

원저

위험 적응형 점수기반 평가모델(RA-SBE)을 활용한 제로트러스트 도입 전·후 효과성 평가 방안

국경완¹, 이종대², 기영채³, 조광희⁴, 이경태⁵, 신삼범⁶

¹국방통합데이터센터 서기관(4급)

²국방방첩본부 해군상사

³국방방첩본부 주무관(7급)

⁴13특임여단 육군대위

⁵지상작전사령부 육군대위

⁶명지대학교 특임교수

교신저자: 신삼범 (ktma3419@hanmail.net)

요약

본 연구는 제로트러스트(Zero Trust) 보안체계 도입 전·후의 보안 효과성을 정량적으로 평가하기 위한 위험 적응형 점수기반 평가모델을 제안한다. 기존 제로트러스트 관련 연구는 체크리스트 방식으로 개념적 아키텍처나 성숙도 수준 제시에 집중되어 있어, 실제 도입 이후 보안 수준이 얼마나 개선되었는지를 객관적으로 측정하는 데 한계가 있었다. 이에 본 연구는 보안 통제 항목별 점수화와 위험요소 가중치를 결합한 평가모델을 설계하고, 위험 수준 변화에 따라 평가 결과가 동적으로 반영되도록 하였다. 이를 통해 단순 도입 여부 판단을 넘어, 제로트러스트 적용에 따른 보안 성과를 수치 기반으로 비교·분석할 수 있는 체계를 제시한다. 제안 모델은 공공·국방 분야와 같이 보안 요구 수준이 높은 환경에서 정책 결정, 성과관리, 보안 투자 효과 분석에 활용 가능하며, 제로트러스트 효과성 평가의 실증적 기반을 제공한다.

핵심어

제로트러스트, 제로트러스트 아키텍처, 위험 적응형, 점수기반 평가모델, 보안 효과성, 보안 성숙도

차례

1. 서론
2. 이론적 배경
3. 위험 적응형 점수기반 평가모델 구현
4. 결론

Open Access

접수일: 2026년 2월 19일
수정일: 2026년 7월 27일
게재승인일: 2026년 8월 07일
출판일: 2026년 9월 30일

Copyright © 2026 Author(s).

This is an Open Access article distributed under the terms of the Creative Commons CC BY 4.0 license (<https://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Original Article

A Before-and-After Effectiveness Assessment of Zero Trust Adoption Using a Risk-Adaptive Score-Based Evaluation Model

Kyoungwan Kug¹, Jongdae Lee², Youngchae Kee³, Kwanghee Cho⁴, Gyeongtae Lee⁵, Sambum Shin⁶

¹Senior Secretary (Grade 4), Defense Integrated Data Center, Republic of Korea

²Defense Counterintelligence Agency, CPO ROK Navy, Republic of Korea

³Defense Counterintelligence Agency, Officer (Grade 7), Republic of Korea

⁴Special Forces, CPT ROK Army, Republic of Korea

⁵Ground Operations Command, CPT ROK Army, Republic of Korea

⁶Professor, Myongji University, Republic of Korea

Corresponding Author: Sambum Shin (ktma3419@hanmail.net)

ABSTRACT

This study proposes a risk-adaptive, score-based evaluation model to quantitatively measure security effectiveness before and after the implementation of a Zero Trust security framework. Prior Zero Trust studies have mainly relied on checklist-based approaches that focus on conceptual architectures or maturity levels, making it difficult to objectively assess actual security improvements after deployment. To overcome this limitation, the proposed model combines scoring of individual security controls with risk-weighted factors, and dynamically adjusts evaluation results in response to changes in threat levels. This enables numerical comparison and analysis of security performance attributable to Zero Trust adoption, rather than a simple binary assessment of implementation. The model is particularly suitable for high-security environments, such as the public and defense sectors, where it can support policy decision-making, performance management, and security investment effectiveness analysis. By providing a structured and quantitative evaluation framework, this study offers an empirical basis for assessing the effectiveness of Zero Trust security implementations.

KEYWORDS

Zero Trust, Zero Trust Architecture, Risk-Adaptive, Score-Based Evaluation Model, Security Effectiveness, Security Maturity

1. 서론

1.1. 제로트러스트 필요성 및 기존 경계보안의 한계

제로트러스트(Zero Trust)는 “절대로 신뢰하지 않고 항상 검증해야 한다(Never Trust, Always Verify)”라는 원리에 기초한 보안 아키텍처이다. 기존 보안모델은 네트워크 내부를 신뢰할 수 있는 영역으로 전제하고, 외부와 내부를 경계장비(Firewall, IDS/IPS 등)로 구분하여 외부 공격을 차단하는 방식이었다. 그러나 클라우드 확산, 재택근무, 모바일 기기 보급, IoT 환경의 등장으로 인해 내부와 외부의 경계가 점차 사라지고 있으며, 이러한 접근은 더 이상 효과적이지 않다.

미국 국립표준기술연구소(NIST)는 SP 800-207¹⁾에서 제로트러스트를 “신뢰할 수 없는 네트워크 환경을 전제로 모든 요청 단위에 대해 사용자·기기·애플리케이션을 검증하고 정책을 적용하는 체계”로 정의하고 있다. 오늘날 위협 환경은 고도화·지능화되어 있으며, 특히 내부망 침투 후의 횡적 이동(Lateral Movement)²⁾, 자격 증명 탈취, 내부자 위협 등은 기존 경계보안 체계만으로는 탐지·차단하기 어렵다. 또한 암호화된 트래픽이 급격히 증가함에 따라 기존 장비 기반의 경계 모니터링이 한계에 직면하고 있다. 기존 경계보안 모델은 “신뢰할 수 있는 내부망과 위협적인 외부망을 분리한다”는 전제 위에서 구축되어 왔다. 그러나 이러한 경계중심 접근법은 현대의 분산형 IT 환경과 하이브리드 업무 형태에서는 구조적 한계를 보인다.[1,2]

첫째, 경계 붕괴(Borderless Network) 문제이다. 클라우드 서비스, SaaS, 원격근무, BYOD(Bring Your Own Device), IoT의 확산으로 인해 네트워크의 경계가 과거와 달리 물리적으로 구분되지 않으며, 전통적 경계장비로는 사용자와 기기를 식별·통제하기 어렵다. 둘째, 내부 위협(Insider Threat)에 대한 취약성이다. 기존 모델은 “내부는 신뢰할 수 있다”는 가정에 의존하므로, 일단 인증을 통과하면 추가 검증이 이루어지지 않는다. 이로 인해 내부자 권한 오남용이나 계정 탈취 후 침입한 공격자가 네트워크 전반으로 자유롭게 확산될 수 있다. 셋째, 암호화 트래픽 증가에 따른 가시성 저하(Visibility Reduction)이다. 최근 네트워크 트래픽의 대부분이 암호화되면서, 경계장비가 복호화를 수행하지 않는 이상 내부 위협 탐지가 어렵다. 복호화는 성능 저하와 개인정보 침해 우려를 동반해 현실적으로 제약이 많다. 넷째, 운영 복잡성과 유지관리 비용의 증가(Operational Overhead)이다. 다계층 구조와 다양한 솔루션 간의 정책 불일치, 설정 오류는 보안 공백(Security Gap)을 유발하여 방어 수준을 저하시킨다. 다섯째, 정적 정책 기반(Static Policy-based) 보안의 한계이다. 기존 경계보안은 사전에 정의된 규칙에 따라 트래픽을 허용·차단하므로, 변화무쌍한 지능형 위협(Advanced Persistent Threat, Zero-day Attack)에는 효과적으로 대응하지 못한다.

결과적으로, 기존 경계보안은 “내부=신뢰, 외부=불신”이라는 이분법적 신뢰 모델에 의존하고 있으며, 복잡화된 네트워크 구조와 지능화된 위협 환경에서는 더 이상 유효하지 않다. 이러한 한계를 극복하기 위해서는 네트워크 경계가 아닌 사용자·기기·애플리케이션 단위로 세분화된 검증과 통제를 수행하는 제로트러스트 접근법이 필요하다. 즉, 제로트러스트는 “최소 권한 원칙(Least Privilege)”과 “지속적 인증·검증(Continuous Authentication)”을 기반으로, 경계중심 방어외의 구조적 취약점을 보완하고 신뢰 기반의 동적 보안 체계를 구현하는 핵심 전략이라고 볼 수 있다.

주요 국가와 기업에서는 제로트러스트를 사이버보안의 핵심 프레임워크로 지정하였으며, 기업 뿐 아니라 정부 차원에서도 전략적 도입이 확산되고 있다. 미국은 2021년 바이든 행정명령(EO

1) 제로트러스트 아키텍처 표준으로, 네트워크를 신뢰하지 않고 모든 접근 요청마다 사용자·기기·애플리케이션을 지속적으로 검증·통제하는 보안 원칙과 구성요소를 제시하고 있다.
2) 횡적 이동(Lateral Movement)은 공격자가 초기 침투 후 내부망에서 다른 시스템으로 이동하며 권한을 확장·정보를 수집하는 공격 기법으로, 자격 증명 탈취와 내부자 위협을 증폭시킨다.

14028)을 통해 연방정부 전 기관의 제로트러스트 전환을 공식화하였고, CISA는 “Zero Trust Maturity Model 2.0(2023)”을 발표하여 인증, 권한관리, 네트워크 세분화, 데이터 보호, 가시성 및 탐지, 대응 및 회복 등 6개 보안 영역을 중심으로 구체적 성숙도 지침을 제시하였다.[3]

한국 정부 또한 제로트러스트 개념을 국가 보안정책에 반영하고 있다. 과학기술정보통신부와 국가보안기술연구소는 공공·국방 부문의 클라우드 보안 전환 전략에 제로트러스트 원칙을 도입하였으며, 국방부의 “국방 사이버안보 혁신 추진계획”에서도 이를 핵심 과제로 명시하였다. 또한 행정안전부는 “디지털정부 보안 전략”을 통해 공공 클라우드 전환 시 제로트러스트 아키텍처 도입을 권장하고 있다.[4]

이와 같이 제로트러스트는 지능화되는 사이버 위협 환경 속에서 가장 핵심적인 보안 전략으로 자리매김하고 있다. 이는 경계 기반 모델을 넘어 데이터·사용자·애플리케이션 중심의 보안을 가능하게 하며, 특히 국방과 공공부문에서 국가안보를 지키는 필수 프레임워크로 작용한다고 볼 수 있다. 더불어 자동화와 통합을 통해 보안 운영의 효율성과 지속가능성을 제고하고, 변화하는 환경에 신속히 대응할 수 있다. 나아가 제로트러스트는 디지털 전환을 안전하게 추진하기 위한 신뢰 기반(Trust Foundation)을 제공함으로써, 정부와 기업의 혁신을 뒷받침하는 핵심 토대가 되고 있다.

1.2. 연구 목적 및 문제 제기

최근 발표된 “제로트러스트 가이드라인 2.0”³⁾[5]은 국가 차원의 보안 패러다임을 기존의 경계 중심 보안에서 “항상 검증(Always Verify)”을 전제로 하는 제로트러스트 기반 보안으로 공식 전환하였다는 점에서 중요한 의미를 가진다. 이는 미국 CISA의 Zero Trust Maturity Model과 NIST SP 800-207을 참조하면서도 국내 현실에 맞춘 성숙도 평가 체계와 체크리스트 기반 접근을 제시함으로써, 국제 기준과의 정합성을 확보하고 국내 적용성을 동시에 강화하였다. 특히 공공·국방 분야에서 제로트러스트 도입을 정책적으로 촉진함으로써, 국가 기반시설 및 행정망의 보안 수준 향상을 전인할 수 있는 제도적 근거를 마련했다는 점은 주목할 만하다.

최근 공공·국방·민간 분야에서 제로트러스트 보안 모델의 필요성은 폭넓게 인정되고 있다. 클라우드, 원격근무, IoT, SaaS 등으로 인해 기존 경계중심 보안의 한계가 명확히 드러났기 때문이다. 그러나 실제 기관 차원에서 제로트러스트를 도입하는 과정은 여전히 주저되는 양상^{6,7)}을 보이고 있다. 선행 조사 및 국내외 기관 대상 설문조사 결과에 따르면, 도입을 주저하는 주요 이유는 △ 기존 인프라와의 호환성 문제, △ 높은 초기 구축 비용, △ 인력과 전문성 부족, △ 도입 후 성과 측정의 불확실성, △ 조직 내 저항감(업무 변화 부담) 등이 지적되고 있다. 일부 기관 인터뷰에서도 “보안이 강화되는 것은 알지만, 도입 효과를 객관적으로 증명할 수 있는 도구가 부족하다”는 응답이 반복적으로 확인되었다.[8]

표 1. 제로트러스트 도입관련 설문결과

주요 설문 결과(출처)	지적된 주저 요인
- 응답 기관 중 47%가 제로트러스트 구현에 자신감이 부족하다고 응답 * Bitdefender / Cybersecurity Insiders 조사	기술 복잡성, 내부 역량 부족, 통합 난제 등
- 응답자의 다수가 제로트러스트 도입을 방해하는 요소로 비용 문제, 기술 격차, 인력 부족, 데이터 보호 규제등을 꼽음 * Okta, “2023년 Zero Trust 보안 현황” 보고서	예산 제약, 기존 시스템 호환성, 전문인력 부재, 규제 준수 부담 등

3) 클라우드·원격근무 확산과 지능형 사이버위협 증가로 기존 경계보안의 한계가 드러남에 따라, 국내 환경에 맞는 제로트러스트 확산·정착과 단계적 도입 기준을 마련하기 위해 제정되었다.

전 세계 기업의 63%가 제로트러스트 전략을 완전 또는 부분 도입했지만, 전략 범위가 조직 전체의 절반 이하인 경우가 많음 * Gartner /CIO 보도	도입 범위 설정 난이도, 리스크 완화 효과 제한, 예산·인력 부담 예상 등
2,200여 명 대상 설문에서 46%는 제로트러스트 모델 전환 중, 43%는 이미 제로트러스트 원칙을 도입했으며 주요 미도입 이유로는 레거시 시스템 이전 업그레이드 시간과 리소스 소모를 지적함 * ExpertInsights 조사	레거시 시스템과의 마이그레이션 부담, 리소스 소모, 구현 복잡성 등
조직들이 직면하는 주요 장애요인으로 솔루션 복잡성, 자원 부족, 상호운용성 문제, 조직 내부 사고방식 전환의 어려움 등이 지목됨 * CDOTRENDS 분석	복잡한 기술 통합, 리소스(예: 인력, 예산) 부족, 기존 시스템과의 상충, 조직 변화 저항 등

* 출처: 인터넷 검색 후 저자 재정리

이러한 맥락에서 본 연구는 정부가 발표한 “제로트러스트 가이드라인 2.0”을 토대로, 체크리스트 기반의 성숙도 수준 분석과 효과성 측정을 활용하여 “제로트러스트 도입 전·후 보안향상 효과를 계량적으로 검증할 수 있는 방안”을 제시하는 것을 목적으로 한다. 즉, 제로트러스트를 단순히 권고적 보안 개념이 아닌, 성과를 정량적으로 평가할 수 있는 실질적 보안 관리 도구로 활용하는 방안을 모색하는 데 초점을 둔다.

많은 기관이 제로트러스트의 필요성에는 공감하지만 실제 도입을 망설이는 이유는 크게 네 가지로 정리된다. 첫째, 기존 네트워크 아키텍처와의 충돌 및 레거시 시스템 대응 문제이다. 둘째, 초기 도입·운영 비용과 전문 인력 확보 부담이다. 셋째, 구체적인 보안 향상 효과를 수치로 입증하기 어렵다는 점이다. 넷째, 내부 사용자 경험 저하, 업무 절차 변경에 따른 조직적 저항이 발생한다는 점이다. 따라서 “도입 후 보안 수준이 어느 정도 개선되는가?”라는 질문에 대한 명확한 검증 프레임워크가 부재한 상황이다.

“제로트러스트 가이드라인 2.0”은 도입 수준 분석을 크게 두 가지 방법으로 제시하고 있다. 성숙도 기반 도입 수준 분석은 표 2와 같이 인증, 권한관리, 세분화, 데이터 보호, 가시성·탐지, 대응·회복 등 6대 영역에 대해 체크리스트를 기반으로 현 수준을 진단하고 목표 수준과의 격차를 분석한다. 침투시험 기반 효과성 분석은 실제 보안 침투 시나리오를 적용하여 도입 전후의 방어·탐지·대응 성과를 비교함으로써 보안 효과성을 검증한다. 이 두 접근은 상호 보완적 성격을 가지며, 성숙도 분석이 정책·운영 수준의 점진에 강점을 가진다면, 침투시험은 실제 기술적 효과성 검증에 강점을 가진다.[9]

표 2. 성숙도 수준 평가 체크리스트 방식

평가 영역	주요 점검 항목(예시) ※예시: ①주요점검 항목 ② 성숙도 단계 ③ 측정지표
인증 (Authentication)	① 사용자 기기 기반 다중인증(MFA), 위험 기반 인증, 신뢰기기 등록 여부 ② 초기: 단일인증, 발전: MFA 부분 도입, 고도화: 위험기반+기기인증 ③ MFA 적용률(%), 위험기반 인증비중(%)
권한관리 (Authorization)	① 최소권한 원칙, 세션기반 접근제어, JIT(Just-In-Time) 권한 부여 ② 초기: 정적 계정권한, 발전: 업무별 권한구분, 고도화: 동적·세션권한 ③ 초과권한 제거율(%), JIT 적용률(%)
세분화 (Segmentation)	① 네트워크·자원 단위 마이크로세그멘테이션, 정책자동화 ② 초기: 단순망분리, 발전: VLAN·VPN 세분화, 고도화: 자원·사용자 단위 분리 ③ 세그먼트 간 불필요 트래픽 차단율(%)

데이터 보호 (Data Protection)	① 암호화, 무결성검증, 접근로그 기록·보관 ② 초기 : 부분 암호화, 발전 : 저장데이터 암호화, 고도화 : 전송·저장 전 구간 암호화 ③ 암호화율(%), 접근로그 보존율(%)
가시성·탐지 (Visibility & Detection)	① 통합로그수집, 이상행위 탐지, SIEM·XDR 연계 ② 초기 : 부분 로그수집, 발전 : 중앙집중식 로그분석, 고도화 : AI기반 이상탐지 ③ 로그 커버리지(%), 평균탐지시간(MTTD)
대응·회복 (Response & Recovery)	① 침해대응 프로세스, 자동화 대응(Orchestration), 복구계획(BIA·BCP) ② 초기 : 수동대응, 발전 : 대응절차 표준화, 고도화 : 자동화·복구훈련 정례화 ③ 평균대응시간(MTTR), 자동화 비율(%)

이 중, 성숙도 기반 도입 수준 분석은 간편성과 체계성이라는 장점을 가지지만, 주관성·정량성 부족·현실 반영 미흡이라는 구조적 한계도 내포하고 있다. 따라서 이를 극복하기 위해서는 정량지표 연계, 증빙자료 기반 검증, 침투시험 병행, 위협 인텔리전스 반영, 기관별 맞춤형 모델 개발이 필요하다. 이러한 발전 방향은 “제로트러스트 가이드라인 2.0”이 단순한 진단 도구를 넘어 보안 성과를 객관적으로 측정할 수 있는 정책적 평가 도구로 자리 잡게 하는 핵심 조건이라고 볼 수 있다.[10]

따라서 본 연구는 제로트러스트 도입의 필요성과 함께 기관들이 도입을 주저하는 현실적 요인을 문제로 제기하고, “가이드라인 2.0”이 제시하는 성숙도 분석 방법론을 검토한다. 이를 바탕으로 체크리스트 기반 접근을 위험 적응형⁴⁾ 점수기반 평가모델(RA-SBE, Risk-Adaptive Score-Based Evaluation Model)을 설계하여 실질적 성과평가 도구로 확장하여, 도입 전·후 보안 향상 효과를 측정·검증할 수 있는 구체적 프레임워크를 제안하는 데 연구의 목적을 둔다.

이 연구는 기관이 제로트러스트 도입 효과를 체계적으로 계량화·검증할 수 있는 평가 도구라는 점에서 의의가 크다. 즉, 기관은 “가이드라인 2.0”을 활용하여 도입 전·후의 보안수준을 수치로 비교·분석함으로써, 정책결정자와 이해관계자에게 도입의 정당성을 입증할 수 있다. 이는 제로트러스트 도입을 주저하는 조직에게 “보안투자 효과를 가시적으로 보여줄 수 있는 근거”를 제공한다는 점에서 중요하다고 할 수 있다.

2. 이론적 배경

2.1. 제로트러스트 개념 및 가이드라인 2.0

제로트러스트(Zero Trust)는 앞에서 설명했듯이 “기본적으로 아무것도 신뢰하지 않고, 모든 접근은 검증한다(Never Trust, Always Verify)”는 원리를 핵심으로 하는 보안 패러다임이다. 기존 경계중심 보안(perimeter-based security)⁵⁾은 내부망을 신뢰 대상으로 간주하고 외부와의 경계에서 방어를 수행했으나, 클라우드 확산·원격근무·모바일·IoT 환경이 확대되면서 내부와 외부의 경계가 무의미해졌다. 이에 따라 제로트러스트는 네트워크 위치와 무관하게 사용자·기기·애플리케이션·데이터 접근 요청을 모두 검증하며, 최소 권한 원칙과 지속적 모니터링을 통해 보안을 보장한다. 제로트러스트 보안모델은 표 3과 같이 크게 세 가지 핵심 원칙에 기반한다. 이러한 원칙은 단일 기술 솔루션이 아니라, 거버넌스·정책·기술이 결합된 종합적 아키텍처로서 제로트러스트를 이

4) 위험 적응형이란 위험 수준, 자산 중요도, 사용자·기기 상태 등 실시간 위험 요소 변화를 반영해 평가 지표의 가중치와 점수를 동적으로 조정하는 개념으로, 고정 기준 평가의 한계를 보완하고 실제 보안 위험을 정량적으로 반영하는 것을 의미한다.

5) 네트워크 내부를 신뢰 구역으로 간주하고 방화벽·IDS/IPS 등 경계 장비로 외부 위협을 차단하는 방식이다. 내부 침투 이후 공격, 원격근무·클라우드 환경에서는 효과가 제한되는 한계를 가진다.

해할 필요가 있음을 시사한다.

표 3. 제로트러스트 보안 모델 원칙

원칙	내용
항상 검증 (Continuous Verification)	모든 요청을 다차원적 맥락(사용자, 기기, 위치, 시간, 행위)에 따라 검증.
최소 권한 부여 (Least Privilege Access)	업무 수행에 필요한 권한만을 부여하고, 동적으로 조정.
침해 가정(Assume Breach)	내부망 또한 이미 침투되었다는 가정 하에 보안정책을 설계.

제로트러스트 아키텍처(ZTA)는 정책기반 접근통제(Policy-Based Access Control) 구조로, 그림 1과 같은 구성요소로 이루어진다. 정책 결정 지점(Policy Decision Point, PDP)으로 접근 요청 주체의 신뢰도를 평가하고, 자원 접근의 허용/거부를 결정하는 핵심 엔진이다. 정책 시행 지점(Policy Enforcement Point, PEP)은 PDP의 결정을 실제로 실행하는 지점으로 네트워크 게이트웨이, 에이전트, 프록시 등이 해당한다. 정책 엔진(Policy Engine, PE)은 접근 주체의 속성, 리소스 속성, 환경 변수, 기업 정책, 위협정보 등을 기반으로 최종 접근 여부를 판단한다.

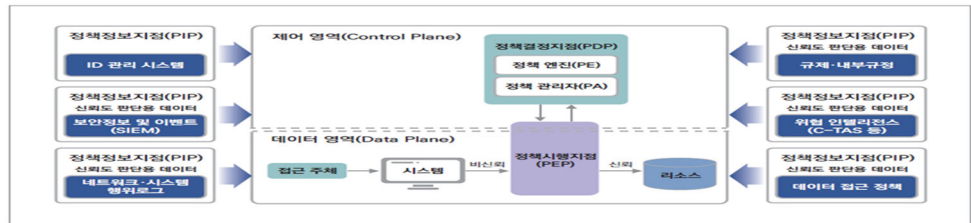


그림 1. 제로트러스트 아키텍처 보안 모델 및 논리 구성요소

이외에도 가이드라인 2.0은 각 영역별 성숙도를 “초기(Traditional) - 발전(Advanced) - 고도화(Optimal)”의 3단계로 구분하고, 체크리스트를 통해 현 수준을 점검하도록 설계되었다. 이는 기관이 제로트러스트 도입 수준을 정량적으로 파악하고, 단계별 로드맵을 수립할 수 있도록 지원한다는 점에서 의미가 크다.

가이드라인 2.0은 추상적 원칙에서 구체적 실행 모델로 전환, 정성적 권고에서 정량적 성과 측정으로 진화, 실증적 효과 검증 체계 도입, 국제 정합성 및 국내 적용성 확보 등의 특징을 가진다고 할 수 있다. 특히, 1.0은 제로트러스트 개념을 알리고 인식을 확산시키는 데 목적이 있었던 반면, 2.0은 영역별 체크리스트와 정량 지표를 제시해 실행력을 높였으며, 침투시험 기반 효과성 분석을 포함시켜, 보안 성과를 실제 위협 환경에서 검증할 수 있도록 했을 뿐만 아니라, 미국 CISA/NIST 모델과 호환성을 확보하면서도 국내 기관의 현실에 맞춘 항목을 반영했다. 즉, 가이드라인 2.0은 “개념적 선언”에서 “정책·성과 평가 도구”로의 전환이라는 의미를 가진다.

이러한 가이드라인 2.0 발표이후 국방부는 2023년 “국방 사이버안보 혁신 추진계획6)”에서 제로트러스트를 핵심 과제로 반영하였다. 이후 국방 전산망, 지휘통제체계, 클라우드 기반 국방통합 데이터센터에 ZTNA(Zero Trust Network Access) 시범 적용을 검토하고 있으며, 2027년까지 단계적 확대를 목표로 하고 있다. 또한 군 CSIRT7)/관제센터에 가이드라인 2.0 체크리스트를 적

6) 지능화되는 사이버위협에 대응하기 위해 제로트러스트 전환, AI 기반 보안체계 도입, 사이버 대응역량과 인력 전문성 강화를 추진하는 중장기 혁신 전략이다.

용해 정기 성숙도 진단 및 성과평가 체계를 도입하는 방안을 추진 중이며, 산업계에서도 이를 준거 프레임워크로 활용하는 사례가 증가하고 있다. 특히 보안 인증·평가 과정에서 “가이드라인 2.0 준수 여부”가 주요 평가 항목으로 자리 잡고 있으며, 이는 민간 기업들에게도 도입 명분과 기준을 제공하고 있다는 점이 주목해야 할 부분이다.[11-13]

2.2. 제로트러스트 가이드라인 2.0 한계 및 극복방안

최근 사이버 위협은 공급망 공격, 랜섬웨어 서비스화(RaaS), 자격증명 탈취 등 고도화된 양상으로 전개되고 있다. 기존의 경계중심 보안(perimeter-based security)은 내부를 신뢰하고 외부만 방어하는 전제에 기초했으나, 클라우드·모바일·원격근무 환경이 확산되면서 그 효과가 점차 한계를 드러내고 있다. 가이드라인 2.0은 제로트러스트 도입을 단순한 “여부(Yes/No)”의 문제가 아니라 단계적 성숙 과정으로 이해한다. 즉, 기관이 현재 어느 수준에 위치하는지를 파악하고, 목표 수준과의 간극을 진단하며, 개선 로드맵을 설계하도록 하는 체계이다. 이를 통해 기관은 현 상태를 객관화하고 도입 효과를 정량적으로 입증할 수 있다. 성숙도 분석의 평가 범위는 6대 핵심 영역으로 구분되며, 각 영역은 다시 초기(Traditional) - 발전(Advanced) - 고도화(Optimal)의 3단계 성숙도로 구분된다. 예컨대 인증 영역에서 초기 단계는 단순 비밀번호 사용, 발전 단계는 MFA 일부 적용, 고도화 단계는 위험 기반 인증과 기기 검증을 결합한 체계를 의미한다.

표 4. 성숙도 기반 분석

평가 영역	주요 점검 항목(예시)
자가진단 (Self-Assessment)	•기관 담당자가 각 항목별로 현재 수준을 선택 (초기/발전/고도화). •문항은 총 40~50개 내외이며, 객관적 증빙(정책서, 로그, 감사결과 등)을 병행.
성숙도 산정 (Maturity Scoring)	•영역별 점수를 3단계(1~3점)로 수치화하여 평균값을 산출. •결과는 레이더차트(Radar Chart) 형태로 시각화하여, 영역별 강·약점을 파악.
격차 분석 (Gap Analysis)	•영역별 점수를 3단계(1~3점)로 수치화하여 평균값을 산출. •결과는 레이더차트(Radar Chart) 형태로 시각화하여, 영역별 강·약점을 파악.
성과 검증 (Effectiveness Validation)	•가이드라인은 체크리스트 평가와 함께 침투시험(PenTest), 레드팀 연습 등 실효성 검증을 병행할 것을 권장함. •이를 통해 ‘준비도(Readiness)’ 평가와 ‘효과성(Effective)’ 평가를 통합 관리.

가이드라인 2.0의 성숙도 기반 분석은 표 4와 같이 자가진단, 성숙도 산정, 격차분석, 성과 검증 등의 방법을 사용한다. 이때 활용되는 대표 지표로는 MFA 적용률, 데이터 암호화율, 평균 탐지 시간(MTTD), 평균 대응 시간(MTTR), 침해사고 건수 등이 있다. 가이드라인 2.0은 단순히 체크리스트 평가에 그치지 않고, 침투시험(PenTest) 기반 효과성 검증을 병행할 것을 권장한다. 즉, 성숙도 분석이 “준비도”를 평가한다면 침투시험은 실제 공격 시나리오에 대한 “실효성”을 검증한다. 이를 결합함으로써 문항 충족 여부와 실제 방어능력 간 괴리를 최소화한다.

이와 같이 성숙도 기반 도입 수준 분석은 첫째, 기관이 제로트러스트 도입 효과를 정량적으로 입증할 수 있도록 해 보안투자 정당성을 강화한다. 둘째, 영역별 성숙도 수준을 시각화함으로써 경영진과 정책결정자가 직관적으로 보안 수준을 이해할 수 있다. 셋째, 단계별 로드맵을 제시하여 점진적·지속적 보안 고도화를 가능케 한다.

그러나 한계도 존재한다. 우선 체크리스트 평가가 응답자의 주관적 판단에 의존할 가능성이 크

7) CSIRT(Computer Security Incident Response Team)는 침해사고 발생 시 탐지·분석·대응·복구를 전담하는 조직으로, 사고 확산 방지와 재발 예방을 위해 기술 대응, 보고 체계, 훈련 및 협력 활동을 수행한다.

다. 또한 평가 결과가 정적(Static)이어서, 실시간 변화하는 위협 환경을 반영하기 어렵다. 마지막으로, 동일한 체크리스트를 모든 기관에 적용할 경우 산업별·조직별 특수성이 반영되지 않는 문제가 있다. 따라서, 제로트러스트 모델이 기존 경계보안 모델의 구조적 한계를 극복할 수 있다고 하더라도, 이를 성공적으로 도입·관리하기 위해서는 성숙도 기반 평가(Maturity-based Assessment)가 단순 진단을 넘어 정량적·지속적·위협 기반 측정 체계로 발전해야 한다.

3. 위험 적응형 점수기반 평가모델 구현

3.1. 성숙도 수준 평가 체크리스트 방식과 한계

“제로트러스트 가이드라인 2.0”은 기관·조직이 제로트러스트 보안을 체계적으로 도입할 수 있도록, 도입 수준을 정량적으로 진단할 수 있는 “성숙도 수준 평가 체크리스트 방식”을 제시하였다. 이는 “준비도(Readiness)”를 평가하는 자가진단 도구이자, 향후 정책수립·투자근거·성과평가의 기반이 되는 프레임워크라고 볼 수 있다.

성숙도 수준 평가 체크리스트 방식은 기존 주관적 판단에 의존하던 보안체계를 수치화하여 기관 간 비교·평가 가능하며, 낮은 성숙도 영역을 식별해 단계적 로드맵을 수립(예: 인증→권한관리→세분화 순 확산)이 가능하며, 체크리스트 결과를 KPI로 환산하여, 경영·정책 성과평가에 활용 가능(MFA율, MTTR 등)하며, CISA(2023), NIST SP 800-207, DoD ZT Strategy⁸⁾ 등과 호환되는 구조를 채택하여 국제표준 수준의 평가체제로 확장 가능하다는 장점이 있다.

그러나, 체크리스트 기반 평가는 조직이 제로트러스트 보안 원칙을 도입하거나 운영할 때, 각 항목(예: 인증, 권한관리, 모니터링, 로그 관리 등)에 대해 그림 2와 같이 “예/아니오” 혹은 등급을 매겨 평가하는 방식이다. 이 방식은 직관적이고 적용하기 쉽다는 장점이 있으나, 주관성 개입, 정성적 요소의 축소 등 표 5와 같은 다양한 한계가 존재할 수 있다.[3,14,15]

이런 한계들은 제로트러스트 평가뿐만 아니라 정보보호 거버넌스, 보안 성숙도 평가 등 다양한 평가 체계에서 지적되는 공통적인 문제이기도 하다. 예컨대, 정보보호 거버넌스 분야에서는 체크리스트 방식만으로는 KPI(핵심성과지표)⁹⁾, 리스크 기반 측정, 성숙도 모델 등을 반영하기 어렵다는 지적이 있다.

세부역량	확인방법	성숙도	Check
사용자 인벤토리	• 사용자 목록에 대한 문서화가 되어있는가?	기초	☐
	• 사용자 역할에 따른 상세 인벤토리가 구축되어 있는가?	초기	☐
	• 자동화된 인벤토리 관리 기구가 도입되어 있는가?	향상	☐
	• 비정상적인 사용자 활동에 대한 탐지가 가능한가?	향상	☐
	• AI 기반 사용자 행동에 따른 관리가 되는가?	최적화	☐
	• 인벤토리가 통합되어 사용자 및 권한 관리 최적화가 되어 있는가?	최적화	☐
ID 연계 및 사용자 자격 증명	• 사용자 자격 증명에 대한 ID 연계 솔루션이 적용되어 있는가?	기초	☐
	• 여러 시스템 간 사용자 자격 증명에 대한 연동이 되어 있는가?	초기	☐
	• ID 통합 관리 시스템이 구축되어 있는가?	향상	☐
	• 글로벌 수준의 ID 연계 솔루션이 적용되어 있는가?	최적화	☐

그림 2. 식별자-신원 핵심 요소 체크리스트 예시

- 8) 미 국방부가 제로트러스트 원칙을 전 영역에 적용해 사용자·기기·데이터를 지속 검증하고, 단계적 로드맵과 성숙도 기준으로 사이버 방어 역량을 강화하는 전략을 말한다.
- 9) 조직의 전략과 목표 달성 수준을 정량적으로 측정하는 지표로, 성과를 지속적으로 점검·관리하고 의사결정과 개선 활동의 기준으로 활용된다.

표 5. 체크리스트 방식의 한계

한계	주요내용
주관성 개입	• 항목별 평가 기준, 가중치 설정, 판단 기준 등이 평가자에게 의존할 가능성이 크며, 동일한 조직이라도 평가자에 따라 점수가 달라질 수 있음
정형화된 항목의 한계	• 체크리스트 항목이 정해져 있으면, 조직의 특정한 환경이나 특이한 위협 모델을 반영하지 못할 수 있다. 즉, “모든 조직에 동일하게 적용되는 항목”만 다룰 가능성이 많이 있음
정성적 요소의 축소	• 체크리스트는 보통 정성적 판단을 정량화하려는 시도로, 모호하거나 복합적인 보안 요소를 단순화해 버리는 위험이 있다. 예를 들어, “모니터링 수준이 충분인가?”라는 항목은 여러 요소가 복합되어 있는데, 단일 문항으로 환원할 시 세부 맥락이 무시될 수 있음
상호의존성 무시	• 제로트러스트 구성 요소들은 상호 연관성이 크다. 예컨대, 인증 체계가 부실하면 모니터링이나 권한 통제가 무의미해진다. 체크리스트 항목이 독립적으로 평가되면 이러한 상호의존성을 반영하기 어려움
동적 변화 반영 미흡	• 위협 환경, 내부 시스템 변화, 운영 조건 등이 시간에 따라 변한다. 체크리스트는 주기적으로 업데이트되지 않으면, 시점 간 비교성이나 적응성이 떨어짐.
가중치 및 중요도 기준 부재	• 각 항목의 중요도가 동일하다고 가정되거나 임의의 가중치가 부여되기 쉽다. 그러나 조직이나 시스템 특성에 따라, 어떤 항목이 더 중요할지에 따라 달라질 수 있음.
과도한 정답 강제 위험	• 체크리스트 문항이 너무 엄격하거나 이상적인 환경을 기준으로 할 경우, 실제 현실과 괴리가 커지며, 조직이 “체크리스트 통과”에만 집중하고 실질 보안 향상은 간과할 위험이 있음.

제로트러스트 보안 모델 자체의 문제점이나 한계점을 다룬 연구에서도, 지나치게 반복 인증을 요구하면 사용성 저하, 내부 사용자 피로, 인증 실패 등 운영 현실과의 충돌 위험 등이 언급되어 오려 부작용이 커질 수 있는 위험요소가 상존한다.

3.2. 위험 적응형 점수기반 평가모델을 활용한 제로트러스트 도입 효과성 평가

3.2.1. 위험 적응형 점수기반 평가모델 설계

앞에서 설명한 체크리스트 기반 한계점을 보완하기 위해 새로운 평가모델을 설계한다. 즉, 항목별 중요도에 따라 가중치를 부여하고, 조직의 위협 프로파일에 맞춘 항목 우선순위를 반영하고, 조직의 산업 특성, 내부 시스템 구성, 위협 모델 등을 반영하여 체크리스트 항목을 동적으로 조정 가능하게 설계한다. 설계 시 또한, 체크리스트 평가 외에 정량적 보안 지표(예: 인증 실패율, 접근 통제 위반 건수, 이상 트래픽 비율 등)를 함께 사용해 평가의 객관성을 높이고, 침투 테스트, 모의 공격, 레드 팀ing 등을 통해 실제 위협 대응 역량을 검증하는 요소를 보충하며, 체크리스트 항목이 “이상 없음 / 부분적 / 미흡” 식의 단순 등급이 아니라, 정량적 점수에 기반한 척도를 사용한다.[15]

조직의 산업 특성, 내부 시스템 구성, 위협 모델 등을 반영하여 체크리스트 항목을 동적으로 조정 가능하게 설계하며, 위와 같은 한계점을 보완하기 위해, 체크리스트 기반 평가 방식에 위험 적응형 제로트러스트 점수기반 평가모델(RA-SBE, Risk-Adaptive Score-Based Evaluation Model)을 제안한다. 이렇게 보완된 모델을 활용하여 성숙도 수준을 비교하여 제로트러스트 도입 전·후 효과성을 평가할 수 있다.

RA-SBE의 목표는 정해진 체크리스트 대신 조직별 위협 특성·자산 영향도·위협 모델을 반영하며, 항목별 중요도 차등 적용, 동적 업데이트(Threat Intelligence 기반)¹⁰⁾ 가능토록 하며, 평가자의 편차를 최소화(정성적 항목의 정량적 해석 제공) 하는 것이다. RA-SBE는 아래와 같이 항목별

10) 최신 위협 정보와 공격 동향을 실시간으로 반영해 보안 정책, 탐지 규칙, 평가 기준을 자동 조정하는 방식으로, 변화하는 사이버위협에 신속히 대응하도록 한다는 의미이다.

중요도 가중치 W_i , 실제 이행수준 L_i , 위험 노출도 R_i 로 구성되며, 필요에 따라 조직규모, 산업규제에 따라 조정이 가능한 보정계수 C 로 구성되며 평가식은 표 6과 같다.

$$RA-SBE = C \times \sum_{i=1}^N (W_i \times L_i^{\alpha} \times R_i^{\beta})$$

표 6. RA-SBE 평가식

구분	설명
항목별 중요도 가중치 W_i	자산 영향도(Impact), 정책적 중요도(Policy Priority), 산업 규제 요건(Compliance), 조직의 핵심업무 반영
실제 이행 수준 L_i	0~5점 또는 0~1 정규화값 * 0 = 미이행, 5 = 완전 이행(운영 정착 + 자동화)
위험 노출도 R_i	- Threat Intelligence 기반 * 공격 빈도(Frequency), 공격 성공 가능성(Likelihood), 시스템 취약성(Vulnerability), 기술부채(Debt) * 0~1로 정규화
α (이행도 민감도)	- 이행 수준 변화가 점수에 미치는 영향 조절 * 자동화 지속성에 높은 가중
β (위험 민감도)	- 위험 변화가 점수에 미치는 영향 조절 * 위험 급증 시 점수 영향 크게
C (보정계수)	조직 규모·산업규제에 따른 조정

3.2.1.1. 항목별 중요도 가중치 W_i

각 평가 항목이 조직의 보안 목표 달성에 어느 정도로 중요한지를 수치화한 값으로, 모든 항목을 동일하게 평가하는 체크리스트 방식의 단점을 보완하기 위해 각 항목의 “중요도”에 따라 차등 가중치를 부여한 값을 말한다. W_i (가중치) 산정 시 고려해야 할 4가지 핵심 요소는 표 7과 같다.

표 7. 항목별 중요도 가중치

항목	의미	예시
자산 영향도 (Impact on Critical Assets)	- 해당 항목이 보호해야 하는 자산이 얼마나 중요한가? * 예: 군 지휘통제체계(C4I) > 일반 내부 서버	- 매우 높음 0.4, - 높음 0.3 - 중간 0.2 - 낮음 0.1
정책적 우선순위 (Policy/Regulatory Priority)	- 국가정책, 국방정책, 기관 내부정책에서 강조되는 항목인가? * 예: 최소권한, 연속적 모니터링, 식별·인가	- 매우 높음 0.3 - 중간 0.2 - 낮음 0.1
위협 환경 중요도 (Threat Landscape Relevance)	- 현재 위협 동향(Threat Intelligence) 기반 중요도 * 예: 최근 랜섬웨어 증가 → 백업 무결성 항목 중요도 증가	- 매우 높음 0.2 - 중간 0.15 - 낮음 0.1
조직 특성 반영도 (Environment Fit)	- 산업군·조직 구조·내부 시스템 구성에 얼마나 중요하게 작동하는가? * 예: 클라우드 중심기관 → ID 기반 접근 통제가 매우 중요, 군 데이터 센터 → 네트워크 세그멘테이션·감사/추적이 매우 중요	- 높음 0.1 - 중간 0.07 - 낮음 0.05

종합 가중치 산정 방식은 다음과 같으며, 각 항목의 중요도를 4요소¹¹⁾ 합산해 0.1~1.0 사이 값으로 산출하며, 산출 예시는 표 8과 같다.

$$W_i = I_i + P_i + T_i + E_i$$

표 8. 항목별 중요도 가중치 “예”

제로트러스트 항목	자산 영향도 (Ii)	정책 우선순위 (Pi)	위험 중요도 (Ti)	조직 특성 (Ei)	최종 가중치 Wi (=I+P+T+E)
ID·인증 강도 (MFA/Passwordless)	0.4	0.3	0.2	0.1	1.0
최소권한(Least Privilege)	0.4	0.3	0.15	0.07	0.92
자산 식별·관리(Inventory)	0.3	0.2	0.15	0.1	0.75

체크리스트 방식은 “정성적 항목을 동일비중으로 단순합산”하는 방식이므로 중요 항목과 중요하지 않은 항목이 동일하게 취급되며, 산업별·조직별 위협 환경 미반영, 항목 간 인과성·상관성이 무시되고, 평가자 편차 발생, 시점 간 비교 어려움 등과 같은 문제가 필연적으로 발생한다. 그러나, Wi(가중치)는 이러한 문제를 보완할 수 있으며, 정량적·객관적·조직 특화형 평가체계를 만드는 핵심 요소라고 볼 수 있다.

3.2.1.2. 실제 이행 수준 Li

Li는 각 제로트러스트 항목이 조직에서 어느 수준까지 구현·운영되고 있는지를 정량화한 값으로 “도입의 깊이·정확도·자동화 수준”을 점수화한 값이다. Li가 필요한 이유는 체크리스트 방식은 “예/아니오” 평가라 수준 차이가 반영되지 않기 때문이다.

표 9. 실제 이행 수준

단계	의미
• Li = 0 : 미이행 (Not Implemented)	• 정책 절차 기술이 없음, 도입 계획조차 마련되지 않음
• Li = 1 : 계획 단계(Planned)	• 부분적 정책 존재, 도입 요구사항 정의됨, 파일럿 검토 초기
• Li = 2 : 초기 구현 (Initial)	• 기술 일부 도입, 제한적 파일럿/테스트 진행 • 적용 범위 제한 / 운영은 대부분 수작업
• Li = 3 : 중간 수준 구현 (Defined/Operational)	• 정책/기술 대부분 구현 / 운영이 일정 수준 정착됨 • 영역별 적용의 편차 존재, 로그·모니터링은 있으나 자동화 미흡
• Li = 4 : 고도화 자동화 (Managed/Integrated)	• 전체 업무영역에 일관 적용 / 탐자·대응 자동화 도입 • 정책 기반 접근제어(PDP/PEP) 연동, 모니터링·로그 연계
• Li = 5 : 최적화 지속적 개선 (Optimized/Adaptive)	• AI·UEBA 기반 행동 분석 적용, 리스크 기반 실시간 정책 변경 • 자동화된 교정·조치(Orchestration) • Threat Intelligence 연동으로 실시간 강화, ZT 완전정착 수준

11) Li: 자산 영향도, Pi: 정책 우선순위, Ti: 위협 환경 중요도, Ei: 조직 특성 반영도

예를 들어 “정책은 있지만 운영은 안 되는 상태”와 “자동화·상시 모니터링까지 되는 상태”가 같은 점수가 되어버리는 문제가 발생하여 실제 도입의 진척도·성숙도를 단계화하여 정량화해야 할 필요가 있다. 따라서 제로트러스트 가이드라인 2.0의 성숙도 개념을 정량 점수로 변환하는 핵심 요소가 바로 L_i 라 볼 수 있다. L_i 점수 기준은 표 9와 같이 0~5 단계를 권장하는데 이는 NIST ZT Maturity Model, ZTA, 국방 ZT 2.0의 성숙도 단계를 참고하였다.

일반적으로 실제 이행 수준 L_i 는 0~5점을 사용하나, RA-SBE 계산식에서는 0~1(예: 5점=1.0, 3점=0.6 등)로 정규화가 가능하다. 표 10과 같이 계산된 L_i 는 기존 체크리스트(“예/아니오”)의 한계를 보완하여 제로트러스트 도입 후 L_i 가 증가한 항목을 기반으로 정량적으로 비교가 가능하여 기존 경계모델 대비 향상되었음을 증명할 수 있다.

표 10. 실제 이행 수준 “예”

제로트러스트 항목	이행 수준 설명	점수(L_i)
ID 및 MFA (다중요소 인증)	전 직원 MFA 적용 및 비정상 로그인 탐지 자동화	4
최소권한 (Least Privilege)	역할기반 접근제어는 있으나 자동 승인/거버넌스는 미적용	3

3.2.1.3. 위험 노출도 R_i

위험 노출도 R_i (Risk Exposure)는 각 제로트러스트 항목이 현재 위험 환경에서 얼마나 공격받기 쉽고, 그로 인한 위험이 얼마나 큰지를 나타내는 값을 말한다. 즉, “지금 바로 공격받을 가능성과 취약성의 정도”를 정량화한 입력값이다. R_i 가 필요한 이유는 “현재 위험이 어떤 방향으로 증가하는지”를 반영하지 못하는 제로트러스트 체크리스트 기반 평가의 치명적 한계를 보완할 수 있다. 즉, 랜섬웨어 증가 → 백업·세그멘테이션 항목의 위험도 증가, 인증 정보 탈취 증가 → MFA·IAM의 위험도 증가와 같이 반영할 수 있다. 즉, R_i 는 “시간에 따라 변하는 위험 상황”을 동적으로 반영하여 평가의 현실성을 높여줄 수 있다. 위험 노출도(R_i) 구성요소 (0~1 정규화)는 표 11과 같이 아래 5가지 요소를 합산하여 R_i 를 산정한다.

표 11. 위험 노출도

항목	의미	예시
공격 가능성 (Likelihood)	해당 항목이 공격에 악용될 가능성	MFA 미도입 → 공격 가능성 매우 높음(0.05~0.3)
취약성 수준 (Vulnerability Severity)	시스템의 기술적 취약성 (CVE, 설정오류 등)	취약성이 클수록 R_i 증가 (0.05~0.25)
노출도 (Exposure Level)	인터넷·외부 네트워크에 얼마나 열려 있는가	외부 서비스 > 내부망 서비스 (0.05~0.2)
위협 동향 (Threat Intelligence Relevance)	최근 공격 트렌드와 상관성	공격 급증 → 항목 위험도 반영 (0.05~0.2)
보안 통제 부재로 인한 영향도 (Residual Impact)	보안통제가 미흡할 때 발생하는 잠재 피해	영향이 클수록 R_i 증가 (0.05~0.2)

위험 노출도 산정식은 다음과 같다. 점수 범위는 0.1~1.0 이며, 값이 높을수록 그 항목이 시급히 보완되어야 함을 의미한다. 표 12는 제로트러스트 평가 항목에 대해 조직의 실제 위험 상황 기반으로 위험 노출도를 산정한 예시를 보여준다.

$$R_i = L_i^{threat} + V_i + E_i + T_i + I_i^{residual}$$

표 12. 위험 노출도 “예”

제로트러스트 항목	공격 가능성 (L)	취약성 (V)	노출도 (E)	위협동향 (T)	영향도 (I)
MFA·ID 관리(=0.85)	0.25	0.15	0.1	0.2	0.15
자산 인벤토리(=0.50)	0.15	0.1	0.05	0.1	0.1
암호화(TLS/At-rest)(=0.50)	0.1	0.05	0.1	0.15	0.1

예를 들어 MFA·ID 항목 $R_i = 0.85$ (매우 높음)은 최근 Credential Attack 증가와 MFA 미흡에 따라 위험이 매우 높음을 나타낸다. 즉, 위험이 높은 항목($R_i \uparrow$)은 점수 계산 비중이 자동으로 커지나, 위험이 낮은 항목은 과도한 평가 비중을 차지하지 않음을 알 수 있다. 따라서 이를 활용하면 동적이고 현실적인 제로트러스트 도입 수준 분석이 가능하다.

3.2.1.4. α (이행도 민감도)

이행도 민감도 α (Alpha, Implementation Sensitivity)는 이행 수준(L_i)이 전체 점수에 “얼마나 민감하게 영향을 미칠 것인가”를 조정하는 지수 가중치이다. 쉽게 말해, L_i (실제 이행 수준)의 중요성을 강화하거나 약화시키는 조정 파라미터이다. α 가 필요한 이유는 체크리스트 기반 평가는 $L_i = 2 \rightarrow 3$ 과 $L_i = 4 \rightarrow 5$ 를 “동일한 차이 1”로 취급하는 치명적인 문제가 있기 때문이다. 예를 들어, $L_i 3 \rightarrow 4$ (자동화 도입) 향상은 매우 큰 변화를 나타내지만, $L_i 4 \rightarrow 5$ (AI 기반 적응형 정책) 향상은 더 큰 효과를 나타낸다. 즉, 고도화될수록 효과가 기하급수적으로 증가하는데 이를 반영하기 위해 α 를 사용하며, 직관적 의미와 “예”는 표 13, 표 14와 같다. RA-SBE 평가식에서 L_i 는 Exponent(지수)로 α 를 갖게 되는데, 즉, L_i 가 높을수록 점수 기여도가 폭발적으로 증가한다는 것을 의미한다. α 는 조직의 정책 목표와 평가 철학에 따라 다르게 설정된다.

표 13. 이행도 민감도 의미

α 값	의미	특징
$\alpha < 1$	저감도	이행수준의 상승이 점수에 미치는 영향 작게
$\alpha = 1$	기본 감도	L_i 를 그대로 반영
$\alpha > 1$	고감도	L_i 가 높아질수록 점수가 훨씬 빠르게 증가

표 14. 이행도 민감도 “예”

Zero Trust 단계	α 값	의미
도입 초기 (기술 불균형 상태)	0.8 ~ 1.0	이행도의 영향 완만하게
중간 성숙도(고도화가 전략 목표)	1.0 ~ 1.3	이행도가 중요한 영향
ZT 고도화(자동화·AI 기반 중시)	1.3 ~ 1.6	이행도 향상에 높은 보상
국방 핵심 인프라(안전성 최우선)	1.6 ~ 2.0	이행 수준에 매우 높은 민감도

표 15는 α 값별 이행도 민감도 결과를 보여주고 있다. $L_i = 4 \rightarrow 5$ 변화는 $\alpha=1.6$ 에서 아주 큰 점수 차이가 발생하므로 제로트러스트 “고도화”가 점수에서 확실히 드러나는 것을 알 수 있다. 제로

트러스트 환경에서 α 를 높게 설정하는 이유는 자동화, 지속적 검증, 정책 기반 제어, 실시간 대응, AI 기반 적응형 보안 등의 이유로 단순 도입(Level 2/3)보다 고도화(Level 4/5)의 효과가 매우 크다고 볼 수 있다. 따라서 α 값을 1.3~1.6 이상으로 두는 것이 실제 효과를 반영하는 데 적합하다.

표 15. 이행도 민감도 결과비교

Li(정규화)	$\alpha = 0.8$	$\alpha = 1.0$	$\alpha = 1.3$	$\alpha = 1.6$	$\alpha = 2.0$
0.2	0.28	0.20	0.14	0.10	0.04
0.4	0.46	0.40	0.33	0.26	0.16
0.6	0.67	0.60	0.53	0.45	0.36
0.8	0.84	0.80	0.77	0.71	0.64
1.0	1.00	1.00	1.00	1.00	1.00

3.2.1.5. β (위험 민감도)

위험 민감도 β (Beta, Risk Sensitivity)는 “각 항목의 위험 노출도(R_i)가 전체 평가 점수에 얼마나 민감하게 영향을 주도록 할 것인가”를 조정하는 지수 가중치로, 표 16에서 보는 것과 같이 R_i (위험 노출도)의 중요성을 강화하거나 약화시키는 조정 파라미터이다. β 가 필요한 이유는 체크리스트 기반 평가는 기본적으로 “위험 환경의 변화”를 반영하지 못하는 구조라고 볼 수 있다. 그러나 실제 환경에서는 특정 공격이 급증(예: 랜섬웨어)하면 → 세그멘테이션·백업·EDR의 위험 중요도 증가, 인증정보 탈취 공격 증가 → MFA·IAM의 위험 중요도 증가 등과 같이 위험 동향 변화가 평가 결과에 즉시 반영되어야 한다. 이를 가능하게 하는 변수가 바로 β 이며, β 의 직관적 의미와 “예”는 표 17과 같다.

표 16. 위험 민감도 의미

β 값	의미	특징
$\beta < 1$	위험 영향 완화	위험 변동이 점수에 미치는 영향 줄임
$\beta = 1$	기본감도	위험을 그대로 반영
$\beta > 1$	위험 영향 확대	위험 증가가 점수에 강하게 반영됨

표 17. 위험 민감도 “예”

조직 특성	β 값	해석
일반 기업	0.9~1.1	기본 반영
클라우드 서비스 중심 조직	1.1~1.3	위험에 더 민감해야 함
금융·전자정부	1.3~1.5	위험 향상에 강한 반응 필요
국방·SOC·국가기반시설	1.5~2.0	위험 상황을 매우 강하게 반영

RA-SBE 평가식에서 β 는 R_i 를 Exponent(지수)로 반영하는데, R_i 가 높을수록 점수에 미치는 영향이 기하급수적으로 커지는 것을 알 수 있다. 통상 β 값은 조직의 위험 대응 철학과 산업군 위험성에 따라 정하는데, 특히 국방 제로트러스트 2.0 수준이면 $\beta=1.5\sim2.0$ 이 매우 적합한 것으로 본다. 표 18은 R_i (위험 노출도)가 0.2~0.9일 때 β 값에 따라 결과가 얼마나 달라지는지를 보여주고 있다. 예를 들어 R_i 가 0.8 → 0.9로 변할 때, $\beta=2.0$ 이면 0.64 → 0.81로 대폭 증가하여 “위험 급증에 매우 민감한 평가”가 된다는 것을 알 수 있다.

표 18. 위험 민감도 결과비교

Ri	$\beta=0.8$	$\beta=1.0$ (기본)	$\beta=1.3$	$\beta=1.6$	$\beta=2.0$
0.2	0.28	0.20	0.14	0.10	0.04
0.4	0.46	0.40	0.33	0.26	0.16
0.6	0.67	0.60	0.53	0.45	0.36
0.8	0.84	0.80	0.77	0.71	0.64
0.9	0.93	0.90	0.87	0.82	0.81

RA-SBE에서 β 를 높게 설정하는 이유(제로트러스트 철학 반영)는 제로트러스트는 공격 전제를 기본 가정으로 하기 때문에 위험 동향 반영은 반드시 정량화되어야 한다. 따라서, β 값을 1.3~1.8 사이로 높게 설정하면 “위험이 증가할수록 평가 결과에 즉각 반영”된다는 것을 의미하며, 이는 국방·공공기관 ZT 성숙도 분석의 핵심 요구사항과 일치한다고 볼 수 있다.

α 와 β 의 설정값은 보안전문가, 정보보호 담당자, 제로트러스트 평가 경험자 등을 대상으로 $\alpha \cdot \beta$ 의 후보 범위를 1.0~2.0으로 제시하고, 이후 조사에서는 평균값, 표준편차, 사분위 범위를 분석하여 전문가 합의도가 높은 1.3~1.6 구간을 최종 적용범위로 설정하였다. 현업에서는 α 와 β 를 고정 상수가 아니라 평가대상 기관의 보안 중요도, 업무 민감도, 위험수용 수준에 따라 조정 가능한 보정계수로 설정하여 사용한다.

3.2.1.6. C(보정계수)

C(보정계수, Calibration Factor)는 한마디로 말하면, 계산된 점수를 “현실에 맞게 조정”하거나 “원하는 스케일로 맞추기 위한 계수”이다. 즉, 조직 규모, 산업 특성, 평가 버전, 목표 성숙도 등에 맞게 점수분포를 조정(Scaling & Normalization)하는 역할을 하며, “그냥 숫자”가 아니라 0~100점, 0~5등급, 성숙도 레벨 등으로 실제 보고서/평가체계에 맞춰주는 마지막 단계라고 볼 수 있다.

보정계수 C_domain 설정 예로 ID & Access: 1.0(기본 중요), Device: 0.9(상대적 중요도 낮게), Network: 1.1(조직 전략상 중요), Data: 1.3(데이터 보호를 최우선으로 강조)라고 하면, 보정 후 영역별 점수는 표 19와 같다. 즉, C(보정계수)는 $Wi \cdot Li \cdot Ri \cdot \alpha \cdot \beta$ 로 계산된 원시점수를 조직·산업·연도별로 비교 가능하고 직관적인 0~100점 스케일로 맞추기 위한 최종 스케일링 인자이며, 필요시 도메인별 중요도 조정을 위해 영역별로도 설정할 수 있다.

$$Score_{domain} = Raw \times C_{domain}$$

표 19. 보정계수 “예”

도메인	Raw Score	C_domain	보정 후 점수
ID & Access	2.0	1.0	2.0
Device	1.5	0.9	1.35
Network	2.5	1.1	2.75
Data	1.8	1.3	2.34

3.2.2. RA-SBE 모델 기반 도입 전·후 효과성 비교

RA-SBE 모델을 활용해 제로트러스트 도입이 기존 경계모델 대비 “어떻게 향상되었는지”를 표 20과 같이 Before-After 평가 모델(Baseline과 비교) 방식으로 확인하여 효과성을 검증할 수 있다.

표 20. ZT 도입 전후 산정식

Baseline 점수(BS)	ZT 도입 후 점수(ZTS)
$RA-SBE_{Before} = \sum_{i=1}^N (W_i \times L_{i,Before} \times R_{i,Before})$	$RA-SBE_{After} = C \times \sum_{i=1}^N (W_i \times L_{i,After}^{\alpha} \times R_{i,After}^{\beta})$

이를 위해 Baseline(Before), 즉 제로트러스트 도입 이전 상태와 기존 “경계(Perimeter) 중심 보안 모델” 기준으로 점수를 산정한다. After(RA-SBE Model)는 제로트러스트를 실제 도입한 이후 상태와 RA-SBE 모델을 적용하여 점수 산정하는 방식이다. 즉, Baseline 점수(BS)와 제로트러스트 도입 후 점수(RA-SBE 모델기준)를 산정하여 이 두 값을 비교하면 된다. BS와 RA-SBE 모델 점수를 산정하기 위해 다음과 같은 예시 조건을 사용한다.

$\alpha = 1.3$ (이행수준 민감도 강화)
 $\beta = 1.5$ (위험 민감도 강화)
 $C = 20$ (0~100점 스케일 맞추기)

그림 3은 본 논문에서 제안한 RA-SBE 모델을 활용하여 Step-1부터 Step-6 까지 적용했을 때 제로트러스트 도입 전(Baseline) 총점은 55.4점, 제로트러스트 도입 후(RA-SBE 기반) 총점은 62.4점이므로 정량적 향상률이 약 12.6%가 개선되어 효과성을 입증할 수 있다.

Step 1. Before(경계 모델)의 W_i, L_i, R_i 설정

항목	가중치 W_i	Before L_i	Before R_i
MFA-ID 통제	1.0	1	0.85
NW 세그멘테이션	0.9	1	0.80
지속 모니터링	0.8	2	0.75

Step 2. Baseline Score(BS) 계산

항목	계산	점수
MFA-ID 통제	$1.0 \times 1 \times 0.85$	0.85
NW 세그멘테이션	$0.9 \times 1 \times 0.80$	0.72
지속 모니터링	$0.8 \times 2 \times 0.75$	1.20
Baseline Raw Score		2.77

$BS = \sum (W_i L_i R_i)$

Step 3. After(ZT 도입 후) L_i, R_i 변화 입력

항목	After L_i	After R_i
MFA-ID 통제	4	0.40
NW 세그멘테이션	3	0.50
지속 모니터링	4	0.40

Step 4. RA-SBE(After Score)계산

$RA-SBE_{After} = \sum (W_i \times L_i^{\alpha} \times R_i^{\beta})$

항목	계산	점수
MFA-ID 통제	$1 \times 4^{1.3} \times 0.40^{1.5}$	1.16
NW 세그멘테이션	$0.9 \times 3^{1.3} \times 0.50^{1.5}$	1.03
지속 모니터링	$0.8 \times 4^{1.3} \times 0.40^{1.5}$	0.93
After Raw Score	$\alpha = 1.3, \beta = 1.5$ 적용	3.12

Step 5. 0~100점 스케일 변환($C = 20$ 적용)

항목	Raw	$\times 20$	점수
Baseline Raw	2.77	$\times 20$	55.4점
ZT Raw	3.12	$\times 20$	62.4점

Step 6. 개선을 계산

$개선율 = \frac{62.4 - 55.4}{55.4} \times 100\% = 12.6\%$

그림 3. 제로트러스트 도입 전·후 개선을 계산

위와 같이 기존 체크리스트 방식은 “예/아니오(0/1)”라 제로트러스트 도입 전·후 비교가 불가능하지만, 표 21과 같이 RA-SBE는 Wi·Li·Ri 기반 정량 평가이므로 동일 항목에 대해 Before와 After를 수치로 직접 비교가 가능하며, 동적 Threat Intelligence를 반영, 이행수준 상승(Li ↑), 위험노출도 감소(Ri ↓), 중요 항목 가중치 반영(Wi) 등으로 제로트러스트 도입 효과를 “데이터로” 증명할 수 있다.

표 21. RA-SBE 적용 전·후 비교

기존 평가	RA-SBE Before-After 비교
정성적	정량적
예/아니오	지수 기반 점수
변동성 미반영	Threat 기반 실시간 반영
ZT 도입 효과가 모호	수치로 개선 증명
산업 맞춤형 불가	가중치 민감도 커스터마이징 가능

4. 결론

기존의 제로트러스트 성숙도 평가체계는 주로 체크리스트 기반의 정성적 점검 방식에 의존하고 있다. 이러한 방식은 이해가 쉽고 적용이 용이하다는 장점이 있으나, 평가자의 주관적 판단에 따라 결과가 달라질 수 있고, 모든 조직에 동일한 항목을 일률적으로 적용함으로써 조직별 리스크 특성과 산업적 맥락을 충분히 반영하지 못한다는 근본적 한계를 지닌다. 이에 본 연구는 이러한 한계를 보완하기 위해 위험 적응형 점수기반 평가모델을 설계하고, 실제 평가식을 적용하여 도입 전·후의 결과 값을 산출·비교함으로써 제로트러스트 도입 효과를 정량적으로 분석할 수 있는 평가 프레임 을 제시하였다.

본 연구에서 제안한 위험 적응형 점수기반 평가모델은 각 평가항목에 대해 정책 중요도(Policy Impact)와 자산 영향도(Asset Criticality)¹²⁾를 반영한 항목별 가중치(Weight)를 부여하고, 여기에 위험노출도(Risk Exposure)와 이행수준(Compliance Level)을 결합하여 종합 점수를 산정하는 방식이다. 이는 단순한 ‘체크 여부’ 중심의 평가에서 벗어나, 항목의 상대적 중요도와 실제 위험 환경을 함께 고려함으로써 보다 정량적이고 객관적인 평가가 가능하도록 설계되었다는 점에서 기존 성숙도 평가 방식과 차별성을 가진다.

이러한 평가 방식의 장점은 다음과 같이 정리할 수 있다. 첫째, 조직 맞춤형 평가의 가능성을 제고한다는 점이다. 조직의 산업 특성, 핵심 자산, 위협 모델에 따라 항목별 가중치를 조정함으로써 보안투자의 우선순위를 현실적으로 반영할 수 있다. 예를 들어 방위산업체의 경우 접근통제·계정관리 항목의 비중을 높게 설정할 수 있으며, 금융기관의 경우 데이터 보호 영역의 가중치를 확대함으로써 보다 합리적인 평가 결과를 도출할 수 있다. 둘째, 평가의 객관성과 반복 가능성을 강화한다. 정성적 판단 대신 정량적 가중치 계산식을 적용함으로써 평가자의 주관 개입을 최소화하고, 동일 기준 하에서 시점 간 비교가 가능하다. 또한 Threat Intelligence 기반의 위험노출도 반영을 통해 변화하는 위험 환경을 평가 결과에 반영할 수 있다. 셋째, 항목별 점수를 KPI 지표와 연계함으로써 보안 활동이 조직의 성과 관리와 의사결정에 미치는 영향을 정량적으로 설명할 수 있다는 점에서, 제로트러스트를 단순한 기술적 과제가 아닌 조직 성과 개선의 수단으로 활용할 수 있는 기반을 제공한다.

12) 자산 영향도(Asset Criticality)는 특정 정보자산이 침해·장애 시 임무 수행, 서비스 연속성, 기밀성·무결성·가용성에 미치는 영향을 평가한 수준으로, 보안 우선순위와 자원 배분의 기준이 된다.

본 연구는 제로트러스트 도입 효과를 대규모 실증 데이터로 검증하기보다는, 도입 전·후 효과를 정량적으로 비교할 수 있는 평가 모델의 구조와 논리를 제시하는 데 연구 범위를 한정하였다. 제안된 평가모델은 파일럿 수준의 실제 운영 환경이나 실험사업에서 적용·검토가 가능한 구조를 가지며, 이러한 적용을 통해 평가 항목 구성과 민감도 설정에 대한 추가적인 검증이 가능하다.

다만, 본 연구에서 제시한 측정 방법은 몇 가지 한계를 지닌다. 첫째, 가중치와 위험노출도 산정의 복잡성과 표준화 문제이다. 자산 분석, 위협 정보, 정책 목표 간의 상관관계를 체계적으로 정립해야 하며, 실제 기관에서는 데이터 불균형과 전문가 의존도가 높아 표준화된 가중치 산출에 제약이 발생할 수 있다. 둘째, 수식 기반 평가 방식은 직관성이 상대적으로 낮아 비전문가나 정책 결정자에게는 단순 체크리스트 방식보다 해석 난이도가 높을 수 있으며, 이를 보완하기 위한 레이더 차트나 히트맵과 같은 시각화 도구의 활용이 요구된다. 셋째, 위험노출도 산정은 Threat Intelligence의 최신성과 정확성에 크게 의존하므로, 위협 정보의 품질이 낮거나 갱신이 지연될 경우 평가 결과가 왜곡될 가능성이 존재한다. 넷째, 향후 기존 경계모델의 Baseline 보안항목을 보다 구체화하고, ZT 도입 후 점수 상승의 비교 타당성과 C=20 보정계수의 비왜곡성을 수학적으로 검증할 필요가 있다.

이러한 한계를 고려할 때, 향후 연구에서는 기계학습 기반의 자동 보정 기법을 활용하여 조직별 과거 평가 결과와 위협 데이터를 학습함으로써 가중치와 위험노출도를 동적으로 조정하는 Adaptive Weighting Engine¹³⁾의 구현 가능성을 검토할 수 있다. 또한 기존 ISA, DoD, NIST 모델을 기반으로 산업별·기관 유형별 특성을 반영한 평가 항목 풀(Pool)을 구성하는 Dynamic Checklist Library¹⁴⁾를 구축함으로써 평가모델의 범용성과 적응성을 확장할 수 있을 것이다. 더 나아가 평가 결과를 KPI 및 성과관리 시스템과 연계하여 보안 성숙도 변화와 개선 효과를 시각화하는 대시보드형 거버넌스 체계로 확장하는 것도 하나의 발전 방향이 될 수 있다. 뿐만 아니라, 향후 공공·국방기관 적용을 위한 단계별 지침을 구체화하고, 중소 조직의 인력·비용 한계를 고려한 간소화 적용방안을 제시할 필요가 있다.

종합하면, 위험 적응형 점수기반 평가모델은 기존 체크리스트 기반 평가가 지닌 단순성과 주관성을 극복하고, 제로트러스트 도입 효과를 보다 정량적이고 위협 기반으로 분석할 수 있는 현실적인 대안으로 기능할 수 있다. 궁극적으로 제로트러스트 보안평가의 방향은 고정된 성숙도 점검에서 벗어나, 변화하는 위협 환경과 조직 특성을 반영하는 위험 적응형 점수기반 지능형 평가체계로의 전환에 있다고 볼 수 있다.

참고문헌

- [1] National Institute of Standards and Technology. Zero Trust Architecture (NIST SP 800-207). 2020.
- [2] Kindervag J. Build Security Into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research. 2010.
- [3] Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model Version 2.0. 2023.
- [4] 국방부. 국방 사이버안보 혁신 추진계획. 2023.
- [5] 과학기술정보통신부, 한국인터넷진흥원. 제로트러스트 가이드라인 2.0. 2024.
- [6] Gartner. Market Guide for Zero Trust Network Access. 2022.

- 13) 위협 수준, 자산 중요도, 운영 환경 변화에 따라 평가 항목의 가중치를 동적으로 조정하는 메커니즘으로, 고정 가중치의 한계를 보완하고 실제 위협 변화를 평가에 반영한다는 것을 의미한다.
- 14) 조직의 환경, 위협 동향, 자산 특성 변화에 따라 평가 항목을 유연하게 추가·제거·조정하는 체크리스트 체계로, 고정 목록의 한계를 극복하고 현실 적합성을 높이는 것을 말한다.

- [7] 한국인터넷진흥원. 제로트러스트 보안 도입 동향 및 주요 이슈 분석. 2022.
- [8] 한국인터넷진흥원. 공공·민간 분야 제로트러스트 보안 도입 동향 및 과제. 2022.
- [9] 김현수, 박성우. 제로트러스트 보안 모델의 성숙도 기반 평가 방법 연구. 정보보호학회논문지, 제32권 제4호, pp. 789-803. 2022.
- [10] 이정민, 최윤석. 침투시험 기반 보안 통제 효과성 평가 기법에 관한 연구. 정보보호학회논문지, 제31권 제6호, pp. 1125-1137. 2021.
- [11] 신규용 등. 한국군 맞춤형 제로 트러스트(Zero Trust) 구축방안 연구. 융합보안논문지, 제23권 제4호, pp. 131-139. 2023.
- [12] 최한선 등. 제로트러스트의 도입과 적용 : 방산 보안의 새로운 시대. 국방과 보안, 제6권 제1호, pp. 78-101. 2024.
- [13] 전자신문. 국방부, ZT 가이드라인 만든다...N·SF·K-RMF도 총망라. <https://www.etnews.com/20250904000268/> (검색일 2025. 9. 4).
- [14] 김승주, 이경호. 정보보호 관리체계(ISMS) 기반 보안평가의 한계와 개선 방향. 정보보호학회논문지, 제28권 제3호, pp. 623-635. 2018.
- [15] 박정수. 제로트러스트 체크리스트 항목 구현 방법론에 관한 연구. 스마트미디어저널, 제14권 제12호, pp. 193-201. 2025.