# 제로트러스트 국제 표준화 동향

박성채, 박준형, 염흥열
순천향대학교

## 요 약

제로트러스트는 최근 보안 분야에서 가장 중요한 키워드 중 하나로 부상하고 있다. "절대 신뢰하지 말고, 항상 검증하라(Never trust, always verify)"라는 원칙을 바탕으로, 국가 정부 기관들과 여러 조직들은 제로트러스트 도입하고 구현하기 위해 노력하고 있다. 그러나 각기 다른 환경 등으로 도입에 어려움을 겪고 있으며, 이를 해결하기 위해 미국 국립표준기술연구소, ITU-T SG 17과 같은 전 세계 표준화 기구들이 제로트러스트에 대한 통일된 기준을 제공하기 위해 관련 국제 표준화를 적극적으로 추진중이다. 이에 본 고에서는 표준화 기구들이 추진하고 있는 제로트러스트 국제표준화 동향에 대해 분석하여 살펴보고자 한다.

## Ⅰ. 서 론

제로트러스트(Zero Trust)라는 개념은 2010년 포레스트 리서치(Forrest Research)의 애널리스트인 존 킨더박(John Kindervag)에 의해 처음 소개되었다[1]. 이는 네트워크 환경의 복잡성과 지능형 사이버 위협의 증가로 인해 기존의 경계 기반 보안 접근 방식의 한계를 극복하기 위해 고안된 개념이다. 특히 코로나19로 인한 비대면 환경의 증가와 디지털 전환의 가속화 등으로 인해 내부와 외부의 네트워크 경계가 모호해지면서 제로트러스트 모델의 중요성이 부각되었다. 기업과 기관들은 제로트러스트 도입의 필요성을 인식하고 있지만, 서로 다른 네트워크 환경으로 인해 도입에 어려움을 겪고 있다. 이에 따라 제로트러스트 기반 기술의 국제 표준화가 촉진되고 있으며, 이는 다양한 환경을 가진 조직들이 안전한 글로벌 보안 환경을 구축하는데 중요한 역할을 하고 있다. 이를 해결하기 위해 ITU-T, NIST 등의 표준화 기구들은 제로트러스트 국제 표준화를 활발히 추진중이다.

본 논문 제2장에서는 ITU-T SG17, ISO/IEC JTC 1/SC 27 등 여러 표준화 기구에서의 제로트러스트 국제 표준화 동향을 살펴보고, 제3장 결론에서는 제로트러스트 관련 국제 표준화 추진 전략을 제시하고, 이러한 표준화 노력이 제로트러스트 모델 및 기반 기술 등의 글로벌 채택과 구현에 미치는 영향을 논의한다.

## Ⅱ. 제로트러스트 국제 표준화 동향

### 1. ITU-T SG17

ITU-T SG17(Study Group 17, 정보보호)은 UN 산하의 표준 개발 및 보급을 담당하는 국제전기통신연합(International Telecommunication Union, ITU)에서 정보보호기술에 대한 국제표준을 개발하는 연구반이다[2]. ITU-T SG17에서 제로트러스트 관련 표준화 작업은 2021년 8월 중국의 제안으로 처음 시작되었다. 2024년 2-3월 회의에서는 우리나라가 제안한 통신 네트워크에서 상위 수준의 제로트러스트 모델과 보안 기능 가이드라인 국제 표준이 채택되어 개발 중이다.

#### 가. ITU-T TR.zt-acp [3]

이 기술 보고서(TR.zt-acp)는 통신 네트워크에서 제로 트러스트 기반 접근통제 플랫폼 가이드라인으로, 2021년 8-9월 ITU-T SG17 국제표준화 회의에서 중국의 제안으로 개발된 기술 보고서이다. 2024년 2-3월 ITU-T SG17 국제표준화 회의에서 최종 채택되었다. 이 기술 보고서는 통신망에서 자원에 접근할 때 발생할 수 있는 보안 문제를 해결하기 위한 보안 요구사항을 정의하고, 제로트러스트 모델을 기반으로 한 접근 통제 플랫폼의 구조와 작동 절차를 제시한다. 또한 제로트러스트 기반 접근 통제 플랫폼을 구성하는 구성 요소를 정의하고, 제로트러스트 기반 접근 통제 플랫폼에서의 인증 절차와 제로트러스트 기반 접근 통제 플랫폼에서의 어플리케이션 및 시스템 리소스 접근 절차를 정의하고 있다.

〈그림 1〉은 통신망에서의 제로트러스트 기반 접근 제어 플랫폼의 참조 프레임워크를 나타낸다. 이 참조 프레임워크는 데이터 계층과 통제 계층으로 구성된다. 데이터 계층은 제로트러스

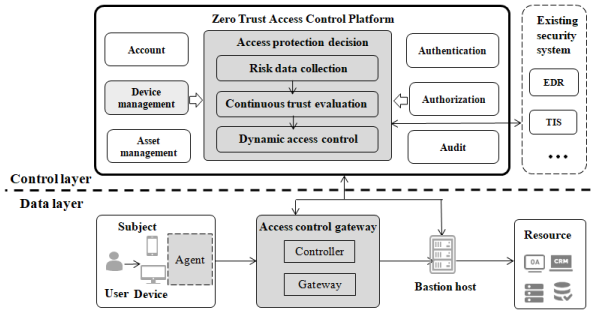


그림 1. 통신망에서 제로트러스트 기반 접근제어 플랫폼의 참조 프레임워크[3]

트 정책 이행점(PEP, policy enforcement point) 역할을 하는 접근 통제 게이트웨이, 자원에 대해서 접근을 요청하는 정보 주체 및 사용자 디바이스 및 정보 자원으로 구성된다. 통제 계층은 정책 결정점 (PDP, policy decision point) 역할을 하는 접근 통제 플랫폼으로 실현되며, 이 플랫폼에는 위험 데이터 수집, 연속적인 신뢰 평가, 동적 접근 통제로 구성되는 접근 보호 결정 기능과 그 외 인증, 인가, 감사, 자산관리, 계정 및 디바이스 관리 등으로 구성된다.

### 나. ITU-T X.ztmc [4]

ITU-T X.ztmc(통신 네트워크에서 상위 수준의 제로트러스트 모델과 보안 기능 가이드라인) 국제 표준은 2024년 2-3월 ITU-T SG17 국제표준화 회의에서 한국이 제안해 채택되었다. 이 국제표준은 통신 네트워크에서 상위 수준의 제로 트러스트 모델과 보안 기능에 대한 가이드라인을 제안하였으며, 〈그림 2〉와 같이 제로트러스트 모델을 구성하는 8 가지 핵심 영역을 정의하고, 각 영역이 갖추어야 할 보안 능력(Capability)을 제공하고 있다.

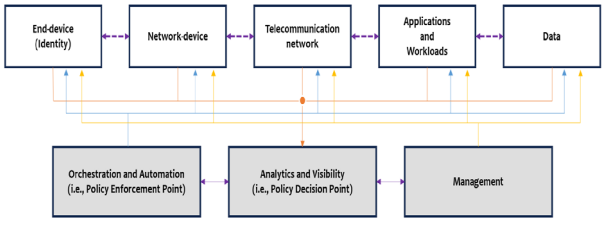


그림 2. ITU-T X.ztmc에서 정의된 8가지 핵심 영역

ITU-T X.ztmc에서 정의된 핵심 영역(Area) 별 요구되는 보안 능력(Capability)은 〈표 1〉과 같다.

표 1. ITU-T X.ztm에서 정의된 핵심 영역(Area) 별 요구되는 보안 능력 (개발 중)

| 핵심 영역 | 보안 능력 |
|---|---|
| 엔드 디바이스 (End-device) | 단말 자산 관리<br>인증<br>위험 평가<br>접근 관리 |
| 네트워크 디바이스 (Network-device) | 정책 강화 및 컴플라이언스 모니터링<br>자산 및 공급망 위험 관리 |
| 통신 네트워크 (Telecommunication network) | 마이크로 세그멘테이션<br>네트워크 트래픽 관리<br>트래픽 암호화 |
| 애플리케이션/워크로드 (Application/Workload) | 보안 SW 개발 및 통합<br>어플리케이션 접근<br>어플리케이션 위협 보호 |
| 데이터 (Data) | 중요 데이터 위험 조정<br>데이터 접근<br>데이터 암호화 |
| 오케스트레이션/자동화 (Orchestration/Automation) | 자동화 및 오케스트레이션 |
| 분석/가시성(Analytics/Visibility) | 가시성 및 분석 |
| 관리 (Management) | 정책 및 관리 |

## 2. ISO/IEC JTC 1/SC 27

ISO/IEC JTC 1/SC 27(정보보호)은 정보보안 분야의 국제표준 개발을 위해 ISO와 IEC 합동 기술 위원회(JTC 1) 내에서 활동하는 하위 위원회이다[5]. 현재 ISO/IEC JTC 1/SC 27에서는 제로트러스트에 관한 직접적인 표준이 개발되고 있지 않은 것으로 추측된다. 대신 정보 보안, 사이버 보안, 개인정보 보호 등 다양한 분야에서 제로트러스트 개념과 원칙을 지원하는 여러 표준들이 마련되고 있다. 특히, ISO/IEC JTC 1/SC 27/WG 4(보안 통제 및 서비스)에서 개발 중인 ISO/IEC 27090은 현재 CD 상태에 있으며, 2025년 5월(또는 9월) 국제 표준 승인을 목표로 하고 있다. 이 국제 표준은 AI 시스템의 전 생애주기에 걸쳐 보안 위협을 식별하고 이를 완화하기 위해서 제로트러스트 원칙을 직접적으로 적용한 보안 통제를 제시함으로써 보다 효과적으로 보안 위협을 완화할 수 있도록 한다[6]. 이 문서에서 식별한 보안 위협을 완화하기 위한 보안 통제에 적용되는 제로트러스트 원칙은 〈표 2〉과 같다.

표 2. ISO/IEC 27090의 제로트러스트 원칙

| | |
|---|---|
| a) | 조직의 정보 시스템이 이미 해킹되었다고 가정 |
| b) | 정보 시스템의 접근에 대해 "절대 신뢰하지 않고 항상 확인"하는 접근 방식을 채택 |
| c) | 정보 시스템에 대한 요청이 종단 간 암호화 사용을 보장 |
| d) | 정보 시스템에 대한 각 요청을 외부에서 발생한 것처럼 검증 |
| e) | 최소의 권한을 갖는 접근 통제 |
| f) | 요청자를 항상 인증하고 인가 요청을 항상 검증 |

또한 기존의 ISO 표준 중 ISO/IEC 27001은 조직이 비즈니스 위험 접근법을 기반으로 정보보안의 확립, 구현, 운용, 모니터링, 검토, 유지 및 개선을 위한 경영시스템에 대한 국제 표준이다. 이 표준은 조직이 보유한 정보 자산의 기밀성, 무결성, 가용성을 유지하기 위한 모든 보안 관리 활동을 체계화하고, 조직의 업무, 장소, 자산, 기술적 특성을 고려하여 구현 범위를 설정하고 이에 대한 요구사항을 제안한다[7]. ISO/IEC 27001은 2022년 개정되었으며, 개정되는 과정에서 제로트러스트의 철학이 담겨 있다고 볼 수 있는데, 특히 위험 평가(Risk Assessment), 접근 제어(Access Control) 및 지속적인 개선(Continuous Improvement) 등이 포함된다. 〈그림 3〉은 ISO/IEC 27001이 제시하는 ISMS 프로세스에 적용된 PDCA 모델을 보여준다. 이는 제로트러스트의 핵심 영역 중에서 관리 및 정책 이행과 연관되는 것으로 볼 수 있다.

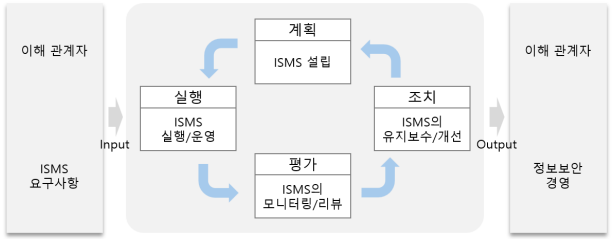


그림 3. ISMS 프로세스에 적용된 PDCA 모델

ISO/IEC 27002는 ISO/IEC 27001의 정보보호관리체계(ISMS) 요구사항과 함께 정보보호관리체계 인증에 필수적인 국제 표준으로, ISMS를 구축, 유지, 관리하기 위해 조직이 정보 자산을 보호하기 위한 다양한 보안 통제 사항을 제시한다[8]. 비록 이 두 국제 표준이 제로트러스트 원칙, 모델 등을 명시적으로 포함하고 있지는 않으나, 제로트러스트가 모든 사용자와 장치를 신뢰하지 않고 모든 액세스 요청을 엄격하게 검증 및 승인하는 보안 모델임을 고려할 때, 이 표준들은 제로트러스트 원칙과 상호 보완적으로 작용할 수 있다. ISO/IEC 27090은 제로트러스트 원칙을 언급하며, ISO/IEC 27002의 8.27절이 정보 시스템이 안전하게 설계, 구현, 운영될 수 있도록 제로트러스트 원칙을 포함하고 있다고 명시하고 있다. 특히, ISO/IEC 27002는 ISMS(정보 보안 관리 시스템) 구현을 위한 113개의 보안 통제를 제공하는데, 이 중 일부는 제로트러스트 개념이나 원칙이 적용된 것으로 볼 수 있다. 〈표 3〉은 ISO/IEC 27002에서 제공하는 보안 통제와 제로트러스트의 핵심 영역에 해당하는 몇 가지 예를 보여준다.

표 3. ISO/IEC 27002에서 제공하는 보안 통제와 제로트러스트의 핵심 영역에 해당하는 예시

| ISO/IEC 27002 통제 항목 | 제로트러스트 핵심 영역 |
|---|---|
| (5.15절) 접근 통제 (Access Control) | 엔드 디바이스(End-device)/신원 (Identity) |
| (5.18절) 접근 권한 (Access Privilege) | |
| (8.22절) 네트워크 분리 (Segregation of networks) | 통신 네트워크 (Telecommunication network) |
| (8.5절) 안전한 인증 (Secure Authentication) | 엔드 디바이스(End-device)/신원 (Identity) – 다중요소인증, 디지털 인증 등을 통한 안전한 신원 관리에 해당 |
| (5.7절) 위협 인텔리전스 (Threat Intelligence) | 분석/가시성 (Analytics/Visibility) |
| (8.16절) 모니터링 활동 (Monitoring Activities) | 오케스트레이션/자동화 (Orchestration/Automation) |

## 3. 3GPP

3GPP는 이동통신 표준을 개발하기 위해 한국, 유럽, 일본, 미국 등의 표준화 기구를 중심으로 설립된 프로젝트 그룹이다. 특히 3GPP 산하 그룹인 SA3는 서비스 및 시스템 측면을 담당하고 있으며 주로 보안과 관련된 표준을 개발하고 있다. 3GPP의 SA3에서는 제로트러스트에 대한 두 개의 표준이 개발 중이다.

### 가. TR 33.794 [9]

3GPP의 기술 보고서 TR 33.794 (Study on enablers for Zero Trust Security (Release 19))의 개발은 2024년 2월에 시작되었으며, 현재는 5월에 배포된 0.3.0 버전이 공개되어 있다. 이 기술 보고서는 보안 모니터링 및 평가를 위해서 수집되어야 할 다양한 정보를 식별하고, 정책 결정점 역할을 하는 외부의 운영자 보안 기능에게 수집되는 데이터를 보내기 위한 다양한 경우의 절차를 제시한다. 수집되어야 할 다양한 정보는 다음을 포함한다.

- 잘못 구성된 메시지에 대한 정보
- 방대한 양의 SBI 메시지
- 인가되지 않거나 또는 실패된 인증을 갖는 NF(Network function) 에서의 서비스 접근 요구
- 해킹된 NF에 의한 정찰 목적의 경고
- 비정상적인 SBI(Service based interfaces) 호출 흐름
- API 보안 위험

핵심 이슈로 두 가지 사항이 제시되었다. 첫째, 운영자의 보안 기능에서 보안 평가와 모니터링을 위한 데이터 노출 문제와 이를 해결하기 위한 관련 데이터 수집 수단에 대한 요구사항이다. 둘째, 서비스 구조에서 정책 이행을 위한 보안 메커니즘으로 공

격을 식별하고 완화할 수 있는 능력이다. 이를 위해 운영자의 보안 기능은 정책 결정점의 역할을 수행하며, 5G NF에 대한 정보를 제공하는 서비스 기반 구조 내에서 정책 이행점을 설정할 수 있는 적절한 수단을 제공해야 한다.

이를 위한 해결책으로써 여러가지 솔루션이 다음과 같이 제시되고 있다.

① 데이터 생성을 담당하는 운영관리 및 유지보수(Operation, Administration, and Maintenance, OAM) 및 네트워크 기능(Network Function, NF)과 데이터를 수집하여 운영자의 보안 기능으로 전송하는 NF, 그리고 정책 결정점 역할을 하는 운영자의 보안 기능의 실체로 구성되며 각 실체간의 수행되어야 할 절차를 정의하였다.

② 데이터 생성을 담당하는 NF와 정책 결정점 역할을 하는 운영자의 보안 기능의 실체로 구성되며 실체 간 수행되어야 하는 절차를 기술하였다.

③ 정책 결정점 역할을 하는 운영자의 보안기능과 운영자의 보안 기능이 정책 결정점 역할을 수행하는데 사용할 수 있는 SDPI(Security data point of ingest), SDPI 또는 다른 인터페이스를 통해 수집된 데이터를 사용하는 SDCF(Security data collection function), 데이터의 저장을 담당하고 운영자가 구성하는 보안 데이터 저장소인 SDRF(Security data repository function), SDPI에 있는 작업을 조정, 승인 및 모니터링하는 중개자 역할을 하는 보안 관리 기능 SADF(Security administration function) 그리고 이 외의 NF가 실체를 구성하고 있으며 각 실체간의 설정 절차와 데이터 전달 절차를 정의하고 있다.

④ SBA 계층에서 손상된 NF를 감지하기 위한 솔루션으로, SBA 계층에 존재하는 여러 개의 NF와 NF 보안 데이터를 수집 및 조정 기능을 수행하는 DCCF(Data collection and coordination function), 수집된 데이터를 분석하고 평가하는 NWDAF나 운영자 보안 평가 및 감시 시스템으로 실체를 구성한다. 또한 각 실체간 데이터의 수집 및 전송 절차를 상위 수준 관점에서 정의하고 있다.

⑤ NF와 외부 보안 관리 기능으로 구성되어 있으며 상호 간 로그 이벤트를 교환하기 위한 절차가 정의되어 있다.

### 나. TR 33.894 [10]

TR 33.894 (Study on applicability of the Zero Trust Security principles in mobile networks (Release 18))의 개발은 2022년 7월에 시작되었으며, 현재는 2023년 9월에 배포된 18.0.0 버전이 공개되어 있다. 이 문서는 5G 시스템에 적용해야 할 7가지 제로트러스트 원칙, 지속적인 모니터링이 필요하다는 핵심 이슈, 코어망 모니터링을 위한 보안 솔루션을 제공한다. 〈표 4〉는 3GPP TR 33.894에 적용되는 7가지 제로트러스트 원칙을 보여준다.

표 4. 3GPP TR 33.894의 7가지 제로트러스트 원칙

| | |
|---|---|
| (원칙 1) | 리소스<br>– 제로트러스트 구조는 모든 데이터 소스와 컴퓨팅 자원이 자원으로 간주된다. |
| (원칙 2) | 모든 통신은 네트워크 위치와 관계없이 보호 |
| (원칙 3) | 접근 세분성<br>– 세션 단위로 자원에 대한 접근이 허용되어야 한다. |
| (원칙 4) | 리소스 접근<br>– 자원에 대한 접근은 능동적 정책에 의해 결정되어야 한다. |
| (원칙 5) | 모든 자산의 무결성 및 보안 상태 유지<br>– 모든 소유되는 자산의 무결성과 보안 상태는 유지되어야 한다. |
| (원칙 6) | 접근 보안<br>– 모든 자원의 인증과 인가는 능동적이어야 하며 접근이 허용되기 전에 엄격히 이행되어야 한다. |
| (원칙 7) | 보안 상태 개선을 위한 데이터 수집<br>– 자산 보안 상태 네트워크 트래픽, 접근 요구, 절차 등에 대한 절차를 수집해야 한다. |

핵심 이슈와 보안 위협, 요구사항 및 핵심 이슈를 해결하기 위한 솔루션은 다음과 같다.

- **핵심 이슈**
  - 지속적인 보안 모니터링 필요
- **보안 위협**
  - 코어 네트워크에 네트워크 기능이 해킹되거나 악의적으로 행동하고 네트워크 기능이 오용되고 있다는 것을 발견하지 못할 경우, 서비스 장애, 데이터 손실과 같은 보안 위협을 초래한다.
- **가능한 보안 요구사항**
  - 5G 시스템은 보안 모니터링을 위해 필요한 데이터를 수집할 수 있는 메커니즘을 지원해야 한다.
- **솔루션**
  - (솔루션 1) 코어망을 위한 보안 모니터링을 가능하게 하는 데이터 수집
  - 데이터 수집을 위한 솔루션은 네트워크 데이터 분석 기능(NWDAF), 네트워크 기능(NF), 운영관리 및 유지보수(Operation, Administration, and Maintenance, OAM)간의 보안 모니터링을 위한 데이터 수집을 위한 절차와 데이터 분석 기능과 3GPP 외부의 보안 평가 및 모니터링 기능에 수집된 데이터를 보내고 평가 결과를 수신하는 절차를 기술한다. 데이터 분석 기능은 프록시로 동작한다.

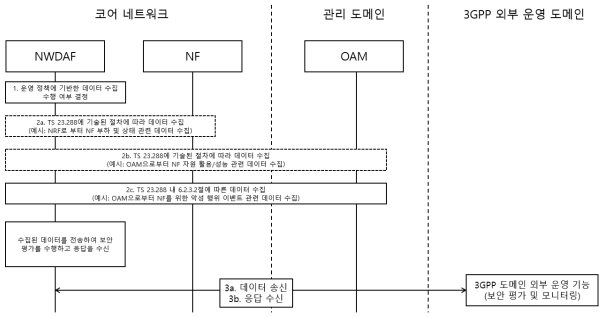


그림 4. NF의 정상적인 활성 단계에서 보안 모니터링을 활성화하는 절차

〈그림 4〉는 3GPP 네트워크에서 보안 모니터링을 활성화하기 위해 NWDAF 와 NF, OAM 간의 제로트러스트 관련 데이터를 수집하는 절차와 NWDAF와 3GPP 외부에서 운영되는 보안 평가 및 모니터링 기능 간의 제로트러스트 관련 데이터를 송신하고 응답하는 절차를 기술한다.

## 4. 미국 국가표준

### 가. NIST ST 800-207 [11]

미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 2019년 제로트러스트 아키텍처 프로젝트를 출범하여 이의 결과물로 2020년 제로트러스트 아키텍처(NIST SP 800-207) 문서를 공개하였다. 이 문서는 제로트러스트 전략을 제시하고, 제로트러스트 구조의 논리적 요소들과 배포 시나리오, 사용 사례, 제로트러스트 아키텍처와 관련된 위협을 정의하고 있다. 또한 기존 미국 연방 지침과의 상호 작용과 제로트러스트 아키텍처로의 마이그레이션 지침을 제공하고 있다.

이 문서에서는 기존 경계 기반 모델에서 벗어나 물리적으로 설정되는 경계를 제거하고 리소스 단위의 세밀한 논리적 경계를 설정하는 제로트러스트 전략을 제시하였으며, 이를 실행하기 위한 7가지 원칙을 〈표 5〉와 같이 제시하였다.

표 5. NIST SP 800-207 제로트러스트 7가지 원칙

| | |
|---|---|
| 1 | 모든 데이터 소스와 컴퓨팅 서비스는 리소스로 간주 |
| 2 | 네트워크 위치에 관계없이 모든 통신 보호 |
| 3 | 개별 조직 리소스에 대한 접근 권한은 세션 단위로 승인 |
| 4 | 리소스 접근은 동적 정책에 의해 결정 |
| 5 | 조직은 모든 소유 자산의 무결성 및 보안 상태를 감시하고 조치 |
| 6 | 모든 리소스의 인증 및 인가를 동적으로 강력하게 적용 후 접근 허용 |
| 7 | 조직은 자산, 네트워크 인프라, 통신의 현 상태에 대해 가능한 많은 정보를 수집하여 보안 상태를 개선 |

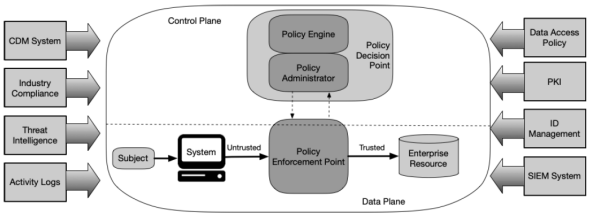


그림 5. 핵심 제로트러스트 논리적 구성요소[11]

〈그림 5〉는 이 문서가 제안하는 제로트러스트의 논리적 구성요소를 나타낸다. 제로트러스트 아키텍처에서 정책을 결정하고 시행하는 것은 핵심적인 보안 기능이며 이를 수행하는 요소가 정책 결정 지점(Policy Decision Point, PDP)과 정책 시행 지점(Policy Enforcement Point, PEP)이다.

또한 제로트러스트 논리 구성 요소의 배치 모델은 조직의 환경이나 기기 또는 리소스의 특성으로 인해 달라질 수 있으므로 이 문서에서는 다음 4가지의 배치 모델을 제안하였다.

① 기기 에이전트 – 게이트웨이 배치 모델
② 리소스 그룹 배치 모델
③ 리소스 포탈 배치 모델
④ 기기 응용 샌드박스 배치 모델

### 나. CISA 제로트러스트 성숙도 모델 [12]

미국 사이버 보안 및 인프라 보안국(Cybersecurity and Infrastructure Security Agency, CISA)은 연방 기관의 사이버 보안 태세를 강화하기 위한 조치로 2021년 8월에 제로트러스트 성숙도 모델(Zero Trust Maturity Model, ZTMM) 1.0과 2023년 4월에 2.0을 발표했다. 이는 2021년 5월 12일 발표한 미국 바이든 행정부의 "국가의 사이버보안 향상에 관

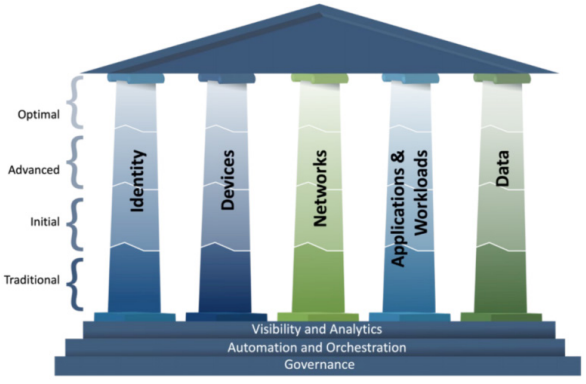


그림 6. 제로트러스트 성숙도 평가[12]

한 행정명령(Executive Order on Improving the Nation's Cybersecurity, EO 14028)[13]"이 연방 기관들이 제로트러스트 아키텍처를 도입하도록 명령한 것에 대한 정책적 일관성을 보여주는 것으로, 미국의 연방 기관들은 이에따라 제로트러스트 모델을 도입하고 제로트러스트 원칙을 기반으로 조직의 보안 계획을 개발해 실행해야 한다. CISA의 제로트러스트 성숙도 모델은 연방 기관들이 이를 잘 수행할 수 있는 지침을 제시할 뿐만 아니라 모든 조직들이 이 문서에 설명된 접근 방식을 검토하고 고려해야 한다고 강조한다.

CISA의 제로트러스트 성숙도 모델은 조직의 보안 시스템의 성숙도를 평가기기 위한 모델로, 2.3절의 NIST SP 800-207이 제공하는 제로트러스트의 개념과 제로트러스트 아키텍쳐 등 여러 문서들을 참조해 개발되었다. 이 문서는 〈그림 6〉과 같이 기관들이 제로트러스트 아키텍처를 구현하기 위해 필요한 다섯 가지 주요 영역(Pillar)을 정의하고 각 영역에 포함되는 세 가지 공통 기능, 그리고 영역 별 단계적 성숙도 (또는 최적화) 상태를 영역의 색에 대한 단계적 차이(Gradation)를 통해 나타내고 있다. 제로트러스트 성숙도 모델을 구성하는 핵심 영역에 간략한 설명은 〈그림 7〉과 같다.

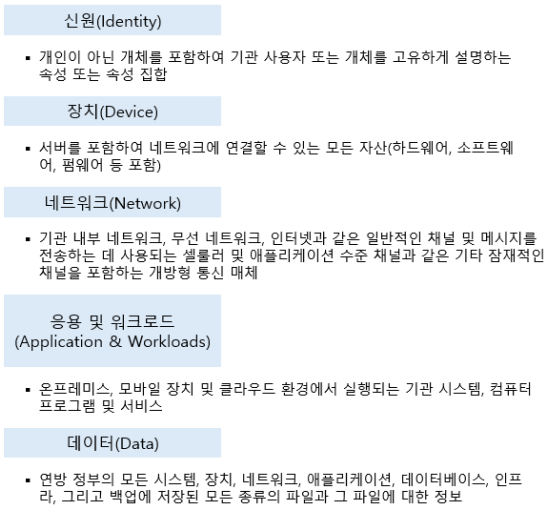


그림 7. 제로트러스트 성숙도 모델의 핵심 영역

또한 이 문서는 제로트러스트의 영역별 성숙도를 평가하기 위한 네 가지 단계를 〈표 6〉과 같이 설명하고, 핵심 영역별 성숙도 단계별 보안 기능도 제공한다.

표 6. 제로트러스트 성숙도 평가의 4가지 단계

| 단계 | 설명 |
|---|---|
| 전통적 수준 (Traditional) | • 수동적 구성: 모든 과정(설치~제거)과 속성 할당(보안 및 로그기록)의 수동적 구성<br>• 정적 보안 정책: 보안 정책이 한 번 설정되면 변경되지 않으며 외부 시스템에 의존적임. 특정 보안 영역만 독립적으로 관리<br>• 최소 권한: 초기 설정 시에만 최소 권한이 설정됨<br>• 분리된 정책 적용: 각 영역이 독립적으로 정책이 적용됨<br>• 수동 대응: 보안 문제에 대한 수동적 대응과 완화<br>• 제한된 상관 관계: 의존성, 로그, 원격 측정 데이터 간 제한된 분석 능력 |
| 초기 수준 (Initial) | • 자동화 시작: 속성 할당과 라이프사이클 구성, 정책 결정 및 시행, 초기 단계에서 외부 시스템 통합을 통해 자동화 시작<br>• 응답성: 초기 설정 이후에도 최소 권한으로 설정 변경 가능<br>• 통합 가시성: 내부 시스템에 대한 통합된 가시성 제공 |
| 고급 수준 (Advanced) | • 광범위한 자동화: 적용 가능한 경우, 라이프사이클과 구성 및 정책 할당이 자동화되고, 영역 간 조정 가능<br>• 중앙 집중식 가시성 및 제어: 중앙에서 모든 가시성과 신원 관리를 제어<br>• 정책 통합: 여러 영역에 걸쳐 통합된 정책 시행<br>• 정의된 대응: 사전에 정의된 완화 조치에 대응<br>• 위험 기반 변경: 위험 평가와 상태 평가에 기반해 최소 권한으로 설정 변경<br>• 기업 전반의 인식: 외부에 호스팅된 자원을 포함해 기업 전체의 인식(Awareness) 수준 검토 및 제고 |
| 최적 수준 (Optimal) | • 완전 자동화: 실시간으로 라이프사이클과 속성 할당이 자동으로 이루어지고, 자산과 리소스가 동적 정책에 따라 자동 보고<br>• 동적 최소 권한: 자산과 그들의 의존성에 대해 최소 권한 접근이 동적으로 이루어짐<br>• 영역 간 상호 운용성: 지속적인 모니터링과 함께 기둥 간 상호 운용성 존재<br>• 중앙 집중식 가시성: 포괄적으로 상황을 인식하고 이를 통해 중앙에서 모든 가시성을 관리 |

### 다. DoD의 제로트러스트 오버레이 1.0 [14]

미국 국방부(DoD)는 2024년 2월 제로트러스트 오버레이를 구축하기 위한 새로운 문서인 DoD 제로트러스트 오버레이 1.0(Zero Trust Overlays 1.0)을 공개했다. 이 문서는 적대적 환경을 가정하고, 침해를 전제로 하며, 결코 신뢰하지 않고 항상 검증하고, 명시적으로 검토하며, 통합 분석을 적용하는 등의 원칙을 기반으로 한다. 또한 DoD 제로트러스트 참조 아키텍처와 실행 로드맵을 토대로 특정 통제를 적용하여 제로트러스트 모델의 기둥들을 구현하기 위한 지침을 제공한다. 이 문서의 토대가 되는 DoD 제로트러스트 참조 아키텍처와 전략 보고서는 NIST SP 800-207를 기반으로 한다[15][16].

## 5. 영국NCSC [17]

영국 국가사이버보안센터(NCSC)는 영국 정부 기관이나 조직

등이 제로트러스트 아키텍처를 설계하고 구축할 때 활용할 수 있도록 NCSC 홈페이지를 통해 제로트러스트 아키텍처 디자인 원칙(Zero trust architecture design principles)을 공개했다. 제로트러스트의 개념과 제로트러스트 원칙 8가지를 소개하였다. NCSC 제로트러스트 아키텍처 디자인의 8가지 원칙은 〈표 7〉과 같다.

표 7. NCSC 제로트러스트 8가지 원칙

| |
|---|
| ① 아키텍처를 이해하라 (사용자, 기기, 서비스, 데이터 포함) |
| ② 사용자, 서비스 및 기기의 정체성을 파악하라 |
| ③ 사용자 행동, 서비스 및 기기의 건강 상태를 평가하라 |
| ④ 정책을 사용하여 요청을 승인하라 |
| ⑤ 모든 곳에서 인증 및 인가를 수행하라 |
| ⑥ 모니터링의 초점을 사용자, 기기 및 서비스에 맞추라 |
| ⑦ 어떠한 네트워크도 신뢰하지 마라 (자신의 네트워크도 포함) |
| ⑧ 제로 트러스트를 염두에 두고 설계된 서비스를 선택하라 |

## Ⅲ. 결 론

제로트러스트 보안은 새로운 보안 패러다임으로서, 모든 조직의 정보 인프라는 제로트러스트 구조로 변환될 필요가 있다. 본 논문에서는 주요 국제 표준화 기구인 ITU-T SG17, ISO/IEC JTC 1/SC 27을 비롯해 3GPP, 미국 국가표준, 영국 NCSC의 제로트러스트 관련 표준을 분석하였다.

향후 IoT, 스마트 공장, 스마트 의료, 6G 등 다양한 네트워크에 적용 가능한 제로트러스트 모델과 구조가 개발되고 표준화되어야 할 것이다. 우리나라는 제로트러스트 관련 기고를 제안해 ITU-T SG17 역사상 최초로 국제 표준 신규 작업 항목으로 채택되었다. 또한 제로트러스트 보안을 다음 연구 회기(2025-2028)에서 신흥 표준화 주제로 제안하여 반영하는 등 제로트러스트 보안 국제 표준을 주도함으로써 이에 대한 향후 국제 표준화를 위한 기반을 마련하였다.

## Acknowledgement

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

## 참 고 문 헌

[1] John Kindervag, “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture” Security & Risk Professionals (https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf)

[2] 박수정, 염흥열, “ITU-T SG17(정보보호) 전자 국제회의 결과”, TTA, 표준 · 시험인증 국제기구 동향 (2021. 05) (https://www.tta.or.kr/tta/preportNewsNDownload.do?sfn=20230507125249670_OtF3.pdf)

[3] 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)

[4] 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)

[5] ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy protection) (https://jtc1info.org/sd-2-history/jtc1-subcommittees/sc-27/)

[6] ISO/IEC CD 27090, “Cybersecurity — Artificial Intelligence — Guidance for addressing security threats to artificial intelligence systems” (https://www.iso.org/standard/56581.html)

[7] KSA한국표준협회, ISO/IEC 27001 (정보보호) (https://ksa.or.kr/ksa_kr/7011/subview.do)

[8] ISO/IEC 27002:2022, “Information security, cybersecurity and privacy protection — Information security controls” (https://www.iso.org/standard/75652.html)

[9] 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)

[10] 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)

[11] 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)
[12] Zero Trust Maturity Model 2.0, CISA, 2023. 04 (https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf)
[13] EO 14028, "Executive Order on Improving the Nation's Cybersecurity", The White House, 2021. 05 (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)
[14] Office of the Chief Information Officer, "Zero Trust Overlays 1.0", Depart of Defense(DoD), 2024. 02 (https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays-2024Feb.pdf)
[15] DoD Zero Trust Strategy, Department of Defense Office of Prepublication and Security Review, DoD, 2022. 07 (https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf)
[16] Defense Information Systems Agency(DISA) and National Security Agency (NSA) Zero Trust Engineering Team, "DoD Zero Trust Reference Architecture 2.0", DoD, 2022.07 (https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf)
[17] "Zero trust architecture design principles", NCSC Guidance, NCSC, 2021. 07 (https://www.ncsc.gov.uk/collection/zero-trust-architecture)

## 약 력

박 성 채

2008년 순천향대학교 정보보호학과 학사 졸업
2021년~현재 순천향대학교 정보보호학과 석·박사 통합과정
2007년~2009년 어울림정보기술(주) 연구원
2010년~2011년 이글루시큐리티 주임연구원
2020년~2022년 ㈜보다비 AI연구소 리더
2022년~현재 순천향대학교 차세대보안 표준전문 연구실 책임연구원
관심분야: 암호 프로토콜, AI 보안, 양자암호통신, 블록체인 보안, 5G/6G 보안, 개인정보보호 기술

박 준 형

2023년 순천향대학교 정보보호학과 학사 졸업
2023년 순천향대학교 정보보호학과 학·석사 연계과정
관심분야: 제로트러스트, 정보보호관리체계, 사이버위협인텔리전스, 악성코드 분석, AI보안

염 흥 열

1981년 한양대학교 전자공학과 학사 졸업
1983년 한양대학교 대학원 전자공학과 석사 졸업
1990년 한양대학교 대학원 전자공학과 박사 졸업
1990년~2024년 순천향대학교 정보보호학과 정교수
2024년~현재 순천향대학교 정보보호학과 명예교수
1982년~1990년 한국전자통신연구소 선임연구원
2009년~2016년 ITU-T SG17 부의장
2009년~2016년 ITU-T SG17 WP3 의장
2011년 한국정보보호학회 회장(역), 명예회장(현)
2020년~2023년 개인정보보호위원회 위원 (역)
2017년~현재 ITU-T SG17 국제의장
2019년~현재 분산신원증명 기술 및 표준화 포럼 의장
관심분야: 정보보호관리체계, 개인정보보호, IoT 보안, 네트워크 보안, 암호 프로토콜, 인공지능 보안과 프라이버시, 블록체인 보안, 5G/6G 보안