정 보 보 호 학 회 지
제34권 제3호, 2024. 6

ITU-T SG17(보안) 제로트러스트 국제표준화 성과 및 향후 추진 방향

염 흥 열*

요 약

제로 트러스트 보안은 새로운 보안 패러다임으로 “절대 믿지 말고, 철저히 검증하라 (Never trust, always verify)” 라는 원칙을 적용한 새로운 보안 구조하고 볼 수 있다. 국제전기통신연합(ITU) 전기통신부문 (ITU-T) 정보보호 표준화를 담당하는 ITU-T SG17[1]에서는 제로트러스트 보안을 차기 연구회기 (2025-2028) 동안 수행할 신흥 표준화 주제(emerging standardization topic) 로 선정한 바 있다. 본 논문에서는 지난 2024년 2월/3월 스위스 제네바에서 열린 ITU-T SG17 회의에서 한국이 주도적으로 제안해 제로트러스트 표준화 분야에서 ITU-T 사상 처음으로 국제표준 (Recommendation) 신규 표준화 과제 채택의 성과와 사전 준비 상황을 살펴보고, 향후 표준화 추진 방향을 제시하고자 한다.

Ⅰ. 서 론

ITU-T에서 정보보호 국제표준을 개발하는 연구반은 SG17 (국제의장: 순천향대 염흥열교수) 이다[1].

제로트러스트 보안 구조는 미국 조 바이든 대통령이 연방정부의 모든 보안 구조를 제로트러스트 기반의 보안 구조로 변경할 것을 요구하는 행정 명령[11]을 2021년 5월에 발표하면서 최근 새로운 보안 흐름이 되고 있다. 미국 NIST 등 연구기관과 공공기관이 제로트러스트 가이드라인을 발표하고 제로트러스트 보안 구조로의 전환을 준비하고 있다[14].

기존 네트워크 보안 구조는 경계 기반으로 구성되어 있다. 경계기반 구성은 원격 근무와 클라우드 환경으로 인해 경계가 허물어지고 있어서 경계 기반 보안 구조를 바로 적용하는데 한계가 있다. 특히, 기존 경계 기반 보안모델은 내부자에 대한 암묵적 신뢰와 함께 높은 권한을 부여함에 따라 고도화·지능화되는 보안 위협에 한계 노출되게 되고, 내부 접속 사용자·기기 또는 내부 트래픽에 대해 외부에서 요구하는 접속과 비교하여 높은 수준의 신뢰성을 부여하는 특성이 있다. 따라서 이러한 최신 공격을 막기 위해서는 제로트러스트 기반의 보안 구조로 패러다임을 변경할 필요가 있다. 제로 트러스트는 자산 또는 사용자 계정의 물리적 또는 네트워크 위치(예: 로컬 영역 네트워크 대 인터넷)만을 기반으로 하거나 자산 소유권(기업 또는 개인 소유)을 기반으로 자산 또는 사용자 계정에 암묵적 신뢰가 부여되지 않는다고 가정한다. 인증 및 인가 (주체 및 디바이스 모두)는 기업 자산에 대한 접근 세션이 설정되기 전에 수행되어야 하는 개별적인 기능이다[14]. 우리나라 과기정통부는 2023년 7월에 우리나라 공유의 특성을 반영한 제로트러스트 가이드라인 1.0[12]을 발표한 바 있다.

본 논문 제2장에서는 TU-T SG17에서 제로트러스트 국제표준화를 추진하기 위한 사전 준비 활동를 제시한다. 제3장은 ITU-T SG17 국제표준화 성과 및 의의를 살펴본다. 그리고 제4장에서는 본 논문의 결론을 제시한다.

Ⅱ. ITU-T SG17에서 제로트러스트 국제표준화를 추진하기 위한 사전 준비 활동

제로트러스트 보안 구조는 통신망의 보안을 위한 매우 중요한 보안 인프라가 될 것이다. 제로트러스트 보안 구조에 대한 표준화를 위해서는 사전에 많은 준비가 필요하다. 본 장에서는 SG17에서 2023년 3월 이후 논의된 사전 준비 활동을 중심으로 기술한다.

본 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임.[*No.2021-0-00112, 차세대보안 표준전문연구실]

* 순천향대학교 정보보호학과/차세대보안 표준전문연구실 (명예교수, hyyoum@sch.ac.kr)

2.1. 차기 연구회기 (2025-2028) 신규 표준화 주제 선정 (2023년 2월/3월 SG17 회의, 2023년도 8월/9월 SG17 회의)

한국은 2023년 2월/3월 SG17 회의에 “차기 연구회기를 위한 신흥 표준화 주제”에 대한 기고서[2]를 제출했다. 이 기고서에서는 제로트러스트 구조는 새로운 사이버보안 패러다임으로 현재의 정적이고 네트워크 기반 경계에서 이용자, 자산 그리고 자원에 집중하는 구조로 전환이 필요하다고 강조했다. 또한 한국은 동 회의에 제로트러스트 표준화 주제를 다룰 연구과제(Question)의 할당에 대한 기고서[3]를 제출했다. 논의 결과 신규 표준화 제안에 대해 대체적인 합의가 있었으나, 계속 논의하기로 결정했다[4].

그 후 2023년 4월부터 6월까지 WTSA-24 준비를 위한 서신그룹 (CG) 활동을 통해, [표 1]과 같은 차기 연구회기를 위한 신흥 표준화 주제를 대체적으로 합의한 바 있다[13].

[표 1] 차기 연구회기 (2025-2028) 를 위한 ITU-T SG17 신흥 보안 표준화 주제 (22개)

번호	신흥 표준화 주제
1	메타버스 보안 및 데이터 보호
2	IMT-2030 보안 등 미래 네트워크 보안
3	SBOM(소프트웨어 자재 명세서)을 포함한 소프트웨어 공급망 보안
4	DevSecOps(개발, 보안 및 운영)
5	**제로 트러스트(ZT) 아키텍처 (메시 보안)**
6	SOAR 등 보안 자동화
7	AI 및 머신 러닝(AI/ML) 데이터 분석
8	데이터 보호를 위한 암호화 알고리즘 사용
9	데이터 마스킹 기술
10	스마트 엔티티를 포함한 섹터 보안
11	디지털 트윈 보안 및 데이터 보호
12	DLT 기반 공개키 기반 구조(DPKI)
13	엔드포인트 보안
14	시뮬레이션 보안
15	플랫폼 보안
16	OT 보안
17	공급망 보안
18	AI 관련 보안
19	QKD 보안
20	생성형 AI 보안
21	RNSS, 위성 등 융복합 네트워크 보안
22	V2X 보안

이후 2023년 8월/9월 SG17 회의에서 제로트러스트 보안 등의 신흥 표준화 주제를 2024년 10월에 열릴 세계표준화총회(WTSA-24)에서 논의된 결의 2(Resolution 2)에 포함될 “연구 일반영역(general areas of study)”과 “표준 개발 지침 포인트(point of guidance)”에 반영했다[6]. 따라서 또한 제로트러스트 보안 신규 표준화 주제를 ITU-T SG17내 연구과제 2 (Q2/17, 보안구조 및 네트워크 보안)를 통해 수행하도록 합의했다. 이러한 신규 표준화 주제의 선정은 한국이 신규 표준화 과제를 제안하는 근거가 되었다.

2.2. 제로트러스트 및 소프트웨어 공급망 보안에 대한 ITU 워크숍 개최를 통한 추천(2023 8월 28일, 킨텍스, 한국)

ITU-T SG17은 2023년 8월 28일 한국 킨텍스에서 제로트러스트 및 소프웨어 공급망 보안에 대한 ITU 워크숍을 개최한 바 있다[7].

이 워크숍의 목표는 다음과 같다.

- 제로 트러스트 및 소프트웨어 공급망 보안에 대한 개요와 해당 분야의 새로운 위협에 대한 인사이트 제공.
- 식별된 위협을 효과적으로 완화하기 위한 기술적 대응책과 조직적 통제 방안 파악.
- 관련 ITU-T 연구반 및 기타 다른 주요 표준화 기구 간의 수행된 활동 소개.
- 제로 트러스트 및 소프트웨어 공급망 보안과 관련된 향후 연구 주제의 향후 추진 방향 등의 권고를 TU-T SG17에게 제공.

이 워크숍을 통해 SG17에게 다음 사항을 권고했다[8].

- 5G 시스템과 통신 네트워크의 제로트러스트에 대한 더 많은 연구를 향후 SG17에서 추진해야 함.
- 네트워크 액세스 및 애플리케이션에 제로트러스트를 적용하는 방법을 연구하고 이를 제로트러스트 성숙도 모델[17]을 개발한 미국 CISA와의 협력을 통해 개발할 필요.
- 다양한 종류의 서비스 및 기능에 대한 보안 환경

을 효율적으로 구현하기 위해 제로트러스트 기술 사용을 고려해야 함.

위 ITU 워크숍에서 나온 추천은 향후 한국이 제로트러스트 신규 표준화 과제를 제한할 때 유용하게 활용되었다.

Ⅲ. ITU-T SG17 국제표준화 성과 및 의의

3.1. 제로트러스트 권고 개발을 위한 신규 표준화 과제 제안 및 채택(2024년 2월/3월 SG17 회의)

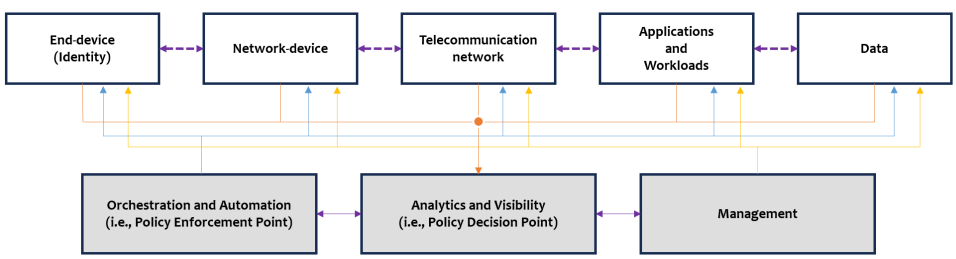
한국은 2024년 3월 SG17 회의에 “제로트러스트 구조와 능력”에 대한 신규 표준화 과제를 제안했다[9].

제안 배경은 기존에 존재하는 다양한 제로트러스트 모델들은 통신 네트워크 관점에서 상호 운용이 가능한 모델의 설계와 운영에는 미흡하고, 제로트러스트는 하나의 새로운 보안 개념으로 통신 네트워크에 적용이 필요하며, 통신 네트워크 관점에서 관련된 보안 영역들과 보안 능력을 정의함으로써, 5G/6G, ITS 등 다양한 산업 영역에서 이용이 가능 등의 제안 배경이다. Q2/17(연구과제 2)에서 논의 결과, 미국, 영국 등 주요국의 지지를 받아 신규 표준화 과제로 제로트러스트 분야에서 국제표준(Recommendation)으로서 ITU-T SG17 사상 처음으로 채택되었다. 논의 과정에서, 다음과 같은 주요 쟁점사항이 제기되었고 그 쟁점이 해결되었다.

- 표준의 역할: 이 표준의 역할에 대한 의견이 제시되었음. 논의결과는 세부 산업부문 (예, 지능형교통시스템, 5G/6G, 스마트 의료, 스마트 공장 등)에 제로트러스트 모델을 정의하지 않고, 이 표준에서는 일반 상위 수준의 모델을 개발하고, 다음 단계로 부문별 세부 모델을 개발함
- 제로트러스트 용어 정의: 기고에서는 NIST 용어 정의를 사용한 근거를 제시했는데, 그 이유에 대한 설명을 요구받은 함. 이유는 이 용어가 기술적인 용어 정의이고, 3GPP SA3에서도 이 정의를 사용하고 있으므로 해명됨
- 라우터간 제로트러스트 모델 적용 여부: 디바이스와 서버간, 라우터와 서버간은모델을 적용하고, 라우터간 모델은 비용으로 인해 적용하지 않기로 합의함
- 통신망 관점의 영역(pillar) 정의 필요: 종단 디바이스(신원)-네트워크 디바이스-통신망-응용 및 워크로드-데이터 주요 영역을 합의함.
- 표준 승인 프로세스 변경 필요: 규제적 합의가 있어서 TAP (traditional approval process)[16] 로 변경함
- 추가 갭 분석 필요: 3GPP에서 진행 중인 제로트러스트 원칙에 대한 TR[15] 추가함

이러한 쟁점이 모두 해결되어 다음과 같은 내용의 신규 표준화 과제가 채택되었고, 필자와 박준형 연구원이 에디터로 임명되었다[10].

- **표준 제목**: 통신망에서 상위 수준 제로트러스트 모델과 보안 능력에 대한 가이드라인 (Guidelines for high-level Zero trust model and its security capabilities in telecommunication networks)
- **표준 범위**: 통신 네트워크를 위한 제로트러트스 모델과 핵심 영역(Key area) 제시, 핵심 영역은 종단 디바이스, 네트워크 디바이스, 통신 네트워크, 애플리케이션 및 워크로드, 데이터 등으로 구성 (그림 1), 제로트러스트 핵심 영역별 보안 역량, 다양한 산업의 제로트러스트 적용 사례 제시, IoT,



[그림 1] 통신 네트워크를 위한 상위 수준 제로트러스트 모델([10])

스마트 공장 등 산업별 제로트러스트 모델을 정의하기 위한 참조 모델로 활용이 가능함.

[표 2]는 기고서와 Q2/17 논의 후 합의된 사항을 나타내고 있다.

[표 2] 제안과 합의된 사항

	제안[9]	신규 표준화 과제[10]
표준 제목	통신망에서 제로트러스트 구조와 보안 능력	통신망에서 상위수준 제로트러스트 모델과 보안 능력에 대한 가이드라인
범위	제로 트러스트 일반 구조와 보안 능력 제시	통신망에서 고수준 제로트러스트 모델과 보안 능력
표준 채택 과정	AAP (alternative approval process)	TAP (traditional approval process)
에디터	염흥열 외 5인	염흥열, 박준형 (한국 순천향대)

3.2. 제로트러스트 국제표준화 추진 의의 및 방향

한국(순천향대)은 ITU-T SG17 사상 최초로 제로트러스트 보안 국제표준(Recommendation)을 신규 표준화 과제로 채택하였다. 이러한 채택은 미국, 영국, 중국 등 주요 우방국과의 지지가 있었다. 이는 향후 세부 표준 개발을 우리나라 주도로 개발할 기반을 마련한 셈이다.

향후 제로트러스트 제품의 상호 연동성 보안을 위한 제로트러스트 국제표준화의 전략적 추진 필요하다. 정부의 정책 수립과 산업체, 학계, 공공 연구기관의 협력을 바탕으로 국제표준을 선점하여 국내 제로트러스트 제품의 글로벌 경쟁력을 확보가 필요하다. 또한 미국, 영국 등과 협력으로 국제 표준화를 계속 추진해야 한다.

또한 IMT2030/6G 네트워크 등 여러 산업 부문에 적용 가능한 제로트러스트 보안 모델의 개발이 필요하다. 제로트러스트 영역(pillar) 별 제품군 식별과 주요 영역간의 인터페이스에 대한 국제표준화를 추진해야 한다. 특히, 6G, 지능형교통시스템(ITS), IoT, 스마트 공장, 스마트 의료 부문의 제로트러스트 보안 모델 추가로 제안하며 이를 위한 국제연대가 요구된다.

Ⅳ. 결 론

본 논문에서는 2024년 2/3월 SG17 회의에서 한국이 제안한 제로트러스트 분야 신규 표준화 과제 제안 내용과 논의 과정에서 주요 쟁점사항, 그리고 향후 표준화 방향을 제시하였다.

제로트러스트 국제표준화는 보안 구조의 새로운 패러다임이다. 이를 위한 전략적 국제표준화 전략이 필요하다. 이에 대한 산학연정의 지혜와 자원의 집중, 그리고 정부의 지원이 절대 필요하다.

참 고 문 헌

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

[2] ITU-T SG17-C-234, “Proposal for SG17's potential hot topics for the next study period (2025-2028),” ITU-T SG17, 2023.03. https://www.itu.int/md/T22-SG17-C-0234/en

[3] ITU-T SG17 SG17-C-235, “Proposal for existing or new Question(s) to address potential hot topics identified by the CG-sg17-wtsa24-prep,” ITU-T SG17, 2023.03. https://www.itu.int/md/T22-SG17-C-0235/en

[4] ITU-T SG17, TD849, “Report of special session on CG-sg17-wtsa24-prep,”2023.3. https://www.itu.int/md/T22-SG17-230221-TD-PLEN-0849/en

[5] ITU-T SG17 TD1178R2, Report of CG-WTSA24-prep (May - July 2023). 2023.08. https://www.itu.int/md/T22-SG17-230829-TD-PLEN-1178/en

[6] ITU-T SG17 TD1357, “Baseline text for SG17 general areas of study, points of guidance to ITU T study groups for development of the post-2025 work programme, lead ITU-T study groups in specific areas of study, and list of Recommendations under the responsibility of the respective ITU-T study groups for the next study period (2025-2028),” ITU-T SG17, 2023.08 https://www.itu.int/md/T22-SG17-230829-TD-PLEN-1357/en

[7] ITU workshop on zero trust and software supply chain, 2023.8.28., Kintex, Goyang, Korea,

https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2023/0828/Pages/default.aspx
[8] ITU, Outcome of ITU workshop on zero trust and software supply chain, 2023.8.28, Kintex, Goyang, Korea, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2023/0828/Documents/Outcomes%20Document.pdf
[9] ITU-T SG17 C526, "Proposal for new work item X.ztac: Zero trust architecture and capabilities for telecommunication networks," ITU-T SG17, Korea (Republic of), 2024.3, https://www.itu.int/md/T22-SG17-C-0526/en
[10] ITU-T SG17 TD1863R5, "Proposal for new work item X.ztmc: High level Zero trust model and its security capabilities for telecommunication networks," ITU-T SG17, 2024.2. https://www.itu.int/md/T22-SG17-240220-TD-PLEN-1863/en
[11] US WH, "Executive Order on Improving the Nation's Cybersecurity," 2021.05. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[12] 과기정통부/인터넷진흥원, "제로트러스트 가이드라인 1.0," 2023.07. https://www.kisa.or.kr/2060205/form?postSeq=20&page=1
[13] ITU-T SG17 TD1178R2, Report of CG-WTSA24-prep (May - July 2023), ITU-T SG17, 2023.08. https://www.itu.int/md/T22-SG17-230829-TD-PLEN-1178/en
[14] NIST 800-207, Zero Trust Architecture, August 10, 2020. https://www.nist.gov/publications/zero-trust-architecture
[15] ETSI TR 33.894, Study on applicability of the zero trust security principles in mobile networks, September 2023. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4086
[16] ITU-T Recommendation A.1, Working methods for study groups of the ITU Telecommunication Standardization Sector, December 2019, https://www.itu.int/rec/T-REC-A.1-201909-I/en
[17] CISA, Zero Trust Maturity Model, April 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

<저 자 소 개>

염 흥 열 (Heung Youl Youm)
종신회원
한양대학교 전자공학과 학사업
한양대학교 대학원 전자공학과 석사
한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 정보보호학과 교수(역), 명예교수(현)
2011년 1월~12월 : 한국정보보호학회 회장(역), 명예회장(현)
2017년~현재 : ITU-T SG17 의장(현)
2019년 8월~현재 : 분산신원관리 기술 및 표준화 포럼 의장(과기정통부)
2022년 9월~현재 : 개인정보 기술포럼 의장(개인정보보호위원회)
2020년 8월 5일~2023년 8월 4일 : 개인정보보호위원회 위원(역)
2009년~2016년 : ITU-T SG17 부의장(역)
2009년~2016년 : ITU-T SG17 WP3 의장(역)
<관심분야> 개인정보보호, 네트워크 보안, IoT 보안, 제로트러스트 보안, 소프트웨어 공급망보안, 인공지능 보안과 프라이버시. 블록체인 보안, 5G/6G 보안