KIPS Trans. Comp. and Comm. Sys.
Vol.12, No.6 pp.189~196
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2023.12.6.189

A Study on How to Build a Zero Trust Security Model

Jin Yong Lee† · Byoung Hoon Choi† · Namhyun Koh†† · Samhyun Chun†††

ABSTRACT

Today, in the era of the 4th industrial revolution based on the paradigm of hyper-connectivity, super-intelligence, and super-convergence, the remote work environment is becoming central based on technologies such as mobile, cloud, and big data. This remote work environment has been accelerated by the demand for non-face-to-face due to COVID-19. Since the remote work environment can perform various tasks by accessing services and resources anytime and anywhere, it has increased work efficiency, but has caused a problem of incapacitating the traditional boundary-based network security model by making the internal and external boundaries ambiguous. In this paper, we propse a method to improve the limitations of the traditional boundary-oriented security strategy by building a security model centered on core components and their relationships based on the zero trust idea that all actions that occur in the network beyond the concept of the boundary are not trusted.

Keywords : 4th Industrial Revolution, Remote Work Environment, Security Strategies, Zero Trust

제로 트러스트 보안모델 구축 방안에 대한 연구

이 진 용† · 최 병 훈† · 고 남 현†† · 전 삼 현†††

요 약

초연결, 초지능, 초융합의 패러다임 기반의 4차 산업혁명 시대를 맞이하고 있는 오늘날에는 모바일, 클라우드, 빅데이터 등의 기술을 바탕으로 원격업무 환경이 중심이 되고 있다. 이와 같은 원격업무 환경은 코로나19로 인한 비대면에 대한 요구로 가속화되었다. 원격업무 환경은 언제, 어디에서나 서비스 및 자원에 접근하여 다양한 업무를 수행할 수 있기 때문에, 업무 효율성은 증가시켰으나 내외부 경계를 모호하게 만듦으로써 전통적인 경계 기반 네크워크 보안모델을 무력화시키는 문제점을 야기시켰다. 본 논문에서는 경계면의 개념을 넘어 네트워크에서 발생하는 모든 행위를 신뢰하지 않는다는 제로 트러스트 사상에 기반한 핵심 구성요소와 이들 간의 관계를 중심으로 한 보안모델을 구축함으로써, 전통적인 경계면 중심 보안 전략의 한계점을 개선할 수 있는 방안을 제시하였다.

키워드 : 4차 산업혁명, 원격근무, 보안 전략, 제로 트러스트

1. 서 론

4차 산업혁명 시대의 초연결 패러다임에 기반하여 원격 접속 기반 인프라가 발전하고 있으며, 코로나19는 이러한 원격 인프라 문화를 확산시켰다[1]. 이와 같은 환경에서의 기업은 여러 개의 내부 네트워크 구성, 로컬 원격 접속 인프라스트럭처 기반의 사무실 운영, 모바일 및 클라우드 서비스 등 다양한 서비스 인프라 환경을 구성하였고, 기존의 경계 기반의 네트워크 보안으로는 통제할 수 없게 되었다[2]. 전통적인 경계 기반의 네트워크 보안 환경에서는 내부 자원으로 접근하는 핵심 입구인 경계면을 식별하여 보안자원을 집중하는 전략으로 운영되어왔다. 따라서 경계면에서 인가될 때까지만 신뢰하지 않는 것이 일반적이었다. 그러나 원격업무 환경에서는 언제, 어디에서나 접속이 가능하여 경계면의 개념을 모호하게 만들었다. 즉, 신뢰와 비신뢰의 구간을 정의하기 어렵게 되었다. 이에 따라 “신뢰하지 않고, 항상 검증한다.”라는 개념의 제로 트러스트 보안이 전통적인 경계 보안의 대체 전략으로 제안되고 있다[3].

본 논문에서는 이와 같은 새로운 보안 패러다임인 제로 트러스트 개념을 현업에서 보다 용이하게 구축·관리할 수 있는 방안을 제시하고자 하였다. 이를 위해 제로 트러스트 사상을 구현하기 위한 도메인 및 핵심 구성요소와 이들 간의 관계를 식별·배치함으로써 제로 트러스트 보안모델의 흐름을 도식화하였다. 더 나아가 제로 트러스트 보안모델의 세부 통제항목을 정의하고 기술함으로써 현업에서 운영 중인 정보보호 관

※ 이 논문은 2022년 한국정보처리학회 ASK 2022의 우수논문으로 “제로 트러스트 아키텍처 기반의 정보보호 관리체계 구축에 관한 연구”의 제목으로 발표된 논문을 확장한 것임.
† 정 회 원 : 숭실대학교 IT정책경영학과 박사과정
†† 비 회 원 : 숭실대학교 IT정책경영학과 박사과정
††† 비 회 원 : 숭실대학교 IT정책경영학과 교수
Manuscript Received : December 19, 2022
Accepted : January 26, 2023
* Corresponding Author : Samhyun Chun(shchun@ssu.ac.kr)

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/ licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

리체계 환경에 보다 구체적으로 적용할 수 있는 방안을 제언하였다.

2. 관련 연구

2.1 제로 트러스트 아키텍처

제로 트러스트는 기술 그 자체나 상용 올인원(all-in-one) 소프트웨어 솔루션을 의미하지 않고, 보안 강화를 위한 개념적 요소이다[3]. 제로 트러스트는 사이버 보안 패러다임이 네트워크 경계로부터 사용자, 자산 및 자원(자산, 서비스, 워크플로우, 네트워크 계정 등) 중심의 방어로 옮겨가는 것을 의미한다. 제로 트러스트는 네트워크 나누는 것이 아니라 자원을 보호하는 것에 초점을 맞춘다. 즉 네트워크의 위치는 더 이상 자원의 보안 상태를 결정하는 주요 요소로 볼 없다[4].

NIST(미국 국립표준기술연구소)에서는 다음과 같이 7개의 원칙을 제로 트러스트 아키텍처의 기본원리로 정의하고 있다.

1) 기업의 자원에 접근할 수 있다면 개인 혹은 기업 소유와 무관하게 모든 데이터 소스 및 서비스를 리소스로 간주한다.
2) 네트워크 위치와 관계없이 모든 통신을 보호해야 한다.
3) 기업 자원에 대한 접근을 세션단위로 허가한다.
4) 동적 정책으로 자원에 대한 접근을 결정한다.
5) 기업은 기본적으로 자산을 신뢰하지 않고 모든 자산의 무결성 및 보안 상태를 감시하고 조치해야 한다.
6) 모든 리소스의 인증/인가를 동적으로 강력하게 실시한 후 접근을 허용한다.
7) 기업은 자산, 네트워크 인프라스트럭처, 커뮤니케이션의 현 상태에 대해 가능한 많은 정보를 수집한다.

이와 같은 기본원리에 의거하여, NIST에서는 Fig. 1과 같이 이상적인 제로 트러스트의 개념 모델을 제시하였다. 해당 모델은 모든 접근 정책에 대한 유효성을 식별 및 판단하여 접근 전략을 수립하는 정책 결정 포인트(PDP: Policy Decision Point)와 수립된 접근 전략을 실제 집행하는 정책 집행 포인트(PEP: Policy Enforcement Point)로 구성된 제로 트러스트의 접근모델을 중심으로 제로 트러스트를 구성하는 논리적 컴포넌트들 사이의 상호 작용을 표현하였다[1, 4].

2.2 제로 트러스트 성숙도 모델

CISA(미국 사이버보안 및 인프라보안국)에서는 Fig. 2와 같이 제로 트러스트 성숙도 모델을 식별자, 디바이스, 네트워크 및 환경, 어플리케이션 워크로드로 구성된 5개 축에 대한 구현 수준으로 묘사하였다.

5개로 구성된 각 축에 대하여 전통적, 진보적, 최적화의 3단계로 성숙도를 각각 정의하고 5개의 축을 통한 가시성을 기반으로 한 분석기능과 자동화된 오케스트레이션 환경을 바탕으로 거버넌스를 확보하는 모델을 제시하였다.

성숙도 단계의 첫 번째인 전통적 단계에서는 수동 설정 및 정적 정책관리와 같이 유연성이 부족한 상태를 의미한다. 따

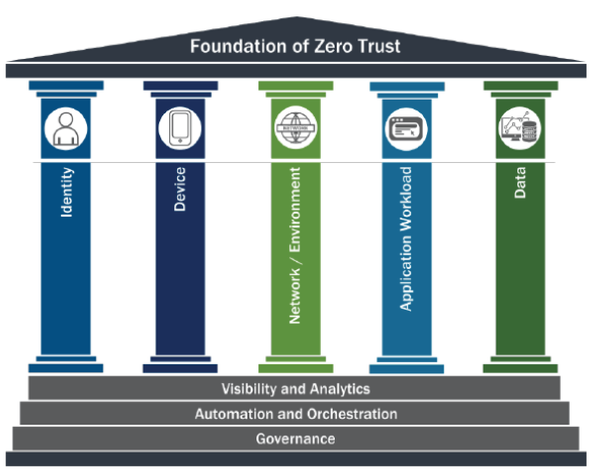

Fig. 2. Foundation of Zero Trust[7]

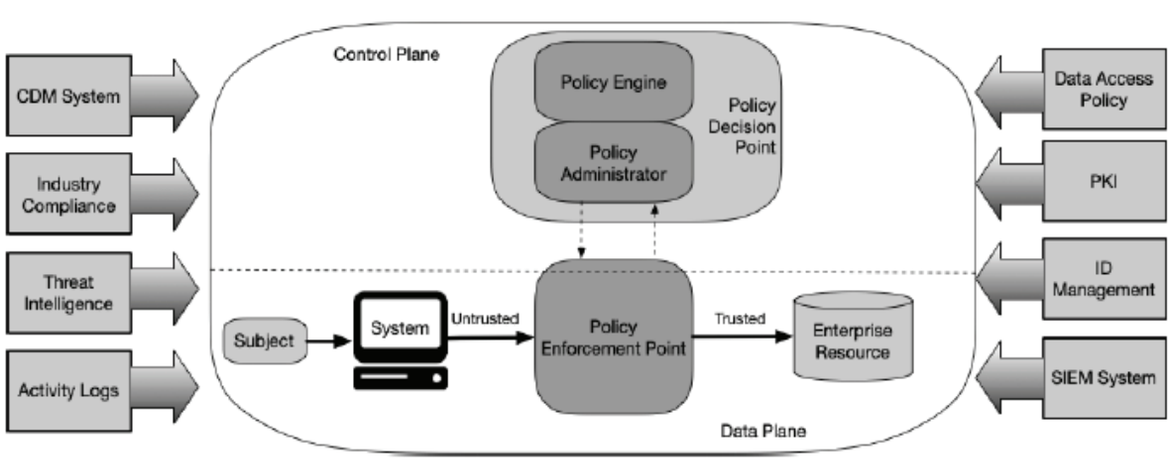

Fig. 1. Core Zero Trust Logical Components[4]

라서 5개의 축이 자연스럽게 연결되지 않고 배타적으로 관리되어 오케스트레이션을 확보하기 어렵다.

진보적 단계에서는 5개의 축 간의 조화를 통해 가시성과 통제가 개선된 상태를 나타낸다. 마지막의 최적화 단계에서는 자동화 및 식별될 수 있는 인프라스트럭처에서 자산과 자원 설정값 등을 동적 정책에 따라 완전한 자동적 수준으로 통제 관리될 수 있음을 의미한다[7].

2.3 기타 연구

제로 트러스트는 관련 연구는 제로 트러스트에 대한 전체적인 관점의 개념적 모델을 기업의 인프라스트럭처에 적용 및 배포하기 위한 연구와 제로 트러스트 개념을 구성하는 개별 컴포넌트의 효과적인 구현을 위한 연구로 분류된다.

기업의 인프라스터럭처에 적용 및 배포하기 위한 연구에서는 기업에서 제공하는 서비스의 인프라스트럭처 특성을 반영하여 제로 트러스트의 구성요소를 배치하는 방법을 제시하고 있다[1, 4]. 이때 기업 내 적용 및 배포의 수준을 측정하기 위한 제로 트러스트 성숙도 모델이 식별자, 디바이스, 네트워크 환경, 응용프로그램 워크로드, 데이터 관점으로 단계별로 제시되기도 한다[7].

이에 반해 제로 트러스트 개념 모델 내 개별 컴포넌트에 대한 연구는 정책 결정 포인트 등 제로 트러스트의 핵심 구성요소의 성능을 향상시키기 위한 머신러닝 알고리즘 적용방안[3], 방화벽의 접근통제 기능을 확장 응용한 VMWARE NSX, 싱글사이온, 접근통제, 사용자 인증 등의 개념을 구현한 구글의 BeyondCorp 등이 존재한다[1, 5, 6].

3. 제로 트러스트 보안모델 구축 방안

본 논문에서는 NIST 및 CISA의 제로 트러스트 아키텍처의 기본원리, 접근통제 및 성숙도 모델 개념[4, 7] 등을 바탕으로 조직 내 제로 트러스트 모델을 구축하기 위한 방안을 제언한다.

3.1 제로 트러스트 보안모델의 흐름 식별 및 구성

Fig. 3은 NIST, CISA의 제로 트러스트 기본원리, 성숙도 등의 개념을 바탕으로 제로 트러스트 보안모델 흐름을 도식화한 것이다. Fig. 3의 ①~⑦ 까지의 구성요소는 2.1에서 언급된 제로 트러스트 기본 7개의 원칙과 대응된다.

제로 트러스트 보안모델 흐름도는 크게 데이터 영역(Data Domain), 통제 영역(Control Domain), 성숙도 영역(Maturity Domian)의 3가지 영역으로 구분된다. 데이터 영역에

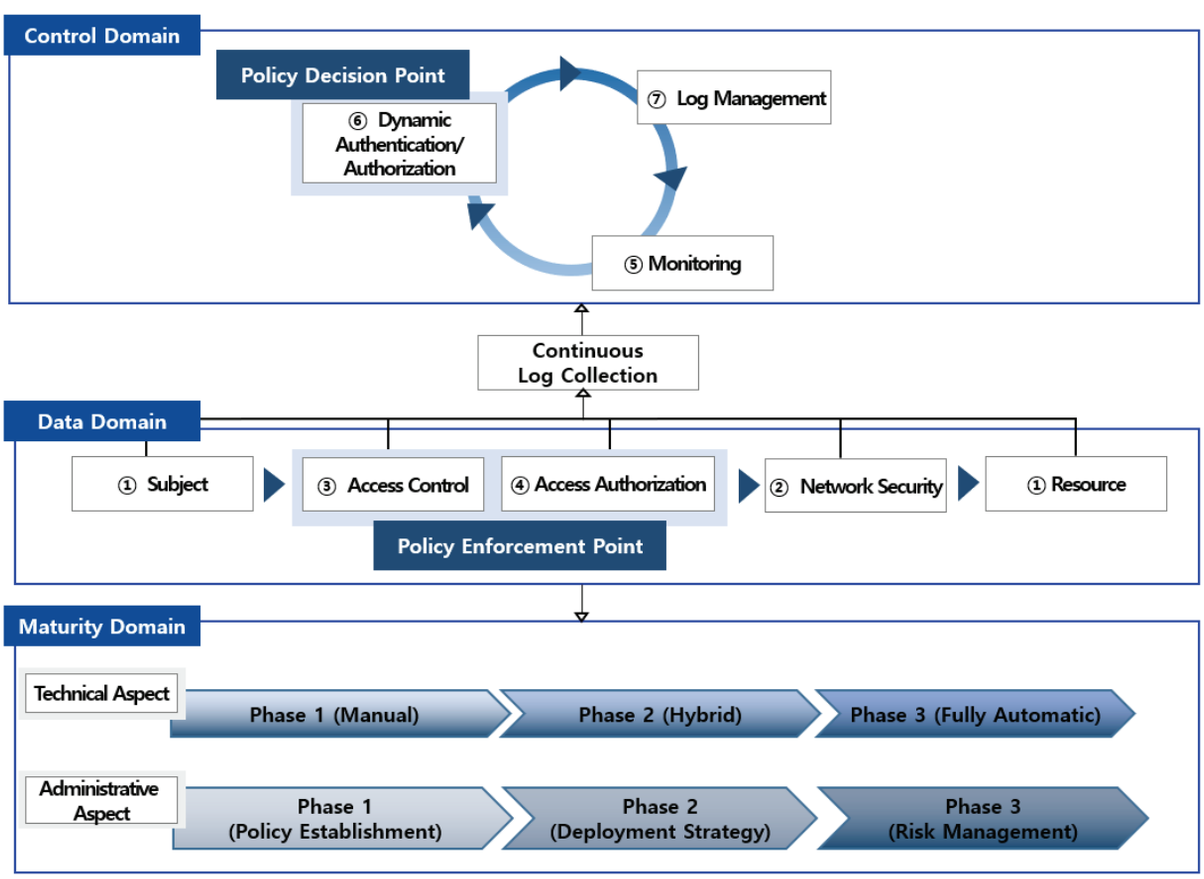

Fig. 3. Zero Trust Security Model Flowchart

서는 접근주체가 자원에 접근하기까지의 제로 트러스트 환경에서의 통제 및 인가 흐름을 보여준다. 다음으로 통제 영역에서는 데이터 영역의 흐름에서 발생하는 각종 통제정책에 대한 전략적 검토 및 생성의 역할을 수행한다. 끝으로 성숙도 영역에서는 기술적 측면에서의 자동화 수준과 관리적 측면으로의 정책수립, 배치전략, 위험관리 수준을 측정하여 제로 트러스트의 성숙도 단계를 평가한다.

데이터 영역에서는 다음과 같은 구성요소의 세부 특징 및 흐름을 보여준다.

① 조직 내부의 서비스, 데이터 등 모든 자원(Resource)에 접근할 수 있는 조직 및 개인 소유의 접근주체(Subject)는 위치, 시간, 보안 설정 상태 등의 상황적 속성과 세션 연결, 데이터 전송 프로토콜, 접속 및 라우팅 경로 등 행동적 속성을 보유하고 있다.

② 네트워크 보안(Security)에서는 접근주체가 자원에 접근하기까지의 모든 흐름은 모니터링할 수 있는 상태를 의미한다. 이를 통해 접근주체와 자원의 상황적, 행동적 속성에 대해 전방위적으로 관찰할 수 있도록 한다.

③ 접근통제(Access Control)는 접근주체와 자원의 상황 및 행동적 속성에 대한 평가된 내용을 바탕으로 접근을 허용한다.

④ 접근허용(Access Authorization)에서는 세션단위의 최소 이동구간 및 최소 접근권한으로 제한하는 것을 의미한다. 이때 접근주체와 자원의 상황적 속성은 마찬가지로 모니터링 되어진다.

접근통제와 접근허용은 제로 트러스트 모델에서의 접근 전략을 실제 집행하는 정책 집행 포인트(Policy Enforcement Point) 역할을 맡는다. 이와 같은 데이터 영역의 흐름에서 발생하는 모든 행위는 통제 영역으로 전송된다.

데이터 영역으로부터 받은 정보를 바탕으로 통제 영역에서는 다음과 같은 구성요소와 흐름을 보여준다.

⑤ 모니터링(Monitoring)은 네트워크 상의 흐름 외에도 자원 및 주체의 보안설정 상태까지 감시한다. 감시는 실시간으로 갱신되어 최신성을 반영한다.

⑥ 동적 인증/인가(Dynamic Authentication/Authorization)에서는 모니터링되고 있는 접근주체와 자원의 실시간 지속적 동적 평가를 통해 접근 및 인가에 대한 전략을 수립하여 정책 집행 포인트에 명령을 전달하는 제로 트러스트 모델의 두뇌인 정책 결정 포인트(Policy Decision Point) 역할을 수행한다.

⑦ 로그관리(Log Management)에서는 제로 트러스트 보안모델의 모든 흐름 내 정형/비정형 로그를 수집하여 연관분석을 수행한다. 이때 연관분석의 정책은 행위기반의 알려지지 않은 신규 공격 유형을 식별하기 위해 적재된 흐름상의 상황 및 행동적 속성 분석을 통한 문맥적 판단에 의해 실시간 갱신이 가능한 구조를 가진다.

끝을 성숙도 영역(Maturity Domain)에서는 제로 트러스트 모델의 수준을 측정하는 단계로 기술 및 관리적 측면으로 측정한다. 기술적 측면에서는 가장 초기 모델인 수동관리 단계에서부터, 수동과 자동의 하이브리드 단계, 끝으로 완전 자동화 단계까지로의 모델에 대한 수준을 측정할 수 있음을 나타낸다. 제로 트러스트 보안모델은 대규모 데이터의 실시간 문맥적 분석을 통해 지속적 접근통제 정책이 개선 되어져야 함으로 수동적 환경에서는 온전한 모델의 구현이 어려운 특성이 존재한다. 다음으로 관리적 측면에서는 조직 내 제로 트러스트 보안모델 구축을 위한 목표를 정의하여 정책을 수립하고, 제로 트러스트의 핵심 컴포넌트의 적정한 배치에서부터 제로 트러스트 모델 자체적으로 발생할 수 있는 위험을 식별 및 관리할 수 있는 단계까지로 성숙도를 정의한다.

3.2 제로 트러스트 보안모델의 성숙도 측정 방안

이번 장에서는 제로 트러스트 보안모델의 성숙도 측정을 위한 접근방법을 제시하며, Fig. 4는 이에 대한 개념도이다.

제로 트러스트 보안모델의 실제 구현 대상인 통제영역과 데이터 영역은 기술 및 관리적 측면으로 성숙도 평가 지표를 각각 도출될 수 있으며, 각 도출된 지표를 최종 결합함으로써 성숙도 수준을 측정할 수 있다.

자동화 수준을 측정하는 기술적 측면에서는 제로 트러스트 보안모델의 데이터 및 통제 도메인 영역에서의 자동화가 요구되어지는 항목을 도출한 뒤, 해당 항목 중 자동화된 것과 자동화가 되지 않은 요소를 구분하여 자동화 비율을 산정한다. 이때 각 요소의 중요도에 따라 가중치를 부여할 수 있다.

관리적 측면에서의 평가 지표에서는 제로 트러스트 구축 목표를 반영한 정책 수립 수준, 제로 트러스트 컴포넌트 배치 관리전략 및 위험관리 수준에 따라 측정될 수 있다.

Table 1은 성숙도 수준 측정을 위한 접근방법에 대한 하나의 예시이다.

기술적 측면에서의 자동화 비율을 산정하기 위해서는 Ae(자동화 구성요소의 성숙도 수준 총합), NAe(비자동화 구성요소의 성숙도 수준 총합), a(가중치 변수), m(추출된 자동화 요소의 갯수), l(추출된 비자동화 요소의 갯수), AE(자동화 개별 요소), NAE(비자동화 개별 요소), TM(기술적 성숙도 평가수준)로 정의할 경우, 자동화 요소와 비자동화 요소의 성숙도 수준에 대한 측정은 각각 Fig. 1과 같이 도출할 수 있으며, 최종 기술적 성숙도 수준은 Fig. 2와 같이 산출할 수 있다. 산출된 TM 값의 범위에 따라 성숙도 단계 수준(1 ~ 3)으로 보정 할 수 있다.

$$Ae = \sum_{n=1}^{m} aAE_n,\ NAe = \sum_{n=1}^{l} aNAE_n \tag{1}$$

$$TM = Ae - NAe \tag{2}$$

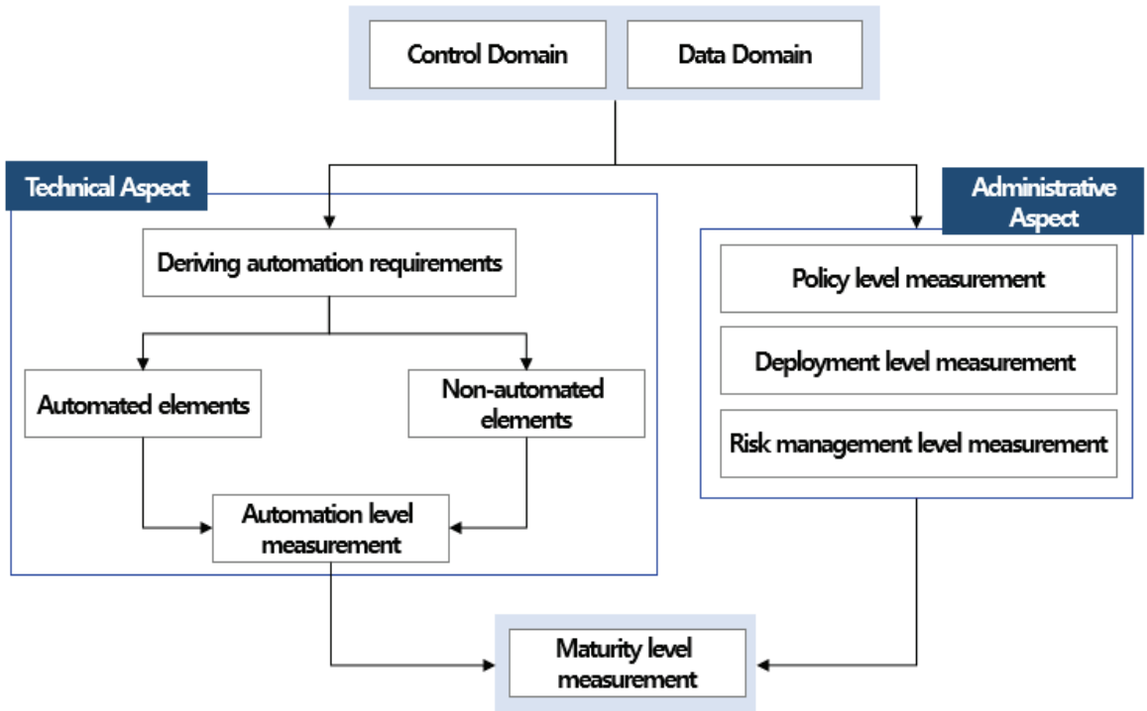

Fig. 4. Conceptual Diagram of Maturity Level Measurement of Zero Trust Security Model

Table 1. An Example of Measuring the Maturity of Zero Trust Security Model

Aspect	Evaluation Factor	Evaluation standard	Phase
Technical Aspect	Automated elements	Total evaluation Index of Automation Elements (Ae)	TM (1~3)
	Non-Automated elements	Total evaluation Index of Non-Automation Elements (NAe)	
Administrative Aspect	Policy or Deployment or Risk Management Level	N/A	1
		Partial Establishment	2
		Overall Establishment & Continuous Improvement Management	3

관리적 측면에서의 평가요소는 정책, 배포, 위험 측면의 프로세스가 정의되어 있지 않은 경우, 부분적으로만 수립된 경우, 전체적으로 수립되어 지속적 개선이 가능한 경우와 같이 세 가지의 범주로 분류하여 수준을 측정할 수 있다.

최종 산출된 기술적 측면과 관리적 측면의 평가 점수는 적정하게 보정하여 결합함으로써 최종 평가 수준을 측정하도록 한다.

3.3 제로 트러스트 위험관리 방안

제로 트러스트 보안모델의 위험은 모델 자체를 구성하는 세부 컴포넌트의 다양한 설정값들에 대한 적정한 설정 관리 분야와 제로 트러스트 보안모델의 운영환경에서 발생하는 다양한 시나리오에 기반한 위험이 존재할 수 있다.

따라서 제로 트러스트를 구성하고 있는 컴포넌트들의 설정값들에 대한 표준 가이드를 수립해야 하고 이에 대한 준수 수준에 따라 위험을 산출할 수 있다. 또 다른 위험으로는 운영환경에서 발생할 수 있는 휴먼폴트, 핵심 구성요소에 대한 내·외부해킹 공격, 장애 및 재해발생 등 다양한 시나리오를 수립하여, 이에 대한 대응 수준의 척도에 따라 위험을 도출할 수 있다.

이와 같이 식별 관리되는 위험은 다양한 상황 및 행동적 특성을 반영한 문맥적 분석·관리를 통해 지속적으로 갱신관리 되어 알려지지 않은 최신 위험에 대응할 수 있도록 해야 한다.

3.4 제로 트러스트 보안모델의 배치 방안

제로 트러스트 보안모델의 배치는 기업 내·외부 인프라 구

Table 2. Control Items for Configuring a Zero Trust Security Model

Field	Control Item	Main Content
1. Identification	1.1 Subject	Identification of all individuals and corporate-owned entities that have access to the resource
	1.2 Resource	Identification of all objects (data, services, etc.) accessible by the access subject
2. Network Security	2.1 Communication Restriction	Continuous behavior evaluation and encryption transmission management based on the non-reliability principle for the subject of communication
3. Access Control	3.1 Access Control	Access permission management through situational and behavioral analysis
	3.2 Access Unit	Minimum access/validity management
4. Access Authorization	4.1 Access Range	Minimal movement path and continuous approach detection management
5. Monitoring	5.1 Security settings	Flow and security settings of subjects and resources, contextual situation monitoring
6. Dynamic Authentication/Authorization	6.1 Recertification & Reauthorization	Establishment and management of standards for re-authentication and re-authorization through continuous evaluation of access permission
7. Log Management	7.1 Collection scope	Identification and management of log scope that can be collected, such as structured and unstructured data
	7.2 Association analysis	Perform correlation analysis of collected logs Manage environment configuration

Table 3. Control Items to Improve the Zero Trust Security Model

Field	Control Item	Main Content
8. Maturity Management	8.1 Technical Aspects	Automatic/manual area identification and operation degree of data area and control area
	8.2 Administrative Aspect	Zero trust security model goal and policy establishment, infrastructure deployment review, risk management performance management
9. Deployment Strategy	9.1 Adequacy analysis of distribution and deployment structure	Continuous behavior evaluation and encryption transmission management based on the non-reliability principle for the subject of communication
10. Risk Management	3.1 Risk in the Operating Environment	Risk management based on various scenarios that may occur in operating procedures
	3.2 Risk of setting configuration values	Risk management that may occur due to problems with the settings of zero trust components

성, 서비스 특성, 클라우드 혹은 하이브리드 구성, 원격근무 환경 등에 따라 정책엔진과 정책 집행 포인트를 중심으로 다양한 컴포넌트들을 배치하는 방안을 수립하는 것이다.

3.5 제로 트러스트 보안모델의 통제항목 구성

Table 2는 제로 트러스트 보안모델 흐름도를 기반으로 제로 트러스트 보안모델을 실제 구성하기 위한 통제항목을 도출한 내용이다.

3.6 제로 트러스트 보안모델의 최적화를 위한 통제항목 구성

Table 3은 구성된 제로 트러스트 보안모델을 지속적으로 개선 및 최적화하기 위한 제로 트러스트 모델 성숙도, 위험관리 및 제로 트러스트의 인프라스트럭처의 배치 관리를 구성하기 위해 도출된 통제항목이다.

4. 결 론

본 논문에서는 4차 산업혁명의 초연결 및 코로나19로 인한 원격근무 환경 등과 같은 시대적 흐름에 부합하고 있지 못하는 전통적인 경계 기반 네트워크 보안모델을 대체하기 위하여, 제로 트러스트 사상에 기반한 보안모델 구축을 위한 전략적 방안을 제시하고자 하였다. 이를 위해 제로 트러스트의 기본원칙에 입각한 핵심 컴포넌트와 흐름을 분석하여 도식화하였으며, 이를 바탕으로 제로 트러스트 보안모델 구축을 위한 통제항목을 도출하였다.

또한 구축된 제로 트러스트 보안모델에 대한 지속적 수준 개선 및 최적화 관리를 위해 제로 트러스트 보안모델의 배치, 성숙도, 위험관리에 대한 방안도 함께 제시하였다.

향후 제시된 제로 트러스트 보안모델에 대한 타당성 검증을 위한 연구, 컴포넌트 구성요소의 효과적인 구현과 운영에 대한 세부 연구, 다양한 산업군(IDC, 전자상거래, 금융서비스, 가상자산거래 등)의 특성 및 비즈니스 시나리오를 반영한 제로 트러스트 보안모델의 배포 전략에 대한 연구가 추가 진행될 경우 보다 효과적인 제로 트러스트 보안모델이 구현될 수 있을 것으로 기대된다.

References

[1] J. Y. Lee, W. B. cho, and H. J. Jang, “A study on the establishment of information security management system based on zero trust architecture,” *Proceedings of the Annual Conference of Korea Information Processing Society Conference (KIPS) 2022*, Vol.29, No.2, pp.210-212, 2022.

[2] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, “Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust,” *Computers and Security*, Vol.110, 2021.

[3] E. S. Hosney, I. T. A. Halim, and A. H. Yousef, “An artificial intelligence approach for deploying zero trust architecture (ZTA),” *2022 5th International Conference on Computing and Informatics (ICCI)*, pp.343-350, 2022.

[4] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “NIST special publication 800-207, zero trust architecture,” *National Institute of Standards and Technology*, 2020.

[5] S. Keeriyattil, “Microsegmentation and zero trust: Introduction,” *Zero Trust Networks with VMware NSX*, 2019.

[6] R. Ward and B. Beyer, “Beyondcorp: A new approach to enterprise security,” *The Magazine of USENIX & SAGE*, Vol.39, No.6, 2014.

[7] Cybersecurity Divsion, “Zero Trust Maturity Model,” Cybersecurity and Infrastructure Security Agency, 2021.

이 진 용

https://orcid.org/0000-0003-0177-6188
e-mail : topjin55@hotmail.com
2008년 연세대학교 컴퓨터과학과(석사)
2017년 ~ 현 재 한국정보통신기술협회 디지털정보보호단 수석연구원
2022년 ~ 현 재 숭실대학교 IT정책경영학과 박사과정
관심분야 : 제로 트러스트, 블록체인, 정보보호 및 개인정보보호 관리체계, IT 및 정보보호 법률·정책

최 병 훈

https://orcid.org/0000-0003-1822-7548
e-mail : choihuni@gmail.com
2004년 숭실대학교 산업정보시스템 공학 (석사)
2022년~현 재 숭실대학교 IT정책경영학과 박사과정
관심분야 : 제로 트러스트, 정보보안, 블록체인, E-Commerce

고 남 현

https://orcid.org/0009-0009-0001-7391
e-mail : paulkoh@korea.kr
2021년 연세대학교 IT정보보호법전공 (석사)
2022년 ~ 현 재 숭실대학교 IT정책경영학과 박사과정
2022년 ~ 현 재 개인정보보호위원회 분쟁조정과장
관심분야 : 제로 트러스트, 행태정보 프로파일링, 정보호호 및 개인정보보호 관리체계, 개인정보 보호 법률·정책

전 삼 현

https://orcid.org/0009-0004-9412-748X
e-mail : shchun@ssu.ac.kr
1989년 숭실대학교 법학과(석사)
1992년 프랑크푸르트대학교 법학과(박사)
1993년 ~ 현 재 숭실대학교 법학과, IT정책경영학과 교수
관심분야 : 제로 트러스트, 블록체인, 정보보호 및 개인정보보호 관리체계, IT 및 정보보호 법률·정책