https://doi.org/10.7840/kics.2023.48.4.423

Beyond 5G 및 6G 보안 국제표준화 동향 분석

이 태 양◆, 이 종 혁°

Study on International Standardization Trends of Beyond 5G and 6G Security

Taeyang Lee◆, Jong-Hyouk Lee°

요 약

2019년 4월, 5G가 상용화된 후, 6G는 2030년 상용화를 목표로 기술개발이 이루어지고 있다. 현재 상용화된 5G는 설계 단계에서 최소한의 보안 기능을 고려함에 따라 5G에서 새롭게 도입된 네트워크 구조 및 가상화 기술에 대한 다양한 보안 위협이 우려되고 있다. 또한, 6G는 기존 5G의 네트워크 구조 및 가상화 기술을 일부 계승할 것으로 논의되고 있기에 5G의 보안 위협이 6G에서도 나타날 것으로 우려되고 있다. 이에 따라, 6G에서 발생 가능한 보안 위협을 사전에 연구하고 설계 단계에서부터 보안 기능을 내재화하기 위한 표준 개발이 요구되고 있다. 본 논문에서는 Beyond 5G 및 6G에서의 보안 내재화를 위한 국내외 표준 기술개발 현황을 분석하고 이를 통해 6G 보안 표준화를 위한 기반을 마련하고자 한다.

키워드 : Beyond 5G, 6G, 보안, 국제표준화, 보안 내재화
Key Words : Beyond 5G, 6G, Security, International Standardization, Security by design

ABSTRACT

After 5G commercialization in April 2019, technologies development is underway to commercialize 6G in 2030. As only minimum security functions are considered in the 5G network design stage, concerns are raised about security vulnerabilities and threats due to introduction of new network structures and virtualization technologies. Furthermore, there are concerns that 6G will also inherit the security vulnerabilities and security threats of 5G. Therefore, specifications development is required for 6G security by design. In this paper, we analyze the status of domestic and foreign standard technology development for security internalization in Beyond 5G and 6G, and through this, we intend to lay the foundation for Beyond 5G and 6G security standardization.

※ 이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00796, 상시적 보안품질 보장을 위한 6G 자율보안 내재화 기반기술 연구)
◆ First Author : Dept. of Computer and Information Security & Convergence Engineering for Intelligent Drone, Sejong University, taeyang@pel.sejong.ac.kr, 학생회원
° Corresponding Author : Dept. of Computer and Information Security & Convergence Engineering for Intelligent Drone, Sejong University, jonghyouk@sejong.ac.kr, 종신회원
논문번호 : 202212-309-B-RU, Received December 20, 2022; Revised January 18, 2023; Accepted February 3, 2023

Ⅰ. 서 론

2019년 4월, 우리나라를 시작으로 하여 세계적으로 5G 상용화가 시작되었다. 5G는 4G보다 향상된 핵심 성능 초고속·초저지연·초연결을 달성함으로써 eMBB (enhanced Mobile Broadband), mMTC(massive Machine Type Communications), URLLC(Ultra Reliable Low Latency Communications) 서비스를 제공할 수 있는 인프라 마련을 위해 분산 코어 네트워크 구조 및 소프트웨어 기반 아키텍처 등의 기술을 도입하여 기술적 진보를 보였다. 그러나, 5G는 이동통신 네트워크에 새로운 기술을 도입함으로 인한 다수의 취약점이 존재하며, 보안 위협에 대한 우려가 지속적으로 제기되고 있다. 또한, 5G 표준 개발 단계에서는 보안 취약점을 고려하여 5G 인프라 설계 단계에서 적용되어야 하는 최소한의 보안 기능만을 고려하였으며, 초연결·초저지연 서비스 제공을 위한 보안 기술 규격은 마련되지 않은 실정이다. 이에 따라, 5G 상용화 이후에 발생하는 보안 위협에 대응하기 위한 기능들이 5G 인프라에 추가적으로 도입되고 있다. 이러한 대응 방식은 5G 이동통신 시스템에 보안을 위한 프로세스를 추가하는 것으로 5G가 달성하고자 하는 데이터 처리 속도와 같은 성능 측면에서의 저하를 야기한다는 한계가 존재한다. 또한, 현재의 5G 보안 기술로써는 5G보다 향상된 신뢰성을 요구하는 6G의 새로운 서비스를 지원하는 데에 한계가 있다는 우려가 제기되고 있다.

5G 표준 개발이 완료되어가고 5G가 상용화된 이후, 2030년을 목표로 6G를 상용화하기 위해 6G 표준 개발에 대한 논의가 이루어지고 있다. 6G에서는 5G가 상용화되기까지 해결하지 못했던 한계점을 개선하려는 노력이 필요하다. 특히, 5G에 적용되었던 신기술 및 서비스가 6G에도 일부 도입됨에 따라 5G에서 제기되던 보안 위협이 6G에도 계승될 것으로 예상된다. 이에 따라, 6G에서는 핵심 성능 지표 중 초신뢰를 달성하고 6G 인프라의 최적화를 위해 6G 설계 단계에서부터 보안 기술을 내재화해야 한다는 논의가 이루어지고 있다[1]. 따라서, 6G 설계 단계에서 보안 기술을 도입하기 위한 국제표준 마련의 필요성이 대두되고 있다. 이에 따라, 본 논문에서는 6G 보안 기술에 대한 국내외 표준화 동향을 분석하였다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 국제표준화 기구와 사실표준화 기구로 구분하여 국외의 6G 보안 표준화 동향에 대해 분석한 내용을 소개하고, 3장에서는 국내 표준화 기구의 6G 보안 표준화 동향에 대해 분석한 내용을 소개한다. 다음으로 4장에서 국내외 표준화 기구별 표준화 항목(Work Item)을 비교 분석한 뒤 마지막으로 5장에서 본 논문의 결론을 맺는다.

Ⅱ. 6G 보안 국외 표준화 동향

2.1 ITU-R IMT-2030 보안 표준화

국제 전기통신 연합(ITU, International Telecommunication Union)의 전파통신 부문에 해당하는 ITU-R(ITU- Radio Communication Sector)의 작업반 WP5D(Working Party 5D)에서는 이동통신에 대한 표준을 개발해오고 있다.

해당 국제표준화 기구에서는 이동통신에 대한 표준 개발을 본격적으로 시작하기에 앞서, 이동통신 기술의 동향을 파악하고 해당 이동통신의 비전(Vision)을 세우는 작업을 수행한다. 이에 따라, 2020년 2월 34차 회의에서 6G에 해당하는 IMT-2030(International Mobile Telecommunications-2030) 이동통신에 대한 기술적 동향에 대해 기술한 문서인 IMT-2030 미래기술동향 보고서(IMT-2030 FTT, Future technology trends of terrestrial IMT systems towards 2030 and beyond) 개발을 시작하였고, 2022년 6월 41차 회의에서 해당 보고서 개발이 최종적으로 마무리되었다. IMT-2030의 비전을 설정하는 IMT-2030 Vision 권고(IMT Vision – "Framework and overall objectives of the future development of IMT for 2030 and beyond")의 경우, 2021년 3월 37차 회의를 통해 개발이 착수되었다. 해당 문서 작업을 위해 비전 하위작업그룹(SWG Vision, Sub Working Group Vision)을 신설하여 현재 IMT-2030 Vision 권고 초안을 개발하고 있으며, 2023년 6월을 목표로 개발이 완료될 예정이다. 다음 그림 1은 IMT-2030 미래기술동향 보고서 및 IMT-2030 Vision 권고 개발 일정을 나타낸다[2].

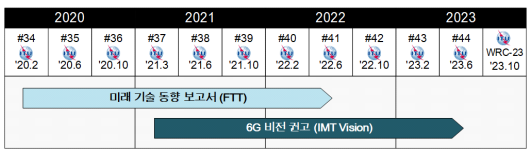


그림 1. IMT-2030 FTT 및 IMT-2030 Vision 권고 개발 일정
Fig. 1. Developing Schedule of IMT-2030 FTT and IMT-2030 Vision

2.1.1 IMT-2030 미래기술동향 보고서

IMT-2030 미래기술동향 보고서는 2021년 10월 39차 회의를 시작으로 목차 정비에 대한 논의가 이루어

표 1. IMT-2030 FTT 목차
Table 1. Contents of IMT-2030 FTT

Chapter	Title	Contents
4	Overview of emerging services and applications	Services, applications, use cases
5	[Emerging] Technology trends and enablers	8 technology categories of new 6G
6	Technologies to enhanced the radio interface	Wireless interface technologies
7	Technology enablers to enhance the radio network	NTN (Non-Terrestrial Network)

졌으며, 40차, 41차 회의를 통해 목차 및 내용에 대한 업데이트가 진행되었다. 표 1은 해당 보고서의 목차를 나타낸다.

IMT-2030 미래기술동향 보고서 4장에서는 IMT-2030에서 등장할 것으로 예상되는 새로운 서비스와 애플리케이션, 유즈케이스에 대한 내용을 확인할 수 있다. 5장에서는 4장에서 제시하고 있는 IMT-2030의 대표적인 서비스들을 실현하기 위한 기술 및 그에 대한 동향을 확인할 수 있다. 6장에서는 무선 접속 기술, 7장에서는 비지상 네트워크(NTN, Non-Terrestrial Network)에 대한 내용을 고고도 플랫폼 기지국에 해당하는 국제 이동통신 기지국(HIBS, High-altitude IMT Base Stations)과 무인이동체(UAV, Unmanned Aerial Vehicles)에 대한 내용으로 한정하여 다루고 있다[3,4].

2.1.2 IMT-2030 Vision 권고

2021년 3월 37차 회의에서 개발이 착수된 IMT-2030 Vision 권고는 39차, 40차, 41차 회의를 통해 목차가 정비되었다. 다음 표 2는 41차 회의에서 정비된 IMT-2030 Vision 권고의 목차를 나타낸다.

IMT-2030 Vision 권고 2장에서는 IMT-2030 관련 동향 및 IMT-2030의 사회 기여 측면, 응용 및 기술 동향, 100GHz 이상 대역에 대한 IMT 기술의 적합성, 주파수 전망 등에 대한 내용이 작성될 예정이다. 3장에서는 IMT가 발전되어온 내용이 작성될 예정이며, 4장에서는 대표적인 IMT-2030 사용 시나리오(Usage Scenario)에 대한 내용이 작성될 예정이다. IMT-2030 사용 시나리오에는 IMT-2020(5G)의 사용 시나리오에 해당하는 eMBB, URLLC, mMTC 보다 진화된 사용 시나리오와 IMT-2030의 신규 항목인 커버리지(Coverage), 인공지능, 센싱(Sensing) 3가지 항목을

표 2. IMT-2030 Vision 권고 목차
Table 2. Contents of IMT-2030 Vision

Chapter	Title
1	Introduction
2	Trends of IMT for 2030 and beyond
2.1	Goals and societal consideration
2.2	User and application trends
2.3	Technology trends
2.4	Studies on technical feasibility of IMT in bands above 100GHz
2.5	Spectrum implications
3	Evolution of IMT
4	Usage scenarios for IMT for 2030 and beyond
5	Capabilities of IMT for 2030 and beyond
6	Additional framework and objectives

포함하여 총 6개의 사용 시나리오에 대한 내용이 포함될 예정이다. 해당 시나리오는 잠정 사항으로 향후 추가 논의를 통해 변동될 수 있다. 5장에서는 IMT-2030 성능에 대한 내용이 포함될 예정이며, 39차, 40차 회의를 통해 제안된 60여 개의 성능 항목이 41차 회의에서 16개의 항목으로 통합되어 차기 회의를 통해 16개의 성능 항목에 대한 추가/삭제 및 정의/목표값에 대한 논의가 이루어질 예정이다. 6장에서는 IMT-2030 기술/상용화/주파수 로드맵에 대한 내용이 포함될 예정이며, 41차 회의에서 6G 타임라인(Timeline)이 확정된 상태이다[5].

2.1.3 ITU-R IMT-2030 보안 표준화 동향

ITU-R에서는 IMT-2030 미래기술동향 보고서를 통해 IMT-2030의 요구사항을 반영하여 발전된 인공지능 기술과 시스템의 신뢰성 및 지속 가능성, 보안성 강화와 다양한 융합 서비스 등장에 대한 내용을 제시하고 있다. 특히, 미래 서비스 구현이 가능하도록 하는 기술 중 네트워크 및 물리 계층 보안 기술의 발전을 통한 IMT-2030 신뢰성 및 보안성 향상을 의미하는 고신뢰성(Enhanced Trustworthiness)을 제시하고 있다. IMT-2030 Vision 권고 또한 신뢰성(Trustworthiness)을 제시하였다. IMT-2020 Vision 권고의 경우, 이동통신 성능에 대한 8가지 중점 항목을 채택하였으나, 보안은 포함되지 않았다[6]. 그러나, IMT-2030 Vision 권고에서 중점 성능 항목으로 신뢰성을 고려하고 있는 것으로 보아 IMT-2030 표준화를 통해 IMT-2020 대비 향상된 IMT-2030 보안을 목표로 정량적/정성적

표 3. IMT-2020 및 IMT-2030의 중점 성능 항목
Table 3. Key Capabilities of IMT-2020 and IMT-2030

IMT-2020	IMT-2030
Peak data rate	Peak data rate
User experienced data rate	User experience data rate
Latency	Latency
Mobility	Mobility
Connection density	Connection density
Area traffic capacity	Area traffic capacity
Spectrum efficiency	Spectrum efficiency
Energy efficiency	Reliability
-	Coverage
-	Positioning
-	Sensing
-	AI
-	Availability/Scalability
-	Trustworthiness
-	Sustainability
-	Device lifetime/power

목표치가 정의될 것으로 보인다. 표 3은 IMT-2020과 IMT-2030의 중점 성능 항목을 비교하여 정리한 것을 나타낸다. 이에 따라, ITU-R의 IMT-2030 Vision 권고 개발을 통해 IMT-2030의 정량적/정성적 보안 목표치가 정의되는 경우, 다른 표준개발기구(SDO, Standards Development Organization)에서도 해당 보안 목표치에 따른 표준 개발이 중점적으로 이루어질 것으로 보인다.

2.2 ITU-T IMT-2030 보안 표준화

국제 전기통신 연합의 전기통신표준화 부문에 해당하는 ITU-T(ITU-Telecommunication Standardization Sector)는 SG13(Study Group 13)의 포커스 그룹 (FG NET-2030, Focus Group Technologies for Network 2030)을 설립하여 IMT-2030에 대한 사전 연구를 수행하였으며, SG17(Study Group 17)을 통해 네트워크 인프라 및 서비스 애플리케이션의 보안을 위한 연구 및 표준화를 수행하고 있다.

2.2.1 ITU-T SG13

SG13은 차세대 네트워크에 대한 연구 및 표준화를 위해 2018년 7월 제네바에서 개최된 회의에서 FG NET-2030을 설립하였다. FG NET-2030은 2030년 및 그 이후에 등장하게 될 네트워크의 성능 및 차세대 네트워크 시나리오에 적합한 아키텍처와 메커니즘을 탐색하는 것을 목표로 NET-2030(6G)에 대한 연구를 수행하였다. FG NET-2030의 활동은 2020년 7월에 완료되었으며, 8개의 연구 결과물을 도출하였다. 다음 표 4는 FG NET-2030의 연구 결과를 나타낸다.

2.2.2 ITU-T SG17

SG17은 2018년 3월에 IMT-2020 보안 표준 개발을 착수하였다[7]. ITU-T는 4년을 주기로 세계전기통신표준화총회(WTSA, World Telecommunication Standardization Assembly)를 개최하여 구조조정, 의장단 선출, 표준화 추진 방향 수립 등에 대해 논의한

표 4. FG NEF-2030의 연구 결과물
Table 4. Deliverables of FG NET-2030

Type	Title	Publication Date
White Paper	Network 2030-A Blueprint of Technology, Applications and Market Drivers Towards the year 2030 and Beyond	2019. 05
Deliverable	New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis	2010. 10
Technical Report	Representative use cases and key network requirements for Network 2030	2020. 01
Technical Report	Network 2030-Gap Analysis of Network 2030 New Services, Capabilities and Use cases	2020. 06
Technical Report	Network 2030-Additional representative use cases and key network requirements for Network 2030	2020. 06
Technical Specification	Network 2030 Architecture Framework	2020. 06
Technical Specification	Network 2030-Terms and Definitions	2020. 06
Technical Report	Network 2030-Description of Demonstrations for Network 2030 on Sixth ITU Workshop on Network 2030 and Demo Day, 13 January 2020	2020. 06

표 5. ITU-T SG17 차세대 네트워크 국제표준화 현황
Table 5. ITU-T SG17 International Standardization Trends for Next Generation Network

Deliverables No. (Temp. No.)	Title	Status
X.1811 (X.5Gsec-q)	Security guidelines for applying quantum-safe algorithms in IMT-2020 systems	Approved (2021.04.30.)
X.1047 (X.nsom-sec)	Security requirements and architecture for network slice management and orchestration	Approved (2021.10.29.)
X.1812 (X.5Gsec-t)	Security framework based on trust relationship for IMT-2020 ecosystems	Approved (2022.05.20.)
XSTP-5Gsec-RM	5G Security Standardization Roadmap	Agreed (2022.05.20.)
X.1813 (X.5Gsec-vs)	Security and monitoring requirements for operation of vertical services supporting ultra-reliability and low latency communication (URLLC) in IMT-2020 private networks	Approved (2022.09.02.)
X.1814 (X.5Gsec-guide)	Security guidelines for IMT-2020 communications system	Approved (2022.09.02.)
X.1815 (X.5Gsec-ecs)	Security guidelines and requirements for IMT-2020 edge computing services	Determined (2022.09.02.)
X.1816 (X.5Gsec-ssl)	Guidelines and requirements for classifying security capabilities in 5G network slice	Determined (2022.09.02.)
X.5Gsec-message	Security Requirements for 5G message service	Under study (2023.03)
TR.cpn-col-sec	Security considerations of collaboration of multiple computing power networks	Under study (2023.09)
X.5Gsec-netec	Security capabilities of network layer for 5G edge computing	Under study (2023.09)
X.5Gsec-ctrl	Security controls for operation and maintenance of 5G network systems	Under study (2023.09)
TR.5Gsec-bsf	Guidelines of built-in security framework for telecommunications network	Under study (2024.03)
TR.zt-acp	Guidelines for zero trust based access control platform in telecommunication network	Under study (2024.03)
X.5Gsec-srocvs	Security Requirements for the Operation of 5G Core Network to Support Vertical Services	Under study (2024.03)

다. 2022년 3월에 개최된 WTSA-20에서는 2022. 03 ~ 2024. 12 연구회기에 대한 논의가 이루어졌다. 해당 총회를 통해 SG17 작업반 WP2/17(Working Party 2/17, 5G, IoT and ITS security)의 Q2/17(Question 2/17, Security architecture and network security) 과제를 통해 IMT-2020 보안에 대한 연구 및 표준화가 중점적으로 수행될 것으로 결정되었다. 이에 따라, 지난 회기를 통해 개발된 권고안 및 기술문서와 금번 회기에 예정되어 있는 권고안 및 기술문서 개발 현황은 표 5와 같다[8].

2.2.3 ITU-T IMT-2030 보안 표준화 동향

ITU-T에서는 SG13의 FG NET-2030을 통해 IMT-2030에 대한 사전 연구를 수행하였으나, 보안 기술을 중점적으로 다루지는 않은 것으로 보인다. ITU-T의 IMT-2030 보안 표준화의 경우, SG17을 통해 중점적으로 수행될 것으로 보인다. SG17의 IMT-2030을 위한 표준화 계획은 공개되지 않았으나, WTSA-20의 결의안 92번(Enhancing the standardization activities in the ITU Telecommunication Standardization Sector related to non-radio aspects of international mobile telecommunications) 내용에 따르면 IMT-2030 보안 측면의 표준화 활동도 고려하고 있는 것으로 보인다. 다음 표 6은 WTSA-20 결의안 92번의 주요 내용을 나타낸다[9].

표 6. ITU-T WTSA-20 결의안 92번
Table 6. ITU-T WTSA-20 Resolution 92

No.	Resolution 92
Title	Enhancing the standardization activities in the ITU Telecommunication Standardization Sector related to non-radio aspects of international mobile telecommunications
Instruction for SG17	・to continue promoting the studies on standardization activities related to network and applications security for IMT-2020 and beyond ・to promote coordination and collaboration with ITU-R and other SDOs, such as the 3rd Generation Partnership Project System Aspects working group 3 (3GPP SA3), on security aspects of IMT-2020 and beyond, in the course of development of the relevant specifications or ITU-T Recommendations

2.3 ETSI 6G 보안 표준화

방송, 통신, 전자 통신 네트워크 및 서비스에 대한 표준화 활동을 수행하고 있는 유럽 지역 표준 기구인 ETSI(European Telecommunication Standards Institute)는 3GPP(3rd Generation Partnership Project)와의 협력 관계를 통해 5G에 대한 표준을 개발하고 있다. ETSI 자체적으로 5G 네트워크 보안 표준을 개발하는 활동은 미비한 실정이다. 그러나, 5G 요소기술에 해당하는 MEC(Multi-access Edge Computing)와 NFV(Network Functions Virtualization)에 대한 표준화를 산업표준그룹(ISG, Industry Specification Groups)을 통해 수행하고 있다.

2.3.1 ETSI ISG NFV

ETSI는 5G 요소기술인 NFV에 대한 표준 개발을 위해 2012년 11월에 ISG NFV를 설립하였다. 해당 산업표준그룹에서는 2년을 주기로 단계별 표준화를 진행한다. 다음 그림 2는 단계별 표준화 내용을 요약한 것이다[10].

ETSI ISG NFV에서는 NFV 보안에 대한 표준화 활동을 Release 2에서부터 Release 4까지 지속적으로 이어오고 있다. 다음 표 7은 현재까지 ETSI ISG NFV에서 개발하여 공개한 NFV 보안 표준문서를 나타낸다. ETSI ISG NFV는 현재 Release 5를 통해 표준화를 진행하고 있으며, 6개의 새로운 표준화 항목이 추가되었다. 새롭게 추가된 표준화 항목에는 보안과 관련된 항목은 포함되어 있지 않았으나, 특정 표준 개발 규격 단계(Release)에서 규격 정의가 완료되지 않고 각 단계에서 점진적으로 보완하고자 하는 작업항목 ENH01(NFV security hardening)을 통해 Release 4에 이어 보완 규격 개발을 진행하고 있다.

2.3.2 ETSI ISG MEC

ETSI는 5G 요소기술에 해당하는 MEC에 대한 표준을 개발하기 위해 2014년에 ISG MEC를 설립하였으며, 3년을 주기로 단계별 연구 및 표준화를 진행하고 있다. 2018년에 시작되어 2번째 표준개발 규격 단계(Phase)에 해당하는 Phase 2를 통해 5G에 MEC를 통합하기 위한 연구 및 표준 개발이 작업 항목 MEC031(MEC integration in 5G networks)을 통해 이루어졌으며, Phase 3에서부터 GR MEC041(MEC Security) 작업 항목을 통해 MEC 보안 규격 마련을 위한 표준화가 시작되었다. 해당 작업 항목을 통해

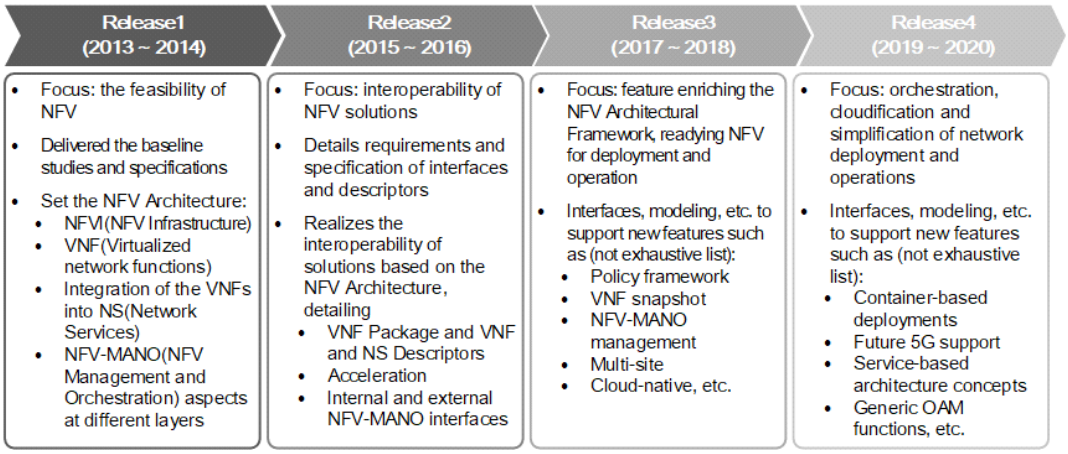


그림 2. ETSI ISG NFV Releases 요약
Fig. 2. Summary of ETSI ISG NFV Releases

표 7. ETSI ISG NFV 보안 규격
Table 7. Security Specifications of ETSI ISG NFV

Rel.	Work Item	Specification
Rel.2	· (R02.CAP08) Package and software image management · (R02.CAP09) VNF Descriptor-VNF information modeling · Security aspects of other specified capabilities	· (ETSI SG NFV-SEC 021 v2.6.1) Network Function Virtualisation(NFV) Release 2; Security; VNF Package Security Specification
	· Security aspects of other specified capabilities	· (ETSI SG NFV-SEC 022 v2.8.1) Network Functions Virtualisation(NFV) Release 2; Security; Access Token Specification for API Access
Rel.3	· (SEC4SNC) Secure sensitive components in NFV Framework	· (ETSI GS NFV-SEC 012) Network Functions Virtualisation(NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components
	· (SECMM) Security management and monitoring for NFV	· (ETSI GS NFV-IFA 026) Network Functions Virtualisation(NFV) Release 3; Management and Orchestration; Architecture enhancement for Security Management Specification · (ETSI GS NFV-SEC 013) Network Functions Virtualisation(NFV) Release 3; Security Management and Monitoring specification · (ETSI SG NFV-SEC 014) Network Function Virtualisation(NFV) Release 3; NFV Security; Security specification
Rel.4	· (SECMM) Security management and monitoring for NFV	· (ETSI GS NFV-IFA 033) Network Functions Virtualisation(NFV) Release 4; Management and Orchestration; Sc-Or, Sc-Vnfm, Sc-Vi reference points-Interface and Information Model Specification
	· (ENH01) NFV security hardening (enhancements)	-
Rel.5	· (ENH01) NFV security hardening (enhancements)	-

MEC 애플리케이션, 보안 플랫폼, 제로트러스트(Zero Trust) 네트워킹, MEC 보안 요구사항 등에 대한 규격 문서 초안 작업을 진행하고 있다[11].

2.3.3 ETSI 6G 보안 표준화 동향

ETSI는 주로 3GPP와의 협력을 통해 5G 및 6G 네트워크 보안 표준화 활동을 수행하기 때문에 자체적인 5G 및 6G 네트워크 보안 표준화 활동은 미비하다. 그러나, 지속적으로 5G의 요소기술인 NFV와 MEC에 대한 보안 규격을 개발하고 있으며, 6G에도 해당 기술이 계승될 것으로 예상됨에 따라 ETSI에서 개발하는 NFV 및 MEC 보안 표준이 다른 표준 개발기구에 준용될 것으로 보인다. 또한, ISG NFV와 ISG MEC 이외에도 TC CYBER(Technical Committee for Cybersecurity), TC LI(Technical Committee for Lawful Interception), SAGE(Security Algorithms Group of Experts)를 통해 5G 보안 표준화 활동을 수행하고 있으며, 해당 작업반의 표준화 활동도 6G 보안 표준화 활동으로 이어질 것으로 보인다.

2.4 3GPP 6G 보안 표준화

사실표준화 기구에 해당하는 3GPP는 2016년 4월부터 착수된 5G 기초 연구를 기반으로 5G 표준화를 시작하였다. 3GPP에서는 표준화 일정에 따라 특정 시기별로 표준화 활동 결과물을 발표하며, 2022년 3월에 Release 17이 완료되어 현재 Release 18을 통해 표준화를 진행하고 있다. Release 18에서는 5G에서 6G로 넘어가는 과도기 형태에 해당하는 5G Advanced에 대한 연구 및 표준화가 진행되고 있으며, 다음 표준개발 규격 단계(Release)에서 6G 표준화의 기반을 마련하는 활동이 이루어지고 있다[12].

3GPP는 SA(Service & System Aspects), CT(Core Network&Terminals), RAN(Radio Access Network)으로 구성된 기술총회(TSG, Technical Specification Group)별로 여러 산하 작업반(WGs, Working Groups)이 있다. 여러 산하 작업반 중 SA WG3(Security)가 5G 보안 표준을 개발하고 있으며, 해당 그룹의 표준화 활동 결과는 TS 33.5XX, TR 33.7 ~ TR 33.9XX로 번호가 부여된 기술규격(TS,

표 8. SA WG3 Release 18 표준화 항목
Table 8. SA WG3 Release 18 Work Item

No.	Work Item
1	Privacy of identifiers over radio access
2	SECAM and SCAS for 3GPP virtualized network products and Management Function (MnF)
3	Mission critical security enhancements Phase 3
4	Security and privacy aspects of RAN & SA features

Technical Specification)과 기술 보고서(TR, Technical Report)를 통해 확인할 수 있다[13].

Release 15에서는 TS 33.501(Security architecture and procedures for 5G System)을 개발하여 5G 시스템의 보안구조, 주요 구성요소의 보안 요구사항, 네트워크 간의 상호 인터페이스 관련 보안 등에 대한 전반적인 내용을 정의하였다[14]. Release 16에서는 TS 33.501에서 정의된 5G 시스템 구성요소에 대한 보안 테스트 절차에 해당하는 보안 보증 명세서(SCAS, Security Assurance Specification)에 대한 기술규격이 개발되었다. Release 17에서는 Release 16에서 다루지 않았던 추가적인 5G 시스템 구성요소 보안 보증 명세서에 대한 기술규격을 개발하였다[13]. 현재 진행 중인 Release 18에서는 5G에서의 개인정보 및 프라이버시 보호, 가상화 네트워크 및 관리 기능을 위한 보안 기능 정의를 위한 연구 및 표준화가 진행될 것으로 보이며, 표 8은 SA WG3의 Release 18 표준화 항목을 나타낸다[15].

2.4.1 3GPP 6G 보안 표준화 동향

3GPP는 5G의 상용화 단계에 따라 보안 기능 및 서비스에 대한 연구 및 표준화를 지속적으로 수행해 왔다. 현재 진행 중인 Release 18에서도 5G 서비스에 대한 개인정보 및 프라이버시 보호, 가상화 네트워크 및 관리 기능을 위한 보안 등에 대한 규격의 초안 작업을 진행하고 있음에 따라 6G 보안에 대한 연구 및 표준화는 미비한 것으로 보인다. 그러나, Release 20에서부터 6G에 대한 선행 연구가 본격화될 것으로 보이며, ITU-R의 IMT-2030 Vision에서 정의한 정량적/정성적 보안 요구사항 지표에 따라 6G 보안에 대한 연구 및 표준화가 본격화될 것으로 보인다.

2.5 O-RAN Alliance 6G 보안 표준화

O-RAN(Open Radio Access Network) Alliance (이하, O-RAN)는 5G 및 B5G(Beyond 5G)에 AI(Artificial Intelligence)를 적용하여 지능형 무선 접속망 개발을 촉진하는 것을 목표로 표준화 및 오픈소스 플랫폼 개발을 진행하고 있는 사실표준화 기구이다. O-RAN에서는 보안 작업반 WG11(Technical Work Group 11)을 통해 Open RAN 아키텍처 보안에 대한 연구와 표준화를 진행하고 있다. Open RAN 표준화의 경우, 다른 기술 작업반과 표준 개발 담당 포커스 그룹 SDFG(Standard Development Focus Group)와의 협력을 통해 수행하고 있다[16]. 가장 최근에 WG11에서 발표한 표준의 경우, Open RAN에 대한 위협 모델링, 보안 요구사항, 프로토콜, 테스트 4가지 관점에서 개발되었다. 다음 표 9는 현재까지 공개된 O-RAN WG11의 보안 표준 문서를 나타낸다.

표 9. O-RAN WG11 보안 표준 문서
Table 9. O-RAN WG11 Security Specifications

Title	Publication Date
O-RAN Study on Security for Near Real Time RIC and xApps 1.0	2022.07
O-RAN Study on Security for Non-RT-RIC 1.0	2022.07
O-RAN Study on Security for O-CLOUD 1.0	2022.07
O-RAN Security Protocols Specifications 4.0	2022.10
O-RAN Security Requirements Specifications 4.0	2022.10
O-RAN Security Test Specifications 3.0	2022.10
O-RAN Security Threat Modeling and Remediation Analysis 4.0	2022.10

2.5.1 O-RAN Alliance 6G 보안 표준화 동향

6G에서는 인공지능 기술을 적용하여 초지능 성능을 지원할 것으로 논의되고 있다. O-RAN에서도 Open RAN의 지능화를 달성하기 위해 지속적으로 연구할 것으로 보이며 지능화된 Open RAN의 도입으로 우려되는 보안을 고려하여 표준화를 수행할 것으로 보임에 따라 O-RAN에서 정의한 표준이 3GPP에 적극적으로 수용될 것으로 보인다.

Ⅲ. 6G 보안 국내 표준화 동향

3.1 TTA 6G 보안 표준화 동향

국내에서 ICT 분야의 표준화를 담당하는 기관인 한국정보통신기술협회(TTA, Telecommunications Technology Association)는 특별기술위원회 STC3 (Special Technical Committee 3)을 기술위원회

TC11(Technical Committee 11)로 전환하여 5G 및 6G에 대한 국내 표준화 활동을 수행하고 있다. TTA TC11은 3GPP의 운영 기관(OP, Organization Partners)에 포함되어 있음에 따라 3GPP의 기술규격을 전환 채택(Transposing)할 수 있는 권한을 갖고 있다. 이에 따라 TTA TC11에서는 5G와 6G에 대한 표준을 자체적으로 개발하기보다는 ITU-T 및 3GPP 등 국외의 국제표준화 또는 사실표준화 기구의 표준화 활동에 적극적으로 참여하며 국내 산업계의 요구사항에 따라 국외 표준화 기구들의 표준 규격을 준용하여 국내 표준을 개발하는 전략을 채택하였다. 이에 따라, TTA에서 5G 및 6G 보안에 대해 자체적으로 표준화를 개발하는 것은 미비한 실정이다[17].

3.2 5G 보안 포럼 6G 보안 표준화 동향

5G 보안 포럼은 국내외 표준 개발을 위한 플랫폼 역할을 통해 5G 보안 기술의 국제표준화를 선도하고 국내 표준 수요에 대응하고자 2020년에 발족되었다. 5G 보안 포럼에서는 표준화 대상을 크게 5G 보안 기반 기술과 5G 보안 응용 기술로 구분하고 있다. 5G 보안 기반 기술로는 보안 위협, 보안 요구사항, 인증 및 키 관리, 제품 및 서비스 보증 지침, 양자 암호 알고리즘 슈트 등이 해당되며, 5G 보안 응용 기술로는 에지 클라우드 보안, SDN 보안, NFV 보안, 공급체인 보안, 보안 관제 등이 해당한다.

5G 보안 포럼에서 기술표준분과를 통해 표준화 활동을 수행하고 있으며, 국내 5G 서비스 및 보안 솔루션, 제품 제조업체 등의 실무적인 의견이 표준에 반영될 수 있도록 국제표준화 기구 및 사실표준화 기구의 표준 제·개정 활동에 참여하고 있다. 표 10은 5G 보안 포럼이 기여한 표준화 활동을 나타낸다[18].

5G 보안 포럼은 국제표준화 선도를 목표로 국외의 국제표준화 기구 및 사실표준화 기구의 표준화 활동에 지속적으로 참여하고 기고서를 활발히 제출하는 등 국제적으로 표준화 활동에 기여하고자 꾸준히 연구 및 표준화 활동을 이어갈 것으로 보인다. 이에 따라 국내에서도 6G 보안 표준화의 기반을 마련하고자 컨퍼런스를 개최하는 등 정보 네트워크를 활성화해

표 10. 5G 보안 포럼 표준화 활동
Table 10. 5G Security Forum Standardization Activities

Standards Development Organizations	Publication Date	Specification / Contribution Title
ITU-T	2021	· Revised baseline text for X.5Gsec-ecs: Security Guidelines for 5G Edge Computing Services (C1004) · Revised baseline text for X.5Gsec-ecs: Security Guidelines for 5G Edge Computing Services (C1139) · Revised baseline text for X.5Gsec-guide: Security guideline for 5G communication system (Proposal for a threat and capability regarding “Service disruption from manipulated RRC connection Request)
	2020	· Revised baseline text for X.5Gsec-q: Security guidelines for applying quantum-safe algorithms in 5G systems · Security requirements for vertical services supporting ultra reliable and low latency communication(URLLC) in the 5G non-public
3GPP	2021	· Countermeasures against a threat of a service disruption due to unprotected RRC messages proposed by 5G Security Forum in South Korea
	2020	· Threat on SIP message alternation and content eavesdropping · Threat on service disruption due to falsely generated RRC message
TTA	2021	· Security Guidelines for applying quantum-safe algorithms in IMT-2020(5G) systems
	2020	· Security Assurance Methodology (SECAM) and its evaluation guideline for Mobile Communication network products · Security requirements for vertical services supporting URLLC in 5G non-public networks
Forum	2021	· Security guidelines for 5G Edge Computing Services · Security Guidelines for applying quantum-safe algorithms in IMT-2020(5G) systems
	2020	· Security Assurance Methodology (SECAM) for 5G network - Terms and Definitions · Security Assurance Methodology (SCA) for 5G network products – valuation · Security requirements for vertical services supporting URLLC in 5G non-public networks

나갈 것으로 보인다.

Ⅳ. 표준화 기구별 6G 보안 표준화 동향 비교 분석

4.1 표준화 기구별 6G 보안 표준화 항목 비교 분석

본 절에서는 앞서 분석하였던 국내외 표준화 기구별 6G 보안 표준화 항목에 대해 비교하여 분석한다. 다음 표 11은 표준화 기구별 6G 보안 표준화 항목을 비교 분석한 것을 나타낸다.

먼저, 국외 표준화 기구 중 국제 표준화 기구에 해당하는 ITU-R의 경우, IMT-2030에 대한 전체적인 표준화 계획을 수립하고, IMT-2030이 달성해야 할 것으로 논의되는 비전 및 사용 시나리오, 성능 등에 대한 요구사항을 정의하여 IMT-2030 표준 기술개발을 위한 기준을 마련하고 있다. 이에 따라, IMT-2030의 성능 지표 중 IMT-2020에서는 중점적으로 고려되지 않았던 보안 성능 지표가 정의될 것으로 보인다.

국제 표준화 기구에 해당하는 ITU-T의 경우, 현재까지 IMT-2030 보안에 대한 구체적인 표준화 항목이 공개되지는 않았다. 그러나, 2022~2024년 연구회기 기간의 과제(Question)에 해당하는 연구 항목(Study Items)에 따르면 보안 아키텍처, 보안 서비스 적용 방안, 인공지능 및 머신러닝 적용 방안, 새로운 네트워크 기술 도입으로 인해 발생할 것으로 예상되는 보안 위협 및 대응 방안 등 IMT-2030 보안에 대한 전반적인 내용을 다룰 것으로 보인다[19].

국제 표준화 기구에 해당하는 ETSI의 경우, 5G와 6G의 인프라 가상화를 위한 요소기술에 해당하는 NFV 및 MEC에 대한 보안 표준화가 중점적으로 이루어질 것으로 보인다. ETSI ISG NFV의 경우, VNF 패키지 보안 요구사항 및 보안 절차, 액세스 토큰(Access Token)과 관련된 보안 위협 및 보안 요구사항, 보안 관리 및 모니터링, 보안 관리 및 모니터링을 위한 아키텍처, 보안 규격을 위한 MANO(Management and Orchestration) 구성요소 등에 대한 논의가 이루어졌다. Release 5부터는 NFV 보안 규격에 대한 항목이 공개되지 않았지만, 6G를 고려하여 NFV 보안을 향상하기 위해 점진적으로 보안 성능을 보완해가는 작업이 이루어질 것으로 보인다. ETSI ISG MEC의 경우, MEC 애플리케이션, 보안 플랫폼, 제로트러스트 네트워킹, MEC 보안 요구사항 등에 대한 논의가 Phase 3에서 이루어졌다. Phase 4에서는 Phase 3에 이어 MEC 041(MEC Security) 작업 항목을 통해 MEC 보안에 대한 규격을 마련할 것으로 보이며, 주로 MEC 시스템 보안 및 개인정보 보호를 개선하기 위한 내용이 주로 다루어질 것으로 보인다[20].

국외 표준화 기구 중 사실표준화 기구에 해당하는 3GPP의 경우, 이동통신에 대한 보안 요구사항을 정의하고 3GPP 시스템의 보안 및 개인정보 보호를 위한 아키텍처와 프로토콜 규격을 정의한다. 또한, 이동통신 보안을 위한 암호화 알고리즘 및 합법적 감청(LI, Lawful Interception)에 대한 내용을 다룬다[21]. 현재

표 11. 표준화 기구별 표준화 항목
Table 11. Work Items of Each SDO(Standards Development Organization)

SDO	Work Items (Not exhaustive list)
ITU-R	· IMT-2030 vision · IMT-2030 usage scenario · IMT-2030 capability · IMT-2030 requirements
ITU-T	· Security architecture · Application method for provide security services · Application method for AI(Artificial Intelligence)/ML(Machine Learning) · Study on security threats and challenges introduced by the emerging network technologies
ETSI	· VNF package security requirements and security process · Security threats and security requirements related with access token · Architecture for security management and monitoring · MANO components for security specification · MEC application · Security platform · Zero Trust networking · MEC security requirements · Security and privacy in MEC systems
3GPP	· Security requirements · Architecture and protocol specification for security and privacy · Cryptographic algorithms · Lawful Interception
O-RAN Alliance	· Security of Open RAN components · Comprehensive security threat modeling · Security test · Security requirements
TTA	-
5G Security Forum	-

까지도 5G 보안 규격을 개발하는 중이며, Release 19에 대한 세부적인 표준화 아이템에 대한 논의가 2023년 9월에 예정되어 있음에 따라 6G 보안에 대한 표준화 아이템은 공개되지 않은 것으로 보인다[22]. 그러나, 6G에서도 5G에서부터 적용된 보안 기능의 성능을 향상하고 새로운 네트워크 기능 도입에 따라 발생할 것으로 예상되는 보안 위협에 따라 보안 요구사항을 도출하는 등에 대한 연구가 이루어질 것으로 보인다.

사실표준화 기구에 해당하는 O-RAN Alliance의 경우, O-CLOUD, Non-RT RIC(Non-Real-Time RAN Intelligent Controller), Near-RT RIC (Near-Real-Time RAN Intelligent Controller)와 같은 Open RAN의 구성요소에 대한 보안과 Open RAN의 포괄적인 보안 위협 모델링, 보안 테스트, 보안 요구사항, 보안 프로토콜을 표준화 아이템으로 하여 표준화를 진행하고 있다.

국내 표준화 기구에 해당하는 TTA와 5G 보안 포럼의 경우, 6G 보안에 대한 표준화 항목을 설정하여 자체적으로 표준을 개발하는 활동은 미비한 상태이다. TTA와 5G 보안 포럼의 경우, 국외의 표준화 기구의 표준 개발 활동에 적극적으로 참여하여 국내의 표준화 기여도를 높이고 표준을 선도할 수 있도록 하는 체계를 갖추면서 국내 산업계의 표준 요구사항을 적극적으로 반영하여 그에 따른 국제 표준을 국내 표준으로 전환 채택하는 전략을 선택할 것으로 보인다.

V. 결 론

6G는 5G에서 구현하지 못했던 성능 및 기능의 한계를 개선하여 보다 발전적인 통신 서비스를 제공하고자 하는 이동통신 기술이다. 5G는 설계 단계에서 최소한의 보안 기능만을 고려하고 설계 이후에 발생하는 보안 위협에 대해서는 필요한 기능들을 추가로 도입하여 대응하고 있다. 그러나, 이러한 대응 방식은 이동통신 기술 성능에 영향을 준다. 6G에서는 5G로부터 계승될 것으로 예상되는 보안 위협에 대한 사전 연구와 설계 단계에서 보안 기능을 내재화하기 위한 표준의 필요성이 대두되고 있다. 따라서 본 논문에서는 국내외 표준화 기구의 6G 보안 표준화 활동 동향을 분석하여 6G 보안 표준화 활동의 기반을 마련하였다. 현재까지는 6G 보안에 대한 국내외 표준화 활동이 미비함에 따라, 6G 보안에 대한 사전 연구를 기반으로 국제표준화 기구에 표준화 항목을 기고하는 등의 활동을 통해 6G 보안 표준화를 선도할 필요가 있음을 확인하였다. 추가적으로 6G의 경우, 통신 서비스의 요구사항이 서로 상이하고 높은 보안성을 요구함에 따라 각 서비스 간의 성능과 보안성에 영향을 최소화할 수 있도록 하는 기술에 대한 연구가 필요할 것으로 사료된다. 6G 이동통신의 인프라를 가상화하여 각 통신 서비스가 요구하는 성능 및 보안성에 따라 별도의 통신 네트워크를 생성할 수 있도록 하는 네트워크 슬라이싱(Network Slicing)과 같은 인프라 가상화 기술을 통해 6G 네트워크 보안을 지원하려는 연구가 지속적으로 이루어져야할 것으로 보인다.

References

[1] Ministry of Science and ICT, *Future mobile communication R&D promotion strategy to lead the 6G era*(2020), Retrieved Dec. 11, 2022, from https://www.msit.go.kr/bbs/view.do?sCode=user&mId=206&mPid=89&bbsSeqNo=122&nttSeqNo=11

[2] H. Lim, et al., “Standardization status of ITU 6G vision,” in *Proc. KICS Conf.*, pp. 654-655, 2021.

[3] S. Baek, et al., “Standardization trends of 6G mobile communications in ITU-R,” in *Proc. KICS Summer Conf. 2022*, pp. 1200-1201, Jeju Island, Korea, Jun. 2022.

[4] J. Im, “The 41st ITU-R WP5D international conference - focusing on 6G international standardization,” (ICT standard & certification) *TTA J.*, vol. 202, pp. 121-124, Aug. 2022.

[5] TTA, TTAR-06.0232/R1, “*Standardization Trends on Beyond IMT-2020 (6G)*,” Technical Report, Oct. 2022.

[6] ITU-R, Recommendation ITU-R M.2083-0, “*IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*,” Sep. 2015.

[7] H.-R. Oh, et al., “ITU-T SG17 5G(IMT-2020) security international standardization trends,” *Rev. KIISC*, vol. 32, no. 4, pp. 85-92, Aug. 2022.

[8] *ITU-T work programme*, Retrieved Nov. 11, 2022, from https://www.itu.int/itu-t/workprog/wp_search.aspx

[9] ITU-T, “*Resolution 92-Enhancing the*

standardization activities in the ITU Telecommunication Standardization Sector related to non-radio aspects of international mobile telecommunications," 2022.

[10] ETSI, *ETSI ISG NFV: Work Program and Releases Overview*(2021), Retrieved Dec. 14, 2022, from https://docbox.etsi.org/isg/nfv/open/Other/ReleaseDocumentation/NFVTSC(21)000004r1_Summary_of_NFV_Releases_by_Jan_2021.pdf

[11] ETSI, *ETSI MEC: An Introduction(almost) everything you want to know about ETSI MEC*(2022), Retrieved Nov. 28, 2022, from https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/ETSI-MEC-Public-Overview_Generic.pdf

[12] TTA, *3GPP Releases*, Retrieved Nov. 12, 2022, from https://3gpp.tta.or.kr/technologies/release#section-7

[13] S. Kwon, et al.,"Current state and future of 5G security standards," *Rev. KIISC*, vol. 30, no. 6, pp. 17-22, Dec. 2020.

[14] 3GPP, TS 33.501 v17.7.0, "*Security architecture and procedures for 5G System* (Release 17)," Sep. 2022.

[15] TTA, *Releases*, Retrieved Dec. 16, 2022, from https://3gpp.tta.or.kr/technologies/release#section-0

[16] FUJITSU, *A Brief Look at O-RAN Security White Paper*, Retrieved Dec. 16, 2022, from https://www.fujitsu.com/global/documents/products/network/Whitepaper-A-Brief-Look-at-O-RAN-Security.pdf

[17] TTA, *IMT-2020(5G) Standardization Handbook*, Dec. 2020.

[18] J. Lee, "5G Security Forum," (ICT standard & certification) *TTA J.*, vol. 199, pp. 14-19, Feb. 2022.

[19] ITU, *Question 2/17* (Study Period 2022-2024), Retrieved Jan. 11, 2023, from https://www.itu.int/net4/ITU-T/lists/q-text.aspx?Group=17&Period=17&QNo=2&Lang=en

[20] ETSI, *Terms of Reference (ToR) for ETSI ISG Multi-access Edge Computing (ISG MEC)*(2022), Retrieved Jan. 11, 2023, from https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/ISG_MEC_ToR_DG_Approved_20220906.pdf

[21] 3GPP, *SA WG3 - Security and Privacy*, Retrieved Jan. 11, 2023, from https://www.3gpp.org/3gpp-groups/service-system-aspects-sa/sa-wg3

[22] 3GPP, The 5G standard(2022), Retrieved Jan., 11, 2023, from https://www.3gpp.org/ftp/Inbox/Marcoms/3GPP_Poster%20v2.pdf

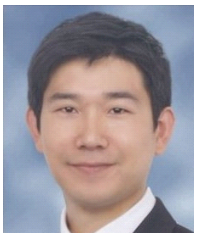
이 태 양 (Taeyang Lee)

2021년 8월 : 제주대학교 경영정보학과 졸업

2021년 9월~현재 : 세종대학교 정보보호학과 석사과정

<관심분야> 네트워크 보안, 네트워크 보안 표준화

이 종 혁 (Jong-Hyouk Lee)



2010년 2월 : 성균관대학교 공학박사

2009년 6월~2012년 2월 : 프랑스 INRIA 연구원

2012년 3월~2013년 8월 : 프랑스 TELECOM Bretagne 조교수

2013년 9월~2020년 2월 : 상명대학교 소프트웨어학과 부교수

2020년 3월~현재 : 세종대학교 정보보호학과 부교수

<관심분야> 프로토콜 엔지니어링, 정보보호

[ORCID:0000-0002-1753-1284]