*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.34, NO.6, Dec. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.6.1431

# 국내 제로트러스트 활성화를 위한 제언: K-제로트러스트 정책 개선 방향성을 중심으로

김 자 현,[1†] 김 법 연,[2] 권 헌 영[2‡]
[1,2]고려대학교 (대학원생, 교수)

# Suggestions for Promoting Zero Trust in Korea: Focusing on the Improvement Directions of the K-Zero Trust Strategy

Ja-Hyun Kim,[1†] Beop-Yeon Kim,[2] Hun-yeong Kwon[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

디지털 대전환의 물결은 새로운 보안 모델 도입의 필요성을 불러일으키고 있다. 어디에서나 기업 시스템에 접속할 수 있다는 점은 네트워크 경계 구분에 근본적인 의문을 던지며 기존의 경계 중심 보안 모델을 무의미하게 하고 있다. 이에 미 연방을 필두로 제로 트러스트 전략을 채택하는 움직임이 일어났으며 국내 또한 정부 차원에서 적극적인 활성화 정책을 펼치고 있다. 1차 실증지원 사업의 성과가 발표된 현시점에서 해당 사업의 실질적인 결과를 분석하여 추후 개선 방향성을 논의할 필요가 있으나, 이에 대한 견해는 제시된 바가 없다. 해당 실증사업 및 제로트러스트 가이드라인 1.0을 분석한 결과 구현 모델의 완전성, 성숙도 평가 체계의 정확성, 가이드라인 고도화의 필요성 등 한계점을 도출하였다. 본 연구에서는 이에 대한 대응방안을 제시하고 나아가 제로트러스트 적용을 통한 국내 정보보호 제도 전반의 개선 가능성을 분석한다. 이를 통해 국내 제로트러스트 활성화를 촉진하고, 나아가 글로벌 제로트러스트 패권 경쟁에서의 경쟁력을 확보하기 위한 토대를 마련하고자 한다.

ABSTRACT

The rapid progression of digital transformation demands advanced security models, as traditional perimeter-based approaches are increasingly inadequate in an era of remote access to enterprise systems. In response, the U.S. federal government has pioneered zero trust strategies, with South Korea following suit through active policy measures. Despite the completion of South Korea's first Zero Trust Pilot Project, a comprehensive analysis remains lacking. This study evaluates the pilot project and Zero Trust Guidelines 1.0, highlighting key limitations in implementation, maturity assessment frameworks, and guideline refinement. Solutions are proposed to address these issues, emphasizing the need for improved policies to advance national information security and position South Korea as a leader in the global zero trust landscape.

**Keywords:** Zero Trust, Zero Trust Strategy, Zero Trust Architecture, Zero Trust Maturity

## I. 서 론

4차 산업혁명의 산물은 지구촌에 디지털 대전환의 시대를 열었다. 사물인터넷(IoT)과 자율주행은 5G/6G 통신 기술을 급속도로 발전시키는 원동력으로 작용하였으며 인공지능(AI)과 빅데이터 및 클라우드 컴퓨팅은 대용량 처리를 가능케 하는 CPU, 그래픽 카드 등 핵심 하드웨어 산업의 성장을 이끌고 있다. 이렇듯 첨단 기술의 발전으로 인해 네트워크와 인프

Received(09. 30. 2024), Modified(11. 05. 2024), Accepted(11. 10. 2024)
† 주저자, jahyun97@korea.ac.kr
‡ 교신저자, khy0@korea.ac.kr(Corresponding author)

라가 확장되면서 점차 더 많은 장치와 서비스가 네트워크의 경계를 넘나들며 정보를 교환하고 있다. 무엇보다도 BYOD(Bring Your Own Device)의 추세가 확산되며 스마트 오피스 및 홈오피스와 같이 장소에 구애받지 않고 전 세계 어디에서든 업무 시스템에 접속할 수 있게 되었다. 이러한 원격 근무의 보편화는 업무의 편의성 증대라는 큰 장점을 불러오나, 접속 장치와 접근 표면이 확장됨으로써 기존의 명확했던 네트워크 경계를 무의미하게 하기도 하다. 즉, 사이버 보안 관점에서 시스템과 인프라 환경의 변화는 새롭게 발견될 결함과 조치에 대해 논의가 필요함을 의미한다.

사이버 범죄의 수법이 날로 교묘해지고 그 빈도가 활발해지고 있는 현 시점에서 이러한 논의의 필요성은 더욱 가중된다. 특히 최근 급속도로 발전한 형태로 수행되는 지능형 지속 위협(APTs)은 전체 사이버 공격의 21.85%를 차지하고 있다는 보고도 있다[1]. 주목할 만한 점은 신뢰할 수 있는 관계를 주요 공격 벡터로 악용했다는 것인데, 이는 공격자가 기업 내부자로 위장하여 시스템으로부터의 신뢰를 획득하고 자유롭게 공격을 수행할 수 있다는 의미이다. 이러한 가운데 접근제어 강화 등이 필요하다는 주장이 제기되고 있으나, 이 방식으로도 내부자로 위장한 악성 공격자의 침입을 탐지하기에는 한계가 존재하며 시스템에서 행해지는 권한 상승 및 데이터 유출 등의 악성 행위를 완전히 추적하는 데는 어려움이 존재한다. 즉, 기존의 보안 전략 하에 세부적인 대응책을 강구한다고 하여 내부자 위협에서 기인하는 APT 공격을 근본적으로 방어하는 데는 분명한 한계점이 존재한다는 것을 시사한다[2]. 이에 미 연방을 중심으로 제로트러스트(이하 “ZT”)를 새로운 보안 전략으로 채택하자는 움직임이 일어났고 관련 백서 및 가이드라인이 배포되며 학술 연구와 보안 제품들이 출시되고 있다. 국내에도 ZT 도입 활성화를 위해 국가 차원에서 다양한 정책들을 펼치고 있다. 과학기술정통부와 한국인터넷진흥원은 2023년 한국제로트러스트위원회(KOZETA)를 발족하고 ‘제로트러스트 실증지원사업’을 주관하여 공공 및 민간기업을 대상으로 ZT 아키텍처 구축을 진행하였으며 2024년에는 ‘제로트러스트 도입·전환 컨설팅’을 통해 자체 투자 여력이 있으나 전략 수립에 어려움을 겪는 기업 등을 대상으로 컨설팅을 지원할 예정이라고 밝혔다. 그러나 △한정된 실증사업 대상과 예산 부족, △솔루션 부재 등 기술적 한계, △ZT 전문가 부족, △구체적인 가이드라인 부재 등으로 인해 아직도 도입을 망설이는 기업들이 존재한다[3], [4]. 기술적 한계와 더불어 ZT에 대한 명확한 가이드라인이 부재하여 ZT를 확실하게 이해하고 있는 전문가가 없다는 현실적 문제에 직면하고 있는 것이다. 이에 본 연구에서는 국내 정책 상 ZT 도입 저해 요인을 분석하여 실증사업 및 가이드라인에서 실질적인 한계점을 도출하고 이에 대한 해결 방향을 제시하고자 한다. 2장에서는 제로트러스트 모델 및 주요국 정책 동향을 분석하고, 3장에서는 K-제로트러스트 실증사업 결과와 가이드라인을 분석하여 한계점의 대응 방안을 제시하며 4장에서는 결론을 제시한다.

## II. 제로트러스트 모델 및 동향

### 2.1 제로트러스트 모델

NIST에서는[5] ZT를 언제 어디서든 위협이 발생할 수 있다는 인식을 기반으로 기업 내부의 네트워크, 시스템 또는 리소스에 접근하려는 모든 사용자 및 장치에 대해 지속적인 인증, 세밀한 접근제어, 최소한의 권한 부여 등 적극적인 신뢰도 평가 없이는 접근을 허용하지 않는 보안 모델로 정의한다. 제로트러스트 아키텍처(이하 “ZTA”)는 논리적 구성 요소로 이루어지며 특정 대상에 대한 리소스 접근 권한을 부여하는 최종 결정 지점인 정책 결정 지점(PDP, Policy Decision Point)과 이러한 결정을 명령으로 변환하고 주체와 리소스 간의 통신 경로를 설정하는 정책 관리자(PA, Policy Administrator), 명령을 받아 주체와 리소스 간의 연결을 활성화 혹은 종료시키는 정책 시행 지점(PEP, Policy Enforcement Point)으로 구성된다. ZTA를 구현할 수 있는 모델로는 Fig.1과 같이 3가지가 제시된다. 첫 번째로, EIG(Enhanced Identity Governance)는 다중 인증 기법(MFA, Multi Factor Authentication), 지속적 인증, 최소 권한 원칙 등 인증 체계의 전반적인 강화를 목적으로 사용자가 네트워크에 접속한 후 주기적 혹은 이벤트 기반으로 신원을 재확인하고 사용자의 행동패턴을 분석하여 이상 징후 탐지 시 추가 인증을 요구하는 특징이 있다. 두 번째로, Micro Segmentation은 네트워크를 워크로드의 단일 혹은 그룹 단위 세그먼트로 나누고 각 세그먼트에 별도 보안 정책을 적용하여 악의적 행위 발생 시 횡적 이동을 차단함으로써 리소스 오염을 최소화하도록 하는 방식이다. 세 번째로, SDP(Software Defined

Perimeter)는 사용자 및 단말이 리소스에 대한 접근을 요청하면 SDP 컨트롤러에서 해당 주체에 대한 신뢰성을 검증한 후 해당 리소스로 접근할 수 있는 단독 데이터 채널을 형성하여 악성 행위자의 리소스 무단 접근을 차단하는 방식이다. NIST에 따르면 3가지 모델을 모두 구현하여야 완벽한 ZTA를 구축할 수 있다[5].

ZTA 구축을 완료한 후 해당 아키텍처가 ZT의 기본 원칙을 모두 이행하고 있는지에 대한 성숙도 평가를 진행하여야 한다. 주요국의 각 기관 및 민간 기업에서는 저마다 성숙도 평가 기준을 제시하고 있다. 이는 CISA에서[6] 발표한 Zero Trust Maturity Model 2.0을 기반으로 Table 1과 같이 그 핵심 요소(혹은 필라)에 차별성을 두고 있으며 국내에서도 제로트러스트 가이드라인1.0 내에 성숙도 평가 체계를 기술하고 있다. 각 성숙도 모델의 공통점으로는 Identity, Data, Device, Network, Application이 포함되어 있으며 국내의 경우 기반 시설 관련 보안 컴플라이언스가 상대적으로 강화된 상황을 고려하여 System이 추가되어 있는 것을 확인할 수 있다[9].

Table 1. Zero Trust Maturity Pillars

| Forrester | CISA | KISA | NSA |
|---|---|---|---|
| • Data<br>• Network<br>• People<br>• Workload<br>• Device<br>• Visibility and Analytics<br>• Automation and Orchest-ration | • Identity<br>• Device<br>• Network/ Environme nt<br>• Applications and Workload<br>• Data | • Identity<br>• Device/ Endpoint<br>• Network<br>• System<br>• Application and Workload<br>• Data | • User<br>• Device<br>• Network and Environ -ment<br>• Applications and Workload<br>• Data<br>• Automation and Orches-tration<br>• Visibility and Analysis |

## 2.2 주요국 제로트러스트 정책 동향

미국은 2020년 8월, NIST에서 SP 800-207 및 35 시리즈를 발표하며 ZTA에 대한 정의 및 구현 아키텍처 사례, 예제 솔루션과 시나리오 등을 제시함으로써 실질적인 ZT 활성화 정책을 시작하였다. 이후 2021년 5월, 바이든 대통령이 '국가 사이버보안 개선을 위한 행정명령'을 통해 미국 공공 ·정부기관에 ZT 전략을 채택하겠다고 발표하고, 이에 발맞춰 CISA에서는 Zero Trust Maturity Model 1.0을 발간하였으며 DoD에서는[17] Zero Trust Strategy을 통해 상세한 기준, 도입 전략, 아키텍처 모범 사례 등을 제시하고 있다.

영국은 2021년 7월, 제로트러스트 아키텍처 설계의 8 원칙을 발표하였다[19]. 미국에 비해 사용자, 기기, 데이터 등 조직의 디지털 자산에 대한 식별 및 상태 점검을 강조하고 있으며, 다수의 보안 서비스가 ZT를 지원하지 않을 가능성이 높고 이러한 서비스와의 통합에 있어 오버헤드가 발생할 수 있으므로 ZT를 고려하여 설계된 대체 서비스를 고려해야 한다고 강조하고 있다.

일본은 2022년 6월, '제로트러스트 아키텍처 적용 정책'을 발표하여[18] ZT 원칙 및 이를 구현하기 위한 방안을 제안하고 있으나 별도의 성숙도 평가 기준이 누락되어 있으며 영국과 마찬가지로 실질적인 아키텍처 모범 사례 등을 추가적으로 발표하고 있지 않다.

이외에도 캐나다, 호주, 싱가폴 등에서도 ZT 도입 원칙을 제시하고 있으나 미국의 행보와는 다르게

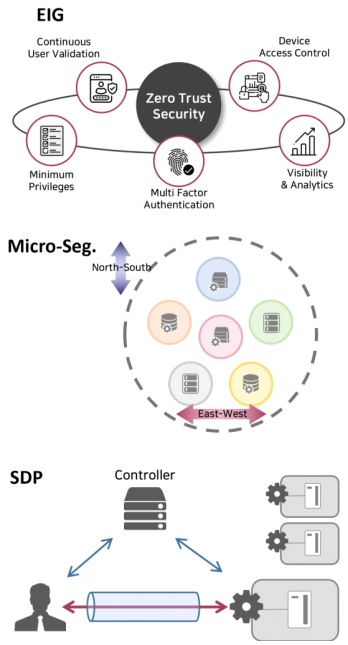


Fig. 1. Varioations of Zero Trust Architecture Approaches

공공 및 민간에 실무적으로 도움이 될 만한 후속 가이드라인은 배포하지 않고 있으며 국가 전략으로 채택하거나 재정을 투입하여 지원하는 등 세부 정책 또한 시행하고 있지 않아 민간의 자율적인 도입을 추구하고 있는 것으로 보인다.

한국은 2022년 10월, 한국 제로트러스트포럼을 발족하여 도입에 대한 산·학·연 간 전문적인 논의를 지속해오고 있으며 2023년 4월, 대통령 직속 디지털플랫폼정부위원회에서는 국가적 차원의 제로트러스트 도입 추진계획을 발표하였다. 이후 과학기술정보통신부에서[9] 제로트러스트 가이드라인1.0을 발표하고 제로트러스트 모델 발굴 및 확산을 위해 약 10억원 규모의 실증지원 사업을 추진하기도 하였다. 국가정보원은 사이버안보 민관합동협의체를 구성하여 국가 및 공공 영역에서의 사이버보안 강화를 위한 정책을 논의하여 2024년까지 K-제로트러스트 구축 가이드 및 시범 적용을 추진하고 있다[6]

## III. K-제로트러스트 정책 분석 및 한계점 논의

### 3.1 K-제로트러스트 실증 지원 사업 개요

디지털플랫폼정부는 제로트러스트 보안을 포함하여 신 보안체계를 2024년까지 도입하겠다고 발표하였다. 이에 과학기술정보통신부와 한국인터넷진흥원은 지난 2023년 제로트러스트 보안 모델 실증 지원 사업을 수행하여 다양한 산업군의 업무 환경에 적용 가능한 제로트러스트 보안 모델을 구현 및 실증하는 비용과 보안 모델에 대한 보안성 분석·평가를 지원하였다. 에스지에이솔루션즈(이하 “SGA”)와 프라이빗테크놀로지(이하 “PRIBIT”)는 각 컨소시엄을 구성하여 국내 공공기관, 이동통신사, 금융사 등 다양한 기업체에 ZTA를 구현하였으며 엔키화이트햇에서 이에 대한 보안성 평가를 진행하였다. SGA 컨소시엄은 제로트러스트 가이드라인1.0의 기본 원리, 핵심요소, 3가지 구현 모델 방법을 준용하여 ZTA를 구축하였다고 밝혔다[7]. 엔키화이트햇은 MITRE ATT&CK 기반 침투 시나리오를 기반으로 공격자 관점의 침투시험(Penetration Test, 모의해킹)을 수행하여 ZT 성숙도를 측정하였다[8]. Identity, Device/Endpoint 등 6개의 핵심원칙을 기반으로 침투시험용 공격전술을 구상하여 침투 성공 여부를 통해 ZT 도입으로 인한 보안성 효과를 측정하였다. 그러나 본 연구진이 주요 ZT 가이드라인을 기준으로 해당 기업에서 발표한 아키텍처를 분석한 결과, 기본 원칙 준수 및 구현 모델의 완전성에 있어 다수의 한계점이 있는 것을 발견하였다. 본 연구에서는 실증사업에 참여한 두 주관사 중 SGA에서[7] 구체적인 ZTA 모델 구성을 발표하였기에 해당 아키텍처를 기준으로 분석을 진행하였다. 두 주관사는 Table 2와 같이 각기 다른 구현 모델을 통해 ZTA를 구축했다. SGA는 EIG 모델을 채택하여 ICAM(Identity, Cridential Access Management)과 ZTNA Zero Trust Network Access) 중심의 강화된 접근제어 체계를 구축하였다. PAM(Privileged Access Management)을 통해 리소스 시스템에 대한 세분화된 접근제어 및 모니터링을 수행하도록 하였으며, ZTNA를 통해 네트워크의 안전한 접근제어를 구현하였다. UEM(Unified Endpoint Management)을 통해 백신 및 패치 업데이트 여부 등을 포함한 엔드포인트의 통압 보안을 실현하였다. RBI(Remote Browser Isolation)를 통해 응용수준에서 논리적 경계를 설정하였으나, 이는 외부의 위협이 확산되는 것을 방어하는 데 목적이 있고 내부 위협에 대해서는 대응하지 못하므로 이를 Micro Segmentation이라고 보기에는 어렵다.

Table 2. Implementation Status of the Zero Trust Archtiecture Model

| Model | SGA | PRIBIT |
|---|---|---|
| EIG | O | X |
| Micro Segmentation | X | X |
| SDP | X | O |

### 3.2 K-제로트러스트 실증 지원 사업의 한계점

본 연구진은 주요국 ZT 가이드라인을 기준으로 실증지원 사업에서 구현한 ZTA를 분석한 결과 (1) 기본 원칙 준수 여부, (2) 구현 모델의 완전성, (3) 성숙도 평가 체계의 정확성에 있어 한계점을 발견하였다.

#### 3.2.1 기본 원칙 준수 여부

실증사업의 ZTA는 국내외 가이드라인에서 제시하는 ZT 기본 원리를 일부만 준수하고 있다. NIST에서는 7개의 원칙을 제시하고 있는데 이 중 “자원 접근은 동적인 정책에 따라 결정”, “모든 자원의 인

증 및 권한 부여는 동적으로 수행하며 접근마다 엄격히 적용", "기업은 자산, 네트워크 인프라, 통신에 대한 정보를 최대한 수집하여 보안 상태를 개선" 원리를 충족하지 못하고 있다는 견해이다. ICAM은 정책 통합관리 시스템으로 시스템에서 사용자를 인증하고 권한을 관리하는 프레임워크이다[7]. 사용자 또는 장치의 디지털 신원을 관리하고 자격증명을 발급 및 추적하여 네트워크나 시스템에서 허가된 자원에 대한 접근을 제어한다[8].

SGA는 ICAM을 통해 모든 접근 결정에 대해 Trust Score를 기반으로 접근제어를 구현하였다. ICAM은 정책 관리자에 의한 정책 수정을 허용하기는 하나 동적인 접근제어 즉, 이벤트에 기반한 실시간 접근제어를 수행하는 기능은 포함되어 있지 않다. 별도로 구축한 PAM과 ZTNA 또한 일정 시간을 주기로 정기적인 접근제어는 가능하나 실시간 보안 상태를 반영한 접근제어는 불가능하다. 또한, 사용자 및 장치에서 컨텍스트 정보를 수집하여야 하나 UEM은 장치 관리와 보안 정책을 주기적으로 적용하는 방식으로 동작하므로 사용자의 행동을 실시간으로 분석하여 즉각적으로 반응하는 동적 접근 통제를 완벽히 구현하는 데는 한계가 있다.

NIST에 따르면 사용자 트랜잭션 중에는 지속적인 모니터링과 재인증 및 재권한 부여가 수행되어야 한다[5]. SP 1800-35B에서는 동적 속성 평가, 지속적인 보안 분석, 상황 기반 정책 적용을 통해 동적 접근 제어를 구현하는 사례를 제시한다[20]. 각 사례에서는 엔드포인트 혹은 소프트웨어의 취약성과 관련된 위협 인텔리전스나 사용자 행동에서 이상 징후가 감지될 경우, 이를 반영하여 동적으로 권한을 재인증할 것을 요구한다. 구체적으로는 PIP를 통해 보안 상태 및 위협 정보를 수집하여 ICAM에 전달하고, 이를 동적 인증 과정에 반영해야 한다. 또한, UBA/UEBA(User and Entity Behavior Analytics)를 도입하여 엔티티의 비정상적 행동을 실시간으로 탐지하거나 SIEM(Security Information and Event Management) 혹은 EDR(Endpoint Detection and Response)을 UEM과 통합하여 엔드포인트에서 발생하는 모든 활동을 실시간으로 분석함으로써 동적 접근 제어를 실현할 수 있다.

### 3.2.2 구현 모델의 완전성

SGA의 ZTA는 Micro Segmentation과 SDP를 적용하지 않아 구현 모델의 완전성이 다소 떨어진다. SGA에서 횡적 이동을 방지하기 위해 설계한 PAM과 ICAM은 권한 관리 및 접근 제어 기능을 제공하지만 네트워크 수준의 트래픽 제어, 위협 탐지, 자동화된 대응 등의 측면에서는 Micro Segmentation을 완전하게 구현했다고 보기 어렵다. NIST뿐만 아니라 국내 가이드라인에서도 완전한 ZT 구현을 위해 세 가지 모델을 모두 적용해야 한다고 명시하고 있다[4],[9]. Table 3와 같이 각 구현 모델은 준수해야 할 기본 원칙 항목이 상이하므로, 모든 원칙을 충족시키기 위해서는 상호 보완적으로 모든 모델을 적용할 필요가 있다. 기업의 상황에 따라 특정 모델을 중심으로 구현할 수 밖에 없는 제한이 있을 수 있으나, 정부 차원의 실증 사업이라는 측면에서 구현의 완전성을 추구하는 것이 필수적이다. 또한, 가이드라인 배포 이후 처음 시행되는 실질적인 정책으로서, 해당 아키텍처가 모범사례로 자리잡을 가능성이 높으므로 Micro Segmentation과 SDP를 포함한 전방위적 구현이 필요하다. 다른 주관사인 PRIBIT 역시 SDP 모델을 채택하였으나, 동일한 이유로 동적 인증 체계 강화 및 Micro Segmentation을 함께 구현하는 것이 바람직할 것이다.

### 3.2.3 구현 평가 체계의 정확성

실증 지원 사업 내 성숙도 평가 체계의 개선이 필요하다. 본 실증지원 사업은 엔키화이트햇에서 모의침투를 기반으로 보안 수준을 진단하고 이에 기반한 성숙도 평가를 수행하였다[8]. 그러나, 제로트러스트 실증사업은 취약점 평가가 아닌 성숙도 평가를 통해 그 구현 여부를 판단하여야 한다[5]. ZT의 목표가 보안성 향상이기는 하나 그 구현을 실증하기 위해서는 ZT 원칙의 부합 여부와 성숙도 모델의 주요 항목 기반의 성숙도 수준을 평가하여야 할 것이다. 또한, 해당 주관사는 침투시험 성공개수를 기준으로 성숙도를 판단하고 있어[8] 국내 가이드라인에서 제시된 기준에도 부합하지 않으며 취약점 진단에 있어 침투시험이 갖는 자체 한계점도 존재하므로 평가 체계의 정확성 및 완전성이 저해될 수도 있다. 모의침투는 모든 시스템이 아닌 제한된 범위에서의 일시적 평가

를 수행하고 알려진 취약점 기반의 체크리스트를 기반으로 시나리오를 작성하므로 공격벡터 개수에 제한이 있어 시스템의 전반적 평가에도 부적합하다[10]. 무엇보다 ZT 성숙도 모델에는 거버넌스, 가시성 확보 및 자동화 등 정성 평가 대상인 항목이 다수 포함되어 있으나[6] 모의침투로는 해당 항목의 보안성 수준을 평가할 수 없다. 따라서, 공인된 성숙도 모델을 기준으로 ZTA 실증 평가를 수행하여야 하며 모의침투는 ZT의 효과성을 판단하는 수단으로 활용함이 적합할 것으로 사료된다.

Table 3. Compliance with Principles by ZTA Implementation Models

| Basic Tenet | EIG | Micro Seg. | SDP |
|---|---|---|---|
| (1) All data sources and computing services are considered resources | O | O | O |
| (2) All communication is secured regardless of network location | - | O | O |
| (3)Access to individual enterprise resources is granted on a per-session basis | O | - | O |
| (4) Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes | O | - | - |
| (5)The enterprise monitors and measures the integrity and security posture of all owned and associated assets | O | O | O |
| (6) All resource authentication and authorization are dynamic and strictly enforced before access is allowed | O | O | - |
| (7) The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture | O | - | - |

### 3.2.4 가이드라인의 실효성

NIST의 SP800-35시리즈는 다양한 산업군에 대한 아키텍처의 모범사례를 구체적으로 제시하고 있는 반면 아직까지 국내 가이드라인은 비교적 일반적인 지침을 제공하는 경향이 있다[11]. 특히 성숙도 평가 항목의 상세 내용에 있어 실제 기술 도구 및 전략을 명확하게 제시하지 않아 평가 시 혼란을 야기하거나 일관된 평가를 저해할 수 있다[12]. 이를테면, 시스템 항목에서 자동화 및 통합 기능의 최적화 수준을 "보안과 성능 최적화를 위한 지속적인 환경 변화에 적응"으로 기술하고 있으나 해당 항목의 명세만으로는 실제 자동화 및 통합 수준을 명확하게 평가하기 어렵다. 시스템을 지속적으로 모니터링하며, 특정 이

Table 4. Comparative Analysis of Domestic Guidelines and CISA's Maturity Model Results

| Pillar | Consistency | Omitted Functionality |
|---|---|---|
| Identity | 71% | • ID Store<br>• Risk Assessment |
| Device | 86% | • Asset and supply chain risk management |
| Network | 86% | • Network Segmentaion |
| Application | 65% | • Application threat prevention<br>• Secure application development and deployment workflow<br>• Application security testing |
| Data | 25% | • Data inventory management<br>• Data classification<br>• Data availability<br>• Data access<br>• Visibility and analytics capabilities<br>• Automation and orchestration capabilities |
| Cross Cutting | 100% | - |

Table 5. Analysis of the Applicability of Zero Trust to ISMS-P

| Category | Applicability | Details | ZT elements |
|---|---|---|---|
| (1) Establishment and Operation of the Management System | 83% | • Executive Involvement<br>• Organizational Structure<br>• Policy Establishment<br>• Information Asset Identification<br>• Risk Assessment<br>• Establishment and Operation of Protection Measures<br>• Establishment and Operation of the Management System<br>• Compliance with Legal Requirements | • Identity<br>• Device<br>• Data<br>• Governance |
| (2) Protection Measures Requirements | 81% | • Policy, Organizationand Asset Management<br>• Personnel Security<br>• External Party Security<br>• Physical Security<br>• Authentication and Authorization Management<br>• Access Control<br>• Encryption<br>• Information System Acquisition and Development Security<br>• System and Service Operation and Security<br>• Incident Prevention and Response<br>• Disaster Recovery | • Identity<br>• Device<br>• Network<br>• Application<br>• Data<br>• Governance |

벤트 발생 시 보안 정책을 자동으로 변경하는 등의 구체적인 기능을 평가 항목에 명확히 기술해야 한다. 추상적인 표현의 사용은 실제 시스템을 평가할 때 광범위하게 해석될 여지가 있어 정성적인 평가를 수행하여야 하는 경우 평가의 정확성이 저해될 가능성이 높을 것으로 사료된다.

또한, 평가 기준의 세분화가 필요하다. 글로벌적으로 통용되는 CISA의 성숙도 모델은 2023년 개정되어 성숙도 수준이 4단계(Traditional, Initial, Advanced, Optimal)로 구체화된 반면, 국내 가이드라인의 평가 기준은 3단계에 머물러 있으며, '공급망 위험 관리', '애플리케이션 개발 및 배포의 안전성', '데이터 분류' 등 세부 항목에서 보완이 필요하다. 본 연구에서 CISA의 성숙도 모델 평가 항목 160개를 기준으로 국내 성숙도 모델을 맵핑하여 비교한 결과 Table 4와 같이 약 32%의 항목이 누락되어 있음을 확인하였다. 특히 애플리케이션과 데이터 필라의 평가 항목을 보완할 필요성이 도출되었다.

## IV. K-제로트러스트 정책 활성화 방안

### 4.1 제로트러스트 가이드라인의 고도화

국내 제로트러스트 가이드라인은 개념적 설명과 도입 절차 중심으로 작성되어 있어 실제 현장에서의 적용을 지원하는 세부 지침이 부족하다. 이로 인해 국내에서 실증한 ZTA 또한 기본 원칙 준수와 성숙도 수준 달성에 있어 일관성과 명확성이 떨어지는 한계가 있다.

이를 보완하기 위해 미국 NIST SP 1800-35 시리즈의 사례를 참고한 고도화가 필요하다. NIST SP 1800-35 시리즈는 ZTA의 설계, 구현, 검증, 규정 준수를 포괄적으로 다루며, 다양한 사용자 층을 고려한 맞춤형 지침을 제공한다. 이를 토대로 국내 제로트러스트 가이드라인은 다음과 같은 개선 방안을 통해 고도화될 수 있다.

첫째, 실질적인 기술 구현 지침이 포함되어야 한다. NIST SP 1800-35B, SP 1800-35C SP 1800-35D는 ZTA 모범사례 및 실제로 적용하기 위한 단계별 설치 및 구성 방법을 구체적으로 설명하고 있으며, 실무자들이 이를 기반으로 조직 환경에 맞게 구체적으로 적용할 수 있도록 설계되어 있다[20], [21], [22]. 국내 가이드라인 역시 조직의 인프라 환경과 요구사항을 반영한 구체적 구현 예시를 제공함으로써, 기술적 적용의 실효성을 강화할 수 있을 것이다. ZTA가 실제 운영 환경에서 어떻게 적용되어야 하는지에 대한 명확한 지침을 제공하여 실무자의 이해와 실행을 지원하는 데 기여할 수 있다.

둘째, 다양한 기능 검증 시나리오와 위험 분석 맵핑의 추가가 필요하다. NIST SP 1800-35D는 [22] 신뢰도 관리, 접근 통제, 세션 관리 등의 보안 기능을 특정 시나리오를 통해 실증하여, ZTA 정책의 실질적 작동 방식을 평가한다. 국내 가이드라인도 각종 보안 시나리오와 테스트 사례를 추가함으로써

다양한 위협 환경에서 ZTA의 효과성을 검증할 수 있는 방법론을 제공해야 한다. 이를 통해 조직은 정책의 실효성을 높이고, 다변화하는 보안 위협에 대한 대응력을 강화할 수 있다.

셋째, 성숙도 모델을 구체화할 필요가 있다. NIST 및 CISA는 조직의 보안 성숙도 수준에 맞춰 단계별로 필요한 구성 요소와 평가 기준을 구체적으로 제시하여, 각 조직이 자사의 보안 상태에 맞는 ZTA 도입 계획을 수립할 수 있도록 한다. 국내 가이드라인 역시 성숙도에 따른 요구사항과 평가 항목을 세분화하여, 조직이 현재의 보안 성숙도에 맞춰 ZTA를 단계적으로 도입하고 점진적으로 발전시킬 수 있는 방향성을 제시할 필요가 있다.

국내 제로트러스트 가이드라인은 실질적인 적용 가능성을 높이고, 규정 준수와 위험 관리 측면에서 보안 성숙도에 따른 맞춤형 지침으로서의 역할을 수행해야 한다. 국내 조직들이 ZTA를 효과적으로 도입하고 운영할 수 있는 종합적 프레임워크를 제공하여, 제로트러스트 보안 모델의 성공적인 구현을 지원하는 데 기여할 수 있을 것이다.

### 4.2 국내 보안 컴플라이언스와의 연계

제로트러스트는 기존 보안 패러다임과 상반되는 개념이 아닌, 보다 세밀한 제어를 통해 보안 수준을 향상시키는 것을 목적으로 하는 새로운 보안 모델이다[4]. 국내 다수의 기업은 일정 조건을 충족할 경우 정보보호 및 개인정보보호 관리체계 인증(이하 "ISMS-P")을 획득해야 하며, 이는 기업의 개인정보 보호 및 정보보안에 대한 대외 신뢰도를 향상시키고 내부·외부의 개인정보 침해 위험을 최소화하기 위한 목적으로 작용하며, 현재 민간 기업의 보안 수준을 평가하는 주요 지표로 사용되고 있다[13].

제로트러스트를 도입하려는 기업들이 ISMS-P를 준수해야 하는 상황을 고려하여, 본 연구는 기존 보안 컴플라이언스인 ISMS-P를 제로트러스트 원칙 및 성숙도 평가 모델을 반영하여 고도화할 가능성을 검토하였다. 이를 위해 NIST, KISA, CISA, DoD, NSA의 제로트러스트 가이드라인을 분석·통합하여 제로트러스트 원칙과 성숙도 평가 항목을 도출하였으며, 이 항목을 ISMS-P 항목과 비교하여 (1) 제로트러스트 원칙이 반영된 경우, (2) 제로트러스트 성숙도 모델의 핵심 요소와 동일한 통제 항목이 있으나 기능상 개선이 필요한 경우, (3) 제로트러스트 원칙을 반영하여 개선할 필요가 있는 경우로 구분하여 ISMS-P 통제 항목을 기준으로 제로트러스트 평가 항목을 맵핑하고 적용 가능성을 분석하였다.

제로트러스트 항목은 총 255개로, Identity, Device, Network, Application, Data, Governance의 6개 분야로 나누어 구성하였다. ISMS-P 통제 항목은 총 101개이며, 세부 항목은 총 328개로 구성된다. ISMS-P는 (1) 관리체계 수립 및 운영, (2) 보호대책 요구사항, (3) 개인정보 처리 단계별 요구사항으로 구성되며, 이 중 (3) 개인정보 처리 단계별 요구사항은 개인정보 수집·이용 동의, 파기 절차, 가명 처리 등으로, 보안성 강화를 목표로 하는 제로트러스트의 6개 분야와 큰 관련이 없어 적용이 어렵다고 판단하였다.

적용 가능성을 분석한 결과, 255개의 세부 항목 중 192개 항목에서 개선 가능성이 확인되었다. 주요 개선 가능 항목으로는 △접근 통제, △인증 및 권한 관리, △시스템 및 서비스 운영·보안 관리, △사고 예방 및 대응, △정보시스템 도입 및 개발 보안, △위험 관리 등이 도출되었으며, 각 항목의 적용 가능성 분석 결과는 Table 5에 제시하였다. ISMS-P의 모든 세부 항목에 대한 적용 가능성은 58.5%로 나타났으며, (3) 개인정보 처리 단계별 요구사항을 제외할 경우 적용 가능성은 87.7%로 도출되었다.

### 4.3 국내 정보보호제도 전반의 개선

현재 국내 제로트러스트 도입 논의는 주로 금융권을 중심으로 진행되고 있다. 클라우드 도입 시 발생하는 계정 관리의 복잡성 및 탈경계화로 인해 제로트러스트 도입의 필요성이 대두되고 있으며, 특히 망분리와 관련한 법제도적 검토가 지속되고 있다. 국내에서는 2003년 KT DDoS 사건 이후 망분리를 중심으로 한 보안 정책이 본격화되었으며, 2006년에는 공공기관 망분리 의무화가 시행되었다. 이어 2013년 방송사 및 금융권 전산망 마비 사태 이후, 2014년 『금융전산 보안강화 종합대책』에 따라 금융권을 중심으로 망분리 환경 구축이 확대되었고 2015년 「전자금융감독규정」 및 「전자금융감독규정 시행세칙」을 개정하며 망분리 규제를 합리화하였다[14].

그러나 2022년 12월 금융위원회는 생성형 AI 도입 활성화 및 클라우드 환경 구축 확대를 목표로 「전자금융감독규정 시행세칙」을 개정하여 망분리 규제를 완화하는 초석을 쌓기 시작하였다. 한편, 망

분리 유지 필요성을 강조하는 견해도 존재한다. 지난 3월 미국 국가안보국(NSA, National Security Agency)은[16] 개정된 「사이버보안 정보 시트(Cybersecurity Information Sheet)」에서 망 분리에 기반한 ZT를 NSA의 기본 보안 전략으로 명시하며, 외부 침해를 완벽히 방어하기 어렵다는 점을 근거로 두 전략의 병행이 피해를 최소화할 방안이라고 주장했다. 국내에서도 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 「개인정보 보호법」 등에 따른 주요정보통신기반시설 취약점 분석·평가 및 ISMS-P는 여전히 망분리를 의무화하고 있다[14], [15]. 따라서 법제도 간 일관성을 확보하고, 망 통합 환경에서 보안을 강화하는 핵심 전략으로서 ZTA 도입을 활성화하는 방안을 모색할 필요가 있다.

## V. 결 론

본 연구는 국내 제로트러스트 정책의 도입을 활성화하기 위해 현행 정책을 분석하고, 이를 통해 발견된 한계점과 그에 따른 개선 방안을 제안한다. K-제로트러스트 가이드라인 및 실증 지원 사업은 국내 보안 체계에 제로트러스트 모델을 도입하는 중요한 첫 걸음이었으나 여러 한계점이 드러났으며, 본 연구에서는 향후 제로트러스트 정책의 실효성 강화를 위한 개선안을 제시하였다.

현재 제시된 가이드라인은 전반적인 지침에 불과하며, 세부적인 기술적 요소나 핵심 기능이 명확하게 반영되지 않았다. 이러한 불완전함은 정부의 실증 지원 사업뿐만 아니라 기업들이 실제로 제로트러스트 모델을 구현하는 과정에서 혼란을 초래할 수 있다. 이를 해결하기 위해서는 세부적인 아키텍처 모범사례를 포함한 실질적인 가이드라인이 제공되어야 할 것이다. 또한, 제로트러스트 구현 평가 체계의 정확성을 확보하는 것이 중요하다. 제로트러스트 구현의 성공 여부는 모의침투가 아닌 성숙도 평가를 기반으로 판단되어야 한다. 현재 국내 성숙도 모델은 주요 국가에서 제시하는 모델에 비해 구체성이 부족하므로, 이를 국제적 기준에 부합하도록 정교화하여야 한다. 더불어, ISMS-P 또는 전자금융감독규정 등 국내 민간 기업들이 준수하여야 할 보안 컴플라이언스와의 조화도 필요하다. 이를 통해 국내 보안 수준을 향상시키고 글로벌 제로트러스트 패권 경쟁에서 우위를 확보할 수 있을 것으로 기대된다.

## References


[1] Kaspersky Gert, Kaspersky Security Services, “Incident response analyst report 2023”, SEUCRELIST, May. 2024

[2] Eduardo B. Fernandez and Andrei Brazhuk, “A critical Analysis of Zero Trust Architecture (ZTA)”, Computer Standards & Interfaces, 89, 2024

[3] He, Y., Huang, D., Chen, L., Ni., Y., Ma and X., “A survey on zero trust architecture: Challenges and future trends”, Wireless Communications and Mobile Computing, 2022(1), 2022

[4] Itodo, Cornelius and Murat Ozer, “Multivocal Literature Review on Zero-Trust Security Implementation”, Computers & Security, 2024

[5] National Institute of Standards and Technology, “Zero Trust Architecture”, NIST Special Publication 800-207, Aug. 2020

[6] Cybersecurity and Infrastructure Security Agency, “Zero Trust Maturity Model”, version 2.0, 2023

[7] Lee et al., “Analyzing empirical case studies for widespread domestic Zero Trust adoption”, THE JOURNAL OF KOREAN INSTITUTE OF COMMUNICATIONS AND INFORMATION SCIENCES, 41(7), pp.33-40, 2024

[8] Lee, C., Choi, C., Jeong, S. and Kwak, “An attacker′s perspective for assessing Zero Trust maturity, planning adoption, and measuring impact”, Review of KIISC, 34(4), pp.45-51, 2024

[9] Ministry of Science and ICT, Korea Internet & Security Agency and KOZETA, “Zero Trust Guideline 1.0”, 2023

[10] Alhamed, Mariam and MM Hafizur

Rahman, “A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions”, Applied Sciences, 12(12), 6989, 2023

〔11〕 M., and Lee.,, “Zero Trust Global Policy Trends”, THE JOURNAL OF KOREAN INSTITUTE OF COMMUNICATIONS AND INFORMATION SCIENCES, 41(7), pp.19-26, 2024

〔12〕 Choi., “Zero Trust adoption considerations and maturity model”, THE JOURNAL OF KOREAN INSTITUTE OF COMMUNICATIONS AND INFORMATION SCIENCES, 41(7), pp.27-32, 2024

〔13〕 Park., Yu. and Chai, “A Linkage Analysis of ISMS-P and GDPR: Focused on Personal Information Protection.”, Journal of Information Technology Service, 18(2), pp.55-73, 2019

〔14〕 Lee. and Kwon., “Research on how to strengthen the new security system through the Zero Trust Clause, focusing on legal improvements in the Electronic Financial Transactions Act.”, KOCOSA, 23(1), pp.9-17, 2023

〔15〕 Korea Internet & Security Agency, “ISMS-P Certification Criteria Guide”, 2024

〔16〕 National Security Agency, “Cybersecurity Information Sheet”, 2024

〔17〕 DoD, “Zero Trust Strategy”, 2022

〔18〕 Governemtn Chief Information Officers’ Japan, “A Mindset for Adopting Zero Trust in Government Information Systems”, 2020

〔19〕 National Cyber Security Centre, “Cyber Essentials: Requirements for IT infrastructure v3.1”, 2023

〔20〕 NIST SPECIAL PUBLICATION 1800-35B, “Implementing a Zero Trust Architecture, Voume B: Approach, Architecture, and Security Characteristics”, 2023

〔21〕 NIST SPECIAL PUBLICATION 1800-35C, “Implementing a Zero Trust Architecture, Volume C: How-To Guides”, 2023

〔22〕 NIST SPECIAL PUBLICATION 1800-35D, “Implementing a Zero Trust Architecture, Volume D: Functional Demonstractions”, 2023

## 〈저자소개〉

김 자 현 (Ja-Hyun Kim) 학생회원
2022년 2월: 서울여자대학교 정보보호학과 졸업
2023년 3월~현재: 고려대학교 융합보안학과 석사과정
〈관심분야〉 정보보호법·정책, 사이버법·정책, 제로트러스트

김 법 연 (Beop-Yeon Kim) 종신회원
2008년 2월: 광운대학교 법학과 졸업, 법학사
2014년 2월: 광운대학교 법학과 졸업, 법학석사
2020년 2월: 고려대학교 정보보호대학원 졸업, 공학박사
2020년 6월~현재: 고려대학교 정보보호대학원, 연구교수
〈관심분야〉 정보보호법·정책, 사이버·법정책, 제로트러스트

권 헌 영 (Hun-yeong Kwon) 종신회원
2005년 2월: 연세대학교 대학원 졸업, 법학박사
2008년 3월~2015년 8월: 광운대학교 과학기술법학과 교수
2015년 9월~현재: 고려대학교 정보보호대학원 교수
2023년 2월~현재: 고려대학교 정보보호대학원 원장
〈관심분야〉 정보보호법·정책, 사이버법·정책, 제로트러스트