제로트러스트 성숙도 평가의 난점과 진단모델 설계 방향: 전문가 인터뷰를 중심으로

서진우*, 서정우*, 공나영*, 송민희*, 박기웅1

세종대학교 정보보호학과 (학부생, 교수1)

Challenges in Zero Trust Maturity Assessment and Design Directions for a Diagnostic Model: An Expert Interview-Based Study

Jin-Woo Seo*, Jeong-Woo Seo*, Na-Young Kong*, Minhee Song*, Ki-Woong Park1

Dept. of Computer and Information Security, Sejong University(Ungraduate student, Professor1)

요 약

본 연구는 제로트러스트 가이드라인 기반 성숙도 평가의 한계를 규명하고, 이를 개선하기 위한 자동화된 성숙도 진단 모듈의 설계 방향을 제안한다. 전문가 인터뷰를 통해 기존 평가 방식이 개념 중심 구조, 정량화 기준 부족, 획일적 체크리스트, 수작업 의존성 등의 문제를 지니고 있음을 도출하였다. 이에 따라 정량적 평가 체계, 환경 맞춤형 동적 평가 모델, 수동·자동 융합형 구조, 표준 기반 통합 및 지속적 피드백 체계를 핵심 설계 원칙으로 제시한다. 본 연구는 실무 환경에서 적용 가능한 제로트러스트 성숙도 평가의 효율성과 신뢰성을 향상시키는데 기여한다.

I. 서론

최근 기업의 IT 환경은 클라우드 전환, 원격 근무 확대, 시스템 복잡성 증가로 내외부 경계가 모호해지며 기존 경계 기반 보안 모델의 한계가 명확해지고 있다[1]. 이를 해결하기 위한 새로운 보안 패러다임으로 "Never Trust, Always Verify" 원칙을 기반으로 한 제로트러스트 모델이 주목받고 있으며 국내외 주요 기관에서도 관련 가이드라인을 발표하고 있다[2][3].

그러나 제로트러스트 모델에 대한 가이드라인은 구체적인 기술 명세보다 개념과 원칙 중심으로 제시되어 있다. 이로 인해 성숙도를 평가할 명확한 근거가 제시되지 않아 정량적 평가를 위한 체계를 갖추지 못하고 있다[4].

따라서 본 연구는 제로트러스트 가이드라인을 기반으로 한 성숙도 진단의 한계점을 규명하기 위해 전문가 인터뷰를 수행하고, 도출된 시사점을 바탕으로 자동화된 제로트러스트 성숙도 진단 모듈의 설계 방향을 제안한다.

II. 전문가 인터뷰 기반 시사점 분석

본 연구에서는 제로트러스트 성숙도 평가의 실무적 어려움과 자동화 요구를 도출하기 위해 보안 전문가 3인을 대상으로 인터뷰를 수행하였다. 질문은 평가 타당성, 자동화 필요성, 기술 구현 현실성, 성숙도 평가 방식의 한계와 핵심 지표 등을 중심으로 다음과 같이 구성하였다.

Q1. 제로트러스트 가이드라인 체크리스트 기반 성숙도 평가 방식이 현업에서 유효한가?

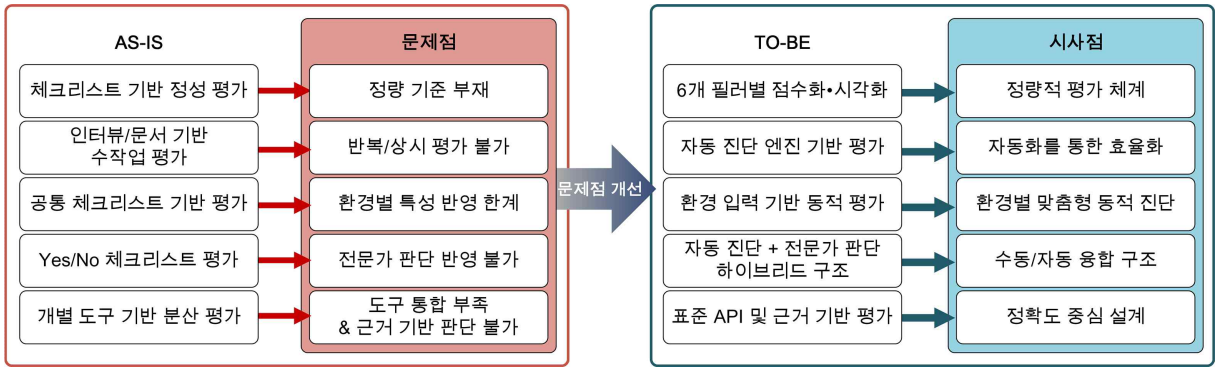
Q2. 기업마다 환경이 다른 상황에서 공통 체크리스트로 커버하는 것이 가능한가?

---

1 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 연구는 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 정보보호핵심원천기술개발(Project No. RS-2026-25519773, 30%; RS-2024-00438551, 10%),

실감콘텐츠핵심기술개발(Project No. RS-2023-00228996, 20%), 대학ICT연구센터(ITRC) (Project No. ,10% IITP-2026-RS-2021-II211816, 10%), 한국연구재단(NRF) 핵심연구사업(Project No. RS-2026-25481431 30%)의 지원을 받아 수행된 연구임.



(그림 1) 인터뷰 기반 제로트러스트 성숙도 평가의 한계와 설계 시사점

Q3. 제로트러스트 도입 시 기업에서 겪는 가장 어려운 점은 무엇인가?

Q4. 성숙도 평가에서 실제로 의미 있는 지표는 무엇인가?

Q5. 기존 제로트러스트 성숙도 진단 방식은 어떠한 한계를 가지는가?

위와 같은 질문을 통해 도출한 제로트러스트 성숙도 진단 방식의 한계는 다음과 같다.

첫째, 개념 중심 가이드라인과 실무 데이터 간의 간극이 존재한다. 전문가들은 제로트러스트가 특정 기술이 아닌 개념 중심의 가이드라인이기 때문에 실제 환경에 적용하고 평가하는 방식이 명확하지 않아 해석상의 어려움이 발생한다고 지적하였다. 특히 클라우드, 온프레미스, 하이브리드 환경이 혼재되고, 컨테이너 및 GenAI(Generative Artificial Intelligence) 환경까지 포함되는 복합 구조에서는 고정된 체크리스트만으로 실제 보안 수준을 정확히 반영하기 어렵다는 점이 강조되었다.

둘째, 평가를 위한 정량화된 기준이 부족하다. 전문가들은 성숙도 평가의 신뢰성을 확보하기 위해서는 명확한 기준과 정량화된 지표가 필요하다고 보았다. 그러나 기존 방식은 명확한 근거 없이 정성적 판단에 의존하여 보안 수준을 객관적으로 수치화하기 어렵다. 특히 성숙도 평가 결과를 의사결정에 활용하기 위해서는 6개 영역(식별자, 기기, 네트워크, 시스템, 애플리케이션, 데이터)별 현재 수준에 대해 명확한 근거에 기반하여 정량적으로 성숙도를 산출하고 이를 시각화할 수 있어야 한다는 점이 제시되었다.

셋째, 획일적 평가 구조는 환경별 편차를 반영할 수 없다. 인프라 환경과 보안 수준은 기업별로 상이하지만, 기존 평가는 획일적인 체크리스트를 적용하는 경우가 많다. 이에 따라 성숙도 수준에 대해 핵심적인 공통 기준을 유지하면서도 조직 환경을 반영할 수 있는 동적 평가 구조가 필요하다는 시사점이 도출되었다.

넷째, 수작업 중심의 평가는 비효율적이다. 기존 성숙도 평가는 인터뷰 및 문서 기반의 수작업 방식으로 수행되며 데이터 수집과 현황 분석 과정에서 많은 시간과 공수가 소모된다. 이에 따라, 평가 비용을 줄이기 위한 자동화 기반 진단 체계의 필요성이 제기되었다. 그러나 성숙도 평가의 전 과정을 완전히 자동화하는 데에는 현실적인 제약이 존재한다. 정책 판단 및 목표 설정과 같은 주관적인 영역에서는 전문가의 개입이 필요하며, 이에 따라 자동 진단과 수동 검토를 결합한 하이브리드 평가 구조가 현실적인 대안으로 제시되었다.

이러한 분석을 통해 도출된 한계는 다음 [표 1]과 같이 정리된다. 특히 기존 성숙도 평가는 정량화된 평가 기준의 부족과 수작업 의존성으로 인해 일관성과 재현성을 확보하기 어렵다는 한계를 가진다.

III. 자동화 기반 성숙도 진단 모듈 청사진 도출

인터뷰 결과를 토대로 본 연구에서는 자동화 기반의 성숙도 진단 모듈 설계 방향을 다음과 같이 제안한다.

(1) 정량적 평가 체계

자동 진단 모듈은 6개 영역별 평가 결과를

정량화된 점수로 환산하고, 이를 기반으로 현재 수준과 목표 수준을 비교할 수 있도록 설계되어야 한다. 정성적인 진단에서 벗어나 의사결정에 활용 가능한 정보가 제공되어야 조직간 성숙도를 비교하거나 보안 투자 효과를 분석할 수 있다. 따라서 평가 기준 및 점수를 환산하는 방식을 명확히 규정하여 일관성 있는 결과를 얻을 수 있어야 한다.

(2) 환경 맞춤형 동적 평가 모델

획일적인 평가 기준 대신 조직의 인프라 및 운영 환경을 반영할 수 있는 유연한 평가 모델이 요구된다. 온프레미스, 클라우드, 하이브리드 환경 등 다양한 인프라를 포괄하기 위해서는 산업군 및 보안 요구 수준에 따라 평가 요소가 동적으로 조정될 수 있어야 한다. 이를 통해 기존 고정형 평가 모델의 한계를 극복하고, 실제 환경에 적합한 성숙도 진단이 가능하다.

(3) 수동·자동 융합형 하이브리드 구조

시스템이 처리 가능한 영역은 모듈을 통해 자동화하되, 정책 해석과 같이 전문가의 판단이 필요한 부분은 수동 검토를 병행해야 한다. 이는 완전 자동화 방식에 비해 현실적인 적용 가능성이 높다. 특히 조직 내부 규정과 같은 정성적 요소는 자동화에 한계가 있으므로 수동·자동 융합형 하이브리드 구조를 설계에 반영하는 것이 필요하다.

(4) 정확도 중심의 통합 구조

다양한 보안 도구를 단순히 통합하는 것에서 그치기보다 필요한 기능과 평가를 위한 증적 평가 자료를 선별하고 연동하여 상위 플랫폼에서 통합 평가를 수행하는 방식이 바람직하다. 또한 REST(Representational State Transfer), OAuth2.0(Open Authorization 2.0), SAML2(Security Assertion Markup Language)와 같은 표준 기반 기술을 적용함으로써 향후 확장성과 유지보수성을 확보할 수 있다. 이러한 구조는 도구 간 불필요한 의존성을 최소화하면서도 다양한 운영 환경에 유연한 대응을 가능하게 한다.

(5) 지속적 진단 및 피드백 구조

성숙도 평가는 일회성 활동이 아닌 지속적인 관리 과정으로 접근되어야 한다. 평가 결과를 토대로 개선점을 도출하고 실질적인 보안 환경 개선으로 이어지는 반복적인 구조가 필요하다. 이러한 지속적인 진단과 피드백 과정을 통해 조직의 보안 성숙도를 점진적으로 향상시킬 수 있다.

IV. 결론

본 연구는 전문가 인터뷰를 중심으로 제로트러스트 성숙도 평가의 실무적 한계를 분석하고 자동화 성숙도 진단 설계 방향을 제안하였다.

이에 따라 본 연구는 기존 성숙도 평가에서 개념 중심 가이드라인, 정량화 부족, 수작업 의존성, 환경 다양성, 전문가 의존성으로 인해 실제 조직 환경에서 일관되고 반복 가능한 방식으로 수행되기 어렵다는 점을 확인하였다. 이를 바탕으로 정량화된 점수 체계, 데이터 기반 자동화 평가, 환경 맞춤형 동적 평가, 수동·자동 하이브리드 구조, 표준 기반 통합이라는 설계 전략을 제안한다. 이는 전문가 인터뷰를 바탕으로 실제 성숙도 평가 과정에서 요구하는 실질적인 내용을 담아냈다는 점에서 의의를 가진다.

향후 연구에서는 다양한 산업군과 조직을 대상으로 실증 검증을 수행하고 제안한 구조를 실제 시스템으로 구현하여 성숙도 평가의 정확성과 활용성을 검증하고자 한다.

[참고문헌]

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” NIST Special Publication 800-207, National Institute of Standards and Technology (NIST), Aug. 2020. DOI: 10.6028/NIST.SP.800-207.

[2] 한국인터넷진흥원(KISA), “제로트러스트 가이드라인 2.0,” 2024.

[3] Cybersecurity and Infrastructure Security Agency (CISA), “Zero Trust Maturity Model Version 2.0,” 2023.

[4] Mushtaq, S.; Mohsin, M.; Mushtaq, M.M. A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains. Sensors 2025, 25, 6118. https://doi.org/10.3390/s25196118