軟體是否處於安全狀態，軟體配置與韌體是否正確，如何設定安全的功能開啟與否，這些都是需要處理的工作。

AT&T 的 Christopher Boyer 則說 5G 雖然是新興技術，但沒有想像中的不安全，畢竟有許多組織如 3GPP 開始添加安全功能到 5G 中。作為電信業者他對供應鏈安全的擔憂是如果有一家供應商，因為國家力量的資助，無視市場規律，搶占市場份額，這樣的結果會導致單一供應商，AT&T 期待的是有競爭且長久的供應鏈市場。

主持人問來自高通的 John Kuzin 關於 4G 與 5G 的不同。John Kuzin 則說 5G 在用戶隱私、加密算法、核心網路上都更安全。DHS 的 Kolasky 則說 5G 的來臨會使得產業界的安全文化改變，安全會變成產業的競爭力。Remaley 認為 5G 除了技術上的改變與經濟競爭力的改變外，這些改變不會獨立發生，美國需要與他的盟友找出值得信任的供應商應該具備甚麼面貌。

主持人再問來自高通的 John Kuzin，高通在 5G 安全的成果是什麼。John Kuzin 則回答高通認為如何確認裝置是被授權用戶使用是該公司認為的安全基礎，高通公司已經在其晶片納入鑑權與授權的功能，使得開發商能夠簡單地使用這個安全功能。

主持人再問關於 5G 標準的制定情況。與談人稍微介紹了 3GPP 標準的制定進度，DHS 的 Kolasky 則補充，從美國政府的觀點，3GPP 標準是全球通用，但如何使得美國在 5G 繼續掌握競爭力，美國持續有 5G 科技的領導力是政府考量 5G 標準的重點，當然美國政府不是制定標準的成員，但政策應引導產業界站立有利位置以符合美國利益。Remaley 則說 NTIA 有參與 3GPP，也有參與 3GPP 的

資安小組，NTIA 會持續與產業界對話，找出激勵機制使得產業界 R&D 成果符合標準。

最後主持人問明年的熱門單字。與談人則回答：5G、量子、IoT、零信任架構(Zero Trust)、工業物聯網、6G。

(三)內部的無線政策：FCC 顧問的觀點

美國無線產業協會(CTIA)法規事務資深副總裁 Scott Bergmann 陳述美國聯邦通信委員會（Federal Communications Commission, FCC）和國家電信暨資訊管理局（National Telecommunications and Information Administration, NTIA）之政策制定專家正在積極推動於美國境內進行無線網路部署工作，包括確保有足夠的頻譜來推動 5G 網路的創新服務以及執行公共安全和普及服務之計畫。此議程探討內容豐富，透過無線網路專家的精闢見解（這些專家均為 FCC 和 NTIA 領導層級），瞭解到美國目前推動/執行無線網路生態系統之內部政策、提供給企業之相關建議、目前經濟問題與決策協調之方式。FCC 的 O'Rielly 委員辦公室無線與公共安全之國際法律顧問 Erin McGrath 由頻譜政策開始談起，再講述到 5G 關鍵基礎設施架構，最後以無線電源充電策略作為結尾。委員會拍賣了 24 GHz 和 28 GHz 頻段，並將在 12 月舉行 37 GHz、39 GHz、47 GHz 頻段拍賣，其中美國無線網路專家將就高頻段之傳輸容量、速度、延遲方面進行相關研究與了解。McGrath 強調應立即重新分配現有頻段，而頻段較高部分可能會帶來挑戰，因此需要快速完成必要的研究，以便我們知道該頻段物理特性，且需要什麼樣的資通安全保護措施。委員會已經在關鍵基礎設施部署方面討論了許多重要問題，尤其著重於小型基地臺的部署討論。儘管目前這些部署的籌設還處於委員會行政審查階段，但是我們可以事先採取其他措施來減少 5G 關鍵

基礎設施部署將會面臨的問題。McGrath 建議將來的電源可能必須具備與傳統電源不同之功能。原因在於對於很多設備，附帶插座的插頭與一次性電池很可能會被無線充電所取代。優勢在於可以避免維修或更換插座、插頭、電池等工作，而且還可以減輕充電設備的重量以及具有更簡便之功能與機制。

FCC 的 Rosenworcel 委員辦公室，無線與國際法律顧問 Umair Javed 描述，Gartner 於分析新興技術發展週期中提到，大家對 5G 的期望都太高，原因是許多電信業者還無法確認 5G 核心業務到底為何，5G 網路將如何推動並提供新形態的產品和服務，以滿足消費者心中真正想要的價值與渴望。關於中頻帶頻譜，FCC 僅在致力於如何通過高頻段頻譜市場化，以支援 5G 無線網路之應用服務。然而，將高頻段頻譜商業化並不容易且價錢不會更便宜，瞭解企業和消費者真正需求將會比密集化網路部署更為重要。面對 5G 網路時代的到來，我們必須思考開放式網路建構模式。我們可以著重於網路化、虛擬化、軟體化等設計面向，替代以硬體為網路設計架構之解決方式。在這種新形態模型中，我們可以使用現成的硬體並透過過軟體定義網路（Software-Defined Networking, SDN）來達到 5G 網路虛擬化之目標。Javed 還認為全球 60％以上的行動數據流量已轉移到 Wi-Fi 上，未來 5G 的需求和業務服務（例如強型行動寬頻通訊（Enhanced Mobile Broadband, eMBB）、虛擬實境（Virtual Reality, VR）及物聯網技術（Internet of Things, IoT））亦將可能使用部分不須執照的頻段來連接與使用，這代表許多無需執照的頻段可以幫助 5G 網路核心業務推廣。

FCC 的 Pai 委員辦公室無線與國際法律顧問 Aaron Goldberger 說明，新型態的 3.5 GHz 頻譜共享概念，反映了小型和大型的電信營運商、設備商、第三方應用服務供應商的高獲利營運模式，且能

改變軟體開發商、晶片製造商、手機與設備製造商之商業經營方式。我迫不及待的期望能看到這種新形態企業組織之組成，且多元化聯盟的合作成果能夠成功。在3.5 GHz頻譜共享的推動上能夠有成果，歸功於特定公私部門之間無私的協作，非常感謝國家電信資訊中心的所有政府部門、行政單位及國防部。3.5 GHz 頻譜共享的推進所涉及的問題很多，但是 FCC 已解決了這些難題。未來 FCC 能持續在 3.5 GHz 頻段上努力，將能為相關機構與單位之間的合作提供一個典範，這是我必須全力以赴的工作。我很感激無線通訊局委員會、工程局及經濟與分析辦公室為此付出之長期努力。

FCC 的 Starks 委員辦公室幕僚長兼無線與國際資深法律顧問 William Davenport 陳述，今天我要傳達的資訊是在技術上的解決方案，是有機會幫助與解決世界上最重要的關鍵問題。5G 網路的啟用帶來新挑戰，並可讓我們用來克服相關難題。5G 網路將連結數十億個設備，讓能源使用更有效率，並降低對國家、地方及當地環境的影響。5G 將智慧電網技術提升到新的境界，讓能源公司能夠在用電高峰期之前先完成前置處置，立即中斷相關的路由器，以達到最有效的供電方式，減少消耗和汙染排放。智慧工廠、智慧建築物及智慧家庭能調整照明和暖氣供應，以減少能源損耗。農民可根據所獲得之數據分析，精準的減少農藥用量、水使用量及有害排放物，同時大幅提高農作物產量。車聯網技術將車輛互通性概念實現，道路交通設施可提供最有時效性之路線給予駕駛參考，大大減少了80％以上的二氧化碳排氣量。這些都是 5G 網路商用化之契機。我相信 5G 將會改變全世界，新形態的電信技術將幫助我們擁有改變這個世界的巨大能力。



圖 3-2-1 政策演講 Everything Policy 議程 - 內部的無線政策：FCC 顧問的觀點

三、 5G 演講

(一)5G 營銷：從速或從優進入市場？

5G 發展優勢一直是新一代行動網路技術的重中之重，但是從速或從優進入市場後所造成的後續效應為何是主要探討之問題。ACG Research 行動與無線網路首席分析師 Chris Nicoll 提出觀點，隨著在 5G 網路消費者身上所獲得的利益的逐漸減少，未來在 5G 網路之獲利將會著重在工業和企業之使用上。5G 技術需要與現有服務兼具互通特性，因此運營商現在應該更專注將最好的產品與應用服務推向市場以及消費者，並且要保證所有應用服務之品質與考慮企業合作在業務面上如何來獲取最大利益，例如工業界、企業界、消費者為什麼要關心和使用 5G 網路與其相關之應用服務。此議程將討論我們是否需要創新的 5G 經營模式與銷售模式思維，而在競爭激烈的市場上誰將成為先知和最後贏家。Opensignal 執行長

Brendan Gill 介紹了 Opensignal 的 5G 技術相關分析。與會中 Gill 探討了行動網路技術中之先發優勢的歷史、其在 5G 無線通信中的運用、最佳市場的地位以及對消費者、用戶及企業的利益之真實意涵。Gill 提出 5G 還處於初期階段，但 Opensignal 已經看到了一些值得注意的地方以及商業網路之利益。5G 網路不僅會提供更快的速度且新技術將提供使用新的高頻寬和高容量結構。高頻頻段亦將有助於減輕頻段擁塞影響了整個行動網路之消費者體驗。而且 4G 升級不僅會體現在速度上，5G 也會大大改善了延遲，創造了一個全新的世界行動應用服務場景，但是要普及到 5G 需要很長時間。Gill 的描述提供了消費者 4G 行動網路體驗的寫照，並隨著我們將步入全新的 5G 網路時代。Airspan 行銷副總裁 Damiano Coletti 描述，隨著全球運營商制定戰略並投資於 4G 網路的不斷增強，並推動 5G 的部署和商業化，網路的架構方式正在發生根本性的變化。為了有彈性的提供容量並為新的 5G 應用服務場景以及應用服務做準備，運營商正在尋求虛擬化，以幫助在日益密集的網路環境中平衡性能和成本。Airspan 是一家屢獲殊榮的 4G 和 5G 網路高密度化解決方案提供商，在全球範圍內部署了近一百萬個蜂巢小區，並提供廣泛的室內和室外之密集型 Femto、Pico、Micro 以及 Macro 基地臺產品組合。利用 mmWave、Sub 6GHz、Massive MIMO、開放式虛擬化 RAN 架構等技術之具創新潛力工具套件，以及針對 PTP 和 PTMP 應用的行業之固定無線接取和回程解決方案組合。Boingo Wireless 首席技術官 Derek Peterson 博士說，5G 是繼 1G、2G、3G、以及 4G 之後的第五代蜂巢網路技術。5G 在前幾代產品的基礎上構建了高速網路，包含實體傳輸網路之前傳光纖、中傳光纖、後傳光纖架置架構的引入，旨在為眾多設備和多種設備保持優越之性能。5G 規範針對的是密集區域，這些區域直接適用於室內使用。5G 的好處

包括更高的流通量、更低的延遲、更大的帶寬以及通過較小的小區使得無線電更靠近邊緣。此外，Peterson 博士強調 IoT 大規模物聯網也是 5G 標準的主要支柱。5G 依靠窄波長訊號，因此需要更近距離的超密集天線節點基礎架構，這是 5G 擴散的重要障礙，也是 Boingo Wireless 的基礎架構專業知識來的地方。Boingo Wireless 對 5G 基礎設施採用融合方法，以互補的方式使用許可的 5G 和未經許可的網路來應對高智能手機使用情況，因應在密集的應用服務場景中支援高速數據需求。Telefonica 網路技術資深副總裁 Juan Carlos Garcia 說明，我們每個人都要率先做到在 5G 這方面從速或從優進入市場這一塊，首先要推動對消費者有用之應用服務程序最為重要。5G 新技術將使我們擁有更好的連接性和更快的反應速度，並為我們所有的消費者提供最佳體驗和最佳解決方案。5G 技術將允許依靠低延遲雲端設備在特定環境中部署關鍵應用服務，而無需更改現有網路設備，甚至擁有一個全球 5G 備份系統且該系統保留與固定網路相同的功能和服務。Telefonica 已與 NOKIA 和 ERICSSON 建立了合作夥伴關係，以在西班牙的 Segovia 和 Talavera de la Reina 城市初步部署 5G 功能，這是 Telefonica 在 5G 技術城市項目上的一部分，而且該項目將引領該國 5G 之發展。



圖 3-3-1 5G 演講議程 - 5G 營銷：從速或從優進入市場？

(二)偏鄉地區之連接：商業模式是否存在？

5G 網路建置與鄉村我們可以很容易理解到其發展矛盾之處，尤其是目前在 4G 網路覆蓋範圍不到 70%的北美地區，而且 2G 網路仍然在使用的情況下。LYA 聯合總裁 Johanne Lemay 簡述，儘管第三代行動電話承諾消費者具有無處不在的網路覆蓋範圍保證，且網路覆蓋率的績效達成持續增高，但是與鄉村的連通性仍然是一個日益嚴重的問題。另該考慮為，目前鄉村之基礎設施建置規劃是否合乎 5G 電信業者經營之核心業務政策與目的，是否是時候該改變一下我們一直處於 5G 建置與發展之彼此競爭之環境。電信公司是否可以不需要搭建 5G 塔臺嗎，第一線和第二線參與 5G 建置的運營商業務模式該如何規劃？在 5G 繼續成為新聞頭條的同時，藉由此議程將探討 4G 和現有傳統基礎設施的關鍵屬性，以便了解鄉村社區的消費者實際使用狀況，並討論 5G 到底能帶來什麼樣的不同的改變？American Tower Corporation 垂直市場副總裁 Steve Baker，

對於行動網路之鄉村地區的連通性是非常大的挑戰對，電信業者必須了解鄉村地區消費這對於 5G 網路之服務需求是什麼，要有將 5G 網路服務品質提升至城市地區的水準，甚至能讓鄉村消費者有超越城市環境之使用體驗。不管鄉村地區或城市地區，只要消費者有所需求就要部署 5G 基礎設施與其使用。在網路之有效利用上並符合電信業者經之營利條件，5G 新技術之軟體無線電（Software Defined Radio）與頻譜共享是可以考慮運用的。此外，鄉村地區智慧電線桿、太陽能電池板及生態系統之部署亦為營運經營的構思，其中 Anchor 租用與第三方電信業者之合作是解決覆蓋率不足的一個解決方案。Cisco 商業服務副總裁 JL Valente，高速移動連接早已為城市區域中的企業和社區之必備條件。但是，在很少有人使用高速網路於鄉村地區之環境，電信網路業者投資高額的頻譜資源於鄉村地區並不總是具有經濟效益，因此許多鄉村地區無法連接至高速網路。由於頻譜共享的出現，我們相信 5G 可以改變這一個現狀，尤其我們必須證明這一點。Cisco 已經在鄉村地區進行了許多不同的 5G 實驗，從相關的鄉業地區之鄉業技術和工業物聯網之無線電廣播等。透過實證，我們希望證明在城市之外投資 5G 連接的價值，以釋放新的經濟機會，這將使全國所有人民享受利益。STC 資深顧問兼執行長 Wael Bayaydh，儘管無線電訊號可能會因潮濕而略微減弱，但是目前的光纖實體有線網路的設計和構建具有足夠的能力解決這樣的問題，可以輕鬆克服即使是大雨或濃霧的影響，但是成本、部署、安裝是 3 大問題。在成本方面，光纖服務對電信業者而言需要很高的投資，結果可能會很昂貴，並且要求服務提供商簽訂長期合約以回收投資成本。然而無線網路部署成本較低，從服務消費者端來說大大降低了電信業者之成本花費。於部署上，無線網路可以在鄉村地區真實環境視察後馬上進行快速部署並且立即安裝和啟動給與

消費者使用。但是光纖網路部署需要開挖鄉村道路和小路才能到達其最是當之佈建位置時。這必須與鄉村地區居民透過簽署協議，來制約且該路線部署是復雜性高或可行及不可行。當鄉村居民不支持在歷史悠久的村莊中安裝光纖後，出現於道路之的坑疤狀況。光纖安裝需要在消費者終端點附近都必須開挖溝渠，這將涉及挖掘鄉村居民的花園或車道。無線網路就不需要任何挖掘工作，因為就像您家的電視天線一樣，無線信號是從物業的高處接收的。英國 DCMS 5G 測試總監 Ian Smith US Cellular 技術長 Mike Arizzarry 說明，US Cellular 選擇了一種獨特的方法來實施 5G 標準，以期獲得競爭優勢，同時改善其農村客戶的服務品質。這些特殊的功能與 US Cellular 經營市場在鄉村地區之特定消費者的專屬應用服務有關。此外，US Cellular 的智慧連接可以通過 US Cellular 智慧連接網路解決方案提供支持偏鄉地區之連接的解決方案，保持聯繫、控制、監視及管理消費者的資產，該解決方案模式專門為消費者在農村地區的生活和工作場所所建立。5G 網路的放性特性適合用於各種應用服務場景，且 5G 的前景令人振奮也確實存在一切未來性的期待。但是，5G 相關的經營模型目前也非很明確。這就是為什麼人們會嘗試使用不同的東西，看看會有什麼樣的效果以及原因。



圖 3-3-2 5G 演講議程 - 偏鄉地區之連接：商業模式是否存在？

(三)5G：力量、全球、利潤

Deloitte 總監 Mic Locker 引道，隨著全世界關注在最新之 5G 創新技術，未來我們對於 5G 網路的依賴性對持續性的成長，這也成為 5G 系統會被持續關注的關鍵目標。不僅要求電信運營商必須要擴大訊號覆蓋範圍，業者本身更還要降低建置與經營成本，以最大努力降低行動網路之佈建對環境所造成的影響。因此，電信業者的主要營運模型是否可以持續承受高複雜度與高成本為營運核心之負擔。到底 5G 對目前環境會有什麼亦想不到的影響和後果，電信業者是否以在短期和長期內獲利並且營收金額是持續性的增加。Cisco 服務提供者業務資深副總裁兼總經理 Jonathan Davidson 描述，Cisco 的精神在於公司的責任就是社會的責任，以積極力影響人類、社會及地球，並加速解決全球問題。在傳輸能量消耗上的創新突破，Cisco 研發的技術在傳輸相同的資料量下，一直持續降低能量耗損，從 2009 年的 10Watts/ Gbps 變成 2019 年 0.2Watts/ Gbps，足足降低

了 50 倍的耗損，進而達到保護環境的政要關鍵技術。服務提供商面臨的經濟挑戰上，包括 5G、數位影像、雲端等服務，其 CAPEX 的 Exabytes / month 從 2007 年的 12MBpm 一直持續增加到 2018 年的 230MBpm。預計在 2023 年可達到 890 MBpm 的驚人營收。Cisco 5G 提供了一種開放的、高度可編程的架構，可將企業、供應商、消費者之多域網路精簡為一個精簡、快速、統一的系統。Cisco 利用對雲端技術、IP 路由、5G 核心、邊緣服務運算、訪問網路、物聯網及安全性的廣泛了解，在 5G 服務中創造了真正的價值。Cisco 5G 架構提供了流量工程，用於頻寬管理，對應用程序的網路進行控制以及支援靈活的網路拓撲，以確保交互式服務的運作。Ericsson 持續發展與企業責任副總裁 Heather Johnson 描述，Ericsson 敢於領導並兼具設計力量，幫助服務提供商突破可能的極限，使 5G 栩栩如生。在專注力的設計概念上，透過提高生產力、娛樂性、沈浸式遊戲的新水平來提升消費者的遊戲水平。將高速連接與低延遲相結合，超優質的解決方案使消費者能夠提供令人難忘的獨特用戶體驗。考量更有效率的設計，城市無線傳輸方案和室內解決方案可為消費者提供廣泛而密集的高訊號品質的覆蓋範圍。每一位消費者都能賞受到一致性的傳輸以及 5G 核心服務之效能，以提供更快、更智慧、更可靠的網路服務。在消費者實際運作上，透過為企業與消費者所配備的智慧、可擴展、靈活的物聯網解決方案，以超高速和高彈性之連接來增加公司之營收。此外，使用上支援 AI 技術、網路切片技術及多重邊緣運算來提高網路整體效率。Spirent Communications 5G 業務主管 Stephen Douglas 接下來描述，Spirent 一直致力於發掘電信運營商在 5G 中取得成功所需的測試和保證解決方案，我們一直在探討在智慧連接的概念上，如何讓 5G 實現並讓企業與消費者有著真實體驗。然而，5G 網路中的智慧連接會涉及到新的天線模

組和晶片模組技術，進而完成新的架構、新的 KPI、新的供應商、雲分佈及新的頻率。因此，行動網路整個生命週期中的智慧測試和服務對於保證 5G 的成功實現至關重要。目前 Spirent 在 5G 獨立核心網路開發上兼具有所有階段之快速驗證技術，以便電信供應商可以按照時程規劃推出高品質量 5G 網路垂直應用服務。Spirent 亦使用模擬的獨立 5G 核心網路，進行主動式測試和監視端到端網路切片運作情形，根據 AI 的特殊技術可確保行動設備上的數位影音質量性能比人工的評估更加便宜、更可重複及更快實現。針對語音，數據，數位影音及位置估計相關之智慧手機和 IoT 設備進行性能測試，以加快 5G 設備的部署並加快實驗室解決問題的速度。因此，Spirent 獨特的測試和保證解決方案，可確保加速 5G 的發展。



圖 3-3-3 5G 演講議程 - 5G：力量、全球、利潤？

(四)5G 網路：深入討論

可以預期的是，5G 時代的來臨將對現行電信生態體系及商業模式產生極大的轉變。另一方面，隨著 IoT 物聯網及 AI 人工智慧的興起，也為服務創新及網路應用開創了新的快速競爭局面。因此行動通訊領導者們的商業思維模式需要進一步考慮未來 5G 的發展

目標、政治因素是否阻礙 5G 的發展、可以提供那些額外功能、是否應以軟體為核心。

本次會議重點集中在 Huawei 技術美國公司首席安全官 Andy Purdy 呼籲採用更全面的 5G 安全檢驗方法，以解決圍繞該技術的長期安全擔憂。同時希望 3GPP 應該著眼於針對不同應用服務的場景威脅建模研究，參考在歐盟和德國建立安全框架的類似工作，並加快對電信產品安全的通用測試標準和法規要求等協調制定工作。Purdy 指出，在美國存在一些分散注意力和混亂的消息，但是他也承認 Huawei 已經考慮了一些政府的關注。他說：「到目前為止，在應對 3G 和 4G 時代的威脅方面，我們已經做出了一些安全性增強工作，這些作為讓人鼓舞，但是我們還有一段路要走。」他也建議國家管理機構需要對產業政策進行重新思考，因為舊的信任模型不再符合未來需要，我們正處在一個需要強化風險管理和增強抵禦能力的網路環境。「我們的想法是，透過與公私單位合作，以我們應該弄清楚作為一個設備供應商需要考慮什麼、做什麼、以及開展什麼研發，以符合國家的新監管模式。」

他最後表示，與全球政府和民間單位組織合作仍是 Huawei 對應網路安全威脅議題的最大優先項目之一。他說：「我希望看到更多的公開測試，讓我們對產品進行公開測試，以便比較網路效能的同時可以比較安全功能；面對各種已發布的漏洞消息，我們甚至可以在有條件、受控制的情況下，提供實時網路進行現場駭客比賽，以便我們可以共享資訊並從這些活動中受益。」



圖 3-3-4 5G 演講議程 - 5G 網路：深入討論

(五)專用網路 vs 5G 網路切片

5G 網路將會較既有 4G 網路更加複雜，因為支援多元化的應用，5G 業者針對大規模的物聯網、虛擬與擴增實境、自駕車等應用、將帶給網路更大更快之效能壓力，必須開始考慮提供具備網路切片、小型覆蓋範圍、微型基地臺等客製化的服務，而這些專用網路與網路切片技術勢必會對電信業者的基礎網路架構產生影響，這都讓電信運營商必須考慮是帶來干擾還是帶來新商機。

首先會議主持人 Besen Group 創辦人兼執行長 Alex Besen 指出，專用網路是針對消費者，企業和物聯網的獨立專用網路。專用網路需具備行動性、安全、高可靠度、足夠覆蓋、低延遲等主要特徵，至今已有超過 33%的工業製造廠商評估過 5G 專用網路，其中並有超過 46%開始進行研究專用網路的部署案例。

ASOCS 執行長 Gilad Garon 則以結合專用網路與網路切片技術的使用範例為題，強調以內網結合邊緣運算之專用行動雲將創造新

的商機，舉出在包括手機/平板控制、影像追蹤、智慧機械手臂、無人機監控、智慧眼鏡等工業 4.0 上的多種應用，以及在運動賽事現場及企業分支機構的使用範例，並期待全球政府能對專網釋出免費或共享的頻譜。他說：「ASOCS 通過開放和虛擬化的軟體解決方案正在改變傳統的 RAN 市場，提供 4G 和 5G 的 LAN or WAN 的行動接取網路解決方案。我們的本地移動雲可通過現成商用的 IT 硬體，提供符合 ORAN 的解決方案，使電信業者及其客戶能夠享受更高水平的性能與可靠性，滿足關鍵任務和本地專用網路。」

座談會小組一致認為隨著大規模的 IoT、VR、AR、以及智慧工廠等多元化應用，將給目前行動通訊網路的效能與容量帶來巨大壓力；為了支援 5G 應用，電信業者需要提供具有網路切片，小型行動基地臺和覆蓋範圍等優勢的客製化 5G 服務網路，而這些量身定制，提供智慧連接時的私有網路興起也將會大幅改變電信業者的商業模式。

Verizon 產品開發與公共部門主管 Nick Nilan 則將焦點放在 5G 對公共安全的影響；他指出專有網路與 5G 行動通訊網路是可以共存並互補，行動寬頻技術的進步將使安全和各種救援團隊將能夠保持即時通訊，替換效率低下的雙向無線電系統或容易延遲的 4G 訊號；各種智慧應變載具、偵測遙控感測器網路、人體攝像機和其他穿戴設備都需要快速的數據傳輸和低延遲才能有效運行。

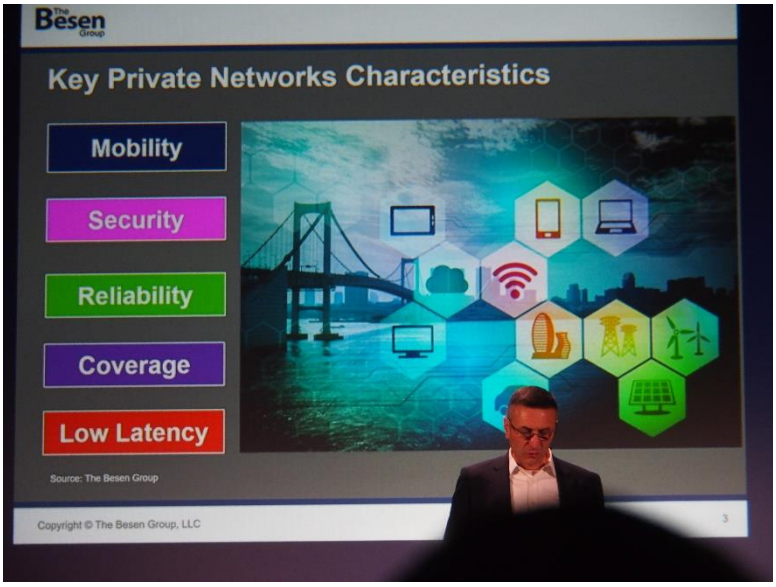


圖 3-3-5 Besen Group 提出之專用網路應具備之特性說明

(六)5G 之網路邊緣

下一代行動網路及服務的第一波浪潮正在持續推進中，5G 技術除了可以大幅提升虛擬與擴增實境等高頻寬體驗外，更可為自動駕駛、遠距控制帶來顯著的延遲優勢，因此邊緣運算技術在 5G 網路中就扮演了關鍵角色；為確保消費者可獲得最佳之服務品質及安全需求，行動網路與邊緣運算間的協作將至關重要。

主持人 GSMA 行動智庫主管 Peter Jarich 在座談會上提到，透過邊緣運算可以讓行動計算資源更接近數據來源，加上 AI 技術的利用可以降低延遲並減少傳輸量、提高容量和彈性；行動計算對邊緣設備的數據分析增加了系統的整體分析能力、獲得更好的安全性和隱私保護，同時處理數據越接近源頭可減少數據量及跨網路傳輸，降低了潛在攻擊面。

Akamai 物聯網及行動技術長 Lior Netzer 提及「Akamai 相信，我們正在提供具有可擴展性、操作簡便性和安全性的下一代資訊傳遞解決方案，以及一個可以讓客戶專注於核心業務的全包式解決方

案，使得客戶無需集成和管理離散但必要的資訊傳遞元件。隨著 IoT 邊緣運算的推出，我們正在利用邊緣的力量並將其帶入由聯網設備和應用程序組成的下一個先進領域。」。

Altiostar Networks 策略及產品管理執行副總裁 Thierry Maupile 則表示，透過開放式虛擬 RAN 解決方案，客戶可以使用同類最佳的解決方案來部署其無線接入網路；這不僅可以實現硬體和軟體的分解，還可以使運營商實現一個平臺，從而可以部署微服務。這個新生態系統的關鍵基本方面之一是，它使服務提供商處於構建供應鏈，控制支出，安全性和自身移動網路集成的主導地位，而不是依靠一兩個供應商而已。



圖 3-3-6 5G 演講議程：5G 之網路邊緣

(七)保障 5G 策略不過時

5G 時代的來臨將使電信業者產生不同的想法，雖然增強行動寬頻應用將是 5G 一開始的核心應用，但隨著新無線接取網路和核心網路的相關技術成熟，自駕車、智慧工廠和遠程醫療手術等新新產業生態系統將逐步實現。面對行動通訊技術發展迅速，電信產業

應提早規劃 5G 長期策略，以確保相關投資可以獲得最佳的投資回報率。

主持人 Price waterhouse Coopers（PwC）合夥人 Dan Hays 現場展示了 PwC 對 5G 迄今進展的分析，並預測了未來 6 個月的進展。隨著 5G 設備的問世以及更多市場上線，5G 部署可能是一個漫長的過程。他說「截至 2019 年 7 月 1 日的分析發現，我們才剛剛起步，不到 1%的美國人口在家中或公司可使用 5G 網路，而且使用的行動設備中只有不到 0.5%啟用了 5G。這兩個數據點的交集反映了美國 5G 市場。前面的路很長，而且在很多方面都比前幾代移動電話要復雜。展望到 2020 年 1 月 1 日的六個月，我們預測美國人口的 10％將獲得 5G 網路覆蓋，而 2%的設備將啟用 5G。」此外，5G 佈建雖然是美國電信業者列為第一優先，但也並非唯一，如 4G 擴建及虛擬化就仍是第二優先規劃，幾乎所有受訪者都已經完成了部分或全部，並將在未來 2 到 3 年內完成核心虛擬化。至於 RAN 的虛擬化則因為技術挑戰和不清楚總擁有成本（Total Cost of Ownership）效益，目前現況尚未明朗。

VMware 執行副總裁兼電信與邊緣雲業務總經理 Shekar Ayyar 則樂觀表示：「5G 將是一種變革性技術，這使我想起了網際網路的早期，因為創新和提高成本效率的潛力是巨大的。」，隨後現場座談會成員並討論到由於既有技術的規範，建立 5G 網路不同於 4G；部署 5G 的成本非常高昂，它需要一個更高密度的網路，該網路面臨監管，成本和運營方面的挑戰，包括它需要非常大的頻譜網段，以及在全國範圍內安裝數十萬個小型蜂巢小區，而且目前消費者並不要求或願意為此付出更多的費用。

5G 承諾增強連接體驗，並改善我們享受多媒體娛樂，購買產品和服務甚至經營我們的家庭和企業的方式。但是理想用例遠非真實情況，行動營運業者需要努力使用戶願意使用 5G 消費，而且產業鏈參與者間的合作結盟仍未產生足夠的吸引力，並給創新帶來了新的障礙。

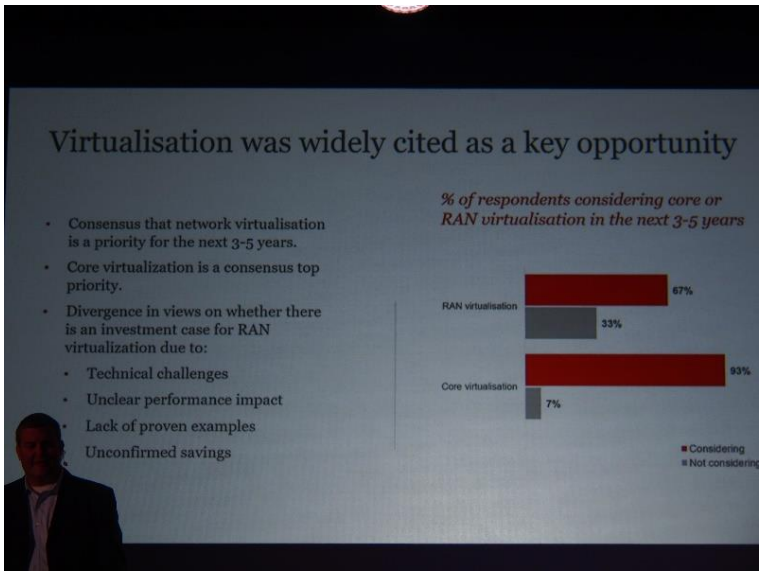


圖 3-3-7 PwC 提出之 5G 網路虛擬化預測趨勢

(八)5G 對您的未來安全嗎？

目前全球已有部份國家商轉 5G，對安全的網路基礎設施需求越來越強烈，相關網路安全議題也被持續廣泛討論；不僅針對 5G 之新技術與服務，繼續存在的前幾代網路技術亦需納入安全考量。除了利用人工智慧進行 5G 網路安全連接之偵測與驗證，更重要的是在設計、建置階段就納入安全考量因素。

主持人 GSMA 產業安全及技術主管 Jon France 提及，在 5G 時代，由於各項垂直應用將高度採用虛擬化與雲端化系統，加上全球資安威脅與攻擊手法與日俱增，強化行動通訊安全是愈發重要且需

要被重視及落實，5G 標準在制定之初就帶來增強的安全性和隱私性的設計。

Nokia 安全副總裁 Mary O'Neill 則強調，5G 需要從架構的第一天開始就考量到安全性，而不是趕快大量部署才在後續對其進行修補；O'Neill 提醒電信業者需要趕快改變現狀，不再可以使用既有的解決方案來面對 5G 安全問題。她說：「我們需要更多的技術，當我為 Nokia 制定策略時，我們將投資於機器學習、演練腳本、工作流程，並且我們非常相信自動化可以改善此問題。」。

McAfee 首席消費者安全宣傳員 Gary Davis 也提及，5G 即將到來，隨之而來的是不斷變化的威脅格局，既有 Mirai 攻擊將透過大量 IoT 轉化成更具破壞力的 Reaper 殭屍網路；隨者 5G 將廣泛應用於生活各層面，越來越多的設備連上網路，提供更多更容易施展攻擊的管道，未來網路犯罪（Cybercrime）將隨著這波趨勢逐步成長且工業化。

Qualcomm 安全產品管理資深總監 Jesse Seed 則將焦點放在 IoT 的安全性議題；她說，2018 對 IoT 惡意攻擊就成長了三倍，因此在 5G 即將推出之時，隨之而來需要增強網路安全性；此外還需要強化終端安全性，在系統單晶片（System on a Chip）設計時就考慮進去，因為當前設備經常缺乏足夠的安全，同時也需要和為 IoT 終端推出國家法規及安全認證標準。



圖 3-3-8 Nokia 提出現今資安面臨新的挑戰

(九)這是我們所熟知的行動終端嗎？

隨者行動寬頻通訊技術的成熟普及，各種智慧型手機已經成為人們日常生活中最重要的隨身工具之一，但隨著 5G 時代逐漸來臨，相關行動虛擬實境、擴增實境、超高畫質串流視訊、人工智慧、物聯網開始快速發展，行動終端亦出現了各種可能之發展，並將轉變演化出適用各種應用服務情境的不同類型專屬行動終端。

主持人 Mobile Ecosystem 常務董事 Mark Lowenstein 特別指稱：未來十年的行動通訊將與過去十年非常不同，包括 eMBB 外更具吸引力的服務與應用、執照與非執照的無線技術的混合、動態共享的頻譜、IoT 的爆發性、以及企業專網的契機，這也帶來很大的挑戰，包括能夠更快地部署的電信基礎系統、仍不明確的商機與案例、企業的基礎架構將以多快的速度被替換？而又由誰付款？另外網路經濟學的透明度仍然很少、而且我們需要 1~2 個重大催化劑（就像我們使用 4G 一樣），以上這些仍有待探討及研究。

HarrisX 則著眼在探討智慧手機是否仍將在 5G 和物聯網世界中佔據統治地位。執行長 Dritan Nesho 說：「我們才剛剛開始掌握 5G 的力量和影響，這項技術有望比 4G 帶來更廣泛，更深入的發展。」,「我們正在推出 5G 情報平臺，以清晰並深入地了解無線和有線服務的業務主管，家庭主管以及訂戶對 5G 的期望，採用和經濟影響，並以此為基礎我們跟踪每種新一代電信技術反應的遺產。」; HarrisX 透過消費者跟踪器、Telephia APP 以及最新的 5G Intelligence Platform 發現在業務決策者（Business Decision Maker）和無線消費者中，實現更高質量的流傳輸和更廣泛的網路覆蓋範圍的速度和可靠性是 5G 的最令人期待的好處。HarrisX 同時也發現越來越多的智慧手機用戶也正在使用更多的互聯設備和技術，隨著 40 億數位化商機和 5G 手機的推出，智慧手機領域還有很大的增長空間；而全球物聯網的市場規模到 2025 年更將達到 1.1 萬億美元。

HYLA Mobile 總裁兼執行長 Biju Nair 也總結如下：5G 首先將在發達經濟體中對我們的生活和工作產生積極影響，還將為其他設備創建用例；行動通訊設備將繼續在當前使用模式中扮演重要角色；其他設備（如 IoT）將繼續增長，並且可能許多設備將增強/替換傳統設備的特定功能；在新興經濟體（如印度）中，智慧手機的採用正在增長，在這些新興市場中，行動通訊將在數位化和經濟增長中扮演關鍵角色。最後他強調：智慧手機的未來還活著，並且在不久的將來仍會很好。

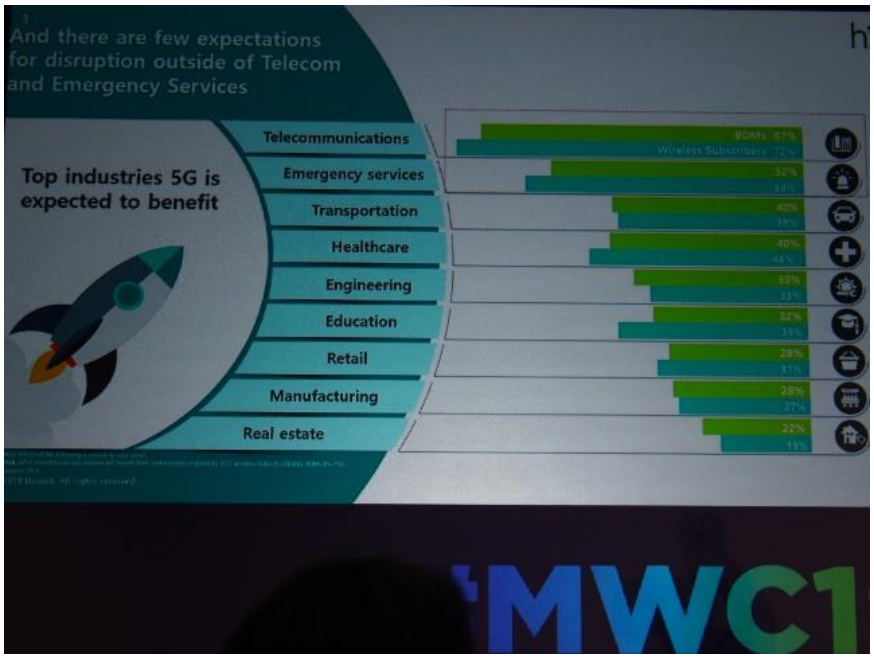


圖 3-3-9 HarrisX 預測未來 5G 的主要營收項目及比重

四、 IoT 演講

(一)擴展智慧物聯網

雖然比預期的時間更長，目前全球物聯網規模終於開始進入了爆發階段，藉由高速行動寬頻網路、物聯網、以及人工智慧的結合，將會開啟許多創新商機。然而隨著各種不同類型的連網設備數量突然大幅持續攀升，電信業者與企業該如何確保其採用之智慧物聯網足夠安全可靠，並如何對物聯網解決方案進行前瞻性驗證以實現真正的可擴展性（scalability）。現場的專家小組一致認為，IoT 市場的參與者應該專注於他們試圖解決的商業應用問題本身，而不是一味追求使用特定先進的技術領域。

Deloitte 電信戰略與運營總經理 Phil Wilson 表示，IoT 發展已即將接近開始大規模部署的臨界點，但迄今為止，仍缺乏將傳統終端機器設備連結無線網路的殺手級應用仍尚未出現。

Ericsson 物聯網業務部技術主管 Kiva Allgood 強調進入 IoT 領域的業者應更多地關注應用服務成果本身。他說:「只關注技術驗證概念意味著您很少能夠擴展，當您這樣做時，您將到達臨界點。」

KORE 總裁兼首席執行官 Romil Bahl 表示贊同並指出他最初對與客戶的一些對話感到困惑。他說:「我對電信公司是陌生的，我來自於具有消費背景的應用服務產業。而這使我感到困惑，例如，當人們想談論天線的尺寸時，所需要的只是拿出可使用的終端連接體驗。我們可以說，任何技術的發展都越來越快，但我們同時也把它變得更複雜難懂了。」。

Cisco 網路副總裁兼首席技術官 Michael Beesley 則表示他並不認為 IoT 發展處於一個臨界點；但他指出目前連接機器和設備的應用價值需要有更多驅使加速動力，因為人們意識到了實際商業應用成果對所需技術配合的相對落差。

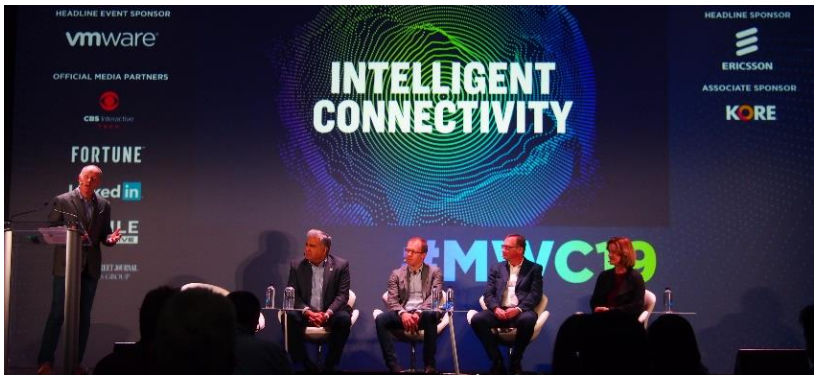


圖 3-4-1　IoT 演講議程：擴展智慧物聯網

(二)邊緣計算：創造新的物聯網應用

隨著 5G 時代各種大規模物聯網應用來臨，可以預期的是當連網設備數目超越一定的量級後，雲端或數據中心的物聯網數據處理效率將會越來越低落，因此需要開始在網路邊緣就進行越來越多的

資料數據分流、儲存及處理程序，進而提高營運效率。展望未來，大多數的物聯網應用都將依靠邊緣計算來提升其價值。

主持人 GSMA Intelligence 主管 Peter Jarich 提及，5G 網路的演進路線讓實現萬物互聯成為可能；5G 網路切片（Network Slicing）技術將可依據終端應用需求，將網路「切開」給不同場景與族群使用，例如其低延遲特性可應用於要求零時差的工業控制需求，而高頻寬特性則可對應工廠內多媒體需求應用。

Corning 技術與市場開發經理 Karen I. Matthews 將物聯網應用的焦點放在工業 4.0，她指出工業 4.0 可以創造新的生產模式並大幅增加營收；達成工業 4.0 願景的背後是 IoT、Cyber-Physical、Systems、Fiber、以及 Deep backhaul 所組成的基礎架構，而 Fiber Deep 傳輸骨幹將能夠滿足巨量數據傳料流的傳輸承載。

負責全球網路基礎架構戰略以及與第五代無線技術相關的解決方案開發，Intel 數據中心副總裁兼 5G 基礎設施部總經理 Caroline Chan 解釋了結合 5G 網路和邊緣計算，將如何使企業利用開發新的數據資料使用方式，創造新的商機並獲得可觀的營收。她強調：隨著 5G 標準和技術的不斷演進，5G 能支援大規模物聯網以及超可靠的低延遲通訊，就帶來邊緣計算能夠發揮作用的地方。首先，無論是智慧展場、數位化零售、智慧工業專用網路等應用場域，皆須利用 5G 帶來的延遲優勢，以及具有即時數據分析能力，因此其計算儲存資源必須離用戶更近，才能善用數據來提供所需服務。

IBM 全球業務服務總經理 Albert Opher 指出，新技術的發展將創造出新的商務架構，公司從傳統處理交易過程，演進到數位化企業，再進化為透過新技術轉變策略、產品、服務的認知型企業；這是一種學習型企業，由各種智慧平臺的 ecosystem 所組成，其競爭

力優劣取決於對及業務環境的轉變有多快的適應及反應力；其核心的工作流程和程序包括：導入專有數據資料，基於 AI、IoT 技術及區塊鏈技術，始終透過機器學習改進，轉變人機界面，整合 IT 和 CT 彈性處理服務數據。Opher 並於現場舉實例說明：鹿特丹港口管理及 Groupama 車載通信服務子公司 G-evolution 皆使用 AI 和 IoT 來提供新服務。



圖 3-4-2 Intel 提出之邊緣運算應用說明

(三)物聯網連接的承諾

在物聯網起飛的時代，使用行動寬頻網路技術已成為大規模物聯網部署的最佳選擇之一，物聯網解決方案公司在實現其應用服務前必須評估物聯網連接性之相關議題，目前及未來對物聯網連接的需求會有那些轉變，是否 5G 網路已準備好應用於物聯網解決方案，以及在擴展物聯網覆蓋範圍時需考慮那些創新技術。

主持人 TM Forum 副總裁 Joann O'Briend 開場表示 5G 生態系統的成功意味著改變既有核心運營和 IT 產業經營模式；也就是促使其他產業進行數位化，預估整個 5G 生態系統將具有 5,820 億美元的市場，但要抓住 5G 商機就需要徹底進行商務轉型，發展 IoT

物聯網絕對是這波趨勢中最重要的產業之一，物聯網的應用廣泛牽涉到包含了環境監控、工業製造、運輸與物流、以及醫療保健等領域；而這些數位化系統轉型計畫需要創建新的重要標準和工具，包括商業模式、商業架構、Ecosystem 平臺獲利方式、以及 IoT 物聯網管理。她在總結說到，「5G 進一步降低了進入這些領域的壁壘，超過一半的實施者正在考慮 5G。」。

Accenture 網路服務全球負責人 Amol Phadke 強調快速可靠的行動通訊網路對於許多行業的擴展至關重要。當 5G 網路無處不在時，蓬勃發展的 IoT 物聯網產業將看到巨大成長的商機；這些很快將帶來變革的服務，如 3D 影視，身臨其境的電視，自動駕駛汽車和智慧城市基礎設施等突破性發展，將釋放出當今難以想像的商機，電信公司將在促進這些前景方面發揮關鍵作用。

Semtech 無線 LoRa 與物聯網副總裁 Marc Pegulu 則強調，即便 5G 時代來臨，已發展多年的 LoRa 技術仍有存在價值，LoRa 具備低頻寬，適用於短距離和長距離的特性剛好可填補其他技術的空白部分；由全球超過 500 個成員的 LoRaAlliance 所發展的 LoRaWAN 可支援最多 10 億個終端設備的部署，LoRa 作為最受歡迎的 LPWAN 技術、蜂巢式物聯網的相容性、以及與行動通訊生態系統的無縫連結將使得 LoRaWAN 能與 5G IoT 長期共存。

Sprint 物聯網與產品開發資深副總裁 Ivo Rook 在座談會上分享了有關該公司 Curiosity 物聯網產品的最新消息，一種新的 NB-IoT 專用網路選項以及與亞利桑那州立大學合作的案例。同時也提到：如果電信公司將支援物聯網趨勢以實現數位化經濟的承諾，則應該規劃建設一個專用網路以實現此雄心壯志；他說：「如果電信公司仍

在考慮智慧手機的情況下設計網路，那麼物聯網彩虹盡頭的金礦很可能會遭到競爭對手的突襲」。

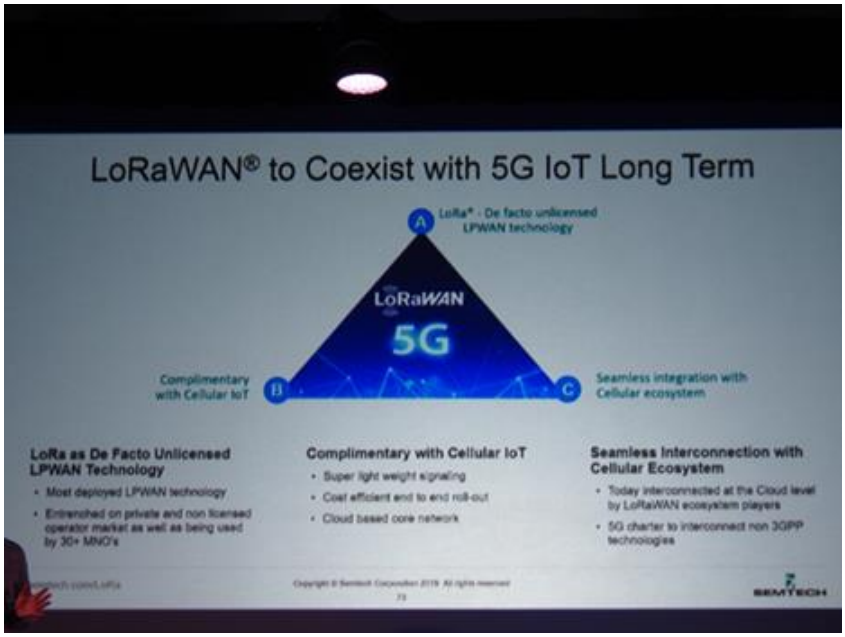


圖 3-4-3 Semtech 提出 LoRaWAN 與 5G IoT 共存

(四)智慧城市及智慧世界

本場次的主持人是來自洛杉磯交通部門的主管，Seleta Reynolds，她已經執行智慧交通的專案很多年了，而她認為交通與通訊皆為基礎設施的一環，故她來通訊大會分享她的經驗，她演講的主題是「軟體是新的水泥」。她首先提到在 1920 年美國大蕭條的時代，因為街口人馬混雜，交通打結，所以洛杉磯提出了禁止行人暫停於街口的法規，這個法令的後果是大家沒人走路，而開始以汽車作為移動工具。二次世界大戰後，幾條高速公路的興建，連接鄰近地區的交通，開始為洛杉磯帶來商機與工作機會。但當一個悲慘的故事發生，一個貧婦帶著她的小孩需要轉車三次才能到達醫院急診室，洛杉磯政府開始認識到這是一個需要解決的問題。洛杉磯政府認識到交通並不是使人可以從甲地到乙地如此而已，交通還關乎到社會正義、人民機會平等與社區的幸福感。她提到在洛杉磯，開

車一小時比較搭乘大眾交通一小時，開車的人所擁有的工作機會增加 12 倍。所以洛杉磯開始了她們的交通行動計畫，政府知道她們沒有足夠的能量，所以政府選擇與科技創新公司開始合作，提供公眾交通即服務(Mobility as Service)，使用工具監控街口的路況。這造成了三個重大變化，第一個變化是使政府部門與科技公司開始對話，而且是用科技公司熟悉的語言來於之對話，商談解決方案。這使得公私協力不像政府單位對私人公司，更像 Google 向其合作廠商的關係一般，交通部門提出交通規劃願景，花半年時間與民間公司一同規劃，在花六年到九年的時間執行計畫。第二的變化是商業模式改變，通訊與資料技術的興起，使得運輸最佳化成為可能，政府要思考的是如何與這些優秀的運輸公司進行合作，使商業模式可持久。第三個改變是 API，路口的號誌可以被視為類比的可視化 API，告訴駕駛人與行人是走還是該停，限速多少等等資訊，但現在是數位時代，要如何使上述優秀的交通公司所提供的服務或產品可以讀的懂這些交通規則與目前的路況，這就是交通的數位 API 該做的事情。在幾年前，當這些數位環境齊備了，一夜之間洛杉磯就滿佈了民間公司的滑板車。到現在洛杉磯的數位交通 API 每天有四百萬次的呼叫，監控 9 百萬筆交通流量紀錄，提供給三萬輛滑板車使用。Reynolds 認為智慧交通的重點不在資料，而在政府如何結合民間業者更好的拓展其交通業務，講者提出交通性福度量測的看法，認為透過幸福度的量測，可以開啟更多有趣的對話，以改善交通。最後 Reynolds 簡單介紹了關於開放行動聯盟（Open Mobility Foundation）的組員情況以及行動數據規範（Mobility Data Specification）。

來自 Bird 滑板車公司的 David Allison，Bird 是洛杉磯市內租用滑板車的公司。該公司除了出租滑板車給市民使用外，也會提供騎乘的 MDS 資料給該城市的交通部門。但是隱私卻成為這些騎行資

料的使用障礙，Allison 指出由於各地方的隱私法案之故，有些不具備隱私保護技術的城市政府單位是不願意接收這些可以用於城市規劃的資料。對於隱私保護，Allison 有兩點保護策略，第一個是改變資料的索取方式，將整批資料餵入資料庫的方式，改成提供 API 查詢，限定存取次數，並且透過數據概略化達成隱私保護。第二個是描述騎行資料時，資料的主體是設備序號，不要待入租用人的資料，根本上避免個資。他最後提到，智慧交通需要公私協力，與交通部門商議派送合理的車子數量，他相信透過資料收集與量測可以帶來更好的決策，使得消費者需要用車的時候，車子就在附近。

來自 Numina 公司的 Tara Pham，Numina 是一間資料服務公司，利用其自建的街頭的監控設施提供去除隱私之後的道路街口行車數據，如車流，行人數等，把街口數位化。Pham 在創業之初就決定要解決車流計數困難，同時也避免監控侵犯隱私，故 Numina 採用的技術是電腦視覺以及邊緣運算，其特色在於影像資料在邊緣運算後，即刪除，回傳的資料都是描述資料與統計資料，已達到匿名化隱私的保護，但隱私的顆粒度也是要視情況調整，例如若社區只有一人坐輪椅，對系統只是一個資料點，但左鄰右舍看到這個資料點馬上可以推論當事人的行蹤，避免這種因上下文情境所做之推論是該公司還要努力的方向。因為採取這樣的設計，曾經有車禍現場想向該公司調出影像紀錄作為證據，該公司是無法提供的。Pham 也坦言到，政府在採用新科技的時候有資源上的困難，不用說政府單位，她們公司自己在 AI 上就有困難，要發展智慧城市，取得這些資源須要公私協作。

來自 Ouster 公司 Raffi Mardirosian，Ouster 是一間 LiDAR 的製造廠商，LiDAR 乃用來量測自身與目標距離的裝置，常用於自駕車技術，了解車子周圍之環境情況。Ouster 的特色是強調提供服務提

供商可負擔的 LiDAR 裝置。Mardirosian 也說明若 LiDAR 裝置設置在街口，亦可了解路口的情況，例如公車是否依照路線轉彎，有多少行人等。Mardirosian 也提到一個有趣的案例，有顧客發生車禍，將車上的 LiDAR 紀錄作為行車紀錄，來證明自己是被撞的一方。而在公私協作上，Mardirosian 需要交通部門給其未來產品的功能設計給出建議。

(五)物聯網裝置：始終傾聽、觀察及學習

Deloitte Consulting 的 Rob Kasegrande 是本場的主持人，他表示，在我們工作、生活和娛樂的任何地方都使用物聯網設備，但是也存在安全風險，我們如何利用物聯網設備的不斷發展的同時，來改善和保護我們周圍的世界，是他想詢問的議題。

來自 Greystar 建築公司的 Dave Denslow 談論到 IoT 與智慧建築的未來願景，未來的建築不僅是單純的住宿功能，還能理解人的需求。他們公司相信智慧建築的成功需要具有三要素，分別是有效率（Efficiency）、體驗（Experience）以及可行動的情資（Actionable Intelligence）。他們公司一直思考智慧建築的意義是甚麼，如何去擁抱科技的進步？他們認為手機是其中的關鍵，他們在建築物中廣佈熱點，使得手機能持續連線，透過手機去控制門鎖，監控溫度等功能。不只這樣，透過對建築物與生活空間的控制、監視與管理，用戶能更好的對生活需求做出決策，以便利他的生活。Denslow 相信建築即服務（Smart Buliding As a Service），這次談話目的是要泡出一個問題：「建築物可以為你做甚麼」，例如你的建築物知道你不在家，它會推論你在公司加班，它就會繼續推論你可能會晚點到家，接著它就會作連線城市資訊系統的動作，告訴你最後一班的公車資

訊，這就是一個很方便的體驗。Denslow 認為隨著連網技術的進步，發展智慧建築是在對的時間，做對的事情。

來自 Boingo Wireless 的 Derek Peterson 談論個人的物聯網，他認為隨著越來越多的裝置會連網，此時要討論的重點應該擺在這些 IoT 裝置要符合個人的使用，要使得 IoT 變成生活的一部分，使得用戶從中獲益，不是單純為技術而技術。他舉例子說明，現在智慧門鎖是用手機當作鑰匙，但技術越進步，裝置連網比對生物與行為資料庫，用戶用其手掌或臉，就可以當作鑰匙。這個轉變就是把科技與人相互關聯，實體世界與虛擬世界相互關聯，且以人為本。而這些科技都要網路來串連才有發生的可能，也就是單一技術是沒辦法獨立帶給用戶更便利的生活，是要整合跨科技與跨地域的各類技術來達成，而其中的整合關鍵就是連網技術。Peterson 繼續說明他認為未來的物聯網有兩個特徵需要達成，第一，社群聯結，與第二，連線方法的聚合。第一個社群聯結指的是用戶不僅止在家中使用服務，他到了外面，例如去拜訪朋友的公寓，想要與朋友有互動，一起聽個音樂或者電腦遊戲，物聯網裝置需要能夠支援這樣的社交服務，但這樣是跨網域連線，其中資訊安全也就很重要，包含資料安全，隔離安全。第二個連線方法的聚合，是指不同的連線技術，例如 WiFi 與 5G，未來的物聯網裝置會有多種連線方式來報障持續在線，你不會想只用 WiFi，而這也要有安全。最後他談論到資料隱私與便利性的兩難，他認為適度的開放隱私資料可以使得消費者有更好的體驗，例如在外地機場出差時，人生地不熟，分享個人的地理位置，可以使得接送的計程車司機更方便的找到客戶的上車地點。這些也是資安議題，需要解決，也比如何設定防火牆更深刻的多。

來自 Ericsson 的 Bodil Josefsson 則說 IoT 使得每個東西都連線，這種新潮流帶來好處，但是越多裝置也代表著許多資安的洩漏點。

所以產業界需要物聯網是可靠且安全的。要達到這樣的狀態，資安要求在設備開發之初時就要納入設計，不能夠等到產品發布後再以事後補充的方式進行功能增補。所以 IoT 安全要先有安全的裝置，例如裝置密碼的設計，再來是安全的通訊連線，最後是平臺安全。IoT 系統的端到端安全是要整體考量的，不能夠只有裝置安全，當然 Ericsson 身為設備商，他們也樂於使得裝置取得認證，希望看到很多認證計畫推出。而未來 5G 技術會使得物聯網裝置越多，連線多表示攻擊面變大，所以 5G 設計之初就有考慮資安，且 5G 的切片與監控可以達到更安全狀態。

來自 Figleaf 的 Pankaj Srivastava 則說未來應該建立以隱私為優先的生態系，他舉例說道現在只要一上網就會有十多種追蹤器，試圖辨識用戶指紋，建立用戶的偏好以推送廣告，這種情況很像小說 1984 的老大哥看著你的預言。但是隱私議題在不同的國家地區有不同態度，這仰賴客戶的對隱私議題的洞見與看法，但他也認為未來客戶會逐步的認識到隱私的重要性，使得公司對隱私保護變成市場競爭力。談到 IoT，他認為 IoT 會產生大量的資料，所謂隱私保護不是指不去產生資料或者不去使用 IoT 裝置，而是要如何減緩隱私外洩後可能的損害，同時也要提生隱私保護的措施，去釐清誰在用我的資料，我要如何控制我的資料，才能兼顧 IoT 的好處與隱私保護。

來自 OMNIFLOW 的 Pedro Ruao 則是介紹 OMNIFLOW 是一間生產街頭上的監控設備的 IoT 系統設計製造公司，他們公司的產品特別強調使用再生能源如太陽能與風力來提供 IoT 裝置的穩定性與強韌性。他也預測未來 5G 的發展會對 IoT 有好處，例如車聯網就需要 5G uRLLC 的特性，但也需要注意額外的安全需求。他也認為 5G 的邊緣計算對該公司的業務有所幫助，透過 MEC 與影像分

析，他們就可以提供街口行為的分析，例如若有人低頭用手機過馬路，透過街口 IoT 系統分析後，可以發出告警給周邊的車輛與行人。

(六)安全的物聯網

本場討論的是物聯網安全性對家用與企業都有巨大的影響。一般 IoT 安全的重點通常放在設備解決方案上，但是本場討論認為物聯網生態系統中的每個參與者都必須儘自己的職責來幫助創建端到端的安全解決方案。本場討論將聚集 IoT 生態系統參與者，一起討論隱私、安全性、公共安全和合規。

主持人是來自 GSMA 的 Ian Smith，他先介紹來自漏洞獎勵平臺 HackerOne 公司的 Alex Rice。主持人請 Alex Rice 先介紹一下他所屬的駭客社群，Alex Rice 回答該公司社群約 500 人，成員的組成很多元，也有來自學術界，又或者最小的成員才 15 歲，但可以說是一群以創新方法繞過保護機制的技術人。主持人接著詢問 Alex Rice 獎勵平臺的獎金制度，Rice 回答促進網路安全的進步，造福人群本身就是這群人的心靈回饋，但他們公司也有提供實質回饋的獎金，依照影響程度的不同，獎金約為 3,000 到 10,000 美金。主持人接著請 Rice 預測 IoT 威脅的未來演變。Rice 回答，他已經看到未來 IoT 的攻擊將朝向有著更大影響層面的裝置，或者可以造成更大經濟上損害的系統，來進行經濟勒索。另一個可能性是朝著更私人的領域進攻，以往勒索軟體是加密檔案，但他認為未來勒索軟體可能會朝向刺探私人的隱私，譬如透過網路攝影機來窺看私人生活，並據以勒索。主持人又問說 IoT 的威脅會越來越大，身為一間商業公司要如何幫助減緩這些威脅？Rice 回答道：的確隨著科技進步，威脅也會不斷發生，他認為做好端到端的安全是一個解決方法。主持人最後問到透過法律與合規是否能夠減緩威脅?Rice 回答道：他

認為可以參考英國的安全法規制度設計，英國除了要求設備商在設計之初就要納入安全原則，即 security by design 以及 security by default，例如設備不能使用一致的預設密碼，英國政府還要求設備商要設立漏洞回報機制，並且要求要在產品生命週期內提供更新服務。

主持人接著請 Rice 下臺，並歡迎新的幾位與談人上臺，並請幾位與談人一一自我介紹。接著主持人問到：隨著聯網裝置的越來越多，這種變化會給產業界帶來哪些資安威脅，產業界又如何應付這個情況。

來自 CUJO AI 公司的 Marcio Avillez 回答說不同的 IoT 裝置有不同的情況，若是家用的 IoT 裝置、智慧家庭等目前的解法不多，但是若談到商用的 IoT 裝置，隨著業務的不同，解決方案就有各式各樣的解法，這樣的資源很多。但總歸的來說，採用 AI 可能是未來可行的解法。Avillez 另外也提到 API 安全也是相當重要的一環。

來自 Cisco 公司的 Nancy Cam-Winget 則從設備商角度，講出工廠業界的看法，她認為工業界講求可用性，而解法採用獨立網段（air-gap）與限制存取（least access），就她的經驗看來，工廠環境基本上沒加密也沒認證，整個網路安全防禦都不存在，如同赤手空拳一般，這種情況非常普遍，甚至美國與歐洲都相同，相同的環境，也就代表威脅是相近的，目前工業界為了處理這種情況，推出 IEC62443 標準，不失為未來的解法。Ncncy 認為由於公司不能處理所有的威脅，故進行風險分析後，使得公司的資安態勢能足夠應付威脅是其中的關鍵。例如對工廠來說，資料外洩的重要性遠不如作業持續營運與人命安全重要，故公司的資安態勢與作為就要先針對作業持續營運與作業安全進行設計。最後 Nancy 再提到能源產業，

以烏克蘭電廠釣魚郵件事件為例，說明可視化（visualization）的重要性，公司有可視化的能力才有可能看到攻擊，Nancy 說到你若看不見，就你不能管理它（You can't manage what you can't see.）。

來自 NIST 的 Michael Fagan 則談論到美國聯邦政府採用 IoT 的經驗，他舉例說即使是政府單位，各單位的差異也相當大，如 NSA 就有集中辦公區域,也有相當技術人員可以好好的管理 IoT 的使用，但是反觀 IRS 可能就沒辦法有相同的條件。他另外也提到說公司若使用家用產品，因為商用與家用對於資安要求等級的不同，有可能造成新的資安缺口。

來自 Blancco 公司的 Russ Ernst 則認為越來越多的 IoT 裝置，同時意味著越來越多的資料，未來的公司要會需要知道如何大量進行資料儲存，處理與管理。而據他的經驗表示，這些資料中 85%的資料是好幾年都用不到的，處於相對靜態的狀態中，若公司不知道如何管理這類資料，擁有這些資料就是本身就帶來風險。

來自 A10 Networks 的 Ravi Raj Bhat 則是先提出來未來的物聯網數量與其產生之巨量資料的預測數字，他認為未來的挑戰是這些資料的安全與隱私。同時他也認為製造商有責任，負擔資安義務，例如裝置不能有預設密碼。又例如在處理惡意程式上，設備供應商也可以負擔相當責任，因為相較於用戶，供應商較有技術能量。此觀點也有與談人附和，他們一致認為從他們的經驗看來，有時駭客擁抱新科技的速度比一般公司都來的快，甚早就進行典範轉移，例如 AI 就是很好的例子，駭客族群很早就擁抱 AI 科技。

主持人接著請聽眾詢問，有人詢問到本場次的主題是 safe thing，但 safe 是主觀的感受，但我們要如何知道現在是安全的，而且將來也是安全的。來自 Cisco 的 Nancy Cam-Winget 則回應說道沒有 100%

的安全，AI 可能是解法，她認為 AI 除了可以作預測分析，AI 也可以做監控，強化可視性與強化機器指紋辨識能力，如此是可以改善資安態勢的，這有助於維持 IoT 系統的安全狀態。來自 CUJO AI 公司的 Marcio Avillez 則接著說明資安態勢，他認為整個安全的過程是需要反饋的，例如給客戶展示，稍微更改配置就可以改善資安態勢，像這樣回饋，會讓客戶有感，也有助於維持安全的狀況。

Cisco 的 Nancy Cam-Winget 繼續補充道：「一般 IoT 的用戶甚至服務提供商都不會知道 IoT 裝置被入侵，製造商應該負擔更大責任，提供資安隨插即用功能、預警系統、資安自動化系統。」，來自 Blancco 公司的 Russ Ernst 則認為也要關注資料的使用情況，符合相關法規，如歐洲的 GDPR 與加州的 CCPA，這些法規規範資料販賣等議題，公司都需要去了解與遵守。

再來主持人提到如何透過法律處理 IoT 安全議題，他舉例說道：如同早年的汽車安全帶與安全氣囊，也都是以法規引導車廠去製造與裝設。來自 NIST 的 Michael Fagan 則說明監管單位當然有其效果，但他認為製造商也有其責任，資安人員不能只想著管制控制，造成用戶不便，這樣反而會有反效果，造成用戶不使用這些資安功能，資安擾人就無效。作為一個資安的研發工程師要盡力使得資安功能是自動化開啟，同時簡單易於使用。他舉了一個例子說沒有人想要返家開冰箱時，還需要輸入密碼。來自 Blancco 公司的 Russ Ernst 則說道：有時合規不等於安全，但合規會驅動安全。

最後主持人請大家各給一個結語。

- A10 Networks 的 Ravi Raj Bhat 說：加密是安全的重要基石。
- Blancco 公司的 Russ Ernst 則說道：資料需分類。

- NIST 的 Michael Fagan 則說道：NIST 指引有參考價值，特別是 NIST 近期會推出專給中小企業的安全指引。
- Cisco 的 Nancy Cam-Winget 則說道：除了法律規範外，製造商也負擔責任在設計的第一天就要加入安全原則，確保隔離性與可視性。
- CUJO AI 公司的 Marcio Avillez 則說 AI 值得花時間去發展。

五、 5G 資安高峰會

(一)網路防護

演講者是來自 Ericsson 的安全解決方案總經理 Keijo Mononen，他在會中指出，5G 行動通訊網路雖是商用網路，但是考量 5G 將滲透到每個國家的各個層面，新的業務和服務交付模型，不斷發展的威脅格局，以及對隱私的日益關注，因此需要新的安全要求是 5G 網路時代一項非常重要的環節，政府應重視此問題，適當地介入並要求 5G 電信業者善盡 5G 資安防護責任。整體來說，所有電信業者對其所面臨的 5G 資安挑戰仍缺乏整體性（End to End）資安可視性，無法得知威脅或風險存在網路何處、資安或隱私合規性，雖然掌握很多資料，但如何保護才符合法令，在應用與違法之間也難拿捏、偵測跟回應威脅能力不足，以及仍以人工抵擋並處理資安攻擊。對此，除了確保製造的設備符合 3GPP 資安標準要求外，Ericsson 針對 5G 網路防護所提供之智慧安全管理方案將在創建公共通訊安全方面開創了先河；他進一步指出，5G 將通過包括安全控管、傳輸機密、識別管理、個人隱私、強韌性等五大資安領域進一步改善電信網路整體安全性，並以 3GPP 等國際資安標準為基礎，從針對新業務環境的初始安全理念規劃、網路產品發展階段導入安全與隱私設計，到網路部署階段的落實端到端安全架構落實、以及之後網路

自動化的安全維運及管理，提供了一個廣闊的，確保安全和隱私的可信賴 5G 網路服務生態系統，促使 5G 能夠成為網路社會平臺的基石。

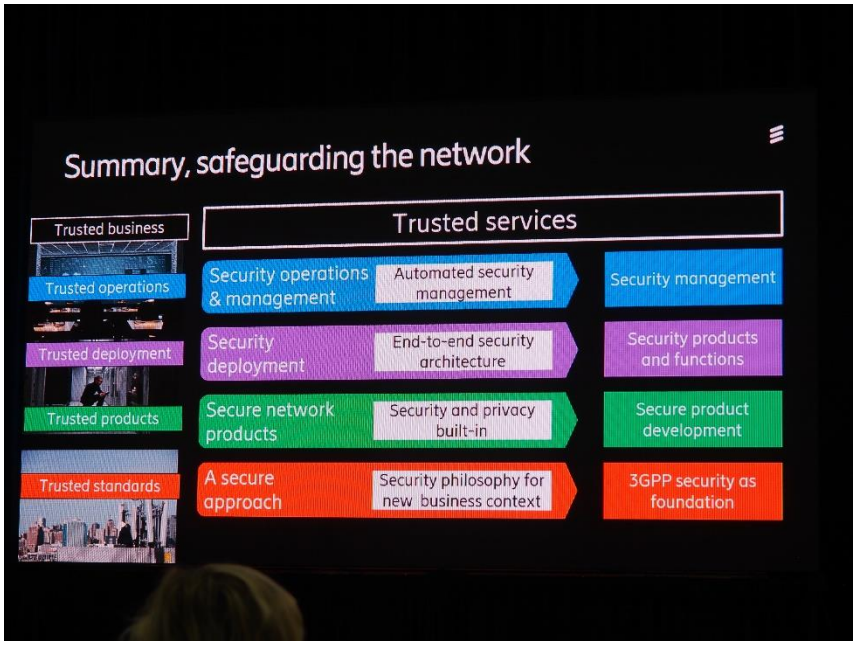


圖 3-5-1 Ericsson 提出確保 5G 網路安全之整體概念

(二)5G 案例及新興資安需求

Nokia 軟體副總裁 Mary O'Neill 完全同意維護資安是 5G 網路時代一項非常重要的環節，5G 雖是商業網路，但是考量行動通訊網路將滲透到每個國家的各個層面，政府應重視此問題，適當地介入並要求 5G 電信業者善盡 5G 資安防護責任。Nokia 針對 5G 網路防護的解決方案強調管理網管人員存取網路系統的記錄並透過 AI 分析每個帳號使用行為，確保即使帳號被盜用仍可在第一時間得到示警。同時也透過收集 5G 網路各種訊令及第三方資安監控設備之資料或日誌檔，持續監控並用 AI 與大數據分析可疑威脅情資並評估威脅等級，提供減緩機制建議。

O'Neill 進一步向行動通訊服務提供商發出了呼籲，要求他們加快 5G 安全的部署速度，並警告說，優先考慮速度而不是安全性可能會導致更大的問題。在會議上，O'Neill 承認，要「更快，更快，更快地」推出 5G 仍在進行中，但為了確保他們贏得部署競賽而損害安全性是一種落後的方法。她說:「從架構的第一天開始就可以構建安全性，而不必之後再對其進行修補而付出更多代價。」這位來自 Nokia 的資安專家強調 5G 安全相關要求已經改變，不可再用現有解決方案來解決所有問題。我們需要更多的技術。當我為 Nokia 制定策略時，我們將投資於機器學習，演練腳本，工作流程，並且我們非常相信自動化可以幫助解決此問題。5G 的好處在於，它是一次轉型。我們可以將所有這些 4G 學習內容帶入 5G。此外 O'Neill 雖然宣稱 Nokia 作為與其他同業競爭對手「差異化產品」之一的安全實力，但她也指出並認為 Nokia 與其主要競爭對手 Ericsson 之間存在相似之處，這將有助於更廣泛的安全工作。「針對其中一些安全的見解，我們應該有很多共同點，我們確實必須在產業中為客戶提供合作。」。

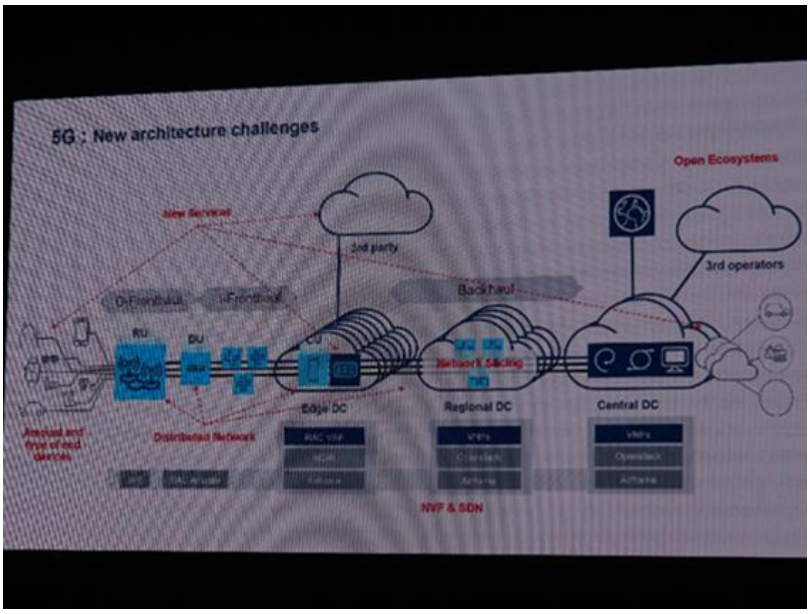


圖 3-5-2 Nokia 提出 5G 新網路架構所面臨之安全挑戰

(三)物聯網安全

主持人 Leo Lax 來自新創加速器 L-Spark，在這個時段中，主持人介紹了三家新創公司，這三家公司利用 eSIM IoT 信任根來增強其產品在各自垂直市場中的安全性。

來自 L-Spark 創新公司加速器的 Leo Lax 是本場的主持人，L-Spark 協助了幾間新創公司連結如黑莓(BlackBerry)的四家大公司，使新創公司可以在四家大公司的平臺上，對 IoT 的安全議題上進行技術開發與創新。這些新創公司的解決方案目前是選擇以 eSIM 為開發基礎,對電信產業提供了基於硬體的高度安全的 IoT 信任基礎,可確保設備及應用程式的安全，使得設備與其應用程式服務平臺之間建立相互信任關係，例如未來的 5G 進行遠距醫療時，整個診斷與治療的過程，這些醫療裝置是要透過身分驗證功能確認與確保其安全可靠，贏得醫師與病人的信任。

來自 Telus 的 Alfred Baghouzian 認為隨著物聯網裝置的變多，連結更密集，AI 與雲端技術的興起，新的機會來到也伴隨著新的威

脅，為了安全，兩個原則必須遵守：第一是安全設計原則（Security by Design），以及第二是把 IoT 是作一個整體來看待安全，GSMA 的推出的 IoT 安全指引是好的框架參考。電信產業使用資安技術已經有二三十年之久，透過硬體來達到安全是電信業一直以來的做法，利用硬體金鑰與認證算法來對終端裝置進行生命周期的管理，這樣的產業供應鏈已經成熟，這樣的經驗 Telus 認為可以應用到目前 IoT 與網路的安全議題，所以 Telus 與新創公司合作在電信平臺上驗證概念測試。

來自 BlackBerry 的 Sarah Tatsis 認為要 IoT 裝置間要進行溝通，IoT 裝置要給人使用，IoT 業務要推展，之中的關鍵是要有信任，以達成消費者所需之隱私、安全與連接可用。BlackBerry 現在是為一家軟體安全公司，以車聯網為例，已經有多個國家使用公司的 IoT 車聯網平臺。BlackBerry 認為要達成端到端的安全是一個挑戰，但大多數的公司都沒有資安背景，也顧不起資安專家，所以他們認為需要有一個中介軟體平臺，把安全功能納入作為軟體開發時基礎元件，對開發人員來說，可以更輕鬆的達到安全要求。另外，採用該平臺也可以達成合規與自動化（zero-touch）的信任。

來自 Solace 的 Eugene Hallinan 則說 IoT 成功的關鍵在於數量，只有數量達到一定規模，至少幾百萬的裝置，才有應用效益，Solace 目標就是要能管理這樣的大量裝置，這挑戰是數百萬的訊息如何有效率的同時安全傳遞。他們的平臺現在在航空業與物流業使用，同使也串好了銀行的金流系統。

來自 G&D 的與會者 Simon 則說在這些大量的 IoT 裝置的安全是仰賴於像 SIM 卡的硬體安全元件。G&D 的目標市場是高端與高價值的物聯網裝置，如車聯網、手機與平板、身分證晶片與金融卡，

G&D 可以提供上述服務的身分驗證安全功能。他認為隨著消費者安全意識的提高，服務提供商需要滿足消費者的安全需求，像消費者展示擁有足夠安全的身分驗證功能相當重要。

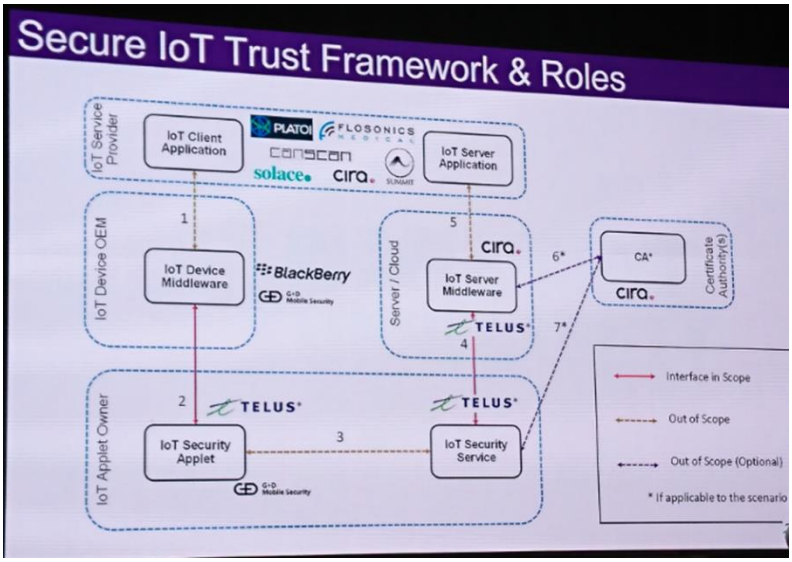


圖 3-5-3 Telus 提出之 IOT 網路信任框架與角色

(四)如何在 5G 時代持續受到保護

本場次的主持人是來自 Light Reading 資安媒體網站的 Mike Dano，他首先詢問在 5G 網路中，一般談論到 IoT 的安全問題是指什麼?

來自 Ericsson 的 Bodil Josefsson 表示，在這個萬物聯網的時代，大家的確會從中獲得一些便利，IoT 服務商也勢必要提供安全的服務，所以服務商要去理解物聯網的資安威脅，理解自身系統的資安態勢（Security Posture），同時也要認清安全功能要在系統設計之初就納入，不能已逐次增加系統的安全功能的方法來去營運 IoT 服務。

接著主持人詢問來自 Verizon 的 Jack Gallagher，身為電信業者，對於資安風險，最擔心的事情是什麼？Jack Gallagher 回答作為業者最擔心的資安風險還是連線中斷的問題。當然端到端的安全也是他

會考慮的，所謂端到端的安全指的是連線通道本身、到手機終端的安全、空中介面安全、後傳網路安全、核網安全，到客戶雲端運算平臺的安全，他都會關心。以上個點也會成為攻擊的進入口，當然要入侵手機終端可以比較困難，可能要實體接觸到手機，也比較沒有效益，但是若是攻擊 IoT 服務的平臺，這就非常吸引駭客去攻擊，因為從平臺可以連接到數以萬計的裝置，平臺也有可能連結到高價值的控制設備。所以如何提供客戶安全的連線服務，甚至未來安全的 MEC 服務業是他會思考的議題。

主持人追問 Gallagher，問他身為電信業者，Verizon 每年都會提供外界資料外洩與駭客活動的報告，在他的職位上，他會特別關注他的網路中發生哪些攻擊類型？Jack Gallagher 回答從他們公司管理的 IoT 裝置，的確在用戶平面上可以看到一些終端裝置中毒的流量，這是他最常看到，身為業者，Verizon 也與客戶一起處理這樣的議題。

主持人轉向問來自 Mocana 的 Dean Weber，詢問 Weber 像他這般的資深資安專家，在看待 5G 系統時，會特別關注哪些資安議題？Dean Weber 則回答，科技是不斷進步，也不斷的有新技術進入系統，而當電信業者談論到端到端的安全，一般指的是從電信網路邊緣的終端設備到另一個電信邊緣的終端設備，而不會更進一步的保護到客戶自身所營運的系統，例如客戶的終端裝置，又或者是客戶所自行建置的 AI 或雲端分析系統。他的公司就是要提供真正的端到端安全，他們公司的服務會進入到數據資料、終端裝置、公司網路、應用伺服器，甚至公司的組織架構以及管理程序，以保證上述各層級是安全的。

主持人接著詢問威脅增長的議題，主持人認為隨著 5G 與 IoT 的發展，公司從中獲利的比例也會逐年增加，但隨著獲利的增加，這些為公司帶來利潤的系統也會變成駭客覬覦的目標，這對公司來說表示越發展就越危險，對公司變成一種兩難局面。Bodil Josefsson 表示這種發展兩難的議題需要發展技術來解決，特別是 5G 安全技術。Gallagher 則表示這些高價值的物聯網設備都會因 5G 而更興盛，例如車聯網，故 3GPP 也發展安全技術來試圖解決。

主持人反問是否因為 3GPP 有發展 5G 安全技術，所以我們就不需要再擔心資安議題。Bodil Josefsson 表示這是錯誤的陳述，這是由於 5G 會持續發展，也會有新的事物進來 5G，新的資安問題也需要關心。Dean Weber 則回答，當然還是要擔心 5G 安全議題，5G 會與 4G 共存，信令安全會是個議題。生動的說若 4G 是雙線道公路，那麼 5G 就是 200 線道的公路，所以當攻擊發生時，受損的速度與後續擴大的影響也是指數增長。

主持人問 Gallagher 關於身為早期進入 5G 的電信業者，Verizon 會採取何種特殊的措施保障來 5G 安全？Gallagher 回答就他自己所知，3GPP 已經做了一些安全的工作，3GPP 也減緩了一些從 4G LTE 時代就存在的弱點，但在 5G 時代，Verizon 還關心供應鏈安全、也關心軟硬體模組元件的安全，端到端的安全，也包含垂直應用領域的特殊需求。

主持人問從終端裝置到網路的端到端安全，其中的哪的環節是較為危險的或者較為有挑戰來確保安全，各位與談人的看法。Dean Weber 則回答供應鏈安全，元件來自各地，要分辨每個元件是否會被攻陷或是被埋入木馬是不可能的任務。但以軟體為例，NIST 發表了相關的指引。他認為軟體供應鏈是新興的重要議題，且因元件

來自各地，這是一個信任與信用問題。Bodil Josefsson 表示端到端安全要先釐清端到端的範圍，只是指加密，還是雲端安全，還是指縱深防禦，Josefsson 認為端到端的安全是很多面向與層次的，而中間的關鍵能力在於可視性，接著是建立資料關聯性，才能達到端到端安全。最後節錄主持人與來賓們之提問與回答：

- 主持人問端到端安全是是誰的責任？Bodil Josefsson 表示當然是服務提供者的負擔最終責任，他們才有做多的資訊與權限。但從責任分擔（share responsibility）的角度，設備供應商與提供連線服務的電信業者也有一定角色。
- 主持人問 Bodil Josefsson 供應鏈安全？Bodil Josefsson 回答該公司自有一套框架監控供應鏈安全。
- 主持人問 Gallagher 關於身為電信業者，在端到端的角色？Gallagher 回答，身為業者當然會有較大的資安能量，來協助消費者發現資安事件或者提供減緩措施，但業者也只能協助，畢竟這些服務也不是電信業者所開發。
- 主持人問誰要驅動供應鏈安全，是政府還是行業組織？Dean Weber 則回答供應鏈安全需要有很多貢獻者，消費者用戶需要安全的平臺與服務，所以不能只有設備商的元件安全，電信業者需要提供網路安全與作業安全，政府單位需要提出法規監管要求，端到端的安全與供應鏈安全息息相關。
- 主持人問目前有那些 IoT 或 5G 的資安認證？Bodil Josefsson 表示現在有許多認證，例如 CITA 的裝置認證，芬蘭也有相關認證。Gallagher 目前 Verizon 沒有採取外部的資安認證，當採購新設備時，Verizon 有自己的測試程序。Dean Weber 則

回答 IE62443，這是個需先風險評估後，找出相應控制方法論。

- 主持人問 5G 會更安全嗎？Gallagher 回答當資源越投入，知識越多，他相信 5G 會越安全。
- 主持人問不同的垂直應用領域是否有不同的安全要求？Gallagher 回答是的，不同的領域有不同的安全。Bodil Josefsson 表示不同的領域，願意支付的保護費用當然不同，防護程度也不同。

  Dean Weber 則回答他認為保護比偵測重要，若一個裝置沒有甚麼保護措施，基本就不應該相信他傳出的資料，也不要與其交換資料。

六、 展場參觀及交流

(一)Sprint Nextel Corporation

Sprint Nextel Corporation（Sprint）公司規模是全美國第四大的電信業者，提供消費者無線與有線的全面性通訊服務電信商，致力於全球性長途網際骨幹網路和無線網路經營，並且提供區域性交換機話務。Sprint 事業群包括行動數據服務、無線網路、區域性電信商業、WiMax 網路建置等。在 MWCLA 會議上，Sprint 參展攤位展示 5G 網路垂直應用服務，包括 VR、AR、機器人技術，並且與 Nokia 和 Ericsson 協作進行 5G 垂直應用服務展覽，其中 Ericsson 於參展攤位展現超人氣電競玩家—高橋茉莉子（AtomicMari），此款遊戲採用 Sprint 公司的 5G 行動網路（Sprint True Mobile 5G）及 Sprint 相關之 5G 系統設備。Sprint 亦使用自身公司之 5G 行動網路，整合 VR 展示真正的 5G 垂直應用服務場景。Sprint 為現場參觀者提供

Microsoft HoloLens 1 頭戴式虛擬實境裝置使用，透過 Sprint 的 5G 行動網路結合雲端伺服器之可靠性、安全性及可擴充性，而體驗到 Sprint VR 場景。透過 VR 浮動式虛擬數據顯示，參觀者本身可自行操作 5G 虛擬城市實境之智慧型城市與智慧型電廠應用展覽，並可以輕鬆的在 Sprint 展場範圍行走體驗無線服務，了解到 Sprint 公司如何在廣闊的美國國土上，解決 5G 網路覆蓋率的難題。在解決 5G 網路覆蓋率問題上，Sprint 在會場展示家庭式和小型企業式專用之新世代全無線圓石（Pebble）和魔術銀盒（Magic Box Silver）室內小型基地臺（Femtocell），其中 Magic Box Silver 室內小型基地臺由我國中磊電子公司（SERCOMM）研發、設計、製造，透過整合高增益收發天線及高階調變技術，提供穩定可靠的超高速傳輸，搭載全向性天線及輕薄化設計，方便靈活布署，可安裝於室內任何位置而不會降低接收訊號品質，並且可以支援 16 個使用者同時接取網路，可廣泛使用在改善網路覆蓋率之問題。搭配新世代全無線室內小型基地臺以及我國宏達國際電子公司（High Tech Computer Corporation, HTC）5G 集線器（HUB），使得展場設置之 5G 智慧手機可現場進行下傳量測評估 5G 網路性能，其中下行鏈路平均速率可達到 200 Mbps，而峰值速率可超過 600 Mbps。另外，Sprint 亦展覽了智慧型城市計畫之好奇號（Curiosity）IoT 應用服務，Sprint 和美國亞利桑那州立大學（Arizona State University）合作，將 5G 網路和 Curiosity IoT 結合，運用分散式大數據運算技術與虛擬化物聯網網路，以窄頻物聯網（Narrow Band Internet of Things, NB-IoT）做為在全國全面佈建長期演進技術（Long Term Evolution, LTE）M 類（Category M, Cat-M）網路的互補，來滿足各種物聯網設備的網路連結需求，其中 LTE Cat-M 是專為物聯網通信而專門設計的新型低功率廣域（Low-Power Wide Area）蜂窩技術、NB-IoT 商業服務

為 Curiosity 核心與 IoT 作業系統（Curiosity OS）進行結合。Sprint 除了展覽 Curiosity 物聯網垂直應用服務展覽議題外，亦與 Ericsson 整合窄頻物聯網與 Cat-M 網路技術結合之 5G 商業服務。我國電信技術中心團隊成員經由參觀 Sprint 展示攤位後發現，在使用 Microsoft HoloLens 1 頭戴式虛擬實境裝置操作上，其系統操作功能與浮動式虛擬數據之重疊功能對焦性不夠精準，無法提供參觀者流暢的 VR 應用導覽服務，也代表目前 5G MEC 技術運用尚未成熟。期待明年 MWC 2020 會場展示，Sprint 公司能結合新一代 Microsoft HoloLens 2 頭戴式虛擬實境裝置與增強型多重邊緣運算平臺運作，讓參觀者能夠真正體驗到 5G 網路殺手級垂直應用服務。此外，Sprint 亦展示建立另一個新的工業 IoT 網路架構與服務管理平臺，並與瑞典 Asea Brown Boveri 公司合作，著力於工業 IoT 之傳感器應用服務，如馬達運轉管理與設備狀態資料統計。

(二)Verizon Wireless

除了 Sprint 公司參展之外，隸屬美國四大電信業者中的 Verizon 公司亦參加此次盛會，Verizon 資產擁有全美國最大的 4G LTE 網路，亦經營全美國規模最大之 3G 網路，是美國境內無線寬頻網路、語音與資料服務最大電信營運商，其中 Verizon 除了使用 Ericsson、Nokia 電信設備大廠系統之外，該公司於美國境內部署亦開放性採用同於大會現場展示之 Airspan Networks 公司所銷售之 4G LTE 協議標準的寬頻無線相關系統終端設備。Verizon 在這次展覽中實現 5G 網路、混合實境（Mixed Reality，MR）、MEC 平臺之結合，並將大量的系統設備部署在會議中心南大廳位置，其中 MR 是 VR 中的一種新型技術，該技術透過在虛擬環境中引入現實場景資訊，在現實環境與虛擬環境中讓使用者體驗兩個環境重疊之視覺感受並且增強使用者所見事物之真實感。Verizon 利用教育性質之 VR 現場

展示、AR 輔助購物應用服務、5G MEC 平臺提供立體三維掃描，透過 5G 相關終端系統設備進行資料整合，並且即時執行商品物件虛擬三維模型建造，進而加速 VR、AR 之使用者所視之虛擬化內容建構。於 Verizon 展覽攤位上，該公司的 5G 網路使用毫米波技術進而提供更大量更快的資料傳輸速度，然而在電信技術中心團隊成員的試用下發現，使用者不能隨意走動並且距離基地臺太遠，以利保持流暢的 MR 應用服務。Verizon 公司人員說明該公司在美國境內目前尚未公佈 5G 網路覆蓋圖，然而隨著 5G 時代的到來，所有現象都表示 5G 網路化、虛擬化架構和 MR 系統效率與使用者體驗是可以得到顯著之改善，由於目前 Verizon 的 5G 垂直服務朝向可視化（Visualization）的應用，並且必須支援多用戶使用，因此 Verizon 開發圖形處理器（Graphics Processing Unit，GPU）切片（Slicing）技術，可以利用單一個圖形處理器切片來運算視覺處理為多位使用者提供 MR 服務。預期在不久的將來，Verizon 能夠提升該公司用戶之 AR、VR、MR 體驗與真實感，並且加入 AI、機器學習（Machine Learning）、深度學習（Deep Learning）等技術，讓遊戲玩家及使用者之體驗品質（Quality of Experience，QoE）大大提升。Verizon 現場展示測試數據，5G 網路搭配 NVIDIA 40 GPU RTX 平臺展示 V 應用服務，測試延遲時間縮短到 5 毫秒，其中 4G 網路的測試延遲時間超過 30 毫秒。此外 Verizon 宣稱，該公司為了發展從主動式防災技術機制，以安全城市概念與技術來改變美國境內之公共安全。會場亦展示具熱顯像功能之 AR 頭盔垂直應用服務，當搜救人員進入火災且高濃霧之現場，使用熱顯像技術可加快找到生還等待救援之民眾。同樣的，未來透過 5G 網路與 AI 融入救災技術中，使用高傳輸量、高速度的 5G 網路可縮短熱顯像運算與成像載入時間，整合 AI 平臺來運算與預測保障救災人員安全，平臺伺服器內運算與預測

之數據資料可能包括火燃燒的範圍與速度、火燒達建築物的時間與距離、建築物內儲存物品、儲存物品是否爆炸或助燃火勢、如建築物內等待救援民眾還剩下多少生存時間、等待救援民眾呼救聲方向與距離等，提供給指揮官與救災人員火場訊息、適當建議、正確預測。

(三)NVIDIA

NVIDIA 公司今年進行創新購物應用服務展示,透過結合 AI 技術將消費者思維和行為融入影像識別概念中。消費者智慧零售採用之智慧科技影像運算關鍵在於影像識別以及應用服務系統之間的整合與協調，並且可以進一步整合至 IoT 系統，提供即時與快速之商品影像偵測與識別服務，以利消費者與零售商之間創造虛擬互動模式有效掌握雙方商業行為，讓消費者舒適又便利的創體驗創新購物模式，創造更適合銷售商可採用之智慧零售辨識商業模式，提高商品管理效益、降低銷售通路成本。

NVIDIA 展示 AI 影像識別於智慧零售上的創舉，考量消費者採買與挑選行為上所需與改變，其中 NVIDIA 於會場展覽新型式無人智慧型冰箱，消費者只要使用手機上的第三方應用程式，掃描冰箱上的快速反應條碼（Quick Response Code，QR Code）並且認證後就可以解鎖並打開冰箱。冰箱上方並裝設攝影機，當消費者拿起飲料,攝影機會透過 AI 影像識別判斷並偵測該消費者下一個動作。假如消費者在挑選過程中拿起商品後又放回冰箱，系統也不會計算其金額，甚至放回冰箱時放置不正確商品位置。消費者最終挑選完商品後關上冰箱，手上的商品才會計入結帳金額，並立即經由該消費者行動支付付款。

(四)Ericsson

今年 Ericsson 公司於會場展覽 5G 基地臺系統設備、物聯網、智慧路燈應用服務等項目，由於積體電路技術日益精進，其 Ericsson 5G 基地臺系統設備日益縮小而且功能項目、運算力越來越增強，可以很輕易的隱蔽在任何公共設備的外殼內，因此造就了智慧路燈應用服務，可提供多元化網路範圍覆蓋部署方案。如前述，Ericsson 展示與 Sprint 公司合作的 Curiosity IoT 平臺，該平臺具有虛擬化核心網路和物聯網應用管理系統，而且展示 Ericsson 於該平臺實現更好的數據和設備管理能力。

Ericsson 亦於現場展示 5G 企業專網解決方案，網路可根據企業的特殊需求進行配置，並可以整合設備數據即時進行管理，為製造產業、輕/重工業、公共安全等各種垂直應用提供即時服務。此外，Ericsson 與加拿大 Solutions Ambra 採礦公司進行合作，於加拿大魁北克省（Quebec）開發 4G 與 5G 企業專網整合，該專網設置於地下 3.5 公里處，供給整個礦場數據及語音服務，地底中亦結合多個 IoT 開發與應用，有效改善人員安全和採礦操作運營。Ericsson 採用 LTE Cat-M 技術提供較高網路頻寬、即時性、移動定位的裝置型態，對於需小區重選的應用來說，LTE Cat-M 是很好的解決方案，可追蹤礦場內工作人員、運輸卡車、監視自動化通風系統。Ericsson 5G 網路發揮特性可就鏟式挖土機、車輛、電鑽機、其他採礦設備等機器進行遠程低延遲控制。Ericsson 設計整體網路解決方案及系統服務整合，再提供給 Solutions Ambra 公司協力進行專網維運，並有效簡化網路建置部署之工程項目。

(五)Nokia 與 Airspan

除設備商 Ericsson 之外，設備商大廠 Nokia 與 Airspan 亦在洛杉磯市區路燈燈桿上整合 4G 與 5G 基地臺，包含小型基地臺與大型基地臺之無線電寬頻頭端設備（Remote Radio Head），燈桿上並附掛整合攝影機與多項感測器等設備，完成智慧城市計畫之通訊基礎設施與垂直應用服務關鍵。Nokia 與 Airspan 公司提供 4G 與 5G 整合之智慧型路燈方案，透過在智慧路燈上安裝各式基地臺，以提供整體城市高密度網路基礎設施建置需求，例如路燈燈桿亦可作為交通號誌或數位看板之應用服務，推廣 5G 網路垂直應用服務商機。



圖 4-6-1 *2019 洛杉磯世界行動通訊大會*展場參觀與交流

陸、 心得與建議

本次前往美國洛杉磯參與 2019 MWCLA，在會議中聆聽北美地區相關電信監管機構、城市管理單位、電信運營商及設備大廠就 5G 產業的部署與應用，包含 IoT、垂直領域、供應鏈安全及商業模式的經驗分享，並於 MWCLA 展場蒐集全球主要 5G 服務提供商與設備業者邁入 5G 時代之推動策略，所得出之心得與建議如下三點。

(一)美國 5G 政策以強化應用市場影響力邁進

首先，美國在政策上已轉向角逐 5G 應用與服務，同時要豐富供應鏈的多樣性，避免單一國家壟斷示場，解決國家安全、經濟領導力與影響力議題，在與 5G 產業鏈逐漸成熟之際，尋求下一個殺手級的 5G 應用，是美國奪取 5G 領導力與影響力的目標，雖然在 5G 部署初期，eMBB 是大多數消費營客戶之需求，但垂直應用需求如車聯網、智慧工廠、醫療、災害監控等 5G 應用是另一個發展關鍵區域。其中 FCC 主任委員於政策演講中表示，透過包含釋出更多頻譜、升級基礎建設及其政策、調適過時的監理法規等三大面向的 5G 加速方案（5G FAST Plan），可有效強化 5G 技術的發展，同時並激勵 5G 創新投資，其中具備前瞻性的頻譜政策尤其重要。另外為滿足 5G 時代的各種應用，預期具備網路切片、高密度小基地臺、廣覆蓋的物連網等企業專用網路垂直場域的應用也將佔相當比例，這些將大幅改變傳統電信業者的商業模式，因此調適既有法令規範亦是政府現行所面臨的挑戰。上述議題討論都對我國在推動 5G 產業發展的政策規劃上提供重要的參考。

(二)5G 應用驅動資安防護技術發展

隨著各地 5G 建設的起跑，眾多與會人士都呼籲初期建設 5G 系統時一定要將網路安全議題納入設計藍圖中，若是等到事後才進行安全功能的增補會耗費更多的成本。會中美國網路安全暨基礎安全局(CISA)總監也特別提到 5G 所面臨之安全議題是非常嚴峻且影響深遠，並認為 5G 網路安全對整個國家的關鍵基礎建設施環境至關重要，是無法承擔任何風險的領域，並需提升通信基礎設施之強韌性、增強防禦態勢。因此美國聯邦政府也正在針對如何提升通訊系統的強韌性與可靠性，蒐集各種攻擊與威脅手法，如透過國土安全部(DHS)的預算補助通訊系統各層間的防護技術研發與創新發展，成立一個跨部門的專屬 ICT 供應鏈風險工作小組，探討相關威脅並提出防護的最佳措施（Best practice），並落實禁止使用可能有資通安全風險疑慮供應商所提供之設備，以確保美國境內 5G 網路的安全；以上可做為我國政府 5G 監理政策發展的重要參考，因為除了面對國際政治上的緊張情勢，我國需要確保關鍵基礎通信環境健全，另外為持續發展資通訊產業，我國需要外銷 5G 系統與應用服務，網路安全也將會是優先考量的議題。

(三)5G 與 AI 將促進智慧城市應用發展：

5G 將促進現有智慧城市發展，例如帶動智慧路燈上整合 5G 基地臺，不僅僅包含無線發射單體之無線發射單體，更會提供附掛多項感測器與攝影機，產生高密度的數據資料數據。這裡我們要指出這是一個多科技融合才能達到的智慧城市的理想境界，5G、IoT、AI、大數據與雲端技術缺一不可。沒有 5G，不能承載與傳輸大量即時數據。沒有 IoT，無法取得異質與多維度數據與控制實體設施，與真實世界產生連接。沒有 AI 技術，機器無法訓練與學習，使人類決策思維重複利用。沒有大數據與雲端技術，資訊基礎建設根本不合成本效益。如何融合這些科技，發展應用創新，將是未來的核

心競爭能力，但這些技術相信不是單一企業可以擁有，缺乏熟練的人才與強有力的領導力，國內要發展 5G 創新應用，如智慧製造、智慧醫療與車聯網，合理的發展策略應該依照國際供應鏈分工下，緊緊跟著主流市場走。而我們在 MWCLA 觀察到的，供應鏈安全與隱私人權絕對是歐美主流市場所心心念念的重中之重，例如邊緣運算中有個需求是將街口的攝影機，利用邊緣運算就去除掉車輛與行人之外觀，回傳後端系統就只有簡單的計數數字與描述資料就是個好例子。而這卻是國人在設計系統時，很難想像的需求。

附件三 「2019 歐盟網路安全法國際會議（International Conference on the EU Cybersecurity Act）」參訪報告

財團法人電信技術中心出國報告

出席 2019 歐盟網路安全法案國際研討會（2019 International Conference on the EU Cybersecurity Act）

單位名稱：檢測暨網通技術組、資通安全組、研究企劃組

姓名職稱：林家樑副主任、李兆文工程師、黃禾田助理研究員

派赴國家：比利時

出國期間：2019/11/16-2019/11/22

報告日期：2020/01

摘　要

歐盟《網路安全法（The Cybersecurity Act，CSA）》已於 2019 年 6 月 27 日生效。該法案除了強化歐盟網路和資訊安全局（ENISA）之權力，亦由 ENISA 主導建立歐盟範圍的網路安全認證框架以因應網路安全的威脅和攻擊。

《網路安全法案（CSA）》通過後，ENISA 將轉型為此一法案之關鍵管理機構，未來 ENISA 將擬定一項資通安全認證框架，該框架可能區分 Basic、Substantial、High 等三種級別，其中在 Basic 級別，ICT 製造商或服務提供商可進行自我評估，而在 Substantial 和 High 等級別，則交由歐盟會員國之安全認證機構，自行訂定與認定。但由於各國對於資通安全認證之規定與要求不盡相同，故在未來相關驗證標準的調和仍須透過討論，才能逐漸向資通安全認證框架對齊。

壹、 目的

本次前往比利時布魯塞爾參加 2019 EU Cybersecurity Act 會議，主要是希望透過參與會議，掌握主要國家之電信監理單位或資通安全管理單位對於 5G 資通安全最新研析、政策及實際作為，以利後續法規調適之參考。

歐盟為加強網路安全結構、增強對數位技術的掌控及確保網路安全應當遵守之法律規範，已於 2019 年 4 月 17 日通過網路安全法案（CSA），並自 2019 年 6 月 27 日生效（部分條款自 2021 年 6 月 28 日生效）。該法除成立一永久性之歐盟網路安全專責機構-歐盟網路與資訊安全局（ENISA），以進一步落實 NIS 指令（包括為基本服務提供者及數位服務提供者使用之網路資訊系統提供資通安全防護建議、指導及最佳實踐等），並責成其協助制定 ICT 產品、服務和流程之資通安全認證框架相關政策及協助各國實施，同時要求各會員國至少指定一個該國國家級的資通安全認證機構。

ICT 產品、服務和流程之資通安全驗證計畫雖屬自願性認證，但如果該產品、服務或流程使用於基本服務提供者（Operators of Essential Services，即我國關鍵基礎設施）或數位服務提供者（digital service providers），則將成為強制規定，該法並授權及要求各會員國於其國內法規中明定違反歐盟資通安全認證相關處分。目前歐盟部分會員國雖已施行資通安全驗證計畫（包括資通安全要求及評估標準），但處於發展初期的歐盟《網路安全法案（CSA）》最終將其整合並建立一個廣泛且獨立於歐盟網路安全法規體系，並作為「單一數位市場」目標之一部份。

5G 網路亦屬 ICT 產品、服務和流程之一部，鑑於德國、義大利、芬蘭、英國、瑞士、愛沙尼亞等歐盟會員國均已提供 5G 服務，且我國亦已規劃於今（108）年年底前釋出 5G 頻段，並期許於明年釋出 5G 特許執照。為確保我 5G 網路安全、強韌及可信賴，實有對其資安驗證計畫深入瞭解，並汲取其經驗，以促進我國產業轉型與發展，奠定數位經濟發展之基礎。

貳、 行程

一、 出國時間：108 年 11 月 16 日至 11 月 22 日

二、 地點：比利時布魯塞爾

三、 本中心出席人員：林家樑副主任、李兆文工程師、黃禾田助理研究員

四、 時間安排：

表 1　行程表

日期		行程
Day 1	11/16	19：40 搭乘國泰 CX451 由桃園機場出發
		21：45 抵達香港國際機場
Day 2	11/17	01：20 搭乘國泰 CX339 由香港國際機場出發
		06：50 抵達布魯塞爾機場
Day 3	11/18	參加 2019 歐盟網路安全法國際會議第一日
Day 4	11/19	參加 2019 歐盟網路安全法國際會議第二日
Day 5	11/20	私人行程
Day 6	11/21	12：55 搭乘國泰 CX338 由布魯塞爾機場出發
Day 7	11/22	07：05 抵達香港國際機場
		09：00 搭乘國泰 CX530 由香港國際機場出發
		11：00 抵達臺灣桃園國際機場

五、 會議議程：

表 2 第一天議程

<table>
<tr><td>08:00-
09:00</td><td colspan="2">REGISTRATION</td></tr>
<tr><td>09:00-
10:30</td><td colspan="2">PLENARY KEYNOTE SESSION
09:00
Conference Plenary Keynote Address (P10a)
Juhan Lepassaar, Executive Director, European Union Agency for Cybersecurity (ENISA)

09:50
Conference Welcome Presentation: The Cybersecurity Act is Here, But What Does This Mean? (P10b)
Sergio Lombán Lage, VP, Digital Trust Services, SGS Group, Spain</td></tr>
<tr><td>10:30-
11:20</td><td colspan="2">NETWORKING BREAK</td></tr>
<tr><td rowspan="2">11:20-
12:30</td><td colspan="2">TRACK SESSIONS 1</td></tr>
<tr><td>Panel Discussion
12:00
Certification for Critical Infrastructures (P11a)
Moderator: Jacques Kruse Brandao, Head of Advocacy Digital Trust Services, SGS Group, Germany
Panelists: John Boggie, Director Head of Certification, NXP Semiconductors UK, United Kingdom; Sergio Lombán Lage, VP, Digital Trust Services, SGS Group, Spain; Julian Meyrick, Managing Partner & Vice President, Security Strategy Risk & Compliance, Security Services, IBM, United Kingdom; Eva Schultz-Kamm, Head of</td><td>Industry Alignment
12:00
ETSI Security Evaluation Standardization Initiatives (A11a)
Sonia Compans, Technical Officer, ETSI, France

12:30
Lessons Learnt in the Commercial Use of Security Certification—From Setting Standards to an Innovator’s Perspective (A11b)
Boris Balacheff, HP Fellow & VP, Chief Technologist for Security Research and Innovation, HP Labs Security Lab, France</td></tr>
</table>

	Global Government Affairs, Siemens, Germany	
12:30-13:50	LUNCH BREAK	
13:50-16:00	TRACK SESSIONS 2	
	Public Policy 14:00 **Update on ENISA Operations and CSA Implementation** (B12a) Slawomir Górniak, Security Tools and Architecture Expert, European Union Agency for Network and Information Security (ENISA), Greece 14:30 **European Cybersecurity Certification Framework, State of Play** (B12b) Aristotelis Tzafalias, Policy Officer, Cybersecurity and Digital Privacy, European Commission, Belgium 15:00 **ECSO's Outlook on the EU Cybersecurity Act** (B12c) Roberto Cascella, Senior Policy Manager, ECSO, Belgium 15:30	Industry Alignment 14:00 **Vendor Self-Assessment—The Good, The Bad, and the Ugly** (A12a) Helmut Kurth, Chief Scientist and Laboratory Director, atsec information security, Germany 14:30 **ISCI WG (International Smartcard Initiative) Who Are We? What Do We Do? How Do We Do It? And How Do We Contribute to The EU Cyber Act?** (A12b) Rachel Menda-Shabat, Director of Security Solution Certification Division, ISCI WG sub-chair, Winbond, Israel 15:00 **Update on The EU Cybersecurity Act: Is The Feared Balkanization of Common Criteria Being Reversed?** (A12c) Martin Chapman, Senior Director, Standards Strategy and Policy EMEA, Oracle, Ireland

	Security Needs to be Consistent—The Role of Process in the Cybersecurity Act (B12d) David Martin, Head of International Assurance, NCSC, United Kingdom	15:30 **The Certification Landscape and What Industry Needs** (A12d) John Boggie, Director Head of Certification, NXP Semiconductors UK, United Kingdom
16:00-16:30	NETWORKING BREAK	
16:30-18:00	TRACK SESSIONS 3	
	Standards for Success 16:30 **CEN-CENELEC JTC13 WG3 Security Evaluation Standardization Initiatives** (S13a) Miguel Bañon, Global Technology Leader for Cybersecurity, Epoche and Espri (a DEKRA company), Spain 17:00 **Comparing National Lightweight Methodologies around Europe** (S13b) Javier Tallon, CoFounder and COO, jtsec Beyond IT Security SL, Spain 17:30 **Implementing and Maintaining a Cybersecurity Program—The Role of Standards** (S13c)	Cloud and GDPR Frameworks 16:30 **Toward the European Cloud Security Certification Scheme: The CSPCERT Final Public-Private Recommendation** (C13a) The European Cloud Service Provider Certification Working Group, Saurabh Ghelani, EMEA Strategic Trust Leader, Google Cloud, et al. 17:00 The EU-SEC Framework (C13b) Lefteris Skoutaris, Research Analyst, Cloud Security Alliance, Greece 17:30 Addressing GDPR Requirements Using the ISO/IEC 27701 Standard. Is the CSA Looking At It? (C13c) Willy Fabritius, Global Portfolio Champion for Information Resiliency, BSI Group, United States

	Raymond Romero, Deputy Director, Board of Governors of the Federal Reserve Systems, United States	
18:00	ADJOURN	

表 3 第二天議程

	TRACK SESSIONS	
09:00-11:00	IoT Challenges 9:00 **Embedded Systems for IoT Products: What is the Current Certification Offer?** (I20a) Dr. Claire Loiseaux, CEO, Internet of Trust, France; Alexander Schasse, IT Security Consultant bei TÜV Informationstechnik GmbH – TÜViT, Germany 09:30 **SESIP: A Practical, Operational, Lightweight CC Methodology** (I20b) Wouter Slegers, CEO, TrustCB, Netherlands 10:00 **EUROSMART IoT Security Certification Scheme (eIoT SCS)** (I20c) Roland Atoui, Managing Director, Red Alert Labs/EUROSMART, France; and Ayman Khalil COO & Managing Partner Red Alert Labs	Industrial Strategies 09:00 **Foundations and Perspectives of the EU's 2019 Cybersecurity Act Certification Legislation for the Industrial Automation and Control Systems** (T20a) Paul Theron, Advisor & Cyb'Air Research Chair, Thales, France 09:30 **Beyond the Theory of the Cybersecurity Act** (T20b) Stefano Bracco, Knowledge Manager, European Union Agency for the Cooperation of Energy Regulators, Italy 10:00 **IEC62443 and NIS Directive: Needs and Opportunities** (T20c) Maria Fravventura, Security Evaluator, Brightsight, Netherlands

	10:30 **X-Gateway as a Modular Part of IoT** (I20d) Markus Bartsch, Business Development, TUViT, Germany	10:30 Building Trust and Hope in 5G Instead of Selling Fear (T20d) Mika Lauhde, Global Vice-President, Cybersecurity & Privacy, Global Public Affairs, Huawei, China
11:00-11:30	NETWORKING BREAK	
11:30-12:30	TRACK SESSIONS	
	IoT Challenges 11:30 Common Criteria as Backbone of IoT Security Certification (I21a) Georg Stütz, Principal Security Certification Expert, NXP Semiconductors, Austria 12:00 **OWASP IoT Project: A Great Ally for the IoT Candidate Schemes** (I21b) Jose Alejandro Rivas Vidal, Security Lab Manager, Applus+ Laboratories, Spain	Panel Discussion 11:30 **Standardization and the EU CSA** (P21a) Discussion on standardization efforts under various national frameworks. **Panelists:** Sonia Compans**,** Technical Officer, ETSI, France; Philippe Magnabosco**,** Policy Advisor for External Standards, ANSSI, France; David Martin, Head of International Assurance, NCSC, United Kingdom[60 Minutes]
12:30-13:30	LUNCH BREAK	
13:30-15:30	TRACK SESSIONS	
	Outlook/Opportunities 13:30 **SOGIS View on the Cybersecurity Act** (L22a) Bernd Kowalski, Chairman, SOG-IS, Germany	Innovations in Assurance 13:30 **Addressing the Continuity of Software Security for Embedded Devices** (N22a) Jasmina Omic, Product Manager Services, Riscure, Netherlands

	14:00 **Overview of Current and Future NIAP and US Government Certification Initiatives** (L22b) Mary Baish, Director, NIAP, United States 14:30 **BSI View on the EU Cybersecurity Act** (L22c) Speaker TBA, BSI, Germany 15:00 **The ROI of Security Evaluations** (L22d) Dirk-Jan Out, CEO, Brightsight	14:00 **Updating Certified Products** (N22b) Gabor Hornyak, CTO, CCLab, Hungary 14:30 **Agile Assurance: Modernizing IT Product Certification** (N22c) Lachlan Turner, Director Consulting, Lightship Security, Canada 15:00 **Making Evaluation Schemes Scale Up: the Tensegrity of Process and Product** (N22d) Tony Boswell, Senior Principal Consultant, DNV GL Technical Assurance Laboratory, United Kingdom
15:30-16:00	NETWORKING BREAK	
16:00-17:00	CLOSING PRESENTATION, SUMMARY PANEL DISCUSSION 16:00 Panel Discussion: Looking Ahead to the Next Generation of Industry Assurance (P23a) **Moderator:** Chris Gow, Director, EU Public Policy, Government Affairs, Cisco, Belgium **Panelists:** Michael Cooper, Manager, Security Testing, Validation and Measurement Group, National Institute of Standards and Technology (NIST), United States; Slawomir Górniak, Security Tools and Architecture Expert, European Union Agency for Network and Information Security (ENISA), Greece; Jonathan Sage, Government and Regulatory Affairs, IBM, United Kingdom; Aristotelis Tzafalias, Policy Officer, Cybersecurity and Digital Privacy, European Commission, Belgium	
17:00	ADJOURN	

參、 會議過程及內容

一、 開幕式及主題演講（Conference Welcome Presentation）

開幕式及主題演講分別由歐盟網路與資訊安全局（ENISA）執行董事（Executive Director）Juhan Lepassaamr 與本次會議最大贊助商 SGS 集團主管數位服務的副總裁 Sergio Lombán Lage 各提供主題演講。

(一)ENISA 執行董事[1]Juhan Lepassaar

Juhan Lepassaar 為愛沙泥亞人，於今年 10 月 16 日就任，在接任執行董事之前，他於歐盟執委會服務 6 年，並曾於前任歐盟副主席 Andrus Ansip 團隊中擔任負責數位單一市場事務的主管。本次研討會邀請他出席提供開幕主題演講。本次演講未設定主題，Lepassaar 執董主要評論網路安全法案（CSA）為歐盟在網路與資訊安全治理帶來的幾項變革，分為三點：

1. 提昇 ENISA 重要性並協助評估 5G 網路安全風險：網路安全法將 ENISA 由臨時性、任務型編組改制為歐盟執委會轄下的官方組織，提昇歐盟在網路安全治理上的專業能力。在網路安全法通過之前，歐盟於 2016 年通過「歐盟網路與資訊安全指令」（EU Network and Information Security directive, NIS

[1] 執行董事負責 ENISA 日常之運作與管理。ENISA 的治理結構分為經營董事會（Management Board）、執行董事會（Executive Board）、執行董事（Executive Director）、ENISA 諮詢小組（ENISA Advisory Group）、成員國聯絡官員網路（National Liaison Officers Network）。歐盟成員國各指定一名成員一起與歐盟執委會指定之兩名成員共同組成經營董事會，任務包括規劃組織發展方向及確保其運作符合歐盟各項法規；從經營董事會中在互選五名成員組成執行董事會，並由五人之中一人做為執行董事會之主席與執行董事，另五人之中需有一名歐盟執委會代表，執行董事會任務則為制定 ENISA 程序性規則。關於 ENISA 組織結構可參見 Regulation (EU) 2019/881 第 13 條至第 18 條。

Directive）[2]，由各成員國建立網路資訊安全協作小組（NIS Cooperation Group）與歐盟執委會合作處理歐盟境內的網路安全事項。ENISA 自設立以來即已就網路與資訊安全事項提供執委會建議與配合 NIS 協作小組，而在制度化後除能更具效率協助執委會與協作小組，伴隨 5G 網路布建衍生的設備安全問題，ENISA 也遵循執委會於今年 3 月發布「5G 網路安全建議書」（Recommendation on Cybersecurity of 5G networks）之要求，協助成員國檢視自國 5G 基礎網路建設所涉特定的威脅與影響因素，歸納各國內容於今年 10 月 6 日綜整提出歐盟層級的 5G 網路安全風險評估報告（EU coordinated risk assessment of the cybersecurity of 5G networks），描述當前歐盟成員國對於 5G 網路風險來源的看法，並劃分 10 類風險情境（risk scenarios），舉例而言，10 種風險情境之一為「缺乏接取控制措施」（lack of access controls），指的是由於組織缺乏足夠的接取控制措施，使得懷有惡意且具備網路管理員權限的分包商得以破壞受保護資訊的機密性、完整性、可用性。

接著 5G 網路安全風險評估報告，ENISA 接下來的工作則是從技術面進一步描繪對 5G 網路安全造成影響的威脅樣態，此項工作針對組成 5G 網路架構的各關鍵元件，提出潛在的網路安全漏洞。這份名為「ENISA 的 5G 網路威脅風貌」（ENISA threat landscape for 5G Network）之文件預計於 11 月 21 日發布[3]，該文件將當前可能的網路威脅種類劃分為濫

[2]全稱為 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union）

[3] https://www.enisa.europa.eu/news/enisa-news/enisa-draws-threat-landscape-of-5g-networks.

用型（Nefarious activity/abuse (NAA)）、攔截型（Eavesdropping/Interception/ Hijacking (EIH):）、物理攻擊型（Physical attacks (PA)）、損害型（Damage (DAM)）、意外損害型（Unintentional Damage (UD)）、故障型（Failures or malfunctions (FM):）、中斷型（Outages (OUT)）、災難型（Disaster (DIS):）、法律型（Legal (LEG)）共 9 類，並將此 9 種類型與 5G 網路元件綜合歸納為對核心網路的威脅、對接取網路的威脅、對多重邊緣運算的威脅、虛擬化功能的威脅、實體基礎建設的威脅、一般性威脅、對軟體定義網路的威脅。ENISA 在盤點完當前對於 5G 網路安全的類威脅後，將依據「5G 網路安全建議書」之指示，訂於本年 12 月底前提出 5G 網路風險減輕措施工具箱（a common toolbox of mitigating measures），提供各成員國參考。

2. 建立網路安全認證框架幫助消費者了解網路安全：網路安全法另一項重要工作在於建立全歐盟適用的資通安全認證框架（cybersecurity certification framework），此一認證框架規範資通訊產品、服務、流程三面向，歐盟執委會的期望是未來藉由認證框架的建立，制定各領域的資通安全驗證計畫（cybersecurity certification scheme），藉由認證有無搭配市場機制運作，希冀能幫助消費者取得相對安全的資通訊產品、服務、與操作流程。ENISA 做為負責建立網路安全認證框架的執行單位，除依據歐盟滾動式工作項目（The Union Rolling Programme, URWP）與執委會指示提出認證框架候選計畫（candidate scheme），另一項工作也包括設立網站，存放各項安全認證框架候選計畫之細節與歐盟官方對於認證一致性（conformity）的聲明，而歐盟的一般民眾則可藉此了解網路

安全認證框架的各項細節，藉此強化個人資安意識，並於未來選購具有安全認證的資通訊產品及服務，淘汰不符合歐盟安全標準的產品與服務。

3. 增強網路安全相關研究：Lepassaar 執董評論的最後一點是基於網路安全法之授權 ENISA 現在有更豐富的資源可針對網路安全風險、預防措施增強相關研究。以 5G 網路為例，由於各成員國已提交各自的網路布建風險評估，而 ENISA 綜整各國內容，盤點未來 5G 網路在布建與運作上可能存在的網路漏洞與網路威脅，並預計提出相應的減輕措施，此即為由於網路安全法使 ENISA 成為歐盟正式官方組織，因此得以進行之工作。未來 ENISA 將運用資源，增強相關網路安全研究，進而協助歐盟成員國建立符合自身需求的網路安全防護措施。



圖 **1**：ENISA 執行董事 Juhan Lepassaar

資料來源：出國報告人拍攝

(二)SGS 副總裁 Sergio Lombán Lage

在 Juhan Lepassaar 之後的主題演講人為 SGS 集團數位信任服務業務副總 Sergio Lombán Lage（如圖 2）。做為國際知名的專業驗證企業，資安驗證服務原即屬 SGS 既有業務之一，然而鑑於未來大量物聯網裝置將遍及各行各業以及 5G 網路的出現，自 2018 起 SGS 將該公司既有的各種資安能量整合成為數位信任服務（Digital Trust Service），提供四項領域的資安服務：資通訊產品及系統、網路通訊及雲端、資安管理系統、服務與專業認證、資料整合（詳參圖 3）。Lage 副總為數位信任服務的負責人，自身於網路安全法草案諮詢期間，以專家身份參與並提供相關意見，他以「網路安全法的出現意欲何為」（The Cybersecurity Act is Here, But What Does This Mean?）為題，從業界實務經驗出發，探問對目前的資安實務而言，這部法律出現的意義為何？



圖 **2**：SGS 副總裁 Sergio Lombán Lage

資料來源：出國報告人拍攝

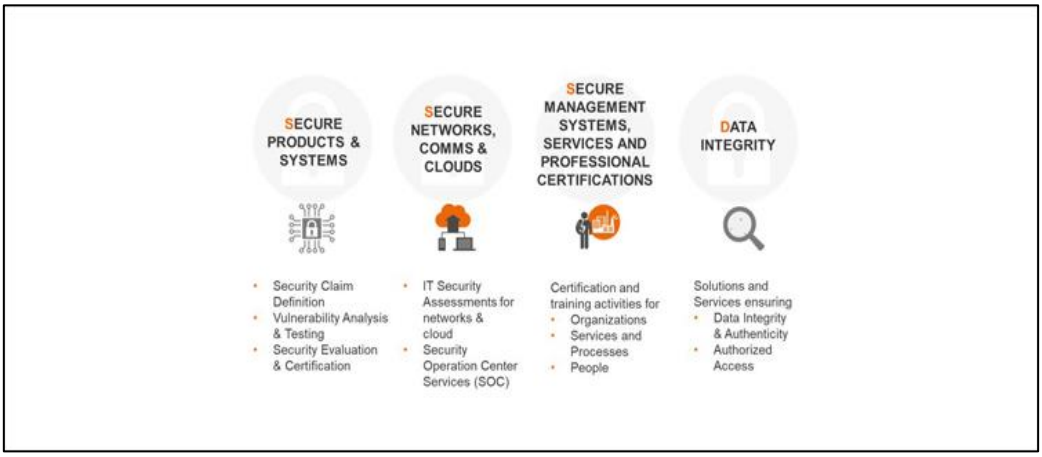


圖 **3**：SGS 數位信任服務業務涵蓋領域

資料來源：SGS 官方網站

1. 法規的目的在於建立人民的信任：Lage 認為在當前數位時代公司治理的主要議題為取得消費者信任及保護企業聲譽，也因此有遠見的企業無論規模大小皆將一部分利潤投資於資安措施，建立良好的資訊安全管理制度與防禦網路攻擊，就此而言，歐盟設立網路安全法，加強 ENISA 職能並試圖建立全歐盟適用的資通安全認證框架，立意良善，提供企業及消費者依循及選擇的基準，並建立對於資通訊產品及服務的信任感。然而從目前法規內容觀之，資通安全認證框架提出基本（Basic）、實質（Substaintial）、高級（High）三種安全保證層級（assurance level），雖可從概念上區分，在認證標準實務上則尚無人提出各方皆可接受的共同基準。換言之，Lage 認為徒法不足以自行，在實務上如何解決共同基準的問題，以及在後續相關配套中提供市場與消費者更具體的措施將是未來有效落實網路安全法的最重要挑戰。

2. CSA 可以像 GDPR 一樣成為全球黃金標準：鑑於歐盟市場的性質，Lage 也認為 CSA 的誕生很可能像幾年前一般資料保護規則（GDPR）一樣，具有成為全球通用標準的潛力，不過要

達成此一目標，各類驗證標準彼此的相互承認將成為國際市場的主要議題。此外，哪些垂直產業（Vertical Industries）為優先建立具體資安認證標準的項目，涉及第三方服務的供應鏈管理議題以及市場本身的喜好也將是未來資通安全認證框架成功落實所需考量的因素。Lage 在演講結束之際，以「產業內真正玩家所參與並回答正確問題」的初步嘗試加以評論網路安全法的制定，並期許未來能藉由該法的落實，使市場發揮良性競爭的潛力。

二、 小組討論

(一)關鍵基礎設施資安認證（Certification for Critical Infrastructures）

本場小組討論之參與人包括主持人 SGS 數位信任服務推廣主管 Jacques Kruse Brandao，報告人兼與談人西門子全球治理事務主管 Eva Schultz-Kamm、與談人 NXP 資通安全驗證主管 John Boggie、TÜV SÜD 資通安全策略主管 Sudhir Ethiraj、SGS 數位信任部門副總裁 Sergio Lombán Lage、IBM 合夥人暨資安服務副總裁 Julian Meyrick（如圖 4），討論主題為「信任憲章」（Charter of Trust）提出之原則在驗證實務上的落實情形。進行方式首先由 Eva Schultz-Kamm 報告「信任憲章」之內容，接著以信任憲章第 2 條及第 7 條原則展開討論。



圖 4：關鍵基礎設施資安認證小組討論現場。左起為主持人 Jacques Kruse Brandao、Sudhir Ethiraj、Eva Schultz-Kamm、John Boggie、Sergio Lombán Lage、Julian Meyrick

資料來源：出國報告人拍攝

1. 開場簡報：信任憲章之概述

信任憲章全名為「資通安全信任憲章」（Charter of Trust on Cybersecurity）為歐洲網通大廠西門子（Siemens）於 2018 年 2 月號召各大企業共同依循的資通安全產業自律規範，包括西門子在內目前共有 16 家跨國企業簽署[4]。信任憲章設定三項目標，分別是保護個人及公司資料、避免損害個人、企業及基礎建設、建立使數位世界可資信賴的基礎環境。信任憲章包含 10 條原則，分別是：網路與資訊安全所有權原則（Ownership of cyber and IT security）、負責任的數位供應鏈原則（Responsibility throughout the digital supply chain）、安全預設原則（security by default）、以使用者為中心原則（User-centricity）、創新與共創原則（Innovation and co-creation）、資

[4] 16 家企業為 AES、AIRBUS、Allianz、Atos、CISCO、DAIMLER、DELL、IBM、MSC、NXP、SGS、SIEMENS、Deutsche Telekom、TOTAL、TÜV SÜD、Mitsubishi Heavy Industries。

安教育原則（Education）、關鍵基礎設施及解決方案之驗證原則（Certification for critical infrastructure and solutions）、透明及回應原則（Transparency and responses）、法規框架原則（Regulatory framework）、聯合倡議原則（Joint initiatives）。

2. 議題討論：

Eva Schultz-Kamm 簡報完畢後，主持人 Jacques Kruse Brandao 首先進一步追問 17 項基準要求的落實程度，並藉此逐一讓其餘專家針對 17 項基準要求發表評論。Eva Schultz-Kamm 與 Julian Meyrick 皆表示此 17 項基準要求只是未來供應鏈生產的基礎要求，Sergio Lomban Lage 亦進一步指出此 17 項基準要求可以說是全球具代表性的企業對於安全的想法，其價值不但在於橫跨多方且也足以符合業界對於效率的要求。

主持人提出的第二項大議題是信任憲章如何與世界主要國家的資通安全法律協調一致，特別尤其是網路安全法提出建置歐盟資通安全認證框架，信任憲章的內容如何符合？在場的專家皆同意信任憲章目標之一即是協助政府更好落實資通安全驗證的工作，特別是以網路安全法而言，該法關注的是政治制度上的調整，而信任憲章則是從產業本身需求思考建立數位信任（digital trust）的做法，但這非易事，對簽訂信任憲章的企業而言也仍處於從實踐中學習的過程。以此觀之，信任憲章實際上是在回應網路安全法的初始設計想法，藉由歐盟資通安全認證框架的機制，配合信任憲章的基準要求，盤點當前已有且可用的標準，以制定後續特定領域的資通安全驗證計畫。

主持人的第三項大議題是信任憲章原則 7 提出關鍵基礎設施的驗證，因此請在場專家說明其意義，實務上如何運作，以及如何支援法規的落實。在場專家表示信任憲章提出對於關鍵基礎設施的驗證，立基於在超高速且萬物聯網的時代，所有資通訊設備以及可聯網的一切裝置皆存在潛藏的資安問題。然而驗證本身不創造安全環境，驗證代表的是對驗證對象的信任程度，因此信任是一切的基礎。就此而言，依據安全設計開發以及具備安全預設的產品即無庸驗證，因為安全設計與安全驗證即是呈現信任的一種措施；進一步而言，原則 7 描述的是企業為關鍵基礎設施提供的產品需要有獨立第三方的驗證，這是基於關鍵基礎設施產品屬於信任規則（Rule of Trust）中的重要部分，而信任規則總是需要一再確認，因此原則 7 才做如此要求。簡言之，並非所有資通產品都需要獨立第三方的評鑑，但在極端要求安全的環境中，獨立第三方評鑑皆會是最核心的部分。

(二)歐盟網路安全法案及標準化（Standardization and the EU CSA）

來自歐洲電信標準組織 ETSI 的 SONIA COMPANS 女士說明 ETSI 有權提供與支持歐盟政策的所需要的標準，ETSI 標準涵蓋範圍是對網路和整個系統進行全面性的關注，ETSI 從一開始就將網路安全列入考量。譬如要定義不同網路功能元件之間使用的加密機制，如何進行身份驗證等等。但 ETSI 在安全與風險評估上沒有太多經驗，ETSI 在 IoT 安全上的出發點是定義安全性要求，針對消費者端的物聯網所使用的技術和流程。目前 IoT 市場的安全議題是處於混亂情況，並且許多公司沒有為其產品提供安全功能與流程。因此當前 ETSI 只邁出非常小的一步，但是如果設法做到這一步，並且所有供應商都做到這一步，那麼將大大提高整體的安全程度。因

此，ETSI 定義了一些安全要求，例如在德國 BSI 的幫助下，ETSI 開始著手定義評估規範。

來自法國資訊安全機構 ANSSI 的 PHILIPPE MAGNABOSCO 先生則說明在 CSA 中，制定網路安全的標準是一件有意義和重要的事情。CSA 理想是希望在公共政策方面採取一些重大且一致的步驟來取得成功。重要的一點是，ANSSI 作為國家網路安全機構，在制定網路安全標準的角色上，要使其他部門標準之間保持一致。當然，多年來使用通用準則 CC 不會消失，因為它們在 CSA 中絕對起著作用，因此 ANSSI 正在努力並花費大量資源試圖使它們變得更好。最後，ANSSI 認為需要使標準被市場接受，標準本身也需要明確準則，以明確所認證的內容，針對什麼級別的認證，標準也需要保持一致性，講者強調這是種能力管理。另外講者也說明通用準則 CC 中存在一個反饋循環的環節，這使 CC 類似於教練，在此過程中評估人員可能會發現缺陷，並且改進這些缺陷，然後才進行評估，若要加速驗證的過程需要切斷反饋迴路，縮小驗證流程規模並集中精力測試產品。

來自德國 BSI 的 HELGE KREUTZMANN 先生則說從 BSI 的角度或從德國的角度來看，始終重要的一點是標準要獲得國家層級的良好實踐與經驗，再建立歐洲或國際標準或前期標準。BSI 參加多個組織，也將 BSI 的經驗帶到了標準化組織，將其帶入了歐洲範圍，然後 BSI 通過許多工作組，並在其中擔任部分職務，試圖將 BSI 的經驗加以推廣，以便將這種經驗進行標準化，最終將標準應用於認證產品。舉幾個例子，計量公路車輛的運行情況，BSI 參與制定歐洲標準，另一個例子是智慧卡，現在也已在歐洲使用。

來自英國資安機構的 DAVID MARTIN 先生則說到大家可能知道英國在幾年前就發展了自己的商用產品保證計畫（Commercial Product Assurance，CPA)，CPA 詳細說明標準的要求，並希望與行業公認的測試方法保持一致，因此需要發展與行業協作的保護配置文件，但這將需要很長時間，並且在英國，大家都迫切需要一種能夠解決多種產品保證問題的工具。CPA 是一項全國性計畫，其優點是若遇到任何困難，可以與國內的 NCSC 聯絡，這一點是國際標準沒有能力做到的。而 CPA 計畫確實有一半要求，是所謂的“Bill Standards”，也就是在很大程度上是作業與流程安全，因此它所執行的不僅僅是通用準則 CC。CC 在流程保證的部分並不那麼強力有效，故採用 CPA 標準可以更有利益。就目前而言，CPA 實際上僅用於英國的智慧電錶，英國的電力輸送配電方式與許多歐洲國家不同，因此要有自己的評估標準。英國一直在評估更廣泛的保證計畫的實施方式，包括電信，人員在內，公司在內，所有這些問題都經過了很長時間的評估討論，但該討論尚未完成。

來自西班牙驗證公司的 MIGUEL BAÑON 則說標準需要時間和資源來開發，驗證公司的實驗室不可能擁有無限資源，因此需要最小化驗證服務所需的資源。自我評估是講者非常關心的事情，可以減少驗證過程所需成本，但自我評估需要擁有足夠的透明度和足夠的細節，自我評估才有意義。若沒有足夠的透明度來建立信任關係，就必須擁有獨立的第三方驗證。講者認為所謂輕量級的認證，應理解為完全面向用戶，而不是硬性定義輕量級標準文件頁數少於 600 頁，講者認為即使標準閱讀起來很多頁數，但是用戶讀起來輕鬆、體驗良好，這樣就無所謂。驗證的一切都與資源有關，就時間成本和驗證項目而言，當談論多少評估成本以及持續多長時間時，

需要很謹慎，雖然驗證公司可能自認為花費不少時間，但開發商可能要花更多時間去解釋疑點與解決問題。

(三)展望下一代行業保障（Looking Ahead to the Next Generation of Industry Assurance）

在此段議題討論，主持人首先提到下一世代的產業保障的議題，也就是在面對快速變遷的產業下，要如何保障包含水平和垂直產品應用的議題，這個議題在兩天的研討會內容中亦有相當多的討論，例如如何縮短但是又有效的提供相關產品認證，或是如何透過開發商自評以確保其產品之資通安全。來自美國 NIST 的與談人 Michael Cooper 提到，在美國亦有類似的狀況，尤其製造商會對政府施加壓力希望可以盡快完成對於加密措施的驗證流程，而針對類似要求，當局則是透過工作流程的自動化，以對應供應商之要求。

接下來討論議題為實作方法以及除了在歐洲推動外，亦逐漸將此做法推向全球市場。而在討論實作方法的過程中，與談人提到此方法需為好的、便宜的保障方案，此外亦須在自動化與工具使用上創新，並了解到什麼是好的做法，以及何種保障可稱之為好，亦即在了解到針對好的保障與好的時做方法的定義後，在思考如何達到快速與便宜，必須在確保達到一定的安全性後，在處理快速與便宜的做法。

在推動下一世代的保障方案時，來自 ENISA 的與談人 Slawomir Górniak 亦提到在依據歐盟的網路安全法案推動相關產業保障的認證時，亦須了解市場上的需求與造成之衝擊，例如針對物聯網相關的產品認證，如果認證的時程過長，亦會造成競爭力上的影響，進而變成推遲相關認證的藉口，相關單位也須了解市場上的聲音，以免曲高和寡。

針對上述對於保障方案以及產品資通安全認證的議題，來自IBM 的 Jonathan Sage 則提到一重要概念，在認證產品的安全性時，應該要再進一步思考產品的開發流程，確保再開發的過程當中，相關的開發流程符合資通安全的規範，與談人亦舉例說明現行的 IoT 裝置多與雲端服務連結，但如果雲端服務的安全性無法得到保障，即使 IoT 的裝置是安全的，但也無法保障整體的 IoT 系統為安全可用的。另外與談人亦提到一重要概念，產品上市得到認證後，如果有相關資通安全議題或漏洞，在進行更新並發布新的韌體後，認證是否為有效，而此議題的建議方向則回歸到如果產品的開發與後續更新發佈的流程是通過資通安全相關認證，且開發商或製造商應該盡可能根據風險作出適當的控制措施，藉此取得顧客對產品的信任。

藉由上述議題的探討，主持人將討論引入此次研討會的重要議題之一，亦即目前歐模的 Common Criteria 共有 28 個會員國，會員國之間相互承認通過 Common Criteria 驗證的證書，但今年歐盟通過的網路安全法案中訂定網路安全框架，亦是讓歐盟對 IT 產品有一至性的安全驗證體系與機制，但這也造成 Common Criteria 和網路安全框架融合之議題，尤其資通訊技術與相關產品在資通安全認證標準在在全球市場上的相互承認涉及各國國家利益，一直以來都是一個複雜待解的問題。但以與談人分享的看法與經驗，縱整來說，Common Criteria 與網路安全框架逐漸融合是勢在必行的趨勢，而在融合的過程中會盡可能以較平穩的方式逐漸走向網路安全框架的認驗證體系，以逐步達到在此框架下的各種驗證邊準可以相互認可。

三、 專題報告

(一)公共政策（Public policy）

1. Update on ENISA Operations and CSA Implementation：本場專題報告首先由 ENISA 資安專家 Slawomir Górniak 以「歐盟資通安全框架-ENISA 的角色」（The EU Cybersecurity Certification Framework- ENISA role）為題，為現場參與者更新網路安全法通過後，ENISA 的定位與職能，以及未來執行該法的規劃方向及首要處理的工作項目。

   A. 網路安全法通過後 ENISA 的定位：Górniak 指出，ENISA 的施政作為依性質可區分為提供專業建議、支援政策執行、與專業社群協力三部分。第一項為針對歐盟境內資通安全議題提出相關建議作為與獨立諮詢意見；其次則是協助歐盟成員國與執委會落實政策之執行與進行政策協調；最後 ENISA 也與歐洲境內各團體，包括非政府組織與企業就資安防護事項積極合作（如圖 5）。ENISA 的施政策略則可大致劃分為網路與資訊安全以及數位單一市場兩方面，其政策依據則來自於歐盟此前通過的諸多法律，如網路與資訊安全指令（NIS Directive）、電子身分認證與信賴服務規章（eIDAS Regulation）、支付服務指令（Payment Service Directive 2）、一般資料保護規則（GDPR）、網路安全法、隱私與電子通訊規章草案，整體施政則以強化歐洲網路系統韌性與培育具競爭力且創新的資安產業為目標（圖 6）。



圖 **5**：ENISA 施政作為之性質

資料來源：Slawomir Górniak 簡報

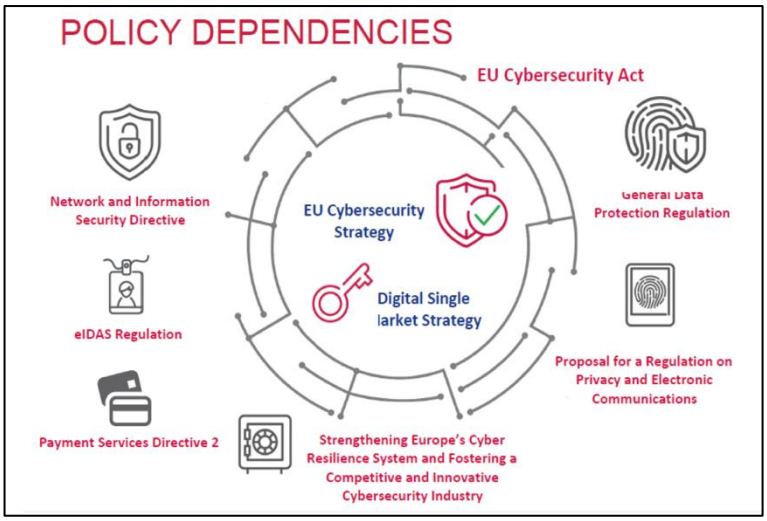


圖 **6**：ENISA 施政策略及政策依據

資料來源：Slawomir Górniak 簡報

B. 資通安全認證框架：背景、內容、產生程序 Górniak 接著介紹資通安全認證框架的產生背景。在網路安全法通過之前，歐盟境內存在數個彼此互不相容的國家型及區域型安全認證計畫，為協助這些安全認證計畫彼此協調，

歐盟執委會於 1992 年成立資訊系統安全資深官員小組（Senior Officials Group Information Systems Security, SOG-IS），以及於 1997 年簽訂 SOG-IS 相互承認協議（SOG-IS Mutual Recognition Agreement）做為各成員國與各安全認證計畫進行協調與產生資訊技術安全評估共同準則（Common Criteria for Information Technology Security Evaluation，簡稱「共同準則」、Common Criteria 或 CC）的合作架構。然而在歐盟建構數位單一市場的既定政策目標指導下，逐步建立一套符合各國需求的認證標準為各方努力方向，為加深歐盟各市場整合，執委會與 ENISA 在這方面的努力即是以網路安全法授權，建立資通安全認證框架，透過法定程序產出某一領域的資通安全驗證計畫[5]，其包括資訊安全要求項目以及檢視這些要求項目達成情形的方法。

資通安全認證框架整併既有的各類產品資安要求，改以三種安全保證層級做為統一的比較基準，並且抹平過往不同認證體系之間的不等比較基準而以一個橫跨全歐盟成員國的協調性框架做為往後認證之依據（如圖 7）。在制定程序上，依據網路安全法規定，產出一項歐盟層級的資通安全驗證計畫需經過四道程序：執委會確認優先發展領域，交由 ENISA 制定與提出候選認證方案，此候選方案經由執委會依立法程序完成採用，交由各成員國檢視及認可並由各成員國的一致性評估機構（conformity

[5] 依據網路安全法第 2 條第 8 款定義，歐盟資通安全驗證計畫（European cybersecurity certification scheme）為「在歐盟層級建立的一組包含法規、技術要求、標準及程序的規定，此組規定用於特定資通訊產品、資通訊服務或是資通訊流程之認證或是一致性評估」，同條第 9 款則定義「國家型資通安全驗證計畫」（national cybersecurity certification scheme），規定在前款產出的特定認證方案之範圍內，成員國之主管機關發展與採用的資通安全驗證計畫。

Assessment Bodies）製作及發放歐盟資通安全認證證書（如圖 8）。

C. 網路安全法成立後 ENISA 的任務與執委會的首件交辦：在網路安全法通過後，ENISA 不但成為歐盟永久性組織，在規模上亦有擴大，年度預算由 1,100 萬歐元增幅至 1,600 萬歐元，人員編制則從 80 人膨脹至 125 人，而依據網路安全法規定，ENISA 未來具體工作則包括：

- 起草及定稿最終候選認證方案。
- 擔任利害關係人資通安全認證工作團（Stakeholder Cybersecurity Certification Group, SCCG）秘書單位並與執委會共同主持 SCCG。
- 協助執委會主持歐洲資通安全認證工作團（European Cybersecurity Certification Group ECCG）。
- 協助檢視已採用的認證方案。
- 經營及維運資通安全認證框架網站。
- 協助各國資通安全認證主管機關彼此之間的同儕檢視。
- 提供關於資通安全認證市場方面的諮詢。

在報告當天，Górniak 也表明執委會已在徵詢 ECCG 與 SCCG 意見後，建立首個聯盟滾動式工作項目（URWP），並交辦 ENISA 執行。此網路安全法的第一項工作為轉換現存 SOG-IS 成為首個資通安全驗證計畫，ENISA 亦於今年 11 月 27 日召開專家質詢工作小組（ad-hoc Working Group）會議進行討論。

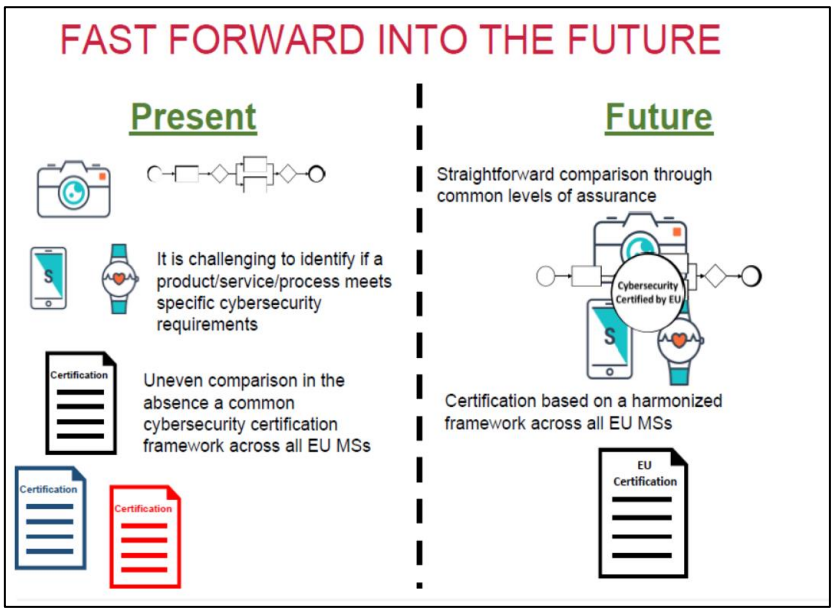


圖 7：資通安全認證框架示意圖

資料來源：Slawomir Górniak 簡報

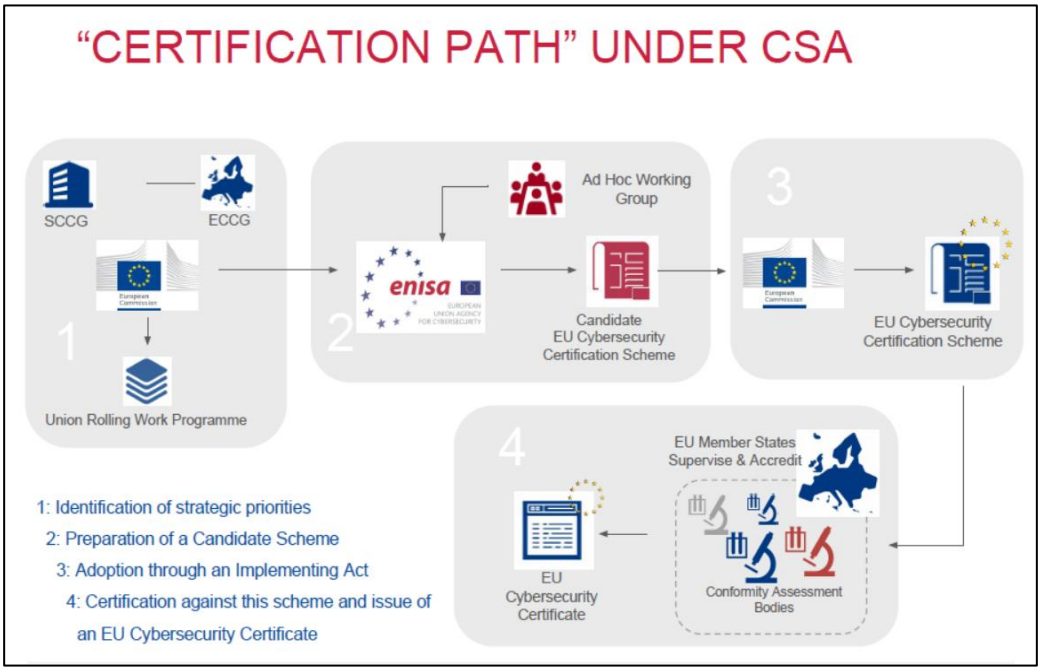


圖 8：歐盟資通安全驗證計畫產出程序示意圖

資料來源：Slawomir Górniak 簡報



圖 9：ENISA 資安專家 Slawomir Górniak

資料來源：出國報告人拍攝

2. European Cybersecurity Certification Framework, State of Play：緊接著 Slawomir Górniak 上臺報告的是歐盟執委會資深政策官員 Aristotelis Tzafalias，他以「歐盟資通安全認證框架之現狀」（European Cybersecurity Certification Framework, State of Play）為題，向與會者從執委會角度報告。

A. 歐盟資通安全認證框架：一種框架，多種方案：資通安全認證框架的設計目的在於結合綜合市場需求端及供給端，增加消費者或終端使用者對於數位產品與服務的信任，允許業者向其消費者顯示其產品及服務已充分符合公正第三方的安全檢驗，透過建立共同的資通安全認證途徑對於建立數位單一市場而言將是重要的一部分。不過執委會也認識到不存在可通用於各類產品的資安認證方案，因此資通安全認證框架要建立的其實是「一個框

架，多種方案」（One Framework, many schemes）的架構，納入各類資通訊產品服務或流程的特定資安要求及評估方式，佐以開放、包容與公開的治理過程，藉重構歐盟目前協作方式並藉由各成員國彼此的同儕檢視建立信任。資通安全認證框架於設計時也將現代社會軟硬體開發的動態過程納入考量，亦即認證框架的內容包括產品生命週期的概念，因此針對諸如資安管理建立、漏洞處理與街路、更新條款的內容皆有相應的認證要求。此外，認證框架對一般使用者而言有具備諸多附加價值，諸如提供資通安全認證與使用指引、網路威脅的減輕措施、聯資安研究人員的聯繫資訊等。

B. 安全保證層級與一致性評估之概述：Tzafalias 簡報第二部分內容則較為細緻的介紹歐盟資通安全認證框架的安全保證層級與一致性評估內容。安全保證層級分為基本、實質、高級，在運作機制上，可分為基本與實質保證層級以及高層級兩個部分。當一項特定產品/服務/流程的歐盟認證方案制定後，各成員國會有國家資通安全驗證主管機關、一致性評估機構、國家認證機構（National Accreditation Body）三種負責不同職能的角色。基本與實質安全保證層級由各國的一致性評估機構依據歐盟認證方案之內容針對產品進行評估及驗證一致性，完成驗證程序後則提交執委會針對各國一致性評估機構發放之證書進行承認；不過高級的安全保證，則需由國家資通安全驗證主管機關針對產品進行評估及驗證一致性，完成後再提交歐盟承認驗證結果（詳參圖 10、11）。

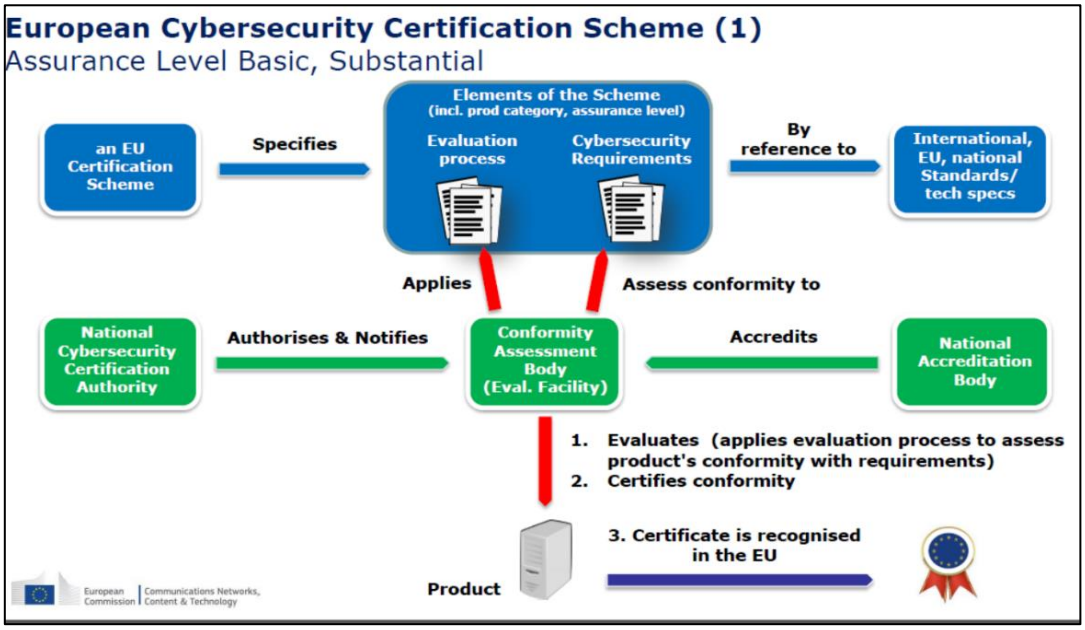


圖 **10**：基本與實質安全保證之運作機制

資料來源：Aristotelis Tzafalias 簡報

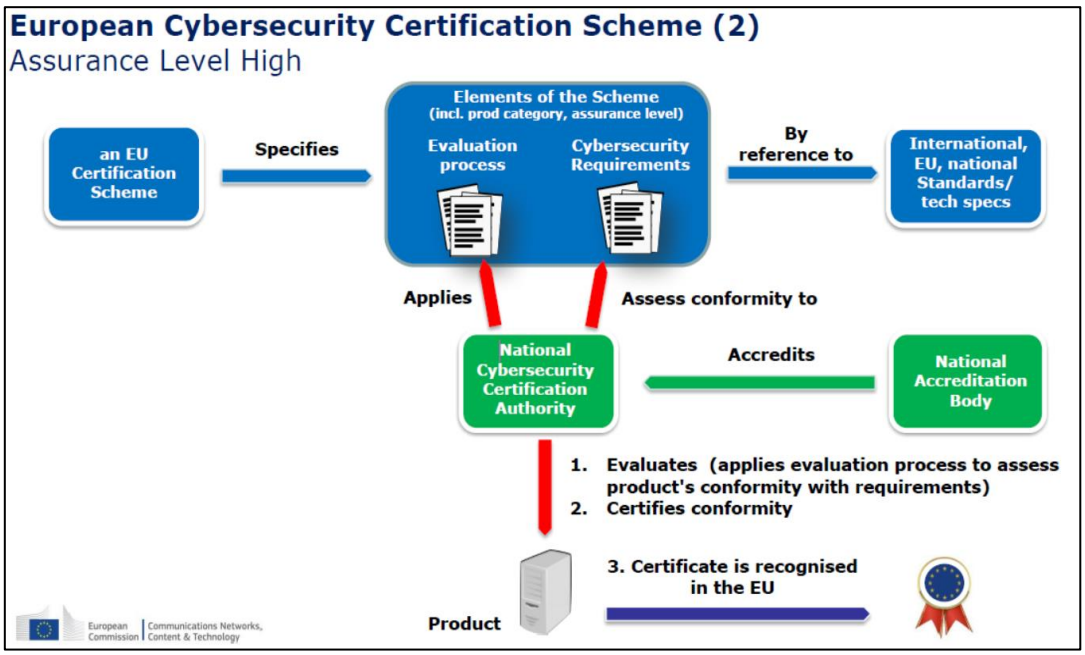


圖 **11**：高級安全保證之運作機制

資料來源：Aristotelis Tzafalias 簡報

C. 資通安全認證框架的現狀及後續討論事項：報告的最後一部分則為截至今年 11 月 18 日時，執委會於落實網路安全法的最新進度，包括自 6 月 27 日開始施行以來，

ECCG 已建立並召開了兩次會議，執委會也交辦 ENISA 預先準備關於建立共同準則基本方案的相關事項，SCCG 之諮詢也在 9 月 17 日結束，執委會將持續準備歐盟資通安全驗證的聯盟滾動式工作項目。而 Tzafalias 也點出依據網路安全法規定，後續制定歐盟資通安全驗證計畫時將，各界可能關注之議題諸如，那些產品/服務/流程將由執委會獲選為優先建立資安認證方案之對象，或是如何評量自願性認證之有效性，或業者提供資通訊產品/服務/流程的補充性資安資訊應包含何種內容等等，而執委會針對前述這些問題將綜合考量政策、法規、市場需求、新興威脅等因素制定資安認證方案。



圖 12：執委會官員 Aristotelis Tzafalias

資料來源：出國報告人拍攝

3. ECSO's Outlook on the EU Cybersecurity Act：第三位報告人為歐洲網路資訊安全組織（European Cyber Security Organisation, ECSO）執行秘書 Roberto Cascella，他的報告內容分為三部分，第一部分介紹 ECSO 組織本身，第二部分則講述該組織主責標準制定、驗證、供應鍊管理的第一工作小組之重點工作內容，第三部分為該組織當前重點工作之一，

制定「可組合性/可合成性文件」（composability document）的工作進度報告。

A. ECSO：歐盟執委會在資安領域的公私協力夥伴：歐洲網路資訊安全組織（ECSO）為一於比利時註冊成立的非營利組織，該組織於 2016 年 6 月成立。歐盟執委會透過地平線 2020（Horizon 2020）計畫，挹注資金於 10 項科技領域發展技術以解決社會問題，為有效運用資金，執委會於此 10 項領域中擇取 1～2 名非營利或非政府組織做為契約型公私協力夥伴（contractual Public-Private Partnership, cPPPs）[6]，協助執委會執行地平線 2020 計畫，ECSO 即是執委會在資通安全領域的合作對象。ECSO 目前擁有超過 260 家的產業組織會員，涵蓋歐洲 29 個國家，2000 名以上技術專家分為 6 個工作小組進行資通安全的各類工作（如圖 13），此 6 個工作小組分別：驗證、標準化小組（WG1）、市場、投資及國際合作小組（WG2）、垂直產業小組（WG3）、支援中小企業及區域小組（WG4）、教育訓練及資安意識培育小組（WG5）、研究與創新小組（WG6）。

[6] 此 10 項 cPPPs 領域分別是：未來工廠（Factories of the Future）、節能建築（Energy-efficient Buildings）、歐洲綠能車輛計畫（European Green Vehicles Initiative）、可持續性製造產業（Sustainable Process Industry）、光子學（Photonics）、機器人學（Robotics）、高效能運算（High Performance Computing）、未來網際網路的先進 5G 通訊網路（Advanced 5G networks for the Future Internet）、資通安全（Cybersecurity）、巨量資料價值（Big Data Value），進一步資訊可參 https://ec.europa.eu/programmes/horizon2020/en/contractual-public-private-partnerships。

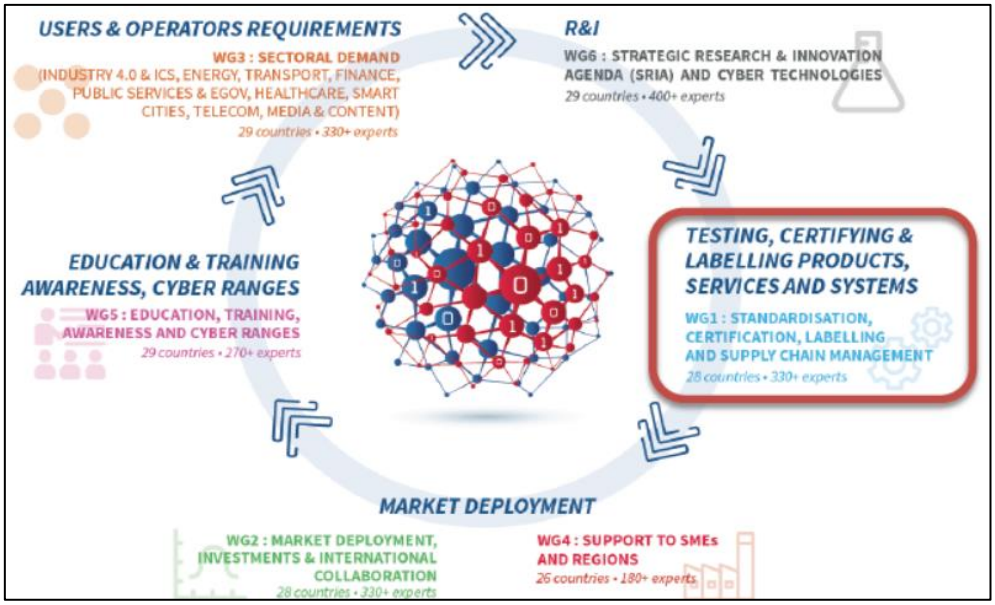


圖 **13**：ECSO 的 6 個工作小組

資料來源：Roberto Cascella 簡報

B. 第一工作小組（WG1）活動概述：WG1 負責資通安全驗證及標準化的相關工作，業務涉及提供執委會關於資通安全的政策及法制建議，比如在網路安全法之立法制定及建構歐盟資安認證框架的後設方法論上 ECSO 皆有著力，此外 WG1 也編撰及出版資通安全教學大綱（State of the Art Syllabus），內容包含當前與資通安全相關的所有技術標準（standards）及規範（specifications），以及這些標準規範的作者、發布日期（如圖 14）。

WG1 設定五項任務及目標：提供歐盟資通安全認證框架及優先項目的建議；協助制定支援資通安全驗證計畫的標準；提供產品內容、系統、服務的資安評估；針對歐洲境內的供應鏈/價值鏈提供測試及驗證；與歐盟各標準組織、機構合作，如在標準化事宜上與 ETSI、CEN/CENELEC 合作，在驗證事宜上與 ENISA 協力。WG1 則透過兩項執行策略完成前述目標，其一依據 CSA

制定與資通安全驗證計畫相關的可合成性/可組合性的方法、標準、驗證方式，其二則研究當前風險管理與專業驗證的需求及途徑。

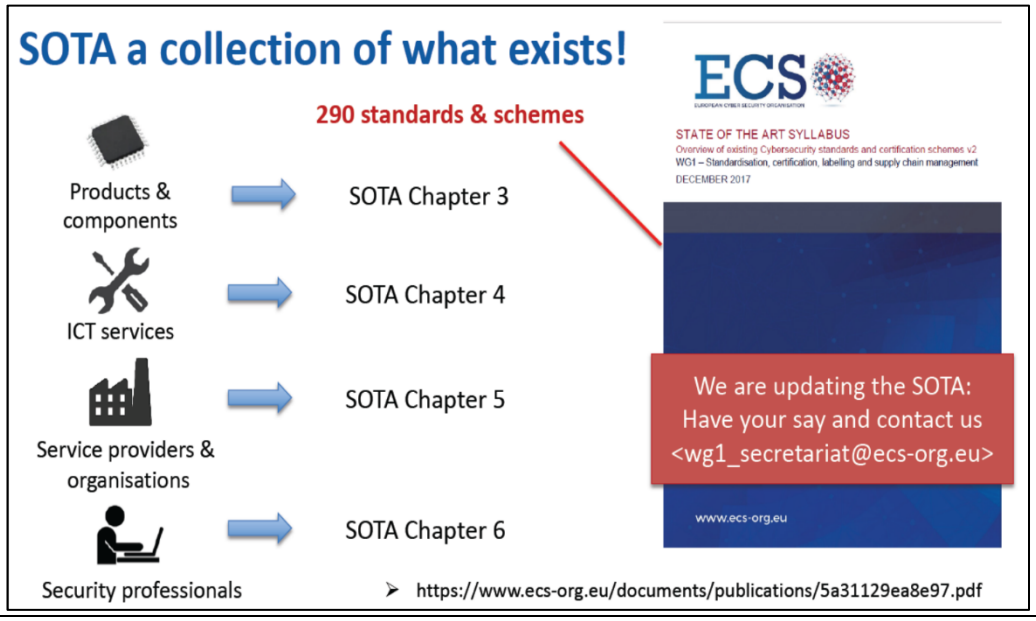


圖 **14**：ECSO WG1 編撰的資通安全教學大綱涉及內容

資料來源：Roberto Cascella 簡報

目前 WG1 正在進行中的工作重點包括三項：

- 撰寫可組合性/可合成性文件：WG1 正在起草第一版文件做為網路安全法後續討論資通安全驗證計畫制定時的基礎；
- 更新教學大綱：WG1 將把網路安全法之法規內容及涉及資通訊標準納入
- 盤點挑戰及優先事項：WG1 將依據未來工作及投資方向盤點可能的挑戰與資源優先挹注項目。

C. 資通安全驗證計畫的可合成性/可組合性：Roberto Cascella 報告的第三部分則是關於「可組合性/可合成性文件」（composability document）之制定的工作進度。此項工作的目標是建議未來的資通訊認證方案之內容應具

備可組合性/可合成性，此將為認證方案提供四項益處，包括驗證與評估證據可重複使用；可降低驗證成本與改善整體文件處理速度；能縮短產品進入市場的時間；在各應用領域可以客製化水平元件（如圖 15）。

至於方案的組合可分為同一認證方案內（標準模式）與跨認證方案兩種類型。前者指的是在同一認證方案內，將評估標準的部分內容重複用於新的評估；後者則是在不同認證方案之間，將評估標準的部分內容重複用於新的評估。進一步說明如下：

- 同認證方案的組合（標準模式）：一項產品內部由不同供應商（different suppliers）提供的不同構成區塊（different building blocks）基於同樣的方法論各自進行驗證。最終此項產品整體將基於同樣的方法論進行驗證，並且將重複使用不同構成區塊內部的驗證。此模式重點在於專注整合及正確使用驗證功能。
- 跨認證方案的組合：一項產品內部的不同構成區塊各自基於不同方法論進行驗證。最終此項產品整體將基於某各方法論進行驗證，此模式需注意的重點是，要仔細定義實現可組合性的規則（rules for achieving composability）。

Cascella 指出未來要推行資通安全驗證計畫的組合/合成，需要考慮三點：第一點是認證方案需要仔細定義哪一類與驗證相關的評估證據（以及評估層級層級）能夠用於組合性評估；第二點則是組合後的認證方案需要定義任何額外的評估標準（additional assessment criteria），

藉以涵蓋引入組合後可能產生的驗證盲點；第三點則是在最終產品裡始終需要將驗證功能的正確執行納入考量。

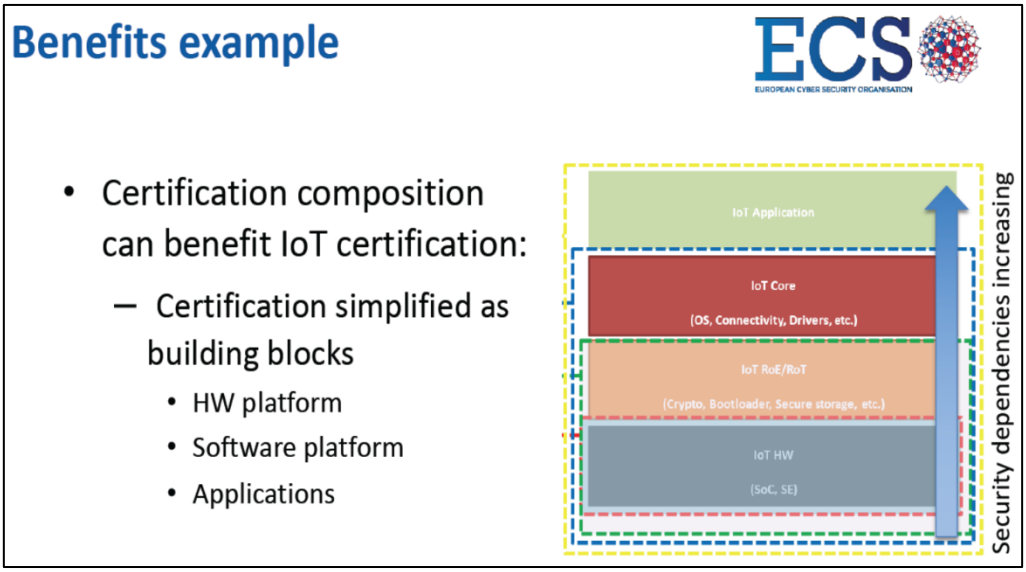


圖 **15**：ECSO 建議認證方案進行可組合化帶來的效益範例

資料來源：Roberto Cascella 簡報



圖 16：Roberto Cascella

資料來源：出國報告人拍攝

4. Security Needs to be Consistent—The Role of Process in the Cybersecurity Act：第四位報告人為英國國家資通安全中心（National Cyber Security Centre, NCSG）國際安全處的主管 David Martin，他針對網路安全法裡面的一些關鍵概念如資通安全（cybersecurity）、安全保證（assurance）、流程（process）、層級（levels）進行分析，並指出這些概念內涵的不一致以及對後續實務的影響。底下即分就前述概念摘錄 David Martin 之評論：

- 資通安全（cybersecurity）：資通安全不僅僅是一個防護盒（boxes）或防護平臺（platforms），從事資通安全工作時具備整體性/系統性/生命週期的思考是極端重要的特質，此外在制定資通安全標準及驗證方法時，軟硬體的開發、支援、

作業流程也都是重要的考量因素。就此而言，CSA 確實提供一個架構促使各類資通安全驗證計畫將產品、流程與服務的驗證皆納入考量。

- 安全保證（assurance）：Martin 以安裝防火牆不會更安全為例來說明安全保證的概念，他說明以前英國諸多資安專家都會建議應將防火牆安裝等級至少通過資通安全認證共同準則（CC）的第 4 級安全保證（EAL 4）及以上，不過這類建議卻輕忽許多方面，例如許多第 4 級安全評估缺乏內在的安全保證，或是攻擊者不一定會從正面攻擊等等。此外，NCSG 幾年前也有相關統計指出，取得產品驗證證書對於產品安全本身只有很小的益處。因此目前 NCSG 普遍觀點是，當一個產品要能合理的運作，產品如何設計、開發與維運才是最重要的安全考量。
- 流程（process）：CSA 將資通安全概念擴展至過程，這並非首創之舉，至少歐盟其他國家在此前已有類似概念，比如英國數位文化媒體運動部（DCMS）於 2019 年 2 月時發布「給製造業的消費者物聯網實踐準則」（Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers）就強調安全設計（Secure by Design）或是德國聯邦資訊安全辦公室（BSI）2018 年 11 月發布「關於連網醫療裝置的資安要求」（Cyber Security Requirements for Network-Connected Medical Devices）。因此隨著網路安全法的施行，接下來一個重要問題即是該如何「評估過程」（assess processes）？Martin 認為要做到這件事在實務上會是相當困難的一件事，而且進一步來說還可能牽涉到智財權的議題。

- 層級（levels）：網路安全法設定安全保證層級，分為基本、實質、高級，不過在該法 51 條 i 款規定「資通訊產品、資通訊服務、資通訊流程皆應屬安全預設及安全設計」，所有層級皆須符合此規定，也因此難以辨別三種層級之間的差異性。即使此三種層級之區分指涉過程驗證的形式，也會遭遇一些問題，比如現存的某些流程如能力成熟度模型（Capability Maturity Model, CMM）即是基於層級概念運作，因此安全保證層級可能無必要；或實務上難以運作，因為層級概念對於開發共同準則驗證沒有助益。



圖 17：David Martin（站立者）

資料來源：出國報告人拍攝

(二)行業調整（Industry Alignment）

1. ETSI Security Evaluation Standardization Initiatives

此議題主要由 ETSI 的技術長 Sonia Compans 講述有關 ETSI 在資通安全倡議的參與成果，包含信託服務、5G 網路、消費者 IoT 安全等領域。

在信托服務主要是在講述對於電子識別與信託服務的認證與相互授權，例如歐盟會員國的學生可以線上註冊歐盟會員國的大學、公民可跨境在國外填寫報稅或是企業可以參與會員國的公開招標，亦即作為數位市場的第一步，應該有一大家共同信任的電子識別。此次 ETSI 主要在推動歐盟的信託服務的相互認證，並根據 ETSI 的標準來強化電子識別之信託服務的整合。

ETSI 在 5G 網路安全的部分提出 Network Equipment Security Assurance Scheme (NESAS)，係針對網路設備訂定安全保證方法，改方法起源於 GSMA 與 3GPP 共同定義行動網路設備的安全保證方法，該方法主要精神在於透過評估檢測網路設備以了解網路設備是否有達到安全基準，此外亦會評估設備製造商的設計、生產等過程是否符合安全要求以及是否依照相關標準指引開發，也就是會從設備本身以及製造商等兩方面進行評估，以確保資通安全。

根據 Gartner 的預測，在 2020 年全世界將會有突破 129 億臺消費型裝置，然而大多數的裝置並沒有完善的資通安全防護，也因此 ETSI 在消費者 IoT 安全認證領域推動 TS 103 645 的標準，此標準為全球第一個物聯網產品相關的通用標準，此標準亦向 GDPR 對齊。此標準並非一次解決或消除消費者在 IoT 產

品中的所有風險與一路，而是以結果導向的方式透過各種安全控制的手段來降低資通安全風險，其主要要求包含：無通用預設密碼、資安漏洞通報管理方法、軟體持續更新、資料保存安全、安全傳輸、減少可被攻擊的面向、軟體完整性的確保、個資確實保護、系統強韌性、遠端感測數值監控、消費者個資刪除、簡化設備安裝與維護、驗證輸入數據等。

綜觀上述 5G 網路與 IoT 資通安全評估方法，可知資通安全除了設備本身，包含上下游供應鏈之生態系管理、系統強韌性規劃等都是重要課題，亦為資通安全維護計畫的重點項目之一，足見我國通傳會在 5G 與資通安全上的努力並與國際接軌。

2. Lessons Learnt in the Commercial Use of Security Certification—From Setting Standards to an Innovator's Perspective

在此主題中，講者主要在分享現行的資通安全認證框架用在商業大型市場產品的經驗。首先講者提到 Trusted Computing Group (TCG) 為非營利組織，主要在開發、定義與推動開放、中立、全球產業規格與標準、支援以硬體為基礎的信任根基（Root of Trust）、具互通性的信任運算平臺（Trusted Computing Platform），而 TCG 其主要技術在於信任平臺模組（Trusted Platform Module）、信任網路通訊（Trusted Network Communications）以及網路安全與自我加密儲存裝置，並針對上述技術提供相對應之認證。

在信任運算架構中，TCG 發明信任根基的儲存、回報與量測，並設計一句信任根基的更新方式以強化韌體安全，亦發明句信任根基的偵測與復原技術以設計具強韌性之硬體，而在相關技術的認證也日形重要。供應商可透或資通安全評估以增

進終端使用者的信任，而另一重點則為中終端使用者的教育，因為資通安全除了產品本身，使用者亦為另一重要關鍵。在進行認驗證時，應採用國際標準，而與國際驗證標準接軌則為驗證方法至關重要的一部分。然而目前的方法針對大型市場除了昂貴也過於緩慢，無法跟上威脅進化的腳步，此項認驗證議題應該針對快速變遷的時代而改進。在 IoT 時代亦帶來更多挑戰，更多的運算裝置融入日常生活、也有更多的資料收集並在網路邊緣進行運算，也引此帶來更多的威脅與風險。

為了降低風險或避免威脅帶來的衝擊，應該鼓勵廠商在設計開發階段採用自願性的資通安全認證方法，並針對認證進行分級，例如自我宣告、基本的第三方認證到更進階的第三方認證，透過認證讓資通安全融入開發流程，從源頭即開始注重資通安全。

3. Vendor Self-Assessment—The Good, The Bad, and the Ugly

在歐盟資通安全法案中，允許製造商或供應商針對 ICT 產品、服務或流程進行自我評估，講者主要在會議中分享自我評估的可行性以及其限制。而大家最關心的議題之一為自我評估是否真的可行？講者提到在有些時候是可行的，而在產品、服務及流程三者當中，又以服務與流程會有較佳的效果，主要是因為其在資通安全的保證要求較低，而產品的資通安全要求通常較高，也因此即使對於安通安全保證要求為低時，仍有適用上的限制。從風險承擔者的角度來看，產品、服務及流程的風險承擔者也不同，服務與流程的承擔者為服務提供商，而提供商有動機會將事情做對、做好，但產品的風險承擔者為使用者而不是開發者。

對於服務、流程等供應商，把事情做對做好可以避免潛在的資通安全問題，對於各種變更的調適以強化資通安全也相對容易，而供應商應付各種變更與調適之責任，對於自我評估到發現事項可立刻回饋到資通安全管控措施，故供應商有強烈動機來執行自果評估。

對於產品開發者來說，自我評估亦有相當好處，由於開發者是最了且其產品的人，尤其相較於第三方有更深入的相關知識，也較其他評估人員沒有學習曲線的困難，在評估時可取得所有所需之資訊，倘若能由開發者進行自我評估，應該最好的選擇。然而實際上，在大多數的狀況下，資通安全並非產品開發的第一要務，尤其自我評估的時間和成本通常不在產品開發的預算之內，故自我評估的發現事項通常會被忽略。除了上述議題外，倘若自我評估的結果為負面或不如預期時，常會陷入天人交戰的情況。

上述內容亦反映出國內相關 ICT 產品的開發現況，除非是有法令法規或是合約要求，通常資通安全並不會是產品開發的第一優先順位，主管機關宜考量在對產品開發者衝擊最小的情況下，適度的要求產品的資通安全自我評估與相關監理或稽核工作。

4. ISCI WG (International Smartcard Initiative) Who Are We? What Do We Do? How Do We Do It? And How Do We Contribute to The EU Cyber Act?

此主題主要在介紹 ISCI WG1 與相關工作，ISCI 全名為 International Security Certification Initiative，其主要工作項目之一為支援 Common Criteria 在資通訊領域包含軟硬體的安全認

證相關詮釋，並讓 Common Criteria 較容易理解與應用以確保相關認證是最佳化的、清楚的及簡明的。

另一主要工作項目為達到在 SOG-IS（Senior Officials Group Information systems Security）中的 17 個成員國對於認證產品評估結果間的相互信任與承認，並定義、支援及推動一通用框架適用於 Common Criteria 的資通安全評估與認證方法，並納入所有評估與認證流程中的角色以強化與調和各國之評估流程並產上一致的節果。

藉由此工作小組的工作說明，可知歐盟逐漸開始朝向相互融合各會員國的資通安全瓶估與認證結果，嘗試打開各國避壘保護措施，但其中牽涉各國產業資深利益與發展，推動時需大量時間溝通與合作，才能逐漸建立各國評估與認證結果之信任。

5. Update on The EU Cybersecurity Act: Is The Feared Balkanization of Common Criteria Being Reversed?

此主題主要在探討 Common Criteria 的巴爾幹化以及 EU Cybersecurity Act 能否反轉巴爾幹化並讓歐盟會員國對於資通安全評估有一致的參考框架，並讓會員國之間能相互信任其評估與認證結果。

由於在 EU Cybersecurity Act 授權 ENISA 成為歐盟永久機構，以強化 ENISA 之地位與權力，建立一個歐洲 ICT 產品資通安全驗證框架（即 Cyber Security Framework），其主要目的在於強化歐盟內在提供網路彈性及應變能力，調和各標準間之相容性，以達成符合歐盟數位單一市場之目標。ENISA 將協助發展受各成員國承認之自願性歐盟認證框架，以確保 ICT 產品與服務在資安方面是安全無虞的，而該認證框架包含相關技術

性要求、標準及程序等內容，但亦可能帶來下列影響：安全設計原則將資通安全應用在產品設計及開發的最初階段，而在 ICT 產品、服務及流程的初始設定時，便讓設定達到簡單、值得信賴與安全，消費者不需具備相關知識或技術原理即能輕易使用，即預設安全。

6. The Certification Landscape and What Industry Needs

在未來的智慧城市，所有的基礎建設與智慧交通運輸包含自駕車、網際網路與通訊系統、油水電與安全系統會全部連結起來。而講者提到一個概念，也就是針對各種裝置、系統，在佈建後我們仍需維持其資通安全，尤其是當一個裝置或系統連上網路後，要假設其是脆弱的，而事實上我們有相當多的個人、財務資料可用來直接攻擊，或是收集相關更有價值的資訊來發動更大規模的攻擊。

針對上述的問題，解決方法則是增加更多的安全防護措施，針對裝置部署後的資通安全維護做為，應包含定期更新韌體與軟體、檢查裝置是否有實體入侵的可能性、預設開啟資料加密、當裝置不用時關閉、考量利用區塊鏈來強化資通安全。

針對認證的部分，應考量兩個面向包含裝置測試與流程認證。透過裝置測試可以找出慘品的脆弱性，且要確保每建立一個新的產品會進行測試，並考量實地稽核或測試的可能性，但須注意其測試僅針對該裝置而不是整個應用系統或情境，亦要注意避測試之裝置。而在流程認證則可以瞭解到公司的整體資通安全政策與規劃，該認證亦可適用於所有產品的流程，但僅針對流程而不是產品測試，而如果廠商惡意欺瞞將不容易發現。

由上述可知，國內通常著重於資訊安全管理面亦即流程面的認驗證，但對於實際用到的裝置卻少有安全測試，故對於未來 5G 與 IoT 時代的來臨，對於相關監理措施宜考量有更積極作為，以同時掌握管理面與裝置面。

(三)成功標準（Standards for Success）

1. CEN-CENELEC JTC13 WG3 Security Evaluation Standardization Initiatives

JTC13 WG3 於此次 EU Cybersecurity Act 會議中，提出一 ICT 產品之資通安全評估方法概念性框架。該框架之概念主要起源於 2019 年歐盟之網路安全法案強調需對所有 ICT 產品進行資通安全評估，而在該法案中將安全保證分為三等級，分別為 high、substantial、basic 等三個等級，也因此產生需對於不同資通安全驗證標準相互融合之需求。

在此會議主題中，點出多數歐盟成員國之需求，亦即需要一簡單也易於使用之資通安全評估標準框架，除了作為歐洲國家認可且有效之評估方法框架，也可輕易調和並對齊不同資通安全評估方法，以達到互通性。此外，透過推廣與部署該評估框架，可讓設備製造商取得資通安全認證與競爭優勢，也能以此贏得使用者與顧客的信任。

在此次提出的概念中，驗證單位可依據實際需求選擇適當的評估方法，並依照選定之方法其相關要求進性驗正，而該框架也提供足夠的彈性已針對不同需求、技術、市場、使用情境等建立評估與驗證方法。目前該框架預計會有下列利害關係人，包含：

產業界：主要會受惠於單一資通安全評估/認證框架，包含於產品在適當的認證成本下保有一定的安全水準。

政府單位：可推動採購具有資通安全認證之產品。

消費者：對於 ICT 產品有更高的信心

非政府組織：對於產品的資通安全能力有更佳的透明度

綜觀歐洲對於資通安全認證已進入到透過一框架以嘗試融合不同評估方法，並提供彈性之作法，臺灣目前常見之資通安全認證仍以管理系統面之 ISO 27001 為主，對於 ICT 產品除銷往歐美外，鮮少有主動通過資通安全評估之認證，藉由歐盟之積極作為，國內宜開始思考建立資通安全評估之框架之可行性。

2. Comparing National Lightweight Methodologies around Europe

此議題主要在說明比較歐洲輕量級的資通安全認證，以了解目前輕量級評估方法趨勢以其未來相互調和之可行性。因目前歐洲常見採用 Common Criteria 進行 ICT 產品的資通安全評估，其優點是包含產品測試、生命週期、產品文件等多面的評估，亦適用於各種不同配別的產品，也因具有不同保證級別而有相當彈性，並盛行於國際間，但 Common Criteria 因其評估時間過長、對於產品驗證過程中過高的花費、過於嚴格的驗證過程、大量時間花費在撰寫文件，其驗證過程亦對於中小企業難以負荷。也因此萌生出輕量級認驗證方法的可能性。

考量產品從設計、開發、生產到銷售所需之時間，且在實務上產品會不斷變更演進，而取得認證卻需花費相當時間，亦有可能在取得認證前產品就已經停止銷售，故在認驗證應有調整之必要性。然而輕量級的認證並非萬能解要，且輕量級的認

驗證僅有部分或僅針對某些功能，而挑選認驗證項目亦須具相關經驗的評估人員以及相當的技術背景，故採用輕量級的認驗證亦有相當風險。

歐美針對 Common Criteria 的議題亦有各自不同的看法，美國試圖建立一評估方法將 Common Criteria 視為一合規工具並將其盡可能的自動化與可重複使用，但在該評估方法中省略掉滲透測試與弱點分析的過程，可能會降低資通安全保證的深度，但可考量應用在沒有已知弱點的大型供應商。而在歐洲的看法會考量採用情境分析的做法並區分為需高度保證與與低度保證的情境，在高度保證的情境中，會採用傳統的 Common Criteria 的做法來建立標準並盡可能地重複使用與維持軟體變更後的相關認證；低度保證的情境會建立敏捷的產品評估與認證標準，並在限制條件下執行弱點分析與滲透測試。

目前在歐洲輕量級的認證已有實際執行案例，歐洲國家也開始累積相關執行經驗，雖然大部分應用在國家行政部門，但亦可應用至消費者市場，未來各國之間的認證也可能相互調和，但如採行輕量級認證需注意對製造商產生之衝擊，為因應各國不同之輕量級認證，可能會產生則外支出與造成各國壁壘效應，故 JVC WG3 正在研擬一通用認證框架，以融合各國輕量級的產品認證。

3. Implementing and Maintaining a Cybersecurity Program—The Role of Standards

此議題主要在說明比較 FISMA、NIST、FedRamp 及其他相關資通安全評估標準與認證等各自特點，讓與會者了解 FISMA、NIST、FedRamp 之間之關聯。

美國於 2002 年頒布「聯邦資訊安全管理法（Federal Information Security Management Act，簡稱 FISMA）」，以立法的形式規範美國聯邦政府對資訊安全管理之要求，並進行 FISMA 相關實作計畫，以奠定並強化美國資訊安全管理措施。FISMA 中定義一框架以保護聯邦政府之資訊安全以預防來自天然與人為的威脅，其中 FISMA 框架適用於所有聯邦政府單位及其資料，並授權 NIST 發展相關資通安全標準與指引，而「預算管理局 (OMB)」之政策亦提到聯邦政府機構必須遵循 NIST 之指引。FISMA 主要內容涵蓋：1.資訊安全與國家安全之定義、2.聯邦政府各機關之責任、3.資訊安全之年度評估、4.NIST 於國家之定位與法律位階，並授權 NIST 開發資通安全標準。其中 FISMA 風險管理框架包含：資訊系統分類、控制措施之挑選、控制措施之實作、控制措施之評鑑、資訊系統之授權、安全狀態之監控，聯邦政府各部門須依照上述框架建立資通安全計畫並予以實作。

NIST 則是依據上述項目分別建立相關指引，在 NIST 800 一系列的指引對應到 FISMA 的風險管理框架，例如 SP 800-60 的資訊資產或系統分類、SP800-53 的控制措施挑選、SP 800-70 的控制措施實作、SP 800-53a 的控制措施評鑑、SP800-37 資訊系統授權、SP 800-37 與 SP 800-53a 對於安全狀態監控等，皆有完整的對應指引。此外，NIST 亦針對非聯邦機構之民間關鍵基礎設施提出 Cybersecurity Reference Framework，作為民間單位見告資通安全防護計畫之參考。

美國在歐巴馬政府時代，推出聯邦雲端運算安全標準：FedRAMP （一 Federal Risk and Authorization Management Program）以因應雲端運算世代的來臨，並提供雲端產品與服務

之安全評估、授權方式、持續監控之標準與方法。透過 FedRAMP 可讓聯邦政府了解雲端服務供應商對於資通安全防護的能力，亦為聯邦政府選擇供應商的標準之。

透過瞭解美國對於資通安全政策之規劃，可知我國對於資通安全政策亦走在正軌上，尤其通傳會在 5G 時代來臨時，對於各業者資通安全維護計畫之要求，並率先提出資通安全維護計畫參考框架，與國際接軌，為我國資通安全之發展上重要里程碑。

(四)雲端與 GDPR 框架（Cloud and GDPR Frameworks）

1. Toward the European Cloud Security Certification Scheme: The CSPCERT Final Public-Private Recommendation：本場專題演講為講述在網路安全法通過之歐盟資通安全認證框架的範圍中，關於未來可能產生的歐盟雲端資安驗證計畫（European Cloud Security Certification Scheme）之設計構想以及最終建議，整體簡報分由四位報告人依序簡報，這四位簡報人分別是德國經濟及能源部代表 Thomas Niessen、法國資訊安全署（ANSSI）代表 Aurelien Leteinturier、Google 代表 Saurabh Ghelani、ENISA 代表 Slawomir Gorniak，以及主持人 Cisco 代表 William Ochs（如圖 18），專題演講重點的摘錄如下。



圖 18：主持人 Cisco 代表 William Ochs（站立者）、左起為法國資訊安全署（ANSSI）代表 Aurelien Leteinturier、Google 代表 Saurabh Ghelani、德國經濟及能源部代表 Thomas Niessen、ENISA 代表 Slawomir Gorniak

資料來源：出國報告人拍攝

A. CSPCERT 是什麼？CSPCERT 為歐洲雲端服務提供商驗證（European Cloud Service Provider Certification）工作小組之縮寫。此團體成立背景係基於歐盟單一市場之需求以及網路安全法建立歐盟資通安全認證框架，需要專家給予歐盟官方組織如 ENISA、執委會及各成員國針對歐洲的雲端服務提供相關資通安全認證建議。CSPCERT 由 32 名成員創立，成員組成涵蓋政府、企業、非政府及非營利團體，目前組成部分除 32 家創始成員，另有 29 名觀察成員，在地理範圍上則涵蓋 52 名歐盟成員與 16 名非歐盟成員（圖 19）。

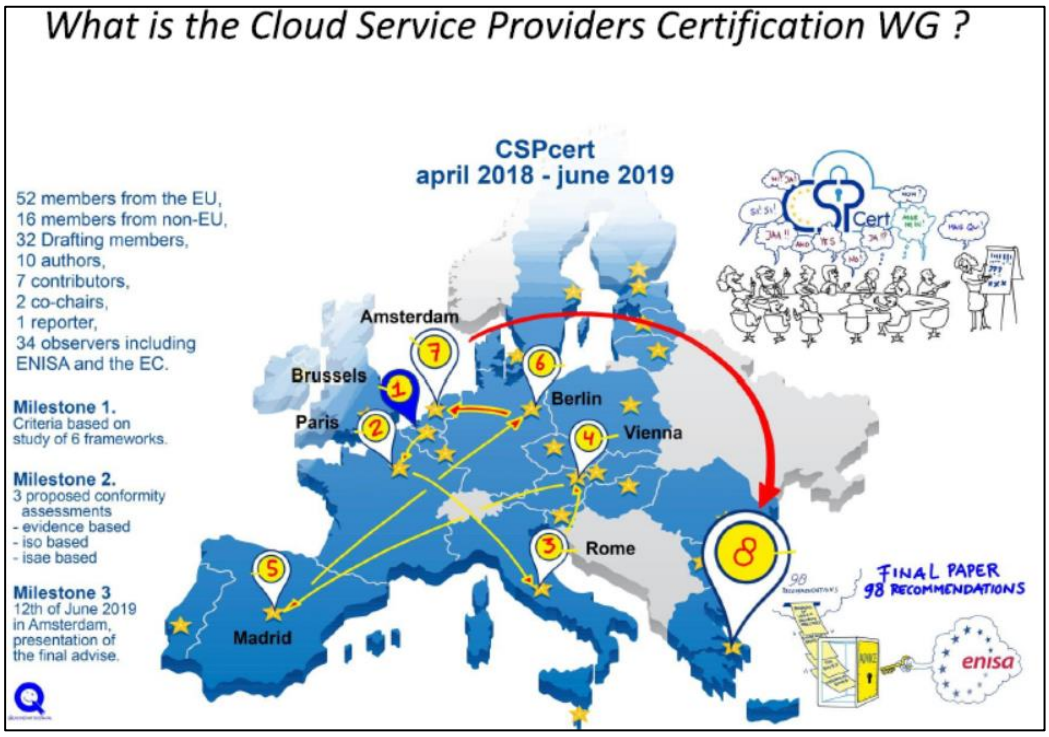


圖 19：CSPCERT 組成概況

資料來源：Thomas Niessen 等人簡報

CSPCERT 最終目標是提出一組驗證用工具包（certification toolkit）供各界參用，這組工具包則包含三階段目標（Milestone）及相關文件，其一是指明驗證對象（what to certify），具體工作則是將各種標準來源如 ISO、SecNumCloud 所設定的資安目標統合成為具廣泛性且和諧一致的一組驗證對象；其次則是說明評估與稽核的方法（how to evaluate and audit），具體內容則是綜合研究國際標準組織如 ISO、ISAE 之稽核方法並將其方法論協調一致，提出可用於雲端服務提供商認證（CSP certification）的方法論；其三則是闡明執行 CSP 驗證計畫的人員及方式（who and how to implement a CSP certification scheme），此部分內容則定義 CSP 驗證計畫的治理方案與指導原則，以協助日後歐盟 CSP 驗證計畫

之執行，目前 CSPCERT 已於今年 6 月發布目標三文件-「雲端服務提供商驗證計畫執行建議報告」（Recommendations for the implementation of the CSP Certification scheme）[7]。

B. CSPCERT 與 CSA 相關的部分：簡報第二部分則針對 CSPCERT 於 6 月時發布之文件進行內容之重點提示，報告人主要突顯此文件提出的三點一般性建議，分別是：

- CSPCERT 未向歐盟執委會與 ENISA 建議全新的驗證計畫，所提出建議主要基於當前產業界及國際採用之實踐準則、方案、標準，其相關內容亦直接扣合 CSA 之要求。
- CSPCERT 建議執委會應將適用全歐盟範圍的雲端安全驗證計畫之發展納入歐盟滾動式工作項目（URWP）
- CSPCERT 請求 ENISA 基於 CSPCERT 所提出之內容提出候選認證方案。

C. CSPCERT 的解決方案：報告人於第三部分簡要報告將來如雲端安全驗證計畫落實，對於雲端服務提供者（CSPs）、中小企業及客戶、主管機關三方有何影響。

首先對雲端服務提供者的影響是，CSPCERT 認為假如渠等建議雲端安全驗證計畫被納入歐盟資通安全認證架構的候選計畫，其將促成一致性的雲端安全認證要求出現，驅動泛歐盟體系承認此一實際上已使用的雲端安全

[7] 該份報告可於此處下載 https://drive.google.com/file/d/1J2NJt-mk2iF_ewhPNnhTywpo0zOVcY8J/view (last visit: Dec. 11, 2019).

認證；由於 CSPCERT 建議的雲端安全認證計畫精簡及強化現存的資通安全要求，因此預期將致使歐盟境內更多地區採用雲端服務；同時雲端安全認證計畫也為新興的未來法規及特定產業部門的資通安全要求提供制定基準，並且降低與多國認證框架相關的第三方稽核的組織成本。對中小企業及客戶的影響則是，雲端安全認證計畫提供標準化框架，此使其能定期對供應商進行盡職調查；由於協助組織簡化法遵優先事項，極大程度降低雲端服務提供者法遵的成本，因此將使更多企業於不同區域進行商業活動；而且此認證計畫由歐盟官方管理因而能提昇對於歐盟資通安全框架的信任度；此外由於預期採用雲端服務比率會提昇，因而也能推動中小企業進行數位轉型。至於對於各國主管機關的影響是，各國主管機關可利用 CSPCERT 的法遵事項滿足產業對於資通安全的特定要求；由於整個歐盟地區存在統一的做法，採用雲端安全認證計畫除可降低國家管理成本，也增強與其他國家主管機關的合作程度；主管機關也能藉由採用雲端安全認證計畫達成資通安全知識與最佳實踐方式之共享，並以此簡化相關資訊以向範圍更廣的行業傳播；採用雲端安全驗證可以視作促進企業進行數位轉型的方式。

2. The EU-SEC Framework：第二場報告則由雲端安全聯盟（Cloud Security Alliance）代表 Eleftherios Skoutaris 分享歐洲資通安全驗證框架計畫（European Security Certification Framework, The EU-SEC Framework Project）的執行情形。

A. EU-SEC Framework 概述：歐洲資通安全驗證框架計畫為一由歐盟資助的專案型計畫，其運作資金來自地平線 2020 計畫，計畫執行期程為期兩年，自 2017 年 1 月 1 日起至 2019 年 12 月 31 日止，計畫參與者共 9 名企業及非營利組織。此計畫成立背景源於當前歐盟資通安全市場存在過多的資通安全驗證方案、其驗證方式也缺乏明確性、各國接受之驗證亦不均等，致使資通訊產品驗證成本過高且缺乏效率。因此本計畫旨在創建可整合現有各類資通安全驗證方案的資通安全驗證框架，使當前的驗證及安全保證方法可以共存，進而提供雲端服務提供者（Cloud Service Providers, CSPs）有效率的雲端安全驗證，提供雲端服務客戶（Cloud Service Customers, CSCs）透明可控且具保證的服務，以及提供涉及各國稽核機構與競爭主管機關多方稽核服務（圖 20）。本計畫的具體產出則包含三項措施：多方互相承認框架（Multiparty Recognition Framework, MPRF）、基於持續性稽核的驗證（Continuous Auditing-based Certification, CABC）、符合 GDPR 規定的隱私行為準則（Privacy Code of Conduct for GDPR compliance, PLA CoC），三者中關於隱私行為準則因非屬本次研討會討論議題，故未做介紹，底下分就 MPRF 和 CABC 簡述報告內容。

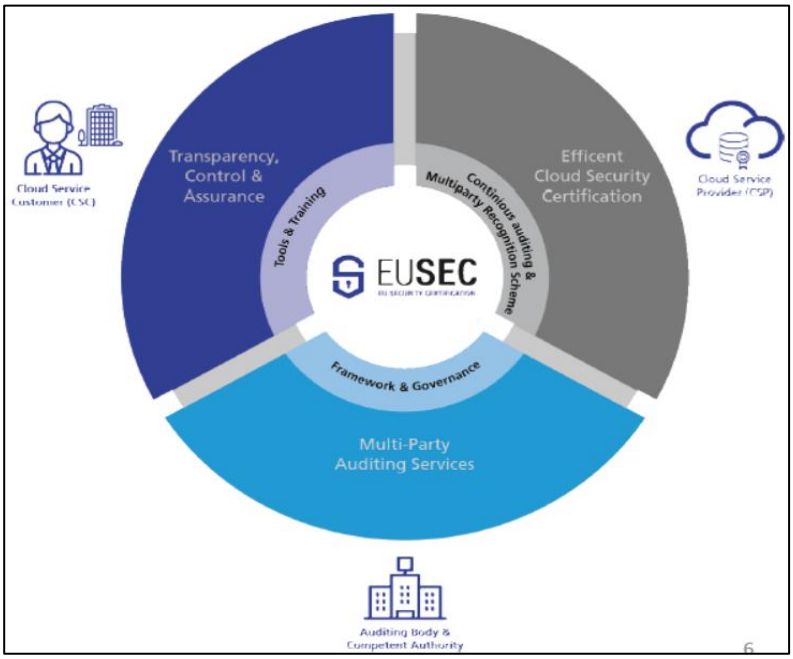


圖 20：EUSEC 計畫架構示意圖

資料來源：Eleftherios Skoutaris 簡報

B. 多方互相承認框架：多方互相承認框架（MPRF）的執行目標有三點：其一，極小化驗證取得負擔，此係指當雲端服務提供者已經取得 X 型驗證時，再行取得相關的 Y 型驗證，其取得成本、程序之花費應降至最低；其二，協助雲端服務提供者/雲端服務客戶正確理解各類方案中關於資安、隱私、稽核要求的文義；其三，簡化雲端驗證過程以提昇效率、增加安全保證並降低重新評估的花費。

在多方互相承認框架的運作中，利害關係人有四方：驗證計畫擁有者或主管機關、治理機構、獲得授權的稽查人、雲端服務提供者。驗證計畫擁有者或主管機關的職責是參與框架運作並提供指導，治理機構則負責運行此框架，獲得授權稽查人則負責支援申請者相關要求，雲端服務提供者則於申請後得到相關資訊（圖 21）。

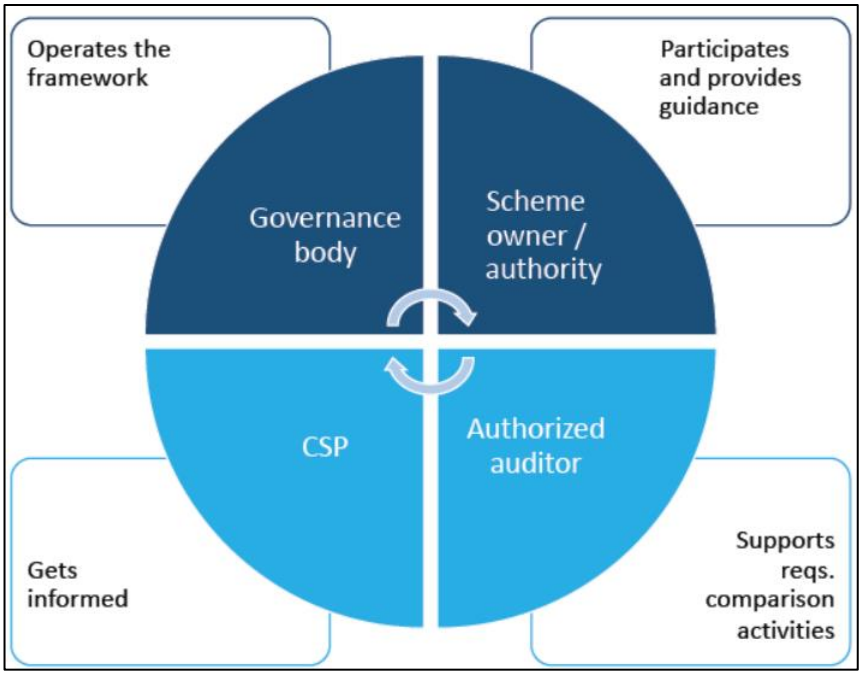


圖 21：多方互相承認框架中各利害關係人之職責

資料來源：Eleftherios Skoutaris 簡報

多方互相承認框架整個運作方式可分為評估(Evaluate)、執行（Execute）、治理（Govern）三個部分。評估係指依據現存的指導原則(principles)、評量標準(criteria)、資安要求(requirements)進行評估，透過 MPRF 的綜合資料庫執行檢視安全控制/要求、隱私要求、稽核要求是否符合。治理則包括兩種流程類型：變更管理流程以及申訴管理流程，用以監督評估及執行部分（圖 22）。

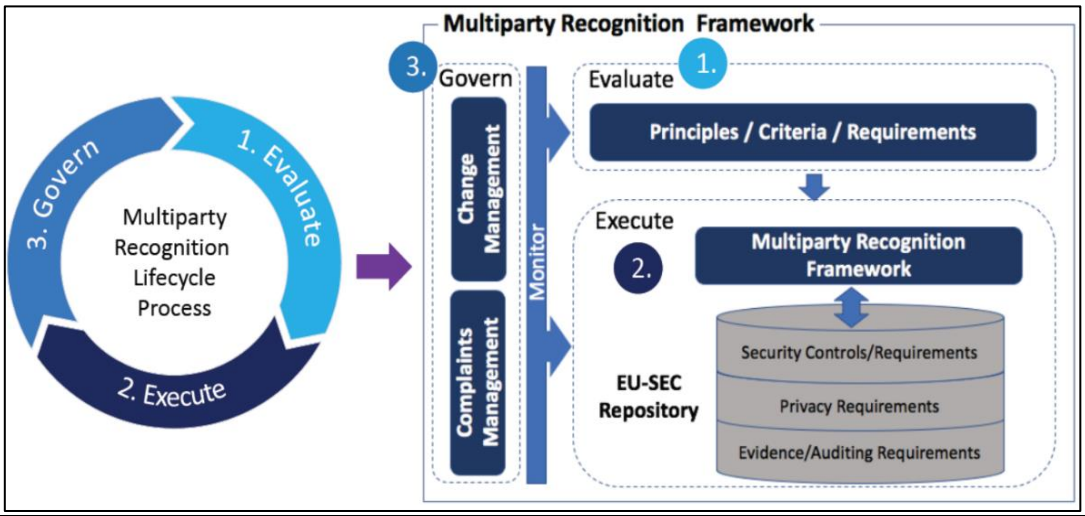


圖 **22**：多方互相承認框架運作週期示意圖

資料來源：Eleftherios Skoutaris 簡報

C. 基於持續性稽核的驗證：EU-SEC 框架另一個重要的部分是以「基於持續性稽核的驗證」取代傳統型驗證。傳統型驗證指的是那些高度管制產業如金融業或醫療業採用的驗證方式，這類驗證方式通常採取定點（point-in - time）、定期（period- of-time）執行資通安全驗證，但對處於高度變動、高風險環境的雲端產業而言，這樣的驗證方式已不足以提供其所需的高等安全保證與透明性。目前傳統驗證方式的資安稽核週期通常間隔 6 至 12 個月（圖 23），這就造成缺乏稽核的空窗期及安全上的不確定性。因此 EU-SEC 框架呼籲應該由「基於持續性稽核的驗證」補足傳統型驗證無法涵蓋的新驗證方式。不過 Eleftherios Skoutaris 也強調持續性稽核驗證並非試圖取代傳統型驗證，而是互為補充，使雲端服務提供者取得相關驗證更具彈性。

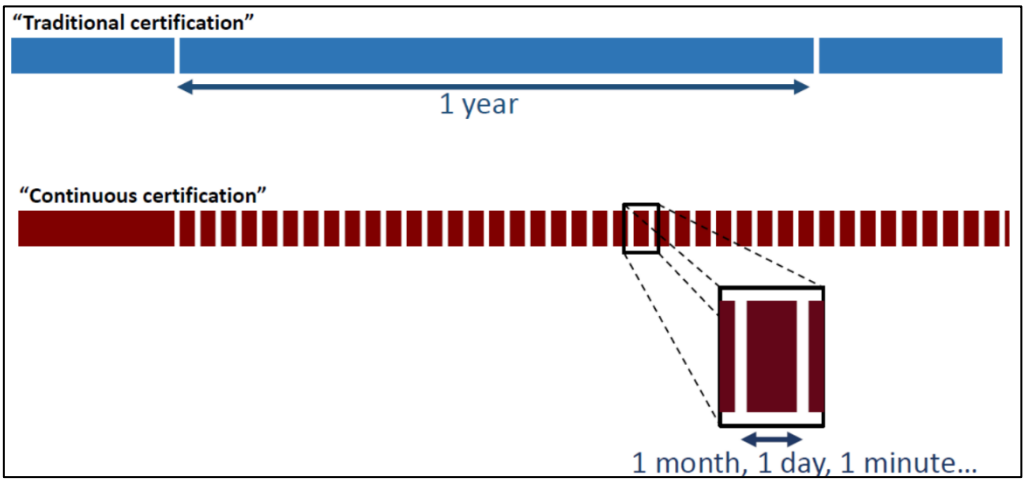


圖 **23**：傳統型驗證 v.s 持續性驗證（週期）

資料來源：Eleftherios Skoutaris 簡報

相較於傳統型驗證只有一種控制目標（control objectives）做為驗證對象，持續性稽核驗證進一步細緻區分安全屬性（security attributes）、度量（metrics）、服務等級目標及服務質性目標（service level objective & service qualitative objective）三種驗證對象，並採用自動化評估方式進行驗證（圖 24）。

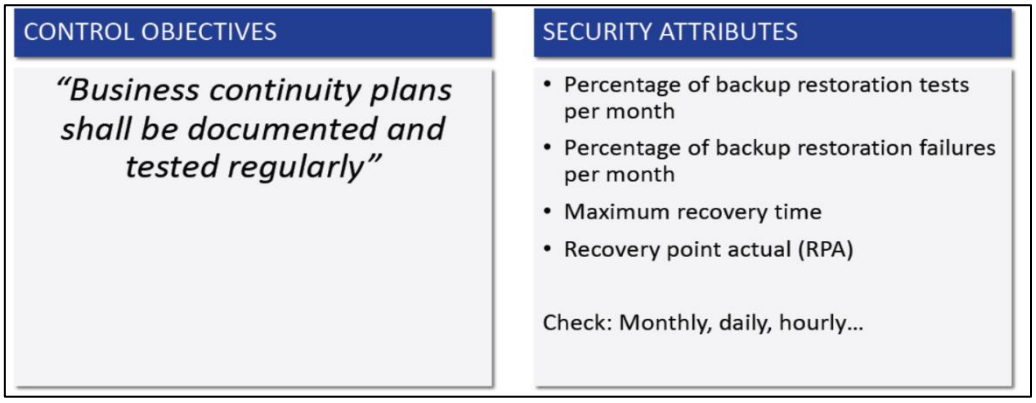


圖 **24**：傳統型驗證 v.s 持續性驗證（驗證內容）.

資料來源：Eleftherios Skoutaris 簡報

做法上，持續性稽核驗證包含五個步驟：預備作業（preparation）、證據蒐集（collection）、測量證據（measurement）、評估目標（evaluation）、提供認證

（certificate）。首先預備作業為開始建立驗證過程且在整個驗證中僅須執行一次，相關的措施包括定義服務等級目標及服務質性目標以描述整個控制過程，並決定評估的頻率、範圍及服務等級目標及服務質性目標，接著蒐集需要驗證的證據，接著決定要用於驗證證據之度量，接著評估目標是否達成，最後依據結果決定是否給予驗證證書，如否則重新蒐集證據後繼續次輪之驗證程序（圖25）。

此種基於持續性稽核的驗證亦可扣合 CSA 提出的三種安全保證等級，比如在基本等級只需雲端服務提供者採取持續性自我評估（continuous self-assessment），而在實質等級層面則採用持續性自我評估佐以擴充型驗證（extended certification），只有在高等安全保證層面才需採用持續性稽核驗證。

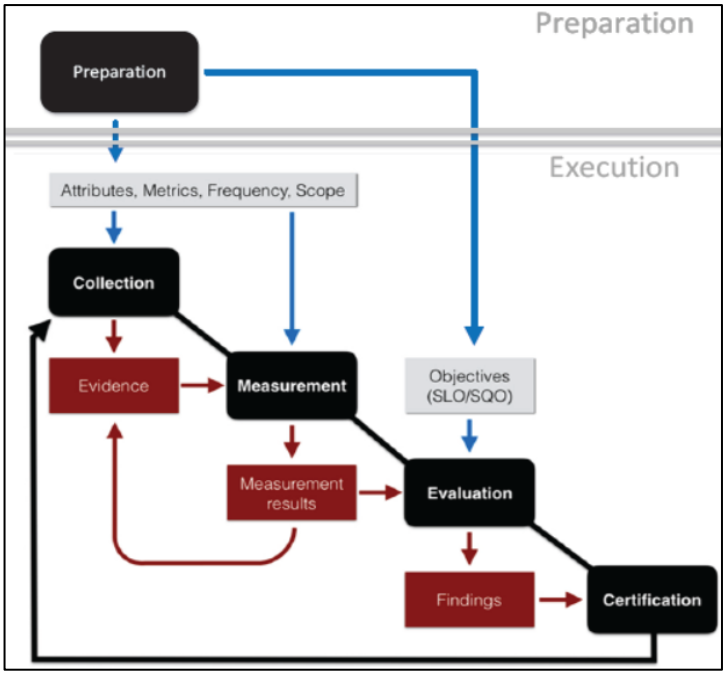


圖 25：持續性稽核驗證的方法論

資料來源：Eleftherios Skoutaris 簡報



圖 26：Eleftherios Skoutaris

資料來源：出國報告人拍攝

3. Addressing GDPR Requirements Using the ISO/IEC 27701 Standard. Is the CSA Looking At It？第三場專題報告由英國標準學會（British Standard Institute, BSI）代表 Willy Fabritius 介紹 ISO 27701 標準，並由微軟代表 Alex Li 補充說明。

   A. ISO/IEC 27701 制定緣由、條文結構：ISO/IEC 27701 隱私資訊管理，正式名稱為「ISO/IEC 27701:2019Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines」，為國際標準組織（ISO）於 2019 年 8 月發布之隱私資訊管理系統（Privacy Information Management System, PIMS）最新國際標準。ISO/IEC27701 發展時期標準編號為 ISO/IEC 27552，自 ISO/IEC 27001 資訊安全管理系統和 ISO/IEC 27002 資訊安全控制措施兩者延伸擴展而來，針對個人識別資訊

（Personally Identifiable Information, PII）的控制者（controllers）與處理者（processors）皆列出實務指引（guidance）與要求（requirements），亦協助個人識別資訊控制者彼此之間的透明度與提供管理個人識別資訊流程的方法，與協助個人識別資訊處理者向客戶提供獲得有效管理之保證。ISO/IEC 27701 條文內容亦對應至包括 ISO/ IEC 29100 隱私框架、歐盟一般資料保護規則（GDPR）、ISO/IEC 27018 保護個人識別資訊、ISO/IEC 29151 個人識別資訊保護實務等法規及標準，目的在於提供隱私保護之指引及要求，以協助組織管理個人資訊以利害關係人提供明確處理流程，以及協助組織遵守各國隱私法律規定。

ISO/IEC 27701 之條文結構共分 8 款與 6 個附錄（Annex A~F），條款 1 至 3 為說明適用範圍、參考規範、術語定義與縮寫。條款 4 為一般性要求，條款 5 及條款 6 分別對應 ISO/IEC 27001 與 ISO/IEC 27002 之特定要求。條款 7 和條款 8 則參照 ISO/IEC 27002，分別自個人識別資訊控制者與處理者之角度，提供額外指引。附錄 A 及附錄 B 為規範性附錄（Normative Annex），分別羅列個人識別資訊控制者與處理者可參照之控制目標及控制措施，做為條款 7 及條款 8 之補充。附錄 C 至 F 為資訊附錄（Informative Annex），附錄 C 至 E 分別對應 ISO/IEC 29100、GDPR、ISO/IEC 27018 與 ISO/IEC 29151 之條款編號以及應用標準之說明，附錄 F 則為說明如何將 ISO/IEC 27701 適用於 ISO/IEC 27001 與 ISO/IEC 27002。

Willy Fabritius 也特別提醒與會者可多注意附錄 D，因其對應 GDPR 條文。

B. 為法規課責設計：另一位報告人微軟代表 Alex Li 接著 Fabritius 補充闡明 ISO/IEC 27701 的設計概念以及為何是適用範圍最廣泛的隱私管理系統標準。Li 本人為附錄 D 的起草人之一，他向與會者說明，由於微軟公司規模及供應鏈複雜度的關係，逐一檢驗供應商是否符合各國隱私法遵事宜，已耗費大量的人力即時間，因此也降低微軟的市場競爭力，故微軟希望有一套萬用標準可以使用，並要求所屬供應商遵循，ISO/IEC 27701 即屬這樣的標準。ISO/IEC 27701 將目前主要市場的隱私法規如歐盟一般資料保護規則（GDPR）、巴西一般資料保護法（Lei Geral de Proteção de Dados, LGPD）、美國加州消費者隱私法（California Consumer Privacy Act, CCPA）之條文對應至 ISO 標準，建立相應的法遵控制措施，要求產品開發者依循相關法遵控制措施以開發產品及服務，並要求組織內部及第三方皆須稽核相關措施，並在組織展現充分法遵措施後取得認證（圖 27）。

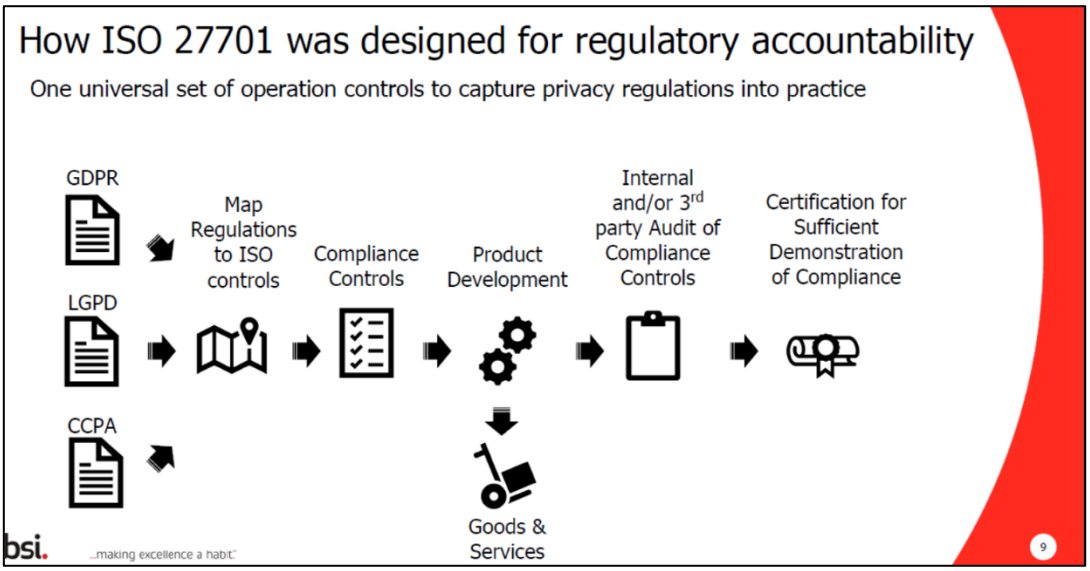


圖 27：ISO27701 架構設計示意

資料來源：Willy Fabritius & Alex Li 簡報

C. ISO/IEC 27701 亦可協助 ENISA 處理個人資料及成為驗證要求：ISO/IEC 27701 同時對個資的處理者及控制者提出指引及要求，因此無論組織大小規模形式皆可取得相關認證或要求其供應商取得驗證。此外，由於 CSA 第 41 條規定 ENISA 在處理個人資料時應遵守 Regulation (EU) 2018/1725，該規則係規範歐盟所屬機關及機構處理個資時應遵守之規範，因此又被稱為「歐盟官方適用的 GDPR」（GDPR for European Union Institutions）[8]。故當 CSA 施行後，未來 ENISA 於執法時需遵照 Regulation (EU) 2018/1725 之規定，建立處理個資的操作規則，為此需要一套合適的標準及驗證做為依據，而 ISO/27701 或許也可成為制定規則之基準。

[8] https://www2.deloitte.com/be/en/pages/risk/articles/gdpr-for-eu-institutions.html




圖 28：Willy Fabritius（左圖一）、Alex Li（右圖）

資料來源：出國報告人拍攝

(五)物聯網挑戰（IoT Challenges）

1. Embedded Systems for IoT Products: What is the Current Certification Offer？

本場次的兩位講者透過 eurosmart 社群的補助，對於目前流行於歐洲的 18 種 IoT 認驗證體系，作了一分詳細的問卷調查，並且在共通的基礎上提出差異分析報告。這 18 種認驗證體系可分為三類：第一類為政府機關所發布，如英國的 Commercial Product Assurance (CPA)認驗證體系、西班牙的 National Essential Safety Certification(LINCE)認驗證體系、法國的 Certification de Sécurité de Premier Niveau(CSPN)認驗證體系以及歐盟的 Senior Officials Group Information Systems Security(SOG-IS)所協調的共同準則(Common Criteria，CC)認驗證體系等。第二類為行業組織所發布的體系，如 ETSI TS 103 655、GSMA IoT Security、

Eurosmart IoT Scheme，以及 GlobalPlatform TEE。第三類為私人公司所發布的體系，如 ARM Platform Security Architecture (PSA) L1&L2、UL 2900、UL IEC 62443，以及 Security Evaluation Standard for IoT Platforms (SESIP)。

在此摘錄問卷之問題種類與問卷結果如下：

A. 認驗證體系概觀(Scheme overview)：80%的體系是這幾年才開始發展。

B. 目標市場與用戶(Targeted market and users)：前三大市場依序為工業控制、IoT 電路板，以及醫療設備。而各認驗證體系的目標用戶種類則是大同小異，皆含括如晶片與設備製造商、應用程式與作業系統開發人員、政府機構、服務提供商、設備供應商與終端用戶。

C. 運作與治理現況(Operational description and governance of the scheme)：

- 頒發證書的工作通常是驗證體系的擁有者所負責頒發。
- 頒發證書的數量每年從 0 件到 50 件不等。
- 整個認證費用則是每個 IoT 設備從 0 元到 1 萬 5 千歐元不等。
- 認驗證體系由專家成工作小組來進行維護管理。
- 證書的效期有數種，如無期限，或者限制為 1、3 或 5 年
- 超過半數的體系需要評估產品生命週期中的風險管理流程

D. 實績(Products evaluated by the scheme)：前三大產品類型為應用程式、網通設備以及 IC 晶片。

E. 評估方法(Evaluation methodologies)：評估方法多採用第三方評估(Independent evaluation by an approved lab)方式，也有 10%的體系採用自我評量(Self assessment)的方式。

- 5a. 實驗室(Evaluation labs)：近 80%的認驗證體系已經提供實驗室清單
- 5b. 步驟過程(Evaluation process)：近 60%的體系支持更新與持續保證(patching and
- assurance continuity)
- 5c. 測試步驟(Testing process)：測試方法(The attack catalog)多由專家小組所設計，且所有體系皆要求提供文檔。另外額外要求提供原始碼(source code)、功能測試(Functional Testing)、滲透測試(Penetration Testing)，以及場地(Developmentand Production sites)這些額外資訊也是在所多見。

F. 與歐盟資安法案合規(Compliance with Art. 54 of the Cyber Security Act)：超過 60%的體系將契合目前已獲通過的歐盟資安法案。

講者最後總結目前歐洲的 IoT 認驗證體系還是在萌芽發展階段，但可以看出將朝著市場需求與風險管理的兩個趨勢前進。且雖然這些認驗證體系都基於 CC 共同準則所開發，但都宣稱可以比 CC 共同準則來的更有效率且更貼近特定產品所需。

2. SESIP: A Practical, Operational, Lightweight CC Methodology

本場次的主講者，相當知名，在會議中相當受歡迎，曾經協助驗證超過 60 項產品，也設置過 5 個認驗證體系，20 年業界經驗，目前是 SESIP 認驗證體系主要的貢獻者。他認為 CC 共同準則的問題在於條文艱澀難懂，許多條文若未經專家解釋跟天書一般無法理解，無法理解就使人無法使用與操作，故講者說明他現在的工作目標是設立一個可操作(Operate)且可持續優化(Optimize)的認驗證體系。講者認為一個良好的認驗證體系有幾個特色，第一個是從驗證到發證的時間是預期且短的，目前 CC 共同準則時間太長。第二是支持已驗證的部件可重複利用(re-ues)。第三是使用產業界已公認且熟知的測試方法與工具。第四是支持大規模化(scale)的驗證。而 SESIP 認驗證體系就是講者給出的答案。SESIP 的特色是使用一般用戶與開發者可理解的語句所撰寫，使得不具備認驗證背景的讀者也能理解。另一個特色是將各類形形色色的安全要求，採用一致化的切分，構成整齊有序的要求項目(Fixed requirements)，這類的整理功夫也只有像講者這樣資深的專家有辦法綜整。SESIP 的驗證等第分為 5 級，各層的分界是用從攻擊者的攻擊強度來區分，從防禦力最強的第五級：等同於智慧卡 CC 驗證，包含 EAL4 + ALC_DVS.2 + AVA_VAN.5 開始，依次為第四級：白箱漏洞分析與不受限時數的滲透測試，第三級：白箱漏洞分析與有限制時數的滲透測試，第二級：有限制時數的黑箱滲透測試，與最低等級的第一級：自我評量與功能驗證測試。因為上述等級可對應攻擊者的能力，所以可以使得通過驗證的廠商有自信可以抵擋各種攻擊場景，這樣的攻擊場景可如：攻擊者在偵查期間與漏洞利用時具有物理訪問權限(第四級)或者攻擊者在漏洞利用後具有加載惡意程式軟件的能力(第四級)，透過這樣自然語言

式的描述，IoT 廠商可以更明確的得知應該選擇哪一個等級的驗證服務，而不是毫無根據地選擇第一級(有作就好)或是最高級(一定要很安全)。最後講者說明 SESIP 目前的進度在於各認驗證體系的對應，使得通過 SESIP 驗證的產品，要取得另一個體系的證書時，較為無痛。他第一個策略是尋求相互承認，第二個策略是提供差異分析，使得客戶能清楚的得知哪些元件必然通過驗證，哪些元件尚待處理，而處理的方式也會提供建議，如採用管理機制或是採用軟體設計。目前 SESIP 已經對應的體系有 ENISA IoT guidelines、GSMA IoT guidelines、ICA Secure (Alibaba Cloud)，以及 IEC 62443 4-2。最後講者提出很有野心的目標，要使得 SESIP 成為大一統的驗證體系，未來要可對應 500 個以上的認證體系，成為國際性的事實標準。

3. EUROSMART IoT Security Certification Scheme (eIoT SCS)

本場次介紹由 Eurosmart 社群所開發的 IoT 認驗證體系，即 Eurosmart IoT Certification Scheme(E-IoT SCS)。講者先簡介 Eurosmart 是一個由產業中資安技術專家組成的社群，他們相信未來 IoT 的安全解決之道需要有生態圈各方參與者以透明協作的方式，以信任關係建立統一且一致的框架來解決。在歐盟通過網路安全法案後，該社群認為是時候提出新的認驗證體系，即 E-IoT SCS，目標是解決現今 IoT 系統缺乏依照威脅模型與風險管理下的整體且共通的資安要求，且要契合新通過的 CSA 的合規要求。該社群所提的體系等級分為高中低三種，低級要求需能最小化已知安全風險與應付已知的攻擊手法。中級要求除包含低級要求外，還寫明能抵擋具有一般技能與資源的攻擊者，我們可以理解為一般因金錢理由驅動的駭客。高級要求則是要求能抵擋國家資助型駭客的攻擊。該認驗證體系吸納了許

多其他驗證體系所具備的優秀觀念，例如依照攻擊者角度進行風險管理、以更新為優先的品質保證(Adapted Assurance Continuity)、主動式的漏洞監控(Active Monitoring/Vulnerability Surveillance)，當然也含括一致性分析(Conformity analysis)與弱點分析(vulnerability Analysis)。講者最後說明採用此驗證體系除了可以符合 CSA 的合規要求外，該驗證體系也提供可預期的人天數，使得廠商能明確知道整個驗證所需的時長，以中級的驗證來說，僅僅需要一個月人天，而以低級的驗證甚至可以短到三個人天，快到難以置信，講者同時歡迎大家能夠參與該驗證體系的前期測試(pilot certification phase)，並且這些文檔都是以開放原始碼的方式分享至其官網，歡迎大家下載 https://www.eurosmart.digital/eurosmart-iot-certification-scheme/。

4. X-Gateway as a Modular Part of IoT

本場次的題目的 X-Gateway 原由來自目前歐洲的開放數據基礎架構 GAIA-X 專案。講者開場把物聯網的層次再拉高一個等級，一般談到物聯網都專注於裝置與服務商本身，但講者拉高到整個生態圈，從上游的設備商、中游的服務提供商，到下游的服務與數據使用者與政府監管機構，講者認為未來的 IoT 系統必然發生多個利害關係人因法令與合約之故，可以被授權存取數據並自動地進行交換，最終導致原本認為數據是被服務提供商給妥善隔離的假設是不復存在。這裡的挑戰在於有多個授權使用者必然導致管理的碎片化與授權不一致，導致授權管理變的異常複雜，難以維護。此時講者提出的解決方案是提供層層堆疊的模組設計來提供安全服務，講者認為需要至少有四個層次，從最外層到裏層分別是：使用者角色授權與權限控管、安全的通訊機制、安全演算法以及金鑰的安全存放，講者在現

場生動地使用俄羅斯娃娃，使聽眾理解何為層層包含的關係。而這樣的層層模組化的安全服務恰好可以透過使用 CC 共同準則這樣的工具來取得重複利用(re-usability)與大量套用的好處。舉個例子，若在底層的金鑰晶片與加密算法，已經獲得驗證，透過層次模組化與重複利用的概念，IoT 開發者只需要再取得安全通訊與權限控制的驗證，而不需要再去驗證底層的晶片與算法，有助於降低驗證成本。講者也繼續說明採用 CC 共同準則的好處是在於CC已經出版了不少保護剖繪(PP)這類的要求，且已經實現在不同的層次，例如 IoT 的安全算法層有 SCA IoT SE PP，而在通訊安全層上，則有 SCA IoT SCA PP，未來各種類似 CC 驗證體系的安全要求都會陸續提出，運用這樣層次模組的概念，很容易有組織地建構 IoT 系統的安全體系。

5. Common Criteria as Backbone of IoT Security Certification

本場次的講者本應該是來自硬體晶片設計製造公司 NXP 的負責驗證業務的負責人，但其因故無法到場，故是由他的同事替補上陣。本場次的主題是使用 CC 共同準則做為 IoT 安全驗證的基石。其主要的論點在於統計 IoT 裝置的應用軟體層及作業系統層的開發商，硬體晶片的製造商數量相當稀少，所以將信任根交由硬體晶片商負責是相當具有經濟效益的決策，這也是 NXP 需要驗證業務的來由。未來因為物聯網裝置的多樣性，以及物聯網裝置背後所帶來的高價值收益，確保 IoT 裝置的安全成為認驗證行業的新一代挑戰，這樣的挑戰體現在三個方面：第一，如何應付 IoT 裝置龐大的量級。第二，如何進行設備的軟體更新。第三如何使設備持續處於安全的狀態。講者提出的解法是透過使用已經過驗證的各層零件來組成安全的 IoT 設備，透過多層次的方法來保證安全。而講者認為採用 CC

共同準則作為 IoT 安全驗證基礎的好處在於：CC 提供了一個一致性描述的通用語言，可以對 IoT 整體以及每個層次的安全問題進行建模。最後講者提出目前歐洲有大量的資安法規、驗證計畫與標準，要如何選擇合適的驗證體系，取得合格證書，這對 IoT 的設備商及服務商帶來的不小的困擾，故講者也稍為介紹了一下 SESIP 這個驗證體系所提供的對應服務，簡單的說即是對其他驗證體系的轉換證書服務，使得已經取得某一認證的產品可以快速的轉換成其他驗證體系所需的安全要求，以增加產品的的驗證廣度。

6. OWASP IoT Project: A Great Ally for the IoT Candidate Schemes

本場次講者來自權威的軟體安全社群 OWASP，代表該社群向與會者介紹該社群一系列關於 IoT 安全工作的現況，本場次的標題是 IoT 驗證體系的好盟友，指的就是 OWASP 社群並不會如一般的認證體系，索取費用來認證實驗室，或者提供證書發放等等作為或服務。OWASP 恰好相反，它提供來自社群專家們免費的資訊安全建議與錯誤態樣排序，而這些安全建議常被認證體系引用作為補充材料，以更好的應對威脅態勢(Threat Landscape)的變化。講者首先介紹的是 OWSAP IoT Project，該工作已經產出兩個年份(2014 與 2018)的 IoT 十大錯誤態樣報告，報告中提示 10 個在設置與營運 IoT 系統時常需要避免的錯誤態樣，並以需處理之優先排序。該專案也衍伸出韌體分析(Firmware Analysis Project)、IoT 攻擊面(IoT Attack Surface Project)、IoT 框架評估(IoT Framework Assessment)、韌體分析工具(ByteSweep Firmware analysis tool)等等專案工作。講者也介紹明年度啟動的專案，IoT Security Verification Standard(ISVS)，ISVS 標準對 IoT 安全控制羅列了許多要求，並且還為開發人員

提供了安全開發的要求列表，雖然 ISVS 名稱中有標準二字，但其作用更像產品型錄，而非一般觀念中的務必要遵守的標準。最後講者說明未來 OWASP 對 IoT 專案的三個工作方向：第一個是 Seek & Understand，這包含每兩年更新錯誤態樣報告與對齊其他資安組織之安全指引，如 ENISA。第二的是 Validate & Test，也就是前述 ISVS 專案與韌體分析工具開發等。第三個是安全治理(Governance)，如盤點其他組織的 IoT 的監理政策與認驗證制度，或者開發 IoT Security Framework 等。

(六)觀點與機會（Outlook/Opportunities）

1. SOGIS View on the Cybersecurity Act

歐盟執委會及 ENISA 代表分別於 11 月 18 日專題報告中已各自就其立場同時宣布網路安全法通過的首件候選資通安全驗證計畫為將現行的資訊系統安全資深官員小組相互承認協議（Senior Officials Group Information Systems Security Mutual Recognition Agreement, SOG-IS MRA）轉換為歐洲共同準則計畫（European CC Scheme）。本場專題即是由 SOG-IS 管理委員會（SOG-IS MRA Management Committee）Bernd Kowalski 主席講解此一任務的執行情形。

A. SOG-IS MRA 概述：Bernd Kowalski 先概述 SOG-IS MRA 及澄清一些常見的誤解。在網路安全法通過之前，歐盟境內存在數個彼此互不相容的國家型及區域型安全驗證計畫，SOG-IS MRA 簽訂時即基於 ISO 共同準則標準（CC standard, ISO/IEC 15408）建立歐洲認證框架，應用驗證的相互承認原則建立各成員國之間的信任，參與者為各國的公共安全主管機關；協議經由官方認證機構

執行公開監督、定期施行各驗證計畫的同裁評定（peer-to-peer assessment）、30 間私人實驗室（ITSEFs）的社群網路確保驗證計畫下的驗證結果具備可比較性（comparability of results）。

SOG-IS MRA 於 1997 年由各成員國簽訂，其後曾更新兩次，一次於 1999 年整併共同準則於協議內，另一次則是於 2010 年時調整制度以納入新型驗證計畫，以及限制各成員國只能於已達成共識的技術性事宜諸如評估方法、實驗室要求、攻擊手法等適用高於第四級安全評估（EAL4）的安全認證[9]。SOG-IS MRA 目前有 17 名會員國，會員國在參與權限上依據其國內有無自身驗證計畫/國家認證機構區分三個層次，無國家型認證機構的為一般等級（consuming participants），國家型認證機構如可執行各類產品驗證至 EAL4 則為授權類參與者（authorising participants）成員，最高級別成員則是能夠評估智慧卡（如晶片金融卡）或硬體安全認證至 EAL7 的認證機構（如圖 29、圖 30）。

由於網路安全法要建立歐盟資通安全認證框架，因此有些論者即質疑 SOG-IS MRA 已無存在必要，而 Bernd Kowalski 也特別於報告中列出對於 SOG-IS MRA 的誤解，包括認為此協議並非屬框架體系，不接受非歐盟成員，不適用於物聯網裝置，實驗室及驗證計畫的同儕評估非屬必要，以及需為歐洲認證市場的零碎化（Market fragmentation）負責任。Bernd Kowalski 強調以上答案皆屬誤解，尤其是所謂市場零碎化肇因各類垂直產業的法

[9] https://www.sogis.eu/index_en.html.

規缺乏協調而非 SOG-IS MRA 未能達成各驗證計畫間的協調一致。

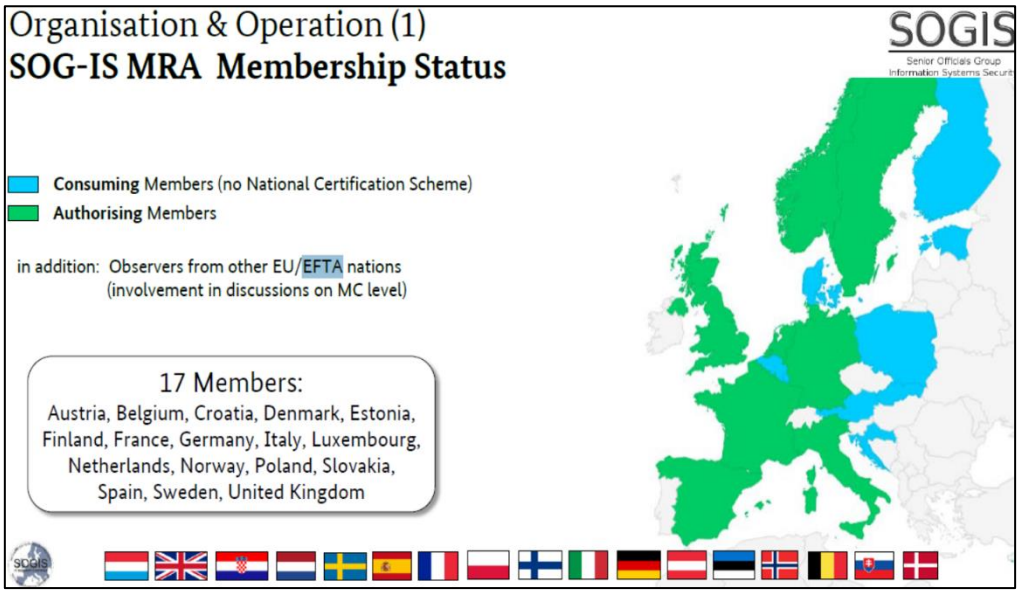


圖 29：SOG-IS MRA 成員國

資料來源：Bernd Kowalski 簡報

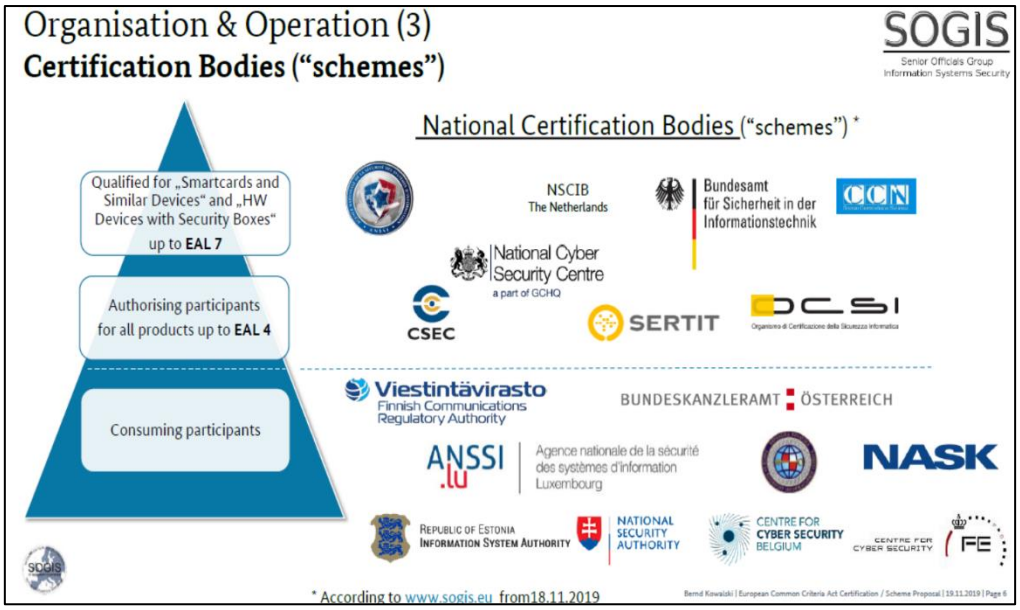


圖 30：SOG-IS MRA 成員國參與等級

資料來源：Bernd Kowalski 簡報

B. 歐洲共同準則計畫草案：前曾述及歐盟執委會在彙集歐洲資通安全認證工作團（ECCG）及利害關係人資通安全

認證工作團（SCCG）意見後，提出第一項歐盟滾動式工作項目（URWP）即是要求 ENISA 將目前 SOG-IS MRA 此一機制轉換為歐盟資通安全驗證計畫（CSA scheme），為此 SOG-IS MRA 管理委員會亦著手準備相關轉換工作，並提出相應的歐洲共同準則計畫草案（Draft Proposal for a European CC Scheme）。

SOG-IS MRA 提出之草案在做法上建議先將 SOG-IS MRA 管理委員會整合至 ECCG，並劃分幾個組織負責：國家資通安全認證主管機關（national cybersecurity certification authorities, NCCA）、歐洲共同準則和諧工作團（European Common Criteria Harmonization Group, ECCHG）、歐盟網路與資訊安全局（ENISA）、一致性評估機構（Conformity Assessment Body, CAB）、資訊安全評估設施（IT Security Evaluation Facility, ITSEF）。此驗證計畫草案特色為以共同準則為標準，用保護剖繪（protection profiles）描述產品類型，範圍上則涵蓋資訊產品與保護剖繪的認證，不涉及特定產業部門，三種安全保證等級皆可適用，不允許自我驗證（self-attestation）、不適用於資訊服務本身及產品服務的工作流程。最後，Bernd Kowalski 也向與會者表明，此草案已提交 ENISA，而至少要至 2020 年上半方成為確定的資通安全驗證計畫候選項目。

2. Overview of Current and Future NIAP and US Government Certification Initiatives

歐盟通過網路安全法案，建立全歐範圍的歐盟資通安全認證框架，對象則是適用於資通產品、服務與流程，因此在國際貿易層面上則涉及非歐盟國家驗證計畫承認的議題。本場專題報告即是由美國國家資訊安全保證夥伴關係（National Information Assurance Partnership, NIAP）主任 Mary Baish 闡明當前美國資通安全驗證運作現況並就歐盟 CSA，以及討論國際資通安全共同準則相互承認協議（common criteria recognition arrangement, CCRA）相容之可能。

A. 美國資通安全驗證及授權概觀：Mary Baish 首先概述美國資通安全驗證的政策框架，其內容大致包括五項法律及政策：聯邦資訊安全管理法（Federal Information Security Management Act of 2002, FISMA）、聯邦資訊處理標準第 140 號(Federal Information Processing Standards, FIPS 140）、國家安全命令第 42 條（National Security Directive 42）、國安體系委員會政策第 11 號（Committee on National Security Systems, CNSS Policies＃11）、國防部指示 8500.01 號（DoD instruction 8500.01）。

   在執行面上，驗證及授權涉及的美國行政機關/機構則包括國家標準與技術研究院（National Institute of Standards and Technology, NIST）負責 FIPS 140、NIAP 負責共同準則、國防部有資訊網路核可產品清單（DoDIN APL）、總務署（GSA）轄下的聯邦政府風險與授權管理計畫（Federal Risk and Authorization Management Program, FedRAMP）則針對雲端服務的風險評估及授權管理提供標準作業規範、國土安全部（DHS）的持續診斷及緩解專案（Continuous Diagnostic and Mitigation, CDM）則為

聯邦機構提供改善資通安全的工具及服務。在送驗流程上則由產品供應商送交實驗室測試一致性（tests for conformance），經各主管機關確認（validates）方可交至使用者手上（如圖 31）。

NIAP 為 NIST 監督之國家型專案，負責管理美國境內共同準則適用的相關事宜。美國目前關於驗證計畫的關注焦點包括提昇安全評估的速度、創新評估技術、建立涵蓋產品生命週期的評定（Assessment）、協調各驗證計畫等。

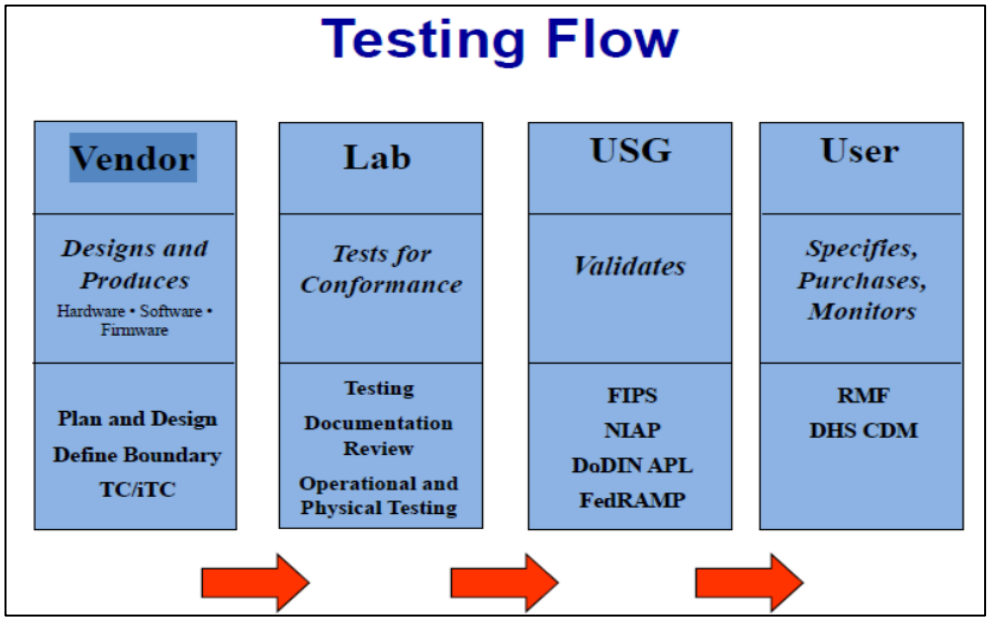


圖 31：美國產品資通安全審驗流程

資料來源：Mary Baish 簡報

B. 歐盟 CSA 與共同準則相互承認協議之競合：共同準則相互承認協議（CCRA）係於 1997 年時由美國、加拿大、法國、德國、荷蘭經多年談判後的成果，後經 2009 啟動改革並於 2014 年更新相關協議內容。美國境內對於適用共同準則的需求自 2018 年 9 月以來上升百分之三十，

顯示共同準則仍是資通安全驗證的核心基礎。由於歐盟 CSA 似乎將建立一套新的驗證框架及標準，然而其內容似乎與共同準則多有重疊、相互衝突之處，這可能導致歐盟成員國與其他簽訂 CCRA 之成員產生分裂，而各國產業皆被迫於兩種體系間擇其一或重複取得評估，此將不利 CCRA 成員之間的合作，以及也可能引發貿易問題。因此就美國立場而言，目前除致力使 CCRA 因歐盟 CSA 引發的影響降至最低，也希望 CSA 未來建立的共同準則驗證計畫除能改善歐盟內部的協調作業，亦能強化與 CCRA 成員國之間的協調合作。



圖 32：NIAP 主任 Mary Baish

資料來源：出國報告人拍攝

3. BSI View on the EU Cybersecurity Act

第三場專題報告由德國聯邦資訊安全辦公室（Bundesamt für Sicherheit in der Informationstechnik, BSI）代表 Matthias Intemann 從該國資通安全主管機關角度評論 CSA 所提供架構之優劣以及後續可能影響。

A. 水平式立法 V.S.垂直式立法：Matthias Intemann 指出歐盟設立的各類規章、指令依其立法架構性質可區分為兩大類：水平及垂直。水平式立法為發展各領域適用的框架，如以烹飪為例即類似於將「香料」（各類產品之安全要求）經由「篩子」（框架制度如歐盟資通安全認證工作團(ECCG)、ENSIA 專家工作小組(AhWG)）統一附加在各類食材（資通領域如雲端、5G、IoT）上（如圖 33）。至於垂直式立法則是以產業為主發展適用規則、指令，如 GDPR、eIDAS，各自有其適用的產業領域（如圖 34）。歐盟 CSA 則屬於所謂的水平式立法，然而其設計允許各國在共同基下促使市場需求促此各類資通領域的安全認證協調一致（如圖 35）。

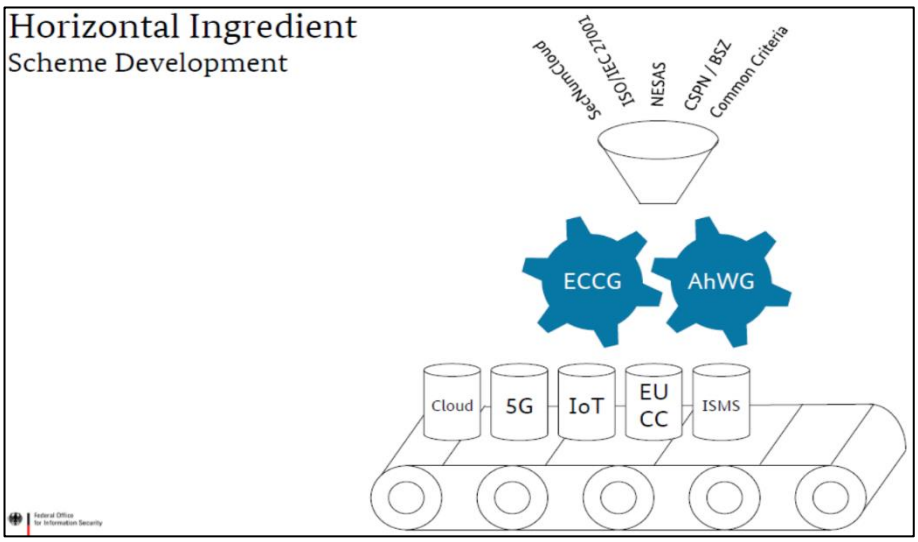


圖 33：水平式立法示意圖

資料來源：Matthias Intemann 簡報

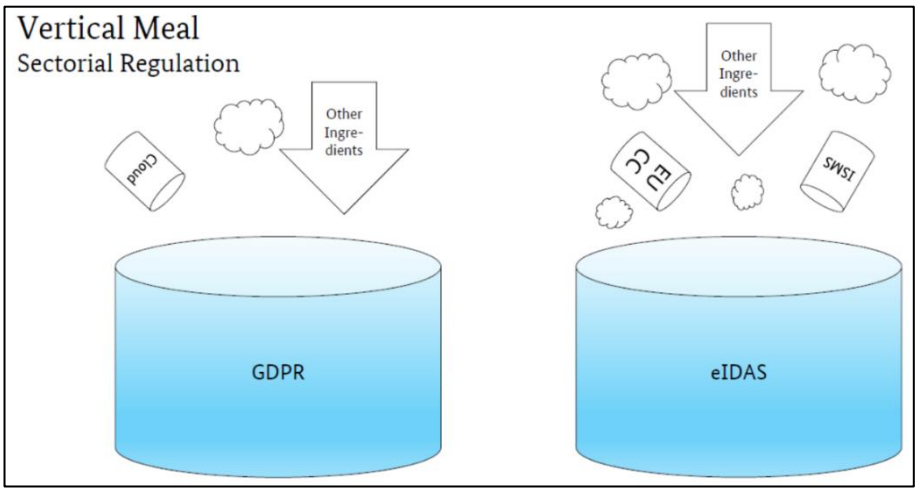


圖 34：垂直式立法示意圖

資料來源：Matthias Intemann 簡報

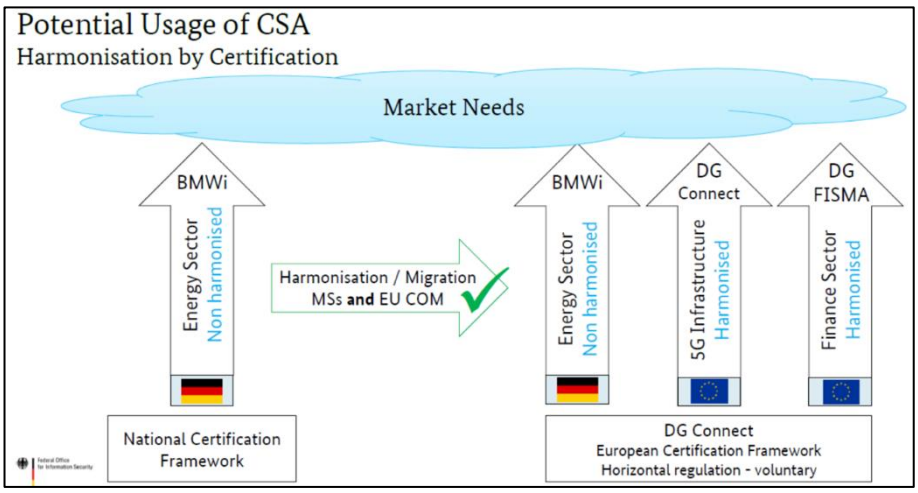


圖 35：歐盟 CSA 的使用方式

資料來源：Matthias Intemann 簡報

B. BSI 對於資通安全驗證計畫候選的期望清單：歐盟資通安全認證框架提供制定單一領域資通安全驗證計畫的立法架構，就德國的立場而言，BSI 認為可優先制定的安全驗證計畫領域包括一般性資通產品、工業自動化及控制系統、雲端產品服務、5G 通訊網路、物聯網。Matthias Intemann 亦於簡報中以 5G 為例提出未來 5G 驗證的可能架構（如圖 36）。

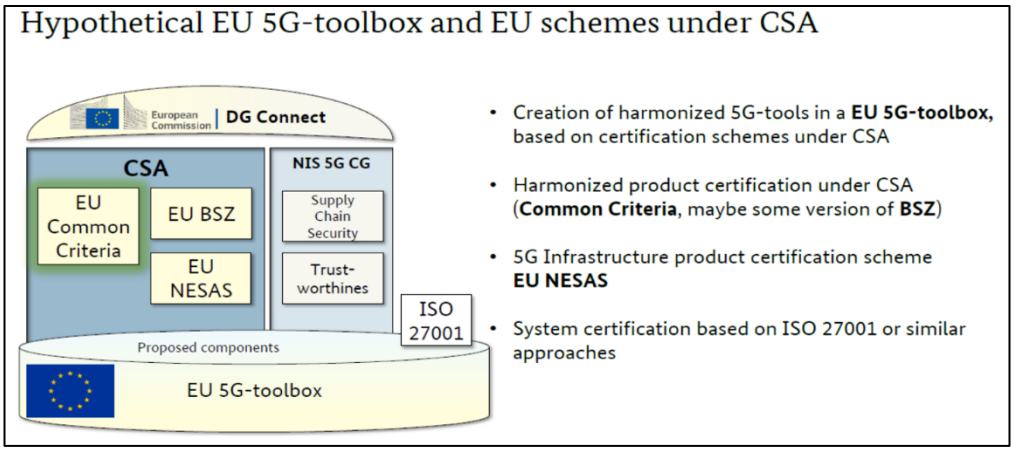


圖 36：BSI 假定的 5G 資通安全驗證計畫架構示意

資料來源：Matthias Intemann 簡報

C. CSA 的利弊分析：在報告最後，Matthias Intemann 提供 CSA 施行後的利弊得失。該法可能缺點有三：其一，歐盟成員國需提供大量資源以運作該法所設制度；其二，該法雖以試圖彌補各類資安標準之間的落差，然而各產業部門本身的法規及驗證仍需逐一解決；其三，各國仍需確認每個驗證計畫具備可比較性，因此認證體系成為各國的基本設置（Accreditation system is the default）。

至於 CSA 的優點則有六點：其一，藉由框架取徑彌平法規與認證之間的落差；其二，引入驗證的可擴充性（scalability）；其三，為所有驗證計畫列出核心需求；其四，框架設計允許各領域之專家處理各垂直產業法規，驗證計畫之運作毋庸負擔相關法規調適需求；其五，該法促使各成員國需針對自身驗證計畫進行交換，方可相容於歐盟範圍的驗證計畫；其六，透過建立協調各類認證有效性與監控產品生命週期的方式，該法具備處理橫跨成員國安全漏洞之功能。



圖 37：BSI 代表 Matthias Intemann

資料來源：出國報告人拍攝

4. The ROI of Security Evaluations

A. 安全認證的投資報酬率：本次研討會的主題之一是歐盟推動全歐盟一致的資通安全認證框架，以驗證資通產品、服務、工作流程的安全狀態，然而對於業者而言，除被動配合政府要求，是否有其他誘因可增加主動配合？其中一項重要因素在於進行安全認證需有足夠投資報酬率（return on investment, ROI），因此本場次最後一場專題報告由民間安全實驗室業者 brightsight 之執行長 Dirk-Jan Out 向與會者說明對於民間業者而言，執行產品安全評估需求從何而來，以及該如何增加業者主動配合政府取得安全認證的誘因。

從商業活動的本質觀之，企業執行一項業務必須同時判斷該業務的投資及回報，投資越低回報越高是企業的首

要考量，企業的此種心理狀態可用最簡易的公式描述：投資報酬率＝回報（收益）除以投資（花費）。如將此投資報酬率公式應用在安全認證，則可簡易描述為：取得安全認證投資報酬率＝認證證書所含的價值除以（付出的金錢及花費的時間）。

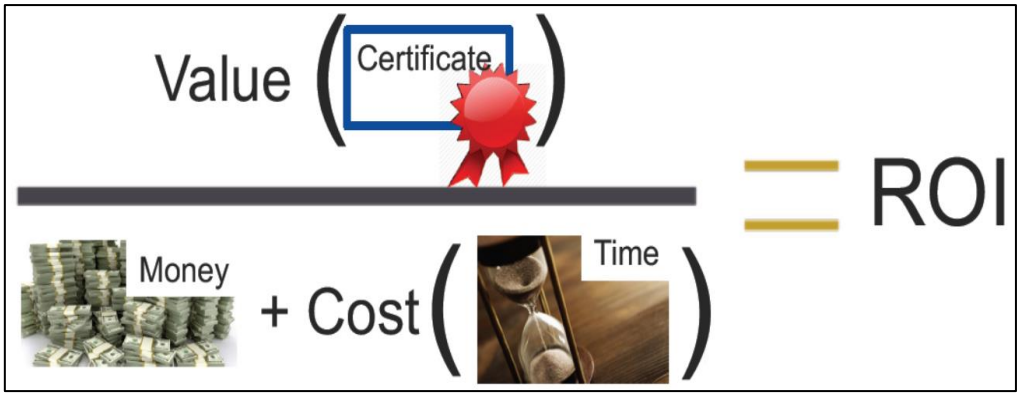


圖 38：業者取得安全認證的投資報酬率公式

資料來源：Dirk-Jan Out 簡報

B. 安全認證的價值考量：符合法令、展現善意、分散責任：基於金錢及時間的花費易於計算也易於評估及節省，然而安全認證本身價值卻不易量化為具體數字也不易評估，因此 Dirk-Jan Out 認為可從三個角度描述取得安全認證的動機：遵循政府法令（compliance）、顯示企業善意（goodness）、分散事故責任（liability）。

- 遵循政府法令：為了進入當地市場販售產品，企業需完成各國政府制定的相關安全認證要求並取得證明，此時對於企業而言安全認證的價值高低即取決於證書內容（content）與嚴格性（strictness）兩項因素。安全認證的內容在於告訴主管機關已有符合保護剖繪，所有各類認證的價值皆屬一致（因為只要有安全認證就會有相關的保護剖繪描述），然而如某類安全認證的安全保證要

求越嚴格，則使該認證就越有價值（因為只會有少數廠商符合，而物以稀為貴）。

- 顯示企業善意：由於有些產品的共同準則驗證、保護剖繪、安全標的與驗證報告非常難以理解以及可能造成誤解，因此企業取得認證動機僅僅就是透過證明向顧客顯示自身的產品非常安全。然而此時這類安全認證的內容因其未具備保護剖繪或保護剖繪難以理解則對於安全認證的價值幾乎不產生影響；而安全認證的嚴格性雖然重要，但也可能造成由於過於嚴格而使產品幾乎無法使用。
- 分散事故責任：最後一種取得安全認證的理由在於分散風險，此時取得安全認證的目標在於稀釋產品開發過程各環節參與者的責任，包括開發者、評估實驗室、驗證機關、送驗客戶、終端使用者，最終目的則是希望發生安全事故時，無人需擔負所有責任（因為各環節已盡其所能驗證產品的安全）。當發生前述情況，則需由司法部門介入以評判驗證的內容及嚴格性。

綜上而言，Dirk-Jan Out 建議應該綜合此三項因素以制定可極大化安全認證商業價值的安全驗證計畫，並應注意非僅是為了展現技術而制定無法應用與難以取得認證的安全認證要求。



圖 39：Dirk-Jan Out

資料來源：出國報告人拍攝

(七)品質保證之創新（Innovations in Assurance）

1. Addressing the Continuity of Software Security for Embedded Devices

今日對 IoT 開發製造公司來說，若欲對一個已經取得證書的 IoT 產品進行軟體更新，是個十分困難的決定。困難的根源有三，首先，更新軟體會使得已經取得之證書失效。再者更新軟體的作業，公司需要花上不少成本。最後，若不提供更新軟體的服務，也甚少人會發現，進而抱怨。

本場次的講者來自一間提供嵌入式裝置安全驗證服務的公司，特別是是在密碼模組的驗證，而非一間嵌入式裝置設計開發製造的公司。講者認為頻繁的軟體更新已經是不可抵擋的趨

勢，但如何調和設備認證與軟體更新的衝突，使得廠商願意不停地提供更安全的軟體，而不會被現行 Common Criteria 共同準則對於重新認證所需的繁複流程與手續所綁架，進而使廠商不願意去更新軟體，最終使用者只好繼續使用不安全的軟體。

講者提出的解決概念是累積型的品質保證(Accumulative assurance)，其觀念想法是整個品質的保證要具備四個支柱相互支持：第一個是半自動化的測試。第二個是安全的軟體開發，又或者可稱之為開發成熟度。第三個是差異修改的驗證評估(Delta evaluation)。第四個是原本就已經存在已久的安全驗證與認證。當這四個支柱都發揮功能時，這樣的驗證會變得更具有彈性，就可以支持頻繁的軟體更新，而不會破壞產品認證的狀態。

2. Updating Certified Products

本場演說的題目是介紹各種驗證體系對已經取得驗證的產品進行更新，如何處理保證的持續有效(Assurance Continuity)。講者來自 International Security Certification Initiative，簡稱 ISCI，也是一個與共同準則(Common Criteria，CC)有緊密關聯的組織。講者首先說明在 CC 中如何進行產品更新，因為 CC 驗證在產品更新的流程手續十分繁複，故講者引介提出幾個與 CC 類似的驗證體系是如何處理相同的議題。

講者首先介紹 CC 目前處理產品更新的邏輯是：只要產品有更新，原證書就失效。進一步說，若是重大更新則要重新驗證(recertificate)，取得新證書，原證書失效。若是輕微更新，則進行局部評估，取得局部的報告(Evaluation Technical Report)。例如，原證書為 1.0，產品更新後，證書 1.0 失效，此時意味著

更新後的產品是無任何認證的，需待審查通過後，其證書改版為 1.a 版。當然 CC 也有另一種將平臺(Loader & Platform)與程式碼(Code)分開驗證的方式，稱之為 Post-delivery code loading。同樣地，採取相同的更新破壞的看法，在法國國內的輕量化類 CC 的 CSPN 體系以及西班牙的 LINCE 體系都有出現，也就是採用 CC 原則：更新破壞驗證(No changes prior to recertification)，此法無疑曠日廢時。

一種稍微改進的替代方法是採取簡易審查機制(speeded-up process)，在智慧卡的驗證機制 EMVCO 以及美國 FIPS 140-2 就是採用如此方式，他們認為，若是輕微的更新，則以由廠商向實驗室提出書面的資安衝擊分析(Security Impact Analysis)，實驗室用一星期的時間審查並更新證書。

上述的做法，可稱之為更新前審查機制，但在目前軟體更新頻繁的時代已經無法適用，較為進步的做法是採用先更新後審查機制。也就是採取廠商先更新，但驗證之效力持續，直到更新後才送件進行審查，如此才能激勵廠商先解決眼前的安全問題，事後再考慮驗證持續有效的議題。採用這個做法的認驗證體系有英國輕量化 CC 體系，CPA、Globaplatform 組織的 CC 體系以及 Eurosmart IoT 體系。但是這種機制需要廠商與實驗室建立信任關係，實驗室要能夠從廠商的開發流程的成熟度來信任廠商能夠在產品更新的過程中，不會引發新的安全漏洞，這需要廠商具有安全的開發流程與自動化工具的配合。

3. Agile Assurance: Modernizing IT Product Certification

本場次講者認為目前所採用的 CC 共同準則與 FIPS140 驗證都是上個世紀 80 年代的產物，雖然還是挺有效，但已經無法

應付頻繁更新的議題。講者點出隨著威脅不斷增長，缺乏更新的產品即便是取得證書且證書時效尚未過期,也是過時的產品,因為該產品無法應付新的威脅。而目前沒有有效的方法，對那些定期更新的 IT 產品提供方便且有效的驗證機制,故講者認為這需要更多的創新與最佳化來使得品質保證過程來的更快速敏捷。講者認為這樣的最佳化創新有三個趨勢，第一個是自動化的測試方法，第二個是安全的軟體開發流程，第三個是可擴展的自動化協作(Expand Automation)。當然並非所有的測試都可自動化，但測試的作業流程是可以標準化與生產線化的，例如由平臺自動地跳出提示、紀錄步驟、收集證據、整理與分類資料與產生報告。透過安全的軟體開發流程與可擴展的自動化協作可以使得實驗室與 IT 公司取得更多的開發證據與更好的資料同步，加速驗證過程。相較傳統的方法，採用自動化測試平臺可以將驗證時程從年月之久，加速到以周計算。但是開發自動化平臺需要大量投資，這樣的挑戰需要透過集體的協作才有可能付的出如此成本。需要在一致且在一定的範圍內定義良好的測試要求，驗證機構也要同步擁有這些測試結果文件，以更快更持續的驗證產品，這些都是有待努力的目標。

4. Making Evaluation Schemes Scale Up: the Tensegrity of Process and Product

本場次的講者來自英國，現場的聽眾都對英國的商業產品保證體系(Commercial Product Assurance，CPA)有什麼樣的創新觀點來處理產品更新的議題很有興趣，而講者也沒讓人失望，他提出以不光是要驗證產品零件(Produce part)，也要驗證產品的生產過程(Process)。他從食品安全所得啟發，認為將產品零件與生產過程當作兩件事情分開看待是沒有道理的事情。他說道

針對產品認證在現實中很難大規模的進行(Scale up)，這有其技術上的難度。替代的方案是對過程(Process)進行評估，這樣就意味著我們不需要評估所有產品，只需要評估過程是否正確，並期待正確的過程就會產生良好的產品，這也是含在英國 CPA 的一個步驟。但是講者同樣也並不認同僅評估過程，他認為也需要同步評估產品零件，他認為過程與產品零件分不開，兩者在一些關節點(skeletal struture)保持連接，缺乏正確的流程使產品零件組裝起來，再好的零件也只是零件。他最後總結道，同時評估產品與過程比只評估兩者之一要來的好。評估產品可類比 X 光的快照，只是當下該筆產品的數據，這些 X 光數據都是單點的，他建議透過過程評估來達成各批次產品驗證的連續性。發展這樣的過程評估能力能夠更好的預測未來驗證通過與否的結果，以及自我評估的準確度。

肆、 心得與建議事項

由於資通訊科技的快速發展，促使人工智慧、大數據、物聯網等應用服務的推陳出新，不論是金融、能源、交通、教育、通訊傳播、醫療健康，乃至政府體系等領域，創新的數位服務已逐漸成熟，更因此帶動了數位經濟之發展。雖然創新數位服務提供民眾前所未有的便利生活及商業契機，然而，新型態的資通安全威脅卻逐漸成為隱憂。隨著資通安全攻擊事件的不斷發生，不僅對民生與經濟造成衝擊，若被攻擊的對象為關鍵電信基礎設施，更將影響社會整體運作，甚至危及國家安全，其危害不可小覷。

面對數位生活日益嚴峻的資通安全威脅，美國 NIST、歐盟 ETSI，以及 OWASP 等資通安全機構，已紛紛發布非強制性的安全框架或指引，而歐盟也於今年 6 月公布「網路安全法（Cybersecurity Act）」，建立 ICT 產品／服務／流程之資通安全驗證方案，以提升歐盟網路安全能力，促進歐盟數位經濟、社會和民主發展。雖然目前這些資通安全建議或驗證方案均非強制規定，但建構「安全可信賴」的 ICT 生態鏈，已為各先進國家為確保數位經濟永續發展的重要目標，更為其強化數位經濟領先地位之重要措施。為了降低風險或避免威脅帶來的衝擊，應該鼓勵廠商在設計開發階段採用自願性的資通安全認證方法，並針對認證進行分級，例如自我宣告、基本的第三方認證到更進階的第三方認證，透過認證讓資通安全融入開發流程，從源頭即開始注重資通安全。

在歐盟網路安全法案中，允許製造商或供應商針對 ICT 產品、服務或流程進行自我評估，從風險承擔者的角度來看，產品、服務及流程的風險承擔者也不同，服務與流程的承擔者為服務提供商，而提供商有動機將事情做對、做好，但產品的風險承擔者為使用者而不是開

發者。對於服務、流程等供應商，把事情做對做好可以避免潛在的資通安全問題，對於各種變更的調適以強化資通安全也相對容易，而供應商應付各種變更與調適之責任，對於自我評估到發現事項可立刻回饋到資通安全管控措施，故供應商有強烈動機來執行自果評估。

然而，除非是有法令法規或是合約要求，通常資通安全並不會是產品開發的第一優先順位，主管機關宜考量在對產品開發者衝擊最小的情況下，適度的要求產品的資通安全自我評估與相關監理或稽核工作。另 GSMA 與 3GPP 為提升行動通信網路資通安全，於 2016 年共同推出一涵蓋網路設備生命週期之安全保障方案 - 網路設備安全保障方案（Network Equipment Security Assurance Scheme，NESAS）。該方案包括由 GSMA 擇定的安全稽核員評估「供應商在產品開發過程及整個生命週期之安全性」及 GSMA 認可的安全測試實驗室評估「網路設備安全性」兩部分。在評估「網路設備安全性」所需之檢測基準則由 3GPP 制定。5G 設備亦屬 ICT 產品之一部分，此次會議中，來自 ETSI 的講者更將 NESAS 列為報告重點之一。顯見，在歐盟大力推展 ICT 產品資通安全驗證下，5G 設備資通安全驗證應指日可待。

歐盟資通安全驗證方案是基於歐盟級別的協議，ICT 產品、服務、流程經歐盟資通安全驗證方案驗證合格者，可通行全歐盟會員國，除助於供應商跨境營運外，更助於消費者識別擬選購之產品或服務的安全功能。輸歐 ICT 產品或服務者，尤其相關產品或服務係應用於歐盟關鍵基礎設施者，應關注歐盟資通安全驗證方案制定階段之發展，並積極送測，以提升產品市場競爭力，並於相關驗證方案成為強制規定時，取得最佳戰略地位。

綜觀上述 5G 網路與 IoT 資通安全評估方法，可知資通安全除了設備本身，包含上下游供應鏈之生態系管理、系統強韌性規劃等都是

重要課題，亦為資通安全維護計畫的重點項目之一，足見我國通傳會在 5G 與資通安全上的努力並與國際接軌。

附件四　「2019 沖繩開放國際會議（Okinawa open days）」參訪報告

財團法人電信技術中心出國報告

出席 2019 沖繩開放國際會議
（2019 OKINAWA OPEN DAYS）
並與日本相關業者訪談交流

單位名稱：檢測暨網通技術組、資通安全組

姓名職稱：吳東興高級工程師、謝仁翔副工程師、李贛麟工程師

派赴國家：日本

出國期間：2019/12/11-2019/12/14

報告日期：2020/01

摘要

Okinawa Open Days 2019 為沖繩開放實驗(Okinawa Open Lab, OOL)一年一度的行動網路國際研討會，基於開放式網路架構與軟體化技術之資訊與通信科技(Information and Communication Technology, ICT)產業基礎設施部署的趨勢，未來將影響到各個領域的服務用戶、電信運營商、設備供應商的經營模式。因此，資訊與通信科技(ICT)技術已經成為每一項新創應用服務之基石，並且不間斷的在持續推進，同時與 5G 網路、AI 技術和 IoT 物聯網相輔相成，這些創新技術預計能改變各個行業的發展藍圖與績效潛力。日本企業和組織正試圖進行數位化生態轉型，成功與否的關鍵在於能否有效的利用這些前瞻性技術，例如透過引入 DevOps (Development and Operations)概念，(軟體開發人員(Dev)、資訊技術(Information Technology, IT)、維運技術人員(Ops)之間的溝通合作)，來運作和分析目前網路營運的核心業務流程和規則。

沖繩開放實驗室(Okinawa Open Lab, OOL)成立於 2013 年，長年致力於將 5G 網路資通安全(5G CyberSecurity, 5GCS)相關技術、軟體定義網路(Software-Defined Network, SDN)開發、網路功能虛擬化(Network Functions Virtualization, NFV)相關功能與雲端計算互相結合，進行具體應用例實現和開源(Open Source)開發，並且是一家全球唯一的研發機構。今年 OOL 快速的將上述趨勢拓展到研究方向，並且擴大了研究領域，致力於資訊與通信科技(ICT)應用領域之數位化網路生態系統開發。在 OOL 營運的 7 年歷史中，相關研究人員進行了下世代網路核心技術研究，開發了相關實驗平臺並進行運作，每年也舉辦了論壇會議，培訓了專業人力資源。另外舉辦國際會議和國際交流，亦研究了實際應用案例和市場調查。OOL 獨特的營運模式，為先進的核心資訊與通信科技(ICT)技術的實際應用和普及做出了貢獻。從 2013 年開始，OOL 一直在致力於將

Okinawa Open Days 論壇會議推向國際，並在會議中展示這些年努力研究的成果。Okinawa Open Days 已經確立了“融合世界變化之開放技術和理念”的精神，提供了數位化技術和市場商業發展、用戶、電信業者、設備供應商、工程師、學生等各種交流機會與分享討論，期待能共同創造出一個新世代的電信網路環境，更可靠、更可信賴的新世代的電信網路使用環境。

壹、 目的

本次前往日本/沖繩參與 Okinawa Open Days 2019 論壇會議，共有來自日本各地區專家、學者、電信商、供應商，近 500 名與會者共同探討 5G 網路資通安全(5GCS)相關技術、軟體定義網路(SDN)、網路功能虛擬化(NFV)相關技術、5G 商用市場應用與垂直服務機會之主要發展趨勢。交流單位包含日本電信通訊商 Nippon Telegraph and Telephone Public Corporation (NTT) Do Communication over the Mobile network (DOCOMO)、日本電信網路商 NTT Communications、日本電氣(Nippon Electric Company, Limited, NEC)公司、日本富士通(Fujitsu)公司等，主要探討日本電信產業鏈於下世代 5G 資通安全保護措施、5G 網路垂直應用服務之發展方向與現況以及相關經驗等。此行能與日本專家、學者、電信商、供應商進行面對面討論與交流，並了解具代表性之電信運營商與設備商於 5G 網路關鍵基礎設施部署、可信任之第三方垂直應用服務提供商構思、商用 5G 網路系統實體架構設計與提供服務之解決方案現況與經驗，作為後續我國資通安全產業推動目標與 5G 網路針對端對端(End-to-End)資通安全測試規範設計參考。因此，本次出國行程主要目的包含：

1. 參加 Okinawa Open Days 2019 論壇會議，就 5G 網路應用服務以及 5G 網路資通安全防護進行面對面討論。
2. 參加 Okinawa Open Days 2019 日本電信業者與設備商會議展場，蒐集日本國內針對 5G 資通安全相關防護措施及其技術發展等相關資訊進行交流。
3. 訪談與交流日本相關業者，如：日本電信網路商(NTT Communications)、日本電氣(NEC)公司、日本富士通(Fujitsu)公司、沖繩開放實驗室(Okinawa open laboratory)等，掌握相關單位對於

5G 資通安全最新研析、實際作為，以利後續法規調適之參考，並持續掌握日本 5G 最新資通安全發展趨勢。

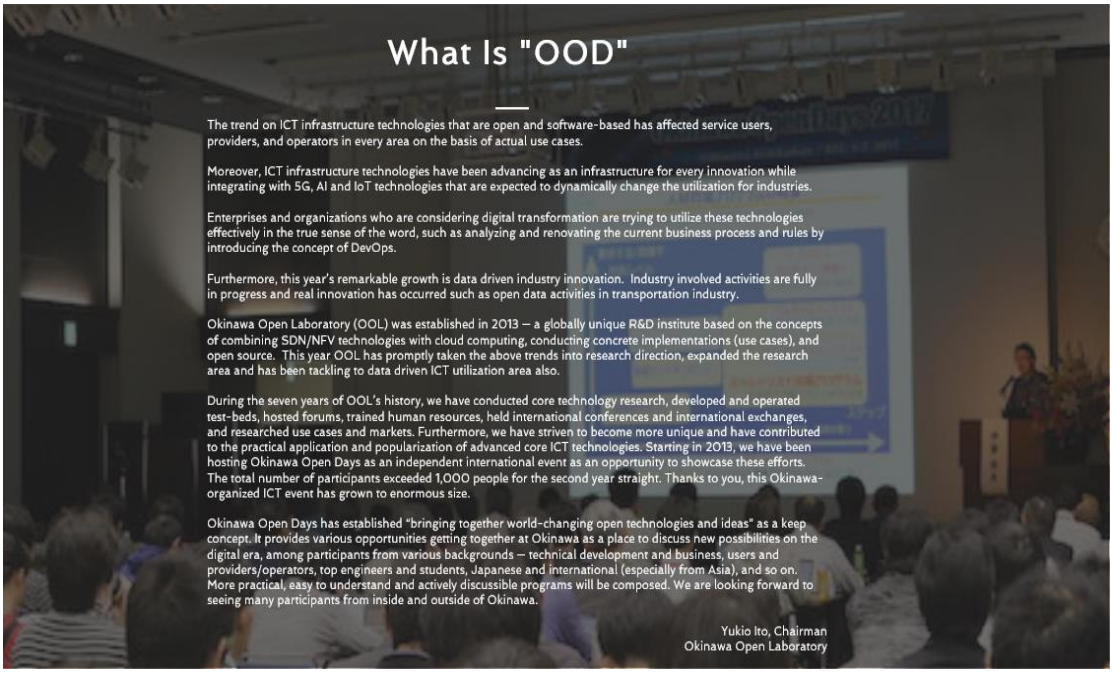


圖 1-1：2019 Okinawa Open Days *論壇會議主題*

貳、 行程

一、 出國時間：108 年 12 月 11 日至 12 月 14 日

二、 地點：日本沖繩

三、 本中心出席人員：吳東興高級工程師、謝仁翔副工程師、李贛麟工程師

四、 時間安排：

日期		行程
Day 1	12/11 (三)	06：55 搭乘長榮 BR112 由桃園機場(第二航站)出發
		09：15 抵達琉球那霸機場(第一航站) 參加 OKINAWA OPEN DAY 2019 會議第三日 【09:00 開場，17:00 第三日議程結束】
Day 2	12/12 (四)	參加 OKINAWA OPEN DAY 2019 會議第四日 【9:00 開場，17:00 第四日議程結束】
Day 3	12/13 (五)	與 NTT DOCOMO、NTT Communications、NEC、Fujitsu 業者交流
Day 4	12/14 (六)	(高雄) 20：00 搭乘中華 CI113 由琉球那霸機場(第一航站)出發 20：50 抵達高雄國際機場(國際航站) (臺北) 20：10 搭乘長榮 BR185 由琉球那霸機場(第一航站)出發 20：55 抵達桃園國際機場(第二航站)

五、　會議資訊：

(一)會議名稱：2019 沖繩開放日 Okinawa Open Day

官網資訊：https://www.okinawaopendays.com/



(二)會議時間：108 年 12 月 09 日至 12 月 12 日

(三)會議地點：日本沖繩縣市町村自治會館 (地址: 沖繩縣那覇市旭町 116-37)

展館資訊：http://mice.okinawastory.jp/zh_TW/venue-foreign/329



(四)會議議程

議程		
12/11	09:30~ 11:30	歡迎辭 伊藤 幸夫 一般社団法人沖縄オープンラボラトリ 代表理事
	09:40~ 09:50	沖繩縣知事致辭 代読:松永 享 沖縄県 商工労働部 産業振興統括監
	9:50~ 10:20	來自垂直的技術創新，可實現資訊通信中的開放式通信，軟件和民主化 中尾 彰宏 東京大学
	10:50~ 11:20	對本地 5G 的期望和擔憂本地 5G 的夢想！？ 中村 修 慶應義塾大学
	11:20~ 11:50	SD-WAN：殺手級應用程序，特洛伊木馬，邊緣平臺 Dan Pitt Senior Vice President at MEF
	13:00~ 13:30	DOCOMO 的 5G 時代行動與願景 太口 努

		株式会社 NTT ドコモ
	13:30~ 14:00	軟銀針對 5G 的舉措 古川 大介 ソフトバンク株式会社
	14:00~ 14:30	5G 帶來的數位化轉型：北美的前景和對開源的期望 Richard L. Colter 富士通（株）/ Fujitsu Network Communications, Inc
	15:00~ 15:30	交通控制為 5G（NW 切片/ MEC） 田中 宏茂 NTT コミュニケーションズ株式会社
	15:30~ 16:00	OSS-基於狀態的最先進的解決方案框架的開發和利用它（OpenMSA）成果 辻川 公章 日本電気株式会社
	16:30~ 17:00	free5GC: free the cellular core networks Dr. Jyh-Cheng Chen Chair Professor of National Chiao-Tung University
12/12	09:30~ 10:00	沖繩縣旅遊二次交通改善項目的未來 山崎 里仁 一般社団法人沖縄オープンラボラトリ
	10:00~ 10:15	沖繩旅遊 DX 瀬底 幸江 沖縄ツーリスト株式会社　地域産業支援室　マネージャ
	10:15~ 10:30	南城的 N 巴士與開放數據的利用 當山 弘哲 南城市役所 企画部情報推進課 係長
	11:00~ 11:30	公共交通的未來創造的開放數據 神田 佑亮 呉工業高等専門学校
	11:30~ 12:00	ResorTech 沖繩 柴崎 貴史

		一般財団法人 沖縄ＩＴイノベーション戦略センター
	13:00~ 13:30	傳統技術人員談論開源引領的創新現實 江藤 圭也 富士通（株）/ Linux Foundation フェロー
	13:30~ 14:00	數位雙胞胎計算 藪下 子 日本電信電話株式会社 NTT メディアインテリジェンス研究所
	14:00~ 14:30	在物聯網平臺 FIWARE 中利用 FaaS 的努力 坂本 諒太 TIS 株式会社 / 一般社団法人沖縄オープンラボラトリ 安座間 勇二 NEC ソリューションイノベータ株式会社
	15:00~ 15:30	用於網路運營自動化的 AI / ML 用例 宮本 達史 KDDI 株式会社
	15:30~ 16:00	從 RPA 開發人員的角度來看 RPA 機器人的可靠性 鄒曉明 株式会社 ドヴァ
	16:30~ 17:00	軟件時代的 IT 基礎架構人員 関谷 勇司 東京大学 / 一般社団法人 高度 IT アーキテクト育成協議会

參、 會議過程及內容

一、 主題演講（Keynote）

(一) 專題演講：DOCOMO 的 5G 時代行動與願景 (5G 時代に向けたドコモの取り組みとめざす世界)

NTT docomo 企業計畫部數位營銷推進室總經理太口努提到，在 5G 時代，與各種合作夥伴合作創建新業務非常重要。NTT docomo 的動作並非日本最快，但身為日本甚至是全球最具規模的電信業者，NTT domoco 追求的是如何利用 5G，徹底改變人類社會的生活品質。「關於 5G，我們思考的是與夥伴合作，一起為用戶創造價值核心體驗。」舉例來說，使用 5G 科技來協助解決日本當前的社會問題，就是 NTT docomo 的方向之一。例如今年五月底，與京都府的智慧城市合作協議內容中，就納入了協助推廣和散步旅遊資訊、健康照護、教育議題納入，而在 311 大地震之後的日本東北重建，也是 NTT docomo 的主要投入場域之一。

既然地方重建(創生)都需要與地方政府協力，在商業上當然更需要與夥伴合作。在與企業的合作方面，也可望加速全新服務的推出。比如因應少子化帶來的現場勞動力不足問題，傳統上需要大量人力的建築業，就成為迫切改革的對象。NTT docomo 與小松製作所、大林組等業者合作，推出建築業的 IoT 平臺，目標把 IoT 的可視化、分析/最佳化技術應用在建築現場中，期望能實現最終的自動化。

另外有關商轉規劃，NTT docomo 已在 9 月與在日本舉行的橄欖球世界盃（Rugby World Cup）合作，使用商轉相同的 5G 基地臺與電波頻段進行賽事轉播的試營運，同時測試大規模體育賽事的訊號傳輸能力；在東京、名古屋、大阪的 4 家 DoCoMo Shop 與世界杯橄欖球

賽的比賽會場將有 5G 訊號，到現場觀看比賽的球迷，可以從手機上看到多角度、高畫質的實況轉播。而 NTT DoCoMo 的 5G 商轉，預訂於 2020 年春天展開。本週 20 日起跑的實驗性服務也被視為正式開臺。朝著商用化的目標努力，NTT DoCoMo 也致力於企業間合作，盼藉此加速推出利用 5G 的新服務。

NTT Docomo 也發表了多款終端，包含索尼 Xperia 1、LG V50 ThinQ、三星 Galaxy S10，以及夏普的室內 5G WiFi 路由器，同時並介紹不同的應用方式；像擁有雙螢幕的 LG 5G 手機可在一個螢幕觀看賽事轉播，而在另一個螢幕則以多重視角來觀賽。

另外 5G 網路的建設也將提前，預計 2020 年 Q2 底前，將在全日本 47 個行政區全面裝設 5G 基地臺。目標到了隔年將完成 1 萬個 5G 基地臺安裝，到 2024 年將超過 2 萬六千個基地臺的長期建設。

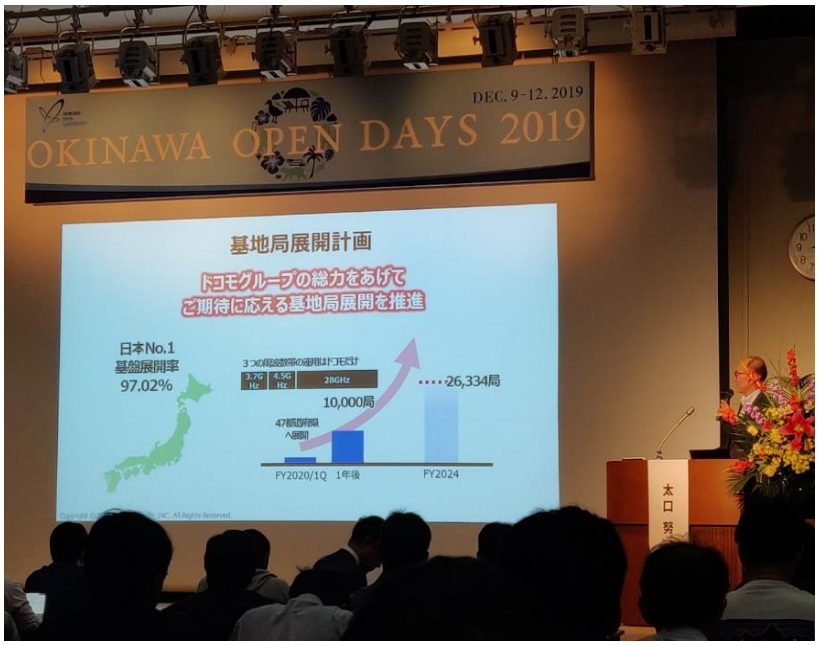


圖 3-1-1 主題演講現場：DOCOMO 的 5G 時代行動與願景

(二)專題演講：軟銀針對 5G 的措施（5G に向けたソフトバンクの取組み）

演講者軟銀科技工程部網路系統部 NFV 推廣部總經理谷川大介則針對 5G 所帶來的變革進行說明；軟銀 Softbank 期待 5G 的實際應用將創造日常生活更加便捷和安全的服務。軟銀計畫通過即將到來的 5G 和 IoT 時代的實際場域測試，開闢各種新的商業應用模式；例如 AI，IoT，智能汽車，機器人和 VR，並將服務商業化。首先是 VR、AR 和 MR（現實與虛擬現實的融合）應用，可以通過利用實現低延遲、高速和大容量的 5G 環境以多種方式應用；預計該技術將在科學研究，醫療保健，產品開發，製造和旅行模擬等各個領域發揮積極作用。

實際實驗案例是在 International Basketball Games 2019 賽事中提供 5G 預服務；這是一種透過 5G 網路傳輸結合 VR/AR 技術以大幅提升觀看體驗。軟銀在日本 Sa 玉超級競技場（Sa 玉市中央區）的特定目標上安裝攝像機拍攝現場賽事並提供即時影像，戴著 VR 頭戴式耳機的客戶可以從三個不同位置（場邊和兩個籃筐目標）欣賞賽事，同時根據不同場景自由切換；此外當安裝 AR 眼鏡時，從觀眾席觀看的實際賽場的頂部會疊加顯示額外的豐富資訊，從而提升觀看體驗。因為 3D 影像的傳輸資訊量至少是 2D 的 5 倍，必須使用 5G 高傳輸速度才得以實現。

SOFTBANK 旨在通過演示實驗從事研發，不斷積累專有技術與經驗，目標在實際快速大量部署的 5G 商業環境中也能實現提供穩定服務的目標。

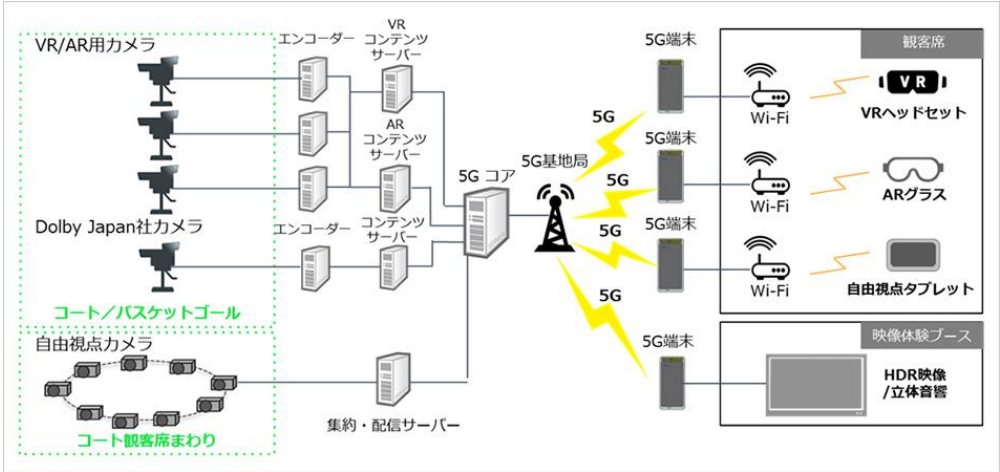


圖 3-1-2 主題演講：SoftBank Basketball Games 5G 預服務與 AR/VR 系統

(三)專題演講:5G 帶來的數位化轉型:北美的前景和對開源的期望（5G がもたらすデジタルトランスフォーメーション：北米における展望とオープンソースへの期待）

演講者是富士通網路通信公司戰略規劃總監 Richard Colter 指稱，在 5G 即將到來的數位化時代，現今企業和市政都正在進行數位化轉型；這將帶來新的商務模式、運營效率和客戶參與方法，而這些新的創新應用都需要 5G 網路來提供必要的容量、低延遲和可靠性。參考北美市場一些關鍵案例，結合行動通訊網路的物聯網應用將是企業數位轉型之關鍵基礎；預期到了 2025 年，28%的物聯網都將使用 5G，而 56%的物聯網都將使用專網提供服務，而全球的 IoT 專網的市場規模更將達到 1.1 萬億美元。

而在美國，他舉了一個實際案例，結合攝像頭 CCD、專用雲端網路與邊緣運算的大都會路邊停車系統應用將可大幅提升使用效率，減少佔位衝突或空閒、增加收益；而且物聯網專用網路使用開源 Open Source 將提供以下好處：可以選擇最適合的方案元件、降低被廠商綁死的機會、提供快速更新的產品生命週期等。

最後的結論是不管是智慧運輸、智慧工廠、以及智慧環控等物聯網垂直應用場域，需要透過專用網路及使用開源物聯網架構才是數位化轉型成功的必要條件。

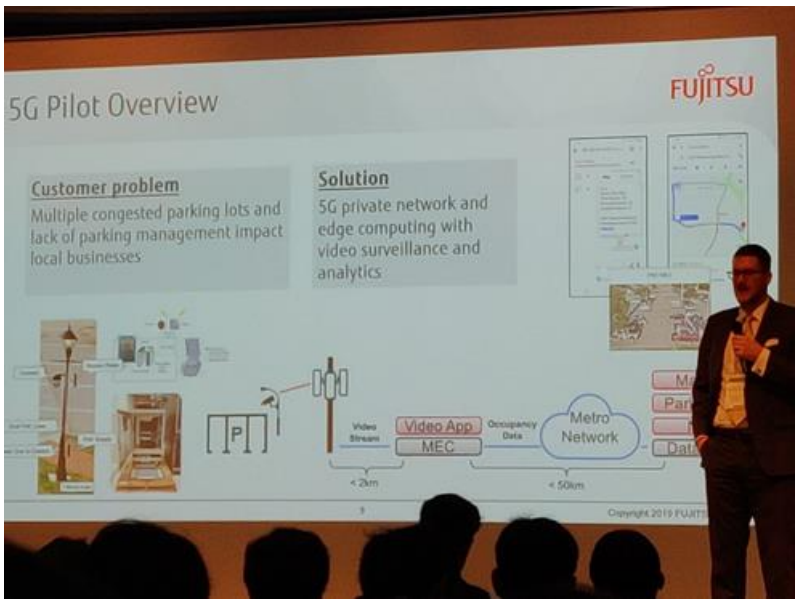


圖 3-1-3 主題演講現場：5G 帶來的數位化轉型：北美的前景和對開源的期望

(四)Free5GC：Free the cellular core networks

演講者是來自基地臺灣交通大學無線網際網路研究與工程實驗室的陳志成教授，他在演講中介紹是 5G 核心網路開源項目的最新成果。他說雖然目前世界上已有一些開源核心網路，但該團隊最新研發的 free5GC 是世界上第一個基於 3GPP 標準所開發之開源核心網路，包括符合 3GPP R15 及後續版本的營運、管理與維護、以及網路切片功能，其最終目標是實現一個完整的商業運營核心網路。

由於完整行動通訊網路非常昂貴，並且獲得設備製造廠商的原始代碼並不容易，對於想要進行開發研究的學術或實驗單位通常只能進行數學分析和模擬來驗證他們的想法；透過成立如 Reconfigurable Core（REC）與 Service Level Virtualization （SLV）等專案計畫並累積多年

努力後，已初步完成具備軟體化及虛擬化特性的 free5GC 平臺，研究人員不僅可以免費獲取原始代碼，而且可以在真實的核心網路環境中進行自己的實驗，另外 free5GC 可用相對低廉的成本作為驗證產品平臺，協助有意投入該領域的 ICT 產業進行相關 5G 通訊產品的開發與測試，這對 5G 產業的發展至關重要。

最後也是最重要一點，透過 free5GC 結合小型開源基地臺，將能夠提供垂直產業建置與管理專有行動網路，並可提供更多服務應用產業，如 AR/VR、8K 高畫質影像傳輸、與專屬車載行動網路服務等，打破行動通訊只有被少數巨頭設備製造商、電信營運商所控制的狀況，透過共通硬體和開源軟體降低開發和銷售門檻的商業模式，這將創造更多商機、使整體行動通訊市場繁榮起來。



圖 3-1-4 主題演講現場：Free5GC：Free the cellular core networks

(五)專題演講：數位孿生（Digital Twin）計算 (デジタルツインコンピューティング)

演講者日本電報電話公司 NTT 媒體情報實驗室的藪下浩子一開頭就提及，隨著 ICT 技術的發展，人類和事物的數位化正在交替創新，已經實現了將現實世界與網路空間連接起來的「數位孿生」（Digital Twin），並期望通過結合人和物來實現數位化應用的爆炸式增長，而且初步成果已經引起製造與應用服務產業的關注。數位孿生是一種精確表示諸如機器零件之類的事物特徵（例如形狀、條件和製造過程）的數位化資訊。舉例來說，人類的數位資訊就是從醫療設備（電腦斷層掃描）獲得的影像和資訊。NTT 所提出數位孿生計算（Digital Twin Computing：DTC）平臺是數位孿生概念的進一步衍生，它的特點是通過使用「數位孿生操作」在網路上不受限制地重建現實世界中的人事物並與之互動，其目的是將反映真實世界的大量高精度數位化資訊結合在一起，以合成各種虛擬世界並產生新穎的服務應用於未來實際社會。

儘管常見的數位孿生主要用於數位資訊觀測或對物理對象的控制，但 DTC 未來可針對各種社會問題和創新服務提供解決方案，包括發現和解決城市問題、疾病的預測與控制、多方面的個人決策、乃至於大到在地球和外太空尺度上的模擬實現。NTT 認為與各行各業合作對推廣 DTC 概念與實際應用至關重要，目前 NTT 正在 DTC 創新論壇上尋找合作夥伴一起創建 DTC 未來的發展與應用。



圖 3-1-5 專題演講現場：數位雙胞胎計算

(六)利用 FIWARE 結合 FaaS 模式在物聯網平臺的應用（IoT プラットフォーム FIWARE における FaaS の活用に向けた取り組み）

來自投入沖繩開放實驗室的 TIS 公司坂本良太與 NEC 解決方案創新部的風間雄二在本段演講中共同介紹開源技術 FIWARE 結合 FaaS 在雲端平臺的發展現況，以及在 IoT 上的實際應用成果；物聯網開源平臺 FIWARE 是一個由歐洲基金資助的獨立開放社群組織，透過開放原始代碼平臺組件的加速框架，可加快智慧化物聯網解決方案的開發，具備使用開源軟體（OSS）、符合標準化 API（NGSI）的組件、以及可以彈性組合所需組件三種特性的物聯網開源平臺 FIWARE 已逐步達到成熟階段，實現無需構建和維護相關基礎架構，以及需要廉價、快速、輕量級部署的功能即服務 FaaS 的雲端計算服務應用。目前也在全球陸續出現實際案例，分別應用於在工業生產、智慧城市、和公用事業項目。

現階段沖繩開放實驗室 OOL 透過實現 FIWARE Orion 通用 API 開發，推出專用於 FaaS 和 FIWARE 管理界面 Meteoroid 開源軟體共通平

臺，結合 OpenWhisk、操控介面 CLI、以及 Docker Compose 構建模組，已成功完成多種異質物連網終端與後端應用服務平臺整合，目前 FIWARE 即用型服務已在沖繩啟動 PoC 實驗，並由 NEC 推出「智慧城市開放平臺」，已經應用於在交通監控、環境安全、和公用事業等項目。



圖 3-1-6 專題演講現場：利用 FIWARE 結合 FaaS 在物聯網平臺的應用

二、 業者訪談（Interview）

本團隊研析各國政府單位對於 5G 網路發展與安全議題之相關作為、研究與建議，旨在協助本國政府推動通訊網路產業之穩定成長，最大化國家社會利益與人民福祉，除了透過網路研析相關資料外，特地於此次參與 Okinawa open days 的研討會中與 NTT Communications 裡的技術開發部門人員以及 Nippon Electric Company (NEC)裡的網路高級工程師進行針對 5G 網路發展與安全相關議題意見交流，極其榮幸有機會可以與兩大業者交換各自發展狀況、看法、研究成果等意見交流，在得到寶貴的意見之外，另一件重要的事情是建立了雙方未來可以合作的橋樑。

(一) NTT Communications：

NTT Communications 隸屬於 NTT 集團，為全日本規模數一數二的資通訊網路產業公司，在面對 5G 網路的崛起，NTT 集團當然投入

了大量資源，為的就是可以讓日本在 5G 網路產業中不失國際競爭力，同時也創造社會利益。此次與 NTT Communications 技術人員談論到了 5G 網路的兩個議題，分別為：

5G 網路將會推動上下游供應鏈的多樣性與複雜性，身為網路服務提供者，如何掌握 5G 系統所帶來的龐大上下游供應鏈生態系，且如何確保網路設備安全，驗證設備是否達到供應商所宣稱之資安防護功能？且 5G 網路服務勢必會有許多第三方服務提供者的加入，如何落實委外服務管理？

NTT Communications 身為日本最大網路服務提供者，除了遵守日本政府的各項規範之外，對於上下游供應鏈的管理在公司內部亦有制定一套標準，並確實落實這套標準，除此之外在上設備商的選擇上，NTT Communications 會盡量選擇國內的設備供應商，也特別強調不會向有任何資安風險疑慮的設備商購買設備，例如中國設備商。另外在購買設備時，會參考這家設備商本身以及其生產的設備是否有符合國際組織所發佈之規範，如 3GPP、GSMA 等，並且是否有取得認證，當然這些認證只是作為公司選擇設備商的一個參考依據，NTT Communications 在公司內部亦有制訂出一套網路設備安全與功能保障規範，且也有成立內部的設備測試實驗室，原則上，不管這個設備商或是設備有沒有取得國際認證，這些設備都必須先經由 NTT Communications 內部的測試實驗室根據內部測試規範來測試通過之後，才會考慮使用，通過內部測試後在設備部署的過程中，第一步會先小區域部署，並經過一連串穩定運作測試後，才會開始大規模部署。

一個網路系統中必定由許多軟、硬體設備組合而成，當這些設備的供應商發布軟體、韌體更新時，身為網路服務提供者如何面對更新

與部署、組態變更之控制管理等安全防護，其管理與因應措施、流程為何？預計要多少時間才可以完成全面更新部署？

當軟、硬體設備商發佈更新時，NTT communications 會先評估這個漏洞更新的影響層級、範圍、以及設備狀態，如果影響層級的風險不大，且範圍小，若再加上設備老舊，則可能不會進行更新以防網路服務中斷之風險，反之，若評估後為必要之更新，會先在內部實驗室進行更新測試，如有必要會尋求設備供應商提供技術支援以整合現有網路系統之組態，待測試通過後，開始進行小區域部署，一旦小區域更新後可以穩定運作將會開始大規模更新，整個流程時間視情況而改變，大約一到三週不等。

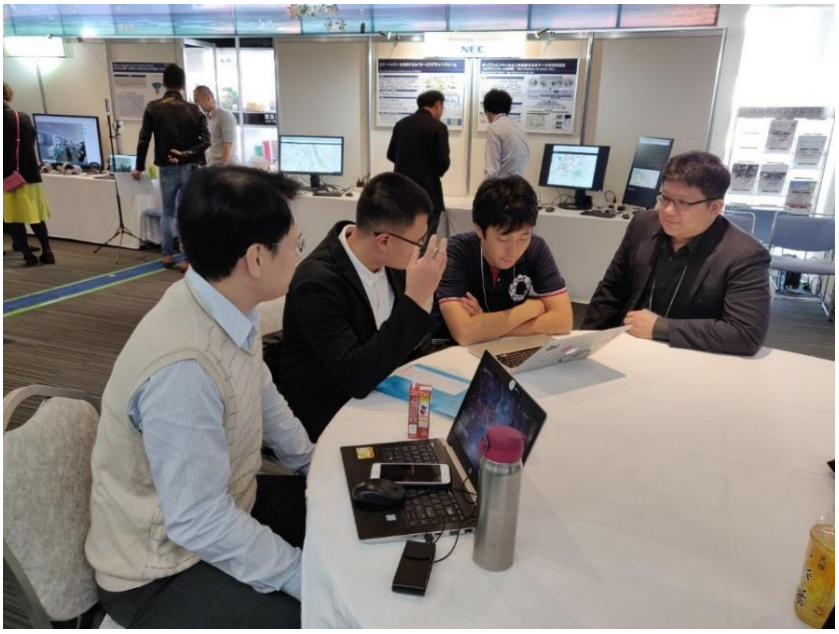


圖 3-2-1 業者訪談現場-供應鏈管理：NTT communications



圖 3-2-2 業者訪談現場-軟體更新部署：NTT communications

(二)NEC (Nippon Electronics Company)：

NEC（日本電氣公司）為日本的跨國電子資訊科技公司，主要為通訊產業以及政府提供資訊科技和網路服務，作為跨國網路資訊科技的公司，同樣地也針對 5G 的發展投入了大量的資源，面對美國對中國設備商的禁令，使得 NEC 期望能夠以地主優勢，站穩相關電信設備市

場，與其人工智慧、物聯網、雲端平臺等結合，並產生產業連動，期盼能夠使日本設備商在國內及海外市場重振旗鼓。此次與 NEC 高級工程師談論到了 5G 網路的兩個議題，分別為

近期由於網路產業日趨擴大，資安事件層出不窮，業者在面對資安事故時，如何快速地通報、因應並隔離受害範圍，讓其餘區域繼續運作，以達到 5G 網路服務的強韌性？

對於資安事件的通報與應變機制，日本政府有成立一個官方的情資單位，並呼籲各業者當發生資安事件時，可以通報予官方單位，並官方單位會將情資通知給各業者，另外面對公司內部的資安事件處理措施，NEC 有成立一個網路安全事件應變小組，且也制定一套標準的事件應變流程，平時也會實地演練，當資安事件發生時，網路安全事件應變小組會根據公司內部所制定的標準流程來迅速的通報、應變、解決，並盡可能地維持服務不中斷。

未來 5G 網路的新穎特性，將會帶來非常多創新應用服務，例如智慧城市、自駕車、智慧工廠與智慧醫療等，物聯網時代的來臨會使得我們的世界變成一個方便的數位環境，然而以上種種應用，為了達成某個目的，或是增進網路服務品質等，不論是業者或是第三方服務供應商必定會掌握到到許多用戶資料，業者應如何確保用戶資訊安全與保護用戶隱私？

日本是一個非常注重隱私的國家，日本政府有制定一套保護用戶隱私的法案，NEC 會絕對遵守，此外，NEC 本身對於用戶隱私的保護看法上，會去考量到誰有權限掌握那些機敏性資料，包含 NEC 本身、第三方服務供應商、第三方之上下游廠商，並且也會去注意那些隱私資料會儲存在何處，儲存的地方是否安全，針對上述議題，NEC 內部也規範用戶隱私保護的策略。

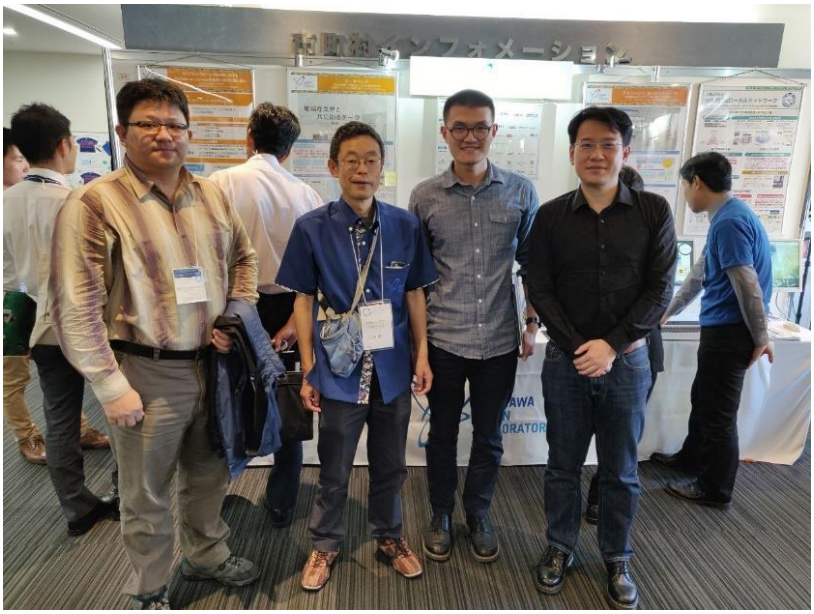


圖 3-2-3 業者訪談現場-資安政策：NEC

(三)NICT：

日本國立研究開發法人情報通信研究機構（国立研究開発法人情報通信研究機構，National Institute of Information and Communications Technology，NICT）於 12 月 6 日撥冗來訪敝公司，故本團隊未安排訪日官方機構行程，並藉由 NICT 此次來訪機會與之討論 5G 相關議題，包含 5G 網路發展以及網路安全，最重要的是也建立了未來雙方可以共同合作的基礎。NICT 是日本唯一一座國家級的 ICT 領域研究單位，為日本總務省（総務省，Ministry of Internal Affairs and Communications, MIC）旗下的一所獨立行政法人機構，總部座落在東京小金井市，成立主要目的為打造健全的資通訊生活環境、促進產官學研的合作、推動國家資通訊產業穩定正向發展、創造社會最高福祉。

5G 網路將會帶來全球 ICT 產業的革命，關係到各方產業的發展以及國家與社會的利益，NICT 作為日本國家級的研究單位，當然也在 5G 網路發展中投入大量資源，此次與 NICT 來訪人員談論 5G 網路發展以及網路安全議題的看法，NICT 目前在 5G 網路的發展中，討論到 5G

網路基地臺的部署，未來 5G 網路將會有大量的小型基地臺，由於小型基地臺的服務覆蓋範圍極小，所以電信業者必須大量部署此一基地臺，以提供高品質網路服務，然而因為成本考量，要密集且廣泛的部署小型基地臺，甚至是部署於室內環境中，並不是一件容易的事，因此 NICT 為解決此上述挑戰，提出了兩個提案，第一個提案為頻譜共享（Spectrum sharing）的機制，頻譜共享的第一個方法為各電信業者可以分享頻譜頻率，分出部份頻率分享給其他電信業者使用，而達到頻率使用最大化，另一個方法為分享基地臺，讓各電信業者可以提供一部分的基地臺資源與其他電信業者共享，而達到基地臺利用的最大效率，以上頻譜共享中的兩種方法均是可以完善網路服務覆蓋率的解決方法之一。另外，NICT 也提出了另一種提案名為微型基地臺電信業者（Micro-cell Operator）的機制，主要概念為可以讓第三方來營運小型基地臺，例如，某地區的所有人都可以部署私人小型基地臺，除了可以架設其專有網路外，亦可以撥分部分頻段與電信業者網路介接，提供網路給社會大眾使用，這樣的合作機制可以降低電信業者建置小型基地臺的成本，且大幅提升網路服務品質。

另一個在 5G 網路安全的議題上，NICT 對於網路情資方面有著值得一提的研究成果，NICT 研究了情資的視覺化，並提供了三種視覺化平臺，包含「NIRVANA 改」、「DEADALUS」與「NICTER」，第一個「NIRVANA 改」平臺可以對於資訊安全監控中心（Security operation center, SOC）所收集的記錄進行視覺化的分析，主要收集進階持續威脅（Advanced Persistant Threat, APT）攻擊的記錄，透過此一視覺化的分析技術，可以讓 IP 所遭受的攻擊種類、以及防火牆之網路攻擊防禦事件變得更清楚明瞭，可以達到網路事件監控之高品質分析的做法。第二個「DEADALUS」平臺也是利用視覺化的技術，從 SOC 中收集暗網（Dark web）的記錄，可以使得 SOC 在偵測到網路攻擊事件時更迅速

地發出警訊。最後就是「NICTER」平臺，此一平臺針對物聯網連接阜的傳輸封包進行分析，以監控封包中是否有任何異常資料傳輸，5G 網路將開啟物聯網時代的革命是眾所皆知的，由此可見日本政府也相當關注未來 5G 物聯網應用的安全，對物聯網裝置的安全提供更上一層的保障。

此次討論了解 NICT 對於 5G 網路以及物聯網的研究投入了不少的心力，談論到 NICT 下一步仍會著重在 5G 網路以及物聯網應用的研究，與之討論了未來可行的合作研究方向，例如情資分享或是網路測試方面的研究領域可以作為未來共同合作努力的目標，雙方也可以合作共同發表論文等，並提到明年如有機會，將會邀請 TTC 相關團隊赴東京參訪，並且盤點雙方在 5G 網路與物聯網的研究上有什麼重複、重要且具體的研究議題，並擬定出後續共同研究議題之參考，除此之外，雙方未來可以考慮簽署 MoU（Memorandum of understanding，瞭解備忘錄）以作為日後合作的基礎。

三、 現場攤位 (Booth) 參觀與意見交流：

(一) Okinawa Open Lab (OOL)：

日本沖繩開放實驗室(Okinawa Open Lab：OOL)是成立於 2013 年 5 月的非營利性組織，其設定目標為：促進下一代資通訊 ICT 平臺技術的實際應用和宣傳，包括軟件定義網路（SDN），網路功能虛擬化（NFV）以及使用開源軟件（OSS）的雲計算。由於近年來 ICT 發展快速，在行動通訊產業湧現出許多新的基礎技術;然而另一方面，相關的應用程序及軟體發展滯後，許多問題亟待提供測試、改進和發展，以滿足提供商和最終用戶的需求用戶。為了彌補這個差距，沖繩開放實驗室積極與工業界和學術界合作，邀請工程師們以開放的方式加入我們的研究與開發，並利用沖繩作為通往亞洲的門戶的獨特地位，為

全球研究活動提供了論壇，並舉辦了一系列的國際會議和技術研討會。而這些工作的成果被公開揭露，以促進下一個項目的實際實施和宣傳。

在 Okinawa Open Day 2019 期間，OOL 展示了以 OSS（自由軟體）Open Stack 為基礎架構開發的雲端系統(Open Stack 也被 NTT 通信公司和 NEC 雲端企業所使用)。OOL 開發測試平臺並用於 Openstack 和 SDN 相關的測試、驗證、研究等。雲端開發業者可以使用遠程模式選擇裸機資源，來設計拓撲架構和部署 Openstack 與其選定的 SDN 元件。OOL 的展示基本上都圍繞在 Open Source 所開發的各式各樣應用，其中一個展示項目是利用影像結合 AI 來判定被拍攝者之年齡，現場經我們實際測試並詢問後，得知其精準度主要依賴充足的資料庫收集樣本數量。

現場主要展示了透過開源平臺 FIWARE 所進行的物聯網（IoT）研究成果；經過多年的努力，OOL 結合 FIWARE Orion 這個 API Context Broker，已成功完成不同種類 IoT Sensor 與後端平臺的整合，達到功能即服務 FaaS (一種類雲計算服務，提供一個讓客戶開發、運行和管理應用功能的平臺，而無需構建和維護相關的基礎架構，通常在構建微服務應用程序時使用。）的成熟應用，實現符合像物聯網這種需要廉價、快速、輕量級部署的無伺服器架構方法。目前 FIWARE 即用型服務已在沖繩啟動，並由 NEC 推出“智慧城市開放平臺”，已經應用於在交通監控、環境安全、和公用事業等項目。

在另一個項目則是展示利用市面 RF 套件、x86 伺服主機、以及開源軟體所組成的小型軟體化 LTE 網路，其中整合 eNB 基地臺與 EPC 核心網路於同一個伺服器硬體，經現場詢問，初步可支援十幾個用戶並提供下行達數十 Mbps 的傳輸速度(無 MIMO 與 CA)，可謂小型專用網路的雛形與概念驗證。

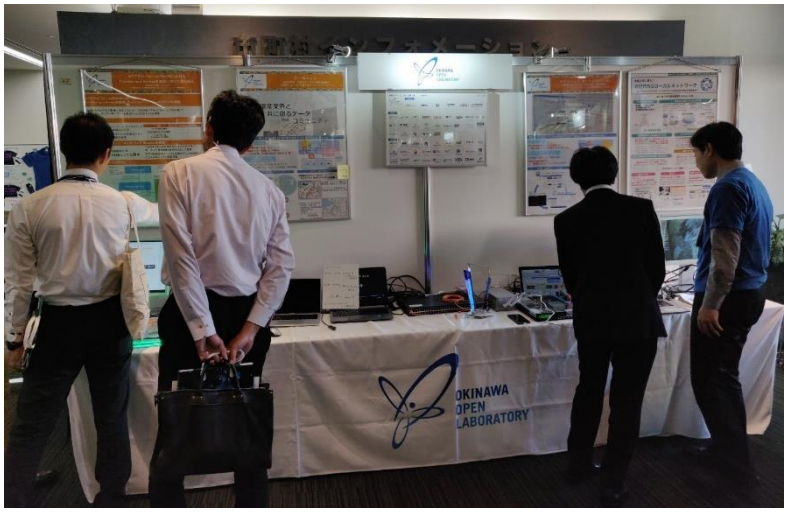


圖 3-3-1 展場攤位：Okinawa Open Lab

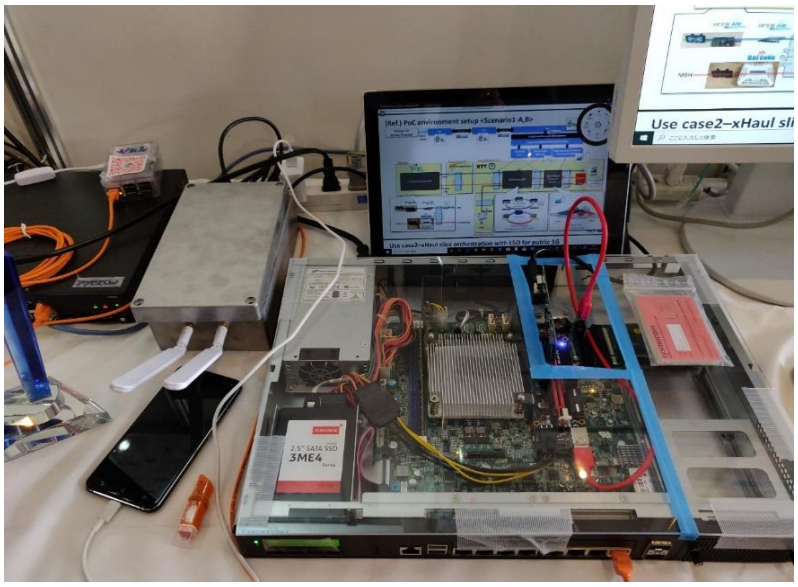


圖 3-3-2 展場攤位：Okinawa Open Lab 開源 LTE 系統

(二)FUJITSU：

富士通在現場的主要展示項目則是利用 OAI(Open Air Interface) Software Alliance、SDR(Software Defined Radio)等概念以及專屬 RF 套件(操作在 sXGP 頻段)、x86 個人主機、以及開源軟體(Ubuntu Linux)所實作組成的小型軟體化 LTE 網路，除整合 eNB 基地臺與 EPC 核心網路於同一個硬體外，另透過專屬 KIBANA 與 ZABBIX 軟體實現網路管理與監控功能，形成完整而商業化的軟體網路系統；其現場宣傳單上

的規格宣稱可支援至六十四個用戶，並可視需要使用更高級的伺服器硬體設備來實現容量與效能擴充，滿足不須執照費用的小型專用網路需求。

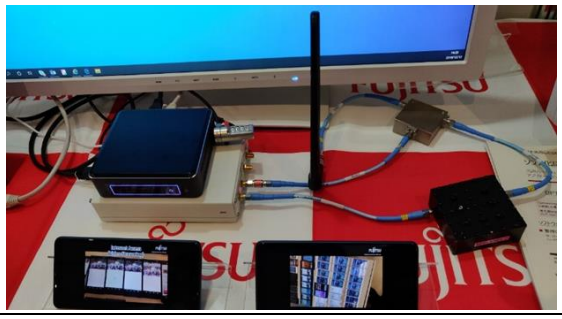


圖 3-3-3 展場攤位：Fujitsu 開源 LTE 系統

此外現場還展示了透過 AI 的動態捕捉攝影技術，能即時分析被攝者最佳拍照瞬間；以及軟件定義的測試環境(Software-Defined Tester)，可以協助客戶的 SDI/NFV 環境穩定運行。該設備實際上是通過專屬開發的硬體加速器 NIC（SmartNIC）結合通用伺服器作為數據封包產生器，結合高相容軟體介面(Python API)並可應用於多種用途，例如開路測試，故障調查，性能測量/監視等。由於該數據封包產器 NIC 可配置於一般便宜的 x86 伺服器，因此可以將低硬件資源花費，與過去專用測量儀器相比，導入測試環境的成本可以降低到 1/3。此外該設備支持從 L2 到 L4 的各種協議（MAC、TCP/IP）以及 TCP/UD 等網路端口處理，並可靈活地增加/修改功能，例如對新協議（VXLAN）和專有協議的支持。



圖 3-3-3 展場攤位：Fujitsu AI 影像捕捉技術

(三) NTT Communications：

該攤位展示了 NTT Communications 正在開發的 Node-AI 概念及初步成果；透過結合 AI 技術的物聯網(AI x IoT)，得以解決以製造業為主的各種客戶業務問題；透過現場人員解說，目前我們目前正經歷著第三次 AI 繁榮期，所有國內外領先的 IT 企業都在加強與 AI 相關的項目，因此這項研究結果也已引起了各個領域客戶的濃厚興趣。

導致 AI 高度發展的因素有三：首先是大數據；隨著物聯網的發展，估計到 2020 年後將有超過上百億臺設備連接到網路，而從這些設備收集的數據量將會非常巨大。第二是處理能力的提高；現在，我們可以處理十年前無法完成的複雜計算。第三是深度學習的技術創新；這項技術大幅改善了語音和圖像識別的準確性。所以現在的情況是我們有潛力應用 AI 來改變各個領域的業務結構。

此外 NTT Communications 正與製造業及政府單位進行合作，包括用於監控垃圾燃燒發電廠的燃燒狀況、以及全日本地震、海嘯、火山災害等預測與異常檢測的實際應用案例，都是透過 AI 結合物聯網進行

深度學習並應用於大數據分析，並透過雲端平臺與 Web 連結執行管控這些複雜過程並以視覺化方式呈現。



圖 3-3-4 展場攤位參觀：NTT Communications

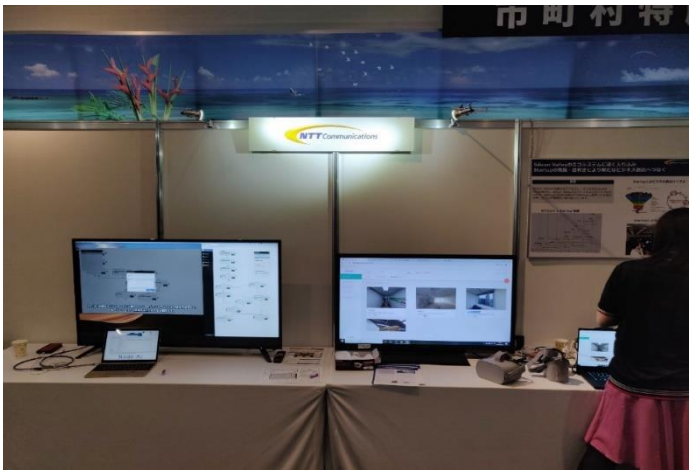


圖 3-3-5 展場攤位：NTT Communication Node-AI

肆、 心得與建議

Okinawa Open Days 主要與 5G 網路安全相關技術、軟體定義網路(Software-Defined Network, SDN)開發、網路功能虛擬化(Network Functions Virtualization, NFV)相關功能以及 5G 商用市場應用與垂直服務機會之國際研討會。5G 行動通訊網路安全相關技術發展，目前正處於從封閉式 4G 網路架構演化到開放式 5G 網路架構之創新技術研究與發展，將為如何保護下一代網路安全是可靠、可信賴的、具隱私性保護等帶來重大的前瞻性革命與經濟利益發展。與會中專家、學者共同熱烈討論 5G 網路威脅、風險、評估等議題，並論及未來 5G 網路時代可能面臨之資通安全挑戰，尤其首先將面臨到之議題為如何克服行動網路電信業者的供應鏈安全問題。會議中先進們指出，大部分的 5G 電信業者很可能因為過度依賴相關供應商所提供的資通安全保護措施，使得日益精進的駭客只需要面對單一防護的攻擊途徑。然而，在未來可預期到數位化的經濟將發展將與 5G 網路息息相關，並成為我國基石命脈，包含通訊、綠能、交通、醫院、銀行、工業、第三方應用服務等，資通安全保護將涉及幾十億物聯網裝置及相關網路系統，因此確保 5G 網路資通安全即是國家安全。

由於開放式之 5G 網路發展將以軟體化網路化為方向，造成軟體漏洞是影響整體資通安全的議題，此原因在於 5G 網路為許多重大 IT 系統之應用基礎，確保 5G 網路之完整性與可靠性將是我國安全首先必須克服的難題。首先，我國 5G 網路電信業者若對不受信任的第三方供應商過度依賴即會造成國安問題，駭客可以利用此被擴大攻擊面輕鬆進行成功之襲擊，因此應與受信任之第三方合作之外，還必須避開單一供應商之風險，此為該供應商是否受信任或受信任之第三方供應商風險指標評估之關鍵要素。政府必須嚴肅的面對該問題，盡速提供不受信任之第三

方供應商黑名單規範，5G 網路業者之基礎設施建置限制，並要求業者進行更進一步資通安全評估審視，另在此次會議中與相關業者談論到資通安全情資分享，日本政府成立一所官方情資中心，主要蒐集來自日本國內、外相關業者之資通安全事件，包含電信業者、產品與服務供應商等，日本國內業者於事件得知或發生時，將於第一時間通報與此中心，然此中心在通報給予相關業者，這樣一來可以大幅降低業者建置情資中心的成本，也可以提升情資流通的透明度，以確保國家 5G 網路安全無虞。

附件五 「5G 垂直應用實證與資安策略國際論壇」紀錄報告

財團法人電信技術中心活動記錄報告

舉辦「5G 垂直應用實證與資安策略國際論壇」紀錄報告

舉辦時期：2019/12/10

報告日期：2019/12/30

摘要

5G 網路架構朝向開放、軟體化演進，這些新技術將會促進各產業及垂直應用服務領域加速發展，是未來智慧化社會的基磐，這些技術的持續成熟與普及將會大幅改變人類的生活方式，然而這個智慧化社會基磐的核心關鍵即是 5G 網路的安全與可靠性，沒有安全，所有的 5G 應用所帶來的數位便利環境都只是空談，如果關鍵核心沒有穩固，往後以 5G 為基礎的智慧化社會都將會是徒勞無功，由此可知 5G 新技術不僅會帶來前所未有的創新與便利環境，但也因為這些開放、軟體化、以及大量服務與創新垂直產業整合的特性，會衍生出許多空前的安全問題。為此，國家通訊傳播委員會與財團法人電信技術中心於 109 年 12 月 10 日於臺大醫院國際會議中心舉辦「5G 垂直應用實證與資安策略國際論壇」，此次論壇包括三大主題，第一實證應用面、第二網路安全面、第三產業轉型面，從上述這三大主題來探討 5G 發展的各個面向，讓各方了解到 5G 所帶來的垂直應用創新、5G 多元應用的商業模式以及可能面臨的資安挑戰進行深度交流。會中邀請許多國內外專家學者分享從理論到實證的經驗，一步一步剖析各個面向所面臨的風險與挑戰，並且最後與各位專家透過討論交流的方式來分享各方的知識與經驗，同時也更近一步了解相關業者的實際作法。

壹、 目的

5G 網路是目前全球各個國家角逐競爭的發展重點，為了讓臺灣在這場 5G 趨勢中搶得先機，提前佈局 5G 產業，並促使 5G 發展，本案計畫團隊與通傳會在 5G 釋照起跑日（2019 年 12 月 10 日）舉辦「5G 垂直應用實證與資安策略國際趨勢論壇」，邀請多位國內外資通安全專家與會，包含產官學研各界人士共同以各自經驗研討 5G 相關議題，冀望 5G 相關產業、垂直應用服務能夠健全正向發展，並建立安全可靠的 5G 服務環境，達到安全、可信賴且具強韌性之 5G 系統，以確保 5G 系統資安規範與國際接軌，針對 5G 系統新興挑戰，協助電信業者提升 5G 應用服務資安防護能力，並有能力提供一流服務使我國用戶與國家能享受頂尖體驗、帶動經濟產業並兼顧安全。

貳、 論壇資訊

一、 論壇名稱：5G 垂直應用實證與資安策略國際論壇（5G What is next? Vertical Applications and Cybersecurity）

二、 官網資訊：
http://bw.businessweekly.com.tw/event/2019/5G_WhatisNext/

三、 舉辦時間：108 年 12 月 10 日

四、 地點：臺大醫院國際會議中心 4 樓（地址：臺北市中正區徐州路 2-2 號

五、 會議議程：

此次議程主要分三大主題：①做實證、②顧資安、③促轉型：

表 1、做實證議程（401 室）

時段	講題主題、講者與對談人
09:00~ 09:30	會議報到 Registration
09:30~ 09:40	開場致詞 Opening Remarks 陳耀祥｜國家通訊傳播委員會委員代理主委 蔡志宏｜行政院科技會報執行秘書
09:40~ 10:10	實現 5G 新世界 Bring 5G into Reality Ja Heung Koo 具滋興｜Director, Global Business Uni, KT Corp
10:10~ 10:40	5G 智慧跨界串聯新風潮 The New Trend of Crossover from Intelligent 5G Yoshinori Ohmura 大村好則｜Secretary Genera, 5GMF
10:40~ 10:50	茶敘交流 Tea break
10:50~	5G 網路之安全性挑戰與考量

11:20	Security Challenges and Considerations for 5G Networks Anna Kahre｜Strategic Product Manager for RAN Security at Ericsson AB
11:20~ 12:20	國際 5G 垂直場域實證案例對我國產業的指標性意義 The New Fields of 5G Smart Tech Exploring 主持人：蔡志宏｜行政院科技會報辦公室執行秘書 與談人： Ja Heung Koo 具滋興｜Director, Global Business Unit, KT Corp. Yoshinori Ohmura 大村好則｜Secretary General, 5GM, Japan Anna Kahre｜Strategic Product Manager for RAN Security at Ericsson AB 劉嘉凱｜智庫驅動股份有限公司執行長 呂新科｜臺北市政府資訊局局長 陳志仁｜野村總合研究所副總經理

表 2、顧資安議程（402 室）

時段	講題主題、講者與對談人
13:30~ 13:40	開場致詞 Opening Remarks 孫雅麗｜國家通訊傳播委員會委員
13:40~ 14:10	5G 應用風險分析 Risk Analysis of 5G Applications 萬幼筠｜勤業眾信聯合會計師事務所執行副總
14:10~ 14:40	國際 5G 資安發展趨勢 The Global Trend of 5G Security Dr. Silke Holtmanns｜NOKIA Bell Labs 國際 5G 資安專家
14:40~ 15:10	5G 網路資安解析 Analysis of 5G Security 游証硯｜思科臺灣首席資安顧問
15:10~ 15:30	茶敘交流 Tea break
15:30~ 16:40	5G 網路的挑戰：新的七大資安議題 The Challenge of 5G: the New 7 Seuciry Issues

	主持人：孫雅麗｜國家通訊傳播委員會委員 與談人： 萬幼筠｜勤業眾信聯合會計師事務所執行副總 游証硯｜思科臺灣首席資安顧問 Dr. Silke Holtmanns｜NOKIA Bell Labs 國際 5G 資安專家 李漢銘｜臺灣科技大學資訊工程學系特聘教授 中華電信代表 臺灣大哥大代表 遠傳電信代表 亞太電信代表 臺灣之星代表

表 3、促轉型議程（402 室）

時段	講題主題、講者與對談人
13:30~ 13:40	開場致詞 Opening Remarks 郭文忠｜國家通訊傳播委員會委員
13:40~ 14:05	迎向 5G 移動新趨勢 - 智慧交通 5G Trend in Intelligent Transportation & Mobility David Oberman｜VP Asia at Innoviz Technologies
14:05~ 14:30	構築 5G 數位轉型新策略 5G Strategy of Digital Transformation 李啓後｜臺灣微軟雲端平臺基地臺事業部副總經理
14:30~ 14:55	5G 時代下的智慧 4.0 Intelligent 4.0 in the 5G Era 王寶慶｜物聯網業務總監，PTC Taiwan
14:55~ 15:15	茶敘交流 Tea break
15:15~ 15:40	翻轉 5G 數位新生活 – 智慧數位內容 丘立全｜啟雲科技股份有限公司執行長
15:40~	企業如何運用 5G 實現產業轉型創新

16:40	How to Achieve Industrial Transformation with 5G 主持人：郭文忠｜國家通訊傳播委員會委員 與談人： David Oberman｜VP Asia at Innoviz Technologies 李啓後｜臺灣微軟雲端平臺基地臺事業部副總經理 王寶慶｜物聯網業務總監，PTC Taiwan 丘立全｜啟雲科技股份有限公司執行長 王揮雄｜文化部資訊處處長 陳銘邦｜基地臺灣諾基亞通信股份有限公司技術總監

參、 會議過程及內容

此份報告摘錄顧資安場次中的三場主題演講以及一場交流討論：

一、 主題演講（Keynote）

(一)5G 應用風險分析（Risk Analysis of 5G Applications）

不同於封閉式的 4G 系統，只要 5G 系統軟體發布或更新過程中，任何環節的安全政策未落實，就有機會被駭入。勤業眾信聯合會計師事務所執行副總萬幼筠以「5G 時代的資安與風險」分析資安威脅與管理，物聯網是近幾年來備受關注的議題，透過 5G 進一步實現自動化與智慧化，但 5G 的風險課題既深且廣，而 5G 應用滲透各個領域，各國都關注供應鏈的安全議題，甚至涉及兩個政治價值體系的競爭。從近期資安事件案例，萬幼筠說明 5G 從基礎的架構到服務，每個環節都需要資訊安全，尤其是企業數位轉型下的物聯網及雲端服務。

由於 5G 的目標市場與技術融合的企圖相較於 4G，5G 的發展目標野心大的多，電信業者正面臨轉型，5G 的場景就是整合 IT 與 OT 的整合應用，並成為國家與社會之數位轉型重要支柱。5G 比的不只是技術升級，還有垂直整合應用服務。在使用跟管理方面，5G 牽涉到資料跨境傳輸，資通訊安全防護趨勢應重視跨國跨組織合作，萬幼筠提到國家安全問題，5G 所涵蓋的虛擬空間都是國土領域，主權是否被侵犯都是電信商要考慮的問題。未來社會跟 5G 的場域緊密相連，龐大且複雜的資通訊建設，完善的營運管理是安全核心。故 5G 的防護層級應從民生拉高到國家經濟競爭力比拼，這表示國家需要從在經濟與社會層次上的發展數位治理能力

最後講者說明由於通訊系統對國家民生有越來越深的牽扯，故各國開始透過法律法規保護這些利益，違反這些法令也會帶來新的風險：

違法風險。講者提出資安法律與其所要保護之法益的分析，這些資安法規形形色色，但從其法益來看，可以分為四種，第一種為國家法益，係指國家或政府安全、監察與情資調查，例如我國的國家安全法。第二種為社會法益，係指民生關鍵資訊基礎設施的保護，如我國的資通安全管理法。第三種為資料所隱私保護，係指隱私與個人資料保護，例如我國的個人資料保護法。最後一種為犯罪預防，包含電腦或網路犯罪，例如我國的刑法。

(二)國際 5G 資安發展趨勢（The Global Trend of 5G Security）

國際 5G 資安專家 Dr. Silke Holtmanns 現為諾基亞貝爾實驗室技術專家，專責為對通訊系統之安全與風險建立技術解決方案，本此邀請其演說「國際 5G 資安發展趨勢」，Holtmanns 首先以一個生動的例子說明 5G 資安與 4G 時代的差異，她表示 5G 像是一臺精良的賽車，是經特殊設計作為高速競技使用，而若僅採取 4G 時代的安全作為，就像是在賽車上裝設一般房車的煞車系統般的不合時宜。Holtmanns 再說明現行跨國通訊使用的跨國 SS7/Diameter 漫遊網路存在著相當協議老舊且彼此間的連接關係錯綜複雜，導致存心不良的國家或者電信業者可以透過 SS7/Diameter 漫遊網路進行位置或詐欺攻擊，雖然 5G 在設計之初已經試圖解決這個本質為身分驗證機制不足的問題，但她相信同樣的問題也會以不同的形式出現在 5G，例如 Rest API 安全或者網路節點的存在系統漏洞。Holtmanns 也給出一些可行的應對技術辦法，例如監控網路流量，採用 SS7/Diameter 防火牆等，但她也認為除了技術解決方案外，這也需要搭配一些情資交換與合約規範的公私協作行為。最後，Holtmanns 清楚的切分設備供應商與電信業者的資安責任，她將 5G 安全的責任區分為設備的軟硬體安全與營運作業安全。她認為供應商負責的防守範圍是設備的軟硬體安全，包含加解密算法實作安全、供應鏈安全、軟體化元件的安全強化與管理功能實作。而營運商需要

負責營運作業的安全，包含人員背景資格與專業訓練、實體安全、事件處理、資產管理等。

Holtmanns 強調，5G 資訊安全防護需要 IT 與 OT 的協作，從設備供應商提供具安全功能的設備開始，到電信業者的安全營運管理，是一道連續的防禦面。尤其 5G 環境不再封閉，加上網路虛擬化、管理建置更複雜等情況，安全準則跟標準化非常重要。未來 5G 應用範圍廣泛，應隨時做好被駭的準備，防患未然。

(三)5G 安全之路（The Road to 5G Security）

思科臺灣首席資安顧問游証硯分享「5G 安全之路」議題，行動通訊系統的演進融合了其他科技，如雲端技術、OpenData 與 IoT，這也帶來新應用、新商務。在這潮流下，安全技術架構與機制不可或缺，要避免以被動式的應變方法來面對未來的資安事件。5G 通訊網路架構與服務鏈，促成電信業者與各產業的跨界合作，物聯網（IoT）又稱爲 M2M，包含機器對機器（Machine to Machine）、人對機器（Man to Machine）、機器對人（Machine to Man），智慧化連結將促進龐大商機。故 5G 架構的安全挑戰在於第一、物聯網設備內置安全性不足，以及加密通道不抵擋從端點來的攻擊；第二、虛擬化後，威脅面增加，各種虛擬物件的威脅控制管理不易；第三、由於核心網路/邊緣計算/網路切片多採用分佈式建置，威脅面增加；第四、5G 乃多項技術融合，技術之間的威脅會互相遷移蔓延(3G to 4G to 5G)。講者認為應對的策略有四個方向，一、網路能見度(Visibility)管理，二、分區管理(Segmentation)，三、減緩與補救措施(Remediation)，四、威脅防禦(Threat Protection)。

他提到 5G 防禦思維為「零信任架構」，使用不同認證技術強化身份管理，配合各層防護縱深，如安全配置、服務埠盤點、流量監控與存取管控等技術作為來架構疊加防護。講者談到新一代通訊技術發展與

演變，產品弱點攻擊需要自動化管理，許多重大資料外洩都是先滲透進入易受攻擊的伺服器，企業應做全盤風險性的考量，例如將網路分區、隔離並加以控制，定期檢測、分析、防禦並擬定災難應變計畫，打造 5G 與 IoT 安全織網。

最後游証硯提出五個 5G 場景的所應具備之安全設計，這五個場景包含一、SDN/NFV、二、5G 網路零信任能力，三、設備及平臺最基本防禦內容，四、IoT 網路安全防禦，五、一般性的 5G 安全方向。

二、 專題討論（Panel）- 5G 網路的挑戰：新的七大資安議題

5G 系統在架構設計上就是以具備強大功能擴充彈性為理念，以因應未來各種潛在應用服務為目標。因此，不同於 4G 系統架構，5G 系統高程度地將過往硬體為主的網路系統設置模式做大幅的分解，將網路功能軟體化，以達到網路功能的快速擴充與彈性。從運算、存儲及軟體運作的角度，5G 系統將納入更多元與廣泛的資訊技術與通訊技術以及平臺與產品在整體網路運營及服務提供等面向。對電信業者而言，這些新穎的架構與開放除將帶來成本和部署的敏捷性外，同時亦將使得 5G 系統面臨更為複雜與多元之資通安全風險與威脅。

隨著 5G 系統服務逐步走向開放式架構，業者所建置之 5G 系統例如軟體或是服務可能委外辦理或由第三方供應商提供，對於其開發與管理之供應鏈及相關人員，必須要有相當之掌握包含了解影響產品或服務安全級別的元件或軟體之來源及產品開發或供應之上下鏈結的生態系，以及產品和服務之維護、更新與修復的透明度，以降低並能管控可能潛在的資通安全風險。

在未來多重接取邊緣運算架構可能提供第三方服務提供者多重接取邊緣運算服務或是開放允許他們設置相關系統於 5G 系統的網路邊緣，此舉對比於 4G 相對封閉式的網路與系統設置，在資通安全維護上將產生新的風險、威脅及挑戰，如何建立完整有效的整體多重接取邊緣運算資安維護之政策、管理制度與防禦機制是一項新的挑戰。

業者在面對軟體更新與部署、組態變更之控制管理等安全防護時，管理制度上必須考量如檔案更新流程、版本制度、相關伺服器主機維運管理、金鑰安全防護、軟體開發流程、軟體發布與部署環節、安全軟體發展生命週期、軟體供應鏈及整體 5G 系統流程管理等資通安全防護及控制措施，並全面掌握可能發生之威脅、風險及盤點防護面向。

5G 系統架構以能夠彈性並快速支援未來各種可能的新興應用服務為核心，業者在建立安全可靠具強韌性之 5G 服務環境時，除前述資通安全議題外，應確保用戶隱私及資料之安全保護。因此，包含網路管理、服務提供、營運管理及資通安全防護目的，得標者於用戶相關資料之蒐集、儲存、處理及利用應提出用戶隱私及資料保護政策與措施並定期檢視執行績效與妥適性。

肆、 心得與建議

5G 技術驅動各產業與應用服務領域加速創新速度是我國未來智慧化社會的磐石，保障 5G 網路是安全、可信賴、保障消費者隱私是能夠達成智慧化服務的關鍵因素。5G 技術的發展是全球電信服務必經的演進及創新過程，當 5G 結合人工智慧、物聯網、擴增實境、虛擬實境、超高畫質影音、多重邊緣運算、無人機、車聯網等技術成熟後，更成為帶動我國產業轉型的關鍵驅動力。我國預計明年將邁入 5G 服務時代，各種創新垂直應用服務領域的引進同時，將會先遭遇到新的問題與挑戰，例如政府單位如何針對 5G 新創應用服務制定相對應之規範、保障我國消費者隱私安全的電信法規調適、5G 資通安全前瞻性布局模式等。5G 創新產業與服務模式及 5G 資通安全保障的思維，考驗到我國政府單位、電信營運商、設備商、第三方應用服務商、法人研究單位之智慧與解決難題的能力。

一、 從傳統思維到前瞻開放，從封閉走向跨界協作

5G 開放性網路架構朝向網路化、虛擬化、開源化、多重邊緣運算等技術演進，與傳統封閉型 4G 網路架構與其資通安全議題應對截然不同。5G 開放性網路運作將改變全球消費者生活，為智慧化服務 5G 採取大量數據的蒐集與運用，大量數據隱私性保護即為資通安全問題，甚至為國家安全之議題。由於 5G 技術兼具大容量、大連結、低延遲、超高速等優越特性，來自於新設備、新接取方式、新技術功能、新應用情境，相較於傳統 4G 網路架構，5G 開放式網路的攻擊介面自然更多，資通安全威脅相對更高。5G 網路安全不再僅限於通訊安全，還延伸至垂直應用服務之安全，使得使用者資料保護在 5G 網路的重要性遠高於 4G 網路。由於 5G 技術提供服務的同時必須蒐集

大量使用者資料，就資料共享的資通安全措施來說，針對不同使用者應給予不同的帳戶與不同級別的資通安全認證與保障。

二、 資通安全防護即為國家安全防護，居安而思危

5G 網路服務的時代即將來臨，各種垂直應用產業整合的新創服務內容與樣式將大量增加，開放式 5G 網路架構雖然更容易加速這些垂直應用服務的實現與商用化，但是資通安全與消費者隱私保護將是首要面對之挑戰。不同於 4G 封閉型網路運作模式，一旦只要遭遇到 5G 系統之軟體更新或佈達的過程，任何一環節的安全政策沒有真正落實，就會反應在資通安全威脅與風險問題上面。資通安全即是國家安全，在整體 5G 網路使用與管理方面將牽涉到資料跨境傳輸，資通安全防護趨勢將邁向跨國家與跨組織合作。5G 所涵蓋的網路化、虛擬化空間都是國土領域，主權是否被侵犯是我國政府單位、電信營運商、設備商、第三方應用服務商、法人研究單位要負責任的問題，而其中我國電信技術中心的重要性，在於協助國家通訊傳播委員會營造國家使用 5G 的安全環境，並提供資通安全評估指引。

三、 保障 5G 安全可信賴，新興應用成敗之關鍵

5G 網路資通安全對策建立在於資訊安全防護需要 OT 與 IT 整合與協作，從供應鏈安全管理進行根本改善，確保系統不容易被駭客入侵。3GPP 標準安全架構制定使用者雙重步驟驗證機制提升系統安全性，保障使用者個人隱私權益，讓資訊安全多一分保障。5G 網路的威脅風險亦包括網路維運安全、垂直應用安全等議題講， 3GPP 5G 網路標準安全架構設計，可解決過去傳統行動通訊網路存在的第七號信令系統（Signaling System Number 7, SS7）以及 Diameter 存續的端點對端點（End-to-End, E2E）認證缺陷所造成之異常識別，利用偵測隔

離與快速應變機制克服 5G 營運管理所遭遇到的問題。5G 資通安全威脅對產業鏈帶來重大影響，對於社會大眾也帶來新興衝擊。我國政府單位、電信營運商、設備商、第三方應用服務商、法人研究單位應秉持協力與合作的方式，配合國家通訊傳播委員會從終端設備到核心網路各面向制定資通安全防護指引、規劃各垂直應用領域必要的危機處理團隊，擔起營造國家 5G 使用安全責任，增進全民福祉。

四、　制定資通安全策略，邁向數位經濟時代

隨著 5G 網路科技發展，資通安全面臨更複雜環境，防毒工作是保障系統與消費者安全可先著力的地方，不論系統設備、網路平基地臺、軟硬體等都必須建立安全防禦機制。資安即是國安，5G 資通安全代表著世界各國的系統設備競賽，當網路流量加快且容量更大，資通安全防禦首先應先思考防毒措施，尤其 5G 環境開放化、網路化、虛擬化、管理建置更複雜等情況，資通安全準則與標準化至關重要，安全技術架構與機制不可或缺，必須以主動式處理已經發生的資通安全事件，甚至及時偵測/預防可能將發生的資通安全事件、威脅、風險等實際環境狀況。所有潛在的網路安全風險都不容忽視，每一個端點設備/裝置都需要保護，端點設備/裝置弱點攻擊需要自動化管理。大部分的重大資料外洩事件，駭客都是先滲透進入較容易受攻擊成功之伺服器，我國政府單位、電信營運商、設備商、第三方應用服務商、法人研究單位應協力合作完成 5G 全面通盤性之威脅與風險之考量，將整體網路以與妥善區分、適當隔離並加以安全控制管理，定期/不定期執行檢測、及時分析、不斷時全面防禦，嚴制與落實災害應變計畫，打造安全、可信賴、保障消費者隱私之 5G 安全網路環境。