정 보 보 호 학 회 지
제34권 제3호, 2024. 6

업무 중요도를 고려한 제로 트러스트 성숙도 평가 방법
(식별자·신원, 기기 및 엔드포인트, 시스템 핵심 요소 중심으로)

박 재 혁*, 이 현 진**, 이 기 욱***, 최 영 철****

요 약

제로 트러스트 패러다임은 비교적 널리 알려졌지만, 기관과 기업이 제로 트러스트 전환을 위한 정책 수립과 구축 계획을 마련하는 데는 많은 어려움이 있는 상태이다. 본 연구는 이러한 문제를 해결하기 위해, 기관과 기업의 대상 서비스 또는 시스템의 제로 트러스트 전환 계획 수립에 기반이 될 수 있는 제로 트러스트 성숙도 평가 방법론을 제시한다. 또한, 업무 중요도를 고려한 제로 트러스트 보안 요구사항 수립과 관련된 핵심 요소별 성숙도 기능에 대해서도 논하고자 한다. 본 연구를 통해 기관과 기업이 효과적인 제로 트러스트 보안 체계와 보안 인프라 구축 및 운영 계획을 수립하는 데 도움이 되는 정보를 제공하고자 한다.

Ⅰ. 서 론

2020년, 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 특별 간행물(Special Publication, SP) 800-207 ‘Zero Trust Architecture’를 발간하여 제로 트러스트의 개념, 구현 전략, 아키텍처 등을 체계적으로 수립하고 제로 트러스트의 선도적인 기준을 제시했다. 미국 백악관은 정책적으로 2021년 사이버 보안 행정 명령 EO 14028을 통해 제로 트러스트를 강조하고, 2024년 말까지 모든 연방 기관이 제로 트러스트 전략을 수립하도록 지시했다. 미국 국방부(Department of Defense, DoD) 역시 제로 트러스트 전략, 레퍼런스 아키텍처, 장기 로드맵을 제시하며 구체적인 방향을 제시했다.

국내에서는 디지털 플랫폼 정부 정책 기조에 맞춰 신(新)보안 체계 도입의 핵심 요소로 제로 트러스트 추진 전략이 발표되었다. 특히, 2023년 4월 공개된 ‘디지털플랫폼정부 실현 계획’은 2025년까지 제로 트러스트를 적용하겠다는 구체적인 목표를 제시했다. 이후 2023년 7월에는 국내 제로 트러스트의 기준이 되는 ‘제로 트러스트 가이드라인 1.0’이 발간되었다.

제로 트러스트를 달성하기 위한 평가 지표인 제로 트러스트 성숙도 모델은 미국 사이버 보안 인프라 안보국(Cybersecurity and Infrastructure Security Agency, CISA)에서 제시한 제로 트러스트 성숙도 모델 V1.0/V2.0과 국내 과학기술정보통신부의 제로 트러스트 가이드라인 1.0에서 제시된 모델이 있다. 또한, Microsoft, Forrester 등 기업에서도 제로 트러스트 성숙도 기준 모델을 제시하며, 제로 트러스트 평가를 위한 다양한 기준을 제시하고 있다. 다만 제로 트러스트 성숙도를 평가하기 위한 컴플라이언스나 기준이 명확하지 않아, 기관과 기업의 대상 서비스 또는 시스템을 대상으로 한 정량적, 정성적인 지표가 부족하여 제로 트러스트 도입 효과를 도출하기에 어려움이 많다.

이에 본지에서는 CISA 제로 트러스트 성숙도 모델과 국내 제로 트러스트 가이드라인 1.0의 제로 트러스트 성숙도 모델을 기준으로 한 업무 중요도별 제로 트러스트 성숙도 평가 방법론에 대해 제안하고자 한다.

Ⅱ. 제로 트러스트 성숙도 모델

2.1. 개요

제로 트러스트 성숙도 모델은 기관과 기업의 제로

* 에스지에이솔루션즈㈜ R&D센터 (차장, jaehpark@sgacorp.kr)
** 에스지에이솔루션즈㈜ R&D센터 (대리, hyunjinlee@sgacorp.kr)
*** 에스지에이솔루션즈㈜ (R&D총괄, kulee@sgacorp.kr)
**** 에스지에이솔루션즈㈜ (대표이사, ycchoi@sgacorp.kr)

트러스트 달성 수준을 가늠하고, 제로 트러스트 전환 및 확대를 위한 제로 트러스트 요구사항의 기준을 제시한다. 현재까지 알려진 제로 트러스트 성숙도 모델은 CISA 제로 트러스트 성숙도 모델, 국내 과학기술정보통신부 제로 트러스트 가이드라인 1.0 제로 트러스트 성숙도 모델이 국가별로 대표적인 제로 트러스트 성숙도 모델이다.

CISA 제로 트러스트 성숙도 모델(V2.0 기준)은 5가지 기둥(Pillar) 및 3가지 교차기능(Cross-Cutting Capabilities)으로 구분하고, 4단계 성숙도를 제시하고 있다.

국내 제로 트러스트 가이드라인 1.0 성숙도 모델은 6가지 기업망 핵심 요소별로 3단계 성숙도를 제시하고 있다.

대부분의 제로 트러스트 성숙도 모델은 기존의 정보보호 체계를 근간으로 하고 있으며, 성숙도 모델별 핵심 요소를 동일(또는 유사)하게 구성하고 있다. 제로 트러스트 성숙도 모델에서 주로 언급되는 핵심 요소는 '계정(Identity)', '장치(Device)', '네트워크(Networks)', '응용 및 워크로드(Application and Workload)', '데이터(Data)'이며, 특수성이 있는 핵심 요소는 '시스템(System)'과 '인프라(Infrastructure)'이다.

〔표 1〕 기관(기업)별 제로 트러스트 핵심 요소 정의

기관(기업)명	핵심 요소(또는 Pillar)
미국 사이버 보안 인프라 안보국	5가지 핵심 요소(Identity, Device, Networks, Application & Workloads, Data)
	3가지 교차 기능(Visibility and Analytics, Automation and Orchestration, Governance)
한국 과학기술정보통신부	식별자·신원, 기기 및 엔드포인트, 네트워크, 시스템, 응용 및 워크로드, 데이터
Forrester	Data, Networks, People, Workloads, Devices, Visibility and Analytics, Automation and Orchestration
Microsoft	Identities, Devices, Applications, Data, Infrastructure, Networks
SAP	Identities, Data, Network, Applications, Infrastructure, Endpoints
DISA/NSA (DoD)	User, Device, Network/ Environment, Applications and Workload, Data, Visibility and Analytics, Automation and Orchestration

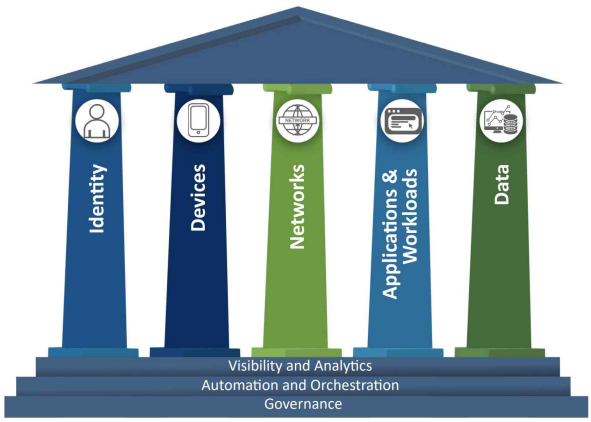
성숙도 모델 핵심 요소별로 전반적으로 고려되는 기능은 '가시성(Visibility)', '자동화(Automation)', '오케스트레이션(Orchestration)', '거버넌스(Governance)'이다. 이러한 기능 요소들은 성숙도 핵심 요소로 포함되기도 하며, 전반적인 제로 트러스트 고려사항으로 분리하기도 한다.

[표 1]은 국제적으로 다양한 기관과 기업에서 정의한 제로 트러스트 성숙도 핵심 요소이다.

2.2. 미국 CISA, 제로 트러스트 성숙도 모델

CISA 제로 트러스트 성숙도 모델 V2.0은 Identity, Device, Networks, Application & Workloads, Data 총 5가지 기둥과, Visibility and Analytics, Automation and Orchestration, Governance 총 3가지 교차 기능을 중심으로 한다. V2.0은 성숙도 단계를 V1.0 보다 세분화해 Traditional, Initial, Advanced, Optimal 등 총 4가지 단계로 구분한다.

제로 트러스트 아키텍처(Zero Trust Architecture, ZTA)로 전환하기 위해서는 ZTA 구현(본 모델에서 설명한 기둥과 기능 포함)에 투자하기 전, 반드시 NIST의 성숙도 단계에 맞춰 현재의 엔터프라이즈 시스템, 리소스, 인프라, 인력 및 프로세스를 평가해야 한다. 이러한 성숙도 단계와 각 기둥과 관련된 세부 정보를 통해 ZTA 구현 및 구축에 필요한 투자를 평가, 계획 및 유지할 수 있다. 각 기둥에는 해당 기둥과 모델 전



〔그림 1〕 CISA 제로 트러스트 성숙도 모델 V2.0 기둥 및 교차 기능 도식도

반에 걸쳐 통합을 지원하는 가시성 및 분석, 자동화 및 오케스트레이션, 거버넌스 기능에 대한 일반적인 세부 정보도 포함되어 있다. 물론 많은 기관은 이미 제로 트러스트 요구사항을 일부 충족하고 있을 수도 있다.

아래의 [그림 1]은 CISA 제로 트러스트 성숙도 모델 V2.0 기둥, 교차 기능 관련 도식도이다.

〔표 2〕 CISA 제로 트러스트 성숙도 모델 V2.0, 기둥 및 교차 기능

기둥	정의
Identity	개인이 아닌 엔티티를 포함하여 사용자 또는 엔티티를 고유하게 설명하는 속성 또는 속성 집합
Devices	서버, 데스크톱 및 랩톱 기계, 프린터, 휴대폰, IoT 장치, 네트워킹 장비 등을 포함하여 네트워크에 연결할 수 있는 모든 자산(하드웨어, 소프트웨어, 펌웨어 등 포함)
Networks	내부 네트워크, 무선 네트워크 및 인터넷과 같은 전형적인 채널과 메시지 전송에 사용되는 셀룰러 및 응용 프로그램 수준 채널과 같은 기타 잠재적인 채널을 포함하는 개방형 통신 매체
Data	연방 시스템, 장치, 네트워크, 애플리케이션, 데이터베이스, 인프라 및 백업에 존재하거나 존재하는 모든 정형 및 비정형 파일 또는 조각과 관련 메타데이터 포함
Application & Workloads	사내, 모바일 장치 및 클라우드 환경에서 실행하는 시스템, 컴퓨터 프로그램 및 서비스 포함
교차 기능	*정의*
Visibility and Analytics	사이버 관련 데이터 분석에 초점을 맞추면서 정책 결정을 알리고, 대응 활동을 용이하게 하며, 위험 프로파일을 구축하여 사고가 발생하기 전에 사전 예방적 보안 조치를 개발하는 데 도움이 될 수 있음
Automation and Orchestration	제로 트러스트는 제품 및 서비스 전반에 걸쳐 보안 대응 기능을 지원하는 자동화된 도구 및 워크플로우를 최대한 활용하는 동시에 이러한 기능, 제품 및 서비스에 대한 개발 프로세스의 감독, 보안 및 상호 작용 유지
Governance	제로 트러스트 원칙과 연방 요구사항의 충족을 지원하기 위해, 보안 위험을 완화하기 위한 사이버 보안 정책, 절차 및 프로세스를 기둥 내 및 기둥 간에 정의하고 관련 집행하는 것을 말함

〔표 3〕 CISA 제로 트러스트 성숙도 모델 V2.0, 제로 트러스트 성숙도 단계

성숙도 단계	정의
Traditional	수동으로 구성된 라이프사이클(즉, 구축에서 해체까지) 및 속성 할당(보안 및 로깅), 외부 시스템에 대한 개별 종속성으로 한 번에 하나의 기둥을 해결하는 정적 보안 정책 및 솔루션, 최소 권한 설정
Initial	외부 시스템의 통합을 통해 속성 할당 및 라이프사이클 구성, 정책 결정 및 시행, 초기 교차 기능 솔루션의 자동화 시작
Advanced	기둥 간 조정을 통해 라이프사이클 및 구성 및 정책 할당을 위한 자동화된 제어 기능, 중앙 집중식 가시성 및 신원 제어 기능, 각 축에 통합된 정책 집행 기능, 사전 정의된 완화 조치에 대한 대응 기능, 위험 및 자세 평가를 기반으로 한 최소 권한 변경 기능, 전사적 인식(외부 호스팅 된 리소스 포함)을 위한 구축 기능 등 제공
Optimal	자동화된/관찰된 트리거를 기반으로 동적 정책을 사용하여 자체 보고하는 자산 및 리소스에 대한 속성의 완전히 자동화된 적시 라이프사이클 및 할당, 자산 및 해당 종속성에 대한 전사적인 동적 최소 권한 접근(적정 수준 및 임계값 내), 지속적인 모니터링을 통한 교차 기둥 상호 운용성 및 포괄적인 상황 인식을 통한 중앙 집중식 가시성

아래의 [표 2]는 CISA 제로 트러스트 성숙도 모델 V2.0 기둥 및 교차 기능별 정의, [표 3]은 제로 트러스트 성숙도 단계별 정의이다.

2.3. 과학기술정보통신부 제로 트러스트 가이드라인 1.0, 제로 트러스트 성숙도 모델

제로 트러스트 가이드라인 1.0의 제로 트러스트 성숙도 모델은 식별자·신원, 기기 및 엔드포인트, 네트워크, 시스템, 응용 및 워크로드, 데이터 총 6가지 기업망 핵심 요소로 구성되고, 성숙도 단계는 기존, 향상, 최적 총 3단계로 구분된다. 이는 CISA에서 2021년에 공개한 CISA 제로 트러스트 성숙도 모델 V1.0과 유사한 성숙도 모델을 갖추고 있다.

가장 큰 차이점은 기업망 핵심 요소 중 '시스템'을 추가로 고려한 점이다. 'NIST SP 800-207, Zero Trust Architecture, Figure 1'을 살펴보면 엔터프라이즈 리

〔표 4〕 제로 트러스트 가이드라인 1.0, 성숙도 모델 기업망 핵심 요소

핵심 요소	정의
식별자·신원	사람, 서비스 혹은 IoT 기기 등을 고유하게 설명할 수 있는 속성 혹은 속성의 집합을 의미함
기기 및 엔드포인트	기기는 IoT 기기, 휴대폰, 노트북, PC, 서버 등을 포함하여 Network에 연결하여 데이터를 주고받는 모든 하드웨어 장치를 의미함
네트워크	네트워크는 기업망의 유무선 네트워크, 클라우드 접속을 포함하는 인터넷 등 데이터를 전송하기 위해 사용되는 모든 형태의 통신 매체를 포함
시스템	시스템은 중요 응용 프로그램을 구동하거나 중요 데이터를 저장하고 관리하는 서버들을 포함하며, 온프레미스(On-Premise) 및 클라우드에 구축 운용 중인 모든 서버 시스템이 여기에 해당함
응용 및 워크로드	응용 및 워크로드, 이에 연관된 API는 기업망 관리 시스템, 프로그램, 온프레미스 및 클라우드 환경에서 실행되는 서비스를 포함하며, 데이터를 주고받기 위한 인터페이스를 제공함
데이터	기업 혹은 기관에서 가장 최우선으로 보호해야 할 리소스이며, 기업 혹은 기관은 데이터 목록을 작성, 분류 및 레이블 지정하고, 필요에 따라 암호화 기법을 적용하여 저장 혹은 전송 중인 데이터를 보호하며 허가받지 않은 데이터 유출에 대응하기 위한 기법을 적용하여야 함

〔표 5〕 제로 트러스트 가이드라인 1.0, 제로 트러스트 성숙도 단계

성숙도 단계	정의
기존 (Traditional)	아직 제로 트러스트 아키텍처를 적용하지 않은 수준으로, 대체로 네트워크 방어에 초점을 맞춘 경계 기반 보안 모델이 적용된 상태(정교한 공격, 내부자 공격 등에 일부 취약성을 가짐)
향상 (Advanced)	제로 트러스트 철학을 부분적으로 도입한 수준으로 제로 트러스트 원칙이 보안 아키텍처에서 핵심 기능이 되는 상태(최소 권한 접근, 네트워크 분할, 로깅 및 모니터링 등이 부분적으로 적용되어 기본보다 높은 보안성 달성)
최적화 (Optimal)	제로 트러스트 철학이 전사적으로 적용된 상태(자동화된 운영, 네트워크 세분화, 신원에 대한 지속적인 검증을 통한 최소 권한의 안전한 접근제어 등을 통하여 보안성이 크게 개선)

소스, 즉 접근 대상 리소스는 시스템(System), 데이터(Data), 애플리케이션(Application)으로 구분하고 있다. 이러한 차원에서도 성숙도 핵심 요소에 데이터와 애플리케이션 외에 시스템 핵심 요소가 추가로 고려된 부분으로 확인된다. 특히나 일반적으로 관리되는 데이터나 운영되는 애플리케이션은 필연적으로 시스템(OS)에서 구동되는 부분이므로, 시스템 핵심 요소에 대한 세부적인 고려사항도 필요하다.

아래의 [표 4]는 국내 제로 트러스트 가이드라인 1.0 기업망 핵심 요소별 정의, [표 5]는 제로 트러스트 성숙도 단계별 정의이다.

Ⅲ. 업무 중요도를 고려한 제로 트러스트 성숙도 평가

3.1. 개요

최근에는 국내에도 제로 트러스트 기술이 많이 알려졌지만, 대부분 개념적인 수준에서 머무는 경우가 많기 때문에 기관과 기업에서 제로 트러스트 전환 정책 수립이나 구축 계획을 수립하는 데에는 어려움을 갖고 있다. 이와 함께 기관과 기업별로 제로 트러스트 전환 정책 기준을 수립하는 데에는 아직 컴플라이언스 체계나 구체적인 사례, 참고 가이드라인이 부족한 실정이다.

본 절에서는 제로 트러스트 성숙도를 평가하기 위해 국내 제로 트러스트 가이드라인 1.0 제로 트러스트 성숙도 모델, CISA 제로 트러스트 성숙도 모델 V2.0을 기반으로 한 제로 트러스트 성숙도 평가를 위한 방법론과 업무 중요도를 고려한 제로 트러스트 요구사항 및 기능 등에 대해 논하고자 한다.

3.2. 유스케이스 조사 및 분석(환경분석)

우선 제로 트러스트 성숙도를 평가하려는 대상 서비스 또는 시스템의 유스케이스(또는 접근 경로) 조사가 필요하다. ‘NIST SP 800-207, Figure 1’에서 언급된 대로, 보호해야 할 모든 리소스 또는 접근 대상 리소스인 ‘Enterprise Resource’를 최종 보호해야 할 기업 자원으로 정의할 수 있으며, 이는 시스템(System), 애플리케이션(Application), 데이터(Data)로 구분한다. 예를 들어, 사용자가 웹 애플리케이션 서비스인 ERP에 접근하면, 웹 애플리케이션, 웹 애플리케이션이 구

동되는 시스템(Unix, Linux, Windows Server 등), 시스템에 저장되어 관리되는 데이터, 총 3가지로 구분하여 정의할 수 있다.

리소스에 접근하는 E2E(End-to-End) 관점에서접근 대상 리소스로 접근하는 모든 주체의 접근 과정을 유스케이스로 분류해야 한다. 접근 경로 유스케이스는 서비스 운영 관점에서 가장 위협적이고, 제로 트러스트 도입을 통해 효과를 얻을 수 있는 최적의 포인트를 포함해야 한다. 최적의 포인트는 서비스 보호 대상의 실효적인 위협을 중점적으로 파악해야 하며, 서비스에 가장 큰 위협을 발생시킬 수 있는 권한을 소유한(또는 권한이 많은) 접근 주체와 접근 경로 중 어느 부분에서 취약한지 고려할 필요가 있다.

접근 경로 조사의 목적은 서비스별로 도출한 접근 경로에 대해 제로 트러스트 성숙도 진단하고자 함이며, 최초 출발지(사용자 유형, 기기 유형, 망 유형 등)에서 최종 목적지인 Enterprise Resource(시스템, 애플리케이션, 데이터)로 접근할 때까지의 접근 경로를 종합적으로 검토한다.

인프라 조사는 서비스별로 도출한 접근 경로의 기반이 되는 인프라와 보안 정책, 보안 기술 등을 확인하여 제로 트러스트 성숙도 분석을 위한 제반 사항으로 활용하는 목적이며, 최초 출발지에서 최종 목적지인 접근 대상 리소스까지의 특정 인프라 구성요소, 보안 기능 요소 등을 식별한다. 기관과 기업별로 관리·운영되는 보안 정책과 인프라가 상이하고, 실무적으로 사용되는 용어에 특수성이 있을 수 있으므로, 성숙도 평가 기간 중 관련 부서 간 지속적 커뮤니케이션을 통해 정확한 조사·분석이 필요하다.

아래의 [표 6]은 대상 서비스 또는 시스템에서 제로 트러스트 성숙도 평가를 위해 주요하게 선정된 유스케이스 예시이며, [표 7]은 선정된 유스케이스에서 조사·

〔표 6〕 대상 서비스 또는 시스템 유스케이스 예시

유스 케이스	접근 네트워크	사용자 유형	사용자 기기 유형	주요 접근통제 및 채널	접근 대상 리소스
A Case	폐쇄망	내부직원 (개발)	PC	방화벽, 물리통제	시스템 (운영서버)
B Case	내부망	외주직원 (운영)	PC	방화벽	시스템 (DB서버)
C Case	외부망	내부직원 (현업)	Mobile	VPN, VDI, 방화벽	애플리 케이션 (ERP)
D Case	외부망	내부직원 (운영)	PC	VPN, 방화벽, IAM, SSO	애플리 케이션 (그룹웨어)
E Case	개발망	외주직원 (개발)	PC	방화벽	시스템 (개발서버)
F Case	내부망	협력직원 (지원)	Mobile	방화벽, IAM, SSO	애플리 케이션 (업무지원 포털)

〔표 7〕 유스케이스(접근 경로) 환경조사 요소 예시

구분	보안 정책 또는 인프라 조사 요소 예시
접근 네트워크	내부망, 외부망, 인터넷망, 전용망, 가상 사설망, 업무망, 운영망, 개발망, 폐쇄망 등
사용자 구분	본사 임직원, 지사 임직원, 협력사 임직원, 내부직원, 외부직원, 구성원, 고객, 특수인, 프리랜서, 계약직 직원 등
사용자 역할	운영자, 개발자, 시스템 관리자, 고객 담당자, 보안 관리자, 연구원, 교직원, 학생, 방문자, 임원, 직원, VIP 등
사용자 기기	PC(Windows, macOS, Linux 등), Mobile(Android, iOS 등), 서버(Unix, Linux, Windows Server 등), IoT, 씬 클라이언트 등
접근 구간 주요 채널	VPN, VDI, 물리적 접근(USB, 시리얼 포트 등) 등
주요 접근제어	방화벽, 서버 접근제어, DB 접근제어, NAC, Secure OS, IAM, SSO, MFA(OTP, FIDO 등), 네트워크 세분화 접근제어 등
접근 대상 리소스 인프라	온프레미스, 클라우드(퍼블릭), 클라우드(프라이빗), 망분리, 폐쇄망 등
접근 대상 리소스	시스템(운영서버, 개발서버, 스테이징서버, DB서버 등), 데이터(Top-Secret, 기밀정보, 영업기밀, 고객정보, 중요 데이터 등), 애플리케이션(웹, C/S) 등
도입 보안 솔루션	SIEM, NIPS, HIPS, 안티 멀웨어, EDR, PMS, Secure OS, 서버 접근제어, DB 접근제어, FIDO 생체인증, 보안 시각화, DRM, DLP, NAC, 방화벽, DLP 등
기타	계정 관리 체계, 인증 체계, 전사 보안 관리 체계 및 부서, 요소별 관리 체계 및 부서, 물리적 통제 여부, 주요 개선 우선순위, 제로 트러스트 요구사항 등

분석되는 유스케이스 환경조사 요소 예시이다.

3.3. 제로 트러스트 성숙도 평가

현재까지 알려진 제로 트러스트 성숙도 모델은 성숙도 단계와 핵심 요소별로 전반적인 성숙도를 판단할 수 있으나, 기관과 기업 대상 서비스 또는 시스템의 현행 성숙도와 목표 성숙도를 계획하기에는 정량적 기준이 부족하다. 본절에서는 CISA 제로 트러스트 성숙도 모델, 국내 제로 트러스트 가이드라인 1.0 제로 트러스트 성숙도 모델을 바탕으로 대상 서비스 또는 시스템의 제로 트러스트 성숙도를 보다 정량적으로 평가할 수 있도록 성숙도 평가 체크리스트를 제시하고자 한다.

미국 CISA, 국내 제로 트러스트 가이드라인 1.0 제로 트러스트 성숙도 모델을 바탕으로 핵심 요소, 핵심 요소에 적합한 제로 트러스트 보안 요구기능(Capability 또는 Function)을 세부적으로 판단할 수 있는 체크리스트를 아래 [표 8]과 같이 구성한다.

제로 트러스트 성숙도 단계는 총 4단계로 '기존(Traditional)', '초기(Initial)', '향상(Advanced)', '최적(Optimal)'으로 구분한다. 성숙도 단계에 해당하는 제로 트러스트 핵심 요소 6가지(식별자·신원, 기기 및 엔드포인트, 네트워크, 시스템, 데이터, 응용 및 워크로드)를 고려한 기능과 세부기능을 도출하고, 성숙도를 평가할 수 있는 체크리스트를 바탕으로 대상 서비스 또는 시스템의 현재 제로 트러스트 성숙도를 평가한다.

예를 들어, 식별자·신원 핵심 요소에서 식별자 관리(사용자 계정 관리) 기능에 대해 '관리 체계 없음', '사용자 계정 개별 관리', '전사 인사 정보 및 계정 연동', '일부 영역에 대해 IdP(Identity Provider) 기반 ID 통합 관리(SSO 및 ID Federation)', '전체 영역에 대해 IdP 기반 ID 통합 관리(SSO 및 ID Federation)' 등과 같이 제로 트러스트 보안 요구사항을 반영한 체크리스트를 구성한다.

기기 및 엔드포인트 핵심 요소에서 데이터 접근제어(기기 접근 인가) 기능에 대해 '관리 체계 없음', '기기 보안 상태 확인 후 접근 인가', '기기 보안 상태 확인 후 접근 인가, 권한 조정', '기기 보안 상태 확인 후 접근 인가, 권한 조정 및 격리 조치'와 같이 제로 트러스트 보안 요구사항을 반영한 체크리스트를 구성한다.

시스템 핵심 요소에서 접근통제(시스템 계정(OS) 인증) 기능에 대해 'ID/PW 단일 인증', 'MFA(지식 기반 또는 소유 기반) 필수 적용', 'MFA(존재 기반) 필수 적용', 'MFA 및 지속적 접근 주체 보안 컨텍스트 기반 접근 인가'와 같이 제로 트러스트 보안 요구사항을 반영한 체크리스트를 구성한다.

결과적으로 6가지 핵심 요소 기능별 체크리스트를 바탕으로 대상 서비스 또는 시스템 유스케이스 및 핵

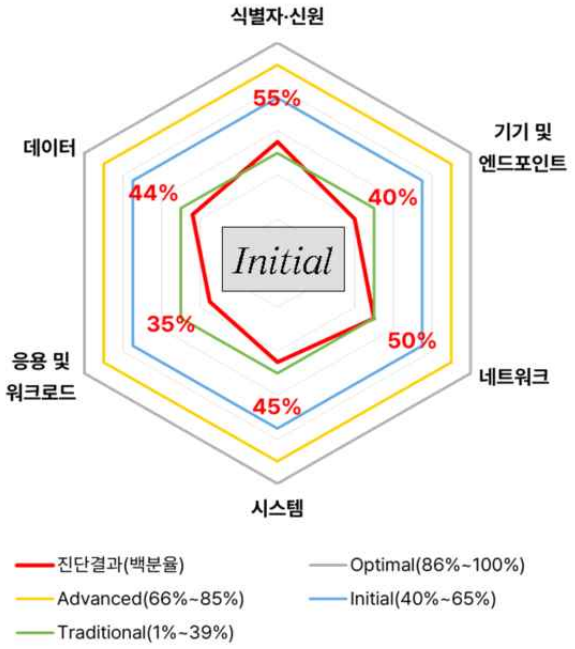
〔표 8〕 핵심 요소별 성숙도 평가 체크리스트 예시

핵심 요소	기능	핵심 요소별 성숙도 체크리스트			
식별자·신원	사용자 계정 관리	사용자 계정 개별 관리	전사 인사 정보 및 계정 연동	일부 영역 IdP 기반 ID 통합 관리	전체 영역 IdP 기반 ID 통합 관리
기기 및 엔드포인트	기기 접근 인가	인증 후 접근 인가	기기 보안 상태 확인 후 접근 인가	기기 보안 상태 확인 후 접근 인가, 권한 조정	기기 보안 상태 확인 후 접근 인가, 권한 조정, 격리 조치
시스템	OS 계정 인증	ID/PW 단일 인증	MFA (지식 또는 소유 기반) 필수 적용	MFA (존재 기반) 필수 적용	MFA 및 지속적 접근 주체 보안 컨텍스트 기반 접근 인가

〔표 9〕 대상 서비스 또는 시스템 및 핵심 요소별 성숙도 평가 결과 예시 (단위 : %)

유스케이스	식별자·신원	기기 및 엔드포인트	네트워크	시스템	데이터	응용 및 워크로드
A Case	54	60	66	61	61	53
B Case	57	45	62	71	67	50
C Case	51	60	68	57	59	60
D Case	55	25	40	20	24	15
E Case	56	20	25	26	30	17
F Case	54	30	36	32	25	15
평균	*55*	*40*	*50*	*45*	*44*	*35*

대상 서비스(또는 시스템) 성숙도 수준 : 45% (Initial)



〔그림 2〕 핵심 요소별 성숙도 평가 결과 예시

심 요소별 체크리스트 답변을 고려하여, [표 9], [그림 2]와 같이 핵심 요소를 기준으로 한 육각형 모형(Radar Chart)의 현행 성숙도 수준을 도출하고, 성숙도 4단계 중 어느 단계인지 평가할 수 있다.

다만, 성숙도 단계별 백분율(%)은 공신력 있는 기관에서 제시된 모델이나 컴플라이언스가 존재하지 않으므로, 성숙도 단계별 수치는 제로 트러스트 보안 요구사항 수준에 부합하도록 단계별 백분율을 구성하였다.

3.4. 업무 중요도를 고려한 제로 트러스트 성숙도 평가 고려사항

본절에서는 업무의 중요도를 구분하는 기준을 제시하는 것이 아닌, 업무의 중요도와 접근 대상 리소스의 중요도별 제로 트러스트 성숙도를 고려할 사안에 대해 논하고자 한다. 본 연구에서는 업무의 중요도를 구분하고 이에 따른 제로 트러스트 보안 요구사항을 명확히 할 필요성에 초점을 맞추고 있다.

업무의 중요도는 보호해야 할 대상인 시스템, 데이터, 애플리케이션의 중요성에 따라 '상(High)', '중(Medium)', '하(Low)'의 세 가지 수준으로 구분한다. 아래의 내용은 업무 중요도별 제로 트러스트 고려사항 예시이며, 업무에 대한 고려사항은 망분리 정책을 기준을 예시로 설명한다.

'상(High)'급 중요도에 해당하는 업무는 최고 수준의 보안 요구사항이 필요하며, 이는 물리적 망분리와 제로 트러스트 보안 체계의 확장을 통해 이루어질 수 있다. 이러한 체계는 중요도가 가장 높은 데이터와 시스템을 보호하는 데 있어 필수적이며, MFA(생체) 인증, 접근 주체의 보안 상태 지속적 검증, 사용자 계정 및 기기 식별자의 통합 자동화 관리 등의 고급 보안 기술을 포함한다.

'중(Medium)'급 중요도의 업무는 논리적 망분리를 기반으로 한 제로 트러스트 체계를 고려해야 하며, 이는 중급 중요도의 데이터 및 시스템을 보호하는 데 적합하다. 이 수준에서의 보안 요구사항에는 MFA(소유) 인증, 필수 구간의 암호화, 내부 및 일부 외부 트래픽의 암호화 등이 포함된다.

'하(Low)'급 중요도의 업무는 일반 수준의 제로 트러스트 요구사항을 적용하며, 망분리 없이 보안성을 유연하고 고도화하는 방향으로 진행된다. 이는 ID/PW 인증, 식별자 통합 자동화 관리, 필수 구간 암호화 등을 포함한다.

업무의 중요도에 따라 제로 트러스트 보안 요구사항을 구분하는 경우, 접근 대상 리소스의 중요도에 따

〔표 10〕 업무 중요도 구분, 고려사항 및 제로 트러스트 요구사항 예시 (망분리 예시)

업무 중요도	고려사항
'상'급 (High)	중요도가 가장 높은 데이터(Top Secret, 비밀정보 등) 및 데이터가 저장되어 관리되는 시스템
	물리적 망분리 기반 강력한 보안 체계
	망분리 체계를 유지하면서 최고 수준의 제로 트러스트 보안 체계까지 확장
'중'급 (Medium)	중요도가 중급에 해당하는 데이터 및 데이터가 저장되어 관리되는 시스템
	논리적 망분리 기반 제로 트러스트 체계 고려
	고수준의 제로 트러스트 요구사항 반영한 체계
'하'급 (Low)	중요도가 하급에 해당하는 데이터 및 데이터가 저장되어 관리되는 시스템
	일반 수준의 제로 트러스트 요구사항을 반영한 보안 체계
	망분리 없이 보안성 유연화, 고도화

〔표 11〕 업무 중요도를 고려한 제로 트러스트 요구사항 예시

업무 중요도	제로 트러스트 요구사항
'상'급 (High)	MFA(생체) + 접근 주체 보안 상태 지속적 검증
	사용자 계정, 기기 식별자 통합 자동화 관리 및 계정 관리 연동
	보안 상태 확인 후 접근 인가 및 권한 조정
	모든 내·외부 트래픽 암호화
	통합 위협 알림 시스템(모든 요소) 기반 위협 알림 및 머신러닝 적용
'중'급 (Medium)	MFA(소유) + 접근 주체 보안 상태 지속적 검증
	사용자 계정, 기기 식별자 통합 자동화 관리
	보안 상태 확인 후 접근 인가 및 권한 조정
	필수 구간 암호화 및 내부 및 일부 외부 트래픽 암호화
	통합 위협 알림 시스템(사용자, 기기, 시스템, 등) 기반 위협 알림
'하'급 (Low)	ID/PW + 접근 주체 보안 상태 지속적 검증
	식별자 통합 자동화 관리
	인증 시 보안 상태 확인 후 접근 인가
	필수 구간 암호화
	개별 영역 위협 알림

〔표 12〕 업무 중요도를 고려한 핵심 요소별 성숙도 요구사항 예시

핵심 요소	기능	접근 대상 리소스	중요도	요구사항
식별자·신원	사용자 접근 인가	운영서버 (Linux)	상 (High)	사용자 보안 상태 확인 후 접근 인가, 권한 조정, 격리
기기 및 엔드포인트	기기 접근 인가	업무 서비스 (도면관리)	중 (Medium)	기기 보안 상태 확인 후 접근 인가
시스템	OS 계정 인증	개발서버 (Unix)	하 (Low)	다중 인증 (옵션)

른 제로 트러스트 체계 도입으로 제도적인 유연성을 높이고 보안성도 함께 높일 수 있을 것이다.

아래 [표 10]은 업무 중요도 구분, 고려사항 및 제로 트러스트 요구사항 예시, [표 11]은 업무 중요도를 고려한 제로 트러스트 요구사항 예시, [표 12]는 업무 중요도를 고려한 핵심 요소별 성숙도 요구사항 예시이다.

Ⅳ. 결 론

본 연구에서는 업무 중요도를 고려한 제로 트러스트 성숙도 평가 방법론에 대해 논하였다. 본 연구를 통해 다양한 시각에서 아래와 같은 시사점을 도출한다.

첫 번째로, 국내에 제로 트러스트 성숙도 진단을 위한 공인된 평가 체계의 부재이다. 현재 기관과 기업에서 대상 서비스 또는 시스템의 성숙도를 평가하고 향후 성숙도 향상을 위한 목표를 설정하기 위한 정량적인 수치화된 평가 방법론이나 정성적인 평가 체계가 부족한 상황이다. 미국 CISA 제로 트러스트 성숙도 모델, 국내 제로 트러스트 가이드라인 1.0 제로 트러스트 성숙도 존재하나, 이를 정량적, 정성적으로 성숙도를 판단할 수 있는 공신력 있는 체계가 부족하다. 또한 기존의 정보보호 인증 체계(ISMS-P 등)와 달리 제로 트러스트 보안 요구사항을 반영할 수 있는 체계가 부족하다. 이러한 실정으로 기관과 기업 자체적으로 제로 트러스트 정책, 기술 전환 계획 수립 시 대처 방안이 부족한 상황이다.

두 번째로, 성숙도 향상을 위한 적합한 제품(또는 솔루션, 서비스)이 부족하다는 점이다. 성숙도 평가가 이루어지고 성숙도 GAP을 개선하기 위해 정보보호 제품(또는 솔루션, 서비스)을 도입하여 해결하는 것이 필요한데 제로 트러스트 보안 요구사항을 만족할 수 있는 대응 솔루션이 부족한 상황이다. 일부 제로 트러스트 요구사항을 달성할 수 있는 솔루션이 벤더사를 통해서 출시되고 홍보되고 있으나, 이는 일부 보안 요구사항을 충족할 수 있는 정도의 수준에 머무르는 것이 현실이다. 이러한 실정이므로 기관과 기업에서는 제로 트러스트 보안 요구사항을 자체적으로 해결하기 위해 장기적인 자체 개발 및 운영을 고려하는 것이 현실이기도 하다.

세 번째로, 성숙도 평가 시 현행 컴플라이언스 고려 및 명확한 기간, 범위 설정이 필요하다. 현재 운영 중인 대상 서비스 또는 시스템에 해당하는 컴플라이언스 체계 및 인증 체계를 고려하여 제로 트러스트 보안 요

구사항을 달성하는 것이 중요하다. 현행 정보통신망법, 개인정보보호법, ISMS-P 등에서 요구하는 필수 보안 요구사항을 충족하면서, 추가로 이러한 컴플라이언스에서 강제적으로 요구하고 있지 않은 제로 트러스트 보안 요구사항을 충족하는 것이 가장 합리적인 성숙도 향상 방안일 것이다. 예를 들어 컴플라이언스에서 요구하는 방화벽, IPS, VPN, 망분리와 같은 정책과 인프라는 유지하면서, 점진적으로 제로 트러스트 보안 요구사항을 달성할 수 있도록 단계적인 전환 체계 수립이 필수적일 수도 있다.

네 번째로, 업무 중요도에 대한 정확한 기준 설정이 선행되어야 한다. 업무의 중요도는 앞서 제안한 접근 대상 리소스(시스템, 데이터, 애플리케이션)을 기준으로 중요도를 산정하는 방안이라고 한다면, 이에 대한 중요도를 구분하여 제로 트러스트 보안 정책을 적용할 수 있는 정책이 수립되어야 한다. 많은 기관에서 제로 트러스트 성숙도 모델을 설명할 때 '데이터(Data)'는 기관이 보호해야 할 가장 중요한 리소스라고 설명하고 있으므로, 데이터를 기준으로 더욱 세밀화된 보안 정책 수립이 되어야 할 것이며, 데이터를 저장하고 운영하는 시스템(System)에 대해서도 추가로 중요도를 구분하여 보안 정책을 세분화하여 운영·관리하는 것이 중요한 사안일 것이다.

본 연구에서는 업무 중요도를 고려한 제로 트러스트 성숙도 평가를 위한 다양한 방안과 기관과 기업이 제로 트러스트 정책 및 인프라를 효과적으로 계획하고 실행하는 데 필요한 실질적인 참고사항을 제시하였다. 본 연구를 통해 더욱 구체적인 후속 연구가 활발히 이루어지길 기대한다.

참 고 문 헌

[1] 과학기술정보통신부, *"제로 트러스트 가이드라인 1.0"*, 과학기술정보통신부, pp.54-66, 2023.

[2] CISA(Cyber Security Infrastructure Agency) Cybersecurity Division, *"Zero Trust Maturity Model V2.0"*, CISA, pp.4-31, 2023.

[3] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, *"SP 800-207 Zero Trust Architecture"*, NIST(National Institute of Standards and Technology), pp.4-27, 2020.

[4] Alper Kerman, Murugiah Souppaya, Parisa Grayeli, Susan Symington, *"SP 1800-35B Implementing a Zero Trust Architecture"*, NIST, The MITRE Corporation, pp.1-5, 2022.

[5] John Kindervag, *"Build Security Into Your Network's DNA: The Zero Trust Network Architecture"*, Forrester Research, pp.2-13, 2010.

[6] NSA(National Security Agency), *"Embracing a Zero Trust Security Model"* pp.2-7, NSA, 2021.

[7] THE WHITE HOUSE, *"Improving the Nation's Cybersecurity"*, THE WHITE HOUSE, pp.26633-266447, 2021.

[8] Forrester, *"The Total Economic Impact Of Zero Trust Solutions From Microsoft"*, Forrester Research, pp.1-5, 2021.

[9] Robert Freter, Department of Defense (DoD) Zero Trust Reference Architecture Version 2.0, Department of Defense, pp.9-52, 2022.

[10] Department of Defense (DoD), *"DoD Zero Trust Capability Execution Roadmap (COA 1)"*, Department of Defense, pp.2-58, 2023.

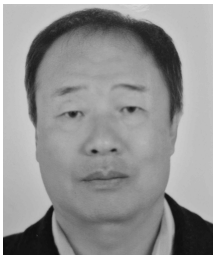
〈저 자 소 개〉

박 재 혁 (Jae Hyeok Park)

2014년 2월 : 고려대학교 경상대학 경영정보학과 졸업
2016년 2월 : 동국대학교 국제정보보호대학원 정보보호학석사
2016년 1월~현재 : 에스지에이솔루션즈㈜ R&D센터 연구원(제품 솔루션 연구 및 사업기획)
<관심분야> 정보보호, MIS, 제로 트러스트, 클라우드

이 현 진 (Hyun Jin Lee)

2021년 : 강원대학교 공학사
2023년 : 강원대학교 공학석사
2023년~현재 : 에스지에이솔루션즈㈜, R&D센터 연구원(제품 솔루션 연구 및 사업기획)
<관심분야> 제로 트러스트, 클라우드 보안, 융합보안



이 기 욱 (Ki Uk Lee)

2019년 2월 : 동국대학교 국제정보보호대학원 정보보호학석사
2021년 4월~현재 : 에스지에이솔루션즈㈜ R&D총괄
<관심분야> 제로 트러스트, 클라우드 보안, 시스템 보안

최 영 철 (Young Chul Choi)

종신회원

2003년 2월 : 성균관대학교 전기전자컴퓨터공학 공학박사
2010년 3월~2012년 5월 : 에스지에이㈜ 부사장
2012년 6월~현재 : 에스지에이솔루션즈㈜ 대표이사
<관심분야> PKI, 제로 트러스트, 클라우드 보안