제로 트러스트 국제 표준화 동향과 전망

염흥열 ITU-T SG17 의장, 순천향대학교 정보보호학과 명예교수
박준형 순천향대학교 정보보호학과 석사과정
박성채 순천향대학교 차세대보안표준전문연구실 책임연구원

1. 머리말

제로 트러스트(Zero Trust)는 DISA(미 국방정보체계국, Defense Information Systems Agency)와 미 국방부가 추진한 '블랙코어(BCORE)' 전략, 그리고 2004년 예리코 포럼의 탈경계화(Deperimeterization) 개념으로부터 시작됐다. 이후 포레스터 리서치(Forrester Research)의 애널리스트인 존 킨더백(John Kindervag)이 제로 트러스트라는 용어를 만들어내면서 구체화됐다.

제로 트러스트는 기존 경계 기반 보안 모델에서 벗어나 개별 트랜잭션 단위로 보안을 평가하는 접근 방식으로, 민간 산업과 고등교육기관은 물론 연방기관도 해당 개념을 도입했다. 당시 미 연방기관들은 10년 넘게 제로 트러스트 보안 구조로의 전환을 권고받고 있었으며, 이에 따라 FISMA, RMF, FICAM 등 여러보안 프로그램과 정책을 개발했다[1]. 또한, 2021년 5월 미국 조 바이든(Joe Biden) 행정부는 '국가 사이버 보안 개선을 위한 행정명령'을 발표해 제로 트러스트 보안 구조로의 전환을 강조했다[2].

이러한 제로 트러스트의 등장은 초기 기술적 한계로 인해 정적이었던 전통적 보안 정책을 변화시켰다. 기술 발전과 함께 동적으로 접근 요청을 분석하고 평가하는 것이 가능해졌으며, 네트워크 모니터링 등을 통해 내·외부 위협으로부터 데이터를 보호할 수 있게 됐다[1]. 하지만 서로 다른 정보 자산 및 환경으로 인해 제로 트러스트 보안 구조로의 전환엔 다양한 어려움이 있다. 이를 해결하고자 NIST(미국 국립표준기술연구소, National Institute of Standards and Technology), ITU(국제전기통신연합, International Telecommunication Union), 3GPP 등 전 세계 표준화 기구들이 제로 트러스트 관련 국제 표준화를 추진하고 있다.

이번 원고에선 NIST, ITU-T, 3GPP 등 전 세계 표준화 기구들의 제로 트러스트 국제표준을 분석해 국제 표준화 추진 동향에 대해 살펴보고, 향후 관련 전망을 제시하고자 한다.

2. 제로 트러스트 국제 표준화 동향

2장에선 제로 트러스트의 국제 표준화 동향을 살펴본다. <표 1>은 제로 트러스트 표준화 현황을 나타낸다.

2.1 ITU-T SG17

ITU-T SG17(정보보호, 의장 순천향대 염흥열 교수)은 UN(국제연합, United Nations) 산하 ITU에서 정보보호 국제표준을 개발하고 제정하는 연구반이다[3]. ITU-T SG17은 2021년 8월 중국이

<표 1> 제로 트러스트 국제 표준화 현황

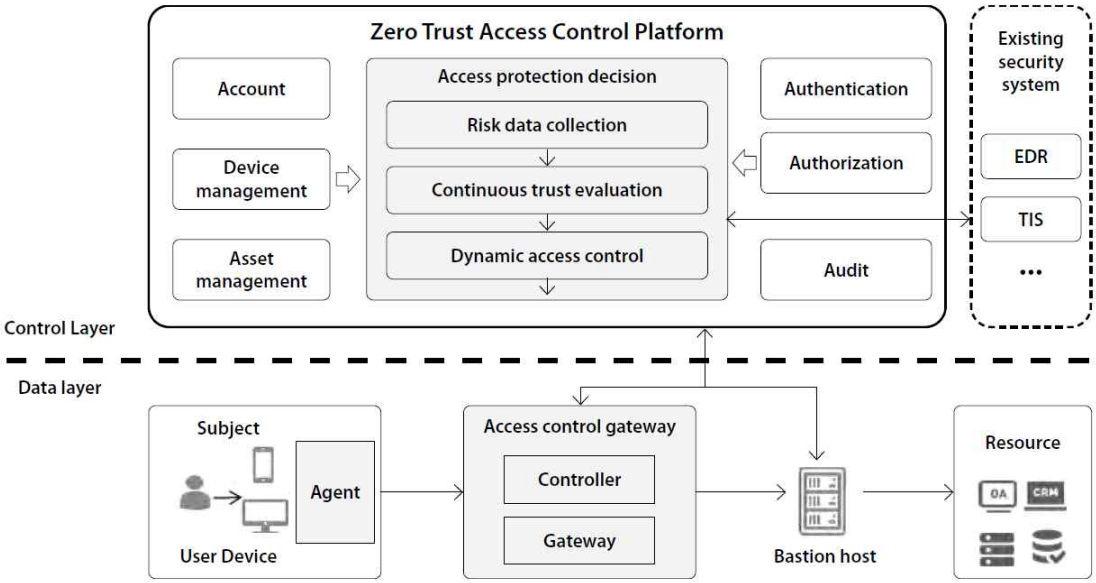
표준화 기구	표준명(또는 프로젝트명)	상태
ITU-T SG17	ITU-T TR.zt-acp, Guidelines for zero trust based access control platform in telecommunication network (통신 네트워크에서의 제로 트러스트 기반 접근통제 플랫폼 가이드라인)	출판(2024. 3)
	ITU-T X.ztmc, Guidelines for High level Zero trust model and its security capabilities for in telecommunication networks (통신 네트워크에서 상위 수준 제로 트러스트 모델과 보안 능력에 대한 가이드라인)	개발 중(2024. 3~ 2026. 9)
3GPP	TR.33.894, Study on applicability of the zero trust security principles in mobile networks (모바일 네트워크에서 제로 트러스트 보안 원칙의 적용성 연구)	출판(2023. 9)
	TR.33.794, Study on enablers for Zero Trust Security (제로 트러스트 보안의 실행 요인에 관한 연구)	개발 중(2024. 2 ~)
NIST	SP 800-207, Zero Trust Architecture (제로 트러스트 아키텍처)	출판(2020.08)
	SP 800-207A, A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments (다중 위치 환경에서 클라우드 네이티브 애플리케이션의 접근 제어를 위한 제로 트러스트 아키텍처 모델)	출판(2023. 9)
	SP 1800-35 (4번째 초안) Implementing a Zero Trust Architecture (제로트러스트 아키텍쳐 구현)	출판(2024.7)
IEEE	3219-2023, Blockchain-Based Zero-Trust Framework for the Internet of Things (사물 인터넷을 위한 블록체인 기반 제로 트러스트 프레임워크)	개발 중(개정) (출판: 2024. 4 / 개정: 2023. 2 ~ 2025. 12)
	P2887, Recommended Practice for Zero Trust Security (제로 트러스트 보안 권장 사례)	개발 중(2020. 6 ~ 2024. 12)
	P3409, Standard for a Zero Trust Security Framework (제로 트러스트 보안 프레임워크 표준)	개발 중(2023. 9 ~ 2027. 12)

제안한 '통신 네트워크에서의 제로 트러스트 기반 접근 통제 플랫폼 가이드라인(TR.zt-acp)[4]'을 기술보고서로 채택해 제로 트러스트에 대한 국제 표준화 관련 작업을 시작했다. 이후, 2024년 2·3월 회의에서 한국이 제안한 '통신 네트워크에서의 상위 수준 제로 트러스트 모델과 보안 능력에 대한 가이드라인(X.ztmc)[5]'을 신규 국제 표준화 항목으로 채택하며, 본격적인 제로 트러스트에 대한 국제표준 개발에 착수했다.

2.1.1 ITU-T TR.zt-acp[4]

해당 기술 보고서는 '통신 네트워크에서의 제로 트러스트 기반 접근통제 플랫폼 가이드라인(TR.zt-acp)'이다. 이는 2021년 8·9월 ITU-T SG17 국제 표준화 회의에서 중국이 제안했으며, 2024년 2·3월 I TU-T S G17 국제표준화 회의에서 최종 채택(Agreement)됐다. 해당 보고서는 통신 네트워크 내자원에 접근하는 과정에서 발생할 수 있는 보안 위협을 완화하기 위한 보안 요구사항을 제안한다. 또한 제로 트러스트 기반 접근통제 플랫폼의 구조와 구성요소를 포함하는 프레임워크도 정의하고 있다. [그림 1]은 통신 네트워크에서의 제로 트러스트 기반 접근 제어 플랫폼의

참조 프레임워크를 나타낸다.



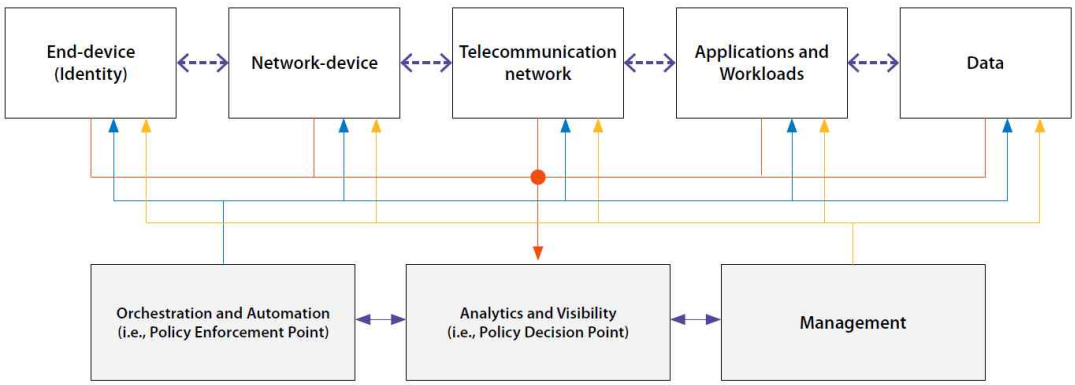
[그림 1] 통신 네트워크에서 제로 트러스트 기반 접근 제어 플랫폼 참조 프레임워크[4]

2.1.2. ITU-T X.ztmc[5]

'통신 네트워크에서 상위 수준 제로 트러스트 모델과 보안 능력에 대한 가이드라인(ITU-T X.ztmc)' 국제표준은 2024년 2·3월 ITU-T SG17 국제표준화 회의에서 한국이 제안했으며, 국제표준(Recommendation) 신규 표준화 항목으로 채택됐다. 이 표준은 2026년 9월까지 개발을 완료해 최종적으로 채택될 예정이다. 해당 국제표준의 개발 배경은 서로 다른 기존 통신 네트워크의 제로 트러스트 모델 간 상호 운용성 문제를 보완하기 위한 것이다. 나아가 IMT-2030(6G), ITS(지능형 교통 시스템, Intelligent Transportation System) 등 각종 산업 영역에 적용 가능한, 상위 수준 통신 네트워크에서의 제로 트러스트 보안 모델에 대한 가이드라인을 제안하고자 했다.

X.ztmc는 통신 네트워크에서의 제로 트러스트 모델을 구성하는 주요 영역(Area)을 제공하고, 각 영역이 갖춰야 하는 보안 능력(Security Capability), 산업별 제로 트러스트 적용 사례를 제시하는 국제표준이다. 제안하는 상위 수준 제로 트러스트 모델은 다양한 산업에서 세부적인 제로 트러스트 모델을 적용하기 위한 참조적인 상위 모델로 활용 가능하다.

[그림 2]는 ITU-T X.ztmc가 제시하는 8가지 주요 영역을 나타내며, 각 영역의 정의는 다음과 같다.



[그림 2] ITU-T X.ztmc에서 제시하는 8가지 주요 영역[5]

- 사용자 장치(End-device): 지속적인 인증 및 접근 제어를 통해 사용자 장치를 모니터링하고 보호하는 영역
- 네트워크 장치(Network-device): 장치의 상태를 파악해 위험결정을 내리고 실시간 검사를 수행하는 영역
- 통신 네트워크(Telecommunication network): 네트워크 환경을 세분화해 접근 제어를 적용하는 영역
- 응용 및 워크로드(Application and Workload): 하이퍼바이저, 컨테이너, 가상 머신을 포함해 응용프로그램과 워크로드를 보호하는 영역
- 데이터(Data): 데이터의 투명성과 보안을 위한 영역
- 오케스트레이션 및 자동화(Orchestration and Automation): 정의된 프로세스와 보안 정책을 기반으로 자동화된 보안 대응을 제공하는 영역
- 분석 및 가시성(Analytics and Visibility): 이벤트와 활동을 분석해 실시간 접근 제어를 지원하는 영역
- 관리(Management): 정보보안 정책과 절차를 정의하고 적용해 보안 위험을 관리하는 영역

2024년 9월 SG17 회의에선, 시스템 장애 및 사이버 공격 발생 이후의 회복력을 의미하는 사이버 복원력(Cyber Resilience), 동적 접근 제어를 위한 사용자 위치 및 행위 기반 실시간 분석 등을 포함해, 각 영역이 갖춰야 하는 보안 능력을 추가적으로 제안할 예정이다.

2.2 3GPP

3GPP는 이동통신 표준을 제정하는 사실표준화 기구로서, 1998년 ETSI(유럽전기통신표준협회, European Telecommunications Standards Institute)를 중심으로 ARIB(일본전파산업회, Association of Radio Industries and Businesses), TTC(일본정보통신기술위원회, Telecommunication Technology Committee), CCSA(중국통신표준화협회, China Communication Standards Association), ATIS(미통신산업협회, Alliance for Telecommunications Industry Solutions), TTA가 참여해 설립했다[6].

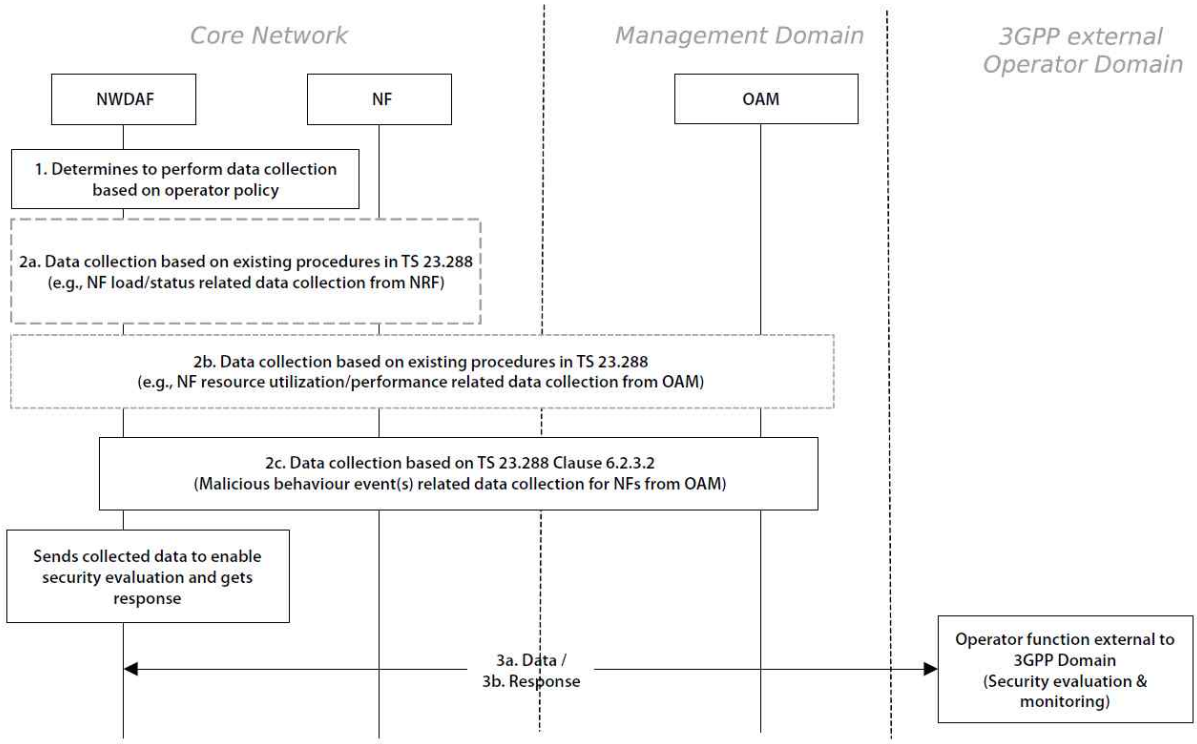
3GPP에서 제로 트러스트 관련 표준화 작업은 산하 그룹인 SA3가 담당한다. 3GPP SA3는 2023년 9월 배포된 '모바일 네트워크에서의 제로 트러스트 보안 원칙의 적용성에 관한 연구(Study on applicability of the zero trust security principles in mobile networks)'와 2024년 2월부터 개발에 착수한 '제로 트러스트 보안의 실행 요인에 관한 연구(Study on enablers for Zero Trust Security)'를 개발하고 있다.

2.2.1. TR 33.894[7]

모바일 네트워크에서 '제로 트러스트 보안 원칙의 적용성 연구(Study on applicability of the zero trust security principles in mobile networks, TR 33.894 V18.0.0)'는 2022년 7월 개발을 시작해 2023년 9월 출판됐다. 이 표준은 5G 시스템 코어 네트워크에 적용 가능한 제로 트러스트

원칙을 제공한다. 이와 관련하여 5G 시스템에서 보안 시나리오를 분석하고 제로트러스트 원칙을 적용했을 때의 이점과 관련된 잠재적인 위협을 식별하여 제공한다.

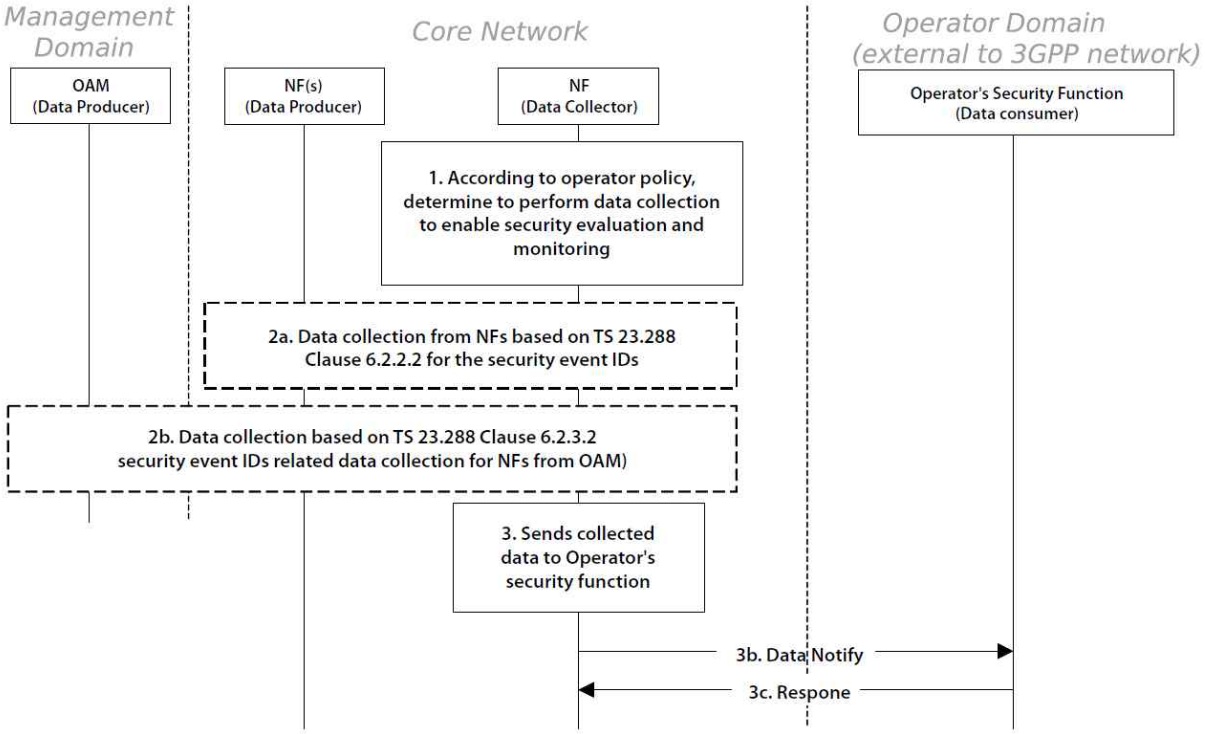
또한 위협을 완화하기 위한 신뢰 평가와 이를 보장하기 위한 보안 메커니즘을 분석하고, 추가적인 보안요구사항도 제시한다. [그림 3]은 5G 시스템에서 이상 행동을 탐지하기 위해, 여러 종류의 데이터 운영·관리·유지보수(Operation, Administration, and Maintenance, OAM) 담당 시스템을 바탕으로 관련 데이터를 효과적으로 수집하고 활용하기 위한 절차를 설명한다.



[그림 3] 네트워크 기능(Network Function)의 정상 작동 상태에서 보안 모니터링을 활성화하는 절차[7]

2.2.2. TR 33.794[16]

3GPP TR 33.794는 '제로 트러스트 보안을 위한 구현 요소 연구(Study on enablers for Zero Trust Security, TR 33.794 V0.3.0)'로, 2024년 2월 개발을 시작해 2024년 5월 0.3.0 버전이 공개돼 있으며 현재까지 개발 중인 표준이다. 이 표준은 5G SBA(Service Based Architecture) 계층에서 발생할 수 있는 잠재적 위협과 공격을 식별한다. 그리고 이러한 위협과 공격을 탐지하기 위해 노출(공개)돼야 하는 데이터가 무엇인지, 추가적인 데이터 공개가 필요한지 평가하는 내용을 제공하며, 식별한 보안 위협을 해결하기 위한 동적 정책 시행의 보안 메커니즘도 제공한다. [그림 4]는 잠재적 보안 이벤트(위협)를 기반으로 데이터를 수집하고, 이를 운영자의 보안 기능에 제공해 공격이나 위협을 신속하게 감지할 수 있도록 지원하는 방법과 절차를 보여준다.



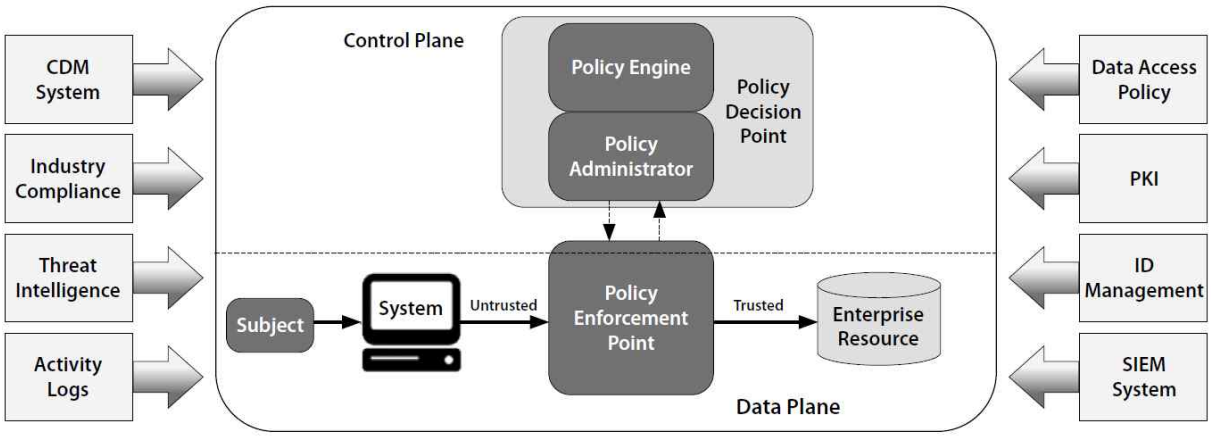
[그림 4] 보안 평가와 모니터링을 위한 데이터 수집 및 공개 절차[16]

2.3 NIST

NIST는 2020년 8월 '제로 트러스트 구조(Zero Trust Architecture, NIST 800-207)[1]' 표준을, 2023년 9월엔 '다중 위치 환경에서 클라우드 네이티브 애플리케이션의 접근 제어를 위한 제로 트러스트 아키텍처 모델(A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments, NIST 800-207A)[8]' 표준을 발간했다. 특히 NIST SP 800-207 표준은 제로 트러스트 관련 표준 및 가이드라인의 기반 문서로써 활용되고 있으며, 2024년 7월에는 NIST SP 800-207에 설명된 개념과 원칙에 따라 이를 구현하는 방법을 소개하는 SP 1800-35의 4번째 초안 문서를 발표했다.

2.3.1. NIST 800-207[1]

제로 트러스트 구조 표준은 제로 트러스트로의 전환을 위한 원칙을 제안하고, 제로 트러스트 구조와 함께 이를 구성하는 논리적 구성요소, 배포 시나리오, 사용 사례, 관련 보안 위협을 정의하고 있다. 또한 서로 다른 조직 환경을 고려해 제로 트러스트 논리구성 요소의 배치 모델을 '기기 에이전트–게이트웨이 배치모델', '리소스 그룹 배치 모델', '리소스 포탈 배치 모델', '기기 응용 샌드박스 배치 모델' 4가지로 제안하고 있다. [그림 5]는 제로 트러스트의 핵심적인 논리 구성 요소를 나타낸다.



[그림 5] NIST 800-207 제로 트러스트 핵심 논리 구성 요소

2.3.2. NIST 800-207A[8]

'다중 위치 환경에서 클라우드 네이티브 애플리케이션의 접근 제어를 위한 제로 트러스트 아키텍처 모델(A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments)' 표준은 클라우드 네이티브 애플리케이션 플랫폼에서 제로 트러스트 아키텍처(Zero Trust Architecture)를 구현하기 위한 요구사항을 제안한다. 해당 표준에서 식별하는 내용은 다음과 같다.

- 서비스 메시 인프라를 포함하는 마이크로서비스 기반 애플리케이션 플랫폼에서 세부적인 접근 제어를 위한 제로 트러스트 아키텍처 요구사항
- 제로 트러스트 원칙을 구성하고, 이를 구현하기 위한 플랫폼구성 요소
- 해당 플랫폼에서 제로 트러스트 아키텍처를 적용하고, 관련 아키텍처가 제공하는 보안 보장을 설명하기 위한 지침
- 제로 트러스트 원칙 시행을 위한 네트워크 영역별 정책과 ID 정책을 결합하는 다중 계층 정책

2.3.3 NIST 1800-35[15]

미국 국가표준기술연구소 산하 국가 사이버 보안 우수 센터(NCCoE, National Cybersecurity Center of Excellence)는 "제로 트러스트 아키텍처 구현" (NIST SP 1800-35) 실습 가이드의 네 번째 초안 문서를 발표했다. 이 가이드는 NCCoE가 24개 벤더와 협력하여 종합적인 제로 트러스트 아키텍처를 구현한 결과와 관련 모범 사례를 제시한다. 문서는 PDF 형식의 문서와 웹 형식의 문서로 제공된다. PDF 문서는 프로젝트 목표, 참조 아키텍처, 제로 트러스트 아키텍쳐 구현에 대한 요약을 제공하고, 웹문서는 사용된 기술의 통합 및 구성, 사용 사례에 대한 심층적인 기술 정보를 담고 있다. 이 가이드는 제로 트러스트 아키텍쳐 원칙을 NIST 사이버 보안 프레임워크(CSF)와 기타 보안 표준과 연계하여 제공하고, 조직이 제로 트러스트 아키텍처를 통해 사이버 보안 역량을 강화할 수 있도록 지원한다. 이 가이드는 2024년 9월 30일까지 공개 의견을 받고 있다

2.4 IEEE SA

IEEE(전기전자공학자협회, Institute of Electrical and Electronics Engineers) SA(표준협회, Standard Association)는 다양한 산업의 기술표준을 개발하는 IEEE 내부 조직이다[9]. IEEE SA엔 여러 산하 위원회가 있으며, 이 중 IEEE CPSC(사이버보안 및 프라이버시 표준 위원회, Cybersecurity & Privacy Standards Committee)에서 제로 트러스트를 포함한 사이버 보안 및 개인정보보호 관련 표준을 개발하고 있다[10]. IEEE CPSC는 제로 트러스트 보안 워킹그룹(Working Group)을 만들고, '제로 트러스트 보안을 위한 권장 사례(Recommended Practice for Zero Trust Security, IEEE SA P2887)[11]', '제로 트러스트 보안 프레임워크를 위한 표준(Standard for a Zero Trust Security Framework, IEEE SA P3409)[12]'을 개발하고 있다.

IEEE CPSC는 제 로 트러스트 보안 워킹그룹(Working Group)을 만들고, '제로 트러스트 보안 프레임워크를 위한 표준(Standard for a Zero Trust Security Framework, IEEE SA P2887)[11]', '제로 트러스트 보안을 위한 지침(Recommended Practice for Zero Trust Security, IEEE SA P3409)[12]'을 개발하고 있다.

2.4.1. IEEE SA P2887[11]

'제로 트러스트 보안 권장 사례(Recommended Practice for Zero Trust Security)' 표준은 2020년 6월 개발이 시작됐으며, 2024년 12월 개발 완료될 예정이다. 이 표준은 네트워크의 경계가 모호해지면서 발생하는 기존 경계 기반 보안 모델의 한계점을 극복해 리소스를 보호하기 위한, 제로 트러스트 아키텍처와 그 구현에 대한 보안 지침을 제공한다.

2.4.2. IEEE SA P3409[12]

'제로 트러스트 보안프레임워크를 위한 표준(Standard for a Zero Trust Security Framework)'은 2023년 9월 개발에 착수했으며, 완료시기는 2027년 12월인 표준이다. 이 표준은 제로 트러스트 관련 용어와 개념, 핵심요소 식별을 포함하는 제로 트러스트 보안을 위한 프레임워크를 제공한다. 이 프레임워크는 조직이 제로 트러스트 솔루션을 구현할 때의 핵심 보안 요소와 고려사항을 식별하고, 기존 경계 기반 모델에서 제로 트러스트 기반 모델로 전환할 때 보안 우선순위를 결정하는 데 활용될 수 있다.

또한 이 표준은 IEEE SA P2887의 제로 트러스트 보안 지침을 구현하기 위한 토대를 마련함으로써 글로벌 관점의 표준 개발에도 유용하다. 향후 ISO/IEC JTC 1/SC 27에서 국제표준 채택도 추진하는 중이다.

2.4.3. IEEE 3219-2023[13]/IEEE 3219[14]

'사물 인터넷을 위한 블록체인 기반 제로 트러스트 프레임워크(Blockchain-Based Zero-Trust Frame work for the Internet of Things)'는 2021년 5월 개발을 시작해 2024년 4월 발행된 표준이다. IEEE 컴퓨터 학회 산하 블록체인 및 분산원장 위원회(IEEE Computer Society Blockchain and Distributed Ledger Standards Committee)의 블록체인 기반 사물인터넷 보안 워킹그룹에서 개발했다[13]. 2023년 5월 개정작업이 시작됐으며, 2025년 12월 완료가 목표다.

이 표준은 사물인터넷에서 일반적인 보안 및 신뢰 문제를 해결하기 위한 블록체인 기반 제로 트러스트 프레임워크를 정의한다. 이 프레임워크는 사물인터넷 시스템에서 블록체인 기술을 지원하는, 논리적 구성요소 모음으로 구성된 시행 모델을 제시하고 있다. 또한 사용자 장치, 클라우드 구성요소에서 사용 가능한 구현 모델과 적용 절차를 제공하고, 기밀성·무결성·가용성·사용성을 제공하기 위한 프레임워크의 일반적인 배포 변형에 대한 설명도 포함한다.

3. 맺음말

제로 트러스트는 새로운 보안 패러다임이다. 이번 원고에선 제로 트러스트와 관련된 주요 표준화 기구인 ITU-T, 3GPP, NIST, IEEE의 표준화 현황을 분석했다.
기술 발전으로 네트워크 경계가 모호해지는 현 시점에서 제로 트러스트로의 전환은 필수적이다. 하지만 국가 및 조직별로 상이한 환경으로 인해 도입에 어려움을 겪고 있다. 글로벌 일관성과 상호운용성을 확보하기 위해서라도 제로 트러스트 국제 표준화는 매우 중요하다.
또한, 우리나라 보안 제품의 글로벌 경쟁력을 확보하기 위해, 국내 산·학·연은 제로 트러스트 관련 기술을 바탕으로 상호 협력을 통해 국제표준화를 주도해야 한다. 더불어, 미국, EU(유럽연합, European Union) 등과도 협력해 지속적으로 국제 표준화를 추진해야 한다.
나아가 다양한 산업 및 분야 특성에 맞춰, 각 부문 별 제로 트러스트 보안 모델에 대한 국제표준화 추진 역시 필요할 것으로 예상된다.

※ 본 논문은 2024년도 정부 (과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임.(No.2021-0-00112, 차세대보안 표준전문연구실)

[참고문헌]

[1] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, 'NIST SP 800-207, Zero Trust Architecture', NIST, 2020. 08(https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-207.pdf)
[2] Executive Order on Improving the Nation's Cybersecurity, 2021.5.12. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity
[3] ITU-T SG17, https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx
[4] SG17-TD1838, Revised baseline text for TR.zt-acp: Guidelines for zero trust based access control platform in telecommunication network (for Agreement), ITU-T SG17, 2024.03. (https://www.itu.int/md/T22-SG17-240220-TD-PLEN-1838)
[5] SG17-TD1863R5, 'Proposal for new work item X.ztmc: Guidelines for high-level Zero trust model and its security capabilities in telecommunication networks', ITU-T SG17, 2024.03. (https://www.itu.int/md/T22-SG17-240220-TD-PLEN-1863)
[6] "3GPP", TTA 정보통신용어사전, http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=062475-3
[7] TR 33.894(ver.0.8.0), 'Study on applicability of the zero trust security principles in mobile

networks', 3GPP SA3, 2023.09
(https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4086)
[8] Chandramouli, R. and Butcher, Z. 'NIST SP 800-207A, A Zero Trust Architecture Model for Access Control in 09 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207A.pdf),
[9] IEEE SA, 'IEEE Standards Association', https://standards.ieee.org/
[10] IEEE Cybersecurity & Privacy Standards Committee,
https://www.computer.org/volunteering/boards-andcommittees/standards-activities/committees/cybersecurity-privacy
[11] IEEE SA P2887, 'Recommended Practice for Zero Trust Security', 2020.04.23, https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/8425
[12] IEEE SA P3409, 'Standard for a Zero Trust Security Framework', 2023.08.03, https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/10955
[13] IEEE 3219-2023, 'IEEE Standard for Blockchain-Based Zero-Trust Framework for the Internet of Things(IoT)', 2024.04.26, https://standards.ieee.org/ieee/3219/11163/
[14] IEEE 3219, 'IEEE Standard for Blockchain-Based Zero-Trust Framework for the Internet of Things (IoT)',2024.04.26,
https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/10492
[15] NIST SP 1800-35 (4th Preliminary Draft), 'Implementing a Zero Trust Architecture', https://csrc.nist.gov/pubs/sp/1800/35/4prd
[16] TR 33.794(ver.0.3.0), 'Study on enablers for Zero Trust Security', 3GPP SA3, 2024. 05 (https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4235)

※ 출처: TTA 저널 제214호