제로 트러스트 국내 표준 적용을 위한 기술 요구사항 분석

(An Analysis of Technical Requirements for Establishing Domestic Zero Trust Standards)

천승은*, 송지영**
(Seung Eun Cheon, Jiyoung Song)

요 약

현대 산업 인프라는 클라우드 확산과 분산 업무 형태로 인해 자원 경계가 모호해지고, 전통적인 경계 기반 모델의 한계를 드러내고 있다. 경계 기반 보안 모델은 경계 내부의 위협과 우회 공격에 취약하며, 이에 대응하기 위해 해외에서는 제로 트러스트(Zero Trust; ZT) 보안 모델에 관한 연구와 표준화가 활발히 진행되고 있다. ZT는 공격자가 네트워크 경계 내부에 존재한다는 전제하에, 지속적인 검증과 최소 권한 원칙을 적용하여 내부 위협과 우회 공격에 대응한다. 본 연구는 국내 ZT 표준 적용을 위한 기초 연구로서, NIST SP 800-207에서 정의한 제로 트러스트 아키텍처(Zero Trust Architecture; ZTA)를 기준으로 ZTA 구축, 사이버 보안 위험 관리, 연방 데이터 보안, ZT 정책 개발 방법론 등의 주요 요소를 비교 분석한다. 본 연구를 통해 해외 ZT 표준의 공통 요소와 차별적 특성을 도출하고, 이를 바탕으로 국내 ZT 표준 수립 및 적용을 위한 참고 지침을 제시한다.

■ 중심어 : 제로 트러스트 ; 요구사항 분석 ; 표준 비교 분석

Abstract

Modern industrial infrastructures have blurred resource boundaries due to the expansion of cloud environments and distributed work models, revealing the limitations of traditional perimeter-based security models. Perimeter-based security models are vulnerable to internal threats and bypass attacks, and to address these limitations, research and standardization efforts on the Zero Trust(ZT) security model have been actively pursued internationally. Zero Trust operates under the assumption that attackers may exist within the network perimeter and addresses internal threats and bypass attacks through continuous verification and the application of the principle of least privilege. This study serves as foundational research for the application of Zero Trust standards in Korea and conducts a comparative analysis of key elements of overseas ZT standards based on the Zero Trust Architecture(ZTA) defined in NIST SP 800-207, including ZTA implementation, cybersecurity risk management, U.S. federal data security, and methodologies for Zero Trust policy development. Through this analysis, the study derives common elements and distinguishing characteristics of overseas ZT standards and presents reference guidelines for the establishment and application of domestic Zero Trust standards.

■ keywords : Zero Trust ; Requirements Analysis ; Standards Comparison

Ⅰ. 서 론

변화하는 현대 산업 인프라 구조에서 네트워크 내부와 외부의 경계가 모호해지고 있기 때문에, 경계 기반 보안 모델이 보호할 수 있는 범위가 점차 초과하고 있다. 전통적으로 사용되어 온 경계 기반 보안 모델(Perimeter-based Security)은 내부 네트워크와 외부 네트워크를 명확히 구분하여 외부로부터의 위협을 차단하는 방식으로 보안을 수행해왔다. 이는 비교적 단순한 네트워크 구조에서는 효과적인 보안 모델이었다. 그러나 내부와 외부의 경계가 모호해진 현대 산업 인

* 정회원, 한남대학교 컴퓨터공학과
** 종신회원, 한남대학교 컴퓨터공학과
본 연구는 원자력안전위원회의 재원으로 소형모듈원자로규제연구추진단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다. (No. 1500-1501-409)
접수일자 : 2026년 02월 20일
수정일자 : 2026년 03월 26일
게재확정일 : 2026년 03월 30일
교신저자 : 송지영 e-mail: jysong@hnu.kr

프라에 경계 기반 보안 모델 적용은 분명한 한계점이 존재한다.

경계 기반 보안 모델은 네트워크 외부로부터의 위협을 차단하는 데 중점을 두고 있으므로, 네트워크 내부에 발생한 위협을 탐지하는 데 한계를 지닌다. 또한 우회 공격이나 네트워크를 악용한 공격과 같은 복합적인 위협에 대해서는 적절한 대응이 어렵다. 이러한 한계점에도 불구하고 실제 산업 인프라 운영 환경에서 내부 위협과 우회 공격 등을 전반적으로 고려한 국내 보안 모델 연구는 여전히 부족하다.

반면, 해외는 경계 기반 보안 모델의 한계점과 고도화 되어가는 현대 산업 인프라에 대응하기 위해 NIST(National Institute of Standards and Technology; NIST)에서 제안하는 '제로 트러스트(Zero Trust; ZT)' 보안 모델을 기준으로 지속적인 연구를 수행하고 있다. ZT는 공격자가 네트워크 내부에 존재한다는 가정을 전제로 하여, 기본적으로 사용자, 기기, 네트워크 위치 등 어떤 요소도 신뢰하지 않고, 지속적인 검증과 최소 권한 원칙에 기반하는 모델이다[1]. 이러한 특성으로 인해 ZT는 경계 기반 보안 모델의 내부자 위협과 우회 공격에 취약하다는 한계점과, 위협 탐지 및 대응 능력을 보완한다. 따라서 ZT는 조직의 네트워크 보안과 데이터 보호 전반에 새로운 대응 전략이 될 수 있으며, 고도화되는 산업 인프라에 핵심 보안 기술로 작용할 수 있다.

본 논문에서는 국내 산업의 보안 강화와 국내 ZT 표준 수립을 위한 기초 자료 제공을 목적으로 해외 ZT 관련 표준의 비교 분석한다. 각 표준이 명시하는 ZT 구현 원칙과 보안 목표 특징을 정리하여, 데이터 보안 및 신원 관리 측면에서 해외 동향을 분석한다. 또한, ZT 표준 수립을 논의할 시, 국내 환경에 적용하기 위한 참고로 활용할 수 있도록 표준 개발 과정에서 고려해야 할 기술적·관리적 요소를 제시한다.

다음 장에서는 해외에서 NIST SP 800-207을 기준으로 ZT 기술 적용과 ZT로 전환할 때 실질적 지침이 되는 관련 연구를 설명한다. 3장에서는 해외 ZT 표준안들을 비교 분석하여 도출된 각각의 특성들, 국내 표준 개발 시 고려할 사항을 설명하고, 마지막 결론에서 마무리한다.

Ⅱ. 관련 연구

이번 장에서는 논문 주제인 해외 ZT 표준안 비교 분석의 주요 대상이 되는 NIST SP 800-207, NIST SP 1800-35, NIST CSF, CIO 연방 ZT 데이터 보안 가이드, ETSI TS 104 102에 대해 소개한다. 본 논문은 국내 도입 시 정책 또는 아키텍처 수준에서 참고할 수 있는 비교를 목표로 하므로, 범용적인 ZT 원칙과 자산 보호 방법을 포함한 표준을 기준으로 주요 대상을 선정하였다. 선정된 주요 대상을 제외한 ZT 관련 연구들은 ZT를 적용한 서비스를 배포하는 상세한 방법 제시나, ZT를 실현하는 접근 제어, 마이크로서비스와 같은 특정 구현 환경 분석 등에 국한되어 있다. 따라서 특정 기술이나 응용 영역에 핵심을 두는 표준은 비교 분석 주요 대상에서 제외했다.

1. 내/외부 위협 대응을 위한 기존 보안 모델

전통적인 네트워크 보안 체계는 신뢰 구역과 비 신뢰 구역을 명확히 구분하는 경계 기반 보안 모델을 중심으로 발전해 왔다. 그러나, 경계 기반 모델 중 방화벽의 경우 패킷 필터링 방식만으로는 침투나 우회 공격을 효과적으로 차단하는 데 한계가 있다. 이에 따라 클라우드 환경이 도입된 현대적 인프라에 보안 실효성을 제고하기 위한 방화벽 기술의 개선과 운영 전략에 대한 논의가 이어지고 있다[2].

또한, 방화벽은 패킷 필터링과 허용/차단 중심이고, IDS(Intrusion Detection System; IDS)는 방화벽을 통과한 트래픽을 감시하는 보완 장치다. 방화벽과 IDS를 상호 운용하더라도 네트워크 확장과 복잡도 증가에 따라 이미 암호화된 공격이나 우회 경로를 통한 위협에 해당 보안 모델

의 실효성이 떨어진다는 분석이 제기되기도 했다[3].

한편, 경계 기반 모델의 한계를 극복하기 위해 ZT 외에도 다양한 보안 모델이 제안 되어왔다. 네트워크 구성을 실시간으로 변화시켜 공격자의 정보 수집을 차단하는 MTD(Moving Target Defence; MTD) 연구가 수행되었으며[4], '인증 전 비가시성'을 원칙으로 하는 SDP(Software-Defined Perimeter; SDP) 모델의 경우 ZT의 핵심 기술로 기능하기도 한다[5].

2. ZT 개념 및 아키텍처 중심

ZT 관련 표준은 핵심 원칙 및 보안 아키텍처를 정의하는 개념 중심 문서와, 이를 실제 환경에 적용하기 위한 구현 중심 문서로 구분할 수 있다. 이번 절에서는 개념 및 아키텍처 중심 문서를 중심으로 살펴본다.

NIST SP 800-207은 ZTA의 대표적인 표준으로, ZT 연구들이 다루는 ZT 개념 및 원칙의 기준선 역할을 한다. 후술할 표준안들이 NIST SP 800-207의 원칙에 의존하고 있다. 해당 표준은 모든 리소스를 잠재적 보호 대상으로 간주하고, 네트워크 위치와 무관한 보호를 원칙으로 한다. 또한, 세션 기반 접근 제어와 동적 정책을 통한 지속적 인증과 권한 부여를 강조하며, 자산 상태 모니터링과 광범위한 보안 정보 수직을 통한 지속적인 보안 상태 개선을 요구한다.

한편, NIST CSF(Cybersecurity Framework; CSF)는 ZT에 특화된 표준은 아니지만, 조직 거버넌스 및 리스크 관리 관점에서 ZT 구현에 참조할 수 있는 프레임워크다. CSF는 사이버보안 성과(Outcomes)를 상세하게 구분하기 위해 'CSF 코어'를 거버넌스(Govern; GV), 신원(Identify; ID), 보호 조치(Protect; PR), 탐지(Detect; DE), 대응(Respond; RS), 복구(Recovery; RC)라는 여섯 가지 기능으로 분류하여 설명하고 있다[6]. NIST SP 1800-35 웹 문서는 CSF 코어에 기반하여 서브 카테고리와 ZTA의 논리적 요소를 매핑한 자료를 제공하고 있다[7].

ETSI TR 103 937의 경우, 사이버 복원력과 공급망 보안 관점에서 ZT 접근 방식을 설명한다. 해당 문서는 자산 관리 관점에서 공급망 관점까지 확장된 ZT를 이해할 수 있는 문서다[8].

3. ZT 실무 구현 및 도입 중심

NIST SP 1800-35는 ZTA를 실제 시스템에 적용하기 위해 참조 가능한 아키텍처와 구현 예시를 정리한 가이드로, NIST SP 800-207에서 정의된 원칙에 기반하여 다양한 구축 사례와 유즈케이스를 제공한다. 지속적인 모니터링과 정책 재평가, 신원·자격 증명 및 접근 관리(Identity, Credential, and Access Management; ICAM), 이벤트 대응과 같은 요소를 중심으로 시나리오를 제공하여 ZTA 구현 방안을 구체화한다[9].

NIST SP 800-207A 및 NIST SP 800-204 시리즈는 ZTA를 다양한 환경에 적용하기 위해 확장된 기술적 가이드를 제공한다. 마이크로서비스 기반 시스템의 보안 요구사항이나 속성 기반 접근 제어(Attribute-Based Access Control; ABAC) 적용을 다룬다[10][11][12].

CIO 연방 ZT 데이터 보안 가이드(Federal Zero Trust Data Security Guide)는 CISA의 ZT 성숙도 모델(Maturity Model)을 활용하여 조직의 관점에서 ZT 도입 수준과 적용 전략을 제시한다. CISA의 성숙도 모델은 조직이 ZTA로 전환하는 단계를 제시하여 실무적인 도입 기준을 제공한다[13]. CIO의 가이드는 데이터 중심 보안을 강조하여 데이터 인벤토리의 구축 및 관리, 조직 간 협력과 같은 거버넌스 관점 요구사항을 제시한다[14].

한편, ETSI TS 104 102 및 104 103은 암호화된 트래픽으로 발생하는 문제와 ZT를 구현하는 요구사항을 다룬다. ETSI TS 104 102는 ZT-Kipling 방법론과 Kipling Criteria를 통해 정책(policy) 정의와 적용 절차를 체계화하여 기

표 1. 분석 대상 선정 기준

구분	기준
포함 기준 1	ZTA 아키텍처 또는 핵심 원칙을 포함
포함 기준 2	자산 보호, 접근 통제, 모니터링 요구사항을 명시
포함 기준 3	특정 기술/환경에 국한되지 않는 범용적 지침
제외 기준 1	특정 기술/환경/응용 분야에 한정된 문서
제외 기준 2	다른 표준과 중복성을 가진 하위 개념 문서

존의 기술 중심 접근을 보완한다[15]. ETSI TS 104 103은 신뢰할 수 있는 통신 환경을 제공하기 위한 ZT 구현 요구사항을 제공한다[16].

4. 분석 대상 선정 기준

본 연구는 해외 ZT 표준 문서를 비교 분석하기 위해 표1과 같은 기준을 적용하여 분석 대상을 선정했다. 첫째, ZTA 아키텍처 또는 핵심 원칙을 포함한 문서를 대상으로 한다. ZT 개념의 이해와 비교를 가능하게 하기 위함이다. 둘째, 자산 보호, 접근 통제 및 모니터링과 관련된 요구사항을 명시하는 문서를 포함한다. ZT에서 요구하는 보안 요구사항을 비교하기 위함이다.

그러나, 특정 기술 구현이나 개별 응용 분야 또는, 다른 표준에서 이미 상세히 설명되어 중복성을 갖고 유의미한 비교가 불가능한 문서는 분석 대상에서 제외했다. 이러한 기준에 따라 NIST SP 800-207, NIST SP 1800-35, NIST CSF, CIO 연방 ZT 데이터 보안 가이드, ETSI TS 104 102를 주요 분석 대상으로 선정했다.

Ⅲ. 본 론

이번 장에서는 논문 주제인 해외 ZT 표준안 비교 분석과 관련하여 각 표준안의 핵심 구성과 관점을 비교하고, 국내 도입 시 요구사항과 고려할 요소를 검토한다. 비교 분석 대상은 NIST SP 800-207, NIST SP 1800-35, NIST CSF, CIO 연방 ZT 데이터 보안 가이드, ETSI TS 104 102의 원문 표준안이다.

표준안의 주요 내용은 2장 관련 연구에서 언급했으므로, 본 3장에서는 표준간 구성과 관점 차

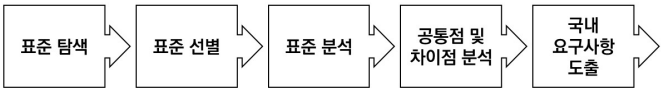

그림 1. 연구 흐름도

표 2. 비교 분석 프레임워크 개요

비교 축	설명
구조적 관점	표준이 개념/구현 중 어디에 집중하는지
네트워크 세분화 관점	자산 분리 및 접근 통제 수준
기술적 관리 관점	인증, 접근 제어, 모니터링 요구 수준
조직적 관리 관점	거버넌스 및 조직 역할 요구 수준

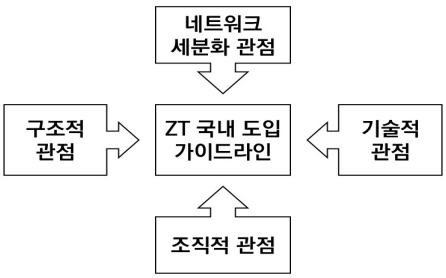

그림 2. 비교 분석 프레임워크 개념도

이를 비교하여 국내 표준 개발 시 고려할 사항을 도출한다. 해외 ZT 표준 비교 분석은 그림 1과 같이 표준 탐색, 선별, 분석의 단계를 거쳐 진행했다.

표준 탐색 단계에서는 공신력 있는 국제 표준화 기구(NIST, ETSI 등)에서 발행한 공식 문서와 최신 공개 자료를 중심으로 ZT 관련 표준을 식별하였다. 또한, 각 표준의 언급된 기관 및 관련 문서를 기반으로 연관 표준을 추가적으로 수집하였다.

표준 선별 단계에서는 수집한 문서를 대상으로 표 1과 같은 기준을 적용하여 분석 대상을 선정하였다. 또한, 표준 분석 단계에서는 선별한 각 문서를 목차 및 세부 절 단위로 구분하여 주요 원칙과 요구사항을 도출하고, 이를 기반으로 표 2 및 그림 2와 같은 기준을 세워 표준 간 공통점과 차별적 특성을 비교하였다.

1. 해외 ZT 표준의 핵심 구성 및 관점 비교

표 3. 해외 ZT 표준안 요약

ZT 표준안	목적	적용 범위	주요 원칙/개념	활용도
NIST SP 800-207	ZTA 정의 및 원칙의 포괄적인 집합 제공	리소스 보호	암묵적 신뢰 배제, 최소 권한, 지속 검증	ZTA 구현 요구사항
NIST SP 1800-35	ZTA 구현 방법 설명	ZTA 구축	ZTA 예제 구축, 유즈케이스 시연	ZTA 구축/전환/검증 프레임워크
NIST CSF	사이버 보안 위험 관리 지침 제공	사이버 보안 위험 관리	CSF 코어, 우선순위	ZTA 보안 프레임워크
CIO 가이드	보안 실무자를 위한 ZT 데이터 보안 가이드 제공	ZT 데이터 보안	데이터 인벤토리, 협력 관계 유지	조직의 ZTA 실행 프레임워크
ETSI TS 104 102	ZT 접근 방법론 제시	ZT 정책 개발	ZT-Kipling, Kipling Criteria	ZT 정책 개발 방법론

이번 절에서는 논문의 주요 대상이 되는 표준안들을 본격적으로 비교 분석한다. 표준안들은 크게 개념 정의, 관리 지침 제공, 구현 방법 설명의 세 가지 특징을 보였고, 이들 중 어느 특징에 더 집중하여 설명하고 있는지에 따라 표준안의 성격이 구분되었다.

3.1.1절에서 표준안의 성격을 구분하고, 3.1.2절부터 3.1.4절까지는 표준안이 네트워크를 얼마나 세분화하여 보안 강도를 높이는지 비교하여, 조직의 네트워크 및 자산 관리 요구 수준을 기술적 관점과 조직적 관점으로 나누어 분석한다.

3.1.1. 해외 ZT 표준의 구조적 비교

2장 관련 연구에서 다룬 각각의 해외 ZT 연구

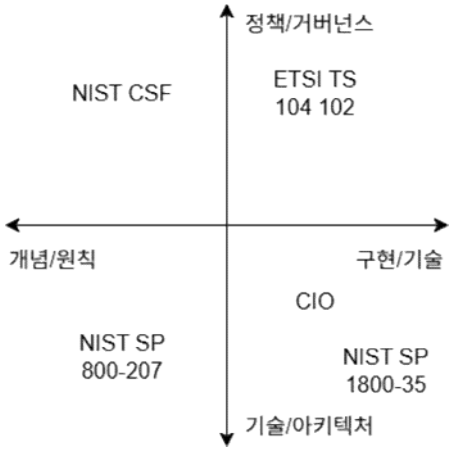

그림 3 해외 ZT 표준안 관점 비교

들은 ZT 및 ZTA라는 키워드를 다루지만, 표면적인 관점에서 각 연구가 다루는 주제들은 지향하는 목적에서부터 차이점이 있었다. 표 3과 그림 3은 2장에서 설명한 상세한 내용을 바탕으로, 비교 대상을 항목별로 정리하고 관점별로 시각화한 것이다.

표 3은 해외 ZT 표준들의 목적과 적용되는 범위, 다루고 있는 주요 원칙 및 개념, 국내 ZT 표준 도입 시 활용할 수 있는 방안을 요약한 것이다. 이 비교 항목들은 각 표준이 중점으로 다루는 범위에서 지향하는 보안 목표를 파악하고, 국내 도입 시 정책 및 아키텍처 수준에서 참고할 수 있는 부분을 분석하기 위해 선정했다.

그림 3은 해외 ZT 표준안별 관점을 정책/거버넌스, 기술/아키텍처, 개념/원칙, 구현/기술로 나누어 분류한 도식이다. 도식에서 X축은 표준이 개념이나 원칙을 중심으로 설명하는지, 또는 구체적인 구현이나 기술적인 면에서 설명하는지를 나타낸다. Y축은 표준이 정책 및 거버넌스 차원에서 보안 지침을 제공하는지, 또는 기술이나 아키텍처를 구현하는 지침인지를 나타낸다.

NIST SP 800-207은 ZTA를 제시하여 본 논문에서 다루는 연구의 기초가 되었다. ZTA의 개념적인 관점에서 다루므로 구축 방법, 보안 거버넌스, 정책 개발 등의 세부 사항들은 다른 연구에서 상세하게 다루고 있다.

NIST CSF는 직접적으로 ZT를 다루지 않았으

표 4. 해외 ZT 표준안별 네트워크 세분화 수준

ZT 표준안	VLAN	마이크로 세그멘테이션	SDN 사용 여부	중앙 제어 범위	문서 관련 위치
NIST SP 800-207	△ (특정 조건)	△ (특정 조건)	△ (특정 조건)	PE/PA, PEP (△, 분산 제어)	Sec. 3, Sec. 3.4
NIST SP 1800-35	X	O	O	-	Sec. 3
NIST CSF	X	X	X	-	Preface
CIO 가이드	X	△ (특정 조건)	X	신원 및 정책 관리, 접근 제어 (△, 분산 제어)	Sec. 3.7, Sec. 3.8
ETSI TS 104 102	X	△ (특정 조건)	X	-	Annex A

나, NIST SP 1800-35에서 진행한 실험과 연계하여 ZT 개념과 보안 기능을 살펴볼 수 있도록 했다. CIO의 연방 ZT 데이터 보안 가이드는 연방기관뿐만 아니라 조직 및 보안 실무자가 참조할 수 있는 ZTA 실행 지침을 제공하며, ETSI TS 104 102는 ZT 개념이나 기능보다는 조직이 ZTA를 구축하거나 전환하는 과정에서 ZT 정책을 개발하기 위한 방법론을 제시했다.

3.1.2. 해외 ZT 표준의 네트워크 세분화 비교

표 4는 해외 ZT 연구 각각이 다루고 있는 네트워크 세분화 수준을 요약한 것이다. ZT는 사용자가 자산에 접근할 때마다 신원을 검증하는 것이 핵심 원리이므로, 접근 통제가 적용되는 자산의 논리적 분리 수준은 자산이 속한 환경의 보안 강도에 직접적인 영향을 미친다. 따라서, 표 4의 비교 항목은 표준에서 자산이 속한 환경을 어느 수준까지 세분화하는지를 기준으로 선정했다.

각 연구에서 ZT를 구현할 때 특정 기술 사용을 설명하고 있는지를 기준으로 표기한다. 관련 서술이 있는 경우 'O', 없는 경우 'X', 일부 내용을 포함하거나 특정 조건에서 사용/설명하는 경우엔 '△'로 표기한다. 단순 VLAN(Virtual Local Area Net work; VLAN) 수준, 마이크로 세그멘테이션 단위, SDN(Software Defined Network; SDN) 사용 여부, 중앙 제어 허용 범위를 기술했다.

표 4에 나타난 바와 같이, 대부분의 ZT 표준은 네트워크 기술보다 정책 및 신원 중심 접근을 강조하며, 기술 중립을 기본 원리로 두고 있다. 그러나 NIST SP 800-207과 CIO 연방 ZT 데이터 보안 가이드의 경우 예시 수준에서 마이크로 세그멘테이션 사용 가능성을 암시하고 있다. 또한, NIST SP 800-207의 경우 정책 엔진(Policy Engine; PE)과 정책 관리자(Policy Administrator; PA)는 중앙이 제어하고, 정책 집행 지점(Policy Enforcement Point; PEP)은 분산 제어가 가능하다고 명시하고 있다.

NIST SP 1800-35는 NIST SP 800-207을 전적으로 따르지만, 실험 아키텍처를 구현하고 테스트를 실행할 때 마이크로 세그멘테이션과 SDN 컨트롤러가 핵심적으로 활용되었다. NIST CSF는 조직 리스크 기반 보안 거버넌스 중심이므로 구현 기술은 조직 전적으로 맡기는 것으로 본다.

CIO 연방 데이터 보안 가이드는 조직이 신원 및 정책을 관리해야 하고, 접근 제어의 경우 분산 처리해야 된다고 설명하고 있다.

ETSI TS 104 102는 정책 개발 접근 방법론이기에 직접적인 명시보다 Annex에서 5G 유즈케이스를 설명할 때 마이크로 세그멘테이션을 구성 요소로 포함해야 함을 제시하고 있다.

3.1.3. 해외 ZT 표준의 관리 요구 수준-기술적 관점

표 5는 신원·접근 관리와 모니터링 세 범주로 나누어 비교한 것이다. ZT는 지속적인 신원 검증과 접근 통제를 전제로 하므로, 사용자가 접근 이후에 보이는 행위를 조직이 감시하는 모니터링 체계가 함께 요구된다. 따라서, 표 5의 비교

표 5. 해외 ZT 표준안별 관리 요구 수준

ZT 표준안	신원 인증·인가	접근 제어 집행	모니터링·로깅	문서 관련 위치
NIST SP 800-207	O	O	O	Sec. 2
NIST SP 1800-35	O	O	O	Sec. 3
NIST CSF	O	X	O	Sec. 2, Appendix A
CIO 가이드	O	O	O	Sec. 3.6, Sec. 3.7
ETSI TS 104 102	O	O	O	Sec. 4.4, Sec. 5.6

항목은 표준이 조직의 모니터링 기능을 어느 수준으로 언급하는지를 기준으로 선정했다.

각 비교 항목별로 기능이나 관련 서술이 있는 경우 'O', 기능이나 관련 서술이 없는 경우 'X'로 표기했다. 대부분의 비교 대상은 조직이 모든 관리 기능을 수행하도록 요구하고 있지만, 각 표준의 특성과 지향하는 바에 따라 관리 기능을 요구하는 방식과 관점에서 차이가 있다.

NIST CSF는 'PR' 기능에서 신원과 자산 관리를 다루고, 'DE' 기능에서 모니터링·로깅을 다룬다. 그러나, CFS 특성상 가이드라인 성격을 가지므로 관련한 기술 구현은 조직 자율로 맡긴다.

반면, NIST SP 800-207과 1800-35, CIO 연방 ZT 데이터 보안 가이드는 신원·접근 제어 및 모니터링을 강조하고 있으며, ETSI TS 104 102는 이를 간주하여 방법론을 제시하고 있다.

NIST SP 800-207은 MFA(Multi-Factor Authentication; MFA) 사용과 ICAM 및 SIEM 시스템 구축을 전제로 ZT 원칙을 정의하므로 신원·접근 제어와 모니터링을 강제하고 있다. NIST SP 1800-35에서 실행한 모든 구현 예시는 IdP(Identifier Provider; IdP), MFA, SIEM, PE, PA, PEP를 핵심 구성 요소로 포함하므로 신원·접근 제어와 모니터링을 필수적으로 다루는 것으로 보인다. ETSI TS 104 102의 경우 ZT 보안 정책 생성(4단계) 시 신원·접근 제어가 포함되고, 모니터링 및 유지보수(5단계)가 ZT-Kipling 생명주기에 포함되므로 모니터링을 전제로 두고 있음을 알 수 있다.

3.1.4. 해외 ZT 표준의 관리 요구 수준-조직적 관점

ZTA 관리 요구 수준을 비롯하여, ZTA를 사용하는 조직이나 보안 실무자 요구사항에서도 차이점이 있다.

NIST SP 800-207과 NIST SP 1800-35는 ZTA 구축 방향성을 제공하는 문서이므로 조직 역할에 대한 언급은 상대적으로 부족하다. 반면, NIST CSF는 'GV' 기능에서 조직의 역할을 정의하고, 조직의 감사 및 규제 항목을 포함한다. CIO 연방 ZT 데이터 보안 가이드는 조직이 ZT 전략을 수립하고 이행할 책임이 있고, ZT 성숙도 목표와 진척 상황을 보고할 것을 명시하고 있다. ETSI TS 104 102는 ZT-Kipling 방법론을 적용하는 조직이 모니터링 및 유지보수 단계를 수행할 것을 설명한다.

2. 국내 도입 시 요구사항 도출

해외 ZT 표준안들은 NIST SP 800-207을 철학적·구조적 기준서로 활용하며, NIST CSF를 조직 리스크 관리와 보안 프로세스를 참고하는 데에 활용하고 있다. 해외 ZT 연구들 비교를 기반으로, 이들 연구가 공통으로 다루는 요구사항들은 다음 일곱 가지로 정리된다. (1) 자산 단위로 권한 세분화, (2) 신원·접근 관리(IAM/ICAM) 적용, (3) 정책 실행·통제의 구조화, (4) 모니터링·로깅, (5) 데이터 보호, (6) 조직 간 책임 분리 명시, (7) 감사·규제 준수로 정리할 수 있다. 그러나, 이들 요구사항은 국내 산업에 즉각 적용하는 데 한계가 있다.

국내 ZT 표준 수립 시에는 표 6과 같이 명확한 지향성이 보이는 구조와 함께, 네트워크 세분화 수준, 기술적 관리, 조직적 관리 관점이 반영되어야 한다.

(1) 구조적 관점

해외 ZT 표준은 대개 개념 정의 후에 관리 지

표 6. 국내 ZT 도입 요구사항 정리

관점	핵심 요구사항	국내 적용 요구사항	적용 대상	적용 범위
구조적 관점	신뢰 경계 재정의, 자산 보호 철학 제시	자산 중요도 및 자산 경계 정의, 국내 법제(개인정보보호법 등)를 반영한 보안 목표 정의	표준 수립 기관	공공/민간
네트워크 세분화 관점	자산 중요도 기반 단계적 세분화 적용	국가정보원 가이드라인에 따른 망 분리 적용 및 보안 통제 항목 제시[17]	네트워크 및 보안 관리 시스템	클라우드/온프레미스
기술적 관리 관점	지속적 모니터링 체계 구축	기존 보안 장치와 ZT 솔루션 간 연동 및 로그 분석 적용	보안 관제 센터	전 조직 및 자산
조직적 관리 관점	역할 분리 및 책임 요소 정의	ZT 원칙에 기반한 접근 승인 프로세스 수립 및 교육	조직/거버넌스	전 조직

침이나 구현 가이드를 설명하는 구조로 구성되어 있다. 단순한 기술 요구사항 나열이 아닌, 신뢰 경계 재정의와 자산을 보호하는 철학을 먼저 제시한 뒤에 세부 통제를 서술하는 구조이다. 따라서, 표준의 적용 범위와 목적, 보안 목표를 명확히 제시하여 표준 활용성을 보이고, 상위 정책 원칙을 먼저 정의한 뒤 하위 세부 정책을 설명하는 구조로 표준의 확장성을 확보해야 한다.

(2) 네트워크 세분화 관점

국내 기업 환경을 고려할 때 초기 단계에서 완전한 마이크로 세그멘테이션 적용이 어려울 수 있다. 자산 중요도나 조직 구성에 기반한 현실적인 전환 방법과 세분화 기준 제시가 필요하다. 또한, 조직 환경과 국내 기술 현황을 고려하여 단계적인 요구 수준이 마련되어야 한다.

(3) 기술적 관리 관점

기술적 관리 관점 또한 기존 자산 관리 및 보안 인프라 간의 연계 가능성과 단계적 전환을 고려한 요구사항 제시가 필요하다. ZTA는 단순히 신규 기술 도입이 아니라 기존 보안 장비와 조직 환경 등의 연동이 함께 이루어지는 보안 전략이다. 따라서, 세분화한 네트워크별로 철저한 모니터링과 접근 통제를 위해 상호운용성을 확보한 전략이 제시되어야 한다.

(4) 조직적 관리 관점

조직적 관리 관점에서는 국내 법제 및 컴플라이언스를 고려한 조직 운영 체계 기준이 제시되어야 한다. ZT 전략은 조직 환경의 연동이 함께 이루어지므로, 조직의 역할 분리와 책임 요소를 명확히 정의해야 성공적인 ZT 운영이 이루어질 수 있다. 또한, 사용자 교육과 지속적인 감사 체계 등의 요소도 포함되어야 한다.

해외 ZT 표준들로 미루어 보아, 국내 도입 시 추가적인 검토가 필요한 점은 네트워크 세분화 정도 및 관리 요구 수준 정의와 국내 산업별 적용 가능성을 분석하는 것이다. 또한, 국내 공공기관 가이드라인을 개발할 시 국내 법제·컴플라이언스와의 충돌 여부를 확인하고, 조직 규모별 도입 비용 및 운영 인력 문제 등의 난이도를 측정하는 연구가 필요할 것이다.

운영 요건이 충족되고 충돌 가능성이 관리 가능하다면, 본 논문에서 분석한 해외 ZT 표준안들은 국내 ZT 표준안 수립에 참조 문서로 활용될 수 있다.

Ⅳ. 결 론

본 논문에서는 국내 ZT 표준 적용에 참고할 수 있도록 해외 ZT 표준의 기술적·관리적 요구사항을 비교 분석했다. 해외 ZT 표준의 접근 방식과 핵심 원칙을 비교한 결과, 각 표준안은 접근 방식과 기술적 강조 부분에서 차이를 보이지만, 최소 권한 원칙, 신원 중심 접근, 지속적인 모니터링과 검증이라는 핵심 원칙에서 공통된 방향성을 확인할 수 있었다.

비교 결과를 기반으로 국내 ZT 표준안을 구축할 때 고려해야 할 기술적·조직적 요구사항과 접근 과정에서 해결해야 할 쟁점을 도출하였다. 조직 거버넌스와 단계적 전환 등의 필요성이 도출되었으며, 이들 요구사항 및 쟁점은 국내 ZT 표

준 수립 시 중요한 기준이 될 수 있다. 그러나, 국내 환경을 고려한 적용 가능성과 단계적 도입을 위한 요구사항 구축에 추가적인 검토가 필요하다. 또한, 실제 적용 사례를 통해 요구사항이 구체화 되고 검증되어야 한다.

REFERENCES

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, *NIST Special Publication 800-207,* Aug. 2020.

[2] S. Thompson and J. Liu, From Perimeter to Cloud: Innovative Approaches to Firewall and Cybersecurity Integration, *International Journal of Trend in Scientific Research and Development,* Vol. 3, No. 5, pp. 2751-2759, Aug. 2019.

[3] Anamika, Network Perimeter Security on Large Scale Networks, *Journal of Advances and Scholarly Researches in Allied Education,* Vol. 16, Issue No. 6, pp.2776-2781, May. 2019.

[4] 김도훈, 최수현. MTD를 활용한 허니시스템 능동방어전략 구축 방안 연구. *한국정보기술학회지,* 20(1), pp. 27-32. Dec. 2022.

[5] 이윤경, 김정녀, 제로 트러스트를 위한 소프트웨어 정의 경계(SDP) 인증 메커니즘 제안 및 ECC 암호 구현, *Journal of the Korea Institute of Information Security & Cryptology,* Vol.32, No. 6, pp. 1069-1080, Jan. 2022.

[6] NIST, *The NIST Cybersecurity Framework(CSF) 2.0*, NIST CSF 2.0, Feb. 2024

[7] Implementing a Zero Trust Architecture: Full Document(2025), https://pages.nist.gov/zero-trust-architecture/VolumeE/Mappings.html (accessed Dec., 6, 2025).

[8] ETSI, Cyber Security (CYBER); Cyber Resiliency and Supply Chain Management, ETSI Technical Report 104 937 V1.1.1, Aug. 2024.

[9] S. Rose, O. Borchert, A. Kerman, M. Souppaya, et al., Implementing a Zero Trust Architecture: High-Level Document, *NIST Special Publication 1800-35,* Jun. 2025.

[10] R. Chandramouli and Z. Butcher, A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments, *NIST Special Publication 800-207A*, Sep. 2023.

[11] R. Chandramouli and Z. Butcher, Building Secure Microservices-based Applications Using Service-Mesh Architecture, *NIST Special Publication 800-204A,* May. 2020.

[12] R. Chandramouli, Z. Butcher and A. Chetal, Attribute-based Access Control for Microservices-based Applications using a Service Mesh, *NIST Special Publication 800-204B*, Aug. 2021.

[13] CISA, Zero Trust Maturity Model(2023), https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf (accessed: Mar., 21, 2026).

[14] CIO, Federal Zero Trust Data Security Guide(2024), https://resources.data.gov/assets/documents/Zero-Trust-DataSecurityGuide_RevisedMay2025_CIO.govVersion.pdf (accessed: Mar., 23, 2026).

[15] ETSI, Cyber Security (CYBER); Encrypted Traffic Integration (ETI); ZT-Kipling methodology, *ETSI Technical Specification 104 102 V1.1.1,* Sep. 2025.

[16] ETSI, *Cyber Security (CYBER); Encrypted Traffic Integration (ETI); Problem Statement review and requirements definition*, *ETSI Technical Specification 104 103 V1.1.1,* Sep. 2025.

[17] 국가사이버안보센터, 국가 망 보안체계 보안 가이드라인 1.0(2025), https://www.ncsc.go.kr/cmm/fms/PdfFileView.do?uuid=56247779-ff9c-441c-af28-8200851e88ed&fileSn=0 (accessed: Mar., 23, 2026).

저 자 소 개

천승은(정회원)

2026년 한남대학교 컴퓨터공학과 학사 졸업.

<주관심분야 : 소프트웨어공학, 소프트웨어 품질보증, 요구사항공학, 데이터 보안>

송지영(종신회원)

2014년 이화여자대학교 컴퓨터공학과 학사 졸업.

2016년 한국과학기술원 전산학부 석사 졸업.

2022년 한국과학기술원 전산학부 학과 박사 졸업.

<주관심분야 : 소프트웨어공학, 소프트웨어 테스팅, 소프트웨어 모델 검증, 프로젝트 관리, 시스템 오브 시스템즈, IoT, CPS>