제로트러스트 체크리스트 항목 구현 방법론에 관한 연구

(A Study on the Implementation Methodology of Zero Trust Checklist Items)

박정수*
(Jungsoo Park)

요 약

사이버 위협이 점점 더 지능화되고 다양화됨에 따라 기존의 경계 기반 보안 모델은 본질적인 한계를 드러내고 있다. 이에 따라 '절대 신뢰하지 말고 항상 검증하라'는 원칙에 기반한 제로트러스트(Zero Trust) 보안 모델이 새로운 패러다임으로 부상하고 있으며, 이를 지원하기 위해 다양한 국제 표준 문서 및 학술 연구가 정책, 보안 통제, 성숙도 모델, 평가 기준 등 여러 요소를 제시하고 있다. 그러나 실제 조직에 도입하기 위해서는 이들 자료를 종합적으로 분석하고 기술적으로 통합한 구현 기준이 필수적이다. 특히 국내의 제로트러스트 가이드라인은 많은 항목을 제시하고 있음에도 불구하고, 기술 구현과 평가의 실효성 측면에서 미국의 주요 표준들에 비해 깊이와 폭이 부족한 한계를 가진다. 본 논문은 기존의 주요 제로트러스트 관련 문서들을 구조, 목적, 적용 방식, 기술 요건 측면에서 비교 분석하고, 이를 바탕으로 실질적 구현 가능성을 중심으로 구성된 일관된 기술 기반의 도입 평가 체크리스트를 구성하기 위한 방안을 제안한다. 제안된 체크리스트 구성 방법론을 통하여 체크리스트를 구성한다면, 향후 조직의 제로트러스트 체계 도입 및 보안 진단 시 구체적이고 실용적인 기준을 구성할 수 있을 것으로 기대한다.

■ 중심어 : 제로트러스트 ; 성숙도 ; 평가 방법론

Abstract

As cyber threats become increasingly sophisticated and diverse, the traditional perimeter-based security model has revealed its inherent limitations. In response, the Zero Trust security model—based on the principle of "never trust, always verify"—has emerged as a new paradigm, with various international standards and academic studies presenting elements such as policies, security controls, maturity models, and evaluation criteria. However, for practical organizational adoption, it is essential to comprehensively analyze these materials and establish technically integrated implementation criteria. In particular, although domestic Zero Trust guidelines present numerous items, they lack the depth and breadth of major U.S. standards in terms of technical implementation and evaluation effectiveness. This paper comparatively analyzes major Zero Trust-related documents in terms of structure, objectives, application methods, and technical requirements, and proposes an approach for constructing a consistent, technology-based adoption evaluation checklist centered on practical implementation feasibility. Through the proposed checklist construction methodology, it is expected that organizations will be able to establish concrete and practical standards for Zero Trust adoption and security assessment in the future.

■ keywords : Zero Trust ; Maturity ; Assessment Methodology

Ⅰ. 서 론

기존의 경계 기반 보안 모델은 사이버 위협의 지능화 및 확산에 따라 방어에 한계를 드러내고 있다. 이러한 문제를 극복하기 위한 대안으로, 모

* 정회원, 강남대학교 컴퓨터공학부

접수일자 : 2025년 10월 24일
수정일자 : 2025년 11월 19일
게재확정일 : 2025년 11월 20일
교신저자 : 박정수 e-mail: jspark@kangnam.ac.kr

든 접근 시 지속적인 검증을 요구하는 제로트러스트(Zero Trust) 모델이 새로운 보안 패러다임으로 주목받고 있으며, 이를 기반으로 한 다양한 연구가 활발히 진행되고 있다[1].

이와 관련하여, 다양한 국제 표준 문서 및 학술 논문들이 제로트러스트 구현을 위한 정책, 보안 통제, 성숙도 모델, 평가 기준 등 여러 구성 요소를 제시하고 있으며, 각 문서는 상호 보완적인 특성을 가진다. 그러나 실제 조직 내 도입을 위해서는 이들 표준 문서를 종합적으로 분석하고 기술적으로 통합한 구현 기준이 필요하다. 현재까지는 이러한 기술 기반의 통합 체크리스트가 충분히 마련되어 있지 않으며, 국내 제로트러스트 가이드라인 2.0[2] 역시 약 200여 개의 체크 항목을 제시하고 있으나, 기술적 구현과 평가 기준 측면에서 미국의 주요 표준들과 비교할 때 깊이나 폭 모두에서 부족한 점이 존재한다. 또한, 기존 문서들은 각기 다른 목적(RMF는 절차, 800-53은 통제 목록, CISA Maturity Model은 성숙도)을 가지고 있어, 이를 ZT 아키텍처 구현이라는 단일한 목적으로 통합하고 일관된 기술 평가 기준으로 재구성하는 작업이 부재한 실정이다.

이에 본 논문은 기존 제로트러스트 관련 문서들의 구조, 목적, 적용 방식 및 기술 요건을 분석하여, 일관된 기술 기반의 도입 평가 체크리스트를 제안하고자 한다. 제안된 체크리스트는 표준 문서를 기반으로 한 실질적인 구현 가능성을 중심으로 구성되며, 향후 제로트러스트 체계 도입 및 진단에 활용될 수 있다.

논문의 구성은 다음과 같다. 제2장에서는 제로트러스트 관련 연구 동향과 기존 문헌에서의 성숙도 모델 및 보안 평가 기법을 살펴본다. 제3장에서는 체크리스트의 구성 방안을 설명하고 이를 활용한 도입 평가 방식을 제안한다. 마지막으로 제4장에서 본 연구의 결론을 제시한다.

Ⅱ. 본 론

Ⅰ. 관련연구

표 1. ZT 성숙도 평가 관련 연구

논문 제목	구현 방식
Zero Trust Cybersecurity: Critical Success Factors and a Maturity Assessment Framework[3]	8개 핵심 성공 요인을 기반으로 성숙도 평가 프레임워크 개발
Zero Trust Maturity Matters: Modeling Cyber Security Focus Areas[4]	기존 사이버 보안 성숙도 모델을 통합하여 제로트러스트 성숙도 모델(ZTMM) 개발
Designing Extended Zero Trust Maturity Model – From Technical to Socio-Technical[5]	기술적 요소뿐만 아니라 사회기술적 요소를 포함한 확장된 제로트러스트 성숙도 모델 제안
Assessing the Impact of Zero Trust on Cybersecurity Maturity[6]	제로트러스트 구현이 사이버 보안 성숙도에 미치는 영향 분석
Maturity Model for Corporate Sector Based on Zero Trust Adoption[7]	제로트러스트 구현 수준을 평가하고 보안 태세를 개선하기 위한 프레임워크 개발

표 1에서 확인할 수 있듯이, ‘성숙도’를 제목에 포함한 제로트러스트 관련 논문들은 주로 프레임워크 설계나 성숙도 수준의 평가에 초점을 두고 있다. 이들 연구는 대부분 이론적 모델 제시에 머무르고 있으며, 제로트러스트를 구성하는 기술적 요소에 대한 구체적인 분석은 부족한 실정이다. 또한, 실험적 접근이나 실제 적용 사례보다는 정성적 평가와 구조화된 분류 체계에 중점을 두고 있어, 기술적인 관점에서 분석하려 할 경우 유사한 논평 구조에 그치는 한계를 보인다. 기존 성숙도 연구들은 대부분 관리적이거나 정성적 수준 평가에 그치는 한계가 있다. 반면, 본 논문에서 제안하는 방법론은 NIST SP 800-53, 1800-35 등의 구체적인 기술 통제 항목을 직접 매핑함으로써, 실행 가능한 기술 중심의 체크리스트를 도출하는 데 차별점이 있다.

[3]번 논문의 경우, 델파이 기법으로 12명의 보안전문가를 대상으로 제로트러스트 구현에 대하

여 8개 Pillar별 내용을 파악하고, 이를 성숙도로 표시할 수 있는 프레임워크를 제시하였다. 하지만 너무 작은 체크리스트 항목으로 제대로 된 판단을 하기 어렵다는 단점을 가지고 있다. [4]번 논문의 경우, 기술적 통제 항목 뿐 아니라 조직, 절차, 인식 등 다양한 요소를 포함하여 제로트러스트 성숙도 모델을 제안하였다. 현재의 조직의 위치를 파악하고 향후 개선점을 확인할 수 있게 하였으나, 기술적 세부 사항이 매우 약하여, 이를 실무에서 바로 적용하기 어렵다는 단점이 있다. [5]번 논문의 경우, 현재 연구와 실무의 차이점을 나타내어 설명하는 것은 기존의 논문들과 차이를 보이고 있다. 하지만 우선 순위에 대한 내용 및 주관성 판단 기준을 사용하고 있다는 점에서 제대로 체크리스트를 구성하기 어렵다는 단점을 가지고 있다. [6]번 논문의 경우, 기존의 CISA의 성숙도 모델과 유사하게 네단계의 티어를 바탕으로 제로트러스트 성숙도를 판단할 수 있게 하였을 뿐 아니라, 원격 근무, 클라우드 호환 환경 등의 특징 별 체크리스트 구현 방법을 잘 나타내었다. 하지만 정량적 지표의 가중치 및 세부 설계가 불확실하고 저자의 판단에 의하여 작성된 측면이 있다. 마지막으로 [7]번 논문의 경우, 기업 환경에 특화된 대상을 모델로 기업 조직의 현실에 반영하기 좋을 수 있는 자가 진단 기능을 포함한 내용을 반영하였다. 또한, 모델에 대한 로드맵을 바탕으로 더 높은 단계의 성숙도 달성을 위한 개선 사항을 도출할 수 있도록 하였다. 하지만, 기술 성능 수준에 대한 구체적 수치가 부족하다는 단점이 있다.

표 2. 체크리스트 구성을 위한 문서 및 추출 요소

목적	참고 문서	추출 요소	선정 사유
기술 구성 요소 정의	NIST 800-207, SP 1800-35[8]	구성요소 구조, 기술 시나리오	ZT의 아키텍처와 실제 기술 스택을 정의하여 체크리스트의 기술적 기반 제공
통제 기반 항목 도출	NIST 800-53[9], DoD ZT Overlay[10]	Control 목록, 기술 통제 기능	구현 가능한 체크리스트 항목을 도출하기 위한 가장 포괄적이고 검증된 기술 통제 목록 제공
단계별 성숙도 기준	CISA Maturity Model[11], NSA Maturity[12]	성숙도별 구현 기준 및 기능	체크리스트가 단순 Y/N 평가가 아닌, 수준별(평가를 가능하게 하는 기준 제공
조직별 책임·절차 기준	RMF[13], ISMS-P	적용 주체, 실행 절차, 제도 기반 기준	ZT 구현을 기술뿐 아니라 관리적/절차적 측면에서 평가하고, 국내 인증(ISMS-P)과의 연계성을 확보
국내 실무 반영	KISA ZT 가이드라인	체크리스트 표현 방식, 국내 적용 예시	글로벌 표준을 국내 환경과 용어에 맞게 적용하고, 실무에서 바로 활용 가능한 예시 참고

결국, 대부분의 논문에서 사용된 방법론 역시 대부분 유사한 경향을 나타낸다. 델파이(Delphi) 기법, 인터뷰 기반 분석, 구조화된 설문조사 등을 통해 성숙도 수준을 구분하고 있으며, 이러한 접근은 정책 및 관리 중심의 평가에 집중되어 있다. 실제 제로트러스트 시스템의 구현 기술을 다룬 연구는 상대적으로 드물며, 이는 실질적인 도입을 위한 기술 기반 체크리스트 개발의 필요성을 시사한다. 따라서, 이와 관련된 체크리스트를 구현하기 위한 방안을 3장에서 소개하고자 한다.

Ⅲ. 제로트러스트 체크리스트 구성 방법론

3.1 체크리스트 구성 요소

표 2는 국내외 주요 문서들이 제로트러스트 체

크리스트 항목 구성 시 어떤 기준으로 활용될 수 있는지를 보여준다. 이들 문서를 기반으로 종합적이고 기술적인 체크리스트를 구성하기 위해 다음과 같은 접근이 필요하다.

우선, RMF(Risk Management Framework)를 기반으로 제로트러스트 위험 관리 체계에 대한 분석이 선행되어야 한다. RMF의 6단계를 중심으로 체크리스트의 주요 항목을 설계하고, 이를 기반으로 CISA(미국 사이버안보 및 기반시설 보안국)의 제로트러스트 성숙도 모델을 활용하여 단계별 체크리스트를 구축할 수 있다. 이 과정에서 CISA 외에도 NSA(미국 국가안보국)의 제로트러스트 성숙도 모델을 함께 고려하여 성숙도 기반의 다층적인 항목 구성이 가능하도록 해야 한다.

표 3. 체크리스트 구성 시 문서에서 추출할 핵심 요소

문서	체크리스트 구성 시 추출해야 할 핵심 요소	설명
NIST SP 800-53 Rev.5	• 통제 항목 (AC, SC, AU, IA 등 Control Families) • 기술 통제 세부 항목의 기능 정의 • 통제 목적 및 구현 설명 • 선택 통제 옵션들	기능별 보안 요구사항의 체크리스트 항목화, 기술 기능별 매핑
NIST RMF (Risk Management Framework)	• 보안 통제 선정·적용 절차 • 조직 내 리스크 기반 보안 통제 설계 원칙 • 통제 실행 시 역할 및 책임자 정의	체크리스트 적용 대상 분류(관리자/사용자/시스템) 및 절차 기반 도출
NIST SP 1800-35	• ZTA 기술 구성도 및 제품 연계 시나리오 • 상용 솔루션 기반 구성 예시 • 정책 설정 예 및 구현 흐름	실제 체크리스트 항목이 구현될 수 있는 기술 스택/사례 제공
CISA Zero Trust Maturity Model v2.0	• 5대 영역 + 3개 교차 기능별 성숙도 • 각 영역별 기대 기능 및 단계별 구현 수준 • 구현된 기능의 평가 기준	체크리스트 항목별 성숙도 레벨 설정 기준 제공
NSA Zero Trust Maturity Model	• ZT 7대 Pillar 기준 요구사항 • 각 Pillar별 보안 조치 • 연속적 모니터링, 최소 권한, 동적 정책 등 전략 원칙 • 단계별 성숙도 적용 수준 및 기대 기능 설명	보안 영역 전반에 걸친 기술 요구사항과 적용 수준을 바탕으로 성숙도 레벨별 체크리스트 구성 가능
DoD Zero Trust Overlay	• NIST SP 800-53 통제를 ZT 관점으로 재분류 • 기술 통제에 대한 필수/선택 구분 • DoD 적용 우선순위에 따른 필터링 기준	체크리스트 항목 필수/권장 여부 표시 및 적용 우선순위 설정 기반
ISMS-P 인증 기준 (국내)	• 인증기준 내 접근통제, 사용자 권한관리, 로그관리 등 관리적/기술적 통제 항목 • 제도 기반 실무 적용 가능 항목 • 개인정보보호법 연계 항목	국내 기업·기관에서 적용 가능한 제도적 체크리스트 구성 가능
제로트러스트 가이드라인 2.0 (KISA)	• 약 200여 개 항목 기반 사전 점검 요소 • ZT 7대 구성요소별 기술 목록 • 국내 기관 맞춤형 예시 항목	국내 현실에 기반한 체크리스트 예시 및 표현 방식 참고 자료 제공

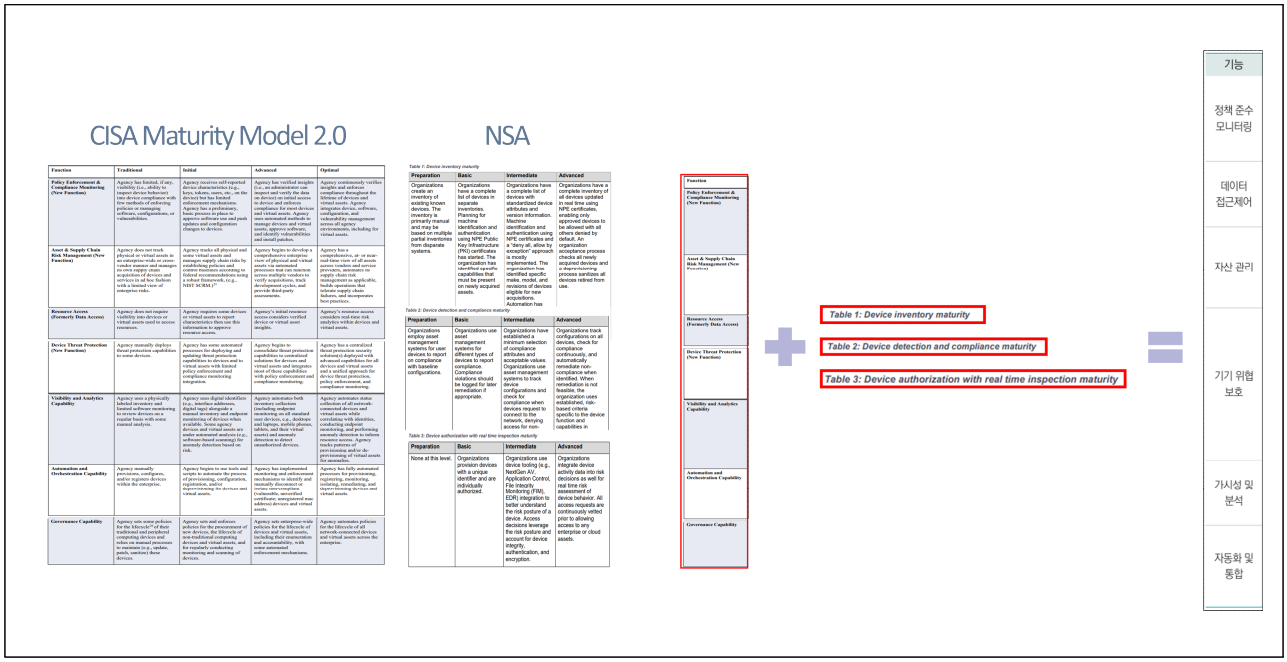
이러한 기반 분석을 토대로 체크리스트의 중분류 항목을 정의하고, 그 하위에 기술적 관점의 세부 항목을 체계적으로 구현할 필요가 있다. 특히, 보안 통제 기반 항목 설계를 위해 NIST SP 800-53의 보안 통제를 제로트러스트 모델에 맞

게 조정하고 적용해야 하며, 이때 국내 관련 법령 및 정책 기준과의 연계도 함께 고려되어야 한다.

또한, 실제 사례 기반의 전략 분석 및 기술 적용을 위해서는 NIST SP 1800-35에서 제시된 기술적 세부 사항을 국내 환경과 실무에 적합하도록 수정·보완하여 활용해야 한다. 더불어, 미 국방부(DoD)의 ZT Overlay를 적용하여 해당 모델

역량을 설정하였다. [그림 2]에서 DoD ZT Capability를 토대로 기능에 매칭되는 항목을 도출하여, 이러한 방법론을 토대로 과학기술정보통신부의 제로트러스트 2.0 가이드라인의 세부 역량을 매핑하였으며, 이후 성숙도 수준에 따르는 정의를 하기 위하여 NIST 800-53, 1800-35의 문서 및 DoD Capability를 참고하여 성숙도 수준에 따르는 정의를 설정하였다.

그림 1. 주요 기능 추출 (CISA Zero Trust Maturity Model v2.0 및 NSA Zero Trust Maturity Model을 기반으로 저자 재구성)



로부터 도출된 핵심 보안 통제 및 요구사항을 명확히 분석하고, 이를 체크리스트 항목에 반영함으로써 실효성을 높일 수 있다.

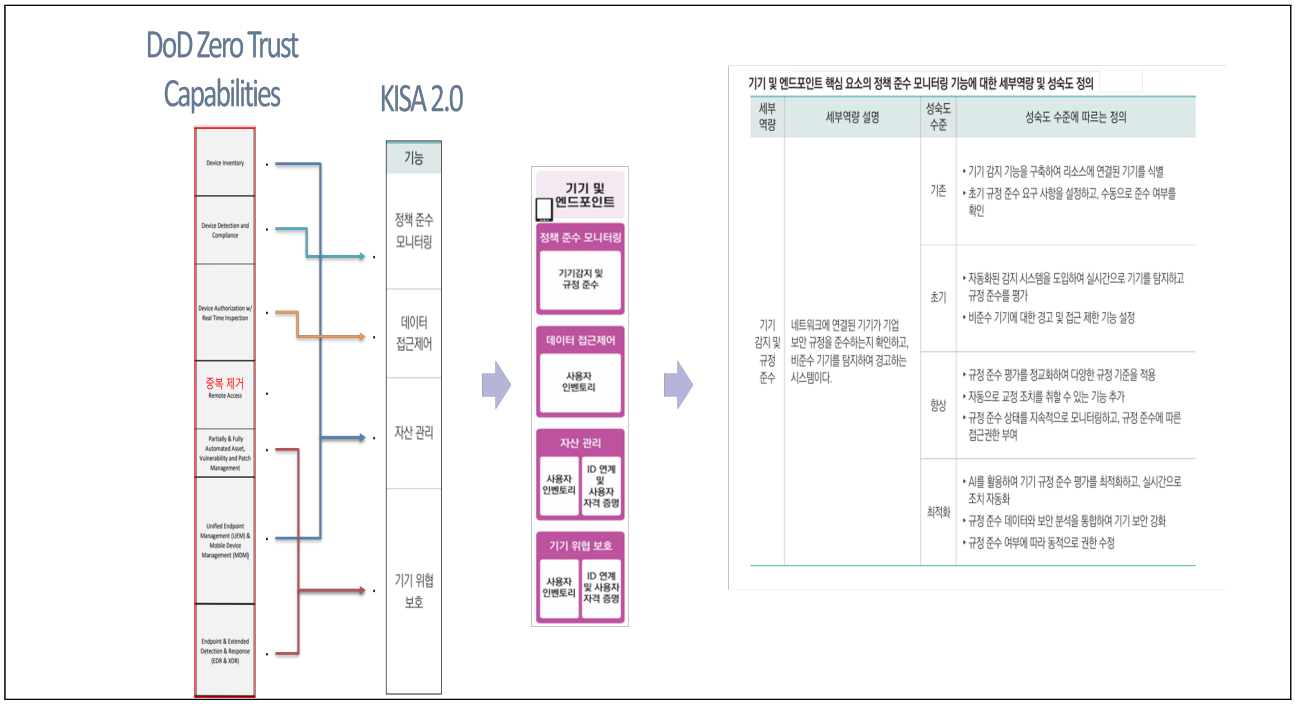
마지막으로, 표 3에서는 각 문서에서 추출한 핵심 요소들을 기반으로 실제 체크리스트에 반영되어야 할 내용을 정리하여 설명하였다.

실제로, 관련된 내용을 참조하기 위하여 다음과 같은 방법을 고려하였다. 우선, 성숙도를 만들기 위하여 주요 기능을 추렸다. [그림 1]과 같이 CISA의 성숙도 모델과, NSA의 성숙도 모델을 토대로 Pillar별 주요 기능을 추출하였다. [그림 1]에서 빨간색으로 표현한 부분이 CISA의 주요 기능(function)과 NSA의 기능(table)을 결합하여 새로운 기능으로 작성을 한 부분으로, 이후 DoD의 문서를 참고하여 [그림 2]와 같이 세부

3.2 체크리스트 구성 방법론 절차

첫 번째로, 참조 문서 선정 및 분석을 수행하였다. 미국의 문서 및 국내 제로트러스트 가이드라인 2.0 등을 기준 문서로 선정하고, 각 문서의 목적, 구조, 보안 통제 항목, 성숙도 구성 방식 등을 비교 분석하였다. 이후, 핵심 영역 도출 및 계층 구조 정의하였다. 분석된 문서들로부터 공통된 핵심 구성요소(예: 자산 관리, 사용자 인증, 네트워크 세분화, 데이터 보호 등)를 도출하고, 이를 기반으로 상위 영역, 중분류 항목, 세부 항목으로 구성된 계층형 구조를 설계하였다. 세 번째로, 보안 통제 매핑 및 기술 요소를 정의하였다. 도출된 항목별로 NIST SP 800-53의 보안 통제 항목을 매핑하고, 각 항목에 요구되는 기술 구성 요소(예: MFA, EDR, Micro-Segmentation 등)를

그림 2. 세부 역량 추출([그림 1]에서 도출된 주요 기능과 DoD ZT Capabilities를 기반으로 저자 재구성)



명확히 식별하여 기술 구현 관점의 기준을 설정하였다. 네 번째로, 성숙도 기반 단계를 정의하였다. CISA와 NSA의 성숙도 모델을 기반으로 각 항목의 구현 수준을 4단계로 정의하고, 초기 상태부터 최적화된 상태까지의 기술적·관리적 성숙도 기준을 정량 및 정성 지표로 구분하여 제시하였다. 이후, 법제도 및 환경 적합성 반영을 위하여 국내 정보보호 법제도, 산업 환경, 조직 특성을 반영하여 일부 항목을 조정하거나 보완하고, 국내 적용 시 유효한 참조 기준으로 활용될 수 있도록 수정하였다. 이러한 구성을 위하여 아래와 같은 방법을 활용하였다.

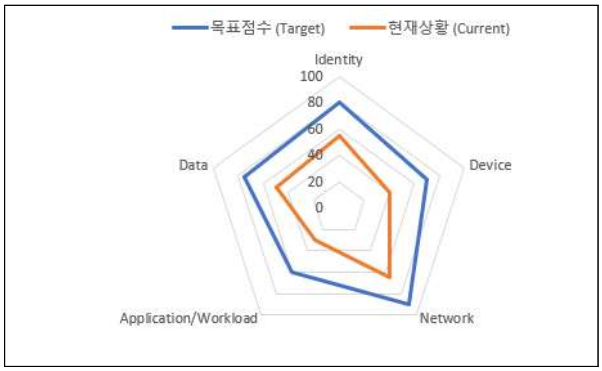
먼저, 핵심 문서 분석 및 요소 식별을 수행하였다. [표 2]와 [표 3]에서 제시한 문서들(NIST 800-53, RMF 등)을 분석하여, Pillar별로 적용할 수 있는 핵심 통제 항목, 절차, 기술 요건을 식별하였다. 이후, ZT 관점 매핑 및 항목을 추출하였다. 식별된 항목을 정의된 Pillar에 매핑하였다." 예를 들어, NIST SP 800-53의 'AC-4 (정보 흐름 통제)'는 시스템 간의 정보 흐름을 명시적으로 승인하고 제어할 것을 요구한다. 이는 제로트러스트의 '모든 트래픽은 신뢰할 수 없다'는 기본 원칙 하에, 워크로드 간의 통신을 세분화하여 제어하는 마이크로 세분화(Microsegmentation)의 핵심 기술 원리와 직접적으로 연결된다. 따라서 이를 ZT의 세부 체크리스트 항목으로 구체화하였다. 이후, 체크리스트 항목을 정제하였다. 추출된 항목을 실제 평가에 사용할 수 있는 명확한 질문 또는 요구사항 형태로 다듬는 작업을 수행하였다. 마지막으로, 성숙도 수준을 적용하였다. CISA/NSA 성숙도 모델을 참조하여, 정제된 항목별로 네단계의 수준을 판단할 기준을 제시하였다.

최초 체크리스트 구성의 경우 [표 4]와 같이, 참조 문서 및 체크리스트 매핑을 통하여 구성하였다. 이후, 이러한 기능을 성숙도 단계에 맞추어 보다 고도화하여 체크리스트를 작성하였다.

이러한 체크리스트는 조직의 제로트러스트 구현 수준을 기술적으로 평가하기 위한 기준으로 활용된다. 평가 방법론은 다음과 같이 구성된다. 첫 번째는 사전 환경 파악 및 자산 범위 정의이다. 평가 대상 조직의 정보 자산, 사용자 유형, 네트워크 구조, 주요 애플리케이션

등을 조사하고, 체크리스트 적용 범위를 명확히 정의하여야 한다. 두 번째는 항목별 기술 구현 여부 평가이다. 각 세부 항목에 대해 구현 여부를 '미구현', '부분 구현', '완전 구현' 등으로 평가하고, 이를 항목별 성숙도 기준과 비교하여 현재 상태를 진단하여야 한다. 세 번째는 성숙도 단계별 점수화 및 시각화이다. 각 항목의 평가 결과를 기반으로 영역별 성숙도 점수를 산출하고, 전체 성숙도 수준을 레이더 차트, 누적 히트맵 등의 시각적 방법으로 표현하여 도입 수준을 직관적으로 파악할 수 있도록 하여야 한다. 이러한 기술에는 Yeoh, William, et al[14]와 같이 델파이 기법을 활용하고 이후, 전문가들이 실제 분석을 통하여 현재 상황을 파악하는 등의 방법이 있다. 이러한 방법의 경우, 각 pillar별로 점수를 측정하게 되는데 세부 역량의 성숙도 수준에 따라 1점에서 5점으로 적용하는 방식이 많이 사용되고 있으며, 총점의 합산으로, 20~ 39점: 준비 단계, 40~59점: 도입 단계, 60~79점: 확산 단계, 80~99점: 성숙 단계, 100점: 최적화 단계 등으로 구분 할 수 있으며, 각 점수 영역을 아래 [그림 3]과 같이 표현할 수 있다.

그림 3. 성숙도 모델 측정 시각화



네 번째는 기술 격차 분석 및 개선 권고 도출이다. 평가 결과를 기반으로 각 항목의 기술적 격차를 분석하고, 구현이 미흡하거나 누락된 항목에 대해 구체적인 개선 방향 및 우선순위 기반의 권고안을 제시하여야 한다. 마지막으로, 정기적 재평가 및 성숙도 추적이 필요하다. 체크리스트 기반 평가를 정기적으로 수행함으로써 도입 수준의 변화와 성숙도 향상 여부를 추적할 수 있으며, 조직의 보안 전략 수립 및 예산 계획에도 활용 가능하다. 이러한 평가 방법의 경우, 기관의 환경과 상황에 따라 달성하고자 하는 목표가 달라질 수 있기 때문에 이를 각 기관의 담당자가 평가하고 측정해야 할 것이다.

표 4. ZT 핵심 요소별 참조 문서 매핑 및 체크리스트 도출 예시

ZT 핵심 영역	세부 구현 목표	참조 문서	참조 문서의 핵심 내용	도출된 체크리스트 항목(안)
Identity	다중 인증(MFA) 강화	NIST SP 800-53	IA-2 (1): Identification and Authentication (Organizational Users)	(질문) 사용자에게 상황별로 다른 MFA를 적용하여 질의가 가능한가?
Identity	역할 기반 접근 통제(RBAC)	NIST RMF	Step 2: Select Controls (AC-3 Access Enforcement)	(질문) 사용자 역할에 따라 명확히 정의된 최소 권한 원칙이 적용되고 있는가?
Network	마이크로 세분화 (Micro-segmentation)	NIST SP 1800-35	Section 4.2.3: Micro-Segmentation (using policies to isolate workloads)	(질문) 워크로드 및 애플리케이션 간의 통신은 기본 거부(Default Deny) 정책을 기반으로 격리되어 있는가?
Network	동적 정책 적용	DoD ZT Overlay	PE-3 (Physical and Environmental Protection): ZT 관점 재분류 (동적 접근 제어)	(질문) 사용자의 위치, 기기 상태, 시간 등 컨텍스트 변화에 따라 접근 정책이 동적으로 변경되는가?

Ⅳ. 결 론

본 논문에서는 제로트러스트 보안 모델의 도입을 효과적으로 진단하고 평가하기 위한 기술 기반의 체크리스트 구성 방안과 도입 평가 방법론을 제안하였다. 기존 표준 문서와 성숙도 모델을 기반으로 항목을 설계하고, 실제 적용 가능성과 기술 구현을 중심으로 체크리스트 구성 방법론을 소개하였다.

제안된 제로트러스트 체크리스트 구현 방법론은 국내 기관 및 기업의 제로트러스트 도입 수준을 진단하기 위한 성숙도 평가 도구를 만들기 위한 방안으로 활용될 수 있으며, 정보보호 정책 수립 시 국제 표준에 기반한 기술 점검 항목에도 활용이 가능하다. 또한, 금융, 공공, 의료 등 산업별 특성을 고려한 맞춤형 보안 점검 템플릿 개발의 기준 자료로 활용될 수 있으며, 보안 컨설팅 기업의 현장 적용을 위하여 체크리스트 구현 시 고려해야 할 사항일 것이다.

더 나아가, 본 체크리스트 구현 방법론은 국내 제로트러스트 가이드라인의 개정 및 실효성 제고를 위한 기술적 근거 자료가 될 수 있다. 이러한 체크리스트의 실질적 활용을 위해서는 보안 점검 항목 내에 제로트러스트 항목을 신설하고, 평가 체계에 이를 적극 반영할 필요가 있다.

향후 연구에서는 실제 산업 분야별 적용 사례를 통해 체크리스트를 실제로 구현하여, 체크리스트의 실효성과 적용 가능성을 검증하고, 자동화된 진단 도구 등을 구현하여 운영 편의성과 확장성을 높이는 방안에 대해 연구할 예정이다.

ACKNOWLEDGEMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학ICT연구센터(ITRC)의 지원을 받아 수행된 연구임(IITP-2025-RS-2020-II201602)

REFERENCES

[1] National Institute of Standards and Technology (NIST), Special Publication 800-207: Zero Trust Architecture, 2020.
[2] 한국인터넷진흥원(KISA), 제로트러스트 가이드라인 2.0, 2024년
[3] Yeoh, W., Liu, M., Shore, M., & Jiang, F., "Zero Trust Cybersecurity: Critical Success Factors and a Maturity Assessment Framework", *Computers & Security,* Vol. 133, 2023.
[4] Modderkolk, M.G., Zero Trust Maturity Matters: Modeling Cyber Security Focus Areas, MSc Thesis, Utrecht University, 2018.
[5] Tokerud, S., Jansen, J.N., Niemimaa, M., & Järveläinen, J., "Designing Extended Zero Trust Maturity Model - From Technical to Socio-Technical", *Proceedings of the International Conference on Information Systems (ICIS),* 2023.
[6] Aiello, S.T., Assessing the Impact of Zero Trust on Cybersecurity Maturity, Master's Thesis, Dakota State University, 2023.
[7] Ilyas, Muhammad, Mustafa Akal, and Qutaibah Althebyan. "Maturity Model for Corporate Sector Based on Zero Trust Adoption." *2024 International Conference on Engineering and Emerging Technologies (ICEET). IEEE,* 2024.
[8] National Institute of Standards and Technology (NIST), SP 1800-35: Implementing a Zero Trust Architecture, NCCoE, 2023.
[9] National Institute of Standards and Technology (NIST), Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5), 2020.
[10] U.S. Department of Defense (DoD), Zero Trust Reference Architecture & Overlay, Version 2.0, 2023.
[11] Cybersecurity and Infrastructure Security Agency (CISA), Zero Trust Maturity Model Version 2.0, Apr. 2023.
[12] National Security Agency (NSA), Applying Zero Trust Principles to Enterprise Environments, 2021.
[13] National Institute of Standards and Technology (NIST), Risk Management Framework for Information Systems and Organizations (SP 800-37 Rev. 2), 2018.
[14] Yeoh, William, et al. "Zero trust cybersecurity: Critical success factors and A maturity assessment framework." *Computers & Security,* vol. 133, no. 10, Jul. 2023.

저 자 소 개

박정수 (정회원)

2013년 숭실대학교 정보통신전자공학부 학사 졸업
2015년 숭실대학교 전자공학과 석사 졸업
2021년 숭실대학교 융합소프트웨어학과 박사 졸업
2024년~현재 강남대학교 컴퓨터공학부 조교수

<주관심분야 : 제로트러스트, N2SF, 컨테이너 보안>