정 보 보 호 학 회 지
제34권 제4호, 2024. 8

# ITU-T SG17 보안구조 및 네트워크 보안 국제표준화 동향

오 흥 룡*, 염 흥 열**

요 약

ITU-T SG17 국제표준화기구는 정보통신(Telecommunication) 관점에서 정보보호 표준들을 개발하고 있는 UN 산하 국제표준화기구이다. SG17 산하에 12개의 연구과제(Question)가 존재하고 있으며, 각 연구범위에서 국제표준을 개발 및 연구하고 있다. 이 중에 연구과제 2(Question 2, Q2/17)는 보안구조 및 네크워크 보안 주제를 다루고 있으며, 5G 보안(IMT-2020) 국제표준을 주도적으로 개발하고 있다[1].

본 논문에서는 최근 SG17 국제회의를 통해 Q2/17에서 네트워크 보안 관련 새롭게 개발된 국제표준과 현재 개발 중에 있는 국제표준화 동향에 대해 살펴보고자 한다.

## Ⅰ. 서 론

Q2/17(Security Architecture and Network Security)는 개방형 시스템 환경에서의 보안구조(X.800 시리즈)와 새롭게 개발되고 있는 네트워크 환경에서의 보안 기술들을 연구하고 있다. 특히, 5G 보안을 위한 SDN, NFV, VoLTE, 가상화, 슬라이싱, 메시지 및 응용기술을 다루고 있으며, 지능화된 네트워크 보안 기술(컴퓨팅파워네트워크(CPN), 컴퓨팅과 네트워크 통합(CNC) 등)과 제로트러스트 보안 기술들을 포함하여 연구하고 있다. 차기 연구회기(2025~2028)에는 6G 보안으로 연구범위를 확대할 계획이다.

## Ⅱ. ITU-T SG17 보안 국제표준화 현황

ITU-T SG17 Q2는 네트워크 보안을 중점적으로 다루고 있으며, 5G 보안 국제표준화 현황은 “ITU-T SG17 5G(IMT-2020) 보안 국제표준화 동향(2022.8월)”에 게재된 논문을 참고하기 바란다[2]. 본 논문에서는 2022.8월, 이후에 업데이트된 네트워크 보안 국제표준들을 다루고자 한다. Q2/17 개발한 국제표준 및 개발 중에 있는 아이템들은 [표 1]과 같다.

### 2.1. X.1817 (X.5Gsec-message)

본 국제표준(X.1817)은 5G 환경에서 비즈니스용으로 많이 활용되고 있는 메시지(예: 챗봇서비스)에 대한 보안 요구사항을 정의하는데 목적이 있다. 특히, 챗봇 서비스는 개인 간 또는 애플리케이션과 개인 간의 메시지를 지원하며, 메시지 내에 다양한 미디어(예: 장문, 사진, 비디오, 오디오, 파일 및 위치)를 지원하고 있다. 본 국제표준은 5G 메시징 서비스의 접근 보안 요구사항, 관리 보안 요구사항 및 제어 보안 요구사항을 다루고 있으며, 5G 메시징 서비스의 보안 요구 사항과 3G/4G/WLAN의 보안 요구 사항 간의 기능적 차이점을 소개한다[3].

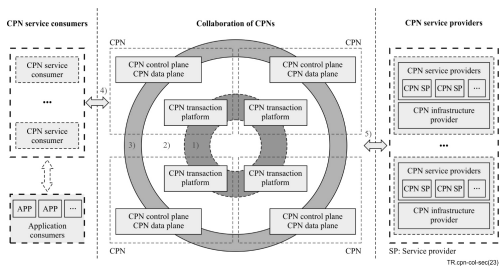
### 2.2. TR.cpn-col-sec

본 기술보고서(TR.cpn-col-sec)는 다수의 컴퓨팅 파워 네트워크(CPN, Computing Power Network)의 협업에 대한 개념, 비즈니스 역할, 활용사례 및 보안 위협을 분석하고, 컴퓨팅 파워 네트워크 관련 일반적인 보안 특성 및 특수한 보안 요구사항, 참조 프레임워크 및 세부 기능을 정의하고 있다. 다음의 [그림 1]은 CPN의 협업에 대한 참조 보안 프레임워크를 보여주고

본 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임.
[*No.2022-0-00009, ICT 국제공식표준화 대응 및 국가표준 연구, **No.2021-0-00112, 차세대보안 표준전문연구실]
* 한국정보통신기술협회 표준화본부 (수석연구원, hroh@tta.or.kr)
** 순천향대학교 정보보호학과/차세대보안 표준전문연구실 (명예교수, hyyoum@sch.ac.kr)

〔표 1〕 ITU-T SG17 Q2(보안구조 및 네트워크 보안) 국제표준화 현황

| No. | 제안 국가 | 국제표준 번호 (권고안 번호) | 권고안 제목 | 완료 시기 |
|---|---|---|---|---|
| 1 | 중국 | X.1811 (X.5Gsec-q) | Security guidelines for applying quantum-safe algorithms in IMT-2020 systems | 2021.4. |
| 2 | 중국 | X.1047 (X.nsom-sec) | Security requirements and architecture for network slice management and orchestration | 2021.10. |
| 3 | 중국 한국 | X.1812 (X.5Gsec-t) | Security framework based on trust relationship for IMT-2020 ecosystems | 2022.5. |
| 4 | 일본 한국 | XSTP-5Gsec-RM | 5G Security Standardization Roadmap | 2022.5. |
| 5 | 한국 | X.1813 (X.5Gsec-vs) | Security requirements for the operation of vertical services supporting ultra-reliable and low latency communication (URLLC) in the IMT-2020 private networks | 2022.9. |
| 6 | 한국 | X.1814 (X.5Gsec-guide) | Security guidelines for IMT-2020 communication system | 2022.9. |
| 7 | 중국 한국 | X.1815 (X.5Gsec-ecs) | Security guidelines and requirements for IMT-2020 edge computing services | 2023.3. |
| 8 | 중국 | X.1816 (X.5Gsec-ssl) | Guidelines and requirements for classifying security capabilities in IMT-2020 network slice | 2023.3. |
| 9 | 중국 | X.1817 (X.5Gsec-message) | Security Requirements for 5G message service | 2023.9. |
| 10 | 중국 | TR.cpn-col-sec | Security considerations of collaboration of multiple computing power networks | 2023.9. |
| 11 | 일본 | X.1818 (X.5Gsec-ctrl) | Security controls for operation and maintenance of IMT-2020/5G network systems | 2024.9. |
| 12 | 중국 | X.1819 (X.5Gsec-netec) | Security capabilities of network layer for IMT-2020/5G edge computing | 2024.9. |
| 13 | 중국 | X.1820 (X.5Gsec-srocvs) | Security Requirements for Operation of IMT-2020/5G Core Network to Support Vertical Services | 2024.9. |
| 14 | 중국 | TR.5Gsec-bsf | Guidelines of built-in security framework for telecommunications network | 2024.9. |
| 15 | 중국 | X.5Gsec-asra | Guidelines and Technical Requirements for 5G Network Asset Security Risk Analysis | 2025.9. |
| 16 | 중국 | TR.sd-cnc | Technical report: Security guidelines for data of coordination of networking and computing | 2025.9. |
| 17 | 중국 | TR.sec-int-cpc | Technical report: Security considerations for interconnection of computing power centers | 2026.3. |
| 18 | 중국 | TR.sg-lmcs | Technical report: Security guidelines for DLT-based lifecycle management of computing services | 2026.9. |
| 19 | 한국 | X.ztmc | Guidelines for Hhigh level Zero trust model and its security capabilities for in telecommunication networks | 2026.9. |




〔그림 1〕 CPN 협력을 위한 참조 보안 프레임워크

있으며, 서로 다른 CNP 서비스 제공자가 CPN control plane, CPN data plane, CPN transaction platform을 통해 협업하는 구조이다[4].

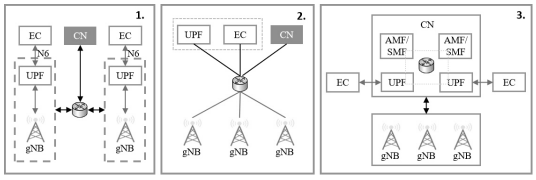
### 2.3. X.1818 (X.5Gsec-ctrl)

본 국제표준(X.1818)은 네트워크 기능 가상화(NFV), 무선 접속망(RAN), 네트워크 슬라이싱 및 멀

티 액세스 엣지 컴퓨팅(MEC)을 포함한 5G 네트워크 시스템을 운영하기 위한 보안 통제 지침을 정의하고 있다. 5G 네트워크 환경에서 상위 수준의 보안위협(Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege, Lateral Movement) 분석과 이를 통제하기 위한 기술 항목(조직관점, 인적관점, 운영관점, 물리적관점, 기술적관점)들을 정의하고 있다. 본 국제표준은 일본 내에서 시행하고 있는 5G 보안 통제 지침을 국제표준으로 추진한 사례이고, 2024.9월 국제회의에서 최종 채택될 예정이다[5].

### 2.4. X.1819 (X.5Gsec-netec)

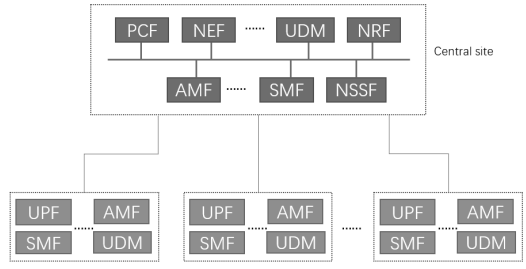
본 국제표준(X.1819)은 5G 네트워크 환경에서 에지 컴퓨팅을 구축할 때, 네트워크 계층의 보안 위협과 이를 대응하기 위한 보안기술을 정의하는데 그 목적이 있다. 현재 5G 네트워크 환경을 구축하는 방법은 국가별, 통신 사업자별로 다양한 형태로 네트워크를 구축하고 있다. 따라서, 본 국제표준은 [그림 2]에서처럼 기지국별로 에지 컴퓨팅을 구축하는 방법, 기지국을 그룹핑해서 구축하는 방법, 무선 접근 네트워크와 코어 네트워크 간에 협업하는 방법 제시하고 있으며, 이러한 다양한 구축방법을 고려한 보안 위협 및 대응방법을 정의하고 있으며, 2024.9월 국제회의에서 최종 채택될 예정이다[6].




〔그림 2〕 5G 환경에서 엣지 컴퓨팅 구축 사례

### 2.5. X.1820 (X.5Gsec-srocvs)

본 국제표준(X.1820)은 버티컬 서비스를 지원하기 위한 5G 코어 네트워크 운영방법에 대한 보안 요구사항을 정의하는데 목적이 있다. 즉, 5G 코어 네트워크가 구축된 중심 네트워크와 버티컬 서비스가 구축된 각 로컬 네트워크들 간에 안전하게 운영하기 위한 보안 요구사항을 정의한다. 본 국제표준의 기본 개념은




〔그림 3〕 버티컬 서비스를 지원하기 위한 5G 코어 네트워크 구축 프레임워크

[그림 3]과 같으며, 각 사이트 간에 운영 및 전송되는 데이터 관점에서의 보안 위협, 네트워크 보안 위협, 물리적 보안 위협 관점에서 보안 요구사항들을 정의하고 있다. 본 국제표준은 2024. 9월 국제회의에서 최종 채택될 예정이다[7].

### 2.6. TR.5Gsec-bsf

본 기술보고서는 정보통신 네트워크를 위한 내장형 보안 프레임워크 지침을 개발하는데 목적이 있다. 현재 구축 및 운영되고 있는 정보통신 네트워크 환경의 문제점들을 분석하고, 계속 새롭게 진화하고 있는 네트워크들의 이슈들을 분석한다. 이렇게 분석된 결과를 기반으로 내장형 보안 프레임워크 설계 원칙, 기능성을 정의하고, 이를 5G 네트워크에 적용하기 위한 구현 사례를 정의한다[8].

### 2.7. X.5Gsec-asra

본 국제표준은 5G 네트워크 운영 및 유지 단계에서 5G 네트워크 자산(Assets)의 범위를 규정하고, 이 자산을 위협하는 보안취약점을 정의하고, 이를 보호하기 위한 기술적 요구사항과 관리적 요구사항들을 정의하는 데 목적이 있다. 본 권고안은 처음 시작하는 단계에 있어 향후 다양한 보안취약점 및 위협사항들을 탐지하는 방법 등을 다룰 예정이다[9].

### 2.8. TR.sd-cnc

컴퓨팅과 네트워킹의 통합(CNC, Coordination of Networking and Computing) 기술은 자원의 활용, 제어 및 관리를 통해 더 높은 컴퓨팅 성능을 제공하기

위한 새로운 서비스로 등장하고 있다. 하지만, 대량의 데이터를 생성하고 수집하는 절차로 인해 기존의 네트워크 환경보다 다양한 데이터 유형의 위협이 증가될 수 있다. 따라서, 본 기술보고서는 2024.3월에 신설된 아이템으로 ITU-T Y.3400(5G와 B5G를 위한 컴퓨팅과 네트워킹의 통합 요구사항) 국제표준을 위한 보안 가이드라인을 개발하는 데 목적이 있다. 특히, 본 서비스에서 사용되는 데이터 분류(자원 운영 및 유지 관리 데이터, 아웃소싱 데이터 및 거래 데이터 등)를 정의하고, 각 데이터의 위협 정의, 이를 위한 보안 가이드라인을 개발할 계획이다[10].

### 2.9. TR.sec-int-cpc

대용량의 컴퓨팅 파워 서비스를 제공하기 위해서는 다수 CPN 간에 상호연동하여 분산된 자원을 효율적으로 활용하는 게 중요하다. 이를 위해서는 최적의 자원 할당을 수행하기 위한 관리 기능 및 오케스트레이션 플랫폼 도입이 필요하다. 따라서 본 기술보고서는 2024.3월에 신설된 아이템으로 CPN 간에 상호연동에 대한 보안측면에서의 고려사항과 보안위협을 정의하는 데 목적이 있다[11].

### 2.10. TR.sg-lmcs

본 기술보고서는 2024.3월에 신설된 아이템으로 컴퓨팅 서비스의 시나리오 및 보안 요구사항과 컴퓨팅 서비스 생태계에 참여하는 다양한 엔티티들 간에 분산원장기술 기반 컴퓨팅 서비스의 생명주기 관리를 위한 보안 가이드라인을 정의하는 데 목적이 있다. 본 기술보고서는 시작 단계에 있어 향후 연구범위 및 세부 기술들의 방향성에 대해 구체화할 계획이다[12].

### 2.11. X.ztmc

본 국제표준은 2024.3월에 신설된 아이템으로 정보통신 네트워크에서 핵심 영역(엔드 디바이스/아이덴티티, 네트워크 디바이스, 정보통신 네트워크, 오케스트레이션/자동화 등)과 보안 능역을 포함한 상위 수준의 제로트러스트 모델을 위한 가이드라인을 개발하는 데 목적이 있다. 본 국제표준에서 정의할 제로트로스트 모델은 다양한 산업 분야(IoT, 스마트 팩토리 등)에서 정의된 제로트러스트 모델에 레퍼런스 모델로 활용될 수 있을 것으로 판단된다. 특히, 본 국제표준은 다양한 국가 및 서비스 도메인에서 사용되고 있는 제로트러스트 모델을 고려해서 국제표준을 개발할 계획이다. 단, 네트워크 디바이스 간 통신 시나리오는 다루지 않는다[13,14]. 이 표준은 제로트러스트 보안 분야에서 ITU-T 사상 최초로 합의된 권고이다.

## Ⅲ. 결 론

본 논문은 ITU-T SG17 Q2에서 연구하고 있는 보안구조 및 네트워크 보안 국제표준화 동향에 대해 살펴보았다. Q2는 다양한 이기종 네트워크 환경에서 보안 표준들을 다루고 있으며, 차기 연구회기(2025~2028)에서는 5G/B5G, 6G 보안과 제로트러스트 관점에서의 네트워크 보안들을 중점적으로 다룰 계획이다. 현재 Q2는 중국 통신사들을 중심으로 국제표준을 개발하고 있어 국내 이통사, 네트워크 보안 기업들의 많은 관심과 적극적인 참여가 필요하다.

## 참 고 문 헌

[1] ITU-T SG17 Homepage, https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx

[2] 오흥룡, 염흥열, “ITU-T SG17 5G(IMT-2020) 보안 국제표준화 동향”, 정보보호학회지, 제32권 제4호, pp. 85-92, 2022.

[3] ITU-T X.1817, Security requirements for 5G messaging service, 2023.09.

[4] ITU-T TR.cpn-col-sec, Security considerations of collaboration of multiple computing power networks, 2023.09.

[5] ITU-T X.1818, Security controls for operation and maintenance of IMT-2020/5G network, 2024.09.

[6] ITU-T X.1819, Security capabilities of network layer for IMT-2020/5G edge computing, 2024.09.

[7] ITU-T X.1820, Security Requirements for Operation of IMT-2020/5G Core Network to Support Vertical Services, 2024.09.

[8] SG17-TD1975, 5th Revised baseline text for

TR.5Gsec-bsf: Guidelines of Built-in Security Framework for the Telecommunications Network, 2024.03.

[9] SG17-TD1954, 1st Revised baseline text for X.5gsec-asra: Guidelines and technical requirements for 5G network asset security risk analysis, 2024.03.

[10] SG17-TD1906, Proposal for new work item TR.sd-cnc:Security guidelines for data of coordination of networking and computing, 2024.03.

[11] SG17-TD1885, Proposal for new work item TR.sec-int-cpc: Security considerations for interconnection of computing power centers, 2024.03.

[12] SG17-TD1870, Proposal for new work item TR.sg-lmcs: Security guidelines for DLT-based lifecycle management of computing services, 2024.03.

[13] SG17-TD1863R5, Proposal for new work item X.ztmc: Guidelines for high-level Zero trust model and its security capabilities in telecommunication networks, 2024.03.

[14] 염흥열, “ITU-T SG17(보안) 제로트러스트 국제표준화 성과 및 향후 추진 방향”, 정보보호학회지, 제34권 제3호, pp. 21-25, 2024.

## 〈저자소개〉

**오 흥 룡 (Heung-Ryong Oh)**
종신회원

2002년 2월 : 순천향대학교 전자공학과 학사
2004년 2월 : 순천향대학교 정보보호학과 석사
2018년 2월 : 순천향대학교 정보보호학과 박사
2004년 2월~현재 : 한국정보통신기술협회 표준화본부 수석연구원
2005년 3월~현재 : ITU-T SG17 국내 연구반 간사(역) 및 위원
2009년~2016년 : ITU-T SG17 Q2 Associate Rapporteur
2017년~현재 : ITU-T SG17 Q2 Co-Rapporteur
2011년~현재 : 한국정보보호학회 학회지 편집위원
2012년 8월~현재 : 국방부 국방정보기술표준(DITA) 자문위원
2017년 9월~현재 : 금융결제원 바이오인증 성능위원회 자문위원
2019년 4월~현재 : 용인시 지역정보화위원회 자문위원
2022년 9월~현재 : 개인정보보호위원회 개인정보기술포럼 표준화분과 간사 및 위원(1기, 2기)
<관심분야> 보안프로토콜, 정보보호표준

**염 흥 열 (Heung Youl Youm)**
종신회원

한양대학교 전자공학과 학사
한양대학교 대학원 전자공학과 석사
한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 8월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수, 명예교수
2017년~현재 : ITU-T SG17 의장
2009년~2016년 : ITU-T SG17 부의장, WP3 의장
2011년 1월~12월 : 한국정보보호학회 회장
2012년 1월~현재 : 한국정보보호학회 명예회장
2020년 8월~2023년 8월 : 개인정보보호위원회 위원
<관심분야> 네트워크 보안, IoT 보안, 블록체인 보안, 개인정보보호, 정보보안 국제표준